CIPHERTRACE

Cryptocurrency Anti-Money Laundering Report, 2019 Q2

CipherTrace
Cryptocurrency Intelligence
July 2019

Executive Summary

Several trends continued or accelerated in the second quarter of 2019. Outright thefts as well as scams and other misappropriation of funds from cryptocurrency users and exchanges continued apace, netting criminals and fraudsters approximately $4.26 billion in aggregate for 2019. Insider thefts were by far the largest offenders, inflecting massive losses on investors and exchange users. 2019 could also turn out to be the year of the exit scam. On top of the QuadrigaCX disaster, which is updated in this report, one alleged Ponzi scheme in this quarter appears to have defrauded millions of users out of $2.9 billion in crypto assets. Other exit scams, such as Coinroom and Bitsane, are still under investigation and those losses are not included and this report's total.

Rivalling robberies in the first quarter, hackers stole more than $124 million from exchanges and infrastructure in Q2, making a total of $227 million stolen from exchanges so far this year. In addition, $851 million was "lost" by Bitfinex. While the total dollar value of Q2 2019 thefts would currently be dramatically higher due to the recovery of cryptocurrency prices from the lows of the crypto winter, this report uses the value of the lost loot at the time of the scam or robbery. Also, these numbers reflect only the losses that CipherTrace has validated; undoubtedly more losses occurred during the quarter. In the case of the Wall Street Market takedown, the principals were prevented from completing their $11 million exit scam (also not included in this report's total) when Europol beat them to the punch by seizing that dark marketplace's crypto and fiat assets.

New FATF Travel Rule Presents Major Hurdle for Exchanges

All of these illicit funds need to be laundered, but bad actors will have a harder time doing so as tough new Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) regulations passed in 2018 are coming into effect globally over the coming months. For example, in June 2019, the Financial Action Task Force (FATF) advised member nations to begin implementing its "Travel Rule," which applies to all crypto-currency transactions over a $1,000 threshold.

The Travel Rule is a major change in regulatory requirements for Virtual Asset Service Providers (VASPs), and it is causing companies to rethink how they manage cryptocurrency transactions and identity information. It requires cryptocurrency exchanges to share sender and receiver information similar to bank wire transfers or SWIFT messaging. This requirement presents a conundrum for exhanges given the current state of cryptocurrency blockchains as it appears to fly in the face of what many see as a foundational characteristic of cryptocurrency—pseudanonymity. Devising a workable solution will require major technological innovation such as cryptographically controlled methods of securely sharing this information. Such privacy enhanced compliance would only reveal personal private details if required to do so by law enforcement.

On top of this, the US has its own travel rule under the Bank Secrecy Act (BSA), and debate about whether Convertible Virtual Currency (CVC) service providers are subject to that regulation also heated up in the second quarter. Although CVC service providers in the US are already subject to the BSA, many didn't know they were also subject to the BSA's Travel Rule. The US Treasury's Financial Crimes Enforcement Network (FinCEN) maintains that CVC service providers including, bitcoin ATMs, as well as peer-to-peer and transaction networks are subject to the regulation.

Tech Giants Looking to Go All-In On Virtual Currencies

Facebook's announced entre into the blockchain and virtual currency rocked the crypto community and legislative chambers alike. In June, the social media megaplatform's Libra stablecoin emerged from stealth mode in a bolder and more ambitious fashion than many expected. It is scheduled to debut in 2020. Facebook leadership and others promoted the positive aspects of the new "global" currency, such as bringing billions of unbanked people into the financial system. At the same time, politicians and policy makers raised concerns ranging from risks of the coin being used for terrorism financing and money laundering to difficulty in enforcing political sanctions to threats to the primacy of the US dollar. The chairman of the federal reserve noted that Facebook's sheer size means Libra would immediately have systemic implications for the global financial system. From any angle you look at it, the price appreciation of cryptocurrency and renewed interest in blockchain innovation following the announcement was hard to miss.

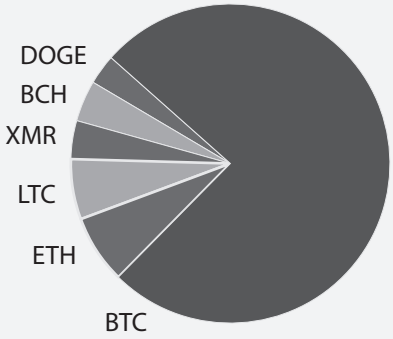
In addition, other tech Titans such as Google, Amazon and Samsung appear to be working behind the scenes on their own flavors of cryptocurrencies. Whether in Washington or European capitals, Libra raised awareness that crypto is here to stay and with major implications for the future of the global economy. It also punctuated the need for more sophisticated AML/CTF regulation as well new technologies capable of enabling compliance while preserving privacy.

Bitcoin is King in Dark Markets and Cybercrime

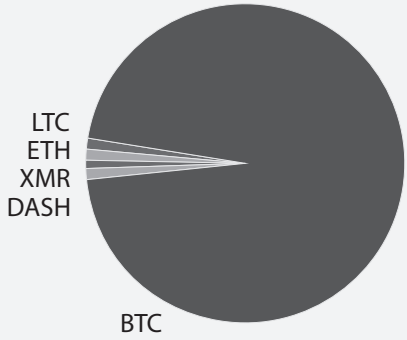
Meanwhile, governments around the world are cracking down on dark markets, which as CipherTrace research shows primarily use Bitcoin for buying and selling of illegal drugs, weapons, and cyber and banking credentials. As we have demonstrated in previous research, a very small portion of the total bitcoin transactions are directly used to conduct criminal activities. However, it is also true that nearly all dark market commerce is transacted in cryptocurrencies.

With another supposed trend being the increasing popularity of privacy coins, especially for illicit activities and sidestepping of AML/CTF regulations, CipherTrace researched the use of various cryptocurrencies—ETH, LTC, XMR, BCH, and even DOGE—in dark markets and in malware/ransomware attacks. The results show that privacy coins are barely used in dark markets and at dark vendor sites (e.g., only 4% of instances involve Monero (XMR). Instead, Bitcoin remains the coin of the realm in this shady world with BTC used in 76% of dark market cases and ETC used in only 7% of instances. In the case of malware and ransomware, the dominance of Bitcoin is even more striking with ETH used in only 1% of instances and BTC used in 98% of cases.

Dark Web & Deep Asset Usage



Malware and Ransomware Asset Usage



What this suggests is that while privacy coins may seem like a boon to criminals, drug gangs and terrorists, the barriers to entry for buying and selling Monero and other anonymous tokens makes them impractical for most dark market purchases and ransomware payments. They are most useful as a payment rail and to obfuscate chain hopping to more liquid tokens. In addition, as regulators around the world implement the FATF's travel rule there will probably be fewer exchanges willing to trade privacy coins due to their ability to anonymize the two parties in a cryptocurrency transaction.

Q2 Highlights

- *Thieves and scammers stole more than $4.26 billion from cryptocurrency exchanges, investors, and users in the first half of 2019.*
- *Users and investors lost approximately US$2.9 billion as "South Korean" Plus Token app and exchange went offline; Chinese police arrested six Chinese nationals in Vanuatu as the alleged perpetrators.*
- *Hackers used advanced cyberattack to steal $44 million from world's largest cryptocurrency exchange, Binance.*
- *Update from Canadian court on QuadrigaCX collapse reveals long history of misappropriation of user funds by QuadrigaCX founder.*
- *Japanese exchange BITPoint hacked for $30 million.*
- *BestMixer mixing service seized by law enforcement authorities.*
- *European authorities seized three dark web markets and assets.*
- *CFTC charged Control-Finance in $147M Ponzi scheme.*
- *Facebook shook up crypto economy and woke up policy makers with Libra announcement.*
- *SIM Swapping victim won $75.8 million judgement against hacker.*
- *More sophisticated exchange hacks used advanced simultaneous takeovers of user and admin accounts.*
- *SEC sued Kik over $100 million unregistered ICO.*
- *CipherTrace research shows Bitcoin still dominates payment method in dark markets despite advent of privacy coins.*
- *Hack may have caused Bitcoin flash crash on Kraken.*
- *European authorities made arrests in two major typosquatting scams that cost exchange users tens of millions.*
- *$23 million in Bitcoin lost and co-owner found dead after Polish exchange Bitmarket shutters due to "liquidity issues.*
- *Iran accused US of attempting to block its virgin Bitcoin as means to compensate for financial hit from sanctions.*
- *UN published report on North Korean government hackers stealing $571 million from Asian exchanges to fund WMD and compensate for sanctions.*

Major Trends And Developments

Advanced Attacks Simultaneously Takeover Account Holder and Exchange Admin Credentials

Despite increased awareness of the risk of exit scams and more emphasis on cybersecurity at exchanges designed to prevent hacks, both continue relatively unabated. This is because exchanges and users are facing a greater sophistication in the tactics, techniques and procedures (TTPs) cybercriminals are using to target the cryptocurrency space. In the case of exchange robberies, hackers have developed advanced methods to overcome even the current "best practice" security in place at the more vigilant exchanges. These include simultaneous takeovers of inside and outside user credentials to defeat security controls.

Advanced Persistent Threats and Blended Attacks Target Cryptocurrency Businesses

For example, many breaches involve blended attacks in which the hacker employs multiple techniques—including SIM Swapping, Phishing, etc.—against multiple targets to take over accounts of users and an administrator. These increasingly are pulled off with the assistance of a compromised insider. The hacker can then suppress security alerts or notifications. In the case of SIM Swapping, users cannot receive alerts because once their phone numbers are switched to the hacker's SIM they suddenly have no voice, email, or SMS service on their phones. As a result, both end users and exchange IT staff are unaware of these highly unusual transfers until the thieves have made off with often millions of dollars in cryptocurrency.

Coordinated Phishing and URL Hijacking Attacks Target Users and Exchanges

Cybercriminals use typosquatting, also known as URL hijacking, to drive victims to clones of well-known websites such as crypto exchanges. Criminals intentionally purchase domain names that are similar to the authentic site's, but have different spellings (e.g., yahooo.com vs yahoo.com) in the hopes of trapping users who make typos. It's also common for typosquatters to use phishing emails or other means to distribute links with intentional typos that lead to the counterfeit sites, assuming recipients will not notice the misspelling.

Facebook Rattles the Blockchain and Governments by Announcing its Own Global Cryptocurrency

On the heels of months of rumor, Facebook announced on June 18 that it is officially in crypto. In a nutshell, the social media giant plans to roll out a stablecoin called Libra. It appears Facebook has been incubating this virtual currency for some five years under great secrecy since the company recruited former PayPal president David Marcus to run its Messenger app. Facebook subsequently asked Marcus—also an expert in the blockchain and an advisor to cryptocurrency exchange Coinbase—to run a new blockchain group. The Libra token was designed and coded by Facebook. Calibra, a Facebook subsidiary based in the US, will act as the Libra wallet provider and payment processor. Meanwhile, unlike Bitcoin which runs on a decentralized public blockchain, Libra will be run on a centralized private blockchain. The Libra Association, a nonprofit also based in Switzerland, will act as the coin's central authority, be responsible for managing the Libra reserves, and make decisions about how the network operates.

The news seemed to awaken a giant that had been sleeping through the crypto winter, as the price of Bitcoin—which had already begun to recover—marched more than 40 percent higher within weeks. Suddenly, it seemed that cryptocurrency and everything blockchain were in vogue again.

Washington Wakes to Concerns Over Everything from Money Laundering to the Supremacy of the US Dollar

The news also roused Washington. And not surprisingly, because now the rumors became real that a Silicon Valley company with massive influence around the globe actually wanted to have its own money. The Wall Street Journal's Paul Vigna commented that "before Facebook's announcement it was hard to find anybody in Congress who really cared all that much about cryptocurrency." After the Libra announcement that quickly changed. The House Financial Services Committee and the Senate Committee on Banking, Housing and Urban Affairs scheduled hearings with Facebook in July to discuss their concerns.

Major worries for those on in Washington included how Libra could potentially impact the US dollar's status as the world's reserve currency and the US government's ability to impose effective sanctions. "Libra raises many serious concerns regarding privacy, money laundering, consumer protection and financial stability," US Federal Reserve Chairman Jerome Powell said during his semi-annual testimony on monetary policy before the US House of Representatives Financial Services Committee on July 10th. "The size of Facebook's network means it (Libra) will be, essentially, immediately systematically important." He added that Facebook's plan to build a digital currency "cannot go forward" until these concerns are addressed. During the congressional inquiry, Marcus, who now leads Calibra, seemed ready to head off this initial skepticism, stating that the coin will not launch until Facebook has "fully addressed regulatory concerns."

Marcus further emphasized the inevitability of blockchain technology and stated that the US needs to lead

in building and regulating it. Otherwise, the innovation will come from other countries "out of reach of [the US] national security apparatus."

Puts Renewed Focus on Virtual Currency Regulation Globally

Congress also raised concerns that Facebook's enormous global user base makes Libra more likely to disrupt global finance than other virtual currencies, heightening the need for regulatory oversight. The fear being criminal and terrorist organizations will seek to take advantage of Facebook's vast network. This makes compliance with AML and CTF regulations more important than ever. Even Treasury Secretary Steven Mnuchin weighed in on July 15th, saying Facebook's proposed digital currency "could be misused by money launderers and terrorist financiers."

Since the congressional hearings, The UK's Financial Conduct Authority has also warned Facebook that it would not authorize Libra's use without close scrutiny. France as well announced that it is creating a G7 task force to examine how central banks can regulate virtual currencies like Libra.

However, according to Facebook's press release, Calibra "will have strong protections in place" and will use "all the same verification and anti-fraud processes that banks and credit cards use" such as "automated systems that will proactively monitor activity to detect and prevent fraudulent behavior." Nevertheless, anti-fraud does not equate to anti-terrorism or anti-money laundering. This means new types of monitoring systems must be developed to secure the Libra blockchain from bad actors. This is especially important in regard to unvetted third-party developers using the Libra network. The whitepaper claims "open access ensures low barriers to entry and innovation and encourages healthy competition that benefits consumers." But poor vetting on third-party applications on the Facebook platform is exactly what led to the Cambridge Analytica scandal of 2018.

Facebook Claims Small Businesses and 1.7 Unbanked People Will Benefit

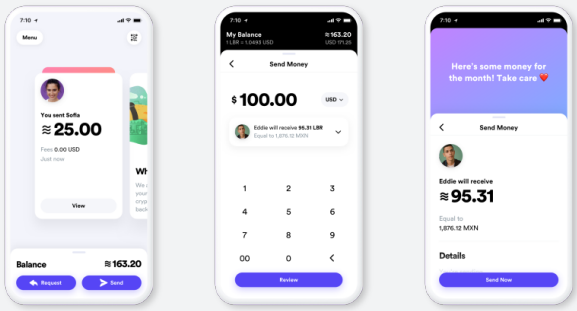
Nonetheless, the whitepaper strongly champions the benefits of Libra, such as giving the unbanked masses a leg up into the financial system. Libra's mission, according to the whitepaper, is to "enable a simple global currency and financial infrastructure that empowers billions of people." Despite the technological advancements of the last decade," 1.7 billion adults globally remain outside of the financial system with no access to a traditional bank, even though one billion have a mobile phone and nearly half a billion have internet access."

"When people are asked why they remain on the fringe of the existing financial system, those who remain "unbanked" point to not having sufficient funds, high and unpredictable fees, banks being too far away, and lacking the necessary documentation."

–Libra Whitepaper

"For many people around the world, even basic financial services are still out of reach: almost half of the adults in the world don't have an active bank account and those numbers are worse in developing countries and even worse for women," according to the official Calibra announcement. "The cost of that exclusion is high—approximately 70% of small businesses in developing countries lack access to credit and $25 billion is lost by migrants every year through remittance fees."

"With Libra, anyone with a $40 smartphone and connectivity will have the ability to securely safeguard their assets, access the world economy, transact at a much lower cost, and over time access a whole range of financial services," Marcus wrote in an early July blog post in which he attempted to clarify Facebook's goals: "We firmly believe that if Libra is successful, it can be a non-linear step change for billions of people who need it the most."



Multinationals Buy into the Libra Association

The potential for Libra to make a huge impact on global finance could rest on not only Facebook's massive user base but also ease of adoption of the Calibra wallet. The sneak preview screens above, which are taken from Facebook's announcement, reveal an experience not unlike PayPal or Venmo with the current complexity of transacting cryptocurrencies essentially made transparent to the end user. The announcement says that in time "we hope to offer additional services for people and businesses, like paying bills with the push of a button, buying a cup of coffee with the scan of a code or riding your local public transit without needing to carry cash or a metro pass." Notably, as a stablecoin, Libra would be well-suited for these purposes as it would eliminate the volatility currently associated with cryptocurrencies. Every dollar a user puts into Libra would correspond to a basket of assets and currencies that would theoretically back the token 1 to 1.

Concern was also voiced over the corporatization of global finance. Similar to other permissioned blockchains such as Ripple, Libra's central authority will determine who may act as transaction validator on their network. The plans call for companies to buy a voting share of control for 10 million dollars. Thus far, only members of the Libra Association will be allowed to run nodes and validate transactions, but Facebook says it aims for Libra to eventually become completely permissionless. Primarily, large multinational corporations such as Visa, PayPal, Uber, Lyft, Spotify and eBay make up the Libra Association. For a business to be a member, it must meet at least two of the following criteria: have more than $1 billion USD in market value or greater than $500 million USD customer balances; reach greater than 20 million people a year, multinationally; or be recognized as a top-100 industry leader by a third-party sector-specific association or media company. For every 10 million dollars invested into Libra, the association member receives one vote on the Libra Council.

In an interview with Endgadget, Calibra Marcus stated, "by the time we launch, [Calibra] will only have one percent of the vote." However, according to Visa CEO Alfred F. Kelly Jr., no companies have officially joined Libra yet. Instead they have only declared interest via a nonbinding letter of intent.
Unlike open, decentralized blockchains like the Bitcoin blockchain, Libra will be run on a centralized, permissioned blockchain with the Switzerland-based Libra Association responsible for managing the Libra

reserves. Similar to other permissioned blockchains such as Ripple, Libra's central authority will determine who may act as transaction validator on its network. As currently designed, only members of the Libra Association will be allowed to run nodes and validate transactions, but Facebook says it aims for Libra to eventually become completely permissionless. According to its website, the association currently has 28 members but hopes to grow to over 100 by launch.

Libra's centralized model raises another concern voiced by legislators, that Libra might not be censorship-resistant. This is an issue that has gained headlines recently, ranging from Google preventing politicians from buying ads to PayPal blocking ecommerce sites that it deems offensive to YouTube demonetizing channels.

Exchange and Infrastructure Thefts Top $480 million in 2019

Japanese Exchange BITPoint Hacked for $30 million

On July 12, the Japan-based exchange BITPoint announced it was hacked for $32 million in crypto assets, $23 million of which were customer funds. Three days later, BITPoint announced that the original hack was closer to $28 million while disclosing an additional $2 million stolen from from exchanges using Bitpoint's trading platform outside of Japan, bringing the total to $30 million. The stolen assets include Bitcoin, XRP, Ether, Litecoin and Bitcoin cash. The exchange has since suspended all services, including withdrawals, trading and deposits as it investigates the matter.

Japan's Financial Services Agency (FSA) had previously taken administrative action against BITPoint. In June 2018, the FSA ordered the improvement of BITPoint business operations after on- and off-site inspections found that the exchange had no effective internal control systems established for AML/CTF, user protection, and system risk management. They gave the company until July 23, 2020 to submit an improvement plan.

It's possible that yet another large cryptocurrency exchange hack—especially one impacting an exchange found lacking in controls—in a country that has suffered some of the world's largest hacks may cause Japanese regulators to rethink their experiment with self-regulation.

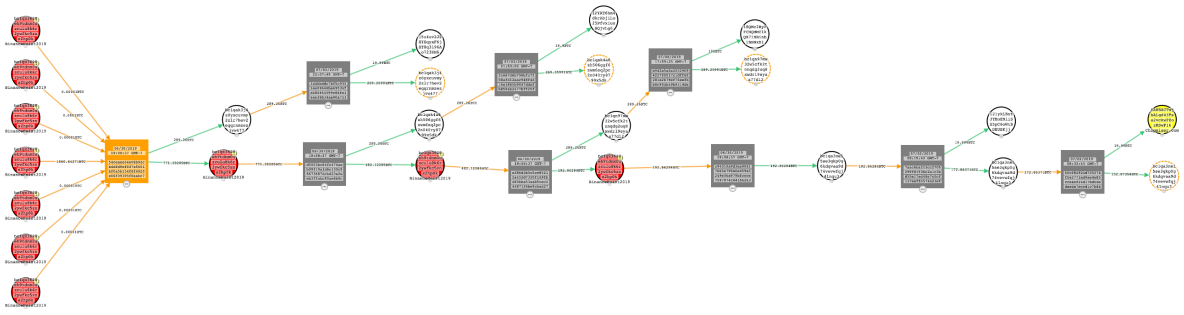
On July 16, the president of BITPoint Japan Co. held a news conference in Tokyo where he claimed the company would reimburse affected customers in cryptocurrency, according to the Japanese news outlet the Asahi Shimbun.

Hackers Steal $40 Million in Crypto from Binance

In May, hackers stole 7,074 bitcoins (worth US$40 million at the time (now $80M) from the world's number-one cryptocurrency exchange, Binance. From what is known by CipherTrace researchers, hackers used a multi-pronged takeover attack to obtain API keys, two-factor authentication codes, and other personal information from a large number of users, including "very high net worth accounts." API keys are unique identifiers that traders use to grant third-party programs special privileges to users' accounts, which often bypass two-factor authentication.

"The hackers used a variety of techniques, including phishing, viruses and other attacks," according to Binance CEO Zhao Changpeng who reported the theft on the same day it was discovered. "The transaction is structured in a way that passed our existing security checks." By the time Binance was able to suspend withdrawals, the hackers had already gotten away with the millions in cryptocurrency.

Zhao also announced that no customer funds would be used to cover losses, as Binance had set up a self-insurance fund, the SAFU fund, in 2018 that accrues 10% of all trading fees in a separate cold wallet.



The screenshot above shows how CipherTrace researchers followed the money as the perpetrators progressively split their haul into smaller and smaller amounts before sending it to a money laundering service to further cover their tracks. In money laundering terms, this stage is known as *layering*.

Recently, the thieves have begun to move some of the stolen bitcoin. The CipherTrace UI shows 1060 stolen Binance BTC begin to move on June 30, having been systematically peeled into large slices (289.26 increments) and small slices (19.99 BTC increments). Only 100 bitcoin remained on the move after July 2. The final (yellow) transaction shows a small amount—19.99 BTC ($216,774)—sent to Chipmixer for obfuscation (mixing) so they could be integrated into the financial system and made available to the criminals as clean bitcoin. In money laundering terms, using the newly "clean" bitcoin to purchase assets or make payments is known as integration.

Two Israeli Brothers Steal Tens of Millions in Typosquatting Scam

On June 21, two Israeli brothers were arrested for a phishing scam spanning three years, during which they stole tens of millions of dollars in crypto. The scammers used "typosquatting" (also known as URL hijacking) to mirror crypto exchanges and wallets. Unsuspecting users would sign in to the fake account, giving the brothers access to account details and private keys to the real sites. Links to their faux website were distributed over a variety of platforms and chatrooms frequented by cryptocurrency traders.

The two brothers are also allegedly responsible for the 2016 Bitfinex hack. Interestingly, the Bitfinex hack-

er's wallet saw movement this June 7 as nearly $1.5 million worth of BTC was transferred to an unknown wallet. Whether this timing has anything to do with the hackers' arrest is still unknown.

Six Arrested in UK and Netherlands over $27M Typosquatting Scam

A few days later, on June 24, authorities in the UK and Europe arrested six people for using typosquatting schemes to steal a total of $27 million from more than 4,000 victims in at least 12 countries. The huge crypto crime sweep involved the UK's South West Regional Cyber Crime Unit (SW RCCU) in a joint operation with the Dutch police (Politie), Europol, Eurojust and the UK's National Crime Agency (NCA).

Hack Suspected as Cause of Kraken Bitcoin Flash Crash

On June 2, Bitcoin flash-crashed on a major Bitcoin trading platform Kraken. The near vertical drop from $11,200 CAD to $100 CAD within moments initially appeared to have resulted from a technical glitch or a fat-fingered trading error by a whale. However, further analysis appears to point towards a clever hack and perhaps an ingenious new form of money laundering.

As has been stated in previous CipherTrace reports, pulling off a successful robbery is only the first phase in stealing cryptocurrency from an exchange. The cybercriminals must still make their getaway. To avoid detection by law enforcement, hackers must somehow launder the stolen cryptocurrency and find an exit ramp into the traditional financial system so they can use the loot as clean fiat to purchase things in the real world. In this case, the available evidence suggests a hacker compromised a whale's account, stole 1200 BTC worth $10.45 million on that date, and then dumped this huge amount of BTC into a highly illiquid BTC/CAD market (compounded by the fact it was on a Friday afternoon). It then appears the same hacker scooped up a similar number of BTC at the bottom of the engineered flash crash with buy orders placed at $100 shortly before the hacked funds were sold as a "market" order.

$10 Million in XRP Stolen from GateHub

On June 1, Ripple (XRP) wallet provider GateHub suffered a security hack in which 23.2 million XRP were stolen from over 103 user wallets, although over 18,000 total accounts may have been affected. According a statement by GateHub, hackers penetrated the wallets after gaining access to a database that contained valid customer access tokens. These credentials essentially tell a server who the users are and keep them logged in. When a user logs out, the access token is destroyed, and the user must log back in to receive a new one. Broken authentication such as compromised access tokens is number two on the OWASP's top 10 attack vectors.

The GateHub team is still investigating the issue, but they believe the hackers found an exploit in their API to support the attack. During the breach, GateHub detected an increased number of API calls (with valid access tokens) coming from a small number of IP addresses. XRP Forensics, a team dedicated to protecting the XRP ledger, has identified 12 potential suspects.

GateHub contacted all affected wallet holders, urging them to immediately transfer their remaining funds

to a GateHub-hosted wallet while it completes its investigation. However, hackers used this as an opportunity to steal more user funds through a typosquatting phishing scam by repeating the email to customers from @gatehub.com (a cloned counterfeit domain) rather than the legitimate @gatehub.net.

The company has since recovered over 500,000 XRP (around US $150,000 at current prices).

Singapore Exchange Bitrue Hacked for More than $4 Million

On June 27, the Singapore exchange Bitrue was hacked for around $4.2 million in user assets — 9.3 million Ripple (XRP) and 2.5 million Cardano (ADA), at the time worth $4.25 million and $225,000, respectively. According to the exchange's public statements, hackers exploited a vulnerability in its "Risk Control team's 2nd review process to access the personal funds of about 90 Bitrue users." Bitrue also announced "100% of lost funds will be returned to users" and the exchange is reviewing "security measures and policies to ensure this does not happen again." The exchanges Huobi, Bittrex and ChangeNOW have since frozen assets and accounts with funds received in relation to the hack.

2019 the Year of the Exit Scam

Massive PlusToken Wallet Ponzi Scheme Impacts 2.4 Million Users

US$2.9 billion worth of deposits appear to have been lost when Chinese police broke up an alleged Ponzi scheme involving the purportedly South Korea-based crypto wallet and exchange, PlusToken. It is unknown how many people were affected, but PlusToken claimed to have between 2.4 and 3 million users/investors.

CipherTrace has not definitively confirmed this apparent fraud or exit scam. The details of who was behind PlusToken and where its custodial funds went are currently shrouded in a mystery involving Chinese nationals, Chinese police, the government of Vanuatu, and the two supposed co-founders—a Russian known only as "Leo" and South Korean who uses the name "Kim Jung Un." If confirmed, it would be the largest such loss ever, dwarfing even the US$600 million exit scam pulled off last year in Vietnam (See CipherTrace Q3 2018 Cryptocurrency AML Report).

The wallet required users to download an app through which they could deposit crypto and also invest in PlusToken (PLUS). The company claimed the PlusToken coin, which is based on the Ethereum blockchain was developed by the core team of a major technology company. The wallet reportedly held Bitcoin, Ethereum, Bitcoin Cash, Litecoin, XRP, DOGE coin, Dash coin, and PLUS coin (the native cryptocurrency of Plus Token). Users accessed the wallet through a mobile app and could trade online at the PlusToken exchange website, pstoex.com. Both were not functioning at the time of this report. However, a copy of the whitepaper is still on LinkedIn **https://www.slideshare.net/ArnoBalzer/white-paper-plus-token .**

A Crypto High Yield Investment Product

Popular in Asia

PlusToken appears to have been a popular in Japan, South Korea and China, and the company claimed it would have 10 million users by July 2019. Typical of a HYIP (High Yield Investment Product), the astounding user growth (if they truly had some 3 million users) stemmed from advertising huge returns. Specifically, PlusToken and its affiliates claimed that even in weak crypto market by using arbitrage among various cryptocurrencies (enabled by a bot called AI-Dog) and cloud crypto mining they could deliver wallet holders an ROI of between 8 and 16 percent each month, which was paid out in PLUS. Users were required to deposit a minimum of US$500 worth of crypto assets to participate.

Source: Business Wire Press Release
https://www.businesswire.com/news/home/20190211005506/en/

PlusToken members could also make money by bringing new users into a multi-level marketing program typical of a pyramid scheme. In fact, new users could only join by through invitation from an existing PlusToken holder. However, it appeared there was no verifiable source of business revenue other than proceeds from new membership.

Meeting with Prince Charles Lends Credibility

All of this led to multiple warnings in the crypto community that PlusToken was a scam. The company's founder publically dismissed those reports. However, after a company press release, replete with photos, claimed that in February, 2019 Leo had met with England's Prince Charles at an Invest in Futures event hosted by the prince's charitable foundation, PlusToken gained some newfound credibility. "Leo and Prince Charles had intimate talks on how the blockchain serves economic society, according to a press release promoting a new PlusToken exchange. Also, he put forward valuable advice on the development of future blockchain-related bills issue in the UK. Besides, Leo donated at the charity dinner generously and won a lot of complement."

With today's potential for deep fake photos, CipherTrace researchers reached out to the Prince Charles Foundation to validate the authenticity of the photos. The Foundation confirmed "Leo" had in fact attended the dinner, however staff were not willing to provide other information, such as his last name, due to concerns over the GDPR.

Alarm Bells Go Off in June as "Technical Difficulties" Prevent Users from Withdrawing Funds

In late June, PlusToken users began to experience trouble withdrawing custodial crypto assets. On June

On June 28, 2019, Chinese police arrived on Vanuatu and arrested the "Plus Token Six" for running an "internet scam." The Island's government allowed China to almost immediately extradite the six—who were either Vanuatu citizens or applying for citizenship—back to the mainland.

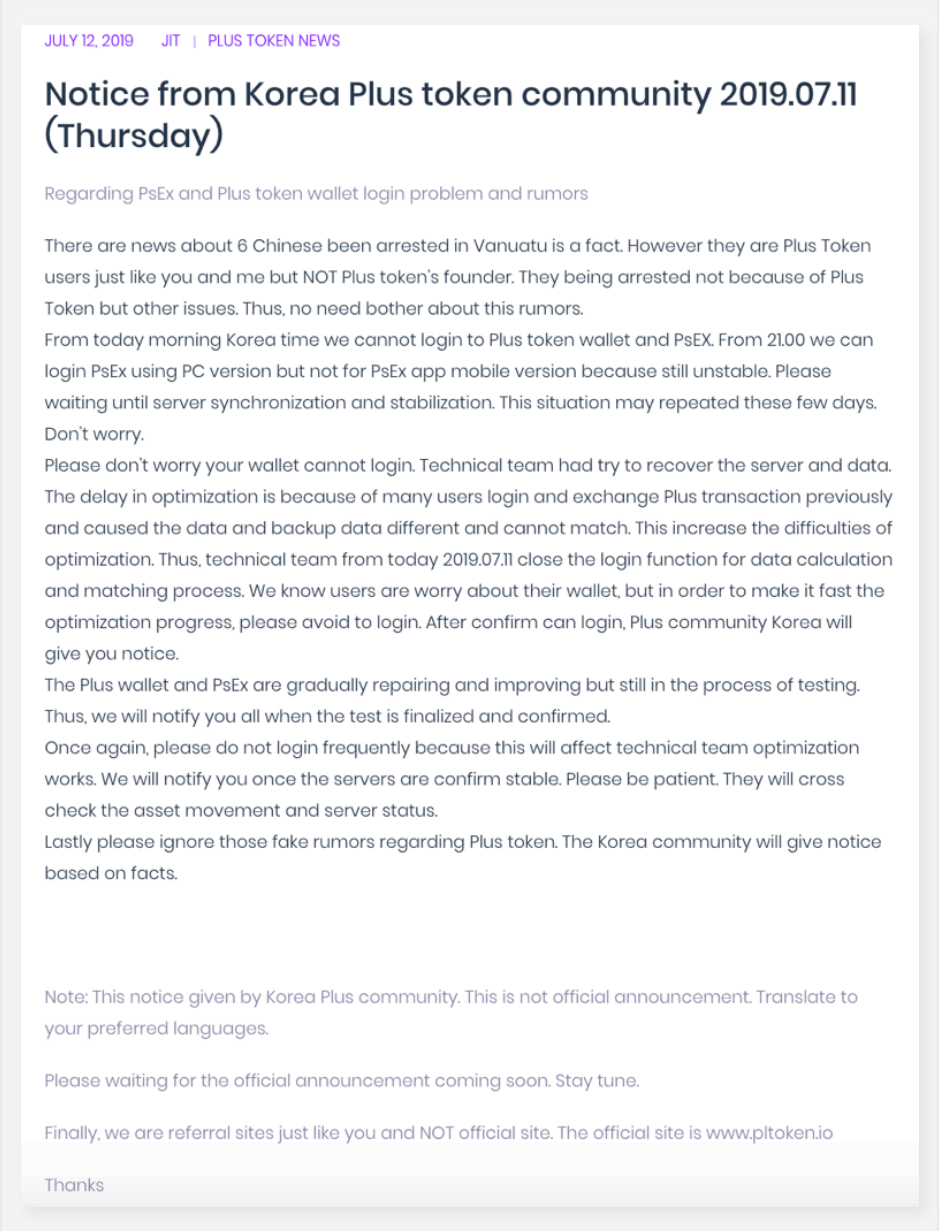
users found that withdrawals on the PlusToken app were frozen due to alleged "technical difficulties," but by June 29 the PlusToken app had completely shut down due to alleged "system maintenance." This caused great concern among the PlusToken Community.

"The PlusToken Six"

Also on June 29, Hong Kong's leading newspaper, the South China Morning Post, reported that six Chinese nationals wanted by Beijing for operating an internet scam were arrested on the Pacific island of Vanuatu and extradited back to China. Vanuatu law enforcement and immigration authorities along with Chinese police raided a property where the six were conducting their operation. Subsequently the Chinese tech news agency 36Kr claimed to confirm that the "internet scam" reported by the Post was, in fact, PlusToken. Specifically, the arrests were for running a multi-level marketing company (pyramid scheme). As reported by the New York Times, China has been making a major crackdown on such business models, including Amway and Herbalife.

On July 12, a PlusToken community website responded to the incident, claiming the six arrested in China were PlusToken users and not associated with the company, and "Thus, no need bother about this rumors (sic)." The statement further claims that withdrawals remain restricted because the server is still unstable and urges users to wait "until server synchronization and stabilization" and not to worry if they cannot log in because its technical team is trying to recover the server and data. The statement then asks users to stop trying to log in until they receive confirmation that the severs are back up.

This was not the first time PlusToken has warned users not to believe "rumors." In October 2018, after news started circulating in China that PlusToken was being investigated for violating Chinese regulations and engaging in fraudulent activity, the company's co-founder, Leo, posted a video on YouTube https://



JULY 12, 2019 JIT | PLUS TOKEN NEWS

Notice from Korea Plus token community 2019.07.11 (Thursday)

Regarding PsEx and Plus token wallet login problem and rumors

There are news about 6 Chinese been arrested in Vanuatu is a fact. However they are Plus Token users just like you and me but NOT Plus token's founder. They being arrested not because of Plus Token but other issues. Thus, no need bother about this rumors.
From today morning Korea time we cannot login to Plus token wallet and PsEX. From 21.00 we can login PsEx using PC version but not for PsEx app mobile version because still unstable. Please waiting until server synchronization and stabilization. This situation may repeated these few days. Don't worry.
Please don't worry your wallet cannot login. Technical team had try to recover the server and data. The delay in optimization is because of many users login and exchange Plus transaction previously and caused the data and backup data different and cannot match. This increase the difficulties of optimization. Thus, technical team from today 2019.07.11 close the login function for data calculation and matching process. We know users are worry about their wallet, but in order to make it fast the optimization progress, please avoid to login. After confirm can login, Plus community Korea will give you notice.
The Plus wallet and PsEx are gradually repairing and improving but still in the process of testing. Thus, we will notify you all when the test is finalized and confirmed.
Once again, please do not login frequently because this will affect technical team optimization works. We will notify you once the servers are confirm stable. Please be patient. They will cross check the asset movement and server status.
Lastly please ignore those fake rumors regarding Plus token. The Korea community will give notice based on facts.

Note: This notice given by Korea Plus community. This is not official announcement. Translate to your preferred languages.

Please waiting for the official announcement coming soon. Stay tune.

Finally, we are referral sites just like you and NOT official site. The official site is www.pltoken.io

Thanks

On July 12, a notice appeared on the Plus Token website urging users and investors to ignore reports of arrests of Chinese nationals who were named as perpetrators of a Plus Token internet scam, while also attempting to explain away users inability to log in and access their funds in the Plus Token wallet.

www.youtube.com/watch?v=r3RTwNvgMu8 shot in his "hometown" of Kazan, Russia, telling users to "not pay attention to any haters."

On July 10, China's Yuncheng Public Security Bureau told the Daily Planet Daily that the case is still under investigation and that there are suspects that have since fled. As of the release of this report, Plus Token's official site, pltoken.io, also appears to be down with the last archive in archive.org occurring on July 1, 2019.

The case has even raised political concerns in the South Pacific, Australia and New Zealand regarding the increasing influence of China. The local newspaper reported that the rapid extradition of people who were either citizens of Vanuatu or applying for citizenship showed how the government bent to the will of the Chinese, and may have confirmed fears that Chinese intelligence was operating covertly in the country. "When they arrived in Vanuatu, Chinese law enforcement provided critical information to Vanuatu police concerning the PlusToken scammers. They not only knew their names; they knew where they lived," said a report in Vanuatu's Daily Post.

This also raises issues for international regulators and cryptocurrency users as to the 3-billion-dollar question: there is no word from the Chinese authorities on the fate of the missing user funds. Certainly this "exit scam" warrants further investigation, because unlike similar cryptocurrency frauds, it is not clear that insiders made off with the loot. CipherTrace will provide updates if available in next quarter's report.

On July 12, PlusToken responded to the incident on its website, claiming the six Chinese nationals arrested in Vanuatu were PlusToken users and not associated with the company, and "Thus, no need bother about this rumors [sic]." (See screenshot above). The statement further claims that withdrawals remain restricted because the server is still unstable and urges users to wait "until server synchronization and stabilization" and not to worry if they cannot log in because its technical team is trying to recover the server and data. The statement then asks users to stop trying to log in until they receive confirmation that the severs are back up. As of now there are no further updates.

Polish Exchange Coinroom Exit Scams with Customer Funds

The Polish exchange CoinRoom appears to have executed an exit scam in April, walking away with an undetermined amount of customer funds. The exchange sent a message to users explaining its was terminating their contracts and gave them one day to withdraw funds. The company stated that after the 24-hour window users would need to request withdrawals by sending an email directly to the CoinRoom Support team. Thousands of customers still have yet to receive requested funds or have reported only partial reimbursement. Subsequently, the exchange vanished: completely stopped responding to withdrawal requests and shuttered its website.

Customers took the Polish-based company to court and reported losses as high as $15,000 per account to the local prosecuter's office. Since the initiation of the lawsuit, CoinRoom has restored its website and offered an explanation of the reimbursement issues. The company outlined plans to file bankruptcy and says it will cooperate with authorities to clarify the situation. CoinRoom also stated "we have returned a large part of the funds to our clients," but added that the issue may take months to resolve.

Irish Cryptocurrency Exchange Bitsane Exit Scams 246,000 Users

In May, Bitsane users found that the exchange "temporarily disabled" withdrawals due to "technical reasons."

However by June 17, Bitsane had taken its website offline and deleted all social media accounts. Emails to the support team bounced back with failure notices. The exact amount of user assets is still under investigation, but the exchange was known to trade in BTC, LTC, ETH, XRP and more. Inability to withdraw funds or a website going down because of technical difficulties seems to be an early symptom of an exit scam.

Report on QuadrigaCX Reveals Long-running Fraud

Ernst & Young (EY), the court-appointed monitor in the QuadrigaCX insolvency case, released its explosive fifth report in June, and it is filled with damning details regarding the fiasco that cost the exchange's users US$195 million in lost crypto assets. See the CipherTrace Q1 2019 Crypto AML Report for a synopsis of the events surrounding the sudden collapse of what had been Canada's largest cryptocurrency exchange following the death of its 30-year-old co-founder and CEO, Gerald Cotten.

According to the new report, Cotten had allegedly committed gross improprieties and used customer funds for years to enrich himself and his wife (then girlfriend), Jennifer Robertson. Significant volumes of customers' cryptocurrency were transferred off the Quadriga platform and into accounts on competitor exchanges controlled by Cotten. Quadriga customers' cryptocurrencies were then either traded on these exchanges or used as security for a personal margin trading account established by Cotten. Quadriga's cryptocurrency reserves ultimately suffered due to his trading losses as well as incremental fees charged by these competitor exchanges.

In addition, "Mr. Cotten created Identified Accounts under aliases where it appears that Unsupported Deposits were deposited and used to trade within the Platform resulting in inflated revenue figures, artificial trades with Users and ultimately the withdrawal of Cryptocurrency deposited by Users," according to the report. Here "Unsupported Deposits" means they were fabricated and not represented by actual fiat or cryptocurrency. According to the Monitor, Cotten used his administrative privileges to credit his alias accounts with a significant amount of fiat and cryptocurrency, but only about 1% of these deposits were supported by any documentation. Moreover, as the Super Admin, Cotten suppressed the logging of all of his activities.

Platform outside Quadriga to competitor exchanges into personal accounts controlled by Mr. Cotten. It appears that User Cryptocurrency was traded on these exchanges and in some circumstances used as security for a margin trading account established by Mr. Cotten. Trading losses incurred and incremental fees charged by exchanges appear to have adversely affected Quadriga's Cryptocurrency reserves. In addition, substantial amounts of Cryptocurrency were transferred to wallet holders whose identity the Monitor has been unable to confirm."

Ernst and Young, Fifth Monitor's report to Supreme Court of Nova Scotia

For those unfamiliar with the events surrounding the implosion of QuadrigaCX, in December, 2018, Cotten travelled to India with his wife where he allegedly died from a gastrointestinal disorder. According to his wife, whom he had married days prior, he took with him to the afterlife or elsewhere, the passwords and keys to accounts that rendered all the assets of the exchange inaccessible. After being unable to redeem custodial funds, the exchange's users learned from an online posting that their crypto assets were supposedly locked up forever. The cryptocurrency community was shocked to learn weeks after Cotten's alleged death that the passwords to more than $200 million CAD in crypto could have been in only one person's possession with no backup.

As CipherTrace reported earlier, other details known at the time pointed to potential foul play and misappropriation of user funds. In fact, the 70 pages of the Fifth Monitor's Report reads as a remarkable litany of financial malfeasance, nonexistent internal controls or accounting records, personal use of exchange assets, and what appear to be misappropriation of funds crimes perpetrated upon the exchange's users by Cotton, his wife and perhaps others.

Specifically, Ernst and Young reports that Cotten misappropriated funds by:

- Using customer funds to pay for QuadrigaCX operating costs without ensuring sufficient funds remained

to support customer fiat balances
- Accepting "cash deposits" and crediting customer accounts without proper controls or accounting to ensure the cash appropriately deposited into third-party payment processor accounts
- Using third-party exchanges to hold customers' cryptocurrencies
- Exposing customers to incremental fees and trading losses by converting cryptocurrencies off-platform
- Using customer funds as security for speculating in off-platform margin accounts (essentially, it appears he was gambling and also using customers' funds to meet margin calls due to losing bets)
- Trading unsupported deposits for real funds and generating artificial trading markets
- Engaging in significant "cash" transactions (the Monitor has been unable to verify if cash deposits were ever deposited into accounts containing User Funds and/or properly recorded)
- Using currency conversion services to trade customers' cryptocurrency holdings
- Transferring customer funds to Cotten's personal accounts
- Used his admin privileges to override KYC requirements
- Using customer funds to purchase personal assets

Earnst and Young also essentially said that Cotten treated Quadriga's user funds like a personal bank account, identifying significant transfers of fiat to Cotten and his wife, Jennifer Robertson. The two took expensive vacations, made use of private jets, and bought numerous properties. The assets they accumulated—including real estate, cash, an airplane, a sailing yacht, luxury vehicles, and gold and silver coins—had a value of approximately CAD $12.0 million.

Finally, the report addressed the significant flaw in Quadriga's operating infrastructure that initially grabbed headlines around the word. "In addition, the Monitor understands passwords were held by a single individual, Mr. Cotten and it appears that Quadriga failed to ensure adequate safeguard procedures were in place to transfer passwords and other critical operating data to other Quadriga representatives should a critical event materialize (such as the death of key management personnel)."

CFTC Charges Control-Finance in $147M Ponzi Scheme

On June 18, the US Commodity Futures Trading Commission (CFTC) announced it had initiated a civil enforcement action against a now-defunct cryptocurrency trading and investment company for misappropriating $147 million worth of Bitcoin. The Complaint charges the defendants—Control-Finance Limited and its principal, Benjamin Reynolds—with exploiting public enthusiasm for crypto assets by fraudulently obtaining and misappropriating at least 22,858.822 Bitcoin from more than 1,000 customers through a classic (HYIP) Ponzi scheme called the Control-Finance Affiliate Program.

The complaint alleges that during a six-month period in 2017, the defendants fraudulently solicited investors to transfer BTC to Control-Finance with the promise of earning money "on the volatility of the cryptocurrency market." The CFTC further alleges Control-Finance falsely claimed that it:

- Employed expert virtual currency traders
- Earned customers 1.5 % in daily Bitcoin trading profits and up to 45% per month
- Used risk diversification methods to protect customers' BTC deposits
- Provided a "safe haven" from Bitcoin market risks

Control-Finance went so far as to provide customers with fabricated weekly Trade Reports, fake account balances and profit figures falsely reflecting trading profits that did not exist. According to the Commission, to keep the pyramid scheme going for as long as possible, Control-Finance disincentivized account withdrawals through profit "reinvestment" options. It appears that customers regarded the Affiliate Program as highly lucrative because most chose to keep their funds in Control-Finance accounts rather than withdraw (and presumably miss out on the supposed passive income). When customers did request withdrawals from their Control-Finance accounts, the company illegally diverted BTC deposited by other customers to satisfy these redemption requests.

Also in classic pyramid scheme style, "Affiliates" were given referral hyperlinks and web banners that could be shared with friends and family online. Each time a referral hyperlink produced a new customer that sent Bitcoin to Control-Finance, the company supposedly credited the Affiliate's account with a nominal amount of BTC. Of course, these credits were all fake and reflected balances that did not actually exist.

Control Finance Vanishes with Customers' BTC

Ultimately, Control-Finance shut down its website, stopped paying customers and Affiliate Program members, and deleted its social media accounts. The company emailed customers claiming an unspecified exchange had "temporarily blocked" its ability to process account withdrawal requests. Control-Finance further claimed that its attorneys were working to unblock the accounts and guaranteed to fulfill their obligations to customers.

Subsequently, the company emailed customers again, claiming to have received information on how to unblock its trading accounts and would soon return all customers' BTC deposits, minus any prior payments. The email also claimed that its website would "temporarily stop working, but all customer databases with their payment and contact details will be stored on a separate server..." The email concluded by reassuring customers that payments would continue and not to worry. According to the complaint, this was simply a ruse designed lull customers into a sense of complacency while Control-Finance completed its misappropriation of BTC deposits. The website never went back online, and customers were never reimbursed.

Bitmarket Co-Owner Found Shot after the Polish Exchange Suddenly Shuts Down in $23 Million Misappropriation of Funds Fiasco

On July 8, the Polish-based exchange Bitmarket abruptly shut down due to liquidity issues. The shutdown

allegedly cost users a total of 2300 bitcoin (approximately $23 million) according to Polish prosecutors. The exchange's official site was replaced with the following message: "We regret to inform you that due to the loss of liquidity, from 08/07/2019, Bitmarket.pl/net was forced to cease its operations. We will inform you about further steps."

Co-Owners Contradict Each Other

After 400 users complained, on July 11, the District Prosecutor's Office in Olsztyn announced they had initiated an investigation into the exchange's actions. Bitmarket's co-owners Marcin Aszkiełowicz and Tobiasz Niemiro denied allegations of misappropriation of user funds. That same day Aszkielowicz claimed the exchange had been hacked for 600 BTC back in 2015, from which the company was never able to recover. Aszkielowicz further claimed the "galloping increase in the cryptocurrency rate" forced them to take "unfavorable actions" to maintain the liquidity of the exchange. He ends his statement saying, "I was left alone by my partners, on a sinking ship, naively believing that it would manage to reach the port."

Niemiro, on the other hand, claimed in a July 13 interview with Money.pl, that he did "not bear any responsibility for the activity and situation of the exchange" and has "no knowledge about the reasons for closing it" apart from the message posted on the Bitmarket website. Niemiro further claimed in the interview that he was also a victim and wanted to clear his name as he was "only a financial investor" and not involved with the management of the company. Niemiro clarifies in his interview that he was told by his partners that the exchange was purchased with a deficit of 600 bitcoins. He then alleged to repay the deficit with his own money and claims to have the contracts to prove it, but cannot confirm if his partners actually used the money to purchase the 600 bitcoin that put the exchange in the red.

One Co-Owner Found Shot Dead

Two weeks later, on July 25, Niemiro was found in a dead forest near his home with a gunshot wound to the head. On July 29, following autopsy, the District Attorney's Office released a statement stating they have no reason to believe the death was the result of "third-parties" at this time but they are continuing to look into both Niemiro's death and the exchange's alleged misappropriation of custodial funds. However, according to a Decrypt news story published on Yahoo! (which has not been corraborated by CipherTrace researchers), people who knew Niemiro suspected foul play. According to the report, a local businessman named Adam Socha claimed in a blog post that he had received an email from Niemiro, a few hours before he died. "The email was long. It seemed like he had found himself in an environment of shady businessmen. He gave names. I will not disclose its content because of the investigation. I forwarded the email to the prosecutor's office. He also wrote that he would provide certain materials, but he didn't have time," said Socha.

Issues with Payment Processors and Banking Partners

Like many exchanges, Bitmarket had a history of issues retaining payment processors and banking partners. In 2015, Bitmarket lost its regional payment processors, CashBill and BlueMedi, a after the payment

processor's partner banks requested they end the relationship. At the same time, Bitmarket's own bank, PKO Bank Polski, had also ended its relationship with the exchange. This was six months after Bank BPH had ended their relationship with the exchange in January 2015.

Issues around maintaining payment processors and banking partners appears to be a common theme among exchanges that have been accused of misappropriating custodial funds. As these exchanges struggle to find a way to stay in business, they are often forced to perform unnatural financial acts to maintain liquidity. One notable case of this is the shady payment processor Crypto Capital's misappropriation of $850 million in customer funds for Bitfinex. Lack of access to the financial system continues to be a problem for many exchanges, especially in poorly regulated countries. Poland continues to have virtually regulations on VASPs other than guidance on the tax effects of trading cryptocurrencies. In January 2018, Prime Minister Morawiecki stated the country will either ban cryptocurrency or introduce regulations to prevent pyramid schemes, however, a draft of such legislation has yet to be revealed.

Legal Actions Against Bad Actors

SEC Sues Kik Over $100 Million Unregistered ICO

On June 4, the Securities and Exchange Commission (SEC) sued Kik Interactive Inc. for raising nearly $100 million in an unregistered securities offering. The SEC's complaint alleges Kik had been losing money for years and the company's management predicted internally that it would run out of money by 2017. To mitigate this shortfall, Kik developed a new mode of business financed through the sale of one trillion "Kin" tokens, raising more than $55 million from U.S. investors alone. However, according to the complaint, Kin tokens are now trading at half the value paid by public investors during the initial coin offering. According to Robert A. Cohen, Chief of the agency's Enforcement Division's Cyber Unit, "Kik told investors they could expect profits from its effort to create a digital ecosystem… [and] future profits based on the efforts of others is a hallmark of a securities offering that must comply with the federal securities laws." By selling $100 million in securities without registering the offer, the SEC alleges that Kik "deprived investors of information to which they were legally entitled, and prevented investors from making informed investment decisions."

Kin hopes to challenge the Howey Rule used by the SEC when determining if an ICO is a security. Kik claims the Kin ICO does not meet the definition of a security offering and hope the lawsuit hopes challenge the Howey Test for how cryptocurrencies are regulated in the United States but that is a long, uphill battle. According to the Howey Rule, an ICO is a security if "there is the investment of money in a common enterprise with a reasonable expectation of profits to be derived from the efforts of others." This, according to SEC guidance, applies to any contract, scheme, or transaction, regardless of whether it has any of the characteristics of typical securities.

First Public Seizure of a Bitcoin Mixing Service — BestMixer

In May, the Dutch Financial Intelligence and Investigation Service (FIOD), Europol, and authorities in Luxembourg collaborated to shut down the supposedly Curacoa-based cryptomixing site Bestmixer.io by seizing six of its servers in the Netherlands and Luxembourg. According to Europol, BestMixer was known as one of the three largest cryptocurrency mixing services at the time and had processed at least $200 million in its one year of business. Because mixing services are not illegal in Curacao, BestMixer advertised itself as a successful method to avoid various anti-money laundering policies through guaranteed anonymity that it claimed to be legal. Throughout their investigation, the FIOD has gathered information on all interactions on the platform in the past year, including: IP-addresses, transaction details, bitcoin addresses and chat messages. The FIOD and Europol will continue to analyze the information and distribute intelligence packages of their findings. CipherTrace had issued an alert in December 2018 about BestMixer's practice of "cryptodusting" users accounts as a means of foiling AML tracing technologies by "dusting" every address with money laundering funds, thereby soiling virtually every user's reputation.

The following week, another mixing service Bitcoin Blender chose to voluntarily close. After posting a short announcement on its website homepage asking customers to withdraw their funds, Bitcoin Blender shut itself down. It is still unclear if the company's termination was planned or a reaction to BestMixer's seizure.

FinCEN Fines Peer-to-Peer Virtual Currency Exchanger $35,000 for Violating AML Laws

In its first enforcement action against a peer-to-peer virtual currency exchanger, FinCEN fined Eric Powers $35,000 for "willfully violating the BSA registration program and reporting requirements." According to FinCEN, Mr. Powers failed to register as a money services business (MSB), had no written policies or procedures for ensuring compliance with the BSA, and failed to report suspicious transactions and currency transactions. This is FinCEN's first enforcement action against a virtual currency transmitter for failing to file Currency Transaction Reports (CTRs) with FinCEN and should serve as a warning to others. In addition to paying a $35,000 fine, Mr. Powers has agreed to a ban prohibiting him from engaging in any activity that would classify him as a "money services business" under FinCEN regulations.

"Obligations under the BSA apply to money transmitters regardless of their size," said FinCEN Director Kenneth A. Blanco. "It should not come as a surprise that we will take enforcement action based on what we have publicly stated since our March 2013 Guidance—that exchangers of convertible virtual currency, such as Mr. Powers, are money transmitters and must register as MSBs. In fact, there were indications that Mr. Powers specifically was aware of these obligations, but willfully failed to honor them. Such failures put our financial system and national security at risk and jeopardize the safety and well-being of our people, as well as undercut responsible innovation in the financial services space."

According to FinCEN's official statement, Mr. Powers advertised his intent to purchase and sell bitcoin on

the internet. He completed transactions by either physically delivering or receiving currency in person, sending or receiving currency through the mail, or coordinating transactions by wire through a depository institution. Mr. Powers processed numerous suspicious transactions without ever filing a SAR, including doing business related to the illicit darknet marketplace "Silk Road," as well as servicing customers through The Onion Router (TOR) without taking steps to determine customer identity and whether funds were derived from illegal activity. He conducted over 200 transactions involving the physical transfer of more than $10,000 in currency, yet failed to file a single CTR. For instance, he conducted approximately 160 purchases of bitcoin for approximately $5 million through in-person cash transactions, conducted in public places such as coffee shops, with an individual identified through a bitcoin forum. Of these cash transactions, 150 were in-person and were conducted in separate instances for over $10,000 during a single business day. Each of these 150 transactions necessitated the filing of a CTR.

New York Denies Bittrex a BitLicense Due to AML Deficiencies

In April, New York regulators ordered cryptocurrency exchange Bittrex to cease operations in the state after rejecting its application for a BitLicense due to the exchange's "failure to demonstrate that it will conduct business honestly, fairly, equitably, carefully, and efficiently". Several shortcomings were cited in the announcement, including deficiencies in BSA/AML/OFAC compliance programs and failure to meet capital requirements. There is no appeals process following a BitLicense denial, so the company would have to reapply if they wanted to be reconsidered.

Bittrex initially applied for a BitLicense in August 2015. Throughout the application process the NY State Department of Financial Services (NYDFS) worked with the exchange to address continued deficiencies and assist with developing appropriate controls and compliance programs, however, due to the number of unresolved deficiencies the NYDFS eventually conducted a four-week onsite review at Bittrex's Seattle and Washington D.C. offices in February 2019 and analyzed transactions conducted between January 1, 2017 and December 31, 2018. NYDFS determined that the exchange's KYC and customer due diligence programs were "seriously deficient," citing missing tax ID numbers, customer names, birthdays, and a substantial number of aliases found as user account names such as "Give me my money," "Elvis Presley," and "Donald Duck." Furthermore, Bittrex's compliance program lacked the process to remain up-to-date with and adequately screen current OFAC lists, resulting in "a large number of transactions for customers domiciled in sanctioned countries (including Iran and North Korea) that had passed through screening and were processed."

European Authorities Seize Three Dark Web Marketplace Platforms and Assets

Three dark web marketplaces enabling trade in drugs, stolen data, fake documents and malicious software were seized by European authorities: Valhalla marketplace (also known as Silkkkitie), Wall Street Market, and Chemical Revolution. In response, Europol's executive director, Catherine De Bolle, stated the seizure

of darknet marketplaces demonstrate how "illegal activity on the dark web is not as anonymous as criminals may think."

Wall Street Market and Valhalla Seized in Same Week

In cooperation with the French National Police and Europol, the Finnish Customs (Tulli) seized Valhalla's server and shut down the dark marketplace in late April. This new influx of traffic significantly raised the amount of money flowing through Wall Street Market's escrow account. For those unfamiliar with how dark web marketplaces work, most marketplaces work as brokers, securing customer funds in escrow until both the buyer and seller agree that the sale was completed successfully. Whether influenced by the flood of new money coming their way, or the fear of being targeted by the police for the site's new status as top dog on the dark web, by mid-April Wall Street Market's admins had begun their exit scam. They alledgedly planned to make off with all the cryptocurrency held in escrow and otherwise stored under their authority (much of it presumably belonging to drug dealers and others using the site for illegal commerce). A successful exit would have net them some USD $11 million if they were able to convert the coins without being caught.

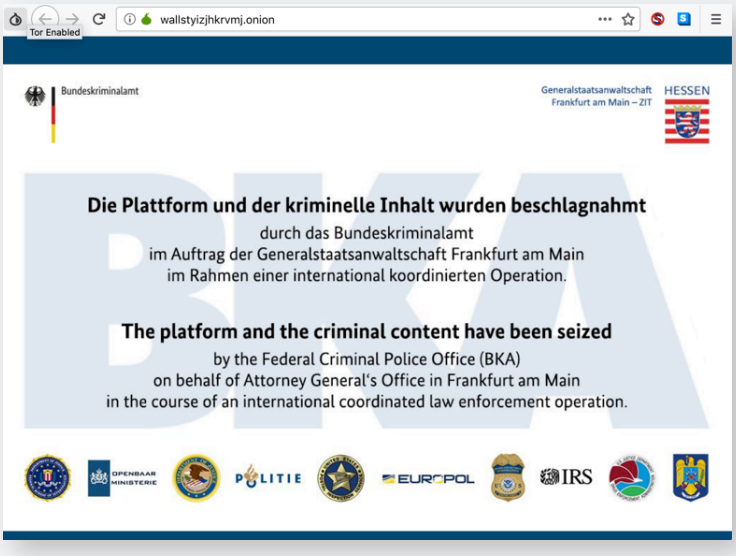
Unfortunately for the fraudsters, the VPN connection of one of the administrators failed while still logged into the marketplace, revealing their true IP address and location. Aware of the potential exit, authorities knew they had to move fast; by May 2nd the entire operation was shut down thanks to the joint efforts of the U.S. Drug Enforcement Administration, the Federal Bureau of Investigation, the U.S. Internal Revenue Service, the U.S. Homeland Security Investigations, the U.S. Postal Inspection Service, the U.S. Department of Justice, the Dutch National Police (Politie), Europol, and Eurojust.

German Police Raid Chemical Revolution

A little over a month later, on June 28th, German police raided another dark web marketplace—Chemical Revolution. The raid led to the arrest of several suspects, with potentially more arrests on the way. Law enforcement also shut down the site's servers. Chemical Revolution was part of an ongoing investigation that involved cooperation from Polish, Dutch, Spanish and French police to stop the transport of narcotics across borders.

SIM Swapping Victim Wins $75.8 Million Judgement Against Hacker

The CipherTrace Q3 2018 Crypto AML Report described how in early 2018 a then-unknown hacker had used an identity theft technique known as SIM Swapping to steal $23.8 million from a well-known entrepreneur and cryptocurrency investor. In May, the investor, Michael Terpin, won $75.8 million in a civil



Authorities replace Wall Street Market website with seizure notice

judgment against Manhattan resident Nicholas Truglia—the hacker who allegedly stole the tokens from Terpin. The $75.8 million award reflects compensatory and punitive damages and is one of the largest court judgments involving cryptocurrency ever awarded to an individual. According to Reuters, Truglia was arrested in November for six other crimes. Terpin said he is preparing action against other members of the SIM Swapping ring.

In a SIM-Swapping attack, hackers use social engineering—including stolen credentials purchased on dark markets—to deceive a telecom provider into transferring the victim's phone number to a SIM they hold. Service providers have developed customer service methods to quickly move a number to a new SIM such as, for example, when a subscriber's phone is lost or stolen. Once cybercriminals receive the phone number, they can use it to reset passwords and break into the victim's accounts, including accounts on cryptocurrency exchanges.

In Q4 2018, CipherTrace also reported cases where SIM Swapping was an insider job in which hackers pay off employees of a service provider, often at a retail location, to aid in the swap. Lieutenant John Rose of the Silicon Valley REACT Task Force said, "If you're working at a mobile phone store and making $12 an hour and suddenly someone offers you $400 to do a single SIM swap, that can seem like a pretty sweet deal."

Terpin is also suing AT&T for for failing to protect his cell phone data. In the lawsuit, Terpin claims AT&T's employees were complicit in the SIM Swap fraud and is seeking $23.8 million in compensatory damages and a further $200 million in punitive damages. On July 19, Terpin won the first round in his suit when a Los Angeles federal judge denied AT&T's request to dismiss the suit. The judge decided the telco should answer Terpin's claims of violation of the Federal Communications Act, breach of contract, and other legal violations.

Japan's FSA Issues Business Improvement Order to FISCO Cryptocurrency Exchange

Despite the country's experiment with self-regulation of crypto asset businesses, Japan's Financial Ser-

vices Agency (FSA) recently inspected Houbi Japan —formally known as BitTrade— and took administrative action against the FISCO Cryptocurrency Exchange. An onsite visit by the agency revealed a number of legal violations, including a lack of proper policies and procedures from the Board of Directors, and inadequate money laundering/terrorism financing risk-management systems. According to a Reuters interview, significant management changes at the exchange prompted the FSA visit to ensure proper customer protection and legal compliance measures. The FSA found that FISCO management "did not recognize the importance of legal compliance," and issued a business improvement order, giving the company until July 22, 2019 to submit a plan to comply with legal obligations.

Major Changes In The Global Regulatory Environment

In the second quarter, governments around the world began to require virtual asset businesses to comply with a wide array of new regulations, many of which were put into law last year. For example, member states of the European Union must adopt AMLD 5 into their AML/CTF regimes within the next six months. G20 countries are also implementing the latest updates and clarification from the FATF, and the UK is addressing both FATF and AMLD 5 regulations in upcoming legislation. Among these new regulations, complying with the FATF's Travel Rule presents crypto asset businesses with one of the biggest challenges.

In the US, the SEC and FinCEN released clarifying guidance to help crypto businesses navigate US regulatory policy. CipherTrace has offered guidance on some of these rules, and in July advised the US Congress on several pieces of pending crypto legislation detailed in the following summary. Meanwhile, countries like Canada, Estonia and Japan all tightened cryptocurrency regulations this quarter at the same time South Korea was deregulating parts of its crypto economy

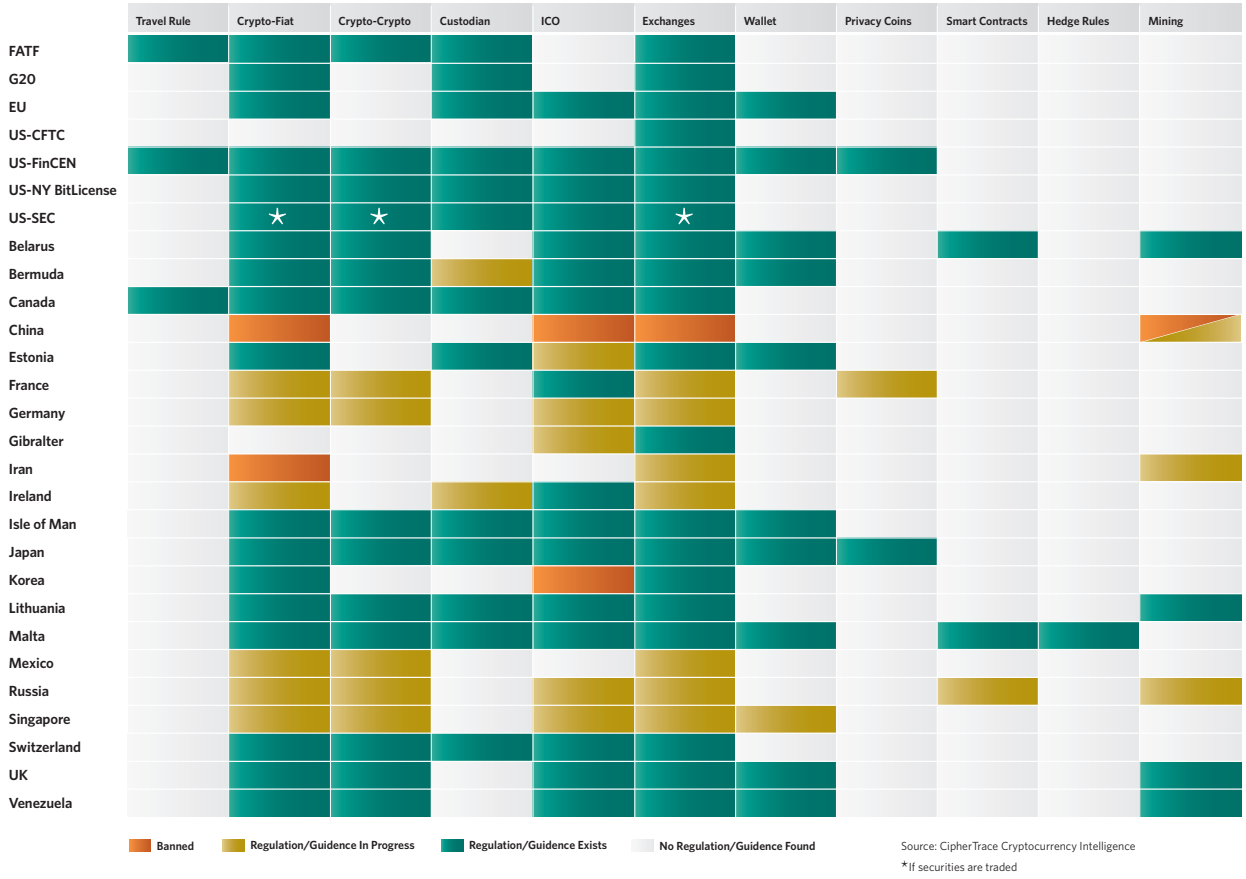
Facebook's recently announced "global" cryptocurrency also put renewed focus on issues such as AML, CTF, KYC and other regulatory issues as well as the need to consider privacy and the role of cryptocurrencies in the global financial system.

The State of Cryptocurrency Anti-Money Laundering Legislation

This quarter saw jurisdictions compete for crypto business based upon regulatory vision and completeness of implementation. The charts below show the widely varying levels of maturity and sophistication in AML/CTF regimes around the globe. The gaps in these regulations present risky avenues that can be exploited by money launderers and terrorist organizations. Specifically, the money laundering potential of crypto-to-crypto exchanges and privacy coins are not well addressed by lawmakers attempting to regulate digital assets based on the physics of fiat currency.

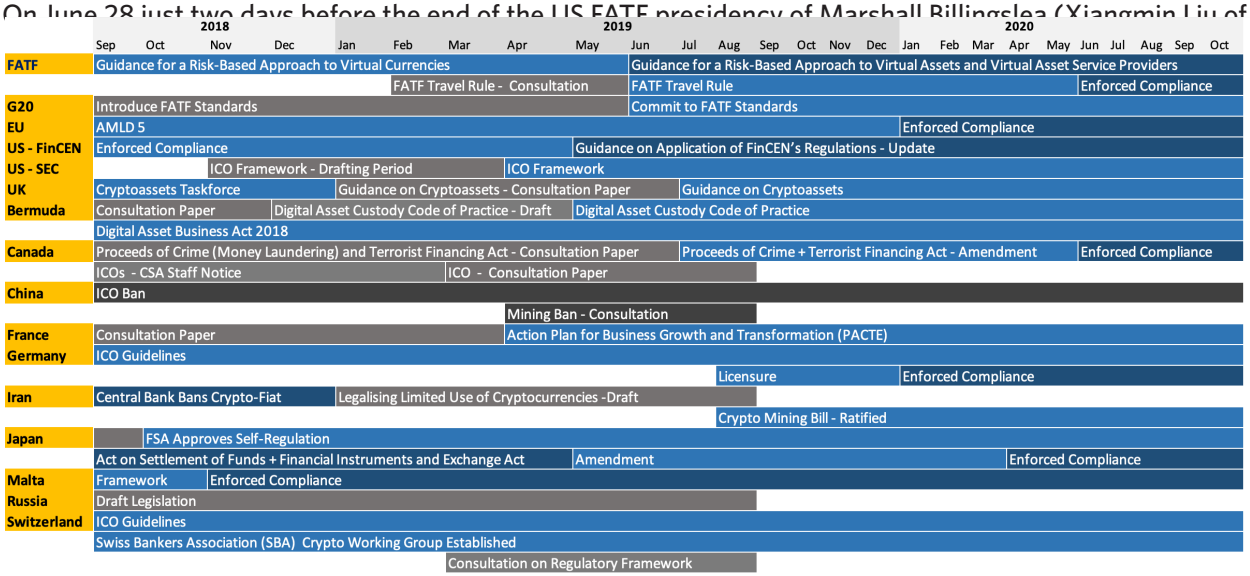
G20 to Adopt Tough New FATF Rules to Cryptocurrencies — Including new "Travel Rule"

Current Implementation of AML/CTF Regulations Globally



Global Cryptocurrency AML Timeline

On June 28 just two days before the end of the US FATF presidency of Marshall Billingslea (Xiangmin Liu of

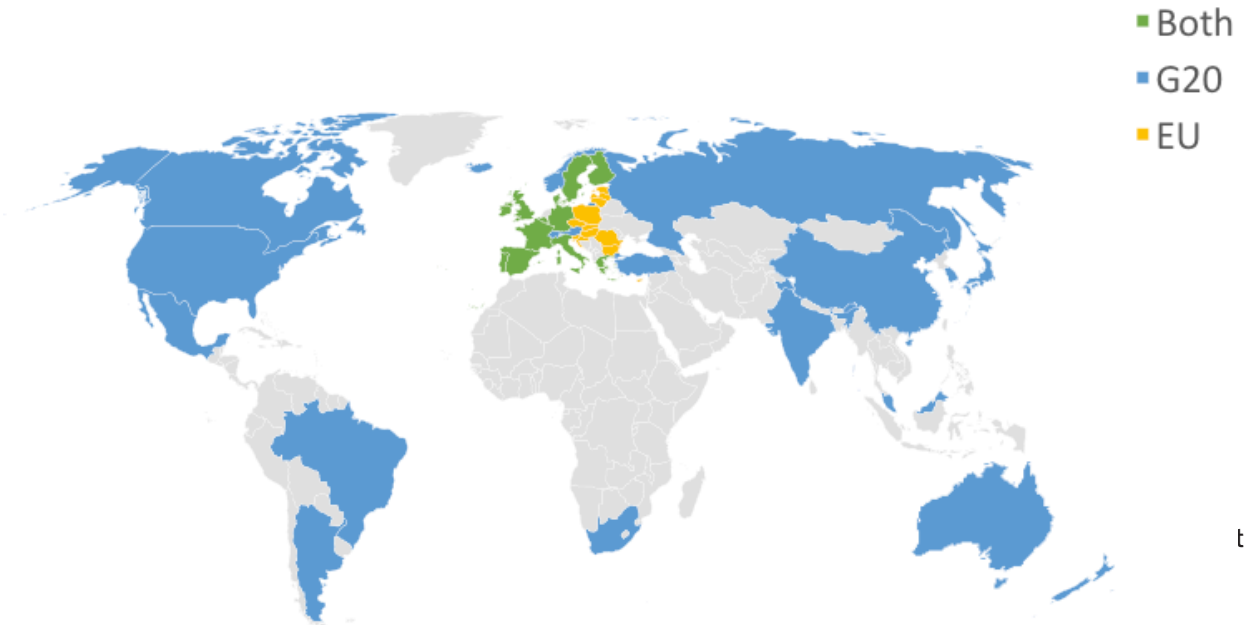


Contact@ciphertrace.com

the People's Republic of China assumed the position of President of the FATF on July 1 2019), finance ministers of the G20 nations committed to deploy recent FATF standards that give guidance on setting tougher operating procedures for exchanges and other virtual asset service providers (VASPs). This is guidance must be implemented with new laws in each of the G20 nations. The new rules go beyond current CDD to align more closely with bank regulations. One example is requiring countries ensure that originating VASPs follow FATF's "travel rule" by sharing originator and beneficiary information with recipient VASPs when conducting virtual asset transfers valued at over $1,000 USD. CipherTrace offered recommendations to the FATF during their public consultation period. Those recommendations can be found on the CipherTrace blog at ciphertrace.com/response-to-fatf-on-vasp-regulation/ .

G20 finance ministers and central bank governors acknowledged that cryptocurrencies "can deliver significant benefits to the financial system and the broader economy" and (prior to the Libra announcement) affirmed that they do not believe crypto assets pose a threat to global financial stability. However, they advised that companies and governments remain vigilant and actively work for consumer and investor protection, anti-money laundering (AML) and countering the financing of terrorism (CFT), asking the Financial Stability Board (FSB) and global standard-setting organizations to continue to monitor risks around crypto assets.

AMLD 5 Regulations Must Be Commited to EU Countries Laws



rules will now apply to entities which provide services that are in charge of holding, storing and transferring virtual currencies," according to the commission.

AMLD 5 further includes mandatory identity checks on new customers. These newly regulated entities will have to identify their customers and report any suspicious activity to the Financial Intelligence Units.

G20 countries account for 85.2% of Global GDP. Most European countries are part of the European Union and the EU Commissioner represents members states in inter-governmental bodies such as the FATF and G20. However, Europe's non-EU states fall under neither the G20's commitments to standardization of the EU 5th AML Directive, creating a potential regulatory loophole that would allow criminals to obfuscate money laundering by using crypto-to-crypto transactions. Furthermore, FATF and AMLD 5's differences in crypto-to-crypto regulations and enforcement timelines, as well as FATF's "non-binding" assessment and categorization of VASPs, VAs, and VA activities further complicates the EU's crypto regulatory regime as member states now have less than a year to decide how to adopt the two into national legislation.

Overlapping Requlatory Regimes

The key points of AMLD 5 include:

- Requires crypto-to-fiat exchanges and custodian wallet providers comply with relevant AML/CFT requirements under AMLD 4
- Requires crypto-to-fiat exchanges and custodian wallet providers be registered
- Permits "competent authorities" to monitor the use of virtual currencies for the purposes of AML/CFT
- Ensures National Financial Intelligence Units (FIUs) can obtain information allowing them to associate virtual currency addresses to the identity of the virtual currency owner
- Requires crypto-to-fiat exchanges and custodian wallet providers to keep customer due diligence (CDD) records for five years after the end of a business relationship or occasional transaction

Crypto-to-crypto controls are not included in AMLD 5. This has been identified as a critical weakness in its effectiveness against money laundering and terrorism financing. For example, the CipherTrace Q1 2019 AML Report revealed a major hole in the current cryptocurrency regulatory fabric with respect to cross-border payments via crypto-to-crypto. An analysis of 164 million BTC transactions by CipherTrace researchers uncovered a 46% increase in the number of cross-border payments from US cryptocurrency exchanges over the last two years. This is important for the effectiveness of AML/CFT regulation because according to the International Consortium of Investigative Journalists, "$8.7 trillion, 11.5 percent of the world's wealth, is hidden offshore."

Also, as reported in previous CipherTrace AML reports, criminals and terrorists can move large amounts of dirty cryptocurrency into poorly regulated exchanges and other crypto-to-crypto services—such as mixers— and turn these funds into "clean" cryptocurrencies. The funds can then be moved into the global financial payments system with little risk of being detected. CipherTrace earlier reported on elaborate

techniques, such as crypto dusting that crypto-to-crypto mixing services like BestMixer.io have used to avoid AML/CFT controls. BestMixer was subsequently shut down by Dutch, and Luxembourg authorities and Europol. Also, in response to the FATF's request for input on its new guidelines earlier this year, CipherTrace recommended "VASPs should be obligated to perform analysis and reporting on crypto-to-crypto swaps (e.g., swap Bitcoin into Ethereum or Monero) at this same level, and to have controls such as KYC on those accounts above the 1,000 EUR mark."

USA

FinCEN Clarifies Regulations to Convertible Virtual Currency (CVC) Businesses

On May 9, FinCEN issued new guidance clarifying its cryptocurrency regulation policies. The guidance does not establish new regulatory expectations or requirements per se. Rather, this clarification is intended to help people and institutions better recognize their BSA obligations by consolidating current requirements and applying them to common cryptocurrency business models such as exchanges, wallets, mixers, and privacy coins. The guidance clarifies which cryptocurrency businesses must comply with BSA regulations (and subsequently the BSA travel rule).

Application of BSA Regulations to Money Transmission Involving CVC

FinCEN further clarified that any persons "accepting and transmitting value that substitutes for currency, such as virtual currency" are money transmitters and are therefore required to register with FinCEN as a money service business (MSB) and comply with AML, recordkeeping, monitoring, and reporting requirements. Furthermore, these requirements apply to all CVC money transmitters conducting business within the United States, whether or not they are physically located in the US.

Note: For the purposes of this guidance, a "money transmitter" is a "person that provides money transmission services," according to FinCEN. A "money transmitter" is "the sender of the first transmittal order in a transmittal of funds," for example a specific exchange or other crypto business.

DApps

Decentralized Applications (DApps) are decentralized application software programs that operate on a peer-to-peer P2P network (e.g., crowdfunding platforms created using the Ethereum blockchain). Despite

this decentralized nature, when a DApp performs money transmission, regardless of whether it operates for profit, the definition of money transmitter will apply to the DApp, the owners/operators of the DApp, or both.

DApp Users

BSA regulations only apply to users engaged in money transmission and FinCEN seems willing and able to take action against DApps users violating money transmitters laws. As previously noted in this report, they fined Eric Powers – who had, according to FinCEN, been operating as a peer-to-peer exchanger of convertible virtual currency — $35,000 for "willfully violating money transmission laws" and banned him from further money services business operations.

However, users engaged in money transmission can be exempt from regulations if the person engaging in such activity "does so on an infrequent basis and not for profit or gain."

DApp Developers Not Money Transmitters

Developers are not money transmitters for creating DApp programs, "even if the purpose of the DApp is to issue a CVC or otherwise facilitate financial activities denominated in CVC."

CVC Trading Platforms and Decentralized Exchanges are Likely Money Transmitters

A CVC trading platform is not a money transmittor if it "is only providing a forum where buyer and sellers of CVC post their bids and offers... and the parties themselves settle any matched transactions through an outside venue (either through individual wallets or other wallets not hosted by the trading platform)."

Hosted vs Unhosted Wallet Providers

Hosted wallets are typically considered money transmitters and must comply with the BSA, including KYC, CDD and travel rule regulations. Unhosted wallets, on the other hand, are typically not considered money transmitters and do not have to comply with BSA.

Cryptocurrency Kiosk and Bitcoin ATMs

An owner-operator of a cryptocurrency ATM that accepts fiat currency from a customer and transmits the equivalent value in CVC (or vice versa) constitutes a money transmitter.

Providers of anonymizing services for CVCs (Mixers)

Anonymizing services providers are categorized as money transmitters. Concealing the source of the transaction does not change their obligations under the BSA.

Anonymizing software provider

Anonymizing software providers are engaged in trade, not money transmission, and therefore not covered under the BSA.

Providers of anonymity-enhanced CVCs (Privacy Coins)

A person that creates or sells anonymity-enhanced CVCs would likely be a money transmitter under FinCEN regulations, whereas people who simply use privacy coins to pay for goods or services on their own behalf would not.

Privacy Coins and the Travel Rule

Money transmitters involved in privacy coin transactions must comply with BSA obligations, including the travel rule. This means they must follow AML risk assessment policies and procedures to determine if and how they will accept or transmit anonymity-enhanced CVCs (privacy coins or regular CVCs that have been anonymized). To comply with FinCEN's travel rule, money transmitters "must not only track a CVC through the different transact ions, but must also implement procedures to obtain the identity of the transmittor or recipient of the value."

Payment Processing Services Involving CVC Money Transmission

Payment processing service providers involving CVC are money transmitters under the BSA. However, the guidance offers no clarification on the Lightning Network— a network of pre-funded payment channels running on top of Bitcoin. Founding President of the Bitcoin Association, Jimmy Nguyen, believes FinCEN's broad interpretation of "money transmitter" would require the intermediaries that make up the network to register as MSBs, and expects FinCEN's guidance "will further inhibit growth of the Lightning Network beyond traditional payment processors who already hold MSB licenses."

Initial Coin Offerings (ICOs)

The sellers of ICOs are considered money transmitters if they conduct a preferential sale of the ICO to a select group of investors because the seller is the only person authorized to issue and redeem new units of the CVC. Other than this, ICOs are typically regulated by the SEC or CFTC.

SEC and FINRA Issue Joint Statement on Broker-Dealers and Crypto Custody Issues

This July, the United States Securities and Exchange Commission (SEC) and the Financial Industry Regulatory Authority (FINRA) issued a joint statement outlining regulatory compliance for broker-dealers.

According to the statement, an entity that "buys, sells, or otherwise transacts or is involved in effecting transactions in digital asset securities for customers" may be classified as a broker-dealer. This would require the entity to comply with financial responsibility rules such as the Customer Protection Rule which "requires broker-dealers to safeguard customer assets and to keep customer assets separate from the firm's assets, thus increasing the likelihood that customers' securities and cash can be returned to them in the event of the broker-dealer's failure." The recent string of crypto hacks highlights the need to ensure strong protection of customers' crypto assets under custodial care.

USA Law Makers Explore Numerous New Cryptocurrency-Related Bills

Illicit Cash Act

On June 10, Senate Banking Committee members U.S. Sens. Mark R. Warner, Tom Cotton, Doug Jones, and Mike Rounds unveiled draft legislation designed to improve corporate transparency, strengthen national security, and help law enforcement combat illicit financial activity being carried out by terrorists, drug and human traffickers, and other criminals. This legislation would comprise the first major upgrade to the Bank Secrecy Act (BSA) in over 50 years.

The Improving Laundering Laws and Increasing Comprehensive Information Tracking of Criminal Activity in Shell Holdings (ILLICIT CASH) Act aims to modernize the BSA. The bill primarily focuses on closing loopholes in beneficial ownership and customer due diligence (CDD) regulations, placing additional obligations on crypto related businesses subject to the BSA and requiring companies to disclose to FinCEN the identity of their beneficial owners for a new federal database. Two sections of the bill address virtual currencies directly.

First, the draft bill amends the classification of "monetary instruments" to include "value that is issued or repurposed to substitute for currency," under which cryptocurrencies would fall. Since cryptocurrency exchanges are already subject to BSA regulations, this change is likely to have little to no immediate impact, but it does open the door to further regulation down the road, especially regarding P2P transactions.

Second, the act would require the Comptroller General of the United States to conduct a study of how virtual currencies are being used to facilitate sex and drug trafficking. The Controller General has a year to submit a report summarizing the results of the study along with any recommendations for legislative or regulatory authorities. The study will primarily focus on how virtual currencies are being used on and off online marketplaces (including the dark web) to facilitate sex or drug trafficking to, from or within the US; how virtual currencies are being repatriated into the formal banking system; and the extent to which virtual currencies and related technologies can be used to deter, detect, track and ultimately aid in the prosecution of illicit funding.

Additionally, the draft bill also proposes transaction monitoring software must be approved by FinCEN.

Transaction monitoring software submitted to FinCEN will be examined for its effectiveness in sorting transactions by riskiness by backtesting and other examination means. However, the use of approved software does not on its own fulfill the BSA/ AML requirements to create a full risk-based compliance system.

Pending House Bill Adds Iranian Cryptocurrency to U.S. Economic Sanctions

Introduced in December 2018, the US House of Representatives have yet to move on the Blocking Iran Illicit Finance Act H.R.7321. If passed and signed into law, the bill would strengthen existing sanctions on Iran and implement new sanctions with respect to the development and use of an Iranian digital currency. The bill defines Iranian digital currency as "any digital currency, digital coin, or digital token that was issued by, for, or on behalf of the Government of Iran."

The introduction of "digital currency" into the sanctions bill was motivated both by Venezuela's use of cryptocurrency to launder money and finance illicit activities, and Iran's rhetoric on using cryptocurrency as a conduit for sanctions evasion. According to the bill's authors, the Deputy for Management and Investment at the Directorate for Scientific and Technological Affairs of Iran claims the currency "would facilitate the transfer of money (to and from) anywhere in the world... [and] can help [Iran] at the time of sanctions." The head of the Civil Defense Organization of Iran also claimed that "cryptocurrencies can help bypass certain sanctions through untraceable banking operations.

The bill aims to prohibit all transactions with Iranian digital currency by a United States person or within the United States. Anyone violating this law could face civil penalties no greater than $250,000 or twice the amount of the transaction that violated the law as well as criminal penalties of no more than $1,000,000, or up to 20 years imprisonment, or both.

Additionally, foreign persons that knowingly support Iran in the development of their digital currency through the sale, supply, or transfer of significant goods or services, or technological support, could be sanctioned. Foreign persons using the cryptocurrency could also face sanctions banning their ability to receive a US visa, limiting their ability to use crypto exchanges operating in the United States, and freezing all funds that are in the United States, come within the United States, or come within the possession or control of a United States person.

Lastly, the bill would give the Secretary of the Treasury 120 days to submit a report to Congress on Iran's progress in its development of a sovereign cryptocurrency. (See the CipherTrace blog ciphertrace.com/analysis-of-irans-crypto-rial-virtual-currency for details on the so-called crypto rial). This report should contain technical details such as whether Iran plans to fork an existing blockchain or create a new one, make the blockchain open or closed, and whether or not they will involve the Central Bank of Iran. The report should also include an assessment of the state and non-state actors assisting Iran, the effect a

successful cryptocurrency would have on US sanctions, the technology and infrastructure Iran would need to be successful, and a list of countries that have agreed to assist the US in blocking efforts to bypass or evade Iranian sanctions.

The Virtual Currency Consumer Protection Act of 2019

A bill currently pending before the US House of Representatives, The Virtual Currency Consumer Protection Act of 2019, H.R. 923, aims to promote fair and transparent virtual currency markets by examining the potential for price manipulation. If passed, it would require the Chairman of the Commodity Futures Trading Commission (CFTC) to submit a report detailing the potential for virtual currency price manipulation. This report should include:

- The methods by which persons could manipulate the price of virtual currencies
- Types of virtual currency, if any, that are more susceptible to being manipulated
- The effects/harm on investors when price manipulation occurs
- An analysis of how regulatory authorities currently monitor the virtual currency market for signs of manipulation
- An analysis on how regulations are enforced when market manipulation is found
- Recommendations for any legislative changes needed to improve the ability of the CFTC to monitor and enforce regulatory compliance and prevent price manipulations of virtual currencies

U.S. Virtual Currency Market and Regulatory Competitiveness Act of 2019

Another bill introduced but not yet passed, the U.S. Virtual Currency Market and Regulatory Competitiveness Act of 2019, H.R. 923, would require the Chairman of the CFTC as well as the SEC and other authorities, to report on ways to promote US competitiveness in the global virtual currency marketplace. This report should include:

- A comparative study of US virtual currency regulations against those of other countries
- Recommendations for any legislative changes that would promote US competitiveness in the global marketplace
- A description of the potential benefits of VCs and blockchain technology in the US commodity market
- Recommendations for legislative changes to help further clarify which VCs qualify as commodities
- Recommendations on how to encourage the adoption of VCs in the segments of the commodity market that could benefit from them
- Recommendations for any new regulatory structures such as Federal licensure, market supervision, or consumer protection
- An analysis of the feasibility, cost, and potential benefit of any new regulatory structure recommended

Fight Illicit Networks and Detect Trafficking Act ("FIND Trafficking Act")

This bill directs the Government Accountability Office (GAO) to carry out a study on how virtual currencies and online marketplaces are used to facilitate sex and drug trafficking and report the findings to Congress along with any recommendations for legislative or regulatory action.

The report should include how:

- Online marketplaces are used to facilitate sex and drug trafficking
- The unique characteristics of virtual currencies are used to facilitate sex and drug trafficking
- Illicit funds transmitted through virtual currencies are repatriated into the US formal banking system
- preventative efforts from federal and state agencies
- The immutable and traceable nature of virtual currencies contribute to the tracking and prosecution of illicit funding

This bill passed the US House of Representatives on in January 2019 and is pending before the US Senate.

Homeland Security Assessment of Terrorists' Use of Virtual Currencies Act

This bill directs the Department of Homeland Security's Office of Intelligence and Analysis to develop a threat assessment regarding the actual and potential threat posed by individuals using virtual currency to carry out or support an act of terrorism. The assessment should be disseminated to state, local, and tribal law enforcement officials.

This bill passed the US House of Representatives on in January 2019 and is pending before the US Senate.

FinCEN Improvement Act of 2019

This bill amends the duties of the Financial Crimes Enforcement Network (FinCEN) to ensure FinCEN works with Tribal law enforcement agencies, protects against all forms of terrorism—domestic or international— and focuses more on virtual currencies. Regarding crypto in particular, this amendment adds "matters involving emerging technologies or value that substitutes for currency" to the list of efforts on which FinCEN should coordinate with financial intelligence units in other countries.

This bill passed the US House of Representatives on in March 2019 and is pending before the US Senate.

The Financial Technology Protection Act

A bill that passed the US House of Representatives in January 2019 and is pending before the US Senate proposes to establish an Independent Financial Technology Task Force to Combat Terrorism and Illicit Financing. Its goal is to provide rewards to whisle blowers for information leading to convictions related to terrorist use of digital currencies, to establish a Fintech Leadership in Innovation and Financial Intelligence Program to encourage the development of tools and programs to combat terrorist and illicit use of digital currencies, and to develop a strategy to mitigate rogue and foreign actors from evading sanctions using digital currencies.

Blockchain Regulatory Certainty Act

A bill still pending before the US House of Representatives, the Blockchain Regulatory Certainty Act, seeks to protect non-controlling blockchain developers and providers of blockchain services by ensuring they are not treated as money transmitters, money services businesses, financial institutions, or any other state or federal legal designation requiring licensing or registration under State or federal law.

UK extends AMLD 5 to Crypto-to-Crypto, P2P and Even Software

The European Union's AMLD 5 entered into force on July 9, 2018. EU member states are obliged to transpose the modified regulations into their respective national laws no later than January 20, 2020. With the deadline fast approaching, the UK has released a consultation paper for its draft plan to implement the Directive. Among the proposals is the addition of new "obliged entities" such as fiat-to-crypto exchanges and custodian wallet providers. Notably, the UK is seeking to go beyond its obligations under AMLD 5 to regulate, in addition to fiat-to-crypto exchanges, providers engaged in "alternative" exchange services. These include crypto-to-crypto exchanges, P2P exchanges, and bitcoin ATMs. This is similar to FinCEN's guidance. However, the UK further extends regulation to cover the publication of open-source software.

Critics of this expansion say it imposes an undue burden on legitimate businesses, which otherwise present little risk of engaging in money laundering or terrorist financing. Supporters say it'll stop Wasabi and other mixing tools from proliferating. If passed, this requirement would be a stark contrast to recently released guidance in the US that excludes software developers from BSA obligations.

The proposal's rationale for going beyond AMLD 5 requirements is to manage risks associated with entities and activities not captured by AMLD 5 or FATF, citing an increase in cases of crypto assets being used to launder illicit proceeds since the 2017 National Risk Assessments of Money Laundering and Terrorist Financing.

Canada Approves New Regulations Requiring Crypto Exchanges to Register as MSBs

On July 10, the Canadian government published amendments to the Proceeds of Crime (Money Laundering) and Terrorist Financing Act on the Canada Gazette — the official website of the Government of Canada. The new regulations classify domestic and foreign crypto platforms that offer services to people located in Canada, as money services businesses (MSBs). The MSB designation means they must "fulfill all obligations (of the Act), including implementing a full compliance program and registering with [Canada's financial intelligence unit] FINTRAC."

Furthermore, similar to Canada's reporting regulations for large cash transactions, any reporting entity that receives CAD $10,000 or more in virtual currency must comply with Customer Due Diligence (CDD) and reporting obligations. However, these reporting requirements do not apply to virtual currency transfers that total CAD $10,000 after feedback from stakeholders indicated that the scope of the activities captured by the draft amendments would be cumbersome. Additionally, reporting entities that send, are

intermediaries, or that receive fund transfers are now "required to keep records of, and include information about the transaction" à la the FATF's new travel rule. Finance Canada will continue to assess the best approach to mitigate the risks posed by virtual currency transactions, aligned with FATF standards.

Cryptocurrency exchanges have until June 1, 2020 to register with FINTRAC and until June 1, 2021 to comply with all other regulations.

Brazil to Require Exchanges to Inform the Tax Authority About Users' Transactions

This June, the Department of Federal Revenue of Brazil (RFB) released new guidance that requires cryptocurrency exchanges to report on the movements of users' crypto funds to the RFB in order to comply with requirements set out in May of this year. This requirement is an attempt to better identify tax fraud by placing the responsibility of reporting on exchanges rather than the customer. The guidance explicitly states that "ALL OPERATIONS MUST BE REPORTED." Exchanges are required to provide the RFB with the following data once a month.

- Date of transaction
- Type of transaction
- Value of transaction
- Value of service charge
- Parties involved
- The balance of fiduciary currencies
- The balance of each type of crypto asset
- The cost of obtaining each type of crypto asset

Some exchanges view this as a positive. For instance, "the crypto industry should regard these new rules as a positive," commented CoinMetro's CEO, Kevin Murcko. "That regulators are beginning to see crypto in the same bracket as traditional financial securities indicates the credibility and popularity that crypto now has. The regulations themselves will serve to legitimize the space and will help to shrug off the accusations of money laundering and fraud that have long-tarnished the industry."

New Estonia Regulations Make It Harder to Obtain a Crypto License

Estonia is arguably the most advanced adopters of blockchain of any jurisdiction in the world. In the first year after Estonia introduced licensing for companies operating in the cryptocurrency industry in late 2017, the number of licenses issued had surpassed 900. Cryptocurrency exchanges in Estonia must have a

service provider activity license to conduct fiat-to-crypto transactions and vice versa. Wallet providers that provide custodian services must also have a license. On May 3rd, Estonia's Ministry of Finance added new crypto regulations that make it harder for these companies to obtain a virtual currency activity license. The new regulation not only increase the license fee by tenfold— from EUR 340 to EUR 3,330— but also extends the processing time from thirty to ninety days. The new regulation further requires the exchange, or a branch of the exchange, be incorporated in Estonia. The registered office address and the board of directors must also be located in Estonia. In addition, members of the board of directors must pass a background and suitability check by the Estonian Financial Intelligence Unit (FIU).

In explaining the rationale behind the tougher regulations, the Minister of Finance, Martin Helme, says in light of last year's Danske Bank money laundering scandal, Estonia had "learned [their] lesson from the banking sector the hard way, and [they] must now deal with new international risks, with cryptocurrencies among the most urgent of these." Virtual asset businesses that already hold a license have until December 31 to comply with the new requirements or risk losing their license.

Japan Tightens Crypto Regulations

On May 31, the Japanese Diet (House of Representatives) officially approved a new bill to amend two national laws that govern cryptocurrency—the Payment Services Act (PSA) and the Financial Instruments and Exchange Act (FIEA). These revisions come into force April 2020 and will tighten regulation on custodian wallets and crypto exchanges, giving them the same level of accountability as banks due to the parallels in common risks such as hacks, bankruptcy of service providers, and money laundering/terrorism financing. Furthermore, the regulations establish a new asset classification called "Electronically Recorded Transferable Rights" (ERTRs) which aim to clarify when initial coin offerings (ICOs) and security token offerings (STOs) are governed by the FIEA— Japan's main law governing securities.

Lithuania Set Low Thresholds for Crypto Transaction Obligations

In June, the Lithuanian Cabinet approved amendments to the Law on Money Laundering and Terrorism Prevention in order to comply with AMLD 5. As with the UK's proposals, several the new obligations go beyond the scope of the EU's Directive. For example, one says any crypto transaction—which includes both crypto-to-fiat and crypto-to-crypto—exceeding EUR 1,000 will be subject to new reporting requirements laid out in the AMLD 5. Furthermore, all transactions over EUR 15,000 must be reported to Lithuania's FIU (Financial Crime Investigation Service). It also requires obligatory ID checks for ICO sales over EUR 3,000. These policies will constitute Lithuania's first set of crypto asset regulations.

South Korea Deregulates OTC Derivatives Market

In an attempt to revitalize the country's derivatives market, the Financial Services Commission (FSC) has cut the barrier to entry for retail investors from roughly US $25,300 to about US $8,500 for futures and

buying options, and US $17,000 for sell options. Furthermore, 80 hours of required class time and trading simulation have been reduced to a mere four hours for new retail investors. Institutional investors will also share in the incentives, as they are no longer required to deposit an extra margin of 10 percent of their credit risk limit under the new regulation.

The FSC also hopes to deregulate other parts of the industry to help facilitate the development and listing of new derivatives. For example, security firms will now have more autonomy in developing new derivative products. Additionally, regulators will begin introducing more incentives to market makers for low-liquidity products. The FSC hopes these moves will help reinvigorate the underperforming local market after stricter regulations in 2011 resulted in a significant loss of local investors.

Sanctions Evasions Escalated in Q2

Russian Bank Sanctioned by US Treasury over Venezuela's Petro

In March, the US sanctioned the Moscow-based bank Evrofinance Mosnarbank over its role in financing Venezuela's petro cryptocurrency. The bank was added to the Office of Foreign Assets Control's (OFAC) Specially Designated Nationals (SDN) list for being the "primary" international bank to help finance the project as "early investors in the Petro were invited to buy the cryptocurrency by wiring funds to a Venezuelan government account at Evrofinance," according to the Treasury. Being on the SDN list means "all property and interests in property of this entity, and of any entities that are owned, directly or indirectly, 50 percent or more by this entity, that are in the United States or in the possession or control of U.S. persons are blocked and must be reported to OFAC." A similar fate could follow any entities looking to help Iran develop their crypto-rial if the Blocking Iran Illicit Finance Act passes congress.

Russia Postpones Cryptocurrency Regulations

After several previous postponements, President Putin's July 1 deadline to adopt a regulatory framework for digital currencies has come and gone without action. The Russian Duma has delayed passing the bill to the Fall 2019 as it continues to debate the role of crypto in the country. According to Anatoly Aksakov, chairman of the State Duma Committee on Financial Market, the legislature is debating two options – either encouraging cryptocurrency trading in Russia or banning it altogether. Aksakov adds that even if a ban were to prevail, Russian citizens would still be allowed to buy and sell virtual currency from foreign cryptocurrency exchanges.

Despite the debate on whether or not to ban crypto in Russia, the government seems keenly interested in collecting and using cryptocurrency. On June 16, it was reported that two viruses associated with a Russian hacker group were found on Coincheck employees' personal computers. The Japanese exchange had

suffered a $534 million hack in January 2018, which was previously attributed to North Korean hackers. Mokes—one of the viruses found—was also used by Russian hackers to steal sensitive NSA data from a contractor's computer back in 2015. The investigation is ongoing.

Previously, according to the 2018 indictment of alleged conspirators involved in hacking the 2016 US presidential election, Russia funded the purchase of computer infrastructure for their activity in part by mining bitcoin. Virgin bitcoins were used to purchase servers and domains used in spearphishing operations, which included typosquatting addresses such as "accounts-qooqle.com and accountÐgooogle.com."

Iran Accuses US of Attempting to Block the Country from Mining Virgin Bitcoins as a Means to Evade Sanctions

The international affairs think tank Atlantic Council recently reported that with Iran's low energy costs (among the cheapest on the planet), BTC mining was profitable for Iranian miners even during the crypto winter. Not surprisingly, with mining constituting such an obvious means to circumvent sanctions and the SWIFT ban, Iran has accused the US of trying to close another sanction loophole, with Iran's Assistant Minister of Industry, Trade and Supply, Saeed Zarandi, saying on July 7th that the Trump administration is working to block BTC mining in the country.

In late June, the government seized two crypto mining farms. The official explanation for raiding the abandoned factories containing 1,000 crypto mining machines was a 7% spike in power consumption in June, which also strained the country's electric power grid. Bitcoin mining has become very popular in Iran as miners can exploit government-subsidized power (Iran pays about $1 billion annually to bridge the gap in real electricity costs and what consumers pay) and free power to schools and mosques. However, there was speculation that the government's real motivation for confiscating the rigs was to use them to leverage Iran's vast energy reserves and create clean, virgin BTC, which the government could then use for foreign trade payments—trade based money laundering.

Virgin bitcoins have no transaction history associated with them. No transaction history means lack of attribution, making them highly desirable for anyone looking to mask the source of funds or launder money. The recipient typically has no ability to verify the source of funds and cannot attribute the coin to a wallet or entity. Because the bitcoin blockchain is public and works as an irreversible, decentralized ledger, it is possible to follow bitcoins' chain of custody to pseudonymous users. There is a cryptographically provable history of ownership and transactions

Venezuela's Petro Developed to Evade US Sanctions

For more than a decade, the United States has imposed sanctions on Venezuela related to terrorism, drug trafficking, trafficking in persons, antidemocratic actions, human rights violations, and corruption.

The sanctions include individuals such as President Nicolas Maduro, his wife and son, and the director of the Central Bank of Venezuela. In an effort to circumvent sanctions, in 2018 Venezuela announced it was developing a sovereign cryptocurrency now known as the Petro (allegedly with the help of Russia), which would be backed by the nation's vast oil reserves. The US retaliated by sanctioning the digital currency immediately after its ICO ended in March of that year.

Thus far, the Petro has not not enjoyed wide adoption. On July 4th, 2019, the Finance Ministry tweeted that Maduro had ordered the country's leading bank, Banco de Venezuela, to accept the Petro at all of its branches. Previously on June 19, Maduro had announced that 924 million bolivars (over $92.5 million) were allocated to the Digital Bank of Youth and Students to open one million Petro wallet accounts for the country's youth.

Cuba Considers Using Cryptocurrency to Bypass US Sanctions

In July, Cuba's Minister of Economy and Planning announced that the country is "planning to explore the potential application of cryptocurrency" and has "decided to study the potential use of cryptocurrency in national and international commercial relations." Despite facing US economic sanctions, Cuba's President Miguel Diaz-Canel promised to raise income for around a quarter of the population and hopes cryptocurrency can be used to boost the economy. There is no timeline for when a sovereign Cuban cryptocurrency may be released.

North Korea Compensated for Sanctions with Major Hacks of Cryptocurrency Exchanges

A recent United Nations report claimed that between January 2017 and September 2018, North Korea's elite state-sponsored hackers are thought to have stolen USD $571 million in cryptocurrency from five exchanges in Asia. In April, the FBI reported that North Korea executed cryptojacking and exchange hacks in response to sanctions that have pinched the country's economy, stating the DPRK was responsible for several of the costliest cyber-attacks over the last two years. That includes some of the most damaging cryptocurrency ransomware attacks, such as the 2017 WannaCry attack. The WannaCry ransomware scheme infected 300,00 machines around the world and caused financial and economic losses of up to USD $4 billion, according to Trend Micro's security and threats report.

In a conference address, Tonya Ugoretz, deputy assistant director of the FBI's cyber division, and Erin Joe, director of the Cyber Threat Intelligence Integration Center under the U.S. Director of National Intelligence, implicated political sanctions and economic pressures as the cause for these increasing North Korean cyber-attacks.

Also, a British defense thinktank, The Royal United Services Institute (RUSI), reported in April that North Korea is most likely "directly funding" its nuclear weapons program using cryptocurrency. They conclude North Korea could seek to use cryptocurrencies as part of its proliferation financing efforts through:

- Fundraising: To sustain its ongoing needs for cash, North Korea may obtain cryptocurrencies with the aim of converting them to fiat currencies in the short term
- Stockpiling: North Korea could accumulate reserves of cryptocurrencies with the objective of eventually spending them or converting them into fiat currency at some point in the future
- Circumvention: North Korea could use cryptocurrencies to pay directly for goods, services and resources that are explicitly prohibited by international sanctions

About CipherTrace

CipherTrace develops cryptocurrency Anti-Money Laundering, bitcoin forensics, and blockchain threat intelligence solutions. Leading exchanges, banks, investigators, regulators and digital asset businesses use CipherTrace to trace transaction flows and comply with regulatory anti-money laundering requirements fostering trust in the crypto economy. Its quarterly CipherTrace Cryptocurrency Anti-Money Laundering Report has become an authoritative industry data source. CipherTrace was founded in 2015 by experienced Silicon Valley entrepreneurs with deep expertise in cybersecurity, eCrime, payments, banking, encryption, and virtual currencies. US Department of Homeland Security Science and Technology (S&T) and DARPA initially funded CipherTrace, and it is backed by leading venture capital investors. For more information visit www.ciphertrace.com or follow us on Twitter @ciphertrace.

