CIPHERTRACE

Cryptocurrency Anti-Money Laundering Report, 2019 Q1

CipherTrace
Cryptocurrency Intelligence
April 2019

Summary

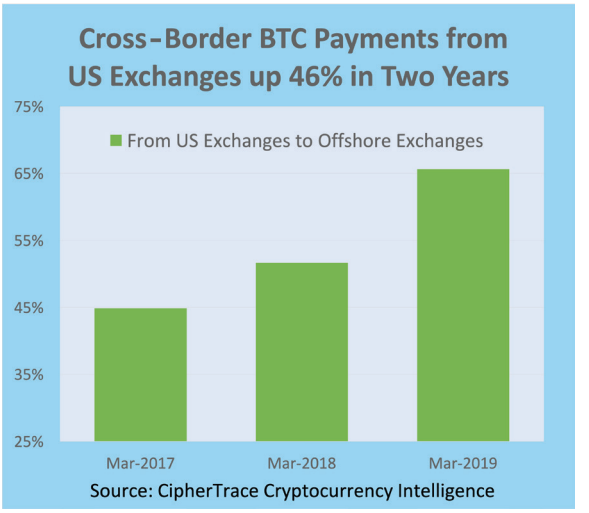
Cryptocurrency Thefts, Scams, and Fraud Could Tally More than $1.2 Billion in First Quarter 2019

Criminals stole more than US$356 million from exchanges and infrastructure during the first quarter of 2019. Among these losses, exit scams—which CipherTrace is considering the implosion of QuadrigaCX to be one—robbed cryptocurrency users of nearly US$195 million. On top of these numbers, the New York Attorney General's Office revealed what they allege is a fraud involving the loss of $851 million by a major cryptocurrency exchange, Bitfinex. Cyber criminals also developed ingenious new techniques to drain millions more from user accounts and wallets. These thefts only represent the losses that are visible. CipherTrace estimates the true number of crypto asset losses was much higher.

46% Increase in the Number of Cross-Border Payments from US Cryptocurrency Exchanges Over the Last Two Years

CipherTrace research conducted in Q1 revealed a major hole in the current cryptocurrency regulatory fabric with respect to cross-border payments. An analysis of 164 million BTC transactions revealed that cross-border payments from US exchanges to offshore exchanges increased 21 percentage points — from 45% from the twelve months ending Q1 2017 to 66% in the twelve months ending Q1 2019. This is significant because according to the International Consortium of Investigative Journalists, "$8.7 trillion, 11.5 percent of the world's wealth, is hidden offshore."

Once these payments reach exchanges and wallets in other parts of the globe they fall off the radar of US authorities. For now, it is uncertain if these cross border inter-exchange payments trigger the FinCEN requirement that "MSBs must keep a five-year record of currency exchanges greater than $1,000 and money transfers greater than $3,000." But experts recommend MSBs retain tax ID/SSN for these transactions.



A Significant Wave of Regulation Is Coming to the Cryptocurrency Economy

Ultimately, thieves and scam artists will need to launder the cryptocurrency stolen or scammed in Q1 2019. Furthermore, this will require innovative new ways to cash out, and turn all that tainted virtual money into clean, spendable fiat currencies. And they will also need to get it done under the much more watchful eyes of government regulators and banks as a tsunami of tough new global anti-money laundering (AML) and counter-terror financing (CTF) regulations will roll over the crypto landscape in the coming year. As of April 2019, 17 countries plus the European Union within the jurisdiction of the Financial Stability Board had at least some regulation or standard-setting bodies dealing with cryptocurrencies. These bodies will be responsible for implementing regulations that enforce FATF policy and AMLD5.

In light of the huge losses suffered by users of QuadrigaCX, regulators in Canada and around the world are rethinking controls on the internal business practices and security operations of exchanges. In addition, regulators are beginning to recommend bans on privacy coins, as criminals are coming to prefer these new anonymous altcoins to bitcoin because they are more difficult to trace. Banks also continue to face problems coping with the coming wave of regulations as they increasingly recognize there are undetected cryptocurrency operations that are using their fiat payment networks and customer accounts. Plus, courts in some countries have ruled that banks must do business with licensed cryptocurrency companies.

A tsunami of tough new global anti-money laundering (AML) and counter-terror financing (CTF) regulations will roll over the crypto landscape in the coming year.

Crypto Crime Evolves and Expands from the Virtual to the Real World

The previous year's crypto crime spree was dominated by major external exchange hacks around the globe—with the biggest occurring in Q1 2018. However, in the first quarter of this year, insiders, extortionists and scammers attempted a more diverse range of crypto crimes. As just one example, kidnappers in Norway demanded nine million euros (approximately US$10.3 million) ransom in Monero, a privacy coin, for a billionaire's wife, who has not yet been returned. There were also two large insider thefts/misappropriations (QuadrigaCX and Bitfinex). This shift suggests that security against external hackers at exchanges is maturing under the pressure from regulators and customers to take necessary measures to prevent losses.

In the first quarter of this year, cyber thieves, extortionists and scammers attempted a more diverse range of crypto crimes.

While not included in the current theft numbers in this report, on March 6, 2019, the UN Security Council reported North Korean state-backed hackers successfully breached at least five cryptocurrency exchanges in Asia between January 2017 and September 2018, causing $571 million in losses. Also, of note, but not included in this quarter's theft numbers was the loss of 1,680 XMR Monero (around $80,000) due to a bug in the Ledger app.

The geopolitical implications of cryptocurrencies also took center stage in Q1 2019 with countries competing to attract crypto businesses and foster related economic growth. Conversely, overt attempts to evade sanctions by hostile nations show that economic adversaries recognize the money laundering and terrorist financing potential of crypto assets. On March 6, 2019, the UN Security Council reported North Korean state-backed hackers successfully breached at least five cryptocurrency exchanges in Asia between January 2017 and September 2018, causing $571 million in losses.

Q1 2019 Crypto Crime Highlights

- Thieves and scammers stole more than $356 million from exchanges and users.
- Customers suffered losses of approximately US$195 million when Canada's major cryptocurrency exchange, QuadrigaCX, imploded after the CEO mysteriously perished in India, allegedly along with the passwords to virtually all of the exchange's assets. CipherTrace analysis casts severe doubt that this was anything other than a theft, fraud, or foul play.
- On March 26, the New York Attorney General's Office brought suit against the parent company of Bitfinex and Tether.
  - The AG claimed Tether had failed to disclose a secret transfer of funds from the fiat pool of funds supposedly backing tether, which converted tether from asset-backed to debt-backed unbeknownst to tether holders.
  - Bitfinex allegedly lost $851 million. The source of the loss was a Panamanian payment processor also used by QuadrigaCX.

- Iran announced the imminent launch of its long-rumored Crypto Rial, a state-backed stable coin developed with the express purpose of circumventing political sanctions and overcoming sanctions-related restrictions by SWIFT.
- The Russian Duma approved international use of the domestically developed SPFS as a 'SWIFT alternative' for cross-border payments in an effort to avoid political sanctions.
- The French government issued a report recommending a ban on privacy coins.
- The UN published the findings of a private report that concluded North Korean hackers looted $571 million from five cryptocurrency exchanges in Asia.
- Courts in some countries forced financial institutions to bank crypto asset businesses.
- The Bank of Mexico reportedly proposed banning financial institutions from transacting with crypto exchanges, citing money laundering and terror financing risks.

Exchange Thefts, Fraud and Exit Scams May Tally More than $1.2 Billion

EXCHANGE THEFTS

Cryptopia

New Zealand based Cryptopia suspended trading after cyber thieves stole $16 million from its platform in January (those losses were estimated by a third-party data analytics firm). This amount represented 9.4 percent of the exchange's holdings. Cryptopia reopened its website in read-only form on March 5.

CoinBene

On March 27, 2019, ZDnet reported on a widely rumored hack on Singapore-based exchange CoinBene. At the time of the alleged cyberattack, the exchange went into maintenance mode, which undoubtedly fueled speculation. ZDnet cited a "cryptocurrency expert" who estimated robbers made off with more than $45 million in cryptocurrency—roughly $6 million in CoinBene Coin and $39 million in Maximine Coin—from the exchange. CoinBene Global, the parent company, responded to the allegations of a hack on Twitter with what appears to be a denial of an attack along with a vaguely worded attachment that says: "With the news sent by multiple exchanges of users (sic) asset theft recently, CoinBene security team took measures to upgrade the wallet immediately to help global users and partners avoid market risks and guarantee the security of all parties' assets." The statement went on to assure customers that "User assets on CoinBene platform are 100% secure, our platform promises that if any user assets will be lost, we will compensate 100%."

CipherTrace researchers have been working to shed light on this event. Thus far, we have verified that during the period of the alleged hack, March 25th to 28th, massive amounts of funds flowed from the exchange's hot wallets to known and unknown wallets, and those funds eventually ended up in other

exchanges. The bulk of these transactions appear to have gone to the unregulated exchange Etherdelta. It seems inconceivable that if those wallets were, in fact, hacked that CoinBene could regain control those accounts—i.e., that the users' assets were 100% secure.

Nonetheless, at the time of this report's publishing events are still unfolding. We can only confirm that during the period of the rumored "hack" US$105 million of Ethereum (CoinBene Coin and Maximine Coin are both Ethereum based) moved to other exchanges where it was being converted to various cryptocurrencies, so we are only tentatively classifying it as a possible theft or exit scam. CipherTrace reached out to CoinBene Global management for comment, but we have not yet received a response. Watch for further CipherTrace alerts with any updates on this research as we continue to monitor the situation.

DragonEx

DragonEx lost more than $1 million USD to a cyber theft, disclosing publicly that the attacker had transferred the funds to other exchanges. DragonEx published destination wallet addresses belonging to the hackers and requested help in freezing and recovering the funds.

Without being specific, the company said they were able to recover some but not all of the money. Authorities in Estonia, Hong Kong, Singapore, and Thailand are said to be assisting the Singapore-based exchange in its investigation.

Bithumb

The largest cryptocurrency exchange in South Korea, Bithumb, was hacked in March, and attackers made away with $14 million in EOS and XRP. According to Bloomberg, Bithumb said the incident was most likely caused by an "accident involving insiders" because an external intrusion path hadn't been revealed after an inspection. This was the second major hack experienced by Bithumb. In June 2018, cybercriminals robbed the exchange of $30.8 million in cryptocurrency.

Coinbin

In South Korea, cryptocurrency exchange Coinbin declared bankruptcy on February 26th after suffering losses of approximately $26 million. The company cited embezzlement from an insider as the main cause of its downfall.

EXIT SCAMS

On top of outright cryptocurrency thefts from infrastructure and wallets, investors lost almost 200 million dollars from inside threats such as "exit scams" in which founders and executives embezzled users' custodial crypto funds, and then slipped away quietly.

Coinbin

While CipherTrace has categorized the $26 million losses in losses experienced by South Korean cryptocurrency exchange Coinbin as an exchange theft, the firm claimed the losses werethe result of an inside job. According to *Business South Korea*, Chan-kyu, Coinbin's CEO, told reporters in its Seoul office on Feb. 20th: "We are preparing to file for bankruptcy due to a rise in debt following an employee's embezzlement." The company also asserted that an executive in charge of managing cryptocurrencies, who previously served as the CEO of Youbit, the predecessor of Coinbin, had committed dereliction of duty and embezzled company funds. The executive reportedly claimed that he had removed hundreds of cryptographic keys to coin wallets containing hundreds of Bitcoin, and also lost the cryptographic key to a wallet containing more than 100 Ethereum coins last November.

QuadrigaCX

During the first quarter, the cryptocurrency community was captivated by the implosion of what had been Canada's largest cryptocurrency exchange. On January 14, 2019, QuadrigaCX customers learned the company's CEO, Gerald Cotten, had died more than a month earlier. His widow posted an announcement on the QuadrigaCX website explaining that Cotten passed away in India while opening an orphanage. Around the same time, customers began having trouble getting their cryptocurrency out of the exchange. This unusual situation led to the immediate speculation that the exchange's funds were gone along with the CEO. Then, on February 9 news broke that Cotten had, in fact, taken the passwords to all the firm's crypto assets with him to the afterlife. QuadrigaCX's customers were stunned to learn their crypto was inaccessible.

How much went with Mr. Cotten to the grave, crematorium, or elsewhere? In a sworn affidavit filed January 31 with the Nova Scotia Supreme Court, his widow, Jennifer Robertson, said the exchange owes its customers roughly 250 million CAD (US$195 million) in both cryptocurrency and fiat.

The enormous size of this case—coupled with an unfathomable lack of internal controls—will undoubtedly lead governments around the world to rethink regulation of cryptocurrency exchanges. Setting aside what was immediate speculation that Cotten had faked his own death and spirited away the funds, questions immediately arose as to how the passwords to all that crypto could have been in only one person's possession with no backup.

QuadrigaCX's customers were outraged to learn that on January 31 the exchange filed an application for creditor protection in the Nova Scotia Supreme Court, citing issues with locating "very significant cryptocurrency reserves held in cold wallets." In the same affidavit, the widow stated that her husband had mostly run the company—Canada's largest cryptocurrency exchange—on an encrypted laptop from "wherever he and his computer were located." Ms. Robertson further claimed that she did not know the passwords or recovery keys, and she could not find them "despite repeated and diligent searches."

In this report, CipherTrace has chosen to categorize the QuadrigaCX losses as a theft. While the details may never be known, based on the rather bizarre circumstances surrounding the demise of the exchange and its CEO, the facts suggest it was either theft due to foul play or an insider theft—i.e., an exit scam. For example, as the QuadrigaCX plot thickens, the auditor appointed by the bankruptcy court, Ernst & Young, revealed it had utilized public blockchain records to review the transactional activity of the six identified cold wallets set up by Cotten, where Ms. Robertson claims the assets were locked up without access to the password keys. However, instead of holding US$137 million, the wallets were empty. Moreover, they had been drained in early April 2018. Ernst & Young also found evidence of what appeared to be 14 fake accounts set up by the company under false names that had been trading large amounts of crypto to accounts on external exchanges.

In addition, citing court records in the U.S. and Canada, the Globe and Mail reported it believes the company's co-founder Michael Patryn aka Omar Patryn is actually Omar Dhanani. Dhanani was arrested by the U.S. Secret Service in California as part of an identity theft, credit card fraud and money-laundering ring in 2004. He served time in a U.S. prison and was later deported to Canada. On top of that, Cotten had filed a will leaving everything to his wife just 12 days before he died, and the couple had amassed millions of dollars in real estate, a yacht, and an airplane. Perhaps further fueling the speculation, Mr. Cotten passed away in an area reputed for having a whole industry devoted to providing fake death certificates and fake doctor's notes to tourists.

Cotten traveled to India in December 2018 for his honeymoon and to celebrate the opening of an orphanage, and while there apparently died from complications from Crohn's disease involving a suspected perforation of the digestive tract. However, there seems to be no chain of custody account of Cotten's body and no official coroner's report. CipherTrace researchers reached out to Dr. Eduardo Peña Dolhun, a Mayo Clinic trained, board-certified family physician with internationally recognized expertise in the field of rehydration science. He has treated disaster victims with dehydration and digestive tract disorders around the globe. "The likelihood of an otherwise healthy 30-year-old dying of complications from Crohn's, assuming reasonable access to adequate healthcare, would be a fairly rare event," said Dr. Dolhun. "But what is highly atypical would be the lack of an autopsy. When an otherwise healthy person dies suddenly at that age, medical ethics and even prudent concern over legal liability dictate an autopsy take place to determine the cause of death and the appropriateness of care. This is especially so where signs of the cause of death are not visible externally. Someone would have demanded an autopsy. And this would be true anywhere, from a major city to a medical facility even in a third-world village. That is how we are trained as doctors."

In addition, as more details emerged from the bankruptcy Monitor's report released in early April, there is the appearance of severe financial stress at the firm. This is partly due to difficulty obtaining satisfactory banking relationships, which led to the use of numerous payment processors. These processor companies are currently refusing to return millions of dollars to QuadrigaCX or its creditors. Also of note, one of the payment processors used by QaudrigaCX, and mentioned often in Cotten's leaked emails, was the same Panamanian entity at the core of the recent $851m Bitfinex debacle—Crypto Capital.

The Monitor also revealed that Ms. Robinson had been attempting to dispose of large personal assets left to her in Cotten's will. The sale of these assets has been frozen as the Monitor discovered that the corporate and personal boundaries between QuadrigaCX and Cotten "were not formally maintained, and it appeared to the Monitor that QuadrigaCX funds may have been used to acquire assets held outside the corporate entity."

So not surprisingly, it appears law enforcement is investigating the potential criminal angle. According to a March 4, 2019 report in Fortune, the CEO of Kraken, Jesse Powell, alleged in an interview that the FBI and the Royal Canadian Mounted Police are probing the QuadrigaCX implosion. The financial news publication reported that in response to its questions both law enforcement agencies said they do not confirm or deny the existence of ongoing investigations. According to the report, Powell told Fortune he did not speak to the law enforcement agencies directly but learned from Kraken's head of compliance of the inquiries.

This saga involves very complex blockchain trails and inter-relationships among many individuals and entities. CipherTrace is actively working to uncover the true cause of this seemingly inexplicable loss of customer funds as well as any potential relationship to money laundering. Watch for updates on this investigation and recommendations to regulators on ways to prevent another such crypto financial crisis.

FRAUD OR MISAPPROPRIATION AND MATERIAL MISREPRESENTATION

Bitfinex and Tether Accused by the NYAG

On April 26, 2019, the New York Attorney General (NYAG) alleged that cryptocurrency exchange Bitfinex had lost $851 million, and then secretly transferred funds from its sister company, Tether Limited, to cover the loss. The trouble began when Bitfinex placed funds with Crypto Capital, a Panamanian payment processor also used by QuadrigaCX. Crypto Capital subsequently says it did not have access to those funds because they were seized by Portuguese, Polish and US authorities. So according to the complaint, Bitfinex borrowed funds from Tether to continue as a going concern. In essence, Bitfinex is accused of misappropriating fiat currency from the pool of funds that Tether ostensibly uses to back the 1:1 US dollar peg of its stable coin.

Moreover, the Office of the Attorney General (OAG) believes that neither the $625 million transfer of Tether reserves in November 2018 nor a subsequent $900 million "line of credit" established against Tether's reserves have been disclosed to customers and investors.

According to the official press release, the OAG obtained a court order against iFinex Inc.—which operates both Bitfinex and Tether—ordering they cease violating New York law and defrauding New York residents.

Key Points from the OAG's Filings Include FundsLost to Payment Processor

Prior to February 2019, Tether represented that every outstanding tether was "backed" by and thus should be valued at one U.S. dollar. Then, on March 4, 2019, more than four months after the transfer of funds to Bitfinex from the pool of fiat funds that back tether, Tether Limited changed its disclosure, representing that "every tether is always 100% backed by our reserves, which include traditional currency and cash equivalents and, from time to time, may include other assets and receivables from loans made by Tether to third parties, which may include affiliated entities (collectively, 'reserves').

In 2014, Bitfinex began a relationship with a Panamanian entity called Crypto Capital Corp. ("Crypto Capital") to act as one of its "payment processors." But at no point known to the OAG has Bitfinex or Tether disclosed to clients that they have used third-party "payment processors" to handle client withdrawals. Moreover, by 2018, Bitfinex had placed over one billion dollars of co-mingled customer and corporate funds with Crypto Capital. Allegedly no contract or similar written agreement was ever entered into between Crypto Capital and Bitfinex or Tether. Bitfinex and Tether have also used a number of other third-party payment processors, including various companies owned by Bitfinex/Tether executives as well as other "friends" of Bitfinex.

In mid 2018, the company began having trouble obtaining funds from the payment processor, leading to delays in resolving client transactions. On October 7, 2018, Bitfinex published a notice to investors ensuring them that the company was not insolvent. Then on October 15, 2018, Bitfinex published a notice to the market stating that "it is important for us to clarify that: All cryptocurrency and fiat withdrawals are, and have been. processing as usual without the slightest interference . . . All flat withdrawals are processing, and have been, as usual." However, documents provided the OAG by Respondents show that during this time, Bitfinex was having severe problems processing client withdrawals.

Bitfinex/Tether Response

Tether issued a statement jointly with Bitfinex strongly disagreeing with the Attorney General's allegations:

"The New York Attorney General's court filings were written in bad faith and are riddled with false assertions, including as to a purported $851 million 'loss' at Crypto Capital. On the contrary, we have been informed that these Crypto Capital amounts are not lost but have been, in fact, seized and safeguarded. We are and have been actively working to exercise our rights and remedies and get those funds released."

Bitfinex took an even stronger stance vis-a-vis the OAG, adding in a statement:

"Both Bitfinex and Tether are financially strong — full stop. And both Bitfinex and Tether are committed to fighting this gross overreach by the New York Attorney General's office against companies that are good corporate citizens and strong supporters of law enforcement."

CipherTrace Observes Parallels Between the QuadrigaCX Case and the Bitfinex Case

Somewhat analogous to QuadrigaCX, which also had an intimate relationship with Crypto Capital, fast-paced and casual relationships with non-bank entities raises a number of issues regarding regulation. First, where these "intimate" relationships exist—i.e., there was no contract in the case of Bitfinex and leaked emails from the late CEO of QuadrigaCX show a similarly cavalier way of conducting business—sound anti-money laundering controls tend to go out the window.

Additionally, exchanges and other crypto asset that do business in less regulated countries, as is in the case of Tether and Bitfinex, typically have difficulty gaining traditional banking relationships. This forces digital asset businesses to deal with "shady" operators, and often in countries like Panama where fraud is sometimes de rigueur. In another recent example, in March 2019, Hong Kong based Gatecoin had to cease operations and liquidate due to what the company said was a problem with its payment processor withholding funds. The net result for cryptocurrency users and investors is risk. CipherTrace strongly believes that sound regulation—i.e., rules designed to keep bad actors out of the crypto economy—not only encourage banks to accept digital asset businesses as customers, but also benefits digital asset businesses, users, investors, and governments trying to build healthy and safe crypto economies.

ATM DOUBLE-SPEND ATTACKS

Authorities in Canada are investigating double-spend attacks on Bitcoin ATMs throughout the country. Thieves seem to have taken advantage of ATMs accepting 0-confirmation transactions, which would require synchronized attacks. Suspects managed to make off with more than US$150,000 through the attacks, which involved 112 fraudulent transactions in seven cities in Canada, largely in Calgary. This brings to light the potential problems involving 0-confirmation transactions. While these types of transactions eliminate the need for ATM customers to wait for confirmations, they are not as secure as those that require confirmations on the BTC blockchain.

Rogue Regimes – Crypto Crimes, Exchange Theft, and Sanctions Evasion

North Korea Accused by United Nations of Stealing $571M from Exchanges

According to private-sector research cited in a UN Security Council Panel of Experts report released March 6, 2019, North Korean state-backed hackers successfully breached at least five cryptocurrency exchanges in Asia between January 2017 and September 2018, causing $571 million in losses. The largest was a January 2018 penetration of Coincheck, a Japan-based exchange. The UN panel also attributed the 2016 theft of $81 million from Bangladesh Bank to a North Korean sponsored cyberattack. In that case, the panel cited a U.S. indictment.

According to the report, targeting cryptocurrency exchanges is particularly useful for evading sanctions because the digital trail is difficult to trace. It also offers Kim Jung Un's rogue regime numerous opportunities for money laundering, according to the report. The panel that created the report included UN analysts as well as experts from China, France, Russia, the United Kingdom, and the United States who advised the Security Council. Of course, North Korea has consistently denied conducting any such cyberattacks.

Iran Launches State-Backed Crypto Currency as Payment Rail to Evade Sanctions

On January 29, 2019, Iran took brazen steps to use cryptocurrency to evade global monetary sanctions by launching its own sovereign cryptocurrency. These sanctions included SWIFT banning some Iranian banks from access to its widely used cross-border payment services in November 2018. SWIFT is the Society for Worldwide Interbank Financial Telecommunication, www.swift.com, a global interbank funds transfer network used by most of the world's banks to perform cross-border payments.

The move by SWIFT came after the United States re-imposed oil and financial sanctions against Iran in response to its alleged missile and nuclear programs. The SWIFT action, which was urged by the U.S. Treasury Secretary, was particularly painful for the Tehran regime as it effectively blocks Iran from receiving payments for oil exports.

The launch of a state-backed "Crypto-Rial" was long rumored to be the result of a collaboration among Iran, China, Russia, Venezuela, and Turkey. In fact, U.S. Senator Ted Cruz on December 13, 2018, introduced legislation (the Blocking Iranian Illicit Finance Act) that was designed to sanction Iran's upcoming sovereign cryptocurrency. The bill called for "an assessment of the state and non-state actors that are assisting the Government of Iran in creating a sovereign cryptocurrency."

By making use of blockchain technology and cryptocurrencies to facilitate transactions, Iran would be joining other blockchain-based payment networks, which many believe could make the traditional SWIFT network obsolete.

Last November, Iran signed a trilateral blockchain cooperation agreement with Russia and Armenia. Russian President Vladimir Putin later said that Russia is "actively working" with partners to establish financial systems that are entirely independent of SWIFT, without naming the partner countries

Mexican Cartels Using Chinese Money Laundering Networks — Bitcoin Mules

As has been widely reported, the U.S. Senate Judiciary Subcommittee, recently held a hearing on Border Security and Immigration that revealed that Mexican drug cartels are increasingly using Chinese cryptocurrency money laundering networks.

The relationship between China and Mexican drug cartels stems from China being a major supplier of precursor substances necessary to manufacture methamphetamine (meth). China is also a major source the extremely dangerous synthetic opioid Fentanyl. It is approximately 50 to 100 times more powerful than morphine and is now also used to boost the potency of illicit cocaine and heroin.

The Chinese money laundering network, also known as the Chinese Underground Banking Systems (CUBS) arose from the country's strict controls on citizens moving money out of the country. Now it appears the Mexican cartels (as well as drug gangs in Europe and Australia) are leveraging CUBS cryptocurrency brokers.

Banks in Some Countries Face Legal Action for Refusing to Bank Crypto Businesses

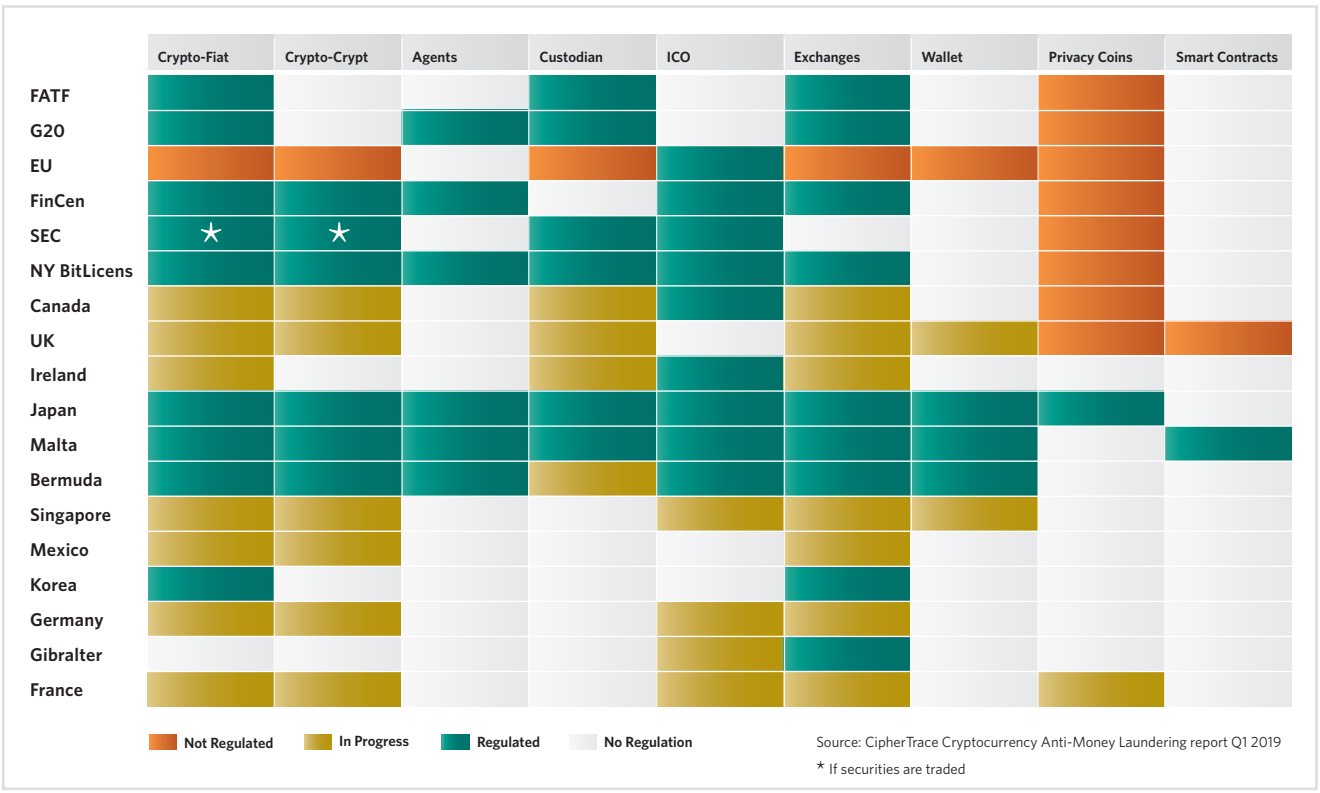
Also, in Q1, banks in Israel and Brazil faced legal action that forced them to reinstitute banking relationships with exchanges and other money service business. It seems that as many MSBs in the cryptocurrency space have cleaned up their acts under the weight of strict regulations. Now some regulators and courts feel that banks should treat these crypto businesses as good corporate citizens. This has added to the needs for banks to monitor hidden crypto asset assets in their customer accounts and payment networks, and to also make it safe to accept crypto customers.

Global Regulatory Moves

2018 saw lawmakers around the world add more teeth and broader scope to AML and CTF regimes, such as the adoption the European Union's Fifth Anti-Money Laundering Directive (AMLD5), which increased the scope of the EU's regulatory perimeter to include cryptocurrency exchanges as well as those that provide custodian wallet services. However, regulatory moves in Q1 2019 were not dominated by such massive legislative actions. Instead, we saw such wide-ranging actions as the French government recommending a ban on anonymous altcoins or the California State Assembly introducing a bill that would allow cannabis-related businesses to pay their taxes and fees in stable coins. The UK and Mexico also drafted new regulations in Q1, which are waiting for comments and approval.

The State of Cryptocurrency Anti-Money Laundering

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 understood by lawmakers attempting to regulate digital assets based on the physics of fiat currency.



Stage of AML Regulation and Depth of Coverage by Region

Global Cryptocurrency AML Timeline

FATF – Published New Draft Interpretive Note Further Clarifying Guidance for Crypto Regulations

The Financial Action Task Force (FATF) was founded to address concerns about money laundering and the threat it poses to the world financial system. The inter-governmental body advises 36 member countries and two regional organizations and is one of the most influential voices globally on combating financial crimes. The FATF's mandate was expanded in 2001 to include efforts to combat terrorist financing (CFT). Its influence also extends beyond its member countries, as a number of regional Financial Action Task Forces around the world provide guidance to regulators in the Caribbean Latin America, the Middle East, and North Africa. Its MoneyVal associate provides guidance to countries of Europe outside the EU, including Malta.

In February 2019, the FATF published a draft of an Interpretive Note to Recommendation 15, further clarifying how its regulation recommendations apply to virtual assets. These changes will guide regulatory authorities in a member country when identifying risk, sharing information, and monitoring virtual asset service providers. Additionally, virtual asset service providers will need to be registered or licensed, agree to monitoring by competent authorities, and comply with FATF Recommendations 10-21 (which include policies regarding customer due diligence, record-keeping, politically exposed persons, higher-risk countries, suspicious activity reports, ad confidentiality). The note will be adopted as a part of FATF Standards in June 2019.

Read CipherTrace's Response to FATF Regarding Regulation and Monitoring of Virtual Asset Service Providers here https://ciphertrace.com/response-to-fatf-on-vasp-regulation/

Canada – New Regulations for Canadian Exchanges Considered After QuadrigaCX Collapse

In March, the Canadian Securities Administrators (CSA) and the Investment Industry Regulatory Organization of Canada (IIROC) released a consultation paper. It aims to gather input from Fintech companies, market participants, investors, and other crypto stakeholders on how to best develop a regulatory framework for Canadian cryptocurrency exchanges. The development of this framework is largely motivated by investor protection concerns following the QuadrigaCX collapse. The paper, titled Proposed Framework for Crypto-asset trading Platform, poses 22 consultation questions and asks that all comments be submitted in writing by May 15, 2019.

Additionally, the paper proposes several solutions to issues of keen interest to regulators. The most notable recommends cryptocurrency exchanges cease short selling and margin trading—two extremely popular methods of trading. According to the paper, "To reduce the risks of potentially manipulative or deceptive activities, in the near term, we propose that Platforms not permit dark trading or short selling activities or extend margin to their participants."

Feedback from the paper will be used to "establish a framework that provides regulatory clarity to Platforms, addresses risks to investors and creates greater market integrity." No cryptocurrency exchanges in Canada are currently recognized as legal exchanges, and therefore are not authorized to operate as a marketplace or dealer. This means any exchanges acting as such in Canada are beyond the CSA' purview. The CSA continues to urge Canadians to be cautious when considering buying crypto assets. As to whether or not this framework could prevent another QuadrigaCX-type debacle, experts believe that without adequate enforcement resources it is unlikely that any new rules would have any dramatic effect.

United States — SEC Releases "New" Crypto Guidance

The United States Securities and Exchange Commission (SEC) published new guidelines this April 2019 to set standards in determining whether or not an ICO is an investment contract and therefore subject to U.S. federal securities law. According to the guidelines, titled Framework for 'Investment Contract Analysis of Digital Assets, an investment contract exists "when there is the investment of money in a common enterprise with a reasonable expectation of profits to be derived from the efforts of others." The framework goes on to further define these three elements as it applies to digital assets.

However, it should be noted that the framework clearly states that it "represents the views of the Strategic Hub for Innovation and Financial Technology [FinHub]. It is not a rule, regulation, or statement of the Commission, and the Commission has neither approved nor disapproved its content." It also does not supersede any case law, legal requirement, or statements or guidance from the Commission or staff. The SEC further explained that the framework was never meant to be an exhaustive explanation of the law but, rather, to give clarity and guidance that makes it easier for token issuers to determine whether or not their ICO would qualify as a security. The Commission says FinHub continues to encourage market participants to seek the advice of securities counsel to follow current securities law.

SEC Publishes First ICO No-action Letter

In what came as somewhat of a surprise decision, a little-known jet-leasing company received unprecedented approval from the SEC to sell a digital token—specifically, one that it does not regulate. The SEC declared that the Division of Corporation Finance would not recommend enforcement action to the Commission if TurnKey Jet decides to sell its ICO token (TKJ) without registering with the SEC. This is the SEC's first ICO no-action letter, confirming TKJ tokens are not securities as long as they abide by the terms set forth in the letter. Among the conditions people who buy the tokens will not receive any ownership stake in TurnKey Jet, the tokens cannot be traded publicly, and the company will face restrictions on using proceeds from coin sales to invest in its business. However, as a result of SEC staff giving Turnkey Jet a No-action letter the company will now be able to sell tokens that customers can use to reserve private jets.

Interestingly, TurnKey's decision to find relief from the SEC results from the limitations it faced with traditional banking institutions. Limited banking hours can stall wires for last-minute private jet flights. According to a CoinDesk interview with James Prescott Curry, a TurnKey lawyer that helped draft the SEC proposal, these things are "spur-of-the-moment… Rich guys have wire money ready to go, but they are subject to banking hours."

While this letter will not likely have broader implications for ICOs overall, it is one example of how blockchain technology can alleviate friction presented by the traditional banking system. This "no action" further seems to add to the SEC's recent trend towards softening the correlations between token and security.

SEC Reconsiders Current Rule on the Custody of Digital Assets

This March, the Commission published an open letter to Karen Barr, president and CEO of the Investment Adviser Association, soliciting input on ways to improve the existing Custody Rule as it applies to digital asset trade and custody. This inquiry is a result of the rapid growth of the digital asset market as more and more investment advisers are seeking to invest in digital assets on behalf of their clients. The letter probes how characteristics specific to digital assets impact compliance with the Custody Rule, especially in regard to non-DVP (delivery versus payment) arrangements, where a client's custodian releases payment or securities before the certainty of settlement. The SEC will use the feedback when considering any regulatory changes.

States

California Bill Aims to Allow Stablecoins for Tax Payments from Cannabis-Related Businesses

In February, the California State Assembly introduced AB-953, which would allow cannabis-related businesses to pay their taxes and fees in stable coins— cryptocurrency that is designed to minimize volatility by fixing its value to a currency or traded commodity. The bill defines stable coins as digital assets that have "price stable characteristics pegged to United States dollars and United States dollars serve as collateral to that digital asset." According to the bill, it will be up to the city or county to determine whether to store the stable coins in a digital wallet controlled by that jurisdiction or to convert any payments made by stable coins into United States dollars and deposit them into an account of that jurisdiction.

Under current US legislation, cannabis-related businesses are still illegal under federal law. For this reason, banks have an aversion to onboarding these clients, resulting in cash-only businesses that have no choice but to pay their taxes in cash.

Under current US legislation, cannabis-related businesses are still illegal under federal law. For this reason, banks have an aversion to onboarding these clients, resulting in cash-only businesses that have no choice but to pay their taxes in cash. The US banking industry's decision to avoid working with cannabis-related businesses opens a gap in a multibillion-dollar industry that digital currency and blockchain technology is ready to fill.

Texas Wants to Ban Privacy Coins

The U.S. state of Texas has also proposed some as yet not clearly defined legislation for mandatory KYC and a ban on privacy coins. The proposed law, Texas House Bill 4371, would require people to verify the identity of senders before receiving cryptocurrency.

New Hampshire Bill Aims to Legalize Bitcoin for State Payments in 2020

Lawmakers in the U.S. state of New Hampshire are currently considering a bill to legalize payment of fees and taxes in Bitcoin (BTC), documents originally published on Jan. 3 reveal.

US State of Wyoming Passes Two New Blockchain, Crypto-Related Bills

The state legislature of Wyoming has reportedly passed two new house bills that aim to foster a regulatory environment conducive to cryptocurrency and blockchain innovation. One bill introduced into the legislature On Jan 18 is bill meant to clarify the classification of cryptocurrencies.

Ireland — Government Amends Anti-Money Laundering Bill to Include Cryptocurrency

In January, the government of Ireland approved a bill to incorporate the European Union Fifth Anti-Money Laundering Directive into their existing legal framework—the Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Bill. These amendments will make it easier for regulators to monitor cryptocurrency exchanges and wallet providers in an attempt to counter the use of virtual currencies for terrorist financing.

France — National Assembly Considers Banning Privacy Coins

The Finance Committee of France's National Assembly has recommended a complete ban on privacy-focused cryptocurrencies. In the committee's report (in French), the committee's president, Éric Woerth, suggests it would be appropriate to propose a ban on activity related to cryptocurrencies built with the goal of providing greater levels of anonymity to users.

Mexico — The Bank of Mexico Proposes Crypto Exchange Transaction Regulation

On March 11, 2019, the Bank of Mexico (Banxico) released a public consultation plan that proposed several regulations to help prevent crypto-related money laundering and terrorism financing. Some observers and the press have called some of these regulations "draconian," essentially having the result of banning financial institutions from transacting with cryptocurrency exchanges; however, CipherTrace has not interpreted Banxico's position as being that extreme. The proposal (translated from the original Spanish publication) states: "...it is considered convenient to maintain a healthy distance between virtual assets and the financial system. However, despite the foregoing, the Central Bank seeks to promote and take advantage of the use of technologies that could have a benefit from the perspective of efficiency or functionality, as long as these technologies are used in the context of the internal operation of the institutions."

Although these proposed regulations do not explicitly ban cryptocurrency exchanges in Mexico, in the case of the more extreme interpretation of the proposal any exchange transacting in fiat currency would essentially be strangled without access to the traditional banking system.

These guidelines are still just draft provisions, and Banxico will be collecting responses from the community for the next two months on how to best amend the proposed regulations.

Japan — New Crypto Regulations Cap Leverage for Margin Trading

In March 2019, Japanese regulators approved amendments to their financial instruments and payment services laws, limiting leverage for margin trading at two-to-four times initial deposits. All exchanges that offer margin trading will be required to register with the government and consent to monitoring similar to securities traders in an effort to protect investors. Enforcement of these regulations will begin by April 2020, and exchanges are required to register within 18 months of that date.

These regulations are a result of investor protection concerns stemming from Japan's recent boom in margin trading. According to the Japan Virtual Currency Exchange Association, margin trading reached about 11 times the scale of cash transactions in Japan by the end of 2018. Therefore, these new regulations will differentiate between cryptocurrency operators that engage in margin trading from those that issue tokens in ICOs. Ideally, this categorization will enable Japan's Financial Service Agency (FSA) to better monitor and prevent scam investment schemes, protecting investors and promoting the overall health of the crypto economy.

Germany — Finance Ministries Publish Paper on Regulation of ICOs and Utility Tokens

In March 2019, the German Federal Ministry of Finance and the Federal Ministry of Justice and Consumer Protection published a paper addressing key issues regarding the regulation of ICOs and utility tokens. Under current German law, securities must be represented by physical documents kept at a central securities depository, meaning ICOs cannot be classified as securities. Therefore, this paper proposes the possibility of regulating the public offer of ICOs and introduces the prospect of electronic securities.

Furthermore, the paper addresses the risks associated with unregulated utility tokens and proposes that utility token providers adhere to adequate risk-disclosure obligations by publishing an information sheet prior to an initial public offering. The paper further states that the content and the order of information on this sheet should be regulated, and the publication must be authorized by the BaFin—the financial regulatory authority for Germany—prior to its release.

UK — Government Says Will Go Further Than AMLD5 On Regulating Cryptoassets

Amid concerns that MSBs could be putting consumers at risk by offering unauthorized services, the UK's financial watchdog The Financial Conduct Authority (FCA), has proposed a consultation on existing guidance around crypto assets. The (FCA), the US equivalent to the Securities and Exchange Commission

(SEC), launched its consultation after the UK Cryptoasset Taskforce requested additional guidance and clarity on the current regulatory framework. The FCA has set a 10-week consultation period to and will publish feedback and the final text of the guidance this Summer.

Iran — New Regulatory Framework for Cryptocurrencies and Introduction of a State-backed Cryptocurrency

The Central Bank of Iran published on its official website on January 28th, 2019 a "Version 0.0" of its regulatory framework for cryptocurrencies. Among other impacts, it would reverse a previous ban on cryptocurrencies, but still impose restrictions on the use of global digital currencies in the Islamic Republic.

Iranian Banks Launch Gold-Backed Cryptocurrency "PayMon"

In February, four Iranian banks—Bank Mellat, Bank Melli Iran, Bank Pasargad and Parsian Bank—partnered with the blockchain startup Kuknos Company to release the gold-backed national cryptocurrency PayMon (PMN). According to Kuknos advisor Soheil Nikzad, PMN is planned for release in a multi-stage token sale, privately to banks at first with the plan to eventually conduct a public securities offering, pending regulations. Kuknos is currently in talks with regulators to determine how best to make the cryptocurrency available throughout the country.

According to Nikzad, although PMN is compatible with international finance systems, the main goal of the national cryptocurrency is to reduce costs and friction in domestic transactions. As it stands, the Central Bank of Iran only allows the use of cryptocurrencies pegged to the Iranian rial and issued by the central bank itself as a payment method, prohibiting the use of "unapproved" cryptocurrencies domestically.

PayMon is the result of last year's newly reinstated US sanctions against Iran. These sanctions led to SWIFT (the Society for Worldwide Interbank Financial Communications) baring a number of Iranian banks from using their financial messaging system—a necessity for most banks engaging in cross-border payments. In other words, without SWIFT, Iranian companies cannot pay for imports or receive payments for exports through the traditional banking system. Theoretically, the PayMon will be able to bypass this ban and give Iranian banks access to cross-border markets again.

Russia — Russian Duma Approves SWIFT-Alternative for International Use

Similar to Iran, the US has imposed political and economic sanctions on Russia. In March, the Russian State Duma approved the international use of SPFS (System for the Transfer of Financial Messages). Russia began developing SPFS in 2014, after the US government threatened to disconnect Russia from the SWIFT system. Although it this new system has severe limitations, as an alternative to SWIFT, it would greatly reduce the risks associated with Western sanctions such as a SWIFT ban, which would make it extremely difficult for Russian banks to process cross-border payments.

Although SPFS has been widely used throughout Russia since 2014, this marks the first time Russia will begin reaching out to international partners to use their system. According to the Central Bank of Russia, SPFS already complies with international standards and foreign players can easily be integrated into it. Anatoly Aksakov, Chairman of the State Duma Committee on Financial Market, has confirmed that Russia is in talks with Iran, Turkey and India about joint use of SPFS. There reportedly are also plans to integrate SPFS with China's Cross-Border Interbank Payment System (CIPS) a payment system that offers clearing and settlement services for its participants in cross-border RMB payments.

Crypto-Ruble Delayed as Reading of Bill on Digital Financial Assets is Postponed

The second reading of Russia's draft law on cryptocurrencies has been postponed to April in order to further define cryptocurrencies, tokens, and smart contracts. Although this bill is mainly focused on the governance of cryptocurrency exchanges and marketplaces, clear cryptocurrency regulations are vital if Russia plans to continue with their proposed Crypto-Ruble. The deadline for the adoption of these regulation has been moved to July, 2019.

Anatoly Aksakov, Chairman of the Russian State Duma's Financial Markets Committee, told local news outlet RIA Novosti in January that the Crypto-Ruble will not differ from the fiat ruble in any way other than existing on the blockchain. According to his calculations, the crypto-ruble may appear in Russia in as soon as two or three years.

Russians Will Need a Special 'Visa' to Fund Crypto Accounts from Russian Banks

If passed by the State Duma, a new law will require crypto owners to obtain a special 'visa' to transfer money from Russian bank accounts into digital financial assets, especially digital tokens.

