CIPHERTRACE

Cryptocurrency Anti-Money Laundering Report, 2018 Q4

CipherTrace
Cryptocurrency Intelligence
January 2019

Q4 2018 CRYPTOCURRENCY ANTI-MONEY LAUNDERING REPORT

Q4 2018 Cryptocurrency Anti-Money Laundering Report

Summary

Bad actors need to launder the $US 1.7 billion of cryptocurrency stolen and scammed in 2018. Furthermore, they need to get it all done before tough new global anti-money laundering (AML) and counter terror financing (CTF) regulations go into effect over the next year.

Of the $1.7 billion, hackers stole more than $950 million from cryptocurrency exchanges and infrastructure during 2018, which is 3.6x higher than in 2017. Cyber crooks also developed ingenious new techniques to drain millions more from user accounts and wallets. On top of that, ICO exit scams, phony exchange hacks, and Ponzi schemes victimized investors and cryptocurrency users for almost three quarters of a billion dollars. These numbers only represent the loot from crypto crimes that CipherTrace can validate; we have little doubt that the true number of crypto asset losses is much larger.

The total dollar value of Q4 2018 thefts was lower than the number for Q3. This is partially due to the falling price of all cryptocurrency. In addition, rather than hacks on exchanges and wallets, inside jobs began to dominate the crypto crime landscape. It appears that a new breed of cybercriminals steeped in computer science and FinTech found it easier to commit fraud against unwitting investors and exchange users as opposed to attacking hardened IT systems.

Bad actors will need to launder $1.7 Billion in stolen and scammed cryptocurrencies before tough new global AML and KYC regulation go into effect over the next year.

Whether it's theft by hackers or inside jobs like exit scams, criminals must launder all of these ill-gotten gains before they can spend those funds in the real economy. In addition, global gangs, terrorist groups, and cyber criminals must hide their money trails. These bad actors are clearly flocking to jurisdictions with weak AML and Know Your Customer (KYC) regimes, because in our Q3 report we published the results of research showing 97% of criminal bitcoin flows into unregulated cryptocurrency exchanges.

While recognizing the tremendous potential for innovation provided by blockchain technology, this dark side of the cryptocurrency ecosystem is not lost on regulators. And 2018 saw major moves around the globe to rein in the Wild West aspect of these markets. By 2020 most modern economies will have deployed strict cryptocurrency anti-money laundering regulations.

The global impacts of this pending legislation are being felt by the money launderers themselves. Those with US ties are choosing to comply, while those in money laundering havens and sanctioned countries continue to innovate.

2018 Highlights

- In the European Union, the Fifth Anti-Money Laundering Directive (AMLD5) went into effect. Entities in the cryptocurrency space must be prepared within less than a year's time to come into compliance.
- To combat entities attempting to circumvent political sanctions, such as those that went into effect against Iran in 2018, the U.S. Treasury Office of Foreign Assets Control (OFAC) for the first time ever sanctioned individuals and identified their digital currency addresses.
- The Financial Action Task Force (FATF) called for an effective global response to the AML / CTF risks associated with virtual asset financial activities. The highly influential global regulatory body announced its recommendations for implementing risk-based AML / CTF regulations. Member countries must implement these strict new guidelines by June 2019, and cryptocurrency exchanges and other entities are already preparing to comply.
- Japan banned privacy coins and allowed exchanges to self-regulate.
- Bermuda extended its global regulatory leadership by rolling out a number of digital asset business (DAB) standards throughout the year, including the introduction of strong crypto custody rules in December.
- Malta became the first country to implement comprehensive AML regulation with the stated goal of attracting Virtual Financial Assets businesses (VFAs).
- For the first time ever, the U.S. Securities and Exchange Commission (SEC) took regulatory action against a cryptocurrency exchange for running an unregistered securities trading operation.
- The U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN) announced a number of major moves in the AML space, including defining crypto-to-crypto services as "money transmitters." This effectively brings mixers and tumblers under the rules of the Bank Secrecy Act (BSA). They also enlisted the help of the IRS to ensure virtual currency money service businesses (MSBs) understand and comply with their regulatory obligations under FinCEN and BSA rules.
- In Vietnam, crypto con artists perpetrated the largest ever ICO exit scam, defrauding investors of $660 million (all dollar amounts in this report are $US, unless otherwise specified).
- In Japan, hackers pulled off the largest cryptocurrency heist in history, robbing users of a major cryptocurrency exchange of $530 million. This breach was followed in October by a $70 million theft from an exchange in Osaka.
- A relatively new form of identity theft called SIM Swapping became popular, with cybercriminals stealing tens of millions of dollars from cryptocurrency exchange users and a California-based crypto start-up.
- Fast freezes stopped crooks before they got away with the money. Starting with Bancor's backdoor incident, the trend in the cryptocurrency community is it to attempt to claw back stolen funds by freezing the tokens at exchanges or through smart contracts.

Top 10 Trending Crypto Threats

1. **SIM Swapping:** An identity theft technique that takes over a victim's mobile device to steal credentials and break into wallets or exchange accounts to steal cryptocurrency (page 9).
2. **Crypto Dusting:** A new form of blockchain spam that erodes the recipient's reputation by sending cryptocurrency from known money mixers (page 11).
3. **Sanction Evasion:** Nation states using cryptocurrencies has been promoted by the Iranian (see page 13) and Venezuelan (see page 13) governments.
4. **Next-Generation Crypto Mixers:** Money laundering services that promise to exchange tainted tokens for freshly mined crypto, but in reality, cleanse cryptocurrency through exchanges.
5. **Shadow Money Service Businesses:** Unlicensed Money Service Businesses (MSBs) banking cryptocurrency without the knowledge of host financial institutions, and thus exposing banks to unknown risk.
6. **Datacenter-Scale Crypto Jacking:** Takeover attacks that mine for cryptocurrency at a massive scale have been discovered in datacenters, including AWS.
7. **Lightning Network Transactions:** Enable anonymous bitcoin transactions by going "off-chain," and can now scale to $2,150,000.
8. **Decentralized Stable Coins:** Stabilized tokens that can be designed for use as private coins.
9. **Email Extortion and Bomb Threats:** Cyber-extortionists stepped up mass-customized phishing emails campaigns using old passwords and spouse names in 2018. Bomb threat extortion scams demanding bitcoin spiked in December.
10. **Crypto Robbing Ransomware:** Cyber-extortionists began distributing new malware that empties cryptocurrency wallets and steals private keys while holding user data hostage.

Thefts and Exit Scams

FY 2018 Exchange and Infrastructure Thefts

In total, $950 million worth of cryptocurrency was stolen from exchanges and infrastructure in 2018. Korea and Japan were home to most of the thefts, 58%, throughout 2018. Whereas in the first three quarters thefts by hackers dominated the crypto crime scene, the fourth quarter was mostly about inside jobs or fraud.

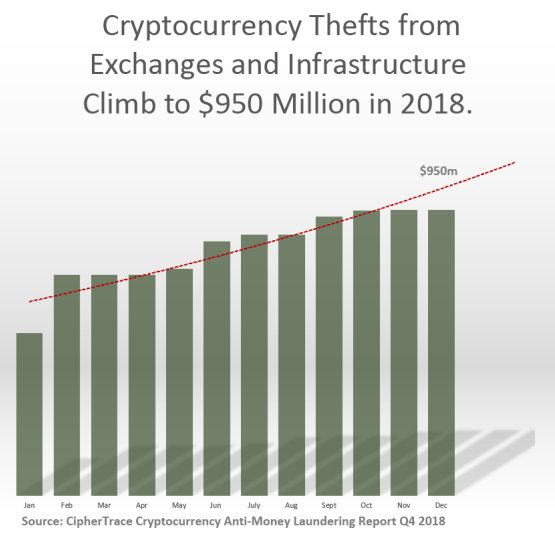


Figure 1: Cryptocurrency Stolen from Exchanges and Infrastructure

The theft numbers were significantly lower in Q4, owing mostly to a lack of mega heists like those that occurred in Italy, Japan and Korea earlier in 2018. The significant price erosion of all cryptocurrencies in the second half also contributed to the lower total dollar value of stolen tokens. However, the total amount stolen in 2018 is 3.6 times as much as in 2017 and over seven times as was stolen in 2016.

Figure 2: Cryptocurrency Thefts for Exchange and Infrastructure since 2016

Exit Scams

On top of outright cryptocurrency thefts, investors lost almost 3/4 billion dollars from inside threats such as "exit scams" in which developers and founders absconded with Initial Coin Offerings (ICOs) or users' custodial crypto funds, and then disappeared into the night.

$3M Frozen from Pure Bit Exit Scam

One recent exit scam in Q4 began on November 4 when a group in Korea called Pure Bit raised nearly $3 million in an Ethereum ICO. The funds were purported to be used to build a cryptocurrency exchange. However, the founders soon fled with all of the Ethereum. Based on a request from a major business publication, the country's second-largest exchange froze the crypto assets and blocked the scammers' accounts. In an odd twist, victims of the exit scam were notified of plans to refund all the missing assets. It wasn't clear whether the sudden change of heart was due to guilt, the involvement of law enforcement agencies, or massive coverage by the country's mainstream business media.

> "This is Pure Bit. First off, I would like to apologize to everyone that was affected by the ICO. Since November 5, I raked in 16,000 ETH and did not open a crypto exchange as promised. I kicked out everyone in our social media chat groups and disappeared without any message. I negatively affected investors in the project psychologically and financially.
>
> "I made an unforgivable mistake that cannot be turned around, blinded by money. It has been less than a day, and I have already started to suffer from guilt. Although it cannot be compared with the hardship faced by the investors, I also felt significant guilt. I sincerely apologize to all of the investors in the ICO who were affected by the operation."

Pincoin ICO Exit Scam Steals $660 Million from Vietnamese Investors

In April 2018, a Vietnamese cryptocurrency company, Modern Tech, launched an ICO raising $660 million from approximately 32,000 people. The scam involved a "Pincoin" token ICO, in which the founders promised constant returns to investors of 48% each month. Investors could also receive an 8% commission for bringing in new investors. The group subsequently launched another token, iFan (a social network token for fans of celebrities).

Initially, Pincoin investors received cash from their investment, but Modern Tech subsequently began paying out rewards to Pincoin investors in iFan tokens. The iFan tokens were supposedly based on Ethereum.

Sadly, it turned out to be the mother of all exit scams. The Mod Tech team disappeared, leaving throngs of duped investors protesting outside their empty headquarters.

BitConnect Promoter Arrested on Suspicion Of Bilking Cryptocurrency Investors Out Of Millions Of Rupees
In August, authorities arrested Divyesh Darji, the Indian head of BitConnect, at the Dubai airport. Darji is believed to have been a core promoter of a scheme to engineer an exit scam. The accused crypto charlatan held seminars in India and other countries at which he promised a daily interest rate of 1% on investments in BitConnect coins. BitConnect raised $14.5 million from thousands of investors. Unfortunately, the coins were virtually worthless when the exchange went belly up earlier in 2018.

MapleChange – $6M "Hack" or Exit Scam?

MapleChange a small, purportedly Canadian Exchange reported in late October that it had lost 913 bitcoin ($US6M) in a "Hack," and could not refund the cryptocurrency to users. The company issued an initial statement:

> "Due to a bug, some people have managed to withdraw all the funds from our exchange. We are in the process of a thorough investigation for this. We are extremely sorry that it has to come to an end like this. Until the investigation is over, we cannot refund anything."

Shortly after, MapleChange announced it would be unable to pay back the cryptocurrency to its users and was closing down.

> "We have sustained a hack, and we are investigating the issue. Because we have no more funds to pay anyone back, the exchange has to close down, unfortunately. This includes all of our social media."

However, the exchange did not mention the involvement of law enforcement or any technical details of the alleged hack. After users demanded more information, and almost immediately after the "hack," the exchange deleted its website, Twitter account, and other social media handles along with the online identities of its executives and chief executive officer.

Sky Mining – $35M Lost in Vietnam Mining scam

Investors in a Vietnamese cryptocurrency mining venture, Sky Mining claim to have lost up to $35 million when the company's founder and CEO went missing along with all the assets and mining rigs in July.

Spankchain Reentrancy Theft Foreshadows Ethereum's Hard Fork Vulnerability

In an attack that used a reentrancy bug similar to the technique used in the 2017 DAO hack, Ethereum-based adult entertainment platform SpankChain suffered a smart contract security breach in October. Anonymous attackers stole 165.38 Ethereum (ETH) or around $38,000 from the platform's payment channel smart contract, and immobilized $4,000 worth of internal tokens. The hack was detected by SpankChain a day after

it occurred. They offered a reward, and the funds were returned after paying the hacker a $9,000 bounty three days later.

Reentrancy vulnerabilities are the reason that the Ethereum hard fork to Constantinople Proof-of-Stake—originally scheduled for January—was delayed until "late February."

Next-Generation Crypto Crime Leverages SIM Swapping to Steal Tokens

"SIM Swapping" represents a new and insidious threat to crypto businesses, users, and investors that became widespread in 2018. This form of identity theft involves transferring the victim's phone number to a SIM card held by a hacker. Once SIM Swapping attackers receive the compromised phone numbers, they use them to reset passwords and break into the victims' accounts, including accounts on cryptocurrency exchanges.

SIM Swapping targets a vulnerability present in a common form of two-factor authentication and two-step verification in which the second factor is an SMS or a call placed to a mobile phone. Users can protect themselves with stronger app-based two-factor authentication and hardware wallets.

The scam revolves around exploiting a mobile phone carrier's ability to swiftly port a phone number to a new SIM when a mobile customer loses a phone. Large cryptocurrency investors are increasingly targets of this attack, which typically starts with the hacker gathering information about the victim either through phishing emails or by purchasing it off the dark web.

> ***"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."***
> **Silicon Valley REACT Task Force**

The attack is often initiated through social engineering or by compromising an insider, often at a retail location. 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."

Using the stolen identity, the hacker then contacts the victim's mobile service provider and asks the provider to port the victim's phone number to the scammer's SIM. In early 2018, a hacker used the technique to allegedly steal $23.8 million from a wealthy investor who, incidentally, is suing AT&T for the millions in stolen loot along with an additional $200 million in punitive damages.

In another instance in the fall of 2018 hackers used SIM Swapping to break into CrowdMachine, a California-based cryptocurrency startup, and steal all of its reserve coins worth a $14 million. CrowdMachine reported

the theft to a California computer crimes task force on September 22, and less than a week later authorities in Oklahoma used a search warrant to arrest two men for allegedly perpetrating the cybercrime.

In July of 2018, Bulgarian police arrested three suspects on suspicion of stealing $5M via SIM Swapping. In the same month, California police charged a 20-year-old college student with stealing $5M. And then in November, the Silicon Valley REACT team arrested a 21-year-old who allegedly stole $1M using the same technique.

“It’s not just stealing millions from millionaires,” according to Caleb Tuttle, a detective with the Santa Clara County District Attorney’s office. “Most of the victims are not in that category. Most are people who are having their life’s savings or their child’s college savings stolen; the reality is there’s a lot of other thefts involving much more diminished amounts that are really negatively impacting peoples’ lives.”

“[the attackers] are predominantly interested in targeting cryptocurrencies for the ease with which these funds can be laundered through online exchanges…”

Lieutenant Rose said even though a successful SIM swap often gives the perpetrator access to traditional bank accounts, the attackers seem to be mainly interested in stealing cryptocurrencies. According to Rose, “[the attackers] are predominantly interested in targeting cryptocurrencies for the ease with which these funds can be laundered through online exchanges, and because the transactions can’t be reversed.”

Erin West, the Santa Clara County deputy district attorney, put out a call for more victims to come forward.

Cryptocurrency Money Laundering Examples

Mixers

Cryptocurrency mixers and tumblers blend potentially identifiable cryptocurrency funds with large amounts of other funds. Since transactions using bitcoin and other cryptocurrencies leave a trail in the public ledger, these services have arisen to obscure the original source of the funds.

Many people use mixers and tumblers to keep their cryptocurrency transactions private. These services typically do not require KYC checks, and they are primarily used to anonymize fund transfers between services. This might lead to the logical conclusion that mixers are almost exclusively used for laundering money or hiding profits from illicit activities. But this is not always the case: some users have legitimate privacy or political reasons for wanting to obfuscate their money trail.

BestMixer Invents "Crypto Dusting" to Promote Itself and Taint Users

On October 23, 2018, Bitcoin users began receiving minuscule amounts of BTC from BestMixer.io along with a message promoting the company's service, which allows users to mix bitcoin, Litecoin, and Bitcoin Cash. These tiny transactions essentially amounted to a cost-effective mass advertising campaign—i.e., blockchain spam.

But it wasn't simply spam advertising: by sending Bitcoin to the top BTC addresses, BestMixer was effectively tainting these users by forcing them to transact with a mixer via these tiny transactions. By dusting every address with funds from a mixer, the campaign had the effect of soiling users' reputations. The reason to dust so many addresses was an attempt to confuse blockchain analytics tools in order to circumvent AML, which was their stated objective.

CipherTrace issued an alert on this campaign, calling it "crypto dusting," because unlike other forms of spam advertising this technique had a more sinister motive. Based in Curacao—one of the world's major money laundering jurisdictions according to the US Department of State—Bitmixer promotes itself as the only legal bitcoin tumbler offering "blockchain analysis resistant coins." The service offers three tiers of money laundering services. Their premium service appears to promise freshly mined coins, but transaction tracing reveals these coins are cleansed at cryptocurrency exchanges with poor AML policies. For more details, see https://ciphertrace.com/crypto_dusting/.

Crypto-to-Crypto

ShapeShift Gets to Know Its Customers

On September 4, 2018, ShapeShift, a well-known crypto-to-crypto swapping service, announced it was implementing a mandatory KYC program. Although it was labeled a "membership" program, in reality it essentially mandated customers to open an account and provide data before trading on the platform. Perhaps as a sign of FinCEN's tougher stance this year (see page 14), the company cited regulatory pressure in its

decision. In an interview with Bloomberg news, ShapeShift's founder and CEO, Erik Voorhees, attempted to explain: “this is a precautionary move to derisk the company amid an ever-changing legal grey area.”

Naturally, the news of ShapeShift’s capitulation caused some consternation in the crypto community among diehard proponents of pure decentralization and anonymity.

It also illustrates that business reality typically gives way to needed regulation, however slowly. For a time, ShapeShift was able to operate an unregulated crypto-to-crypto swapping service, but growing global regulation finally began to bite. In 2018, ShapeShift assisted with 60 law enforcement inquiries from around the world including, 18 from US agencies, eight from Germany, and six from the UK.

In early January 2019, Shapeshift announced it was laying off a third of its employees. In a post on *Medium*, Vorhees cited a number of factors in its “Crypto Winter,” including the declining value of crypto assets held by the company. He also blamed ShapeShift’s sudden change in fortunes on its decision to bow to regulatory pressure and implement KYC, which “caused many of our most valuable API partners to leave us for competitors who have not perceived regulatory risks in the same way.”

Sanction Evasion

Iran Responds to Sanctions with Cryptocurrency

As U.S.-led sanctions against Iran went into effect in November, the Treasury's Office of Foreign Assets Control (OFAC) stepped up its focus on cryptocurrency. In an unprecedented move, OFAC not only began adding cryptocurrency players to its sanctions blacklist but also made associated cryptocurrency addresses public. As part of these enforcement efforts, OFAC for the first time ever also publicly identified digital currency addresses associated with these individuals.

"Treasury will aggressively pursue Iran and other rogue regimes attempting to exploit digital currencies and weaknesses in cyber and AML/CFT safeguards to further their nefarious objectives," explained Treasury Under Secretary for Terrorism and Financial Intelligence, Sigal Mandelker.

On October 10th, FinCEN warned virtual currency administrators and exchanges to watch for Iran using virtual currencies to circumvent sanctions. And then on October 30th, Iran announced its intent to use virtual currencies to avoid sanctions stating, "Cryptocurrencies can help bypass certain sanctions through untraceable banking operations." On November 4th, sanctions against Iran went into effect.

Venezuela Petro Turns Oil into Cryptocurrency

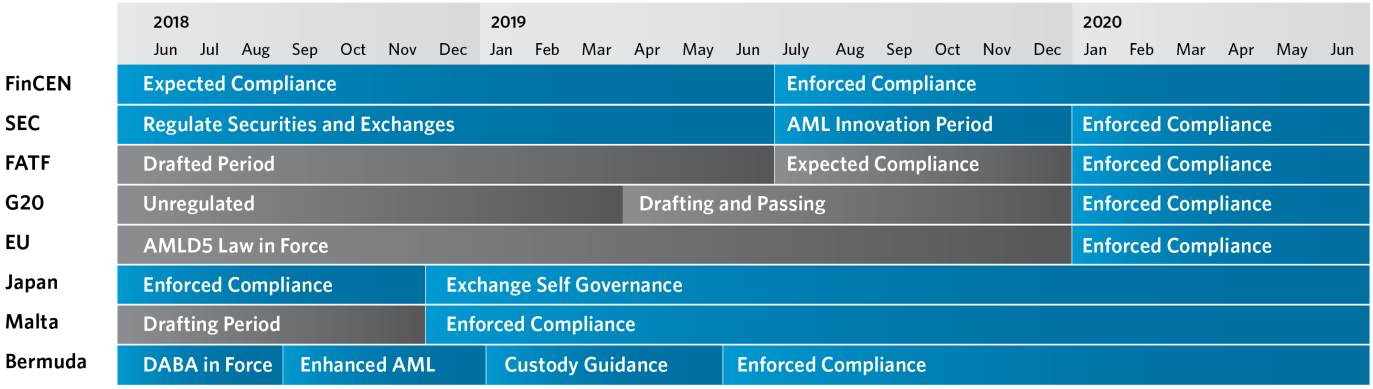
Venezuela continues to hope that the Petro, its supposedly oil-backed virtual currency, will enable the South American country to circumvent US led sanctions. On December 28, 2018, Venezuela filed a dispute (DS774) with the Word Trade Organization (WTO) to the US Presidential directive banning the Petro. See https://ciphertrace.com/first-presidential-cryptocurrency-order-blocks-russia-sanction-evasion-experiment/

The United States has 60 days to answer Venezuela's WTO complaint, after which time President Nicolas Maduro's government could ask the WTO to adjudicate.

Global Regulatory Changes

Global Timelines and Scope

2018 was a formative year for global cryptocurrency regulations both at a national level and at higher level. Some countries are taking a leadership position, others are grappling with the complexities, and most will be subject to one or more AML regime within the next 18 months. Some nations are accelerating the adoption of strict AML/CFT while others appear to be potential havens for money laundering, fraud, and tax evasion.



Source: CipherTrace Cryptocurrency Anti-Money Laundering Report Q4 2018

Figure 3: Global Cryptocurrency AML Timeline

United States

FinCEN – Broad Implications for Regulation and Enforcement of Crypto-To-Crypto

In the second quarter, the Director of U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN), Kenneth Blanco, gave a lengthy speech that is still rippling through the global cryptosphere. In addition to pointing out the mushrooming number of complaints regarding suspicious transactions received by the agency, he gave a glimpse into the agency's regulatory moves. These range from broader emphasis on enforcing AML rules to renewed scrutiny of anonymizing services (mixers and other crypto-to-crypto businesses) to delegating the Bank Secrecy Act (BSA) examiner role to the IRS.

Blanco took a balanced approach to the new possibilities created by innovation in FinTECH versus the dangers of criminals and other bad actors misusing blockchain technology. "Innovation in financial services can be a great thing—providing customers greater access to an array of financial services and at faster speeds than ever before," explained Blanco. "However, as industry evolves and adopts these new technologies, we also must be cognizant that financial crime evolves right along with it, or indeed sometimes because of it, creating opportunities for criminals and bad actors, including terrorists and rogue states."

Blanco's remarks dealt with defining crypto-to-crypto businesses: "individuals and businesses involved in accepting and transmitting anything of value that substitutes for currency, including virtual currency, are considered money transmitters," said Blanco. "Therefore, they must register with FinCEN according to rules in

the BSA. According to FinCEN rules, this also applies to anonymizing services (commonly called “mixers” or “tumblers”). Since they accept and transmit convertible virtual currency, they, therefore, have regulatory obligations under the BSA. Thus, our regulations cover both transactions where the parties are exchanging fiat and convertible virtual currency, but also to transactions from one virtual currency to another virtual currency.

SEC Chairmen Remarks on Need for AML in Crypto Asset Trading

At a CoinDesk event in Manhattan at the end of November, Jay Clayton, chairman of the U.S. Securities and Exchange Commission (SEC), showed some of the regulator’s cards regarding future plans for oversight in the crypto space. Among other topics, he gave his thoughts on the exchange ecosystem and the issue of when the Commission considers ICO-derived tokens to be securities. A key takeaway from his remarks was the need for anti-money laundering protections in crypto trading platforms.

EtherDelta

In a development that could have broader implications for the future use of smart contracts, the SEC targeted an Ethereum-based blockchain platform in the fourth quarter. The Commission took regulatory action against the company, EtherDelta, because of the way it was using smart contracts. According to the SEC, “EtherDelta’s smart contract was coded to, among other things, validate order messages, confirm the terms and conditions of orders, execute paired orders, and direct the distributed ledger to be updated to reflect a trade.” In other words, it looked to the SEC that the company was actually using the Ethereum blockchain to run an unregistered, and thus illegal, securities trading platform.

This represents the SEC's first enforcement action against a cryptocurrency platform operated as an unregistered national securities exchange, and the penalties turned out to be relatively painful. On November 8, 2018, the SEC announced that it had settled charges against EtherDelta’s founder, Zachary Coburn. Without admitting or denying the findings, Coburn consented to the order and agreed to pay $300,000 in disgorgement plus $13,000 in prejudgment interest and a $75,000 penalty. The SEC's order said it recognized Coburn's cooperation, “which the Commission considered in determining not to impose a greater penalty.”

In explaining the action, Stephanie Avakian, Co-Director of the SEC's Enforcement Division, said: "EtherDelta had both the user interface and underlying functionality of an online national securities exchange and was required to register with the SEC or qualify for an exemption.” Additionally, the SEC took issue with the way the platform works: “… an entity that provides an algorithm, run on a computer program or on a smart contract using blockchain technology, as a means to bring together or execute orders, could be providing a trading facility.”

"We are witnessing a time of significant innovation in the securities markets with the use and application of distributed ledger technology," said Steven Peikin, Co-Director of the SEC's Enforcement Division. "But to

protect investors, this innovation necessitates the SEC's thoughtful oversight of digital markets and enforcement of existing laws."

Airfox and Paragon Receive First Civil Penalties for ICO Violations
On November 16, 2018, the SEC settled charges against two companies, Airfox and Paragon Coin, that sold digital tokens in ICOs. These actions represented the first cases of the Commission imposing civil penalties solely for ICO securities offering registration violations. Both companies have agreed to return funds to harmed investors, register the tokens as securities, file periodic reports with the Commission, and pay $250,000 in penalties.

The Financial Action Task Force

FATF Q4 2018 Report on Virtual Currencies to Have Major Impacts in 2019
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. FATF's mandate was expanded in 2001 to include efforts to combat terrorist financing (CFT).

> ***"Crime never stops: criminals continue to find different ways to circumvent the measures that have been put in place to combat money laundering and terrorist financing. Technological innovations introduce efficiencies, but also provide opportunities for criminals, and new challenges for countries who need to regulate the use of these technologies."***

The FATF'S 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.

While technically a policymaking body, the FATF and these regional associates act as watchdogs that monitor the progress of countries in implementing necessary AML and CTF techniques. They also report on deficiencies in AML/CTF, including a bi-annual blacklist of high-risk countries. According to the FATF, this broad reach is critical because "countries which have not implemented sound measures to stop their financial system from abuse, present a risk to the entire global financial system."

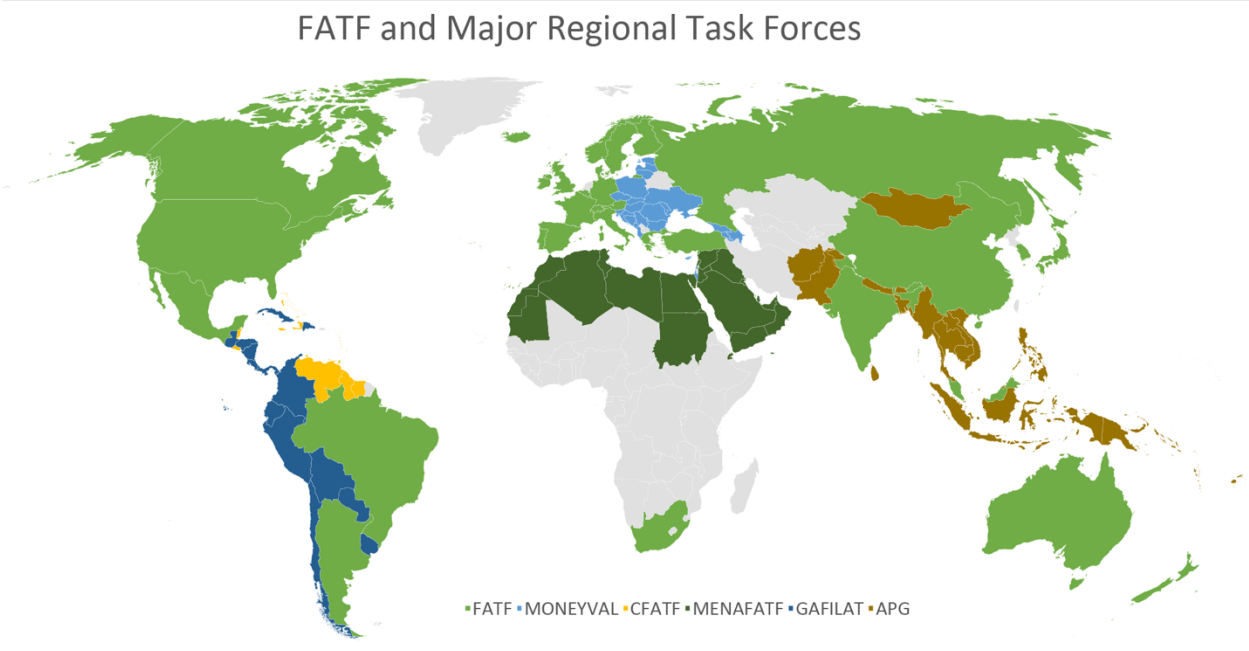


Figure 4: FATF's reach extends to a number of G-20 countries and countries of Europe outside the EU

G-20 leaders ask the FATF for tougher AML guidance at December meeting

At G-20 Leaders' Summit held in Argentina from November 30 to December 1, 2018, the FATF provided a report to the leaders on its efforts to combat money laundering and terrorist financing. The G20 expressed its continued support for the FATF's efforts in setting international standards for AML, but the leaders also requested FATF clarify how those standards apply to cryptocurrency activities. It is likely that since the EU had significantly raised the regulatory bar on AML/CTF with the enactment into law of AMLD5 G-20 member countries in other parts of the globe had requested guidance on implementing similar laws. With AMLD5 applicable only to EU member countries, the G20 leaders intimated their desire to have FATF's recommendations be more specific and comparable to the AMLD5.

FATF assured the G20 that under its new presidency (which began when Marshall Billingslea of the United States assumed the position in July 2018) the FATF is prioritizing actions aimed at assuring countries properly regulate and oversee financial activities involving virtual assets.

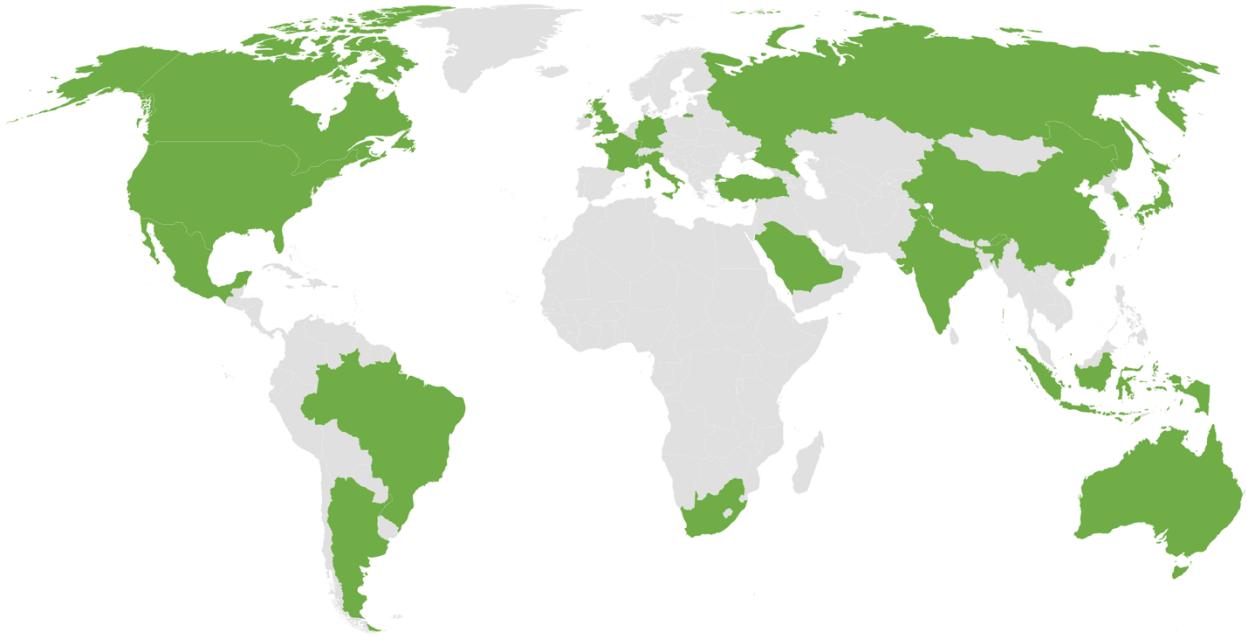


Figure 5: G20 consists of 19 individual countries plus the EU representing 90% of the gross world product

The FATF Report to the G20 Summit also served as a year-end review of the FATF's activities and plans for 2019. In addition, it substantially summarized its October 19, 2018 publication on the Regulation of Virtual Assets, in which the FATF called for an effective global, risk-based response to the AML/CFT risks associated with virtual asset financial activities.

The FATF's members also added to the glossary new definitions of "virtual assets" and "virtual asset service providers"—such as exchanges, certain types of wallet providers, and providers of financial services for ICOs.

The FATF has decided to adopt the term "virtual asset" as a basis for these requirements, defined as a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. This includes the technologies referred to by the G20 as "crypto-assets" and those referred to as "virtual currencies" in some national legislation. This terminology will help to ensure the revised FATF recommendations are neutral with respect to different technologies and can accommodate future developments.

The report further provided the G20 with an update on the task force's work on building a virtual asset program. It recognized the positive advantages and innovations that blockchain and other distributed ledger technologies might bring to the financial system and the global economy. However, it also outlined the risks that cryptocurrencies pose—risks that the FATF closely monitors and which are the subject of internal reporting and surveys. This includes the use of virtual assets for money laundering, terrorism financing, and facilitating a variety of illicit activities.

Major Impacts Coming in 2019

The FATF wrapped up its G20 brief on virtual assets by stating that all jurisdictions should urgently take legal and practical steps to prevent the misuse of cryptocurrency. These steps should include an assessment of those risks associated with cryptocurrencies within their respective jurisdictions, implementing risk-based AML/CFT regulations to cryptocurrency entities, and then identifying effective systems to conduct risk-based monitoring or supervision of those entities.

The FATF wrapped up its G20 brief on Virtual Assets by stating that all jurisdictions should urgently take legal and practical steps to prevent the misuse of cryptocurrency.

The most significant development for regulators and digital assets business such as cryptocurrency exchanges was the announcement by the FAATF that will go into effect by June 2019. The FATF wrapped up its G20 brief on Virtual Assets by stating that all jurisdictions should urgently take legal and practical steps to prevent the misuse of cryptocurrency.

The Glossary further defined virtual asset service provider to mean any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:

- Exchange between virtual assets and fiat currencies
- Exchange between one or more forms of virtual assets
- Transfer of virtual assets
- Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets
- Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset

These recommendations will address challenges in investigations and confiscation of cases where criminals exploit virtual assets for money-laundering and terrorist financing purposes. The June 2019 deadline also includes an update by the FATF of its 2015 Risk-based Approach Guidance on Virtual Currencies. The FATF encourages appropriate and consistent safeguards for activities in the cryptocurrency space that reduce the potential for regulatory and legal arbitrage globally as a result of inadequate or non-regulation and supervision in many jurisdictions.

The FATF also noted the changes it made in October 2018 to its Recommendations and Glossary to provide additional clarification that the Recommendations apply in the case of financial activities involving virtual assets. Furthermore, throughout the next 12 months, due to the accelerated development of the range of financial functions served by virtual assets, the FATF will review the scope of activities and operations covered

in the amended Recommendations and Glossary to determine if further updates are necessary to ensure the FATF standards stay relevant.

Notably, a new section to Recommendation 15 on new technologies sets out that "to manage and mitigate the risks emerging from virtual assets, countries should ensure that virtual asset service providers are regulated for anti-money laundering and counterterrorist financing purposes, and licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations." This includes, for example, conducting customer due diligence and reporting of suspicious transactions.

EU – AMLD5 in Force

The European Union's Fifth Anti-Money Laundering Directive (AMLD5) increases the scope of the EU's regulatory perimeter in terms of AML/CFT controls to include cryptocurrency exchanges as well as those that provide custodian wallet services. Under AMLD5, both service providers "obliged entities" are now subject to the requirements of the AMLD legislation.

AMLD5 also requires all member states to enforce mandatory registration of such providers and to report any suspicious activity that occurs on their platforms. This is designed to stop organized criminal activity from exploiting the pseudo-anonymous nature of cryptocurrency and blockchain technology.

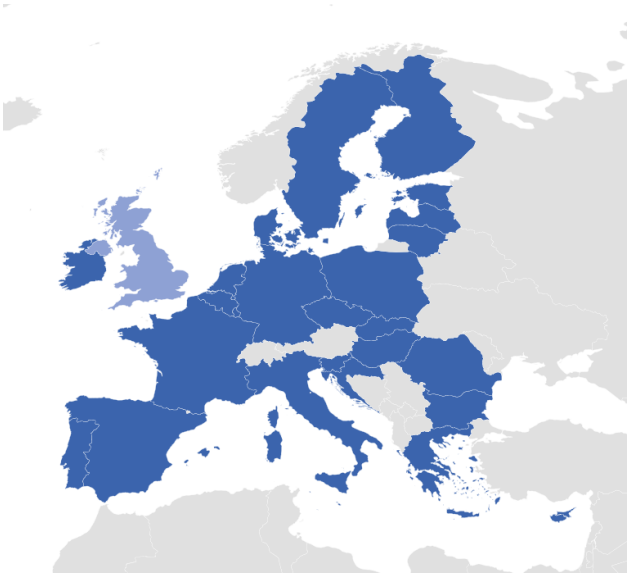


Figure 6: The European Union (EU) consists of 28 member nations.

AMLD5 imposes much tougher due diligence criteria on business relationships and transactions that involve high-risk jurisdictions, which includes acquiring additional information on the customer, the sources of funds, and wealth. The Directive also suggests that member states should impose restrictions on transactions or relationships with institutions from high-risk jurisdictions.

AMLD5 addresses cryptocurrency by expanding the scope of the directive to include virtual currency exchange platforms ("VCEPs") and custodian wallet providers ("CWPs") as "obliged entities" subject to EU regulations.

VCEPs function as electronic currency exchanges that trade virtual currencies for fiat currencies. It has described CWPs as holding virtual currency accounts on behalf of their customers—effectively serving as banks offering a current account into which fiat money can be deposited, stored, and transferred.

As obliged entities, VCEPs and CWPs will now face the same regulatory requirements under the amended directive as banks and other financial institutions. These include obligations to register with national anti-money laundering authorities, implement customer due diligence controls, regularly monitor virtual currency transactions, and report suspicious activity to government entities.

These obligations are similar to the AML obligations posed upon virtual currency exchanges in the U.S., which represent MSBs as subject to the Bank Secrecy Act, requiring them to register as MSBs with FinCEN.

AMLD5 provides Financial Investigative Units (FIUs) with direct access to information held by obliged entities—including VCEPs and CWPs—regardless of whether these entities have filed suspicious transaction reports.

Second, AMLD5 increases transparency of virtual currency transactions executed without VCEPs or CWPs. As the Commission has recognized, including VCEPs and CWPs as obliged entities "does not entirely address the issue of anonymity attached to virtual currency transactions, as a large part of the virtual currency environment w[ould] remain anonymous because users can also transact without these providers."

The revised directive proposes that member states create central databases comprised of virtual currency users' identities and wallet addresses—not just those using VCEPs or CWPs—as well as self-declaration forms submitted by virtual currency users. In addition, AMLD5 directs member states to authorize national FIUs to access the information in these databases.

Third, AMLD5 streamlines member states' regulatory frameworks for virtual currency by defining key terms and instructing member states to implement these definitions into their AML legislation. For example, the amended directive defines "virtual currency" as a "digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically." It also defines a CWP as an "entity that provides services to safeguard private cryptographic keys on behalf of their customers, to hold, store and transfer virtual currencies."

Bermuda Extends Global Regulatory Leadership to Cryptocurrency

Bermuda recently added another pillar to its regulatory framework and continued to roll out strong Digital Asset Business standards. On December 12, 2018, the island nation's financial watchdog, the Bermuda Monetary Authority (BMA), published details on proposed cryptocurrency custody regulation. The draft document, Consultation on Code of Practice for Digital Asset Custody, outlines the BMA's proposed cryptocurrency custody standards, which include business and technology procedures.

The code attempts to protect client assets and encourage banking relationships through a number of provisions. These include detailed guidance for cryptocurrency custody services, ranging from cybersecurity to issues such as handling transaction incident reporting, hot and cold storage, and generation of keys. Licensed digital asset businesses (DABs) will be responsible for maintaining the safe generation and storage of client private keys. It also prescribes transaction and operational controls such as multi-signature authorization and two-factor authentication.

According to an official press release, Bermuda's regulatory framework was built to protect consumers, ensure the stability of the island's institutions, and maintain integrity and confidence in its financial markets. The new standard also aims to further position Bermuda as one of the 'regulatory leaders in digital assets,' stated Craig Swan, the Managing Director in charge of reinsurance and digital assets at the BMA.

The BMA is collecting feedback on these proposed standards during a period of public comment ending January 18, 2019. Once enacted, the new rules regarding how custodians of digital assets must operate would be obligatory.

A Year of Steady Progress Toward Becoming a Major Crypto Island

This proposed action follows nearly a year of significant steps taken toward the goal of making Bermuda a major crypto island. Bermuda is also a leader of the Caribbean Financial Action Task Force (CFATF).

In June, the island nation passed the Digital Asset Business Act, DABA, which formed a new virtual currency and distributed ledger technology regulatory framework designed to foster innovation and trust. It created two tiers of licensing so startups can graduate to a permanent license when they qualify. The DABA also imposes physical presence requirements, which require DABs to be managed and directed from Bermuda.

The regulatory framework was further enhanced in September 2018 with the adoption of the Digital Asset Business (cybersecurity) Rules, Digital Asset Business (client disclosure) Rules, Digital Asset (prudential return / annual filing) Rules, and a Digital Asset Business Code of Practice.

In September 2018, the BMA issued policy Sector-Specific Guidance for Digital Asset Business, enhancing AML and CTF obligations specific to DABs. It made Bermuda one of the few jurisdictions to have comprehensive legislation for both the prudential and AML/ATF regulation of the broad DAB ecosystem, including digital asset exchanges, initial coin offerings, payment service provider with digital assets, custodial wallet service providers, and market makers/dealers/traders of digital assets.

Also, in May the government passed the ICO Act to regulate "digital assets," which includes various equity, security and utility tokens or coins that are issued as ICOs. Then in October, the government granted the first license for an ICO to Uulala.

Malta Enacts Favorable Crypto Asset Framework

Malta's goal of becoming a blockchain finance and technology center took a big leap in 2018. In July, it became the first country to establish official regulations for cryptocurrencies with the passage of three bills that provide an integrated framework for regulating distributed ledger technology (DLT). The laws officially went into effect on November 1, 2018.

> The Malta Digital Innovation Authority (MDIA) Act — Allows for the formation of the Malta Digital Innovation Authority, which focuses on not only regulation but also promoting the country's crypto economy.
>
> The Innovative Technology Arrangements and Services Act (ITASA) — Provides legal clarity on many aspects of blockchain technology to help developers certify the quality and governance of blockchain technology used by companies who seek the approval of domestic operation.
>
> The Virtual Financial Assets Act (VFAA) — Provides a regulatory structure for all entities that handle virtual financial assets, including Security Token Offerings (STOs). It includes a test to determine whether or not an offering constitutes a security.

Essentially, the three laws comprise a holistic regulatory framework for the blockchain and cryptocurrency space that should reduce fraud, money laundering, terrorist financing, and investor abuse. The framework is specifically designed to attract trustworthy blockchain businesses to the island nation. It also allows the Malta Digital Innovation Authority (MDIA) and the Malta Financial Services Authority (MFSA) to receive applications for licensing from those interested in operating in Malta. Furthermore, the clarity provided by this regulatory should promote accelerated FinTech development and innovation.

Imposes Strict Crypto-to-Crypto AML

Notably, the new regime imposes AML/CFT obligations on more virtual service providers than does AMLD5, including cryptocurrency exchanges, brokerages, portfolio managers, custodian services providers, investment advisors, and eWallet providers. It does not, however, extend to miners. The "Malta government is strictly behind AML crypto-crypto and will enforce all its power through MFSA and VFA to prevent that," explained, Silvio Schembri, Maltese MP.

Canada

In June, the Canadian government pre-published measures to introduce strong AML, KYC, and CTF legislation, similar to those that currently apply to traditional MSBs. Final publication is expected in 2019. The updated measures are anticipated to come into force 12 months after final publication.

Under the current Canadian federal legislation, cryptocurrency exchanges do not qualify as MSBs unless they do one of the three following activities: foreign exchange, money transferring, or issuing/redeeming money orders or other similar instruments. This has created an environment in which some businesses are regulated, while others are not. Canada's AML regulator, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), has issued several policy positions to help cryptocurrency businesses understand whether or not they must register (and be compliant) at this time.

"Logically, companies that are engaged in crypto-to-crypto exchange only cannot register as MSBs currently, as none of their activities can be construed as being any of the three qualifying activities," said Amber D. Scott, CEO of Outlier Solutions, Inc. "So many businesses were trying to register as MSBs that FINTRAC changed their system to move to a preregistration form. Unless one of the three qualifying activities is checked off, the applicant gets a call from FINTRAC to let them know that they 'can't register at this time'."

In 2019, the Canadian government may feel pressure from its brethren in Europe who have put AMLD5 into effect. Additionally, in a rare show of unity at its summit in Argentina in December 2018, the G20—of which Canada is a member—announced that its member countries would be taking concerted action to regulate cryptocurrencies. The Group of 20 countries called for implementing significant regulation of crypto assets, exchanges, and other DABs. They cited the need to deal with a range of key issues such as money laundering, terrorist financing, speculative risks, and facilitating fair taxation across borders. The G20 aims to have regulations in place by 2020 based upon the FATF recommendations.

UK Government Says Will Go Further Than AMLD5 On Regulating Crypto Assets

Under pressure from members of parliament to deal forcefully with risks posed by cryptocurrencies, in December 2018 the government moved to consolidate authority of crypto assets under the Financial Conduct Authority (FCA).

Previously, the UK's Chancellor of the Exchequer had brought together the HM Treasury, the FCA, and the Bank of England in a Cryptoasset Taskforce. The taskforce's final report was published at the end of October, which stated: "To combat financial crime risks, the Treasury will undertake one of the most comprehensive responses globally to the use of cryptoassets for illicit activities by applying and going further than the existing directive, the fifth EU Anti-Money Laundering Directive (5AMLD). On this, HMT will first consult and then legislate on how to transpose 5AMLD and broaden the scope of anti-money laundering and counter-terrorism financing regulation further."

Part of the plan for tougher AML/CFT regime includes strict regulation of the following:

- Exchange services between different cryptoassets, to prevent anonymous 'layering' of funds to mask their origin

- Platforms that facilitate peer-to-peer exchange of cryptoassets, which could enable anonymous transfers of funds between individuals
- Cryptoasset ATMs, which could be used anonymously to purchase cryptoassets
- Non-custodian wallet providers that function similarly to custodian wallet providers

Japan Allows Exchanges to Self-Regulate

In December, Japan's Financial Services Agency (JFSA) published new draft cryptocurrency regulations that address hacking incidents, self-regulation, "deemed dealers," privacy coins, insider trading, and margin trading. In October, it also granted the Japan Virtual Currency Exchange Association (JVCEA) rights to act as a self-regulatory organization.

The JVCEA was formed partly in response to the $534 million hack of cryptocurrency exchange Coincheck in January 2018. All 16 registered exchanges in Japan comprised the initial membership, which will be extended to other exchanges. Five more exchanges—Coincheck, Everyone's Bitcoin, Lastroots, LVC and Coinage—joined as Type II members, a classification for companies that handle virtual currency-related services such as wallet dealers.

The FSA draft report also addressed "deemed dealers"—companies that have been allowed to operate cryptocurrency exchanges while their applications were being reviewed. Japan's three deemed dealers, Coincheck, Lastroots, and Everybody's Bitcoin, cannot expand their business or add new tokens until they are registered and must post a warning on their websites that they are not currently registered.

One of the JVCEA's core tasks will be to establish and oversee AML policies. Toward that end, the rules prohibit exchanges from accepting new coins that "cannot be traced to previous sellers"—aka privacy coins like Monero and Dash—according to a report by Japan's leading financial newspaper, the Nikkei. The FSA had already been pushing domestic exchanges to drop support for privacy coins, citing their potential for facilitating money laundering. The draft rules effectively ban privacy coins.

The proposed rules are also designed to improve security. The JVCEA's member exchanges will be required to report internal audits to the self-regulatory body and better safeguard customer assets by storing private keys offline to minimize the risk of a hack or theft. The Coincheck hack resulted from tokens stored in online hot wallets that are more vulnerable to compromise.

Korea

South Korea was home to some of the most spectacular cryptocurrency heists in 2018, and recently to some of the world's most rigorous KYC laws.

Checks of Exchanges Find Basic IT Security Lacking at Many

After a first half punctuated by five multi-million-dollar cryptocurrency exchange thefts—such as the $40 million Coinrail hack in June—Korea stepped up its efforts to regulate and oversee the market. For example, between September and December 2018, Korea's Ministry of Science and Technology (MoST) and the Korea Internet Development Agency (KISA) conducted an IT security survey of exchanges. They judged 85 basic security requirements, including: administrative security, operational environment security (including network separation and account management), system security, network and database access control, backup, and virtual currency wallet management. In early January 2019, Korea's The Ministry of Economy and Finance (MOEF) released the results of the assessment, revealing that of 21 crypto exchanges checked only seven—Upbit, Bithumb, Gopax, Korbit, Coinone, Hanbitco, and Huobi Korea—had adequate security. The other 14 exchanges failed an average of 61 out 85 of security areas examined.

Six New Bills introduced in December To Strengthen Crypto Regulation

According to a widely reported exclusive story by Coindesk, the government is seeking to further strengthen its regulatory posture and improve investor protections with six new bills introduced in December 2018, which extend the Financial Services Commission's (FSC) oversight to crypto assets.

Korea Number-One User of Monero

Nonetheless there are some contradictions in the reality of cryptocurrency regulation in the country. For instance, the government banned the use of anonymous virtual accounts in 2017, which allowed banks and other financial institutions to comply with AML and KYC obligations. But on the other hand, South Koreans were the leading users of privacy coins in 2018, accounting for 83% of the market in Monero.

Gibraltar

The British Territory of Gibraltar made news in 2018 with a significant cryptocurrency financial innovation. The Gibraltar Blockchain Exchange (GBX) is now providing insurance coverage for crypto assets listed on its platform. It is partnering with a local insurance company to cover both hot (online) and cold (offline) wallets listed on the peninsula's stock exchange.

