CIPHERTRACE

Cryptocurrency Anti-Money Laundering Report

2018 Q3

CipherTrace Cryptocurrency Intelligence

2018 Q3 CRYPTOCURRENCY ANTI-MONEY LAUNDERING REPORT SUMMARY 2

97% of Criminal Bitcoin Directly Received by Exchanges Flowed into Those Located in Countries with Weak AML Laws 2

Key Takeaways 4

MEASURING THE IMPACT OF REGULATION ON DIRECT CRIMINAL CRYPTOCURRENCY PAYMENTS 5

Metrics for Defining Weak AML 5

EMERGING THREATS 8

CRYPTOCURRENCY THEFTS CLIMB TO $927 MILLION USD FOR THE FIRST THREE QUARTERS OF 2018 9

Analysis of Major Cryptocurrency Thefts Reported at Exchanges and at Platforms in Q3 2018 10

1. Bithumb – Exchange Hack 10

2. Bancor – Exchange/ICO Hack 11

3. Geth – Platform Vulnerability 11

4. Coinrail – Exchange Hack 11

5. Bitcoin Gold – Blockchain 51% Attack 11

6. Zaif – Exchange Hack 12

7. Taylor – ICO/Trading Platform Hack 12

REGULATORS PRIORITIZE CRYPTOCURRENCY ANTI-MONEY LAUNDERING GLOBALLY 13

Global Developments in Q3 13

AMLD 5 13

FATF and Regional Financial Action Task Forces 13

Notable Regulatory Activity by Country 16

Bermuda 16

Malta 16

Canada 16

Japan 17

Mexico 17

South Korea 18

North Korea 18

Saudi Arabia 18

United States 19

ABOUT CIPHERTRACE 21

2018 Q3 Cryptocurrency Anti-Money Laundering Report Summary

97% of Criminal Bitcoin Directly Received by Exchanges Flowed into Those Located in Countries with Weak AML Laws

A quantitative analysis of all the transactions on the 20 top cryptocurrency exchanges globally revealed that 97% of direct bitcoin payments from identifiable criminal sources were received by unregulated cryptocurrency exchanges.

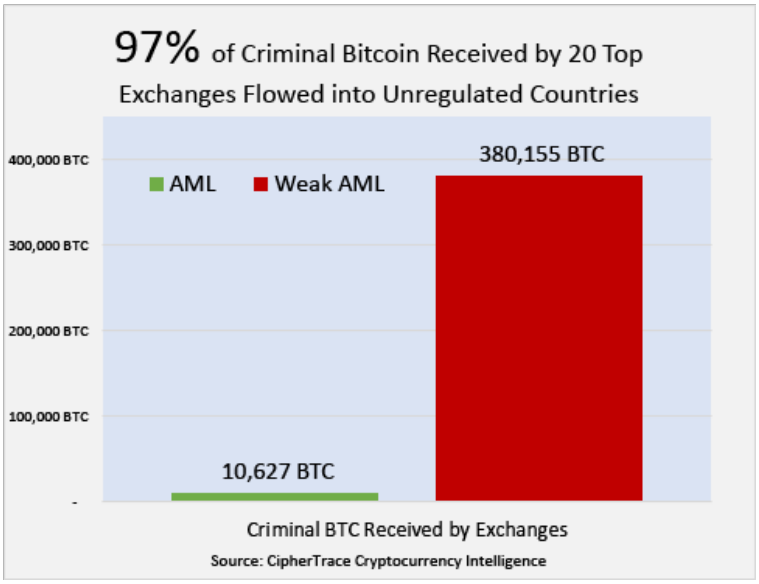

Fig 1. Criminal Bitcoin Received by 20 Top Exchanges

A direct payment is defined as one that moves from an identified criminal actor or service into a cryptocurrency exchange. An indirect payment is one that moves through one or more cryptocurrency wallets or addresses before being deposited into an exchange for conversion into either fiat currency or another cryptocurrency.

The analysis also identified 380,155 bitcoins that were received by cryptocurrency exchanges directly from criminal sources between January 9, 2009 and September 20, 2018. In other words, 36 times more criminal bitcoin was received by crypto exchanges in countries where AML is either lax or lacking.

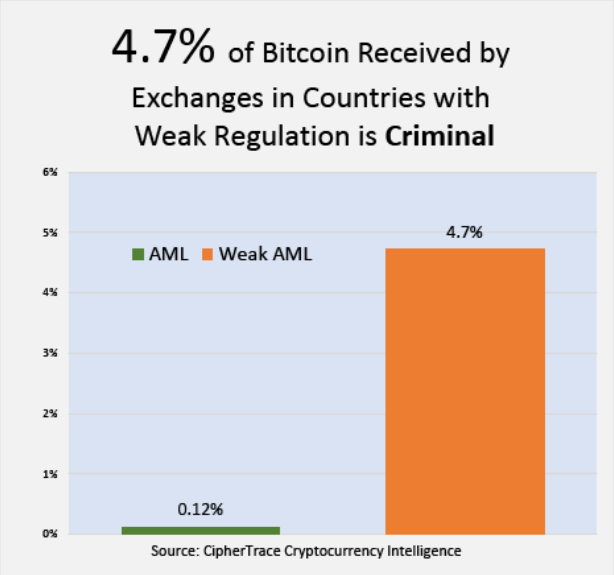

Fig 2. 4.7% of Bitcoin Sent to Unregulated Exchanges Is Criminal

These results indicate that money laundering activity using cryptocurrencies is directly correlated to AML regulations and their enforcement on exchanges. They also show that cryptocurrency exchanges in countries with weak AML regulation receive nearly 5% of their payments directly from criminal sources. This analysis does not cover indirect criminal payments.

In fact, analysis of the data reveals that the top exchanges have laundered a significant amount of bitcoin, representing approximately $2.5 billion at today's prices.

Essentially, criminals are flowing large amounts of dirty bitcoin into these poorly regulated exchanges and other services—such as mixers—turning it into "clean" cryptocurrencies. Then, they can move funds into the global financial payments system with little risk of being detected.

This extensive analysis shows that criminal transactions are reduced in the presence of strong AML regulation—with the obvious benefit of reducing illegal and illicit activity in general. Since criminals use the funds to finance illicit activity—such as international drug gangs that use the laundered funds to produce and distribute more illegal substances—the benefits of well-enforced AML regimes to society are obvious.

Moreover, these money-laundered funds comprise only the transactions that CipherTrace was able to directly monitor and designate as criminal or highly suspect. There are likely 50% more criminal transactions than those that were traced for this report because criminals are typically very clever and deft at hiding their tracks.

Key Takeaways

1. 97% of direct criminal bitcoin payments are sent to unregulated exchanges.
2. 36 times more criminal bitcoin is received by cryptocurrency exchanges in countries where AML is either weak or not enforced.
3. Cryptocurrency money laundering on top exchanges involves a significant amount of bitcoin—some 380,000 bitcoins or $2.5 billion at today's prices.
4. In the first three quarters of 2018, $927 million of cryptocurrency was stolen by hackers; since the Q2 report, CipherTrace have recorded new reports of $166 million.
5. US FinCEN clarified its stance on regulating mixing services and included crypto-to-crypto in its definition of money service businesses, MSBs, that are subject to the Bank Secrecy Act (BSA) rules. It also enlisted the IRS to examine 100% of cryptocurrency MSB transmitters for BSA compliance.
6. Opportunities to launder cryptocurrencies will be greatly reduced throughout 2019 and 2020 if cryptocurrency AML regulations are successfully enacted and enforced globally.
7. New cryptocurrency crime threats continue to emerge, including highly targeted mass cyber extortion, SIM swapping, and advanced cyberattacks on exchange personnel.

Measuring the Impact of Regulation on Direct Criminal Cryptocurrency Payments

This research is the first major quantitative effort to measure the level of criminal activity to definitively characterize criminal bitcoin payments. CipherTrace Cryptocurrency Intelligence analyzed 45 million transactions at the 20 top cryptocurrency exchanges globally. These transactions were identified as criminal if they came directly—one degree of separation—from a criminal source. The study defined 'criminal sources' as dark market site, extortion, malware, mixer/tumbler/money laundering site, ransomware, and terrorist financing that CipherTrace has been able to identify and validate as of 9/29/2018.

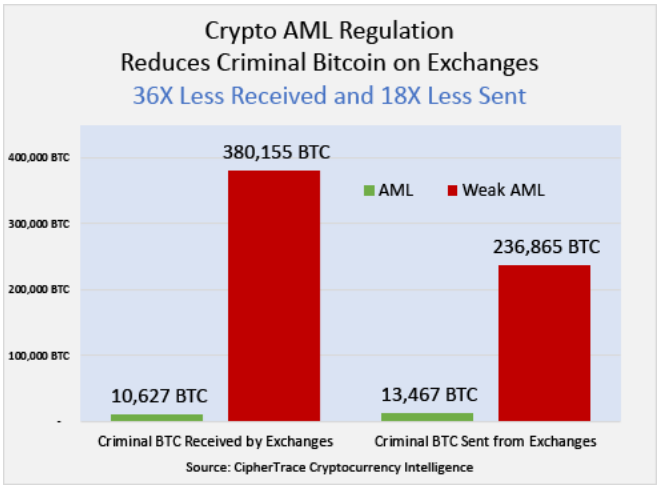

Fig 3. Cryptocurrency AML Regulation Reduces Criminal Activity on Exchanges

Metrics for Defining Weak AML

CipherTrace researchers used the US Department of State Bureau for International Narcotics and Law Enforcement Affairs *Money Laundering and Financial Crimes Country Database*[1] as the source data for determining if the exchanges were located in countries with weak anti-money laundering regulation or not. This comprehensive database includes reports on anti-money laundering and financial prudence in 212 countries. Referencing the US State Department data, CipherTrace determined that 79 countries have weak AML regimes because they haven't implemented one or more of the following controls:

- Regulate Illegal drug dealing
- Regulate money laundering related to criminal activity other than illegal drugs
- Enforce Know-Your-Customer (KYC) regulations
- Report large transactions
- Report suspicious transactions
- Maintain records over time

[1] https://www.state.gov/documents/organization/258726.pdf

While this rubric comprises strict criteria, it recognizes that AML regulations are only as strong as their weakest links.

The research also identified which of the top crypto exchanges are located in countries deemed by the US Dept of State not to have strong AML regulation. This resulted in two samples sizes within 10% of each other both in terms of transaction volume and bitcoins.

At the same time, these unregulated or weakly regulated exchanges have also been used to purchase 236,865 bitcoins worth of criminal services, representing $1.5 billion at today's prices.

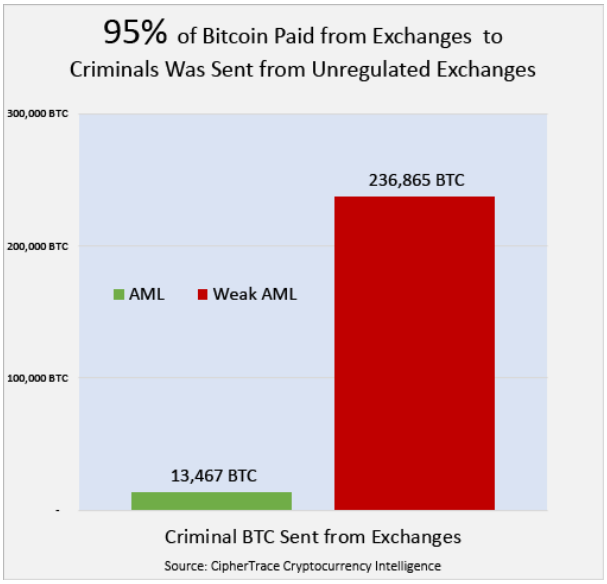

Fig 4. 95% of Bitcoin Paid from Exchanges to Criminals Was from Unregulated Exchanges

95% of outgoing payments that were traceable to criminals were made from unregulated exchanges.

Consequently, CipherTrace compared direct payments to two of the top 10 global cryptocurrency exchanges over the last 12 months to analyze criminal and risky transactions.

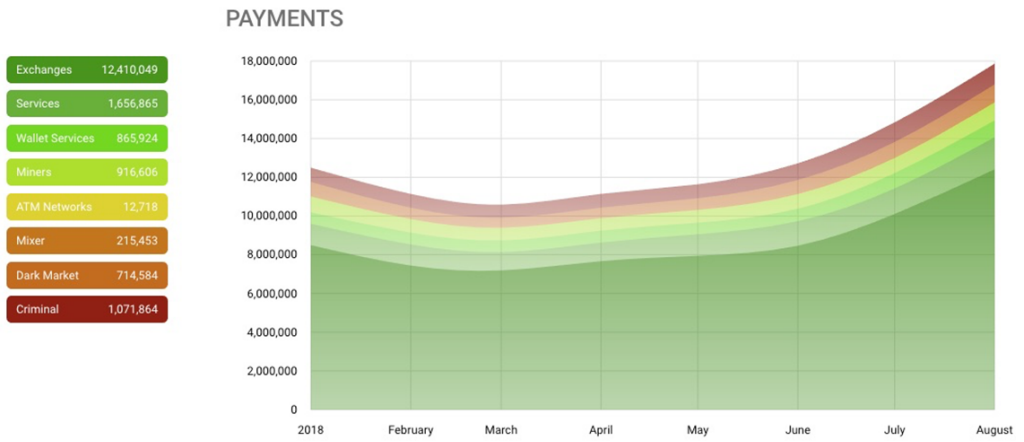

Fig 5. Transaction Analysis of a Top 10 Global Cryptocurrency Exchange with Strong AML

As the chart above shows, a top 10 regulated exchange processed a constant small percentage of criminal/dark market/mixer transactions. While the exchange experienced 50% growth in criminal transactions over the period, the percentage of those transactions did not grow, presumably due to active AML measures at the exchange.

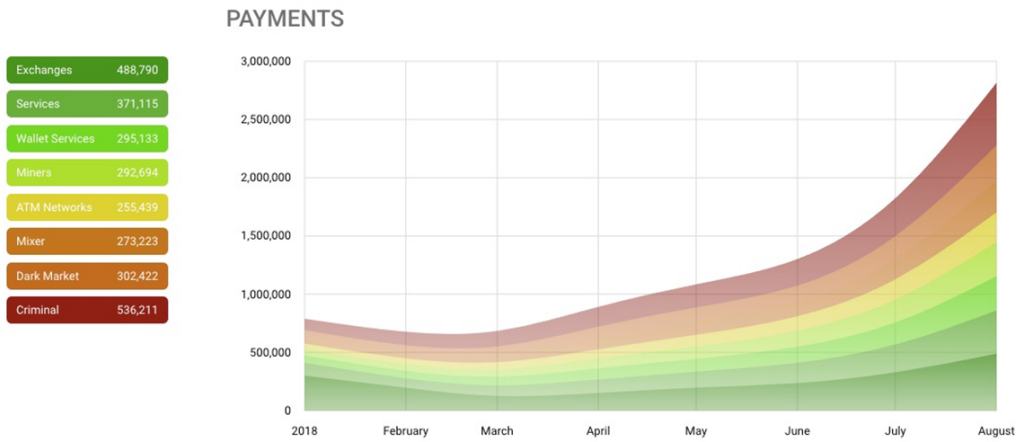

Fig 6. Transaction Analysis of a Top 10 Global Cryptocurrency Exchange with Weak/No AML

This chart shows that an unregulated top 10 exchange processed more risky transactions than non-risky transactions. It further indicates that the unregulated exchange is growing at 300%, with risky transactions and criminal transactions growing fastest.

Emerging Threats

This report focuses on cryptocurrency money laundering and does not detail threats to ordinary citizens and the financial system that are rapidly emerging in the blockchain security stack—and in some instances increasing at an alarming rate—during the period. For instance, in July, CipherTrace issued an alert on a spike in online mass customized extortion (spear phishing) using cryptocurrency as payment for ransom or blackmail. Other threats include advanced malware targeting crypto exchange personnel. Another new threat, SIM swapping, is becoming widespread. It 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. In one instance, a hacker used the technique to allegedly steal $24 million from a wealthy investor.

Of course, all of this criminal activity, whether it involves illicit business in dark markets, outright theft, extortion or malware attacks, increases the demand for money laundering. Because these ill-gotten cryptocurrency gains must be laundered before the criminals can spend them in fiat currency.

Cryptocurrency Thefts Climb to $927 Million USD for the First Three Quarters of 2018

Theft of cryptocurrencies at exchange and platform layers continued to represent a major problem in the third quarter of 2018, albeit in a slightly evolved form. In the 2018 Q2 Cryptocurrency Anti-Money Laundering Report, CipherTrace revealed a three-fold increase in cryptocurrency thefts during the first half of 2018 compared with the entire year of 2017. Most notable were the $530 million worth of tokens stolen in Japan from Coincheck and $195 million worth of tokens stolen from BitGrail.

Fig 7. Cryptocurrency Thefts Continue in 2018

These cyberattacks bring the total amount of cryptocurrencies reported as stolen in 2018 through the end of Q3 to $927 million. CipherTrace estimates this trend will bring the total stolen and reported in 2018 to well over $1 billion by the end of the year.

$50 million in estimated CoinHoarder phishing thefts have been excluded from this report, but will be added into the 2018 annual report if they can be fully substantiated. Additionally, CipherTrace is aware of over $60 million in cryptocurrency that was stolen but not reported publicly.

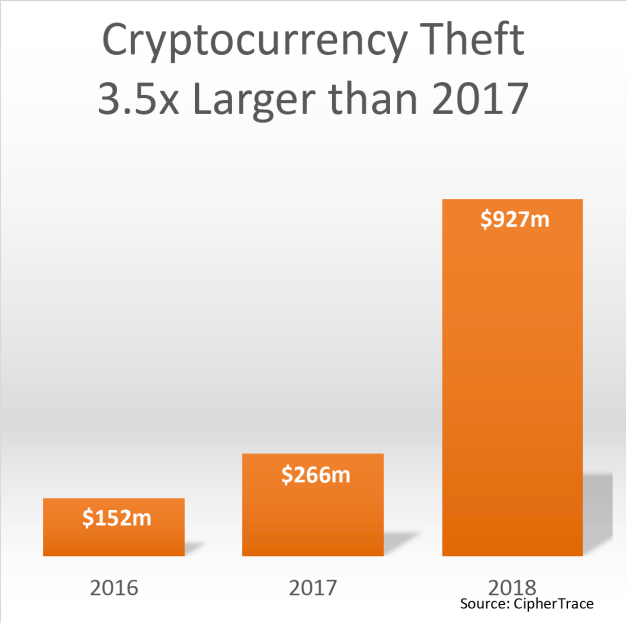

Fig 8. Cryptocurrency Thefts from Exchanges and Trading Platforms 3.5 Times Larger First Three Quarters of 2018 than in 2017

Year-to-date cryptocurrency thefts continue to set records with $927 million in cryptocurrency reported as stolen in the first three quarters of 2018. This represents 3.5 times as much cryptocurrency as was stolen in all of 2017. Criminals will need to quickly launder these stolen tokens before stronger cryptocurrency anti-money laundering controls are deployed globally over the next 18 months.

Analysis of Major Cryptocurrency Thefts Reported at Exchanges and at Platforms in Q3 2018

Nothing in the third quarter could compare with the massive $520 million Coincheck exchange robbery earlier this year. However, the most recent data shows a steadily growing number of cryptocurrency thefts, which included several heists in the $20-$60 million range, totaling $166 million since reported in the second quarter of 2018. This data indicates a pattern of smaller robberies on a regular basis and sophisticated professional cyber thieves who carry out hacks at both the exchange and platform levels by capitalizing on exposed vulnerabilities, as well as by socially engineering employees who work at these companies.

1. Bithumb – Exchange Hack

South Korea based Bithumb—the world's sixth-largest cryptocurrency exchange—reported a loss of $30 million in cryptocurrency due to a cyber intrusion. According to Bithumb, the theft was caused by "unauthorized access to its online wallets." Once the attack was recognized, Bithumb urgently disabled deposits on the platform and also began to move all coins stored in online wallets to more secure offline 'cold' wallets to prevent further theft.

2. Bancor – Exchange/ICO Hack

At the beginning of July 2018, hackers stole $23.5 million in cryptocurrency from the 'decentralized' crypto exchange Bancor. The loss included $12.5 million in Ethereum along with BNT and NPXS tokens totaling $11 million. This massive security breach forced the firm to shut down operations. Bancor had been one of the more high-profile Initial Coin Offerings (ICOs) of 2017, raking in $153 million during its token sale event. According to Bancor, a wallet used to update some smart contracts was breached and used to withdraw the cryptocurrency.

3. Geth – Platform Vulnerability

Security experts revealed that hackers had stolen more than $20 million in Ethereum by using insecurely configured Geth clients. Geth is one of the most popular clients for running the Ethereum node. Its JSON-RPC interface allows users—and thieves—to remotely access the Ethereum blockchain and node functionalities, including the ability to send transactions from any account which has been unlocked before sending a transaction. Once unlocked, however, the port stays opened for the entire session. The unwitting victims had opened their JSON-RPC port 8545 to the outside world, allowing hackers to breach their Ethereum wallets.

4. Coinrail – Exchange Hack

Korea-based coin exchange Coinrail lost more than $40 million in altcoins (ICO-issued tokens) in an apparent weekend cyber heist. Most notably, the hackers got away with $19.5 million worth of NPXS tokens that were issued by payment project Pundi X's ICO. On top of that crypto loot, "they scored a further $13.8 million from Aston X, an ICO project building a platform to decentralize documents, $5.8 million in tokens for Dent, a mobile data ICO, and over $1.1 million Tron, a much-hyped project originating from China," According to TechCrunch.

The tokens had been maintained on the exchange's servers, but following the discovery of the hack, Coinrail immediately moved to secure its cryptocurrency assets by taking its wallets offline. The exchange also worked with affected ICO companies in an attempt to freeze the stolen funds.

5. Bitcoin Gold – Blockchain 51% Attack

BitCoin Gold was compromised by a "51 percent attack" in which the hackers apparently employed rented computers to achieve this previously theoretical type of cyberattack. These attacks occur when one entity gains control over more than 51% of the network hash-rate. Then, the successful attacker can not only prevent valid transactions from occurring but also reverse previously completed transactions on the blockchain. This degree of control even enables a single coin to be spent twice from the same origin—a so-called double-spend attack like the thefts that occurred on Bitcoin Gold.

This attack netted thieves in excess of $18 million. Possibly the blame for the Bitcoin Gold trouble lies with the fact that it uses the Proof of Work (PoW) consensus protocol of Bitcoin in a small pool to create distributed trustless consensus. However, these thefts raise questions

regarding the wisdom of utilizing the PoW to solve the double-spend problem in smaller cryptocurrencies with a small network of miners.

6. Zaif – Exchange Hack

On September 14, 2018, Japan-based cryptocurrency exchange Zaif, which is operated by Tech Bureau, was hacked. The perpetrator made off with ¥6.7 billion (about $60 million) worth of cryptocurrency, including 5,966 bitcoins. After the Coincheck mega heist of $520 million in NEM tokens in January, the Financial Services Agency (FSA)—Japan's financial watchdog agency—launched a series of inspections of cryptocurrency exchanges in the country to assess their security measures. Notably, the FSA had already issued a business improvement order to Tech Bureau in March specifically regarding the need for security and anti-money laundering enhancement.

7. Taylor – ICO/Trading Platform Hack

The cryptocurrency trading platform Taylor suffered a robbery where the hacker stole all of the 2,579.98 ETH ($1.35 million) raised by the project during its recently conducted ICO along with native TAY tokens. The Taylor team also suspected the hacker attempted to launder the stolen funds by dumping the tokens on the IDEX platform. Consequently, they instructed IDEX to temporarily delist TAY tokens.

Regulators Prioritize Cryptocurrency Anti-Money Laundering Globally

The international community has made the fight against money laundering and the financing of terrorism a top priority. These efforts aim to not only make it difficult for those engaged in crime to profit from their criminal activities but also cut off the financial resources available to terrorists and protect citizens from theft and scams.

As evidenced by the data in this report, regulators face a number of challenges. Cryptocurrency exchanges and services like mixers represent fertile ground for criminal activity and money laundering. In addition, the fast-moving and highly speculative market in cryptocurrencies—including Ethereum-based ICOs and smart contracts—is making companies and initiatives built on the blockchain technology ripe for frauds ranging from Ponzi schemes to bogus ICOs.

Global Developments in Q3

In addition to starving terrorists, global drug cartels and other bad actors of cash, one major emphasis observed in Q3 is countries around the globe looking to grow their digital asset economies by rolling out and enforcing strong Crypto AML/CTF regulations. Establishing their countries' reputations as 'safe' digital markets helps to attract trustworthy cryptocurrency exchanges and digital asset businesses.

A number of regulatory changes happened around the world during Q3 2018.

AMLD 5

On July 9, the European Commission's 5th Anti-Money Laundering Directive (AMLD 5) entered into force. Member states are obliged to put the regulations into law by January 20, 2020. Among a number of changes, AMLD 5 extends AML and Counter Terrorism Funding (CTF) rules to virtual currencies. It will also bring crypto-related services in line with the standards applied to other financial products such as those offered by banks.

AMLD 5 further includes mandatory identity checks on new customers. "The rules will now apply to entities which provide services that are in charge of holding, storing and transferring virtual currencies, to persons who provide similar kinds of services to those provided by auditors, external accountants and tax advisors which are already subject to the 4th Anti-Money Laundering directive and to persons trading in works of art," according to the commission. "These new actors will have to identify their customers and report any suspicious activity to the Financial Intelligence Units."

FATF and Regional Financial Action Task Forces

The Financial Action Task Force (FATF) is the global standard-setting body for anti-money laundering and combating the financing of terrorism. It promotes the adoption and implementation of appropriate AML/CTF measures globally. While it technically is a 'policy-making body,' FATF and its regional associates act as watchdogs that monitor the progress of FATF's 37 member countries in implementing necessary AML and CTF techniques. FATF advises

a number of regional Financial Action Task Forces around the world (See fig. 9) For example, one FATF associate in the EU, MoneyVal, has powers to conduct ad hoc inspections of public and private sectors entities in countries of the European Commission beyond those in the EU.

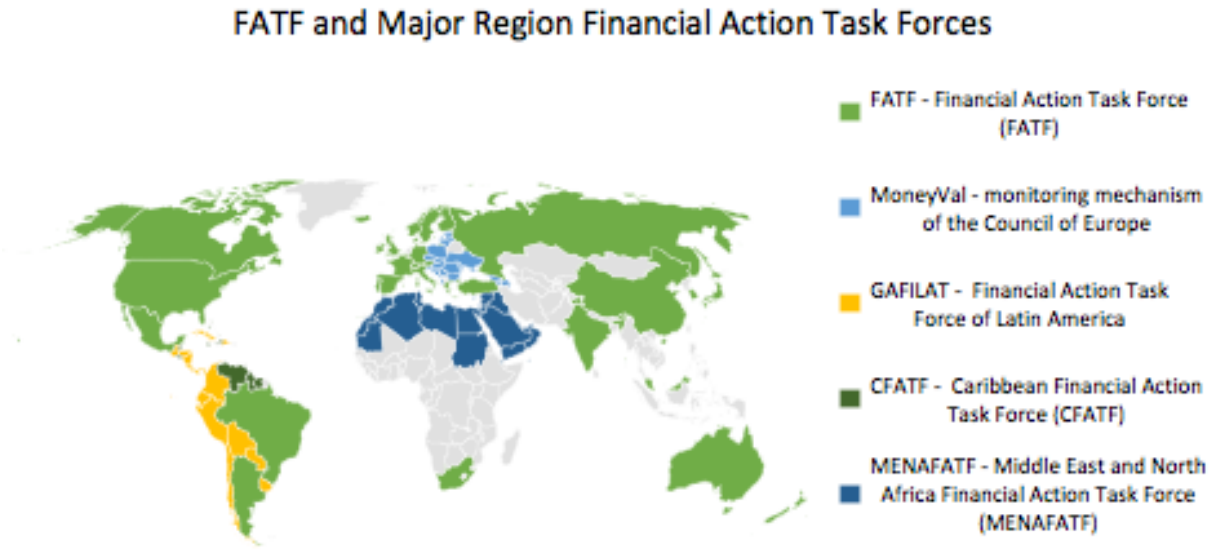

Fig 9. FATF and Associates Map

The FATF Report to G20 Leaders' SummitG20 includes a commitment to implement FATF standards and support for work on crypto assets.

Each year there is a new president from a different region. This year's president is Marshall Billingslea of the United States. He said currently the adoption of anti-money laundering standards and regimes pertaining to digital assets and virtual currencies is "very much a patchwork quilt or spotty process," which is "creating significant vulnerabilities for both national and international financial systems." He also explained during his tenure as a US president, the FATF will prioritize work on preventing the financing of the proliferation of weapons of mass destruction; expand the current emphasis on combating terrorist financing; and foster improvements in the regulation and supervision of virtual currencies/crypto-assets

Mr. Billingslea further cited the FBI concerns regarding an emerging use of virtual currencies by terrorist organizations, including ISIS, as well as in extortion schemes, such as the WannaCry attacks. His comments come after some observers argued that authorities such as Europol, Europe's law enforcement agency, should devise a centralized system that flags cryptocurrency wallets linked to nefarious activities to major exchanges. This system would enable them to block the owners from exchanging those funds for hard cash, according to the Financial Times.

Noting that virtual currencies/crypto-assets raise issues with respect to money laundering and terrorist financing, they committed to implement the FATF Standards as they apply to virtual

currencies/crypto-assets. They looked forward to the FATF review of those standards, called on the FATF to advance global implementation, and asked the FATF to provide an update on this work in July 2018. The FATF will take this work forward under its US presidency, which spans from July1 to 2018 to June 30, 2019.

The FATF has developed a comprehensive approach to respond to the increasing use of virtual currency/crypto-asset activities for money laundering and terrorist financing. This approach is intended to ensure that all countries exercise a sufficient level of oversight on virtual currency/crypto-asset activities taking place within their jurisdictions and to encourage a more consistent approach to the regulation of virtual currencies/crypto-assets across different countries.

Besides small-scale drug trafficking and fraud, the link between virtual currencies/crypto-assets and other predicate crimes appears to be growing. Virtual currencies/crypto-assets facilitate easy online access and global reach which make them attractive to move and store funds for money laundering and terrorist financing. The FATF is actively monitoring the risks associated with virtual currency/crypto-asset payment products and services, including pre-paid cards linked to virtual currencies, Bitcoin ATMs, and ICOs.

Also, in July, the FATF published its most recent list of ‘rogue states,’ which includes Democratic People’s Republic of North Korea, Ethiopia, Iran, Pakistan, Serbia, Sri Lanka, Syria, Trinidad and Tobago, Tunisia, and Yemen. Many Jurisdictions such as Malta use this list to inform their AML efforts.

Notable Regulatory Activity by Country

Bermuda

Bermuda took major steps toward becoming a crypto island in the third quarter when it passed significant financial markets regulation. Local banks, in what the government viewed as a threat to the growth of the island's crypto economy, had been hesitant to provide banking services to companies in the emerging FinTech sector. The Bermuda banks cited their aversion to risk and significant regulatory barriers as the prime reasons for their unwillingness to cooperate. However, in July, 2018, the government passed a Digital Asset Business Act and an ICO Bill, which made changes to Bermuda's Banking Act with the goal of creating a new class of banks that could work with and attract emerging FinTech, cryptocurrency and blockchain startups to the island.

In September, the Bermuda Monetary Authority, BMA, released an Information Bulletin outlining what documentation is required when submitting an application for a digital asset business (DAB) license with a focus on maintaining the highest standards of AML/ATF. This makes Bermuda one of the few jurisdictions that has 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.

Malta

Another emerging powerhouse crypto island, the EU nation of Malta, has established itself as a leading jurisdiction for various sectors such as iGaming, financial services, and cryptocurrency and blockchain. The Malta Financial Services Authority's (MFSA) has developed extensive regulations and licensing requirements for cryptocurrency businesses including ICOs and exchanges. These regulations go into effect November 1, 2018.

The government of Malta and the FIAU are also working to reduce their AML exposure, seize the crypto regulatory high ground, and dispel any perception of the island nation turning a blind eye to money laundering. In September, CipherTrace CEO, Dave Jevans, spoke at the MSA's seminar on Due Diligence and Cybersecurity in Relation to DLT. He explained tracing crypto transactions through distributed ledgers as well as the latest global Crypto Regulation trends to local authorities and industry luminaries.

Canada

On June 9, Canada's Department of Finance announced proposed updates to the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (PCMLTFA). The proposed updates require that payment processors and crypto exchange platforms in the country be treated as money service businesses (MSB). Among a number of requirements such as stricter KYC rules, crypto players would need to report transactions in excess of 7,700 US dollars, or 10,000 Canadian dollars.

These updates were expected to take effect in the fall of 2018. However, at the end of August, Canada backed away from what some had seen as extremely burdensome anti-money launderings rules, with the government saying the more rigorous AML/CTF regime will not go into effect until late 2019. According to Bitcoin focus, “This is being seen as a positive move by many who see it as a backward step by the government which had proposed stricter regulations in the draft version published earlier in June 2018. There are also others who believe that this delay might harm their competitive advantage in the crypto market…”

Japan

Still reeling from the massive Coincheck heist, Japan continued a post-incident regulatory clampdown on exchanges and digital asset businesses. For example, the CEOs of bitFlyer and Bitbank—who also worked at the helm of The Japan Virtual Currency Exchange Association (JVCEA) as president and vice president—were served with business improvement letters by the Financial Services Agency (FSA), Japan’s top financial watchdog agency.

The financial regulator also recently unveiled the current state of the crypto regulations in the country. Three crypto operators are currently being reviewed. With 160 companies wanting to enter the space, the FSA plans to add more personnel to help review new applicants. In addition, a self-regulatory plan for crypto exchanges has also been submitted to the regulator.

The FSA published several documents from its fifth crypto study group meeting on Wednesday, September 12. In overviewing the current state of the crypto environment, the agency confirmed that only three of 16 companies that have been allowed to operate crypto exchanges while their applications were being reviewed survived the agency’s recent inspections. Currently they are reviewing Coincheck, Lastroots, and Everybody’s Bitcoin, and the regulator will periodically conduct on-site inspections of registered exchanges.

Citing their biggest problem as the large number of new operators—160 companies wanting to enter the market—the FSA is also expanding its crypto team in order to swiftly review applicants.

Mexico

On September 9, the Bank of Mexico (Banxico), Mexico’s central, bank announced "The institutions of electronic payment funds must request authorization from the Bank of Mexico so that they can use those technologies associated with any of the virtual assets," as established in the general provisions issued by the central bank. This is the follow-up to the country’s crypto currency bill, which intends to reduce money laundering and extremist financing. Under the new rules, cryptocurrency businesses must apply for permits to deal in cryptocurrencies and provide details of operations as well as how they plan to verify the identity of the customer and beneficiary.

South Korea

Blockchain-based cryptocurrency trading and brokerage businesses in South Korea witnessed an increase in illegal activities related to hacking, money laundering, overheating and blockage issues. As a result, the government decided to set up a separate business sector, and stated that blockchain-based cryptocurrency trading and brokerage businesses will not be included in the business venture enterprises.

In September, South Korea openly requested more cooperation between countries worldwide in the regulation of cryptocurrencies and ICOs. In making known his country's bid for more cooperation, Seok-Hun, the head of the South Korea's Financial Supervisory Service (FSS) said, "For new risks involving cryptocurrencies and ICOs, we must calm overheated speculation and crack down on illegal activities and improve transparency."

North Korea

On June 29, 2018, the FATF issued a statement that it remains concerned by the failure of the Democratic People's Republic of Korea (DPRK) to address the significant deficiencies in its AML/CFT regimes and the serious threats they pose to the integrity of the international financial system. "The FATF urges the DPRK to immediately and meaningfully address its AML/CFT deficiencies. Further, the FATF has serious concerns with the threat posed by the DPRK's illicit activities related to the proliferation of weapons of mass destruction (WMDs) and its financing," said the agency.

The FATF reaffirmed its February 25, 2011 call on its members and urged all jurisdictions to advise their financial institutions to give special attention to business relationships and transactions with the DPRK, including DPRK companies, financial institutions, and those acting on their behalf. In addition to enhanced scrutiny, the FATF further called on its members and urged all jurisdictions to apply effective counter-measures, and targeted financial sanctions in accordance with applicable United Nations Security Council Resolutions, to protect their financial sectors from money laundering, financing of terrorism and WMD proliferation financing (ML/FT/PF) risks emanating from the DPRK. They advised that jurisdictions should take necessary measures to close existing branches, subsidiaries and representative offices of DPRK banks within their territories and terminate correspondent relationships with DPRK banks, where required by relevant UNSC resolutions.

Saudi Arabia

FATF recently said "Saudi Arabia's financial intelligence unit is not able to conduct sophisticated financial analysis, although it does provide a wide variety of information that is available to and used by competent authorities. While money laundering investigations have increased in recent years, Saudi authorities are not investigating and prosecuting money laundering in a proactive fashion, particularly when it comes to complex money laundering schemes. They do not systematically pursue confiscation of proceeds."

United States

In Q3 2018, there were a number of significant developments on the AML regulation and enforcement front around the world. For instance, in July, President Trump signed an executive order establishing a new task force that will pay particular attention to financial crimes such as digital currency fraud, money laundering scams, and other digitally enabled financial crimes. It is led by the Justice Department and includes the SEC, the Federal Trade Commission, and the Consumer Financial Protection Bureau. The group's formation speaks to the fact that crypto-related crime is becoming a key issue in Washington, especially since the executive order specifically mentions "digital currency fraud" as one its prime targets.

Also, in the third quarter, the SEC delayed the decision to allow ETFs by several months.

In the U.S., there have also been moves to add teeth to AML/ATF regulatory schemes. There was also increasing scrutiny of non-trustworthy players or those with weak AML regimes. For example, on September 18, the New York Attorney General's office released the findings of a months-long investigation. The report said that cryptocurrency exchanges are not only vulnerable to market manipulation but also lack the standards of consumer protections commensurate with established financial markets.

In September, the New York Department of Financial Services (NYDFS), creator of the "BitLicense" framework for cryptocurrency companies, confirmed that it had given two chartered companies, Gemini Trust Company and Paxos Trust Company, permission to begin issuing these so-called "stablecoins" to clients.

FinCEN

Speaking at a tech conference this August, FinCEN's Director, Kenneth Blanco, revealed some important revelations regarding actions the agency is taking in regulation and compliance with respect to cryptocurrency money laundering services and crypto-to-crypto exchanges. These range from broader emphasis on enforcing AML rules to renewed scrutiny of anonymizing services to delegating the Bank Secrecy Act (BSA) examiner role to the IRS.

The FinCEN Director lauded crypto innovation while citing the need to reign in bad actors. "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, explained Blanco." He also warned, "we will hold companies and individuals accountable when they disregard their obligations and allow the financial system to be exploited by criminal actors, whether in wire transfers or cryptocurrencies."

Now receiving 1500 Crypto SARs per month

Blanco also lauded the substantial increase in crypto SAR (suspicious activity report) filings over the past few years as a great success. The agency now receives more than 1,500 SARs per

month describing dubious activity involving virtual currency. He cited the recent BTC-e case—the agency's first action against a foreign-located MSB and its most recent civil action involving virtual currency—and the crucial role SARs played in that investigation. "This information is critical to our mission of keeping our country strong, our financial system secure, and our families and communities safe from harm," explained Blanco.

This growth of SARs, especially since it has continued throughout the 3rd quarter of 2018, also points to a degree of lawlessness that persists in the cryptocurrency markets. Blanco further explained that his agency is working hard to ensure that virtual currency MSBs understand and comply with these regulatory obligations. Part of that effort involves working closely with delegated BSA examiners at the IRS. Together with the IRS they have examined 30% of all registered virtual currency exchangers and administrators since 2014 and intend to continuously monitor 100% of crypto exchanges.

Blanco underscored FinCEN's position the need for money transmitters to understand and implement AML. He explained that in order to comply with their obligations under the BSA., virtual currency money transmitters must do three things:

1) Register with FinCEN as a money services business.
2) Develop, implement and maintain an AML program designed to prevent the MSB from being used to facilitate money laundering and terrorist finance.
3) Establish recordkeeping, and reporting measures, including filing SARs and Currency Transaction Reports (CTRs).

These requirements also apply to domestic and foreign-based convertible virtual currency transmitters who conduct a substantial part of their business in the U.S., even if they have no physical presence there.

The Director further clarified FinCEN's position on crypto-to-crypto and blockchain hopping, which has obvious value for criminals laundering ill-gotten gains in cryptocurrencies. He said FinCEN's regulations cover not only transactions where the parties are exchanging fiat and convertible virtual currency but also transactions from one virtual currency to another virtual currency. "In short, individuals and entities engaged in the business of accepting and transmitting physical currency or convertible virtual currency from one person to another or to another location are money transmitters subject to the AML/CFT requirements of the BSA and its implementing regulations," continued Blanco. According to FinCEN rules, this also applies to anonymizing services (e.g., mixers or tumblers). Since they accept and transmit convertible virtual currency they, therefore, have regulatory obligations under the BSA.

About CipherTrace

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

