

Cryptocurrency Anti-Money Laundering Report, 2019 Q3

CipherTrace
Cryptocurrency Intelligence
November 2019



Executive Summary	4
Q3 Highlights	5
Major Trends And Developments	5
CipherTrace Research: Two-thirds of the 120 Most Popular Crypto Have Porous or Weak KYC	5
The FATF and FinCEN Bring a Harsh New Reality to the Crypto Space—Funds “Travel Rules”	7
<i>Travel Rule Reality Has Arrived — Nine Months Left for Nations to Pass Laws and for VASPs to Comply</i>	7
<i>The BSA Travel Rule - FinCEN Says It Has Been an Obligation for Crypto Asset Businesses Since 2011</i>	8
<i>How New FATF Rule Compares with Existing BSA Rule for US Banks</i>	10
<i>Will the Travel Rules Comprise a Needed Catalyst to Mature the Crypto Asset Sector?</i>	10
<i>FATF and FinCEN on Anonymizing Services and Anonymity-Enhanced Products</i>	11
Recent Reports of the Death of Privacy Coins Have Been Greatly Exaggerated	12
<i>Can Exchanges List Privacy Coins and Still Comply with the Travel Rules?</i>	13
<i>FATF Guidance May Have Caused Privacy Coin Valuations to Take a Major Hit</i>	14
<i>Will Privacy Coins Have a Place in a Post Travel Rule World?</i>	14
<i>Not All Exchanges Are Jettisoning Privacy Coins</i>	15
63% of Exchange that Trade Privacy Coins Have Weak or Porous KYC	15
Lowest Quarterly Thefts and Scams in Two Years	16
Trends Involving Virtual Assets by Terrorists and Rogue Nations	17
<i>OFAC Sanctions Crypto Addresses</i>	17
<i>Terrorist Use of Cryptocurrencies</i>	18
<i>Non-Compliant Networks Won't Survive the War on Terror</i>	19
Crypto Crime Trends	20
Researchers Warn of Extremely Dangerous Bitcoin QR Code Scams	20
New Malware Swaps Out Crypto Wallet Addresses as You Type Them	20
Ryuk Ransomware Targeting Cities Globally	20
Legal Actions	21
Crypto Capital Arrest	21
Bitcoin ATM Operator May Face Life in Federal Prison for Operating an Illegal Money Transmitter	22
SEC Halts Telegram's \$1.7 Billion Unregistered Digital Token Offering	22
Block.one to Pay \$24M Penalty for Unregistered ICO	23
The SEC Order Disapproves Rule Change Proposed By NYSE Arca	23
Kik Sold to Media Lab	23
Two Suspects in EtherDelta Hack Indicted by U.S. Authorities	24
SEC Sues Cryptocurrency Startup ICOBox for Selling \$14.6M Worth of Unregistered Tokens	24
Principal of Cryptocurrency Escrow Company Volantis Indicted For \$7 Million Fraudulent Scheme	24
Thefts, Scams and Fraud	25
Fusion Network Hacked for \$6.4 million	25
ETH Smart Contract FairWin Loses \$8M	25
Nigeria-Based Satowallet Disappears with \$1M of User Funds	26
PayFair Cold Wallet Hacked	27

Changes In The Global Regulatory Environment	27
Japan—Crypto Donations in Elections Are Legal	28
UK—FCA Provides Clarity on Current Cryptoassets Regulation	28
South Korea—Court Orders Exchange to Cover User's Stolen Cryptocurrency	28
Sanctioned Countries	29
Venezuela	29
<i>Venezuela Wants Central Bank to Hold BTC and ETH in Reserves, Considers Moving its Bitcoin and Ethereum Holdings</i>	29
<i>Maduro: citizen can soon use cryptocurrencies as a "method for free national and international payments"</i>	29
North Korea	30
<i>New UN Report: North Korea Hacked \$2 Billion from Banks and Cryptocurrency Exchanges to Fund WMD Production</i>	30
<i>UN Accuses North Korea of Laundering Money Through Blockchain Firm</i>	30
Iran	31
<i>Crypto Mining Now Legal, Trading—Illegal</i>	31
<i>Iran Crypto Developers Launch Platform to Bypass Sanctions for Flood Victim Aid</i>	31
Appendix	33
Privacy Coins Have Well Developed Plans for Travel Rule Compliance	33
<i>Monero</i>	33
<i>Zcash</i>	33
<i>DASH</i>	34
<i>Decred</i>	34
<i>The Privacy Coin Compliance Debate</i>	35

Executive Summary

Several major trends in Q3 2019 impacted the crypto asset community and financial institutions that deal in virtual assets. CipherTrace research also revealed important trends and issues around the status of anti-money laundering (AML) and counter terrorism funding (CTF) regulation and compliance.

First, the third quarter saw growing awareness of perhaps the biggest clampdown on virtual asset transactions to ever impact crypto exchanges as well as banks and other financial institutions. After months to absorb its implications, these businesses are coming to grips with the fact that in just seven months they will need to comply with the so-called FATF funds Travel Rule. In a major challenge to business models and user privacy, among other changes this rule requires virtual asset service providers (VASPs) to securely transmit (and store) sender and receiver information whenever cryptocurrency moves. At the same time, US regulators emphasized that a similar Travel Rule which has long applied to fiat funds transfers—also applies to cryptocurrency transactions. This has left firms struggling to find a technical solution in time to avoid potentially severe penalties or blacklisting.

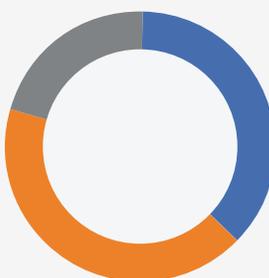
“(The Travel Rule) is the most commonly cited violation with regard to money service businesses engaged in virtual currencies.”

Kenneth Blanco, FinCEN Director

Next, CipherTrace researchers found that **two-thirds of the 120 most popular cryptocurrency exchanges have weak or porous know your customer (KYC) practices**. The results of this large-scale study constitute the first-ever comprehensive data on KYC policies at cryptocurrency exchanges around the globe.

CipherTrace research further found that 63% of exchanges that trade privacy coins have weak or porous KYC. This suggests privacy coins will find it harder to survive in a post FATF Travel Rule world if exchanges do not develop the proper KYC procedures necessary to mitigate the AML/CTF compliance risks that come with their anonymity-enhancing features.

63% of Top 120 Exchanges that Trade Privacy Coins have Weak or Porous KYC



■ 37% Strong ■ 42% Porous ■ 21% Weak
Source: CipherTrace Cryptocurrency Intelligence

Speculation has also abounded that new crypto AML regulations such as those from the FATF would spell the end of privacy coins. Although the FATF announcement in June initially caused a drop in the market value of privacy coins, many major privacy coin developers have well-developed plans for compliance using various techniques. Nonetheless, most crypto exchanges do not yet have a technical solution for complying with the FATF guidance. This is why CipherTrace developed an off-chain solution, and has given it to the community as open source.

Also, after two years of large, high-profile exchange hacks and exit scams, Q3 2019 witnessed a significant reduction in total cryptocurrency crimes from previous quarters. In fact, Q3 witnessed the lowest quarterly thefts and scams in two years. This sharp drop owes in part to the outsize influence of two enormous and still mysterious exit scams—QuadrigaCX (US\$192 million) and PlusToken (US\$2.9 billion). So far this year, the total of cryptocurrency-related frauds and thefts stands at **US\$4.4 billion**.

Another disturbing trend is that while the use of cryptocurrency by terrorists is not new, they are developing new, more sophisticated ways to obfuscate the flow of funds.

Q3 Highlights

- *Research: Vast majority of popular exchanges have poor or porous KYC.*
- *Research: 32% of popular exchanges trade privacy coins.*
- *VASPs and financial institutions need immediate technical solution for complying with the FATF and BSA funds Travel Rules to avoid major penalties.*
- *FinCEN director says Travel Rule is most often cited violation and banks and MSBs must comply with their obligations under the BSA.*
- *SoCal man faces potential life in prison for operating bitcoin ATM without adequate AML/CTF/KYC and for money laundering.*
- *FinCEN director says crypto related companies can help in the war on opioids by alerting of suspicious crypto transactions.*
- *While thefts and frauds fell in Q3, annual total so far in 2019 stands US\$4.4 billion.*
- *OFAC sanctions web addresses of three Chinese nationals involved in drug trafficking.*
- *New UN report says North Korea hacked \$2 billion from banks and cryptocurrency exchanges to fund WMD production.*

Major Trends and Developments

CipherTrace Research: Two-thirds of the 120 Most Popular Crypto Exchanges Have Porous or Weak KYC

During 2019, CipherTrace analysts gathered data on the KYC requirements at the top 120 crypto exchanges. This data includes their different KYC tiers and what a customer receives in return for providing the information. CipherTrace researchers tested all the exchanges using a standardized criteria and rated them as Weak, Porous, or Good based on how easy it would be to launder money after opening an account.

65% of Top 120 Exchanges Have Weak or Porous KYC

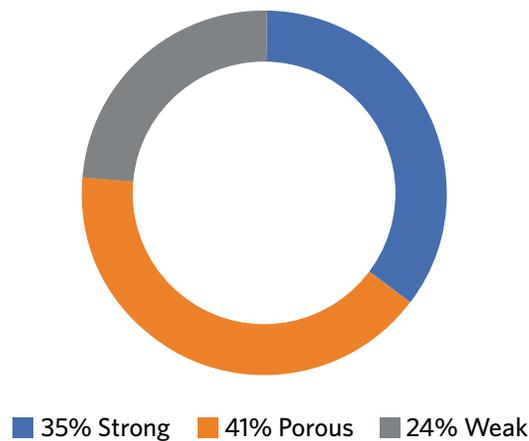


Figure 1

Source: CipherTrace Cryptocurrency Intelligence

The research results revealed that the lion's share—more than two-thirds—of exchanges do not have good KYC. The breakdown of the ratings shown in Figure 1 are as follows:

- Weak - These exchanges allowed CipherTrace researchers to withdraw at least .25 BTC daily with very little to no KYC.
- Porous - These exchanges require some sort of ID verification process.
- Strong - These exchanges require a very strenuous KYC process, which required several steps to complete before the researchers were able to make a deposit or withdrawal. They not only require an ID verification process but also proof of address. Some require a phone call or video chat to complete the KYC process.

The FATF and FinCEN Bring a Harsh New Reality to the Crypto Space—Funds “Travel Rules”

This quarter also saw crypto asset businesses at a loss for a technical solution to one of the biggest regulatory obstacles to ever hit the industry. On June 21, 2019, many virtual asset businesses were caught flat-footed when the global financial watchdog, the Financial Action Task Force (FATF), released its “Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. It recommended the FATF’s member countries adopt strict new regulations for virtual assets.

This tough stance should not have come as a surprise. For at least a half year, the FATF had been communicating the need for more stringent guidelines on monitoring and transferring virtual assets to counter what it perceives as growing threats of money laundering and terrorist financing. On February 22, 2019, the FATF released a Public Statement, “Mitigating Risks from Virtual Assets,” which was intended to clarify how the FATF standards apply to activities or operations involving crypto. The organization went so far as to open a short window to receive public comments on its proposals. CipherTrace gave its recommendations to the FATF in April (see *Response to FATF Regarding Regulation and Monitoring of Virtual Asset Service Providers: <https://ciphertrace.com/response-to-fatf-on-vasp-regulation/>*).

More oversight and regulation of virtual assets was also stated as a top priority of the FATF’s US president, Marshall Billingslea, and he seems to have kept his promise before turning over the reins to a new Chinese FATF presidency at the end of June.

United States Presidency Priorities for the Financial Action Task Force (FATF) — 2018-2019

Virtual currencies are increasingly being used to launder the proceeds of crime, but are not explicitly acknowledged in the FATF Recommendations. Most countries, including the majority of the FATF members, still do not regulate and supervise virtual currency providers for anti-money laundering/counter-financing of terrorism (AML/CFT). In light of emerging risks, there is an urgent need to explain how the FATF standards apply to virtual currency providers and related businesses, including for customer due diligence, funds transfers, supervision, and enforcement.”

— Marshall Billingslea, outgoing FATF president

Travel Rule Reality Has Arrived — Seven Months Left for Nations to Pass Laws and for VASPs to Comply

Despite this forewarning, when the reality of the new guidance finally hit, it turned the VASP world upside down. Among numerous AML and CFT clampdowns on cryptocurrencies, the FATF recommended that its 37 member countries—representing some 80 percent of the world’s GDP—enact what in US banking has long been referred to as a funds “Travel Rule.” Basically, the FATF’s new cryptocurrency Travel Rule compels VASPs to securely share customers’ information with other VASPs whenever crypto assets move (for transactions above USD/EUR\$1,000). Furthermore, they need to obtain and hold required originator information as well as required and accurate beneficiary information.

Specifically, according to the **FATF Interpretive Note to Recommendation 16**, originator and beneficiary information should include the following:

- Name and account number of the originator and benefactor
- Originator's (physical) address, national identity number, customer identification number, or date and place of birth
- Name and account number of the beneficiary

According to the FATF, cross-border transfers below the USD/EUR 1,000 threshold should also include the names and account numbers of originator and beneficiary. However, this information does not need to be verified for accuracy unless there is a suspicion of money laundering or terrorist financing.

The industry reaction to the Travel Rule ranged from complaints that it constituted a significant threat to the operability of crypto asset businesses to headlines calling the new regulation "Draconian." Crypto proponents cried foul, claiming the FATF new guidelines are antithetical to the prevailing notion of cryptocurrencies being inherently pseudo-anonymous. Others in the industry questioned whether compliance with the information sharing requirements is even possible given current blockchain technology.

Moreover, the FATF recommended a relatively short fuse—a 12-month period starting June 21, 2019—for member countries to codify the new recommendations and for VASPs to implement measures for complying with them. "The threat of criminal and terrorist misuse of virtual assets is serious and urgent, and the FATF expects all countries to take prompt action to implement the FATF Recommendations in the context of virtual asset activities and service providers," read the announcement. "The FATF will monitor implementation of the new requirements by countries and service providers and conduct a 12-month review in June 2020."

Given the huge obstacles the guidance throws in front of growing crypto asset businesses and the short time given to prepare, many in the VASP world were skeptical that the guidance would be broadly adopted. Those doubts were put to rest at the end of June when the G20 issued a statement at the close of its summit in Osaka, Japan. "We welcome the adoption of the Financial Action Task Force (FATF) Interpretive Note and Guidance... We call for the full, effective and swift implementation of the FATF Standards," said their communique.

Now, after nine months of disbelief, VASPs have just seven months left to comply with these tough new AML and CTF regulations.

Given that the FATF had for some time been telegraphing its intent to implement this type of guidance, CipherTrace began developing a solution almost a year ago. In order to help VASPs deploy a solution in time to avoid significant penalties or even existential risks to their business, it uses building blocks that have been proven for years in internet commerce, online banking, and government communications. The result, the Travel Rule Information Sharing Architecture (TRISA), is an open source solution that crypto exchanges and financial institution can begin deploying today and works at the speed and scalability required for the crypto economy.

The BSA Travel Rule — FinCEN Says It Has Been an Obligation for Crypto Asset Businesses Since 2011

As if the FATF had not thrown a big enough monkey wrench into the workings of the crypto economy, companies must also comply with another Travel Rule. According to the US Bank Secrecy ACT (BSA) rule [31 CFR 103.33(g)], for funds transfers above a USD 3,000 threshold financial institutions are required to share sender and receiver information. Enforcement of this rule lies with the US Treasury's Financial Crimes Enforcement Network (FinCEN). Anyone who has initiated a bank wire transfer in the US is surely familiar with these requirements.

Nonetheless, many cryptocurrency exchanges, banks and other financial institution did not understand that the BSA funds Travel Rule also applies to virtual assets. In May 2019, FinCEN clarified to money service businesses (MSBs) that going forward it would be strictly enforcing the BSA Travel Rule with regards to cryptocurrency transactions.

Then in a keynote address at the Cryptocurrency Travel Rule Compliance Conference held on November 5, 2019 in San Francisco, California, FinCEN Cyber and Emerging Tech Policy Specialist, Carol House, went further than the clarification issued in May. She reminded cryptocurrency MSBs that the BSA travel rule has applied to crypto assets since 2011, and that FinCEN is serious about enforcement.

House also reminded banks and other financial institutions that crypto exchanges are, in fact, Financial Institutions. In other words, when dealing with convertible virtual currencies (CVCs)—aka crypto assets—both entities are bound by BSA obligations, including the funds Travel Rule, which, in addition to the information sharing requirement, requires the party initiating a transfer of CVCs to know the VASP on the other side of the transaction.

Specifically, as with the FATF regulations, FinCEN requires a financial institution that is acting on behalf of a transmitter of value—or on behalf of another financial institution—to pass on any information about the transmitter and the transactions to the next financial institution in the transmittal chain. That is, compliance with both Travel Rules requires a financial institution to know when their counterparty is a financial institution. But House questioned if financial institutions fully understand these obligations, saying: "It would be interesting to know how many financial institutions operating in this space are able to identify a recipient as a financial institution on the basis of its wallet reference number, or the other information that it currently has available to it."

At the same appearance in San Francisco, House also cautioned that both the initiating financial institution and the receiving VASP are bound by BSA obligations, including the funds Travel Rule.

"Let's be clear and upfront on an issue that I think there's been some confusion around how that impacts a culture of compliance. The so called FATF travel rule that's in discussion here and in other places—many call it the FATF Travel Rule—has been a regulatory obligation for businesses in the United States dealing in virtual currency since 2011. Our delegated examiners at the IRS have been examining and issuing citations

for noncompliance with these requirements since they began conducting examinations on virtual currency businesses as of 2014,” emphasized House. She also cited Ripple and BTC-e among several examples of enforcement actions.

In an update on FinCEN’s website on October 20, FinCEN Director Blanco stated emphatically that FinCEN won’t accept the rationale that a company can’t comply with the law. “Any firms which do not believe they are able to fulfill the requirements in the BSA should not come to market,” Bianco explained. “It (the Travel Rule) applies to CVCs (convertible virtual currencies) and we expect that you will comply period.”

On November 15, Reuters reported the FinCEN head had strongly reiterated his agency will strictly enforce the BSA funds Travel Rule. “That’s what our expectation is. You will comply. I don’t know what the shock is,” Blanco emphasized. “FinCEN...has been conducting examinations that include compliance with the funds’ travel rule since 2014.”

Blanco added that it (the Travel Rule) is the most commonly cited violation with regard to money service businesses engaged in virtual currencies.

“The so called FATF of travel rule that’s in discussion here and in other places—many call it the FATF of travel rule—has been a regulatory obligation for businesses in the United States dealing in virtual currency since 2011.”

Carol House, the US Treasury’s FinCEN

How New FATF Rule Compares with Existing BSA Rule for US Banks

Figure 2 shows a comparison of the current BSA Travel Rule as it applies to banks (which now also applies to crypto asset transactions) and the soon-to-be-implemented FATF Travel Rule. Like the BSA, the FATF rule also requires VASPs to share originator and beneficiary information with recipient, although, as the chart shows, there are significant differences.

Will the Travel Rules Comprise a Needed Catalyst to Mature the Crypto Asset Sector?

If the industry can quickly adopt a common technical protocol for off-chain compliance, the FATF’s new regulations will potentially create a consistent international framework for virtual assets. This framework could significantly reduce criminal use of jurisdictional arbitrage to find the path of least resistance for money laundering—while at the same time addressing legitimate privacy concerns.

Travel Rule (BSA vs FATF)

General	BSA	FATF
Threshold	USD 3,000	USD/EUR 1,000
Information should be sent with the transmittal order or virtual asset transfer	✓	✗
Originator	BSA	FATF
Name	✓	✓
Account number	●	✓
Address	✓	✓
Identity of financial institution	✓	✗
Transmittal amount	✓	✗
Execution date	✓	✗
Recipient	BSA	FATF
Name	●	✓
Account number	✓	✗
Address	●	✗
Identity of financial institution	●	✓
Any other specific identifier of the recipient	●	✗

 Required
  When available
  Not required

Figure 2 *Address can be substituted for national identity number, or customer identification number, or date and place of birth
Source: CipherTrace Cryptocurrency Intelligence

“The AML framework provided by the Travel Rule “is a public good, including explicitly some of the requirements for financial institutions to know their customers and to know with whom they are doing business...,” concludes House. “The AML framework is good for investigators, it enables us to counter illicit networks and identify those illicit funds flows that are enabling criminal activity across multiple sectors and businesses when required and authorized by law to do so. The AML framework is good for the industry and customers as well. It helps institutions manage their reputational risk and it can help financial institutions establish conditions where even investors and other financial institutions and customers are eager to do business with the sector because there are necessary controls in place.”

FATF and FinCEN on Anonymizing Services and Anonymity-Enhanced Products

Both the FATF and BSA requirements for virtual assets and virtual asset service providers go beyond simply sharing PII, and privacy coin developers should fully understand these obligations. While at first glance it may appear that the Travel Rules only require the transmission of sender and receiver information, a closer look reveals much more.

Similarly, the FATF states in its recent guidance that anonymity-enhanced products or services are high-risk instruments that require enhanced monitoring that should “extend beyond the immediate transaction between the VASP or its customer or counterparty.”

While this guidance does not state how many hops on a transaction chain an exchange must be able to look back on to be in compliance, the theme remains the same: blockchain monitoring is vital for compliance when it comes to higher-risk transactions such as those involving privacy coins. Not only must VASPs know their customer, but they must now also know their customer’s customer.

Privacy coins with mandatory enforced anonymity features such as Monero—as well as the mainstream coins with privacy features added—must comply out of band with this regulation if they wish to continue to be traded on exchanges with Travel Rule obligations. (Note that “out of band” here means not on the blockchain). FATF explicitly states that if the VASP cannot manage and mitigate the risks posed by engaging in activities that involve the use of anonymity-enhancing technologies or mechanisms, **“then the VASP should not be permitted to engage in such activities.”**

While there is nothing in the FATF or BSA regulations that explicitly prohibits the use of privacy coins, their appeal comes from the notion that financial privacy is a protected/inherent right for individuals and investment funds alike. Moreover, in oppressive regimes such a currency can be used to counter government efforts to control and monitor citizens.

Recent Reports of the Death of Privacy Coins Have Been Greatly Exaggerated

Some experts once predicted the demise of Bitcoin and similar widely used cryptocurrencies because criminals and others wanting to keep their movement of funds secret had wised up to how the blockchain works. The digital ledger records which addresses send and receive funds, essentially stamping each transaction with the exact time and amount. With the rising sophistication of analytics technology, law enforcement can increasingly trace criminal activity of wallets addresses used by bad actors and not only make arrests but also successfully prosecute criminals.

The growing awareness of the traceability of transactions on public blockchains and de-anonymization technologies have led to the development of privacy coins to satisfy some users’ desire for protecting anonymity. Specifically designed to protect financial privacy and avoid transaction tracing, these alt-coins are not new nor are their intended use cases. As far back as the fall of 2017, an Interpol report noted that Monero, Ethereum and Zcash were gaining favor among “the digital underground.” And Monero in particular has since become a more popular method of payment in ransomware attacks. However, as verified by CipherTrace researchers (see CipherTrace Q2 2019 Crypto Currency Anti-Money Laundering report), 76% of dark market transactions and ransomware use bitcoin for payments.

These “privacy coins” still rely on a public ledger but use technology that obfuscates the path of the transaction. In some cases, it might still be possible to determine that a certain amount of cryptocurrency was sent, but the path leading from sender to recipient is concealed. The way in which various privacy coins go about this involves widely varying technologies.

Can Exchanges List Privacy Coins and Still Comply with the Travel Rules?

Cryptocurrency users ultimately have to cash out to fiat currency somewhere to spend their money in the real world. That involves linking to blockchain addresses to user accounts at off ramps such as exchanges, P2P marketplaces, bitcoin ATMs and other MSBs. This has led several regulated exchanges to begin delisting privacy coins out of fear they may violate AML regulations.

Because these alternate cryptocurrencies have the capability to obfuscate the flow of funds, some media outlets are predicting the Travel Rule will spell the death of privacy coins. This is because the regulation threatens to block the off ramps that allow users to easily convert privacy coins to fiat by requiring crypto exchanges to transmit personally identifiable information (PII) that would reveal the sender and receiver. Satisfying this requirement may or may not be possible on-chain, such as, for example, storing the PII in encrypted memos fields that are built into privacy coins like Zcash. Other coins are looking at using off-chain options—such as TRISA—to comply with the Travel Rules.

Thus, two challenges exist for privacy coins: 1) complying with the Travel Rule, and 2) proving the source of funds was not from an illicit business. As a result, many exchanges have already dropped coins like Monero (XMR) and DASH (DASH) in preparation for compliance. Japan has banned them and France is also threatening to ban them.

South Korean exchange Upbit, for example, determined the exchange could not continue to list the privacy coins and still comply with the new FATF recommendations. Consequently, Upbit ended transaction support for Monero (XMR), DASH, Zcash (ZEC), Haven (XHV), Bittube (TUBE) and PIVX (PIVX) as of September 30, 2019. A notice on the company website, gave the reason for delisting the coins as eliminating the possibility of money laundering. It also said the exchange would continue to consider crypto assets that present anonymity functions as candidates for delisting.

Other exchanges, such as Coinbase and OKEx, have begun delisting privacy coins as well. Coinbase delisted ZCash over the summer of 2019, while OKEX dropped five privacy coins in September, citing FATF Travel Rule regulations as the reason. At the same time, some exchanges are de-listing privacy coins, other coins such as Litecoin (LTC) and Decred (DCR) are in the process of adding new privacy features.

According to an August 28 Decred blog post, for instance, the company has developed new privacy features for its DCR token. Similarly, in an October 22 tweet, the Litecoin Foundation shared drafts of two Litecoin Improvement Proposals to implement the opt-in privacy feature MimbleWimble, clarifying that the foundation is moving forward with their proposed move towards privacy. These proposals can be found on GitHub: LIP-0002 EB and LIP-0003 MW.

FATF Guidance May Have Caused Privacy Coin Valuations to Take a Major Hit

Since the release of the FATF guidance in June and the accompanying loss of privacy coin support across several exchanges, Monero, Litecoin, Dash and Zcash have all lost between 50%-60% of their market value while the price of bitcoin has remained relatively stable in comparison (see figure 3).

Will Privacy Coins Have a Place in a Post Travel Rule World?

While this drop in price may appear discouraging, speculation of the death of privacy coins has been greatly exaggerated. FATF and FinCEN are not advocating an outright ban on privacy coins as long as controls are in place to mitigate the risks associated with their anonymity-enhanced features. FinCEN, for example, has clarified what it requires MSBs to fulfill their AML/CTF obligations under the BSA funds Travel Rule. When knowingly accepting anonymity-enhanced CVCs—i.e., privacy coins—money transmitters “must not only track a CVC through the different transactions, but must also implement procedures to obtain the identity of the transmitter or recipient of the value.”

This position is reflected in FinCEN’s \$110 million enforcement action against BTC-e in 2017. The regulatory agency did not specifically take action against BTC-e for its use of DASH per se. Rather, they took issue with the lack of appropriate money laundering controls in place while offering privacy-enhanced featured.

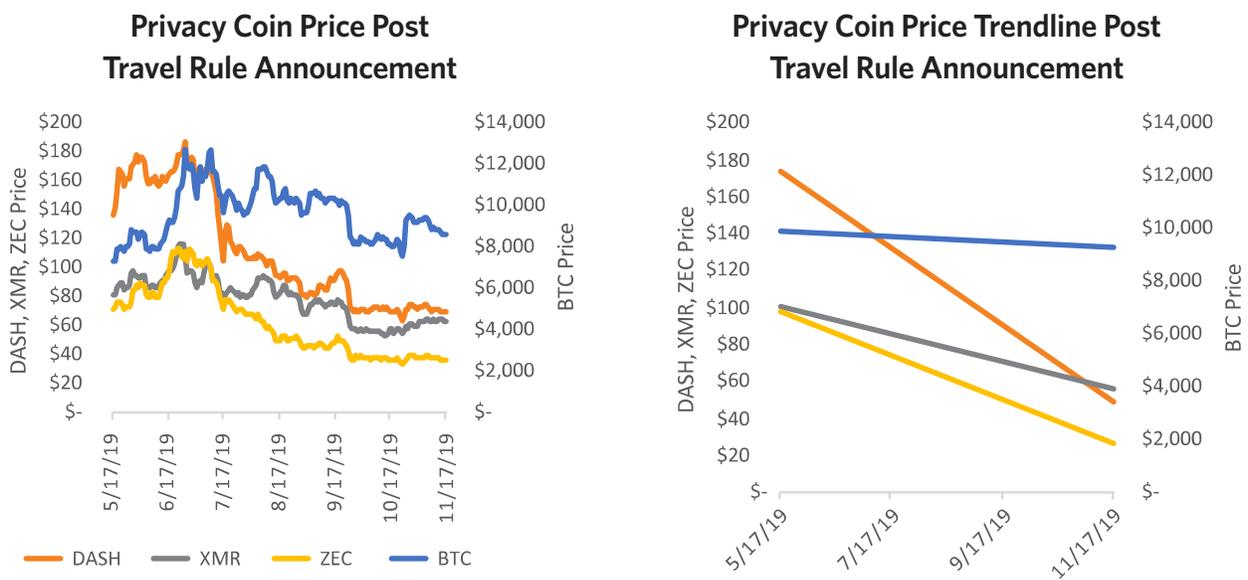


Figure 3 Source: CipherTrace Cryptocurrency Intelligence

The BTC-e case also offers an example of the broad reach of the US Treasury's Bank Secrecy Act Travel Rules. Although BTC-e was not a US-based exchange, its onboarding of US customers gave the FinCEN jurisdiction to apply BSA regulations on the company. So any VASP doing business with US persons should be cognizant that they have US AML obligations under the BSA.

Not All Exchanges Are Jettisoning Privacy Coins

On September 17, 2019, almost three months after the release of the new FATF guidelines, Zhao Chang-peng, Binance's chief executive officer, announced on Twitter that the company would support Monero, Zcash and Dash on the grounds that privacy is a fundamental right. On October 10, OKEx Korea reversed its earlier decision to delist ZCash and DASH pending a further compliance review. ZCash responded to the reversal in a CoinDesk interview, stating, "Zcash is entirely compatible with all FATF recommendations, including the Travel Rule. We've been working with OKEx and others in South Korea and happy to hear that OKEx has decided to take additional time to further evaluate Zcash support based on newly available compliance information." For a deeper dive into how various privacy coins plan to comply with the Travel Rules, see **Appendix A**.

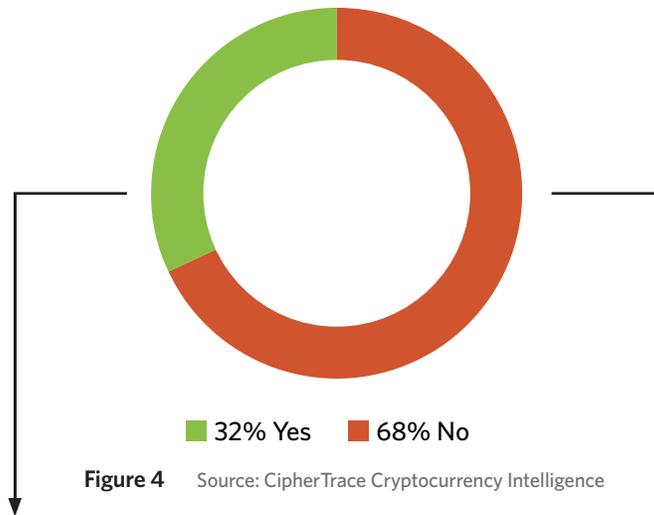
63% of Exchanges That Trade Privacy Coins Have Weak or Porous KYC

While the privacy coins have many use cases for individuals with legitimate concerns about anonymity and confidentiality, they can also provide payment rails to facilitate fraud, tax evasion, money laundering, terrorism financing, and cyber extortion. Based on U.S. Secret Service investigations into criminal use of digital currencies, criminals prefer digital currencies with the following characteristics:

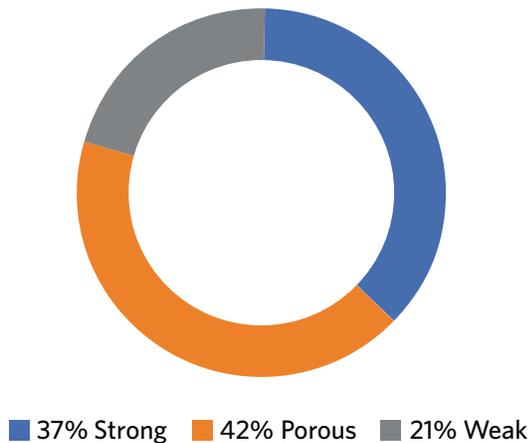
- The greatest degree of anonymity
- Widespread adoption as a medium of exchange for intended criminal activities
- Protection against theft, fraud, and lawful seizure
- Can be readily exchanged to and from their preferred currency

While bitcoin may still be king among criminals on the darkweb, as discussed in CipherTrace's Q2 2019 Crypto AML Report, it is also bitcoin's open blockchain that allows investigators to apprehend darkweb criminals, such as the recent takedown of the largest-to-date child sexual exploitation market "Welcome to Video". While KYC procedures at exchanges allow for visibility into some privacy coin transactions—such as transactions on the exchange or transfers to a new wallet—a majority of their use is still hidden from investigators.

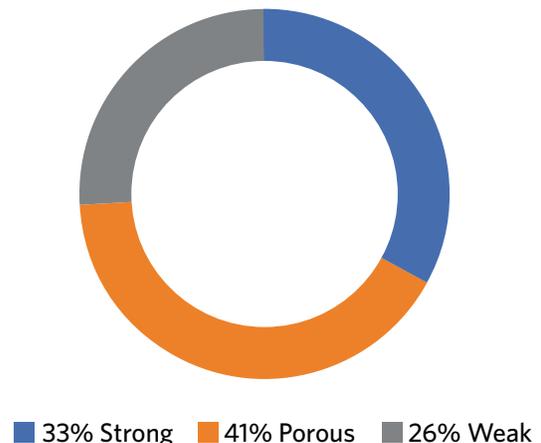
Only 32% of Top 120 Exchanges Trade Privacy Coins



63% of Top 120 Exchanges That Trade Privacy Coins Have Weak or Porous KYC



67% of Top 120 Exchanges That Don't Trade Privacy Coins Have Weak or Porous KYC



Lowest Quarterly Thefts and Scams in Two Years

After two years of large, high-profile exchange hacks and exit scams, Q3 2019 witnessed a significant reduction in total cryptocurrency crimes from previous quarters. This sharp drop owes in part to the outsize influence of two enormous and still mysterious exits scams—QuadrigaCX (US\$192 million) and PlusToken (US\$2.9 billion). So far this year, the total of cryptocurrency-related frauds and thefts stands at US\$4.4 billion.

This quarter, cybercriminals stole \$6.5 million from cryptocurrency exchanges, while insiders bilked cryptocurrency users out of \$9 million in exit scams and Ponzi schemes. This total of \$15.5 million represents the smallest number of cryptocurrency crimes of any quarter in the past several years. Certainly, if the lower altitude of this trend line persists it should provide a confidence boost for users and investors in an industry rocked by one exchange heist, scam or Ponzi scheme after another.

While CipherTrace has no hard data to explain this drop—except for the anomalous nature of the QuadrigaCX and PlusToken frauds skewing the numbers in previous quarters—one possible explanation is that government regulation of the industry is having a positive impact. CipherTrace had previously speculated that the shift from outright thefts to exit scams and other frauds perpetrated by insiders suggested that crypto exchanges had begun to adequately invest in hardening their IT infrastructures. Also, increased regulatory scrutiny of initial coin offerings (ICOs) and security token offerings (STOs) has either increased their quality or screened out fraudulent and poor-quality token offerings (often referred to as sh1t coins).

Thefts, Hacks and Scams by Year

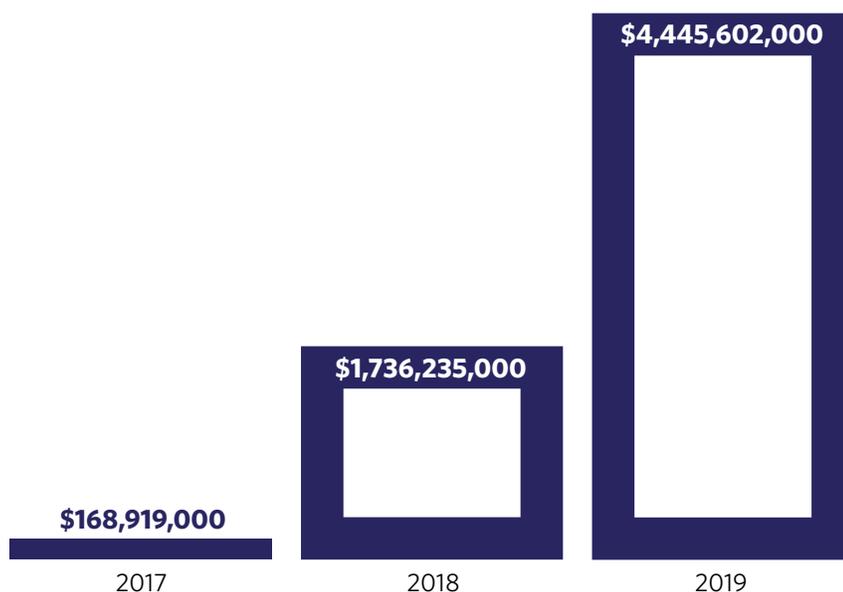


Figure 7

Source: CipherTrace Cryptocurrency Intelligence

While the year-over-year trend for thefts and scams is up, Q3 2019 saw a significant drop in crypto crime. Several huge exit scams and misappropriation of funds in 2019—Plus Token at US\$2.9B, QuadrigaCX at US\$192 million, and the Bitfinex misappropriate of US\$851 million—skewed this yearly total to the upside.

Trends Involving Virtual Assets by Terrorists and Rogue Nations

OFAC Sanctions Crypto Addresses

On August 21, 2019, the US Treasury Department’s Office of Foreign Asset Control (OFAC) sanctioned several Chinese nationals, adding them and their associated Bitcoin addresses to the Specially Designated Nationals and Blocked Persons (SDN) list as significant foreign narcotics traffickers. An in depth look at these designations can be found in our blog: <https://ciphertrace.com/cryptocurrency-analysis-combats-the-opioid-crisis/>

However, these designations are just the tip of the iceberg when it comes to these drug trafficking organizations. While OFAC is further identifying BTC addresses associated with these drug traffickers to maximize the disruption of their financial dealings, CipherTrace analysts have already identified multiple

wallets associated with the sanctioned individuals. This blockchain intelligence helps to ensure crypto exchanges and investigators have the most up-to-date data. The information also helps crypto asset businesses to be a force in combating drug trafficking and the opioid crisis.

According to FinCEN's Blanco, the US is working towards "making the financial sector aware of tactics and typologies behind illicit schemes to launder the proceeds of these fatal [fentanyl] sales, including transactions using digital currency and foreign bank accounts. Financial institutions must be on alert to red flags and other indicators of the complex schemes fentanyl traffickers are employing so that financial institutions can report and share relevant information with law enforcement, and ultimately help save lives."

Terrorist Use of Cryptocurrencies

Terrorist organizations and their supporters and sympathizers are constantly looking for new ways to raise and transfer funds without detection or tracking by law enforcement. On September 11, 2019, the recently retired United States Treasury undersecretary Sigal Mandelker stated that, "without the appropriate strong safeguards cryptocurrencies could become the next frontier."

She noted that Hamas—which has been designated a terrorist organization by several countries and international organizations—has already tried to use cryptocurrency as a payment rail, asking supporters via social media to send bitcoin donations to two addresses.

Hamas asked for bitcoin donations via a telegram channel run by its military wing known as the Qassam Brigades. Accompanying the request was a video detailing how to acquire and send bitcoin without tipping off authorities as well as several promotional posters asking for crypto donations. To further obfuscate the flow of funds, every donor is given a unique bitcoin address. The operation brought in roughly \$5000 to the terrorist organization.

"While this may not seem like a lot of money, a FinCEN analysis found remittances linked to terrorism averaged less than \$600 per transaction," explained Mandelker. "As we know, the cost of carrying out a terrorist attack can be very low. But the human costs to victims is always extraordinarily high."

For more color on this topic, CipherTrace researchers contacted Jason Blazakis, former director of the Counterterrorism Terrorism Finance and Designations Office at the U.S. Department of State's Counterterrorism Bureau and current director of the Center on Terrorism, Extremism, and Counterterrorism.

"Terrorists don't have to raise a lot of crypto or cash to maintain sanctuary for sleeper cells or, worse yet, the ammunition, guns, and bombs that can maim innocent civilians," explained Blazakis. "While a thousand dollars may not seem like a lot of money, in the hands of the wrong person, it can do all of the above and much more."

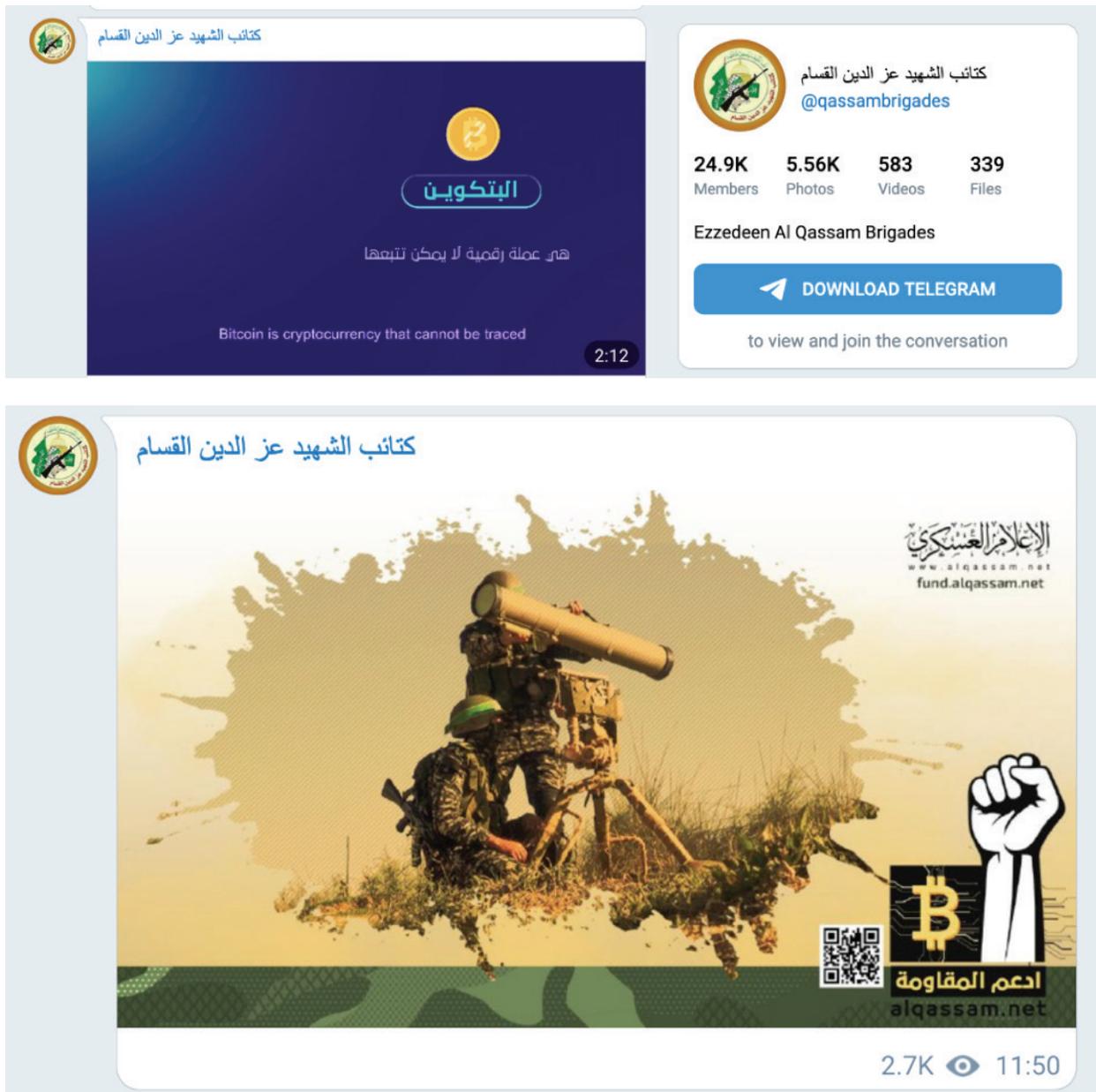


Figure 8 Screenshots from the Qassam Brigade's Telegram channel asking for donations in bitcoin

Non-Compliant Networks Won't Survive the War on Terror

The digital asset industry has spent a tremendous amount of energy and expertise in developing new systems to transmit value," added Melakar. "That industry now needs to harness that technological expertise and apply it to the tough problems we need to solve in illicit finance—both because not doing so threatens national security, and because it is the only way for them to pass regulatory muster. Absent appropriate safeguards to keep our nations and our communities safe from terrorists, rogue regimes, and others who threaten us, the U.S. will work with governments around the world to make sure that non-compliant networks and fintechs do not survive."

Crypto Crime Trends

Researchers Warn of Extremely Dangerous Bitcoin QR Code Scams

Cryptocurrency users face a new and pervasive danger of fraud related to QR codes. Researchers from cryptocurrency wallet provider ZenGo have found that four of the first five Google search results for “bitcoin QR generator” led to scam websites. When an unsuspecting crypto user tries to create a QR code for their own bitcoin address, the bogus site will instead create a QR code for the scammer’s wallet.

According to Forbes, ZenGo’s co-founder, Tal Be’ery, wrote in a blog post, “Scammers do not even bother with generating their fake QR themselves, instead they shamelessly call a blockchain explorer API to generate the QR for their address.”

ZenGo’s researchers calculate that some \$20,000 has recently been lost to QR code scams, calling their findings “just the tip of the iceberg,” as thieves likely regularly change their bitcoin and crypto addresses to avoid detection and blacklisting.

New Malware Swaps Out Crypto Wallet Addresses as You Type Them

Masad Stealer, a new strain of malware, has the ability to replace wallet addresses as users type them into an infected web browser. In addition to wallet addresses, the malicious code can also steal credit card numbers and user information such as passwords and files, and can even take a screenshot of the victim’s desktop.

From there, the sensitive stolen data is stored in the malware command and control—a Telegram account. It is important to note that the malware can change Monero, Litecoin, Zcash, Dash and Ethereum addresses automatically. It can also intercept legitimate crypto transactions once the address swap is complete.

Bad actors can purchase Masad Stealer for \$40 on the dark web and custom-configure it. This malware is believed to be an active and ongoing threat.

Ryuk Ransomware Targeting Cities Globally

On October 2, the FBI issued a new “high-impact” warning regarding ransomware attacks—which lock access to computers and networks until victims pay a ransom—claiming they are an ongoing cyber threat facing U.S. businesses and organizations. These attacks often ask victims to pay the ransom in cryptocurrency.

According to the alert, these attacks are becoming more targeted, sophisticated, and costly, and are more frequently targeting health care organizations, industrial companies, and the transportation sector.

One ransomware in particular is especially prevalent—Ryuk. On October 1st, the day before the FBI's release, three hospitals owned by Alabama-based DCH Health Systems were struck by the Ryuk ransomware, infecting all 1,500 of the hospitals' computers. As a result, the facilities were forced to turn away nonemergency patients as they were locked out of their systems. In order to regain control, the hospitals chose to pay the bitcoin ransom demands despite the FBI warning that paying the ransom only encourages more attacks and attackers don't always deliver decryption keys.

Ransomware like Ryuk is frequently used to target organizations such as hospitals, public utilities, and municipal governments because they require quick access to their networks, making them more likely to pay the ransom. In June 2019 alone, the hackers using the Ryuk ransomware collected over \$1M from Florida municipalities. Lake City, Florida, authorized its insurer to send hackers 42 BTC—worth roughly \$500,000—after Ryuk disabled city servers, phones, and email. A few weeks earlier, the Riviera Beach City Council authorized its insurer to pay a 65 BTC ransom—worth about \$600,000 at the time—after the Ryuk ransomware encryption took most of the city's IT systems offline.

But Ryuk is not just impacting organizations in the US. On June 22, 2019, the UK's National Cyber Security Centre (NCSC) released a detailed security advisory on the threat and how the ransomware is targeting organizations globally. To defend against or mitigate the damage done by Ryuk, the NCSC recommends:

- Keeping backups of important files
- Protecting devices and networks by keeping software up to date
- Whitelisting applications
- Installing antivirus software
- Using URI reputation services
- Employing multi-factor authentication to reduce the impact of password compromises

Legal Actions

Crypto Capital Arrest

On October 24, Crypto Capital President Ivan Manuel Molina Lee was arrested by Polish authorities for suspected money laundering and his involvement in an international drug cartel. According to Polish media, Lee was laundering money for Colombian drug cartels through cryptocurrency exchanges.

Crypto Capital's payment processing services were used by several prominent exchanges, such as Binance, Kraken and BitMEX. However, most notably, Crypto Capital played a key role in the recent Bitfinex and QuadrigaCX scandals. For more information on Crypto Capital, see the CipherTrace Q2 2019 Cryptocurrency Anti-Money Laundering Report.

Bitcoin ATM Operator May Face Life in Federal Prison for Operating an Illegal Money Transmitter

According to an announcement from the US Department of Justice, a Westwood, California man has agreed to plead guilty to federal criminal charges for owning and operating an unlicensed money transmitting business where he exchanged cash and virtual currency for individuals, including Darknet drug dealers and other criminals, some of whom used his Bitcoin ATM.

According to a release from the US Attorney's Office, Kunal Kalra—aka "Kumar," "shecklemayne," and "coinman"—allegedly laundered up to \$25 million in cash and crypto for drug dealers and other criminals. The list of charges includes: distribution of methamphetamine, operating an unlicensed money transmitting business, laundering of monetary instruments, and failure to maintain an effective AML program. Kumar could face a maximum possible sentence of life in prison.

These charges against Kalra are believed to comprise the first federal criminal case charging an unlicensed money remitting business that used a Bitcoin ATM kiosk. The complaint specifically cites a lack of AML and KYC controls. For example, customers who used the kiosk were not required to provide their identities, and the defendant had not installed cameras or implemented other measures requiring customers to identify themselves.

Kalra also faces money laundering charges. According to the plea agreement, he "admitted that in 2017 he exchanged approximately \$400,000 in cash for Bitcoin for an undercover agent who contacted him online and later met him in person on multiple occasions at a coffee shop in Los Angeles. The undercover agent told Kalra that his virtual currency was proceeds of drug trafficking, and Kalra continued with various transactions." Kara also set up bank accounts in the names of others and fake businesses, which allowed him to launder the money.

Bitcoin ATM operators have previously been largely unmolested but notorious for compliance risks that come with inadequate AML control. CipherTrace has developed an **AML compliance solution for Bitcoin ATMs** that enables compliance-minded kiosk vendors to easily adopt and enforce a risk-based AML compliance policy.

SEC Halts Telegram's \$1.7 Billion Unregistered Digital Token Offering

On October 11, the SEC filed an emergency action and obtained temporary restraining order against Telegram Group, Inc. and its wholly owned subsidiary TON Issuer, Inc. in response to their \$1.7 billion unregistered digital token offering.

According to Steven Peikin, Co-Director of the SEC's Division of Enforcement, the SEC has "repeatedly stated that issuers cannot avoid the federal securities laws just by labeling their product a cryptocurrency or a digital token... Telegram seeks to obtain the benefits of a public offering without complying with the long-established disclosure responsibilities designed to protect the investing public."

Block.one to Pay \$24M Penalty for Unregistered ICO

On Sept 30, the SEC announced charges against Cayman Island based blockchain firm Block.one for conducting an unregistered initial coin offering. The ICO raised US\$4 billion between June 2017 and June 2018. Block.one agreed to settle the charges by paying a US\$24 million civil penalty without admitting or denying its findings.

“Block.one did not provide ICO investors the information they were entitled to as participants in a securities offering,” explained Steven Peikin, Co-Director of the SEC’s Division of Enforcement. “The SEC remains committed to bringing enforcement cases when investors are deprived of material information they need to make informed investment decisions.”

The SEC Order Disapproves Rule Change Proposed By NYSE Arca

On Oct 9, the SEC announced an ETF proposal from Bitwise—a San Francisco based venture-backed cryptocurrency index and fund provider—filed in conjunction with NYSE Arca, did not meet legal requirements to prevent market manipulation or other illicit activities. According to the SEC, the onus for proving the listing exchange is designed to prevent fraudulent activity falls on NYSE Arca, as “NYSE Arca has not met its burden under the Exchange Act and the Commission’s Rules of Practice to demonstrate that its proposal is consistent with the requirements that the rules of a national securities exchange be ‘designed to prevent fraudulent and manipulative acts and practices.’”

Bitwise hopes to be the first company with a Bitcoin ETF in America, which would allow BTC to be traded like stocks or bonds on an exchange.

Kik Sold to Media Lab

As reported in the CipherTrace Q2 2019 Anti-Money Laundering Report, on June 4, 2019, the SEC sued Kik Interactive Inc. for raising nearly \$100 million in an unregistered securities offering. The SEC’s complaint alleged Kik had been losing money for years and the company’s management predicted internally that it would run out of money by 2017. To mitigate this shortfall, Kik developed a new mode of business financed through the sale of one trillion “Kin” tokens, raising more than \$55 million from U.S. investors alone. However, according to the complaint, at the time, Kin tokens were trading at half the value paid by public investors during the initial coin offering.

In a move to keep the Kin cryptocurrency afloat, Kik CEO Ted Livingston announced in late September that the Kik Corporation would shut down its messaging app to fund its battle with the SEC. However, by October 7, Livingston tweeted that Kik had signed a letter of intent with a company interested in buying the messaging app and keep its integration with Kin. On October 13, the Kik tweeted that their messaging app was “here to stay” despite their September announcement.

The messaging app Kik was on the verge of shutting down, but a holding company, MediaLab, bought it and will invest in its future, the company said.

At its peak, Kik had hundreds of millions of registered users and the company earned a private market valuation of \$1 billion, placing it in the elite ranks of tech unicorns.

Two Suspects in EtherDelta Hack Indicted by U.S. Authorities

On August 13, the United States attorney's office for the Northern District of California indicted Elliot Gunton and Anthony Tyler Nashatka for the 2017 hacking of EtherDelta—a crypto exchange built on the Ethereum blockchain. According to the indictment, Gunton and Nashatka were able to modify the exchange's domain name system setting by gaining access to the phone number of an EtherDelta employee and using that number to access the employee's email and, ultimately, to the domain name system account. Once they were in the system, they were able to redirect the website's traffic to a fake website resembling the real EtherDelta platform, and thereby steal users' private keys.

The two are charged with conspiracy to commit computer fraud and abuse (10-year maximum penalty); transmission of a program, information, code, and command to cause damage to a protected computer (10-year maximum penalty); unauthorized access to a protected computer to obtain value (5-year maximum penalty); conspiracy to commit wire fraud (20-year maximum penalty); and aggravated identity theft (2-year maximum penalty).

SEC Sues Cryptocurrency Startup ICOBox for Selling \$14.6M Worth of Unregistered Tokens

On September 18, the SEC announced it was suing ICOBox and its founder, Nikolay Evdokimov, for allegedly running an illegal token sale in 2017 that brought in more than \$14.6 million. The SEC asserts ICOBox sold its illegal ICO tokens to more than 2,000 investors without registering them as securities. Furthermore, ICOBox failed to register as a broker despite operating as one by facilitating ICOs for other startups, raising over \$650 million on behalf of dozens of clients.

Principal of Cryptocurrency Escrow Company Volantis Indicted For \$7 Million Fraudulent Scheme

On September 30, the United States Attorney for the Southern District of New York charged Jon Barry Thompson, the principal of the cryptocurrency escrow company Volantis with two counts of commodities fraud—each of which carries a maximum sentence of 10 years in prison. The Feds also brought a two counts of wire fraud—each of which carries a maximum sentence of 20 years in prison—for allegedly taking \$7 million from two victim companies after making false promises in connection with Bitcoin transactions. According to Manhattan U.S. Attorney Geoffrey S. Berman, Thompson “repeatedly lied to

investors in cryptocurrencies about the safety of their investments made through his companies. As a result of Thompson's lies, investors lost millions of dollars."

Separately, the U.S. Commodity Futures Trading Commission (CFTC) also filed civil charges against Thompson for "a deceptive and fraudulent scheme by knowingly or recklessly making false representations to customers in connection with the purported purchase of virtual currency." According to the complaint, neither Thompson nor his companies had possession or control of the bitcoin he promised to safeguard and deliver to his customers. Instead, Thomson transferred customer funds into accounts that benefited him and others. Additionally, Thompson lied about why he was unable to deliver the bitcoin, as promised.

Thefts, Scams and Fraud

Fusion Network Hacked for \$6.4 million

On September 28, Fusion Network announced that one of its wallets containing 10 million of native FSN tokens and 3.5 million ERC-20 FSN tokens had been emptied, resulting in the loss of US\$6.4 million. They traced the cause of the compromise to the theft of the wallet's Private Key and suggested an insider may have been behind the theft. To close the hacker's potential off-ramps, exchanges OKEX, Huobi, Bitmax, Citex, Hotbit have since suspended deposit and withdrawal of FSN tokens and all remaining funds have been transferred to a cold wallet.

Since the hack occurred, of the 13.5 million tokens stolen, 7.52 million were sent to exchanges and 5.98 million remain in the criminal's accounts according to the October 3rd "Fusion Foundation Wallet Theft Update." Since November 12, 2019, the theft has been officially classified as a crime in China. The company plans to issue a new ERC20 FSN smart contract address as a way of removing the ERC20 FSN tokens still in the hacker(s)' possession.

ETH Smart Contract FairWin Loses \$8M

On October 1, someone emptied the smart contract for the Ethereum-based gambling platform FairWin, which was recently accused of being the fastest-growing Ponzi scheme on Ethereum. This occurred only a few days after smart contract researcher Philippe Castonguayit and his team publicly disclosed the presence of vulnerabilities in the smart contract that could allow the admins to steal all users' deposits. At the time of the disclosure, the contract held roughly 50,000 ETH (US\$8M). Four days later, it held zero ETH.

The team found that the Ethereum contract was filled with typos and bugs and the Fairwin.me website contained red flags such as the use of famous artists and Instagram stars' photos to represent their executive team. A look at the website (Figure 9) now shows that these have been replaced with cartoons.

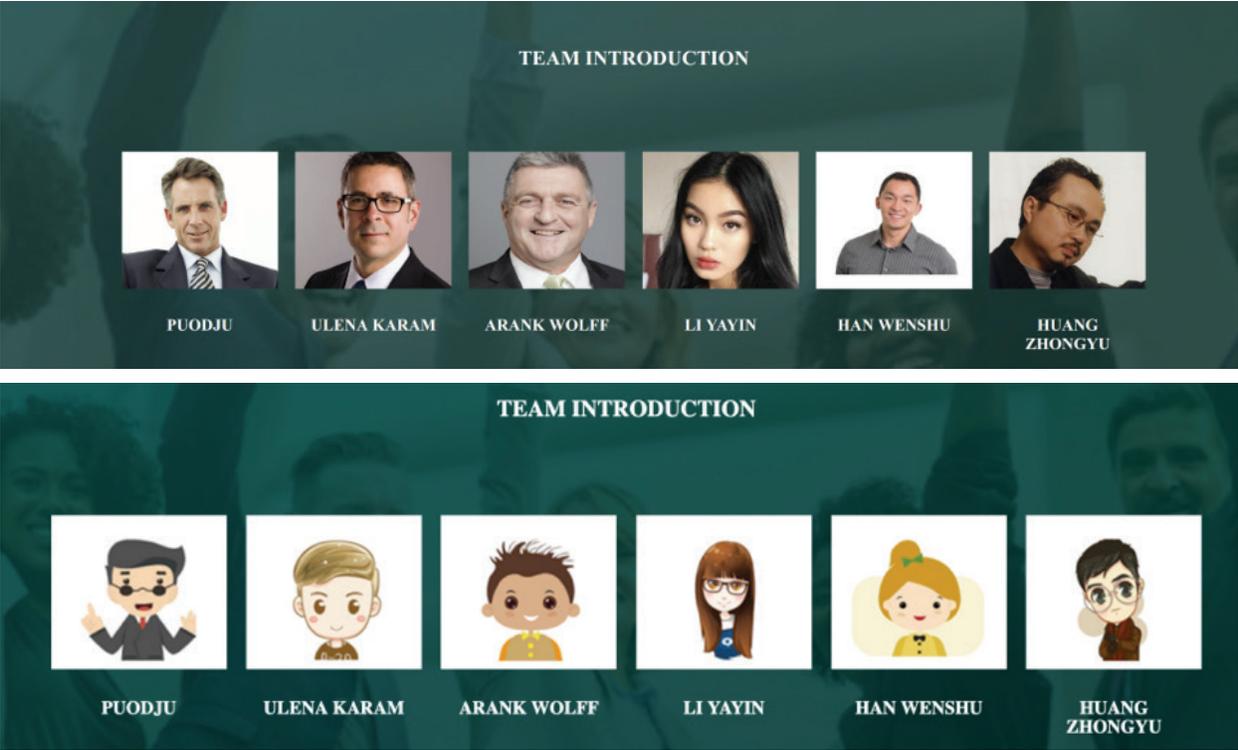


Figure 9

At the time of this report, FairWin’s balance remains at zero ETH, and there is no news on what has happened to the management team responsible for the loss. While the Fariwin.me website is still up, the company has not responded to inquiries regarding the incident or accusations of foul play. Castonguayit’s team has found no concrete evidence to suggest that the contract vulnerability was exploited.

Nigeria-Based Satowallet Disappears with \$1M of User Funds

In September, Satowallet, a Nigerian crypto wallet, allegedly pulled off an exit scam, disappearing with an estimated US\$1 million worth of users’ funds. In a since-removed Medium post, the CEO Samuel Ben wrote that crypto assets after purported server issues took down its site and app. After restoring the server data, Ben “noticed that the coins were no longer there from the backups and private keys” and accused OVH of fraud and trying to steal their wallet servers. Nigeria-Based Satowallet Disappears with \$1M of User Funds

In September, Satowallet, a Nigerian crypto wallet, allegedly pulled off an exit scam, disappearing with an estimated US\$1 million worth of users’ funds. In a since-removed Medium post, the CEO described how purported server issues took down its site and app. Ben claimed that after restoring the server data he “noticed that the coins were no longer there from the backups and private keys.” He accused Satowallet’s hosting provider, OVH, of fraud and trying to steal their user’s funds from its wallet servers.

Affected users have been quick to point out the flaws in Ben’s story on Twitter, as the hosting providers shouldn’t have access to the private keys, meaning the cryptocurrency should be recoverable if Satowallet was a legitimate operation. Satowallet’s Twitter account has since been suspended and their website still appears to be offline.

PayFair Cold Wallet Hacked

On October 2, PayFair—a decentralized escrow and P2P exchange—closed its website because one of its main cold wallets was emptied, leading many to speculate about a possible exit scam. On September 29, Payfair disclosed on its Telegram channel that the private key to one of its cold wallets was compromised, which led to a hack. Their team says it is still unsure of how the private key was compromised but is conducting an internal investigation into the matter. While user funds have since been transferred to backup wallets, part of the ETH that was stolen has not been recovered. Despite announcing that the platform would only be down “until the end of the week,” the PayFair.io website still appears to be down and they have not updated their social media since July 29.

Changes in the Global Regulatory Environment

Current Implementation of AML/CTF Regulations Globally

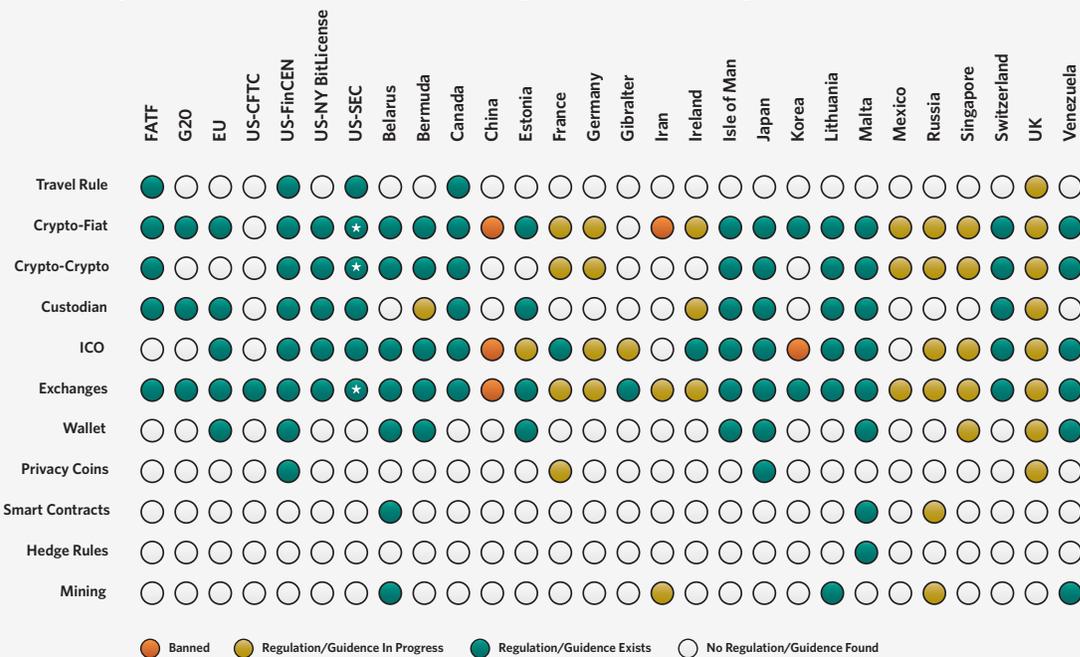


Figure 10 Source: CipherTrace Cryptocurrency Intelligence
* If securities are traded

Global Cryptocurrency AML Timeline



Figure 11

Japan — Crypto Donations in Elections Are Legal

On October 5, the Internal Affairs and Communications Minister of Japan, Sanae Takaichi clarified the legality of cryptocurrency donations, especially in regard to election laws. According to Takaichi, because virtual currency is not legally equivalent to money in Japan, crypto contributions do not face the same restrictions as fiat contributions under the Political Funds Control Act (PFCA). Under the PFCA, it is prohibited to make anonymous contribution in connection with elections or other political activities and there are limits to the amount any one person or entity can contribute per year. This loophole, however, allows individuals to make crypto donations to political parties without having to adhere to any of these regulations. The use of privacy coins would completely obfuscate from whom or how much a politician is receiving in campaign funds.

UK — FCA Provides Clarity on Current Cryptoassets Regulation

On July 31, the UK's Financial Conduct Authority (FCA) published its Final Guidance (PS19/22), which sets out the specific cryptoasset activities it regulates. Similar to FinCEN's May 9 guidance, this guidance will help firms understand whether their cryptoasset activities fall under FCA regulation or not. This guidance will help firms have a better understanding of what they need to do to ensure they are compliant.

The Final Guidance sets out instances where tokens are likely to be:

- Specified investments under the Regulated Activities Order
- Considered E-Money under the E-Money Regulations
- Captured under the Payment Services Regulations
- Outside of regulation

South Korea — Court Orders Exchange to Cover User's Stolen Cryptocurrency

On September 25, a South Korean court ruled that cryptocurrency exchange CoinOne must reimburse 25 million won (\$20,800 USD) to a user after he was hacked. While the thief used the victim's personal login credentials to steal 45 million won (\$37,600 USD), a daily withdrawal limit of 20 million won was supposed to be in place and could have prevented the full amount from being taken. The victim also argued that the exchange should have blocked the foreign IP address the hacker was using to access his account because it was different than his normal access point. However, the judge in the case found that the exchange was not liable for this type of safeguard—just for the failure of the withdrawal limit. CoinOne is therefore responsible for covering the additional losses over the 20-million-won limit.

Sanctioned Countries

Venezuela

Venezuela Wants Central Bank to Hold BTC and ETH in Reserves; Considers Moving its Bitcoin and Ethereum Holdings

Despite having its own national cryptocurrency, it is very likely that Venezuela is also using Bitcoin and Ether to evade international sanctions. According to Bloomberg, tipsters say the country's central bank is testing the possibility of holding cryptocurrencies in an effort to help the state-controlled oil company Petroleos de Venezuela SA (PDVSA). The oil firm supposedly has troves of Bitcoin and Ether, resulting from its attempt to bypass economic sanctions that are designed to limit international trade with the company. However, without the help of the central bank, converting its reserves to fiat to pay its suppliers may prove to be difficult. The central bank is also incentivized to start counting the cryptocurrencies towards its international reserves as what it currently holds has plummeted in recent years due to economic sanctions.

Reports indicate that Venezuela central banking officials are in the process of running internal tests regarding the potential to incorporate Bitcoin and Ethereum into national banking operations. PDVSA represents the state-owned oil and natural gas company, whose operations include conducting international trade in Venezuelan oil.

As for the PDVSA, their requests towards the Venezuelan central bank to integrate cryptocurrency is likely far more pragmatic: a cooperative central bank means not having to communicate financial records to third party exchanges.

Maduro: Citizens Can Soon Use Cryptocurrencies as a "Method for Free National And International Payments"

Due to the hyperinflation of the bolivar, Venezuela's national currency, Venezuelans are no strangers to cryptocurrencies—and this was true before the country's developed its homegrown cryptocurrency—the Petro. It's not uncommon for citizens to use virtual assets such as bitcoin to protect their wealth or build their savings. However, to use these funds Venezuelans must often look to peer-to-peer exchanges that facilitate trades between buyers and sellers, such as localbitcoins, or even Telegram groups.

Maduro tried to minimize the effects of sanctions with the Petro— a state-issued cryptocurrency pegged 1:1 against barrels of Venezuelan oil—believing it would flow independently across borders like other blockchain protocols. However, the Petro's lack of success as a means of cross-border payment has led the country to explore other solutions. One of them is globally used, decentralized cryptocurrencies such as Bitcoin. In an October 10 press conference, Maduro stated that "within a short time" everyone in the country, including the public and private sectors, will be able to use cryptocurrencies as a method of "free national and international payments."

North Korea

New U.N. Report: North Korea Hacked \$2 Billion from Banks and Cryptocurrency Exchanges to Fund WMD Production

A new confidential UN report is said to reveal that the Democratic People's Republic of Korea (DPRK) has generated an estimated \$2 billion for its weapons of mass destruction (WMD) programs by hacking banks and cryptocurrency exchanges. UN experts said North Korea "used cyberspace to launch increasingly sophisticated attacks to steal funds from financial institutions and cryptocurrency exchanges to generate income." The report also said the Pyongyang regime used cyberspace to launder the stolen money.

According to Reuters, which claims to have seen the report, the U.N. experts said North Korea's attacks against cryptocurrency exchanges allowed it "to generate income in ways that are harder to trace and subject to less government oversight and regulation than the traditional banking sector." There were at least 35 cases of North Korean state actors executing cyberattacks on financial institutions and cryptocurrency exchanges. Crypto mining has also been used to earn foreign currency to finance the DPRK's WMD and ballistic missile programs.

U.N. Accuses North Korea of Laundering Money Through Blockchain Firm

An August 30 report by the United Nations Security Council's Sanctions Committee on North Korea accused the country of using a Hong Kong-based blockchain firm as a front to launder money. The Sanctions Committee conducted an investigation into North Korea's various strategies to evade sanctions through the use of cryptocurrencies and found that "Marine China platform Limited"—a Hong Kong based, blockchain-focused shipping and logistics firm—was created by North Korean state actors to use as a shell company for money laundering efforts. The report indicates that the shell company's start-up funds likely came from online extortion campaigns that required payment in cybercurrencies.

The UN report also alleges that North Korean intelligence services groom cyber agents from "a very young age" for future careers as hackers skilled at stealing cryptocurrency and targeting financial institutions.

To obfuscate its cryptocurrencies money laundering activities, North Korean attackers use a digital version of layering that creates thousands of transactions through one-time-use cryptocurrency wallets. According to the report, "stolen funds following one attack in 2018 were transferred through at least 5,000 separate transactions and further routed to multiple countries before eventual conversion to fiat currency, making it highly difficult to track the funds."

The UN report also alleges that North Korean intelligence services groom cyber agents from “a very young age” for future careers as hackers skilled at stealing cryptocurrency and targeting financial institutions. Regarding cryptocurrencies, the UN’s Sanctions Committee panel recommends that member states ensure:

- Regulation of cryptocurrency exchanges
- Financial institutions—including cryptocurrency exchanges—take independent steps to protect against North Korean cyberactivities
- Cryptocurrency exchanges share the same AML obligations as banks, such as monitoring suspicious transactions, providing governments with information on accounts after attacks, freezing assets of sanctioned entities under their control and blocking malicious transactions

Iran

Crypto Mining Now Legal but Trading—Illegal

Long gone are the days when crypto miners could use Iran’s highly subsidized energy to their advantage. After Iran’s power grid was hit by a massive, crypto mining induced power surge in June, the Iran Ministry of Energy declared that the power that once fed the country’s cryptocurrency miners would be cut off.

While it appeared Iran was planning to ban crypto mining in the country, Iran officially recognizing cryptocurrency mining as a legal industry on July 21. Officials are currently working on a new pricing arrangement for miners that had previously taken advantage of the country’s energy prices, which are among the world’s lowest. In addition to new energy pricing, the most recent draft of the bill calls for all miners to register with the government to receive an annual mining license. To receive a license, miners will be required to disclose their business practices, the value of their investments and assets, their employment status, the lease for their mining space, and the length of the mining project.

However, crypto holders in Iran may find it difficult to trade their bitcoin for fiat. In July, Nasser Hakimi, a technology official for Iran’s central bank, announced that trading Bitcoin in Iran is illegal. This was shortly before Iranian authorities confiscated one thousand mining rigs from Iranian mining farms. To read more on this, check out CipherTrace’s Q2 2019 Cryptocurrency AML Report.

Recent reporting by Chainbulletin claims that the government has the government has already confiscated about 80,000 devices over the last quarter.

Iran Crypto Developers Launch Platform to Bypass Sanctions for Flood Victim Aid

Volunteer cryptocurrency developers in Iran have created the blockchain platform IranRescueBit, on which people can make charitable donations to flood victims using a variety of cryptocurrencies, including: Bitcoin (BTC), Bitcoin Cash (BCH), Bitcoin SV, Ether (ETH) and Litecoin (LTC), Zcoin, Verg, and Tron. The government is reportedly not involved in this project.

By using cryptocurrencies, donors from anywhere in the world are able to circumvent US sanctions that have thus far prohibited international donations to the Iranian Red Crescent Society (IRCS)—a humanitarian NGO in Iran. According to the IRCS, US sanctions had been impeding relief efforts such as receiving foreign financial aid, preventing them from helping flood victims.

IranRescueBit executive director Hamed Salehi told news organization Al Jazeera that once the platform's campaign is finished, crypto donations will be converted to fiat using local exchanges. The fiat would then be sent to a local IRCS bank account.

According to their public transaction history, the organization has raised over \$3000 so far, with over half of the donations coming from Bitcoin users. A CipherTrace analysis of the bitcoin address (35wGf6Wk-JVdhGzRr3WPzedFybaV9uziocr) reveals that at one hop away most of the donations received are from personal wallets, with only one donation coming directly from an exchange. Of the 29 bitcoin transactions received, nine are from addresses CipherTrace has deemed high risk based on their transaction histories. A deeper look into these transactions reveals the source of the funds from these high-risk wallets all originate from one of the largest Chinese mining pools—Antpool. In April it was reported that Chinese miners were exploiting Iran's low energy prices for mining after a proposed mining ban in China. In July, Iran's Information and Communication Technology Minister Mohammad Javad Azari Jahromi told Islamic Republic News Agency that they "do not have any evidence of Chinese activities in Iran" but have heard about the issue.

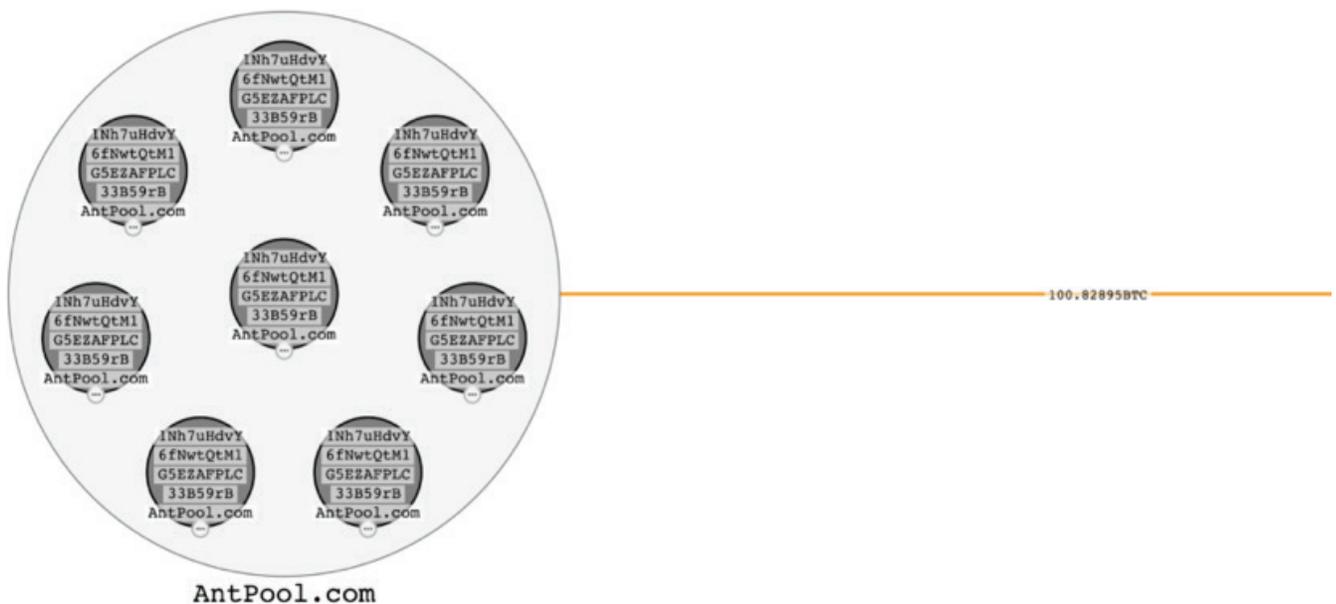


Figure 12

Appendix A

Privacy Coins Have Well-Developed Plans for Travel Rule Compliance

The Travel Rule requirements to transmit originator and beneficiary information with cryptocurrency transactions obviously defeats the purpose of privacy coins. Nonetheless, many of the top coin developers have already released statements on how they could comply.

Monero

According to a September 19 Bloomberg interview, developer teams behind Monero claim they can be in full compliance with the FATF Travel Rule. While it was never explained what compliance would look like for Monero, it was hinted that the “view keys” feature, which lets coin owners monitor transactions, could play a role.

However, this open source cryptocurrency uses an obfuscated public ledger, which means wallet addresses don't appear on the blockchain. Although anyone can broadcast or send transactions, outside observers cannot discern the source, amount or destination of transactions. Additionally, Monero has many privacy features such as always-on privacy; ring signatures that produce multiple signatures for any one given transaction to obscure the true sender; stealth addresses that hide the receiver; and ring confidential transactions that hide the amounts being sent. Unless changed, these characteristics could prevent Monero from demonstrating compliance in order to remain on exchanges.

Zcash

Although Zcash has the option of transacting in a “transparent” or “shielded” pool, both pools use protocols developed specifically to comply with the FATF Travel Rule through encrypted memos attached to transactions. Unlike Monero's enforced privacy features, Zcash allows for “selective disclosure”—i.e., private users can choose whether to comply with AML regulations or not. However, as UpBit's recent delisting has shown, some exchanges are not willing to accept the risks associated with any privacy coins, even if privacy is a choice and not a mandatory feature.

According to an April 2019 Zcash Regulatory and Compliance Brief, “The fact that a VASP supports Zcash or that a customer intends to trade Zcash does not impact the VASP's ability to carry out CDD checks... Zcash was designed to be compliant with the Travel Rule. The required originator and beneficiary information can be attached directly to a shielded transaction using the encrypted memo field. As the name implies, the contents of this field are encrypted when the transaction is added to the blockchain, thus preventing inappropriate or unauthorized disclosure of personal information.” Furthermore, the Zcash protocol was also designed to support the disclosure of shielded transaction information to third parties, if necessary.

DASH

Dash was created from a fork in the Bitcoin Protocol. Formerly known as Xcoin and Darkcoin, it was rebranded as Dash in 2015 after Darkcoin became known for popularity as a payment rail in dark marketplaces. Dash gives users the option to make either normal or “untraceable” transactions. Normal transactions can be sent through InstantSend, which bypasses mining and requires a consensus of masternodes to validate a transaction. This approach increases transaction speed. PrivateSend, on the other hand, makes transactions “untraceable” by mixing participating users’ unspent Dash before executing a transaction.

During the Cryptocurrency Compliance Conference in San Francisco in November 2019, Ryan Taylor, chief executive officer at DASH Core Group Inc., explained, “Dash is identical to Bitcoin and is 100% capable of meeting the requirements [of FATF’s Travel Rule].” While this is true for the coin’s InstantSend transactions, using the privacy enhancing PrivateSend feature may make it tougher for DASH transactions to be processed by exchanges. However, ultimately PrivateSend transactions are no different than bitcoin transactions using privacy enhanced overlays such as coinjoin or zerolink. Exchanges may take the same approach to Dash’s opt-in privacy features that they do with the privacy enhanced features available to bitcoin when attempting to mitigate the risk from bad actors.

While it may seem natural for privacy coins to be the go-to for criminal activity, CipherTrace research has found that despite privacy coins like DASH, Zcash and Monero being offered as alternatives to bitcoin on darknet marketplace, bitcoin is still king. In other words, the hard data suggests the perceived dangers of these coins outweighs the reality. To counter this perception, Taylor added “we tend to treat cryptocurrencies very binary... they’re either privacy coins or they’re not. What does that actually mean? In the case of Dash, we were the first to implement a feature that was proposed by Bitcoin at the time called CoinJoin. It’s a wallet level technique that allows any transparent blockchain to enhance the user privacy. Since Dash did it in 2014, Bitcoin did it in 2015. Then they added off-chain transactions with Lightning. Does that now make bitcoin a privacy coin? It should if Dash is one.

“I think we need to go beyond this binary treatment, look at the actual technology, how can we adapt to it, are there ways to deal with it. The answer to Dash is... if you can do it with bitcoin you can do it with Dash. It’s a fully transparent blockchain. Every single transaction reveals the inputs, the outputs, the amounts; it’s all there.”

Decred

According to an August 28 Decred blog post, the company has developed new privacy features for its DCR token, which implements a variant of CoinShuffle++ in its wallet. This method is prunable, meaning the blockchain can drop historical transactions from their full nodes.

Despite claiming community voting is a key feature in Decred's governance model, the new privacy feature was not put up to the community but instead secretly funded by Decred Project Lead Jake Yocom-Piatt. On the surface, funding privacy features may appear to conflict with governance espoused by the project, investors close to the project were not surprised and felt it privacy was a feature they expected to be added to Decred.

It is still unclear how this decision will affect DCR in the future.

The Privacy Coin Compliance Debate

Two fundamental questions exist in the privacy coin compliance debate: can exchanges trading privacy coins comply with data travel, and can exchanges demonstrate the privacy coins are not from an illegal source?

Although FATF and FinCEN have both taken stances on privacy coins, the FATF's recent (June) guidance is less explicit about privacy coins than FinCEN's. According to the FATF, features that increase anonymity and obfuscation of transaction flows make those transactions "more susceptible to abuse by criminals, money launderers, terrorist financiers, and other illicit actors." These situations should be deemed high-risk for an exchange, and therefore require enhanced monitoring that extends "beyond the immediate transaction between the VASP or its customer or counterparty." A broad interpretation of this statement suggests the FATF is not advocating all exchanges should delist privacy coins, but is recommending that exchanges offering privacy coins should have the capability to monitor these transactions beyond existing due diligence. However, the level of scrutiny needs to be based on a specific exchange's institutional risk assessment and individual customer risk profiles.

	Bitcoin	Monero	Zcash	DASH	Decred
Privacy Technology	Open blockchain (Project SnowBall)	RingCT	Zk-SNARKs	PrivateSend	CoinShuffle++
Chain Origin	Bitcoin	Bytecoin	Zerocoin	Bitcoin	Bitcoin
Market Cap	\$147,899,181,193	\$996,250,178	\$279,451,992	\$623,301,626	\$153,263,120
Volume	\$16,741,992,391	\$84,770,451	\$132,467,560	\$212,239,093	\$7,258,444
Compliance Strategy	Open blockchain	"view keys" feature	Encrypted memos	Coinfirm	None

Figure 13

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

