

Cryptocurrency Crime and Anti-Money Laundering Report, Spring 2020

CipherTrace
Cryptocurrency Intelligence
June 2020



About CipherTrace

CipherTrace enables the blockchain economy by protecting cryptocurrency companies and financial institutions from security and compliance risks. Years of research have gone into developing the world's most complete and accurate cryptocurrency intelligence and forensics, covering more than 800 currencies. This visibility into the blockchain and virtual asset businesses helps protect banks and exchanges from cryptocurrency laundering risks, while protecting user privacy. CipherTrace also works with government agencies to bridge the gaps between regulation and the world of cryptocurrencies and blockchain.

CipherTrace is a founding member of TRISA, the leading open source industry standard to meet the Travel Rule requirement for secure information sharing while protecting cryptocurrency user privacy. TRISA enables cryptocurrency companies to comply with the Financial Action Task Force regulations that will shape the world of cryptocurrencies, and bring them to institutional prominence as investment and cross-border payment technologies. Learn about the open source Travel Rule Information Sharing Architecture at trisa.io.

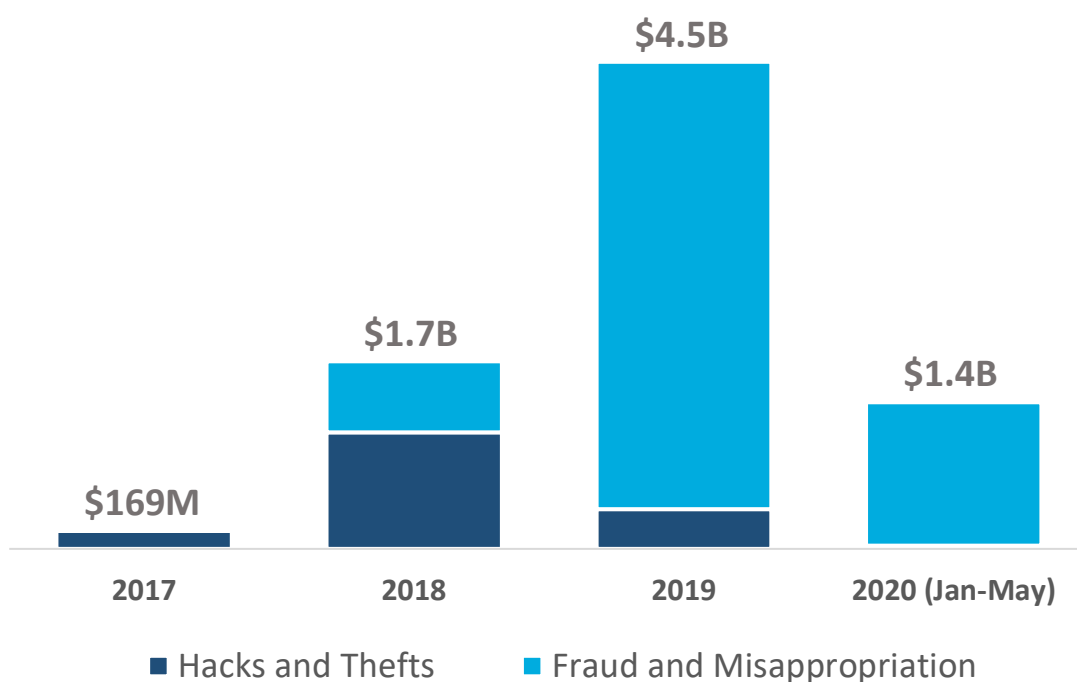
| | |
|--|-----------|
| Executive Summary | 5 |
| Major Trends and Developments | 8 |
| Proportion of Directly Illicit Funds Received by Exchanges Halves | 8 |
| LocalBitcoins Leads as Go-To for Direct Criminal Funds for Third Year in A Row..... | 11 |
| Cross-Border Exchanges Comprise Three Quarters of Exchange-to-Exchange Transfers..... | 13 |
| US Bitcoin ATM Users Increasingly Prefer High-Risk Exchanges | 14 |
| Major 2020 Enforcement Actions..... | 18 |
| OCC Hits New York Based Bank with First-Ever Enforcement Action for Lack of Crypto AML Compliance | 18 |
| Crypto Ponzi Victims File Class Action Lawsuit Against Wells Fargo..... | 19 |
| “Helix” Tumbler Bust Reveals \$300 Million Bitcoin Laundering Scheme Linked to Notorious Dark Market | 19 |
| SEC Calls Out Meta 1 Coin as a Security Fraud..... | 21 |
| Child Exploitation Masterminds Arrested in Netherlands and South Korea | 21 |
| Thefts, Scams, and Fraud | 22 |
| COVID-19 Scams Spread | 22 |
| Massive Wotoken Ponzi Scheme Defrauds Investors of Over \$1B Worth of Crypto | 27 |
| Five of the six on trial plead guilty to defrauding investors. | 27 |
| The anatomy of a Ponzi Scheme | 28 |
| Early Warning Signs | 28 |
| Cryptocurrency Exchange FCoin Insolvent After \$130M Bitcoin Shortfall | 29 |
| Digital Wallet That Promised High Yields on EOS Deposits Exits with \$52 Million..... | 30 |
| Hacker on Compromises DeFi Protocol to Steal \$25 Million in Crypto | 30 |
| CFTC Charges Multiple Firms for \$15 Million Crypto and Binary Options Scam..... | 30 |
| Chinese Cosmic Cryptocurrency Ponzi Absorbs \$11 Million in Three Weeks | 31 |
| Travelex Reportedly Paid \$2.3 Million Ransom to Restore Operations..... | 31 |
| IOTA Wallet Hacker Steals \$1.4 Million USD of MIOTA..... | 31 |
| Bisq Exploit Results in \$250k Theft of Bitcoin and Monero from Platform..... | 31 |
| XRP Giveaway Scam Steals \$205k USD of XRP..... | 32 |
| Crex24 Exchange Accused of Hiding Hack from Customers..... | 32 |
| Global Regulatory Environment Rapidly Matures | 33 |
| Travel Rule Industry Cooperation and Open Standards Produce Viable Options | 33 |
| FinCEN Reminds VASPs Operating in US That Crypto Travel Rule Is Already Being Enforced..... | 33 |
| Compliance and confidentiality conundrum | 34 |
| Presenting Travel Rule Information Sharing Architecture to FATF in Paris | 34 |
| Built on proven trust models and security technologies..... | 35 |

| | |
|---|------------------|
| Progress in fast-tracking a Travel Rule compliance standard..... | 36 |
| AMLD5 Is Here: EU Crypto Businesses Faced with Tough New Regulation..... | 36 |
| UK—FCA Becomes AML and CTF Supervisor for UK Cryptoasset Activities | 37 |
| US—On Crypto AML/CTF, FATF Finds U.S. “Largely Compliant” | 37 |
| Canada—Toronto Stock Exchange Trades 3iQ Corp Bitcoin Fund | 38 |
| Japan—Revised Crypto Laws in Japan Begin Enforced Compliance..... | 38 |
| IOSCO—Global Stablecoins May Be Subject to Securities Regulation | 38 |
| India—Crypto Ban Overruled..... | 38 |
| <i>Sanctioned Countries.....</i> | <i>39</i> |
| Venezuela | 39 |
| U.S. Accuses Venezuelan President of Using Crypto to Conceal Illicit Drug-Running..... | 39 |
| North Korea..... | 39 |
| Chinese Nationals Added to OFAC SDN List and Charged by DOJ for Laundering \$100 Million in Cryptocurrency Stolen by North Korea | 39 |

Executive Summary

In the first five months of 2020, crypto thefts, hacks, and frauds totaled \$1.36 billion, suggesting 2020 could see the second-highest value in crypto crimes ever recorded. In a trend that continues from last year, fraud and misappropriation still make up most of the year's stolen crypto compared to hacks and thefts. Of the \$1.36 billion stolen, fraud and misappropriation account for 98% of the total value—nearly \$1.3 billion.

Blockchain Fraud Continues to Vastly Exceed Hacks and Thefts in 2020



Source: CipherTrace Cryptocurrency Intelligence

Figure 1.

On the regulatory front, CipherTrace data revealed 74% of the bitcoin that moved in exchange-to-exchange transactions was cross-border. The abundance of cross-border transactions highlights the need for exchanges to adopt appropriate cross-border controls to ensure AML and CTF compliance. The need for compliance is especially profound in light of impending Travel Rule enforcement and the recent statement by FinCEN Director Kenneth Blanco reminding the crypto community that Travel Rule compliance is already the expectation in the United States.

Highlights of key findings are as follows:

Thefts, Hacks, and Fraud

- In the first five months of 2020, crypto thefts, hacks, and frauds totaled \$1.36 billion, indicating 2020 could see the greatest total amount stolen in crypto crimes outside 2019's \$4.5 billion.
- Coronavirus-inspired fraud is generally executed by luring victims off legitimate platforms into chat rooms where payment in bitcoin can be requested.
- COVID-19-related phishing sites were found to be the most popular COVID-19-related products sold on the dark web; dark web PPE sales have been mostly unsuccessful.

Exchanges and Darknet Marketplaces

- The global average of direct criminal funds received by exchanges dropped 47% in 2019.
- This trend marks a three-year low for cryptocurrency exchanges around the world, with only 0.17% of funds received by exchanges in 2019 coming directly from criminal sources.
- Based on CipherTrace's examination of one prominent darknet marketplace, while 9.8% of the dark market's one-hop interactions went directly to exchanges, 31% of its two-hop interactions went to exchanges—more than tripling the risk exposure to exchanges.
- Finnish exchanges ranked #1 for highest percentage of criminal BTC received for the third year in a row, with 12.01% of all BTC funds received coming directly from criminal sources. LocalBitcoins, one of the largest peer-to-peer marketplaces, received over 99% of these criminal funds.

Cross-Border Transactions

- 74% of the bitcoin moved in exchange-to-exchange transactions were cross-border.
- 88% of funds sent by US Bitcoin ATMs to exchanges in 2019 were sent offshore.

Bitcoin ATMs

- On average, US BATM users sent more funds to high-risk exchanges than low-risk exchanges in 2019.
- The percentage of funds sent to high-risk exchanges from US BATMs has doubled every year since 2017.

Total Value Stolen from Crypto Crimes on Track to Be Second-Highest on Record

In the first five months of 2020, crypto thefts, hacks, and frauds totaled \$1.36 billion. The largest contributor to this high sum is a billion-dollar Ponzi scheme by Wotoken in China. The scam promised investors unrealistic returns using a non-existent algorithmic trading

software. Ultimately, Wotoken operators (one with ties to the infamous PlusToken Ponzi scheme) stole an estimated \$1 billion in crypto from over 715,000 victims.

Coronavirus scams also contributed to the net earnings of crypto crime. While governments funnel resources into mitigating the impact of the pandemic, criminals are taking advantage of the lack of oversight, resulting from the need for urgent action. COVID-19 fraud has taken the form of impersonations of legitimate entities (i.e. The Red Cross) to extract personal information and/or payment in cryptocurrencies, applications that claim to support victims but actually spy on users, and the sale of PPE-- supposed treatments, testing kits, and phishing kits. Though the majority of COVID-19-related products advertised on darknet markets did not net many sales, phishing kits were relatively successful.

Crypto AML Measures Prove Effective, But Criminals Are Getting Savvier

Though the total value collected by criminals from crypto crimes is among the highest recorded, the global average of criminal funds sent directly to exchanges dropped 47% in 2019. This suggests that many criminals are finding it harder to offload their illicit funds directly into cryptocurrency exchanges, indicating effective implementation of AML measures around the world. It's worth noting however, that criminals seem to be getting better at obfuscating the origins of their stolen funds prior to cashing out on exchanges. CipherTrace's examination of one prominent darknet marketplace revealed that risk exposure to exchanges tripled for secondary transactions (two-hops out) compared to primary transactions (one-hop out).

Regulatory Arbitrage Precedes Travel Rule Sunrise

Impending Travel Rule enforcement hangs over the cryptocurrency economy as VASPs seek to adopt solutions prior to the June 2020 Financial Action Task Force (FATF) meeting. CipherTrace found that 74% of the bitcoin moved in exchange-to-exchange transactions was sent cross-border, underlining the importance of global AML/CTF standards, such as those set forth by the FATF.

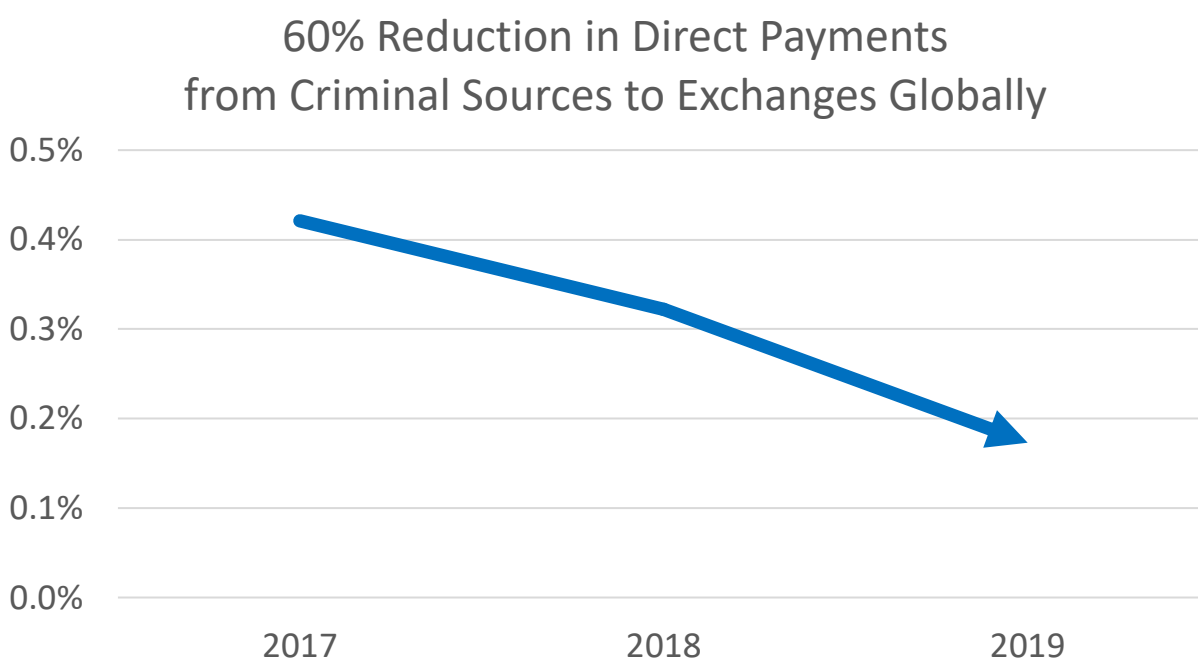
Bitcoin ATMs (risky business and growing)

CipherTrace research revealed US bitcoin ATM users sent more funds to high-risk exchanges, which are more likely to be used for money laundering, than low-risk exchanges in 2019. This finding, combined with last year's enforcement action taken against Kunal Kalra for his BATM money laundering scheme, indicates bitcoin ATMs are likely to be the next major regulatory target.

Major Trends and Developments

Proportion of Directly Illicit Funds Received by Exchanges Halves

The global average of direct criminal funds received by exchanges dropped 60% from 2017 to 2019, most of which occurred in the last year with a 47% drop from 2018 to 2019. This trend marks a three-year low for cryptocurrency exchanges around the world, with an average of only 0.17% of funds received by exchanges in 2019 coming directly from criminal sources. As more crypto AML regulations are implemented around the world (including AMLD5 in Europe), many criminals are finding it harder to offload their illicit funds directly to cryptocurrency exchanges—the most common crypto-to-fiat offramp.



Source: CipherTrace Cryptocurrency Intelligence

Figure 2.

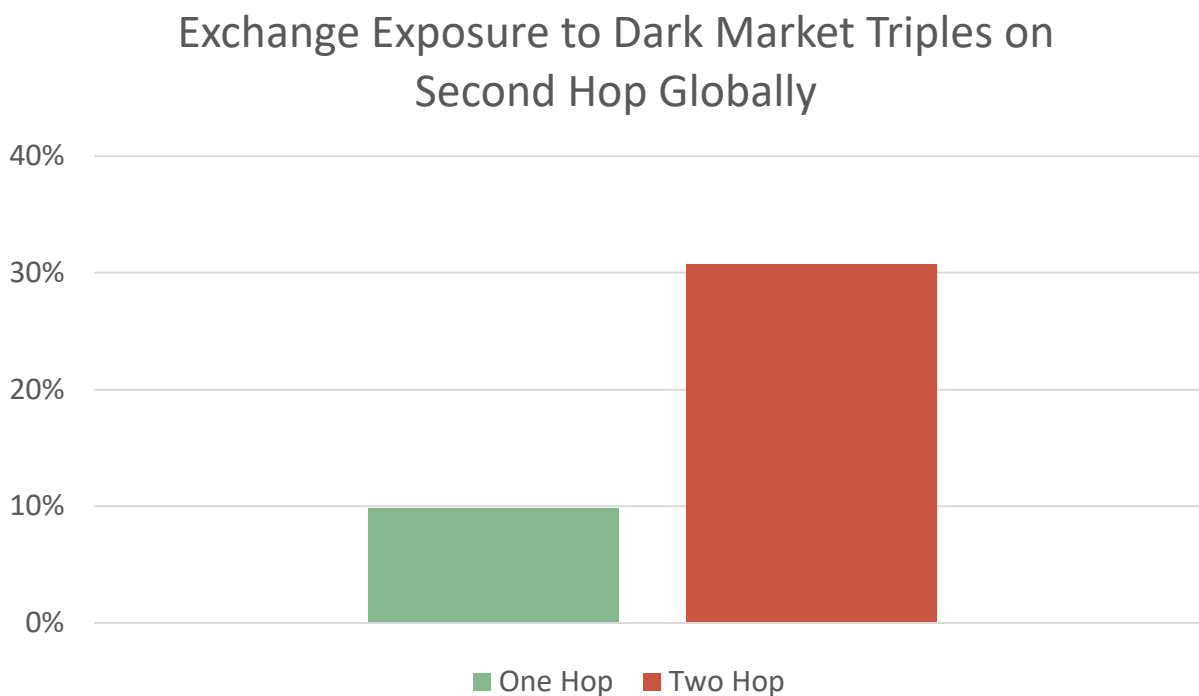
Global Average of Direct Criminal Funds Received by Exchanges Dropped 47% in 2019

However, a drop in the global average does not necessarily mean exchanges are actually receiving fewer criminal funds. As exchanges begin to develop stronger KYC and AML protocols, it becomes harder for criminals to directly deposit tainted funds into an

exchange. Instead, savvy criminals must layer funds through multiple transactions and even private wallets before cashing out via regulated fiat off-ramps such as exchanges. This means exchanges must remain diligent to not only their direct (one-hop) exposure risk to criminal funds but should be looking at their multi-hop risk to best understand their risk exposure.

For example, using CipherTrace Monitor to examine the weekly interactions for one prominent darknet marketplace, CipherTrace researchers were able to see that while only 9.8% of the dark market's one-hop interactions were directly with exchanges, 30.7% of its two-hop interactions were with exchanges—more than tripling the risk to exchanges. This is demonstrated in figure 3.

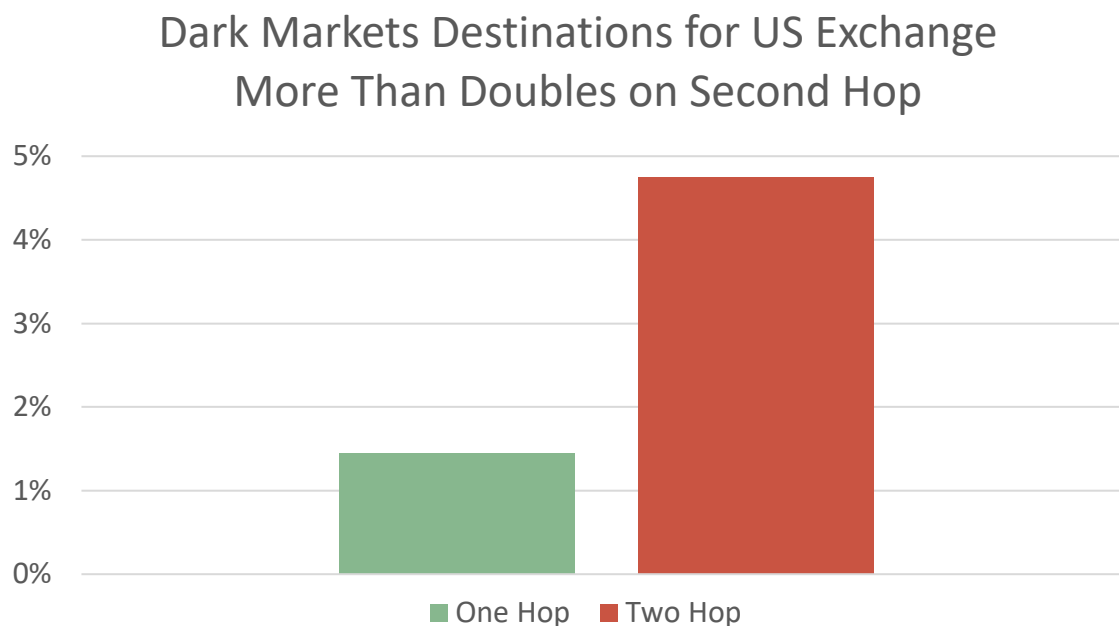
While only 9.8% of the dark market's one-hop interactions went directly to exchanges, 30.7% of its two-hop interactions went to exchanges—more than tripling the risk exposure to exchanges.



Source: CipherTrace Cryptocurrency Intelligence

Figure 3.

When looking at a prominent US-based exchange, with strong KYC, CipherTrace Monitor was able to demonstrate that the exchange's risk exposure to dark markets also more than tripled between one and two hop interactions, as demonstrated in figure 4 below.



Source: CipherTrace Cryptocurrency Intelligence

Figure 4.

In most AML regulatory environments, money transmitters dealing in convertible virtual currency—such as cryptocurrency exchanges—are considered non-bank financial institutions (NBFIs). FATF identifies these digital asset entities as Virtual Asset Service Providers (VASPs) and in the US Money Service Businesses (MSBs). Although the complete definition of VASP extends beyond being a virtual asset money transmitter, the conversion between virtual assets and fiat makes these digital asset entities of particular interest to banks.

CipherTrace research presented in the 2019 Q4 CAML Report revealed that banking and virtual currency is increasingly intertwined as 8 out of 10 US retail banks harbor illicit crypto MSBs, and a top 10 US retail bank will typically process upwards of \$2 billion in crypto-related transactions annually that are not being detected. It is important for banks to both identify any VASP counterparties in customer transactions and any VASPs attempting to hide the fact that they are digital asset customers. Failure to identify these digital asset entities can lead to operational, legal, financial, reputational, and counterparty risks for the bank.


However, virtual asset entities could also prove to be lucrative customers to many financial institutions. The proper tools—such as CipherTrace Aramda— help ensure that banks have insight into all digital asset entities which may be operating in their payment


networks or transacting with their customers. These insights can allow banks to safely grow their potential customer base by understanding operational and transactional risk associated with cryptocurrencies and VASPs. Insight into a VASP's two-hop interactions can produce more robust risk scores and give financial institutions a more authentic picture of the realistic risk associated with a VASP's customer base.

LocalBitcoins Leads as Go-To for Direct Criminal Funds for Third Year in A Row

CipherTrace examined the inflow of funds to exchanges globally to determine the amount each country's exchanges received directly from criminal sources. A summary of the results has been graphed in figure 6.

For the third year in a row, Finnish exchanges ranked #1 in highest percentage of criminal BTC received, with 12.01% of all BTC funds received coming directly from criminal sources. Finland-based LocalBitcoins, one of the largest peer-to-peer marketplaces, received over 99% of these criminal funds. In August 2019, Kunal Kalra, aka Shecklemaayne, pled guilty to US federal criminal charges for owning and operating an unlicensed MSB, exchanging nearly \$25 million through his LocalBitcoins account and Bitcoin ATM.

 LocalBitcoins.com Buy bitcoins Sell bitcoins Post a trade Help ▾

shecklemaayne 

Phone 347-518-8539

Information on shecklemaayne

| | |
|----------------------------|--|
| Trade volume | 500+ BTC |
| Number of confirmed trades | 100+ ...with 191 different partners |
| Feedback score | 100 % |
| First purchase | <u>4 years, 12 months ago</u> |
| Account created | <u>6 years, 1 month ago</u> |

Unregistered US MSB Advertising on Finnish P2P Exchange
Figure 5.

Russian exchanges were the #2 destination for criminal funds in 2019 with 5.23% of all funds received coming directly from criminal sources... UK exchanges ranked #3.

CipherTrace also found that Russian exchanges were the #2 destination for criminal funds in 2019 with 5.23% of all funds received by Russian exchanges coming directly from criminal sources such as dark markets, ransomware, hacks, and other illicit activity. In examining Russian exchange interactions further, CipherTrace researchers discovered that 86.8% of the criminal BTC received directly by Russian exchanges in 2019 came from Hydra Market—a Russian dark market featured in CipherTrace’s 2019 Q4 CAML Report.

UK exchanges ranked #3 in highest percentage of BTC received directly from criminal sources in 2019. Interestingly, when reviewing these interactions, CipherTrace discovered that 31.2% of the criminal BTC also came directly from Hydra Market. This number is down from 2018 when 57.6% of the criminal funds received directly by UK exchanges came from Hydra. The pervasive presence of Russian dark markets on UK exchanges exemplifies the cross-border nature of crypto as criminals sell in Commonwealth of Independent State (CIS) countries—where Hydra operates—and cash out in the UK as either a means of jurisdictional arbitrage or because that’s where they are based.

In the past, lack of regulatory clarity in the United Kingdom has made the country’s exchanges a hotspot for criminals to quickly and easily cash out. In an attempt to combat criminal use of virtual assets, Britain’s Financial Conduct Authority (FCA) announced in January 2020 that they will now monitor AML/CTF for crypto asset activity.

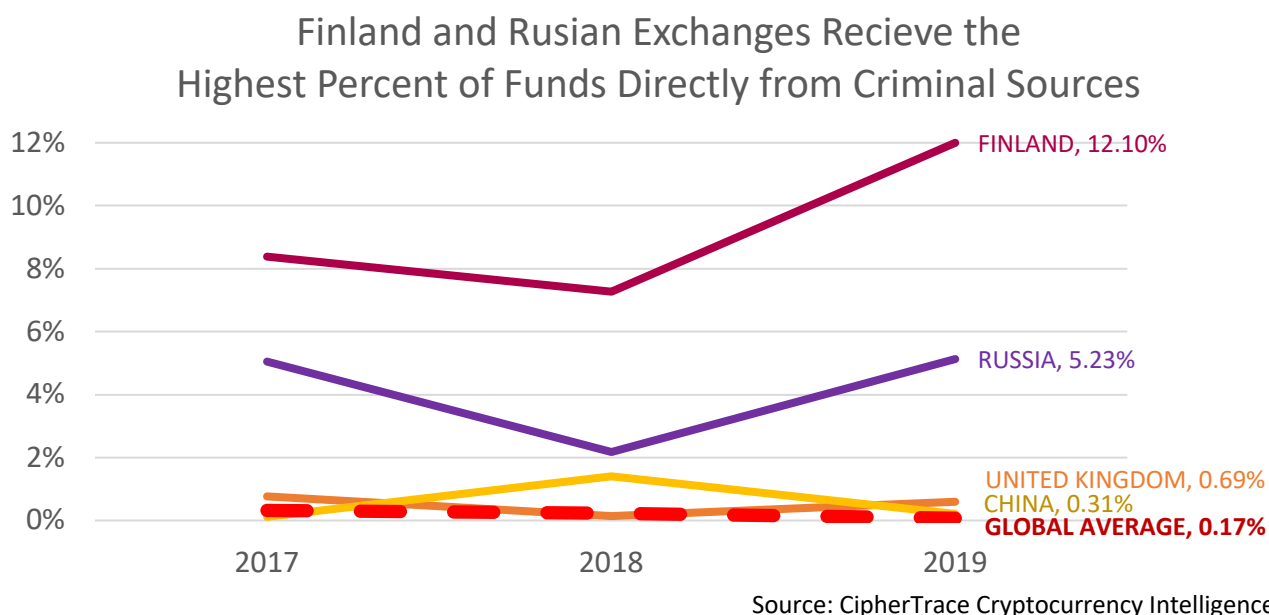
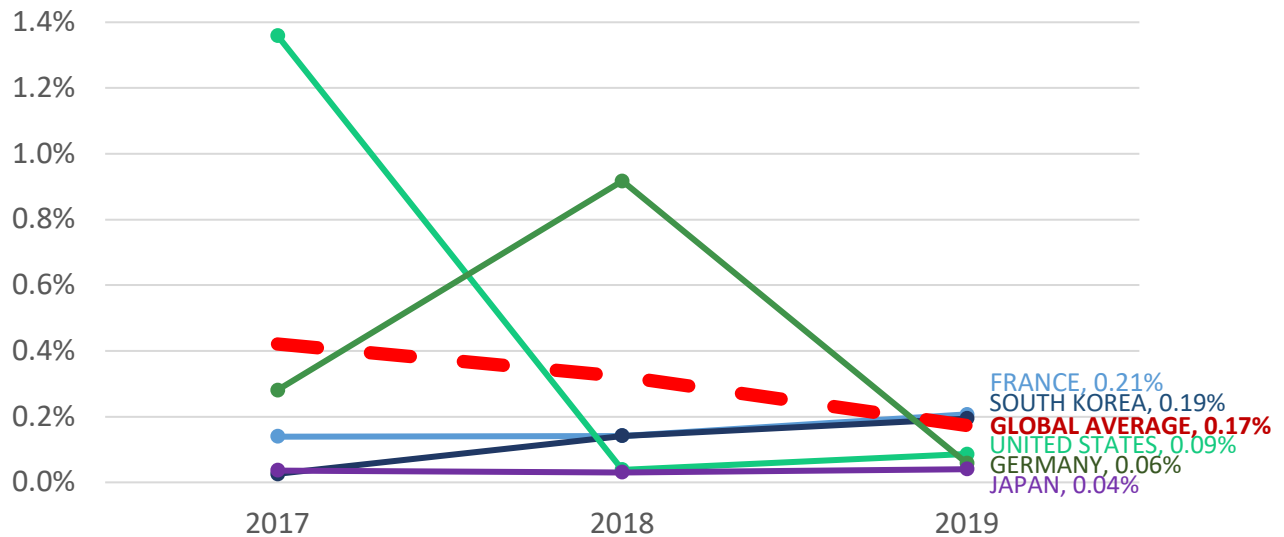


Figure 6.

Direct Payments from Criminal Sources to Exchanges Drops to Less than 0.1% in Germany, Japan and US



Source: CipherTrace Cryptocurrency Intelligence

Figure 7.

Cross-Border Exchanges Comprise Three Quarters of Exchange-to-Exchange Transfers

On average, 74% of the bitcoin moved in Exchange-to-Exchange transactions was moved cross-border in 2019. This highlights the importance of global AML/CTF standards, such as those set forth by the FATF. Criminals are known to engage in jurisdictional arbitrage, where they take advantage of the discrepancies between regions with stronger and weaker crypto AML regulations.

74% of the bitcoin moved in Exchange-to-Exchange transactions was moved cross-border

As enforced compliance with the FATF Cryptocurrency Travel Rule begins in June 2020, not only will VASPs need to know when they are sending to another VASP, but the VASP on the other end will need to have the infrastructure to securely accept the incoming personally identifiable information (PII) that is shared. The sunrise problem exchanges will face as different countries begin to implement the regulations in different ways, at different times, has long been a topic of deliberation for the Travel Rule Information Sharing Architecture (TRISA) working group and this new statistic underscores the prevalence of the issue. Exchanges in jurisdictions around the world must work together to ensure they

are part of the discussion about what compliance looks like. For more on TRISA, or to join the working group, visit www.trisa.io.

Further increasing the struggles VASPs now face in determining when and how to send PII, CipherTrace has found that over half of the BTC sent from exchanges is sent to private wallets. In 2019, 61% of the total value of BTC transactions on exchanges globally were sent to private wallets. If a majority of the BTC being sent out of an exchange is to non-VASP entities, VASPs must ensure they don't violate user privacy by accidentally sharing a client's PII with a non-obliged entity. Doing so could have severe legal, regulatory and reputational risks for a VASP and be antithetical to cryptocurrency as a whole.



61 % of the total value of BTC transactions on exchanges globally were sent to private wallets

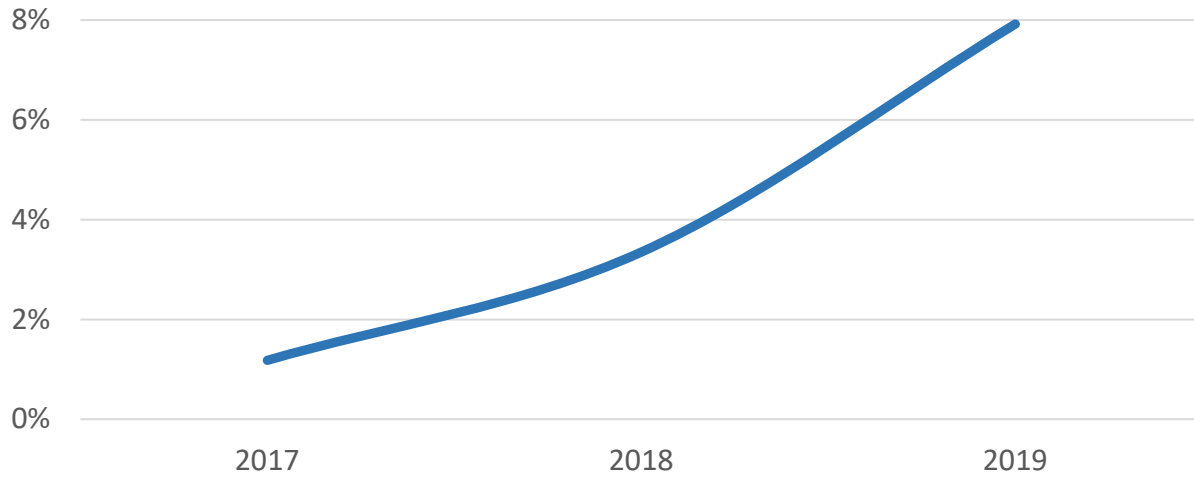
US Bitcoin ATM Users Increasingly Prefer High-Risk Exchanges

CipherTrace researchers conducted a review of all US-based bitcoin ATM (BATM) interactions and found that, on average, US BATM users sent more funds to high-risk exchanges than low-risk exchanges in 2019. The percentage of funds sent to high-risk exchanges from US BATMs has seen exponential growth, doubling every year since 2017. CipherTrace classifies high-risk exchanges as nefarious exchanges known for facilitating criminal activities and money laundering. Although high-risk exchanges are not inherently indicative of criminal activity as many also have a number of legitimate exchange users, the flow of criminal funds through such exchanges makes transacting with a high-risk exchange a red flag.



US BATMs Sent More Funds to High-Risk Exchanges Than Regular Exchanges in 2019

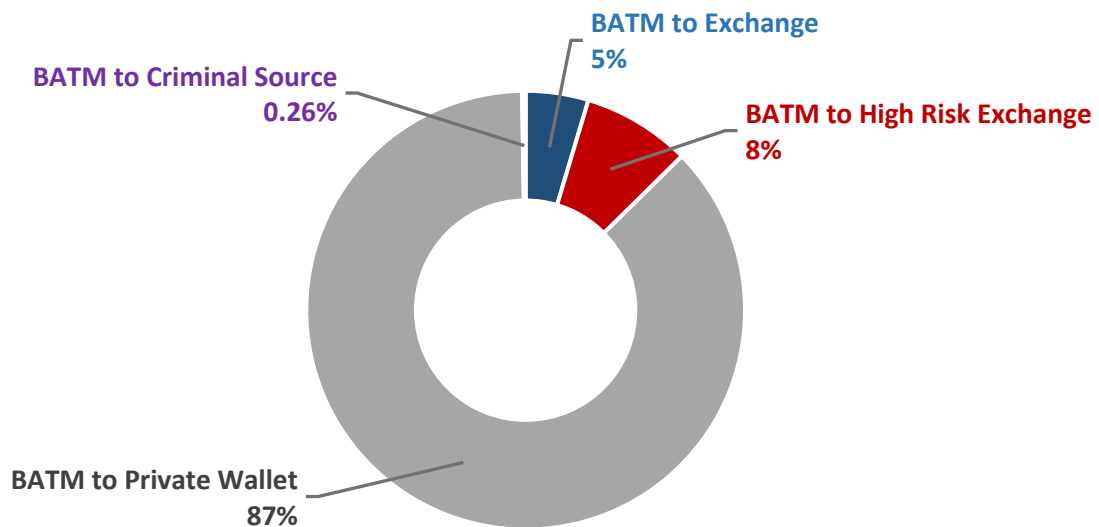
Funds Sent to High-risk Exchanges from US Bitcoin ATMs Grows Exponentially



Source: CipherTrace Cryptocurrency Intelligence

Figure 8.

8% of all US Bitcoin ATM Payments are Sent Directly to High Risk Exchanges

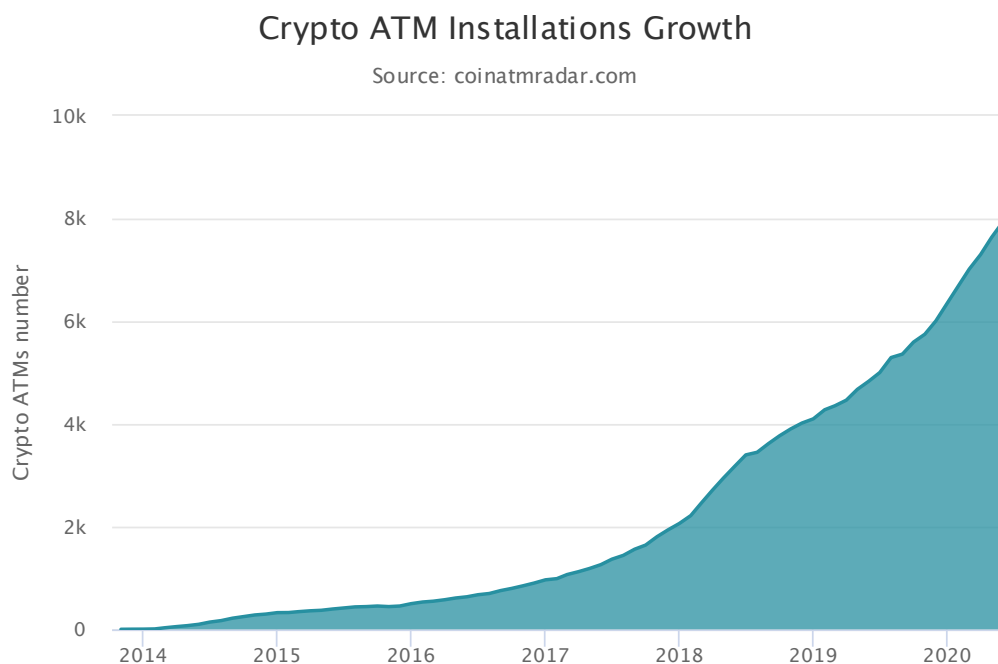


Source: CipherTrace Cryptocurrency Intelligence

Figure 9.

Only 12% of Funds US BATMs Sent to Exchanges in 2019 Were Sent to US-Based Exchange

While there is no way to know how much of the funds sent to private wallets were cross-border transfers, only 12% of funds US BATMs sent to exchanges in 2019 were sent to US-based exchange—meaning 88% of the BTC sent to exchanges was sent cross-border. This is higher than the global average for cross-border exchanges-to-exchange transactions, further indicating support for the high cross-border convention of VASP-to-VASP transfers.



Bitcoin ATMs see exponential growth over the past three years.

Figure 10.

More than half of the top 500 VASPs employ weak or porous KYC

Criminals are also working to undermine “know your customer” processes in the remote environment. Virtual currency businesses should remain vigilant against attacks targeting their onboarding and authentication processes
-FinCEN Director Kenneth Blanco

On May 13, in a Consensus: Distributed keynote presentation, FinCEN Director Kenneth Blanco explained that criminals are actively undercutting customer due diligence at crypto exchanges, warning that “criminals are also working to undermine ‘know your customer’ processes in the remote environment. Virtual currency businesses should remain vigilant against attacks targeting their onboarding and authentication processes.”

In reviewing the KYC procedures at the top 500 VASPs, CipherTrace has found that 57% of these VASPs still have weak or porous KYC processes. To gather this data, CipherTrace analyzed the different KYC tiers and what a customer is permitted in return for providing the information. CipherTrace researchers tested all the exchanges using a standardized criterion and rated them as Weak, Porous, or Good based on how easy it would be to launder money after opening an account. Weak KYC processes not only leave the VASP at risk for money laundering and terrorism financing, but the crypto economy as a whole, as well, as exchanges are the on and off ramps that bridge the crypto and fiat worlds.

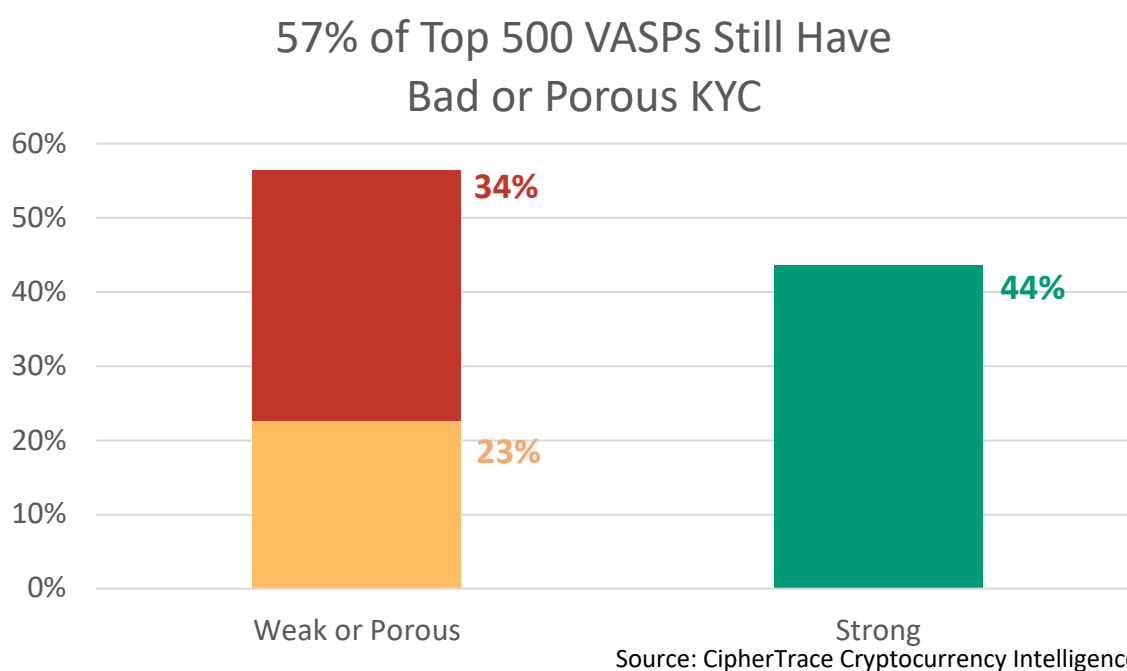


Figure 11.

- **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 but may allow withdrawals of up to .05 BTC daily with no KYC.
- **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.

Major 2020 Enforcement Actions

OCC Hits New York Based Bank with First-Ever Enforcement Action for Lack of Crypto AML Compliance

A recent cease and desist order issued by the Office of the Comptroller of the Currency (OCC) constituted the first-ever enforcement action against a U.S.-based bank. The OCC alleged that for more than two years M.Y. Safra Bank (MYSB), which is headquartered in New York City, failed to fully vet its cryptocurrency customers and transactions in high-risk jurisdictions.

The order was wholly focused on deficient anti-money laundering (AML) practices for compliance and monitoring of the bank's Digital Asset Customers (DACs). The lack of AML controls cited include opening accounts for Digital Asset Customers without sufficient customer due diligence (CDD) and a lack of adequate monitoring and investigating of suspicious transactions linked to these customers. The entities included cryptocurrency exchanges, bitcoin ATM operators, ICOs, incubators, and virtual OTCs as well as other crypto-related businesses.

According to the order, these deficient policies and procedures prevented MYSB from effectively identifying and investigating suspicious activity linked to crypto-related accounts. This lack of visibility into risky transactions also meant the bank failed to send suspicious activity reports (SARs) to Financial Crimes Enforcement Network (FinCEN).

Under the enforcement action, MYSB must now implement a number of measures to update its AML and Bank Secrecy Act (BSA) compliance programs. While no monetary penalties were assessed in this first-ever crypto-related enforcement action against a bank, it sends a strong message to the financial service industry. MYSB will face increased business costs and other burdens related to ensuring their compliance programs adequately address all corrective actions mandated by the enforcement action.

If the action taken against MYSB is any indication, bank regulators such as the OCC, Federal Reserve Bank, and the FDIC have already begun to scrutinize banks' cryptocurrency exposure during examinations. It also demonstrates that these regulators expect banks to be able to identify and properly risk-rate consumer and commercial customers who buy, sell, exchange or administer cryptocurrency.

Read more details on the blog: <https://ciphertrace.com/occ-hits-new-york-based-bank-with-first-ever-enforcement-action-for-lack-of-crypto-aml-compliance/>

Crypto Ponzi Victims File Class Action Lawsuit Against Wells Fargo

In a complaint filed in March 2022, the SEC sought penalties and other relief against an Ohio man, Michael Ackerman, for allegedly de-frauding investors of over \$35 million in a cryptocurrency trading scheme—Q3 Trading—along with two unnamed founding partners. The SEC has labeled the project as an “ongoing” securities fraud, alleging that the three falsified screenshots of their trading account to create the false impression that it held as much as \$310 million in assets when it actually contained no more than \$6 million at any given time. Investors’ funds were transferred directly into the fraudsters’ personal bank accounts where the money was spent lavishly on luxury properties and vehicles, among other things.

A class-action lawsuit revealed that one of Ackerman’s partners, James Seijas, promoted himself as an investor working on behalf of Wells Fargo Advisors. The suit accused Wells Fargo of failing to inquire into Seijas’s activities. The plaintiffs claimed that Wells Fargo failed to make the appropriate inquiries into Seijas as required by the company’s policy mandating that employees regularly report the work they do outside the scope of their employment with Wells Fargo. The lawsuit emphasized that because Seijas promoted himself as an investor working on behalf of Wells Fargo, “the acts and omissions described herein were committed in his capacity as an agent for Wells Fargo Advisors.” The lawsuit also named Wells Fargo Advisors in counts of unjust enrichment, negligence and fraud.

“Helix” Tumbler Bust Reveals \$300 Million Bitcoin Laundering Scheme Linked to Notorious Dark Market

In one of the most significant takedowns of a cryptocurrency-anonymizing service, Federal law enforcement authorities arrested Larry Dean Harmon of Akron, Ohio, for money laundering. Harmon’s Helix “tumbling” operation moved approximately \$300 million in bitcoin. The Department of Justice alleged that Helix had partnered with now-defunct underground marketplace AlphaBay, which was known for drug dealing and other illegal activities until it was shut down in 2017 by law enforcement.

According to the indictment, Helix made it possible for customers to send bitcoin in a manner that was designed to conceal the transaction and the owner of the bitcoin. Think of a tumbler or “mixer” as being analogous to a blender into which you put various types of fruit to make a smoothie. Once the blades spin it is virtually impossible to distinguish the banana from the strawberry. Likewise, once the anonymizing service mixes clean crypto with cryptocurrency that was stolen or used for criminal activities such as selling drugs, it becomes very difficult to trace the bad funds back to the source. “The brazenness with which Helix operated should be the most appalling aspect of this operation to everyday citizens,” said Don Fort, chief of the IRS Criminal Investigation division. “There are bad actors and then there are criminals who facilitate hundreds of other crimes. The sole purpose of Harmon’s operation was to conceal criminal transactions from law

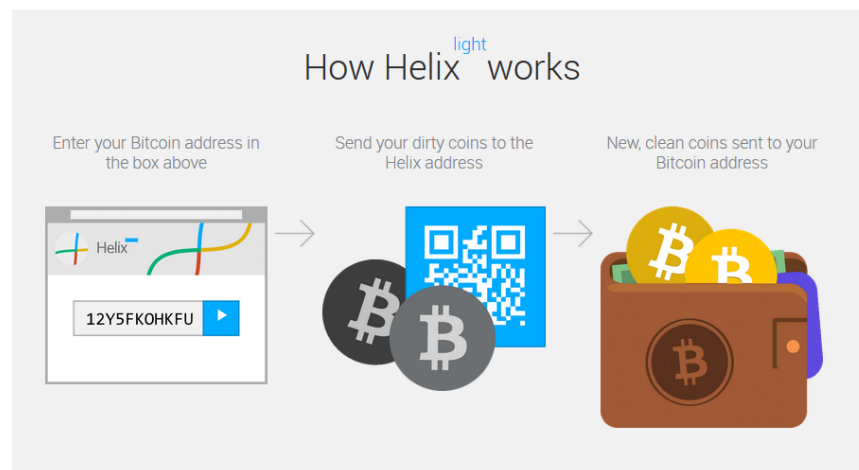


Helix made **simple**.

Enter the BTC address the clean coins will be sent to...

Let's go!

Up to 5 addresses separated-with-dashes, e.g. address1-address2-address3



Simple

1 transaction in,
Many transactions
out

The Helix Light system is very simple. Give us the address you want the bitcoins sent to. We give you an address to send them to. You have **8 hours** to send 1 transaction between .02 and 21 bitcoins. Helix takes a 2.5% fee and sends you brand new coins.

Speedy

Cleans coins in 30
minutes

After the initial transaction you send to Helix has 2 confirmations, the coins will be cleaned and sent back to you with 1 transaction immediately. The process can take up to 2 hours, but because of reserve clean coins, 95% of all helixes are sent with in 30 minutes.

Easy

No account needed

Unlike regular Helix you don't need to sign up for a Grams' account. This means **no entry fee**, no pgp key verification, and no link to you (even your online identity) at all. One-click **random delay** and **randomized transactions** buttons makes for simple, fast, and secure bitcoin cleaning.

Figure 12.

SEC Calls Out Meta 1 Coin as a Security Fraud

On March 16, the SEC froze the assets of Meta 1 Coin, an alleged crypto scam supported by former Republican Senator for the state of Washington, Dave Schmidt. Meta 1 claimed to be backed by art and gold assets and, as of April 2018, had raised \$4.3 million with the promise of a 224,923% return to investors without proof of legitimate tokens. The SEC fined the parties involved in lieu of jail time and labeled the project as an "ongoing securities fraud." Meta 1's website and social media pages are still currently active.

Child Exploitation Masterminds Arrested in Netherlands and South Korea

On March 14, a federal grand jury in the District of Columbia indicted Dutch national Michael Rahim Mohammad, also known as "Mr. Dark"—operator of Dark Scandals, a site on both the Darknet and Clearnet that featured violent rape videos and child pornography. Speaking on the indictment, Don Fort, Chief, IRS-CI warns "Criminals should know if you leave a digital footprint, we will find you. If you thought you were anonymous, think again. The dark web is not quite as dark today due to the hard work of IRS-CI and our partner agencies."

Less than two weeks later, on March 25 prosecutors in South Korea began reviewing whether to formally charge a man arrested for allegedly operating an online sexual exploitation and blackmail ring. Police perp-walked the handcuffed 24-year-old suspect, Cho Ju-bin, in front of waiting journalists at the Jongno Police Station in Seoul before driving him to the prosecutors' office. Prosecutors allege Ju-bin operated a secret Telegram chat room, "Nth Room," where he posted graphic videos of women and young teens in return for cryptocurrency payments.

Police investigating the Nth Room pedophile ring also served search warrants on the country's leading crypto exchanges, including Upbit, Bithumb, Korbit, and Coinone. They are attempting to track down people who paid as much as 1.5 million won (US\$1,200) in cryptocurrency to watch sexually exploitive and sometimes violent video footage featuring women and underage girls.

Two investigative journalists infiltrated the now-notorious chat room and revealed the story. Police believe Nth Room had been operational since 2018 and involved as many as 74 victims. In total, it took in millions of dollars' worth of Bitcoin, Ethereum and Monero.

Thefts, Scams, and Fraud

COVID-19 Scams Spread

While governments are funneling the majority of resources to mitigating the health and economic impacts of the coronavirus pandemic, bad actors are taking advantage of the resulting lack of regulatory oversight and enforcement. In the rush to institute government programs, there will inevitably be corruption and misallocated funds, creating a ripe environment for money laundering. Additionally, scammers and fraudsters are benefiting from fear created by the health crisis and selling masks, vaccines, life-saving drugs and other non-existent medical supplies to unaware consumers.

FinCEN and U.S. law enforcement have seen reports of cybercriminals leveraging COVID-19 themes as lures, often targeting vulnerable individuals and companies that seek healthcare information and products or are contributing to relief efforts.

-FinCEN Director Blanco 5/23/2020

Such fraud is generally committed by convincing consumers to leave a “trusted” website they are on to join a messaging platform where the scammer can convince the victims to pay crypto in exchange for PPE, medicines, and other in-demand supplies. CipherTrace has also seen a variety of new darknet markets pop up claiming to sell COVID-19 diagnostic tests, secret vaccines and cures, or limited supplies of PPE. Even some vendors in larger darknet marketplaces have moved from selling their traditional illicit products to masks and drugs such as chloroquine that claim to cure COVID-19.

In terms of cryptocurrency related scams, CipherTrace found that scammers have used multiple ways to use COVID-19 to their advantage. Below are some examples of specific cases that CipherTrace has analyzed.

New Ransomware Strains Named after the Coronavirus

Many ransomware strains have capitalized on COVID-19, utilizing the name, or a variation of it, due to the notoriety and recognition. Strains include:

- Corona Ransomware
- CoronaVi2022
- N2019cov
- SARS-CoV-2

There have also been ransomware strains that aren't COVID-19 related by name, however, they are strategically attacking hospitals and other healthcare providers. One example of this noted below, sent its bitcoin to a Canadian crypto payment processor.

- EDA2 (associated with HiddenTear)

Malicious "Covid-Related" Applications and Websites

Additionally, multiple cases have been reported of malicious Android applications that claim to offer information about the virus. These allow the attacker to spy on the user through their devices or encrypt the device and hold it for ransom. Examples include:

- COVID19 Tracker
- Wisecleaner.best (coronaVi2022)

Phishing Attacks with Covid Lures

Open source intelligence identified several email campaigns that attempt to impersonate official groups in order to extract personal information and/or cryptocurrency payments. The Red Cross scam also sent its bitcoin to the same Canadian crypto payment processor as some COVID-19 related ransomware. Examples include:

- CDC Email Scam
- Cdc-gov.org Email (steals email credentials)
- Delayed payment confirmation caused by COVID-19 Email (steals email credentials)
- Red Cross Email Scam
- WHO Email Scam



We are all affected by the growing COVID-19 pandemic. It's an unprecedented health challenge and we know people and organizations everywhere want to help. The World Health Organization is leading and coordinating the global effort, supporting countries to prevent, detect, and respond to the pandemic.

The greatest need right now is to help ensure all countries are prepared, especially those with the weakest health systems. Donations support WHO's work to track and understand the spread of the virus; to ensure patients get the care they need and frontline workers get essential supplies and information; and to accelerate efforts to develop vaccines, tests, and treatments.

See below for information on other ways to give, tax-deductibility and corporate and foundation giving options.

Now you can help us by donating any amount what you want help with the BITCOIN NETWORK

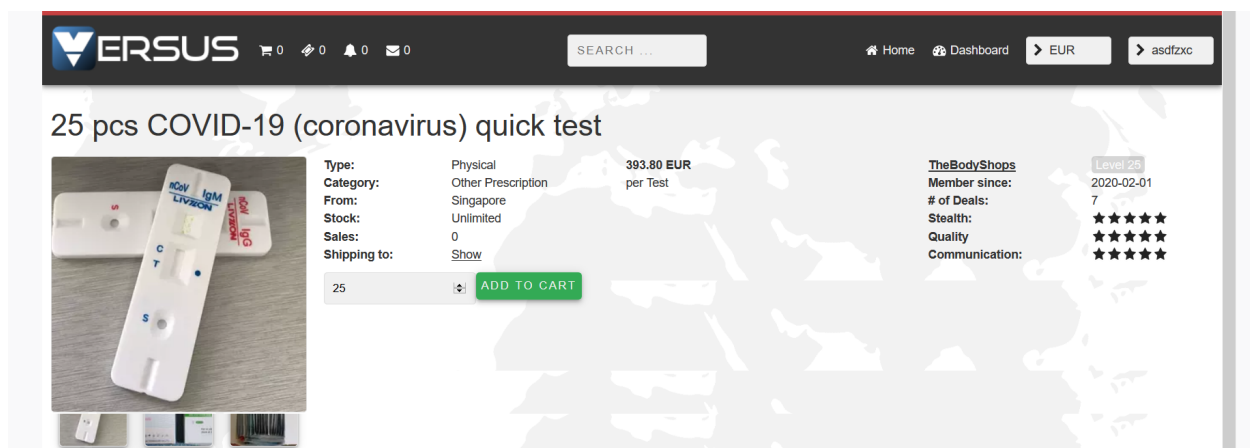
Donate Now with Bitcoin payment.

Figure 13.

Dark Markets for Covid Products Fail to Flourish

Vendors on the dark web are selling products at inflated prices, everything from masks to a cure. As always, there is most likely a lot of scam dark web sites that are selling products supposed to protect one from COVID-19, but in reality, they will never send any product to the purchaser.

Fortunately, most of the COVID-19 scams found on darknet marketplaces see no sales. Like an illicit Ebay or Amazon, these marketplaces publicly display sales and ratings for items and vendors. In figure 14 below, it is evident that faux tests and cures have little to no market on the dark web.



This coronavirus quick test received 0 sales in the single month CipherTrace observed its status. As of May 16, 2020, the vendor has yet to sell a quick test.

Figure 14.

Personal protective equipment, such as a variety of masks, hazmat suits, and hand sanitizers, can be a hit or a miss in darknet marketplaces. The most commonly found COVID related item in darknet marketplaces were masks and respirators, with one marketplace being flooded by different vendors trying to unload a variety of different masks. In reviewing the sales of darknet PPE, however, CipherTrace found that after over a month of observation, most PPE on darknet marketplaces retained no sales.



After one month, with over 119 views, one vendor failed to sell any hand sanitizer on this darknet marketplace.

Figure 15.



Figure 16.

Other darknet marketplaces can be seen selling COVID-19 related phishing sites. These items, by far, have the highest sales and feedback of all COVID-19 related items on the dark web. This may be indicative of the type of person that often visits darknet marketplaces as one trying to buy the material to scam others. These faux web pages claim to imitate legitimate entities such as The Red Cross to ask for donations, linking to major banks where victims inadvertently give up their banking credentials to scammers, as seen in figures 17 and 18 below.

+Fraud

REDCROSS COVID FULL INFO SCAMPAGE+SHOWING 16 BANKS



Sold by: medpage
Trust rating: High
Feedback score:99
[Contact medpage](#)
[View medpage's profile](#)

Buy now

200 CAD

141 USD

You are protected by
ESCROW

Product Description

[Refund Policy](#)[Seller's Feedback](#)

UNDETECTED SCAMPAGE + SHOWING 16 BANKS

SHOWING BANKS :

ATB, BMO, CIBC, DESJARDINS, HSBC, LAURENTIAN, MANULIFE, MERIDIAN, MOTUS, NBC, RBC, SCOTIA, SIMPLII, TANGERINE, TD N VANCITY

INFO FORMAT :

BANK INFO :

USER N PASS, QUESTIONS N ANSWER

FULLNAME, DOB, MMN, SIN, DLN, EMAIL N PASS

NAME ON CARD, CARD NO, EXP, CVV, ATM PIN

Figure 17.

Canadian Red Cross

Franglais

YOUR GIFT DONOR INFORMATION PAYMENT

By Interac

Select your financial

| | |
|----------|------------|
| ATB | BMO |
| CIBC | DESJARDINS |
| HSBC | LAURENTIAN |
| MANULIFE | MERIDIAN |
| MOTUS | NBC |

Your \$160 donation goes where it is needed most.

Your donation will be used to fund the Red Cross Society of China's response to the Novel-Coronavirus (COVID-19). Response efforts include prevention and control of the spread of the infection, social mobilization and risk communication to communities affected or at risk, and support to government hospitals.

Figure 18.

enforcement on the Darknet, and because of our growing expertise in this area, he could not make good on that promise.”

Massive Wotoken Ponzi Scheme Defrauds Investors of Over \$1B Worth of Crypto

On May 14, the trial against six core operators responsible for organizing and leading multi-level marketing (MLM) activities for Wotoken began in the People's Court of Binhai County, Yancheng City. According to the public hearing, this ponzi scheme was active from July 2018 to October 2019 and had 715,249 registered users. In its little over a year of operation, the scheme netted the Wotoken fraudsters more than 7.7 billion yuan (roughly \$1.09B USD) worth of crypto. This was further broken down into:

- 46,000 Bitcoin
- 2.039 million ETH
- 292,000 Litecoin
- 56,000 Bcash
- 684,000 EOS

Five of the six on trial plead guilty to defrauding investors.

Yet, despite the leadership facing trial, CipherTrace has discovered that the Wotoken funds continue to move at the time of this report, following common cryptocurrency money laundering typologies. CipherTrace investigators will continue to monitor the wallets associated with Wotoken to trace the funds to their final destination.



CipherTrace Inspector displays how the Wotoken fraudsters continue to launder illgotten funds. Here, a portion of the funds is traced after being split into multiple peel chains, reconsolidated, and sent through mixers.

Figure 19.

The anatomy of a Ponzi Scheme

Similar to Plustoken, Wotoken claimed to generate returns for users through special algorithmic trading bots and referral commissions to affiliates, which would all be paid out in Wotoken's personal WOR token, have no value outside of WoToken itself.

Some WoToken promotional material claimed:

- invest in \$1000 worth of WOR tokens and receive a 0.25% to 0.5% daily ROI
- invest in \$5000 worth of WOR tokens and receive a 0.3% to 0.65% daily ROI

Like any typical ponzi scheme, Wotoken also boasted multiple levels of referral commissions, which were also paid out in WOR tokens. To participate in any of the MLM income opportunities, however, a minimum \$1000 worth of investment in WOR tokens was required. This was done by depositing cryptocurrencies into your Wotoken wallet and converting them into WOR tokens.

Early Warning Signs

On December 23, 2019, police in Baotou, a city of Inner Mongolia in northern China, warned the public of a possible Wotoken exit scam after many investors reported that withdrawals were stopped. Soon after, the Wotoken wallet app ceased operations.

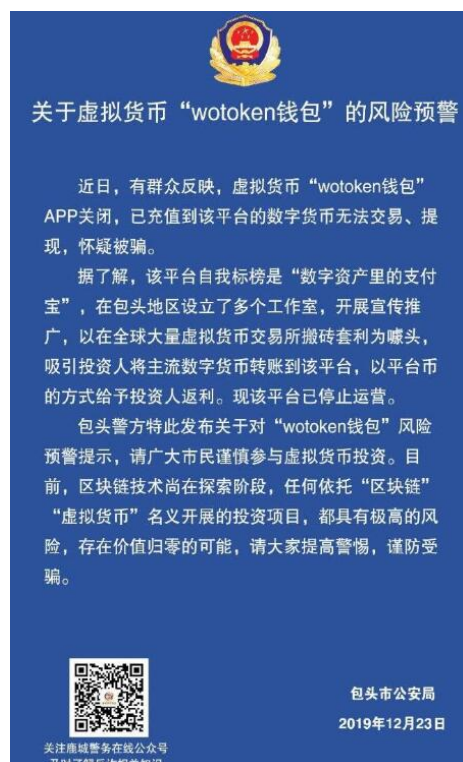


Figure 20.

Even earlier, on October 2, 2019, the British Columbia Securities Commission in Canada issued an investor alert on “smart wallet apps that purportedly store a person’s crypto-assets and earn money for depositors.” The warning specifically called out Wotoken for their claims that “users will realize earnings of six to 20 per cent monthly by activating the trading software” and adds, “Big promises and pyramid-like payouts are both classic warning signs of risky investments. We urge everyone to approach these apps with extreme caution.”

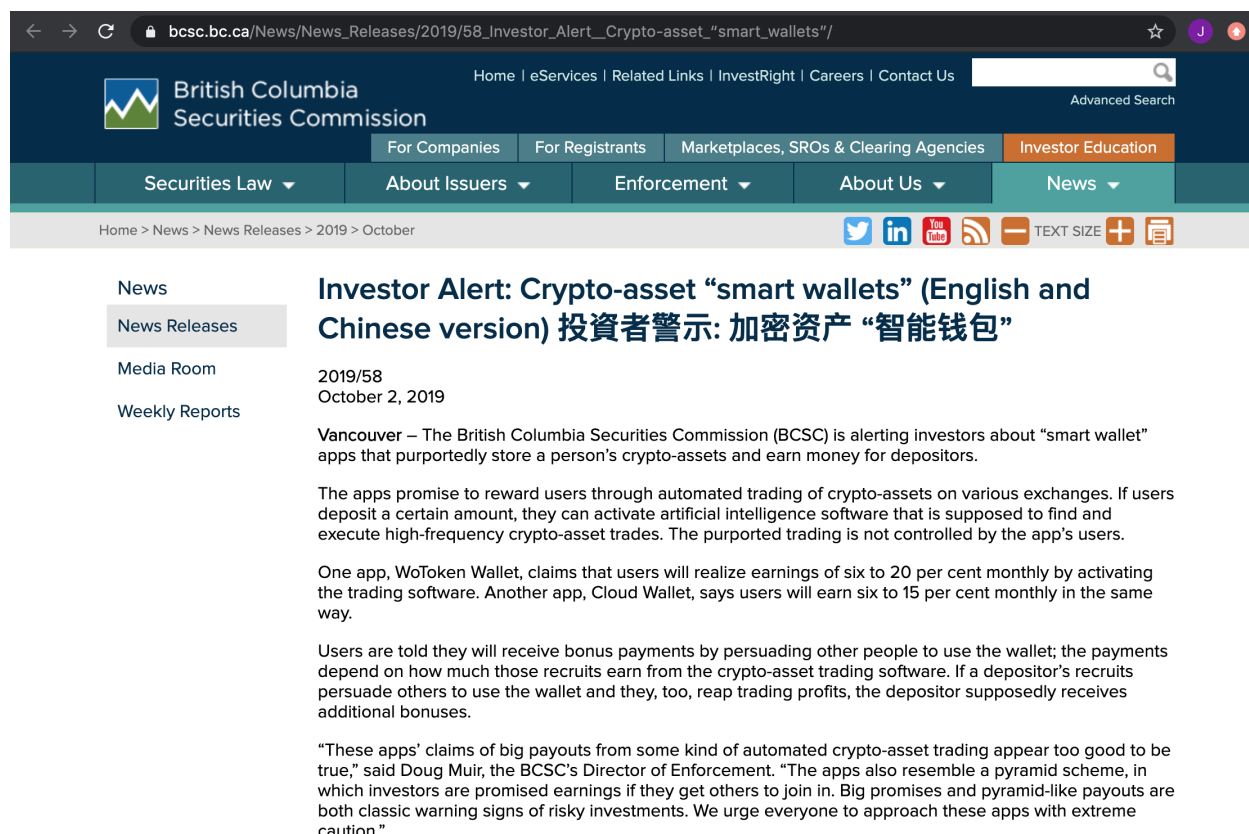


Figure 21.

Cryptocurrency Exchange FCoin Insolvent After \$130M Bitcoin Shortfall

On February 17, Chinese cryptocurrency exchange FCoin revealed that flaws in the company’s incentive structures gave the exchange a roughly \$130M deficit in its crypto reserves. Zhang Jian, former Huobi CTO and Founder of Fcoin, said the liability was a result of traders receiving too many financial incentives for transacting on the exchange. While the exchange is no longer processing withdrawals, in a statement on the Fcoin website, that has been removed, Jian claims he will compensate everyone for their losses, but warns to expect slow efficiency as he will personally be handling all withdrawals.

Digital Wallet That Promised High Yields on EOS Deposits Exits with \$52 Million

On April 20th, a report came out revealing another crypto exit scam. EOS Ecosystem, a wallet that enticed investors with promises of favorable returns, stole close to \$52M USD from users.

A local Chinese media investigation found that, as of the morning of April 20th, 19.36 million EOS tokens (equivalent to \$52 million) had been transferred into an EOS account apparently belonging to the EOS Ecosystem business. Transaction metadata indicates that the funds may have already been siphoned into an exchange, which promised to freeze the funds upon detection.

The scam appears to have been conducted by a team called "w.io." The group claimed to be part of a Chinese EOS network crypto wallet company in order to garner attention from investors and run their scam operation.

Hacker on Compromises DeFi Protocol to Steal \$25 Million in Crypto

On April 19th, Cryptoslate reported that an Ethereum user had stolen over \$25 million worth of cryptocurrency from Lendf.me, a decentralized lending protocol operated by Chinese DeFi upstart dForce. The perpetrator had created the address attached to the hack in the hours leading up to the theft, and efforts to identify the criminal in question have come up short. Within a few hours Lendf.me had lost 57 percent of its value and warned users to halt any deposits into the protocol.

Ultimately, the hacker managed to slip away with \$25 million worth of Ethereum, Tether's USDT, and various other tokens, wiping the protocol clean. In the wake of the attack, Lendf.me has silenced their Twitter account and taken down their website. As of April 19th, Lendf.me issued a statement that legal action is imminent in addition to private negotiations that are already underway to recover the stolen funds from the hacker.

In a strange twist, on April 21—two days after the hack—the dForce hacker returned about \$24 of the \$25 million that was stolen. However, the tokens the hacker returned were in different values of other types of tokens. At the time of this report it is unknown why the hacker returned a different set of tokens from those that were stolen, or why the hacker returned any of the funds at all.

CFTC Charges Multiple Firms for \$15 Million Crypto and Binary Options Scam

On May 5, the Commodity and Futures Exchange Commission (CFTC) charged executives of Tal Valariola and Itay Barak of Israel-based Digital Platinum Limited for aiding the US-based firm All In Publishing (AIP) in creating and promoting numerous misleading investment schemes to US and foreign investors.

The defendants allegedly spent an estimated \$50,000 to create slick videos of customer success stories, which were used to prompt 51,917 users to open binary options accounts and 8,043 users to open digital asset trading accounts. The digital marketing campaigns utilized "at least five email auto-responders, each with a database of approximately 200,000 emails." Ultimately, the perpetrators were caught and now face charges on four counts, including options fraud and CTA fraud.

Chinese Cosmic Cryptocurrency Ponzi Absorbs \$11 Million in Three Weeks

By the end of April, scammers running Antimatter Kingdom (AK), a new Chinese crypto Ponzi scheme, appear to have netted at least \$11 million worth of bitcoin. The scam marketed itself as "the evolutionary cornerstone of the blockchain industry." Preying on FOMO, AK claimed in their promotional material that investing in their platform now was like buying bitcoin in 2008 or Ethereum in 2015. A review of their whitepaper illustrates a series of hyperbolic language, sensationalisms, referral incentives, and pyramid imagery. The scheme requires user maintain a balance of at least 0.1BTC, with more funds equating to more "mining power" and more returns for the user. CXCBLOCK's website and social media are still online and continue to promote Antimatter Kingdom.

Travelex Reportedly Paid \$2.3 Million Ransom to Restore Operations

A New Year's Eve ransomware attack to Travelex—a fiat money-exchange kiosk company—resulting in the company eventually paying \$2.3 million in bitcoin to cybercriminals. The hackers infiltrated the system with malware known as Sodinokibi (also known as REvil or Sodin), resulting in a shutdown and ransom payment of 285 bitcoin. Travelex was forced to take its internal networks, consumer-facing websites and app offline, which stalled delivery of cash from Travelex's network of vaults to banks.

IOTA Wallet Hacker Steals \$1.4 Million USD of MIOTA

On February 12, IOTA—an open-source distributed ledger and cryptocurrency—announced on its website that it had started to receive reports of thefts from several users' Trinity Wallets. Hackers netted more than 8.5 million in IOTA's native token MIOTA, worth approximately \$1.4 million at the time, due to an exploit found in a third-party integration. The stolen funds were repeatedly merged and split to obfuscate the investigation. IOTA founder David Sonstebo has since declared he would repay those affected by the hack from his personal IOTA holdings.

Bisq Exploit Results in \$250k Theft of Bitcoin and Monero from Platform

On April 8th, decentralized exchange Bisq revealed a hacker had stolen \$250K in cryptocurrency from their platform. A bad actor was able to exploit a software flaw to steal an estimated \$22K worth of bitcoin and \$230K worth of Monero. The hacker set the

default fallback address for other users as his own address so that when any trade failed, the funds would be transferred to the hacker's own account. To accumulate the ultimate sum of \$250K, the hacker pretended to be a seller starting a trade with a buyer. When the time ran out, the funds would arrive to the hacker, along with the buyer's security deposit.

[XRP Giveaway Scam Steals \\$205k USD of XRP](#)

In early March, a fake YouTube account was attempting to lure viewers into participating in an XRP giveaway scam started circulating on social media. The scam involved fake “Ledger Live” extensions on the Google Chrome web browser, which have been used to steal roughly 1.4 million XRP—worth about \$205,000 at the time. On March 25, Ripple published a blog post on “How to Spot XRP Giveaway Scams”, noting that neither the company nor any of its executives has ever offered – or ever will offer – any digital assets to the public for free.

[Crex24 Exchange Accused of Hiding Hack from Customers](#)

On March 6, reports that Estonian crypto exchange Crex24 had suspended 61 altcoin pairings and froze withdrawal and deposit services began circulating the internet, causing many users to suspect an undisclosed hack. Crex eventually disclosed that 200 million Htmlcoins, worth about \$11,200 at the time, were stolen from its wallets and that it would be working with the Htmlcoin team to reimburse investors. According to a Medium post by HTMLcoin, while user deposits at the exchange were frozen, the hackers also attempted to blackmail Crex24, demanding a 25 BTC ransom within 48 hours if the exchange wanted to keep the hack private.

Global Regulatory Environment Rapidly Matures

Travel Rule Industry Cooperation and Open Standards Produce Viable Options

While the FATF is often called a global anti-money laundering and counter terrorism financing watchdog, it doesn't actually have any enforcement authority. Nonetheless, when the FATF speaks, governments listen because negative repercussions including a grey listing, a form of financial ostracism.

Last June, the FATF announced a much-anticipated clarification of its cryptocurrency-related regulatory guidelines for member states. It caused quite a stir in the virtual asset community, especially after the G20 announced full support for the recommendations during its summit in June 2019. The updated guidance rocked the cryptocurrency community because it contains a number of new rules for VASPs, which the FATF said are needed to counter rising threats of money laundering and terrorism financing.

One of the most contentious recommendations in the FATF's updated *Guidance for a Risk-based Approach to Virtual Assets and Virtual Asset Service Providers* has since become known as the FATF funds "Travel Rule." Among other requirements, it obliges VASPs to:

"obtain, hold, and transmit required originator and beneficiary information, immediately and securely, when conducting VA transfers."

The FATF also set a fairly short fuse—one year from the June 2019 announcement—for when member nations should have the new guidance transposed into their local laws. The world is now a month away from this deadline, but is the industry any closer to compliance with the new regulations?

FinCEN Reminds VASPs Operating in US That Crypto Travel Rule Is Already Being Enforced

On May 13, crypto legal and regulatory experts from around the world gathered at the Consensus: Distributed virtual conference to discuss how ready crypto is for the Travel Rule. In his keynote presentation, FinCEN Director Kenneth Blanco stressed the importance of the Travel Rule on global AML/CTF. Blanco applauded the steps taken by the FATF to adopt an International Standard for crypto AML, stating that:

"any asset that allows the instant, anonymized transmission of value around the world with no diligence or recordkeeping is a magnet for criminals, including terrorists, money launderers, rogue states, and sanctions evaders."

Blanco further added how FinCEN is “optimistic about the growth of various cross-sector organizations and working groups focusing on developing international standards and solutions addressing the Travel Rule.” According to him, most of the challenges FinCEN sees relate to governance and process rather than technologies. Because of FinCEN’s technology neutral approach, Blanco encouraged the virtual currency sector to continue collaborative efforts to develop and implement Travel Rule solutions.

One key working group making strides in this area is the Travel Rule Information Sharing Architecture (TRISA) Working Group. The TRISA Working Group is made up of leading experts in the crypto industry—from thought leaders, legal experts, blockchain developers, and Chief Compliance Officers from VASPs around the world. The working group meets weekly to discuss the unique challenges the Travel Rule presents on the community and how best to overcome them, in addition to developing the governance body and processes that FATF and FinCEN is keen on. To join the initiative, visit www.trisa.io to learn more.

Blanco ends his discourse on the Travel Rule by reiterating FinCEN’s stance that the United States maintains that the Travel Rule has applied to VASPs for years and continues to expect any VASP operating in the United States or with US persons to understand who is on the other side of a transaction.

Compliance and confidentiality conundrum

Trouble is, a number of severe challenges make complying with the Travel Rule—while protecting VASPs’ customer data—no easy feat.

First, transmitting and storing senders’ and receivers’ information is antithetical to what crypto-libertarians generally perceive as a cornerstone of cryptocurrencies—pseudo-anonymity. Concerns for preserving VASP customers’ privacy plus the wording in the FATF guidance regarding data protection rules in general means any solution should deliver both security and confidentiality.

“As the guidance makes clear, relevant authorities should co-ordinate to ensure this can be done in a way that is compatible with national data protection and privacy rules.”

-The Financial Action Task Force

Presenting Travel Rule Information Sharing Architecture to FATF in Paris

TRISA Chairman Dave Jevans, was invited to Paris in mid-February to present an update to FATF representatives on TRISA’s progress toward a solution. CipherTrace developed the open, distributed TRISA architecture and released it to the community as open source. CipherTrace also co-founded the TRISA standards body. Jevans explained to the FATF

representatives that TRISA association has become a mature ecosystem with a governance committee, board of directors, and steering committee.

A further consideration is time. When FATF announced the new guidelines in June 2019, the FATF gave a 12-month window before it would report on the progress of individual member nations on transposing the guidance local implementation measures. So far only Japan, Switzerland, and the United State have made significant travel rule progress.

As if that didn't put enough pressure on VASPs, in May 2019 the U.S. Treasury's Financial Crimes Enforcement Network (FinCEN) issued an advisory to Money Services Business engaged in convertible virtual currencies, VASPs in FinCEN parlance, to prepare for enforcement actions if they fail to comply with the long-standing funds Travel Rule under the U.S. Bank Secrecy Act (BSA).

All of these characteristics should enable the ultimate goal of making it practical and cost-effective for VASPs to comply with the Travel Rule by June. Jevans also announced that TRISA had achieved a two major goals in January by standing up a testnet and having early adopters integrating and testing the software. Passing these two milestones keeps the initiative on a timeline designed to deliver a working, industry-wide solution by June 16, 2020.

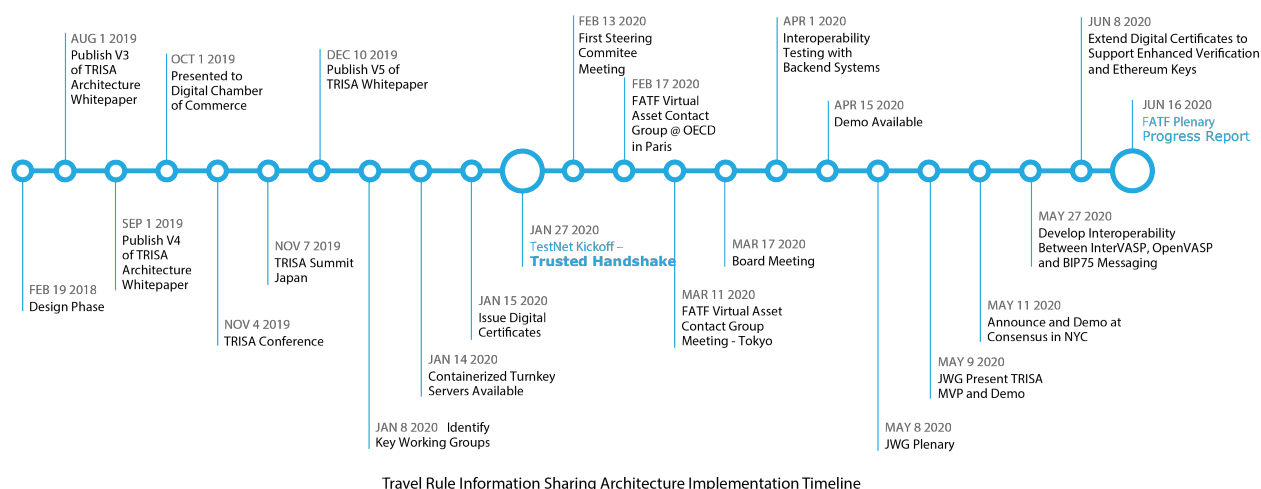


Figure 22.

Built on proven trust models and security technologies

Jevans next described how a peer-to-peer discovery approach makes TRISA secure and reliable, ensuring privacy, decentralization, high performance, and low impact on transaction workflows. He also detailed key aspects of the solution's approach to security and privacy. It includes employing a strong root of trust, mutual authentication, revocation and blacklisting, encryption of transmitted data, and TLS 1.3 with forward secrecy.

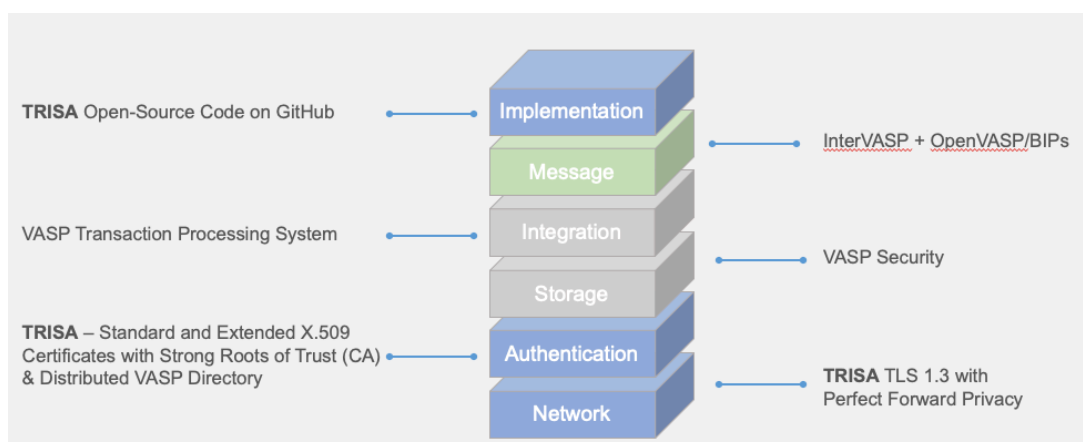


Figure 23.

The FATF member also got a peak inside a TRISA and how it works,” which at the core involves applying enhanced validation certificates and the Certificate Authority (CA) Trust Model. The CA model makes it possible reliably identify and verify VASPs to ensure PII will not be sent to wrong VASP. It works by guaranteeing that an individual (or machine) granted a unique certificate is, in fact, who he or she says they are.

TRISA also makes it possible to establish secure communications and mutual authentication between VASPs.

Jevans finished his technical overview by providing FATF a detailed technical overview of how TRISA’s open Infrastructure securely interoperates with established and emerging standards.

Progress in fast-tracking a Travel Rule compliance standard

In addition to sharing technical details about TRISA, Jevans updated the FATF on organizations that have chosen to join the TRISA movement. These span exchanges, kiosks, privacy advocates, regulators, and even privacy coins. Key industry names include Binance, eToro, Coinsource, MIT, the Blockchain Alliance, the Digital Chamber of Commerce, and representative of the Japanese virtual currency industry.

AMLD5 Is Here: EU Crypto Businesses Faced with Tough New Regulation

As of January 10, the EU’s 5th Anti-Money Laundering Directive, variously referred to as 5AMLD or AMLD 5, went into effect in a bid to make fiat-to-crypto transactions more transparent. Partly prompted by the terror attacks in France, the new regulations are designed to fight terrorist financing and money laundering, while making information more accessible to European financial regulators. The directive also includes tough new regulations for VASPs such as virtual-to-fiat exchanges and custodian wallet providers. Noncompliant crypto service providers may be subject to fines up to €200,000.

Many European crypto asset businesses have been unable to meet the new regulatory guidelines. Already, several companies have ceased operations, citing the extensive know-your-customer (KYC) and AML requirements as AMLD 5 becomes a reality. However, all the technology needed to quickly and cost effectively bring VASPs into compliance are readily available.

Not all European VASPs are making the investment in updating their compliance regimes to meet the new AMLD5 requirements. Dutch crypto derivative platform Deribit, for example, moved to Panama in early February to avoid these regulations. Despite some arguments that the costs of compliance will not be significantly higher, Deribit believes that the new regulations create too many barriers for the majority of traders.

UK—FCA Becomes AML and CTF Supervisor for UK Cryptoasset Activities

On January 10, the United Kingdom's Financial Conduct Authority (FCA) became the anti-money laundering and counter terrorist financing (AML/CTF) supervisor for businesses carrying out cryptoasset activities under the amended Money Laundering, Terrorist Financing and Transfer of Funds Regulations. This amendment is a result of the implementation of AMLD5 into the UK's national legislation. Under the new regulations, cryptoasset businesses operating in the UK are now required to register with the FCA before providing services within the country, on top of integrating traditional AML requirements such as undertaking customer due diligence, enhanced due diligence, reporting, and monitoring.

US—On Crypto AML/CTF, FATF Finds U.S. “Largely Compliant”

On March 31, the FATF released an anti-money laundering and counter-terrorist financing measures report that reevaluated the United States' regulations relating to cryptocurrencies and virtual assets. The FATF found the United States has met or mostly met most of the new criteria set out by Recommendation 15 and retains a rating of “largely compliant.” According to the report, while US authorities “understand and are aware of the ML/TF risks emerging from virtual assets,” the FATF expressed concerns that the US does not adequately deal with VASPs that are incorporated in the US but do not operate in the country.

The findings of the global anti-money laundering watchdog highlight the importance of continued conversation and collaboration between various regulatory bodies at the international, national, and local levels. Since the last assessment in 2016, the FATF has updated its policies to reflect the new Travel Rule guidelines, requiring greater scrutiny to reveal levels of compliance. The Travel Rule requires Virtual Asset Service Providers (VASPs) to store and share certain information pertaining to the sender and receiver in any cryptocurrency transaction over a given value threshold. This requirement presents new challenges for VASPs in achieving compliance without sacrificing user privacy and while dealing in largely pseudonymous currencies. CipherTrace has proposed a solution, known

as TRISA, which is designed to facilitate open-source, secure information sharing among VASPs seeking to comply with FATF's new rules.

Canada—Toronto Stock Exchange Trades 3iQ Corp Bitcoin Fund

On April 9, Canadian investment fund manager, 3iQ's The Bitcoin Fund, began trading on the Toronto Stock Exchange (TSX) under the symbol QBTC.U. New York based crypto exchange Gemini will act as custodian of the bitcoin in the Fund. The listing on TSX is the end result of an extensive, 3-year long process with the Ontario Securities Commission (OSC). This marks the first public Bitcoin fund listed on a major stock exchange.

Japan—Revised Crypto Laws in Japan Begin Enforced Compliance

On May 1, Japan's newest crypto AML laws, amendments to the Payment Services Act (PSA) and the Financial Instruments and Exchange Act (FIEA), began their period of enforced compliance. These amendments tightened regulation on custodian wallets and cryptocurrency exchanges, giving them the same level of accountability as formal financial institutions such as banks due to the parallels in common risks such as hacks, bankruptcy of service providers, and money laundering/terrorism financing. The regulations also establish a new asset classification called "Electronically Recorded Transferable Rights" (ERTRs) which aim to clarify when initial coin offerings (ICOs) and security token offerings (STOs) are governed by the FIEA—Japan's main law governing securities.

IOSCO—Global Stablecoins May Be Subject to Securities Regulation

On March 23, the Board of the International Organization of Securities Commissions (IOSCO) published *Global Stablecoin Initiatives*—a report examining the possible implications of global stablecoin initiatives on securities markets regulators and how existing IOSCO Principles and Standards could apply. The report features a hypothetical case study of a stablecoin set to be used for domestic and cross-border payments, using a reserve fund and a governance board. The Report concludes that, depending on its structure, global stablecoins could and would likely fall within securities market regulatory frameworks.

India—Crypto Ban Overruled

On March 4, the Supreme Court of India overturned a cryptocurrency ban by Reserve Bank of India (RBI) in 2018. The ban prohibited banks from dealing with virtual asset businesses, as well as individual engaging with cryptocurrency businesses. RBI plans to contest the Supreme Court's decision to overturn its ban, warning that increased cryptocurrency trading could put the banking system in India at risk.

Sanctioned Countries

Venezuela

U.S. Accuses Venezuelan President of Using Crypto to Conceal Illicit Drug-Running

On March 26, the Department of Justice indicted Venezuelan President Nicolás Maduro and 14 other officials for operating a narcotics ring involving drug runners, Colombian revolutionaries, and narco-terrorism. In a related press release, Department of Homeland Security's (DHS) Homeland Security Investigations (HSI) alleged the conspirators used crypto to conceal their crimes.

At a press conference, United States Attorney General William Barr, along with the head of the Drug Enforcement Administration and the top federal prosecutors in Manhattan and Miami, accused Maduro of conspiring with a faction of the Colombian Revolutionary Armed Forces (FARC) rebel group "to flood the United States with cocaine," and "devastate American communities."

HSI Acting Executive Associate Director Alysa D. Erichs alleged the conspirators used crypto to conceal their crimes. "Today's announcement highlights HSI's global reach and commitment to aggressively identify, target and investigate individuals who violate U.S. laws, exploit financial systems and hide behind cryptocurrency to further their illicit criminal activity," explained Erichs. "Let this indictment be a reminder that no one is above the law — not even powerful political officials."

North Korea

Chinese Nationals Added to OFAC SDN List and Charged by DOJ for Laundering \$100 Million in Cryptocurrency Stolen by North Korea

On March 2, the U.S Treasury's Office of Foreign Assets Control (OFAC) added two Chinese nationals to the Specially Designated Nationals (SDN) list for their roles in laundering stolen cryptocurrency from a 2018 exchange hack. The two, Tian Yinyin and Li Jiadong, are purportedly associated with the Lazarus Group—North Korean state-sponsored cybercriminals believed to have been behind the Sony breach and WannaCry malware attacks, and \$2 billion in thefts from banks and crypto exchanges.

According to the Treasury press release, Tian and Li received approximately \$100.5 million worth of stolen crypto from North Korean controlled accounts. Tian ultimately moved more than \$34 million worth of these illicit funds through a bank account linked to his crypto exchange account. Li moved an additional \$33 million through linked accounts at nine different banks.

As a result of these sanctions, all property belonging to Tian and Li in the US or in the possession or control of US persons and entities must be blocked and reported to OFAC.

In addition, persons or entities that transact with Tian or Li, or with their sanctioned addresses, may find themselves penalized for sanctions violations or placed on the SDN list.

In parallel, the US Attorney for the District of Columbia has brought a Verified Complaint for Forfeiture in Rem against 113 virtual currency accounts linked to the theft and money laundering process. “Today's actions underscore that the Department will pierce the veil of anonymity provided by cryptocurrencies to hold criminals accountable, no matter where they are located,” said Assistant Attorney General Benczkowski of the Justice Department’s Criminal Division.

While the identities of virtual currency address owners are pseudonymous, these sanctions demonstrate how law enforcement can identify the owner of a particular cryptocurrency address by applying advanced blockchain analytics such as CipherTrace cryptocurrency intelligence. The use of accurate tools with high-quality attribution can not only reveal additional addresses controlled by the same individual or entity but also ensure that a financial institution or its customers are not transacting with sanctioned entities. Tian and Li’s use of bank accounts linked to their crypto exchange accounts also demonstrates the importance of banks being able to detect crypto-related transactions in their payment networks.

Read our full analysis here: <https://ciphertrace.com/chinese-linked-dprk-laundering-analysis/>

Follow this code to read all of CipherTrace's quarterly reporting and learn more.



<https://ciphertrace.com/resources/>

CipherTrace protects financial institutions from cryptocurrency laundering risks and helps grow the blockchain economy by making it safe for consumers, trusted by investors and, accepted by governments.

Editorial Board, **Pamela Clegg and Dave Jevans**

Editor-in-Chief, **John Jefferies**

Financial Crime Analyst, **Julio Barragan**