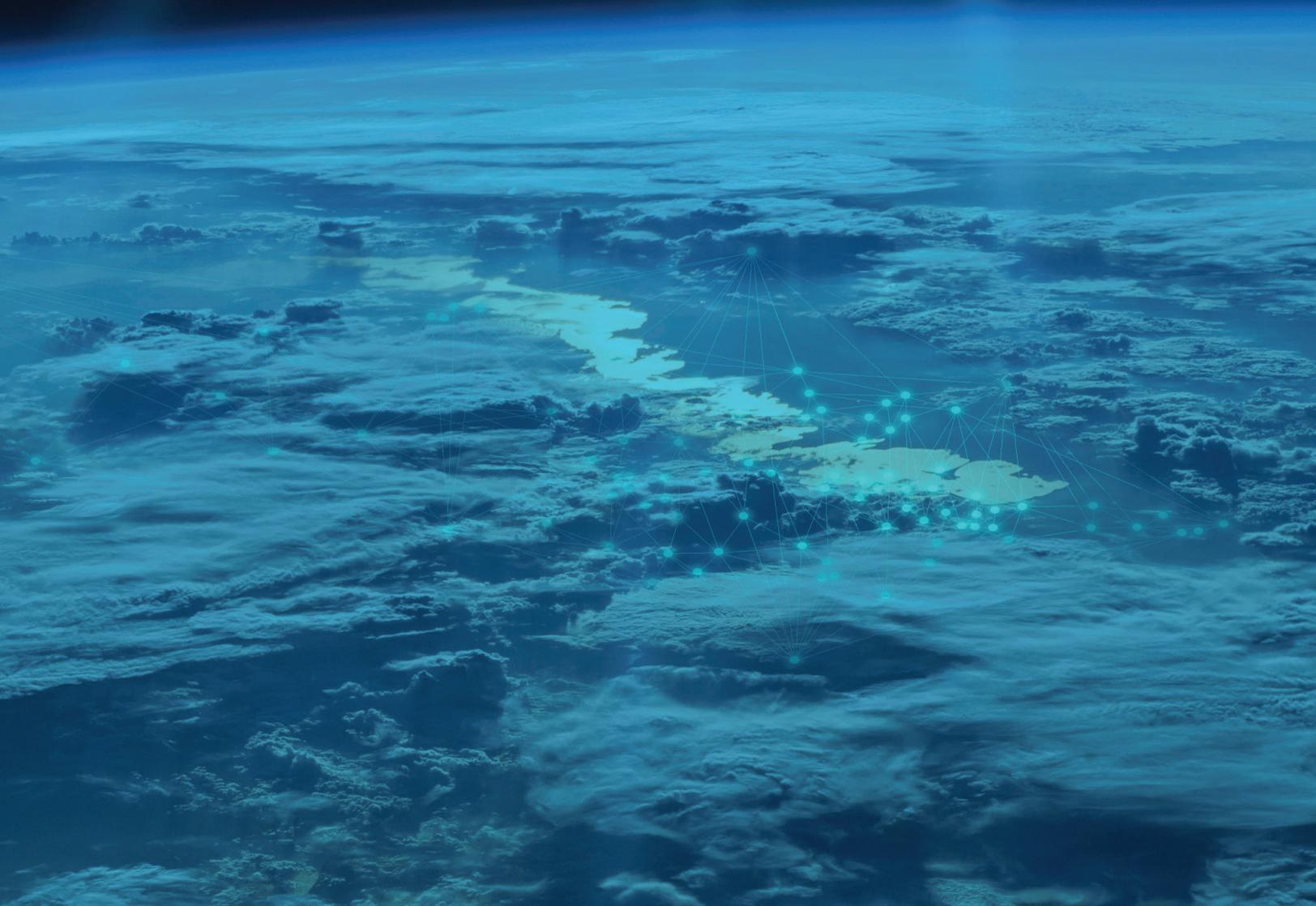


Cryptocurrency Anti-Money Laundering Report, 2019 Q4

CipherTrace
Cryptocurrency Intelligence
January 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	4
Major Trends and Developments	9
<i>Banking and Cryptocurrencies Are Increasingly Intertwined</i>	9
<i>Why it Matters: Banks Unknowingly Sending Fiat to VASPs Causes Exposure to Money Laundering Risks</i>	9
<i>New Research Finds 8 out of 10 U.S. Retail Banks Harbor Illicit Crypto MSBs</i>	10
<i>Illicit Crypto Merchants</i>	11
<i>Banks Received US\$6.2 billion in AML Fines During 2019</i>	11
<i>sResearch Reveals Two-Thirds of the Dark Market Vendors Sell Stolen Payment Products</i>	12
<i>97% of Ransomware Uses BTC as the Payment Rail</i>	13
Thefts, Scams and Fraud	16
<i>Canadian Einstein Exchange Lost US\$12 Million</i>	16
<i>IDAX Exchange Experiences Withdrawal Issues After CEO Disappears</i>	17
<i>Upbit Hack Costs 342,000 ETH Worth US\$52 Million USD</i>	17
<i>QuadrigaCX Update – Victims Demand Authorities Exhume Former CEO’s Body</i>	17
Near Crypto Crimes	18
<i>BitClub Network - Four Arrested in US\$722 Million “Cryptocurrency Mining” Ponzi Scheme</i>	18
<i>OneCoin – Widely Publicized Faux Cryptocurrency Ponzi Scheme</i>	18
Potential Blockchain Vulnerabilities	19
<i>Maker DAO Vulnerability Could Have Frozen US\$100M DAO</i>	19
<i>MimbleWimble Transaction Privacy Proven to be Vulnerable</i>	19
Changes in the Global Regulatory Environment	20
<i>The State of Cryptocurrency Anti-Money Laundering Legislation</i>	20
<i>FinCEN, CFTC, and SEC Clarify Areas of Authority</i>	21
<i>Basel Committee Issues Advisory on Banks’ Crypto-Asset Risk Exposure</i>	22
<i>Joint Statement by the EU Council and the Commission Regarding Stablecoins</i>	23
<i>US – IRS Increases Focus on Cryptocurrencies</i>	24
<i>US – Cryptocurrency Act of 2020</i>	24
<i>US – House Bill Would Classify Stablecoins as Securities</i>	25
<i>AMLD5 Effective Across EU after January 2020</i>	25
<i>Germany Adopts AMLD5 Regulation into National Law</i>	26
<i>Ukraine – New Crypto AML Regulations Based on FATF Guidelines</i>	26
<i>Russia Enacts New Crypto Law for Smart Contracts</i>	27
<i>Russia – “Crowdfunding” Law Takes Effect</i>	27
Sanctioned Countries	28
<i>North Korean Crypto Conferences Help Fortify Regime’s Crypto Laundering Efforts</i>	28
<i>Iran—Rouhani Calls for Muslim Cryptocurrency</i>	29
<i>Iran—Crackdown on Illicit Crypto Mining Escalates</i>	29
<i>Venezuela—Maduro Continues to Force Petro on Citizens</i>	29
<i>Russia—Largest Russian Dark Market Launches ICO to Fund Western Expansion</i>	31

Executive Summary

If crypto crime had a Person of the Year in 2019, it clearly would have been The Malicious Insider. Exchange hacks and other forms of outright larceny have driven headlines of user losses in previous years. However, 2019 was dominated by Ponzi schemes, exit scams, and other forms of cryptocurrency financial fraud.

These frauds include almost US\$200 million being spirited away from what once ranked as Canada's largest cryptocurrency exchange and a mysterious Asian Ponzi scheme purportedly bilking investors out of several billion dollars. Also, on April 25, the New York Attorney General's Office brought suit against the parent company of Bitfinex and Tether alleging that it lost US\$850 million of assets to Crypto Capital, a Panama-based payment processor that handles customer withdrawals. Interestingly, Crypto Capital was also used by the scandal-ridden QuadrigaCX exchange.



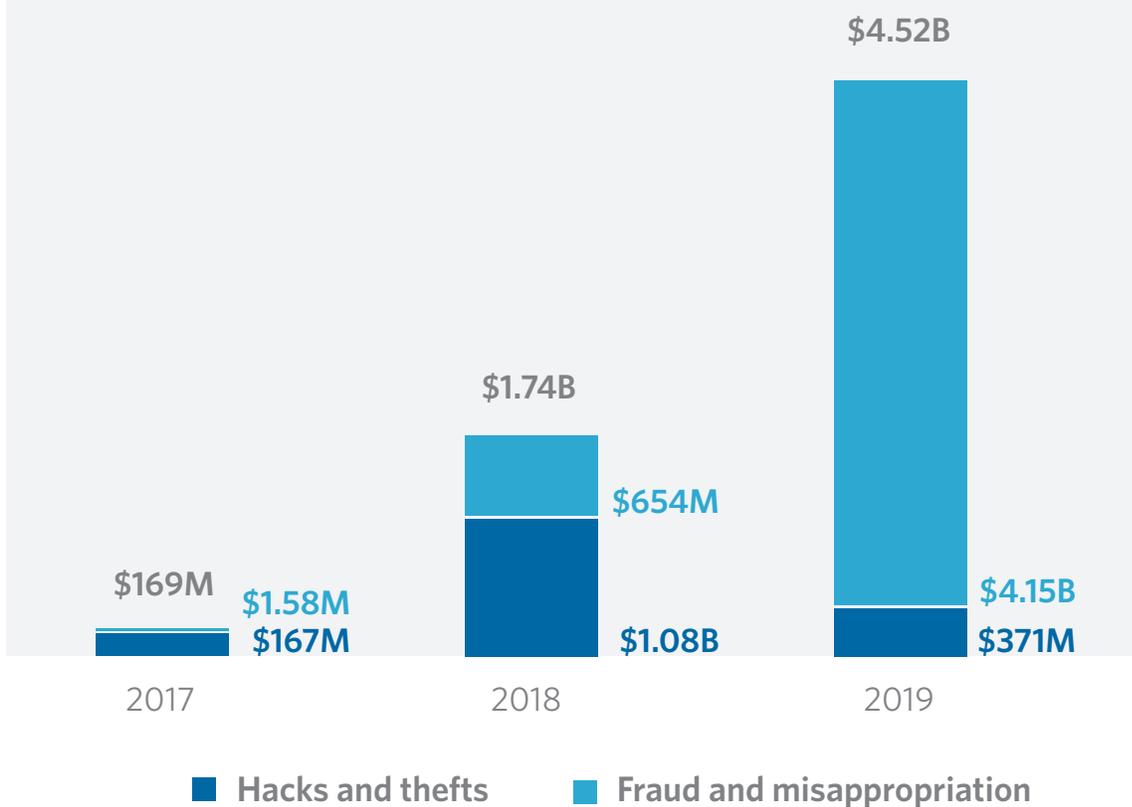
For the year, losses from fraud, misappropriation of funds, exchange hacks and thefts add up to US\$4.5 billion.

In Q4 2019, other major frauds included the Canadian exchange, Einstein, which caused US\$12 million in losses when it executed an exit scam, and the China-based IDAX exchange, where the disappearance of the CEO left an unknown amount of cryptocurrency missing. In aggregate, thefts, frauds, and misappropriation of funds for Q4 totaled US\$70 million.

Compared to 2018, cryptocurrency user and investor losses due to fraud and misappropriation in 2019 increased by 533%, while hacks and thefts decreased by 66%. For the year, losses stemming from fraud and misappropriation of funds—along with US\$370.7 million in exchange thefts and hacks—add up to US\$4.5 billion. While at first glance this eye-popping number would suggest cryptocurrency is becoming riskier, Figure 1 shows outright thefts have not risen as dramatically as total for thefts and fraud year over year. Again, the culprit behind what looks like a logarithmic rise in total losses is the malicious insider.

This disparity also shows the potential benefits of rational and appropriate regulation. Supervision of ICOs, IEOs, STOs, stablecoins and other crypto virtual asset businesses can help to eliminate fraud. It can also help to make crypto asset businesses safe for banks to accept as customers. By making virtual assets as well as virtual asset service providers (VASPs) trusted by investors and accepted by governments, well-conceived regulation can also help to grow the blockchain economy.

Blockchain Fraud Vastly Exceeds Hacks & Thefts in 2019



Source: CipherTrace Cryptocurrency Intelligence

Figure 1

The losses from insiders are so big that the impacts of these frauds continue to reverberate in the crypto economy. QuadrigaCX, for instance, has been the subject of a major international investigation and accounting audit with a move by victims to exhume the supposedly deceased ex-CEO's body being the most recent development.

Some in the cryptocurrency community have tried to pin major downward moves in cryptocurrency markets on the PlusToken scam, which CipherTrace reported in the Q2 2019 Cryptocurrency Anti-Money Laundering report. Based on extensive research, CipherTrace stated that "unlike similar cryptocurrency frauds, it is not clear that insiders made off with the loot." Despite the mystery still surrounding the scam, some people claim to have traced the perpetrators dumping large blocks cryptocurrency during Q4.

Another key trend is the increasingly intertwined nature of banking and virtual assets. In Q4 2019, CipherTrace Labs released results of a major study that found almost all the top 10 U.S. retail banks have illicit cryptocurrency MSBs—including crypto exchanges—transmitting funds on their payment networks. Analysis further revealed that a typical large U.S. bank processes billions annually in undetected cryptocurrency-related transfers. These clandestine operations create AML compliance risks because criminals must find ways to launder ill-gotten crypto profits.

All of the top 10 U.S. retail banks have illicit cryptocurrency MSBs—including crypto exchanges—transmitting funds on their payment networks.

Source: CipherTrace Labs

The pervasive and often unnoticed presence of crypto assets in financial systems exposes banks to anti-money laundering (AML) and counter terror financing (CTF) compliance risks. In fact, CipherTrace research found that banks globally paid more than US\$6.2 billion in AML fines in 2019.

AML/CTF compliance is not the only risk related to lack of visibility into crypto assets in customer accounts and payment networks. It also opens banks to possible enforcement actions for failing to abide by economic and trade sanctions imposed on rogue nations such as Iran and North Korea. These sanctions are strictly enforced under U.S. law by the Treasury Department's Office of Foreign Assets Control (OFAC). 2019 saw some ground-breaking enforcement actions by OFAC, such as sanctioning individual addresses and publishing the names of the owners.

OFAC takes non-compliance as a serious risk to national security, and it can impose criminal fines of up to US\$20 million, depending the offence, not to mention prison sentences as long as 30 years. Civil penalties for violating the Trading with the Enemy Act can reach up to US\$65,000 for each violation.

OFAC takes non-compliance as a serious risk to national security, and it can impose criminal fines of up to US\$20 million, depending the offence, not to mention prison sentences as long as 30 years.

Darknet marketplaces represent another threat vector for banks. CipherTrace research reveals that 64% of dark market vendors sell compromised bank accounts and stolen financial products. Additionally, darknet marketplaces made it extremely easy to obtain off-the-shelf ransomware for as little as US\$4.99 for the malware. Additionally, the research found that 97% of the ransomware cataloged in 2019 requested payment in bitcoin. BTC is well-suited as a payment rail for ransomware crimes as it is the easiest cryptocurrencies to convert to fiat. Bitcoin is also relatively easy to obtain compared to other coins.

On the regulatory front, one of the key issues percolating through the cryptocurrency community in the fourth quarter of 2019 was a move officially announced at the end of Q2. In June, the global anti-money laundering watchdog, the Financial Action Task Force (FATF), updated its guidance to member nations to include what has since become known as the “Travel Rule.” Among other new guidelines, the Travel Rule is designed to reduce what the FATF sees as a growing threat of money laundering and terror financing. The new funds Travel Rule requires VASPs to share and store sender (originator) and receiver (beneficiary) information.



The new FATF funds Travel Rule requires VASPs to share and store sender (originator) and receiver (beneficiary) information of the participants prior to processing virtual asset transactions.

Moreover, in May 2019, the US Treasury’s Financial Crimes Enforcement Network (FinCEN) clarified its guidance to categorize VASPs as financial institutions, or money service businesses (MSBs) in FinCEN parlance, which means they must now comply with the long-standing funds Travel Rule under the U.S. Bank Secrecy Act (BSA). This clarification means banks must also comply with the know-your-VASP requirement when customers transact with these entities.

During Q3 and Q4, cryptocurrency exchanges and other VASPs struggled to come to grips with this harsh new regulatory reality. Concerns immediately arose in the virtual asset community that complying with the Travel Rule is not only impractical given current blockchain technology but also antithetical to the original pseudonymous nature of cryptocurrencies.

Nonetheless, at the time of this report’s publishing, exchanges and financial institutions have less than six months to find a solution for dealing with this major compliance conundrum. In other words, they must quickly find a way to fulfill these new information sharing obligations while at the same time protecting user privacy—and all at the speed, scale and cost-effectiveness required by VASPs. Among other potential solutions, CipherTrace launched the Travel Rule Information Sharing Architecture (TRISA), and released it to the community as open source. As of January 2020, several VASPs have already begun to integrate and test the solution.

During 2019, cryptocurrency exchanges and other VASPs in the 28 member states of the European Union (EU) have also been facing another major set of new regulations. The 5th Anti-Money Laundering Directive, variously referred to as 5AMLD and AMLD5, came into force on January 10, 2020. Partly prompted by the terror attacks in France, the new regulations represent a bid to make fiat-to-crypto transactions more transparent, while making AML/CTF 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 VASPs may face fines up to €200,000. In reaction, some exchanges have opted to move their operations out of the EU.

It is worth noting that the totals in this report for Q4 frauds and scams, and for the full year, do not include any losses from two very widely publicized and extremely costly financial frauds.

The first is the OneCoin scam. This Ponzi scheme has been widely covered by the world press because in the end it may rank as the largest financial fraud in history. Although U.S. prosecutors have alleged the scam raked in approximately US\$4 billion, some have said it may top even Bernie Madoff's US\$19.4 billion Ponzi scheme. The disappearance of Dr. Ruja Ignatova, a co-founder of the Bulgaria-based company—whose disappearance was chronicled in the popular BBC podcast series *The Missing Crypto Queen*—only fueled the fever in the press. While OneCoin was promoted as a new digital currency with a private blockchain, CipherTrace chose not to include it in this report's total because it lacks two important characteristics of a true cryptocurrency like Bitcoin. For example, there was no virtual assets (tokens) nor blockchain technology behind the scheme.

The second involves a worldwide fraud pulled off by the BitClub Network (BCN). The BCN promoters solicited money from investors in exchange for shares of pooled investments in cryptocurrency mining, and as is typical of a Ponzi scheme, they also rewarded existing investors for recruiting new investors. Unfortunately, the BitClub Network never actually owned any pools. In early December, U.S. authorities arrested the firm's leadership—who according to the indictment had referred to their investors as "dumb," "sheep," and "idiots"—for operating the US\$722 million Ponzi scheme. CipherTrace researchers chose not to include this in our totals for cryptocurrency crime and fraud because it did not involve an actual token or ICO.

Had these scams been included, the totals in this report would be dramatically higher.

Q4 and Full Year 2019 Highlights

- Total of cryptocurrency-related frauds and thefts stands at a staggering US\$4.5 billion including:
 - US\$370.7 million lost in exchange thefts and hacks and
 - US\$4.1 billion of losses stemming from fraud and misappropriation of funds.
- 66% of dark market vendors sell stolen payment products, with compromised accounts sometimes selling for as low as 1% of the account balance.
- Banking and cryptocurrency increasingly intertwined as 8 out of 10 U.S. retail banks harbor illicit crypto MSBs.
- 97% of ransomware uses BTC as the payment rail.
- FinCEN, CFTC, and SEC clarified areas of authority in joint statement as U.S. Congress works to codify which agencies regulate and enforce the various blockchain regulations.
- IRS for the first time asks taxpayers to list their cryptocurrency earnings on tax form.
- Largest Russian dark market launches ICO to fund Western expansion.

Major Trends and Developments

Banking and Virtual Currencies Are Increasingly Intertwined

The benefits of distributed ledger technology and cryptocurrency have been widely promoted over the last year. These include everything from stablecoins bringing approximately 2 billion of the world's unbanked into the financial system to blockchain-based clearing making credit derivative trades safer and more efficient. While some banks have embraced virtual assets based on their many benefits and enormous revenue potential, many banks continue to shy away from them for various reasons.

However, like them or not, crypto assets have become pervasive in the global financial system. They are also increasingly intertwined with traditional banking businesses. And still, cryptocurrency related transactions often go unnoticed in bank accounts and payment networks.

Why it Matters: Banks Unknowingly Sending Fiat to VASPs Causes Exposure to Money Laundering Risks

As more mainstream consumer and institutional investors embrace cryptocurrencies, it becomes increasingly difficult, if not impossible, for traditional financial services firms to avoid entanglements with the crypto economy. For example, significant counter-party risks stem from customers interacting with dicey crypto exchanges. Other risks include:

- Sending and receiving money to and from a virtual asset service provider (VASP) without knowing it.
- Hosting illicit money service businesses.
- Sending money to OFAC sanctioned entities, individuals, and blockchain addresses.
- Unwittingly facilitating terrorist financing.

Not having an effective and automated way to assess the relative riskiness of VASPs causes many banks to turn away potentially lucrative customers. In so doing, they also inadvertently risk forcing crypto firms to hide their transactions as well as the true nature of their businesses. In doing so, they create multi-billion-dollar blind spots that prevent banks from fully assessing and understanding their AML compliance risk exposure. This lack of visibility into crypto assets also opens them to the risk of failing to meet their BSA obligations.

Furthermore, when banks turn away viable virtual asset businesses there is a detrimental effect on the blockchain economy. Once rejected by banks, these businesses may turn to dicey alternatives such as, for example, the Panamanian payment processor previously mentioned in this report.

Meanwhile, some banks are striving to improve their ability to detect and react to hidden crypto asset risks by using open source tools to examine the public blockchain. But these tools often lack the intelligence (including risk ratings on crypto exchanges around the globe) necessary to perform anything but bare bones analysis. Forward-looking banks are starting to lower their AML/CTF exposure by using specialized tools built to identify risky virtual asset service providers and other compliance risks stemming from crypto asset businesses.

New Research Finds 8 out of 10 U.S. Retail Banks Harbor Illicit Crypto MSBs

Highlighting another concerning trend, extensive research by CipherTrace Labs in 2019 uncovered individuals operating illicit crypto MSBs at 8 of 10 U.S. retail banks. These illegal MSBs use their bank accounts as a conduit for accepting cash payments in exchange for crypto to support the illegal trade of fiat for crypto. They often do this by a simple wire transfer or walkup cash deposits at a depository institution. Many banks and other regulated financial institutions unwittingly provide a conduit for these illegal transactions.

CipherTrace researchers and government agencies are increasingly finding people who register businesses online using fictitious or stolen IDs to create corporate entities. They then create corporate bank accounts that can be used to fund investments or operate unlicensed money service businesses. Naturally, they fail to report these crypto asset activities to the financial institution. Criminals and terrorists choose this technique because direct deposits and large sums of money moving in and out of business bank accounts—as opposed to personal accounts—are less likely to trigger fraud alerts or suspicious activity reports (SARs) at financial institutions.

Banking and Cryptocurrencies Are Increasingly Intertwined.

\$2B Annual crypto-related transactions on top 10 bank payment networks

65% of the top 120 VASPs lack good KYC

10 OF 10 TOP US RETAIL BANKS have consumers or small businesses transacting with VASPs

8 OF 10 of the top us banks **Unknowingly** harbor illicit MSBs

66% of payments sent internationally by US exchanges to other VASPs

Source: CipherTrace Labs

Figure 2

CipherTrace analysts have also uncovered numerous peer-to-peer (P2P) marketplaces that are specifically designed to help people buy and sell bitcoin and other virtual currencies. They facilitate the transfers from any bank that allows for walk-up cash deposits into business accounts. To conceal their illegal MSBs, buyers of bitcoin on these P2P marketplaces are told not to inform bank tellers that they are making deposits for the purchase of BTC, but rather are purchasing “digital services.” Similarly, for wire transfers, customers looking to buy bitcoin are directed to avoid mentioning bitcoin in any communication. These P2P exchangers don’t want their banks to catch wind of their underground money service businesses.

In addition to being unregistered, many of these P2P exchangers lack any kind of AML program and perform little or no know your customer (KYC) due diligence. This lack of controls presents huge AML risks to banks and other financial institutions.

In the case of Europe, CipherTrace Labs research revealed that only 5 out of the 10 top banks harbored illicit MSBs. While this trend may appear to be less prevalent in the EU than the U.S., it is important to note that, with the advent of the AMLD5, much of the EU is only now beginning to regulate cryptocurrency exchanges. The ability to go around regulated exchanges that have strong KYC is one thing that entices criminals to work through P2P exchangers instead. As a result, European banks may see an uptick in illicit crypto MSBs clandestinely operating in their payment networks as more exchanges become AMLD5 compliant.

Illicit Crypto Merchants

In addition to illicit cryptocurrencies MSBs, CipherTrace research also uncovered illicit crypto merchants operating the financial system. These merchants sell crypto either directly or in partnership with high-risk exchanges. These transactions are often obfuscated by intentionally using incorrect merchant category codes (MCCs) to hide the fact that they are engaging in crypto-asset transactions. All cryptocurrency transactions involving credit or debit cards should be processed under the correct MCC 6051.

Banks Received US\$6.2 Billion in AML Fines During 2019

Regulators levied US\$6.2 billion in AML fines on banks globally in 2019. This large number perhaps foreshadows even larger fines as FinCEN, as it has stated, gets more serious about crypto related enforcing new regulatory regimes—and as AMLD5 and FATF become codified in local laws of EU and G20 nations. The average fine was US\$443.6M, with the largest fine standing US\$5.1B. Removing the US\$5.1B outlier leaves a trimmed mean of US\$85.4M.

Research Reveals That Two-Thirds of Dark Market Vendors Sell Stolen Payment Products

CipherTrace research also found that 66% of the products and services offered by dark web vendors throughout 2019 comprised stolen payment products from compromised financial institutions. The breakdown included 40% coming from stolen bank account or credit card credentials and 24% coming from compromised payment services accounts, and 2% coming from compromised private keys. The remaining 34% was distributed among other illicit products and services as shown in Figure 3. CipherTrace research found that some compromised accounts can sell for as little as 1% of the balance on the accounts, as seen in figure 4.

2019: Over 66% Darkweb Vendors Offered Stolen Financial Products



Source: CipherTrace Cryptocurrency Intelligence

Figure 3 Stolen financial products dominate the dark markets that means risks of payment fraud for banks.

While most of these goods and services are offered on darknet marketplaces which often house hundreds of different vendors, 2019 has seen dark markets beginning to focus on smaller, single-vendor shops (aka Dark Vendors). This has likely resulted from the recent rash of darkmarket takedowns—as discussed in the 2019 Q2 CAML Report—as well as a series of DDoS attacks that have since hit the more prominent marketplaces.

Compromised Bank Accounts For Sale on Dark Markets

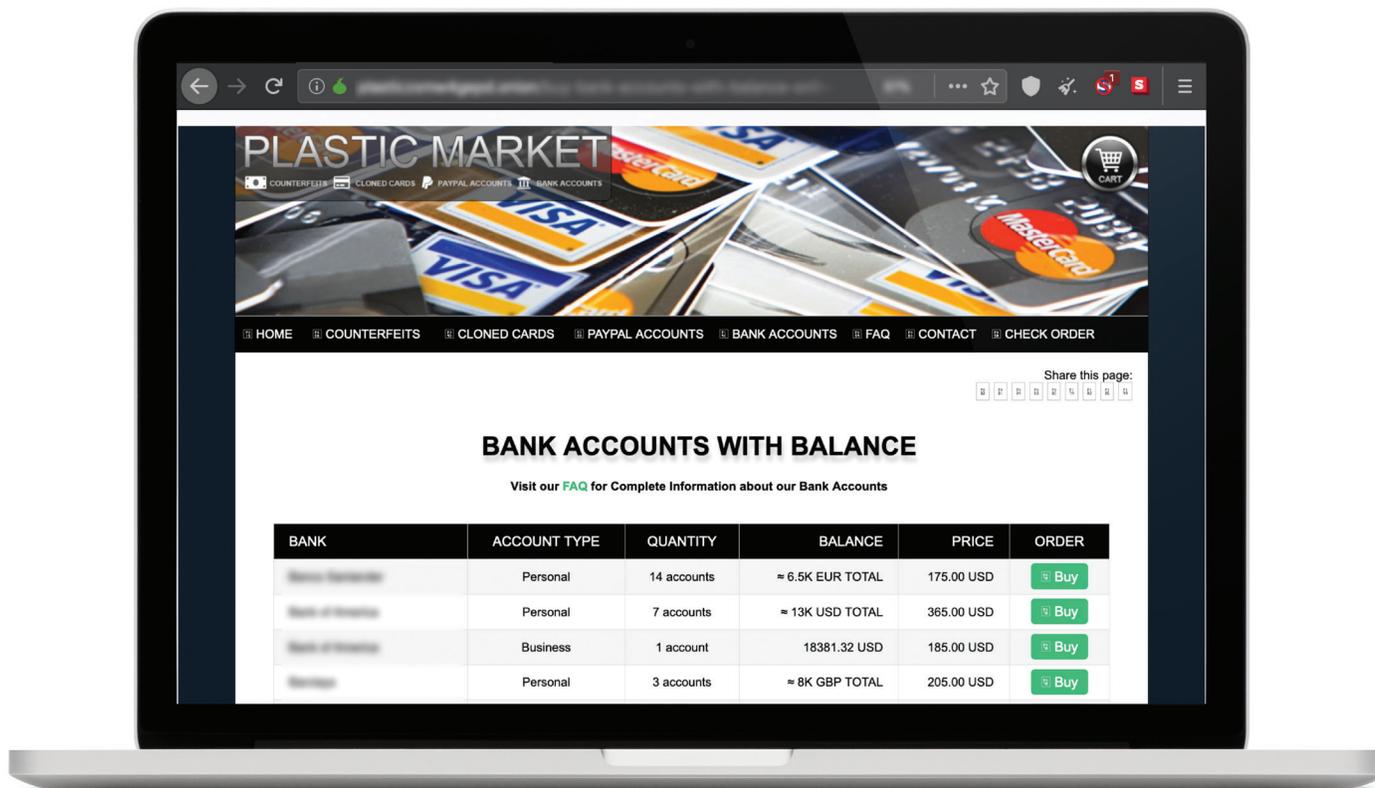


Figure 4 2019 witnessed surge in suppliers of payment fraud products, which are all paid for in cryptocurrency.

According to Europol's 2019 Internet Organised Crime Threat Assessment (IOCTA), "There are increases in single-vendor shops and smaller fragmented markets on Tor, including those catering for specific languages. Some organised crime groups (OCGs) are also fragmenting their business over a range of online monikers and marketplaces, therefore presenting further challenges for law enforcement."

97% of Ransomware Uses BTC as the Payment Rail

According to the same Europol IOCTA assessment, ransomware "clearly and overwhelmingly retains its position as the top cyber threat faced by European cybercrime investigators," and was the second most prominent cyber threat facing the private sector. Ransomware can be state sponsored, as the world saw with the massive North Korean Wannacry attacks in 2017, or simply bought off the dark web for as little as US\$4.99 according to CipherTrace dark market research. And the exploit kits that allow bad actors to inject the malware sells for even less.

Ransomware for Sale

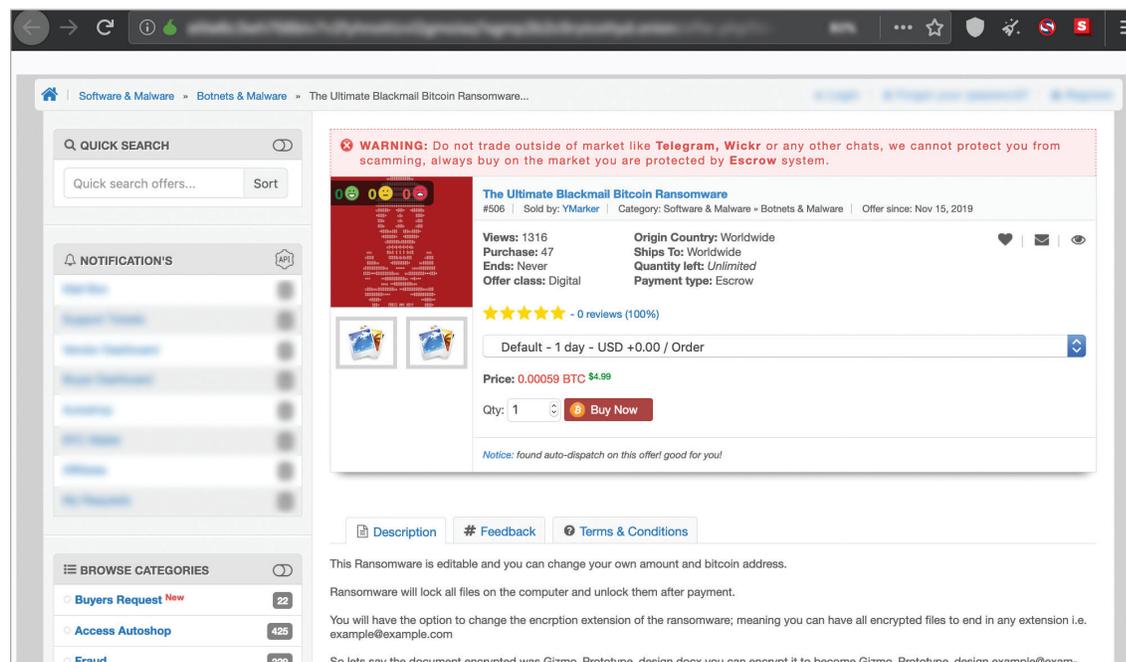


Figure 5 Cyber criminals can malware off the dark web for as little US\$4.99 paid in bitcoin.

CipherTrace researchers also found that, of all the ransomware cataloged in 2019, 97% of attacks demanded payment in BTC, while 1.8% accepted DASH, 0.9% asked for ETH, and 0.3% requested LTC. While some coins like DASH have optional privacy-enhanced features that could be beneficial for obfuscating stolen funds received from ransomware payments, bitcoin still appears to be king among criminals. BTC's popularity is likely due to its greater accessibility and ease of use in comparison to other cryptocurrencies and privacy coins.

Even on a ledger as transparent as the bitcoin blockchain, following the money from a ransomware attack can prove difficult. However, given the proper tools it is not impossible. Figure 6 shows an example of the path several transactions from the Wannacry ransomware wallets took before making their way to fiat off ramps.

While the routes may have many twists and turns as the criminals attempted to obfuscate the source of funds, CipherTrace was able to track the transactions to several exchanges that engage in fiat-to-crypto trading.

Depending on the AML compliance protocols of the exchanges, the funds should have been recognized as originating from these Wannacry wallets and immediately frozen. This highlights the importance fiat-to-crypto exchanges can play in keeping the crypto economy safe when proper AML compliance protocols are in place.

Unlike the banking industry, the immutability and transparency of blockchain in the crypto sphere allows for businesses with the proper tools to easily see the risks associated with any address. This holds true whether the transaction involves one, two, five, or even more hops away from a dark market vendor or ransomware wallet.

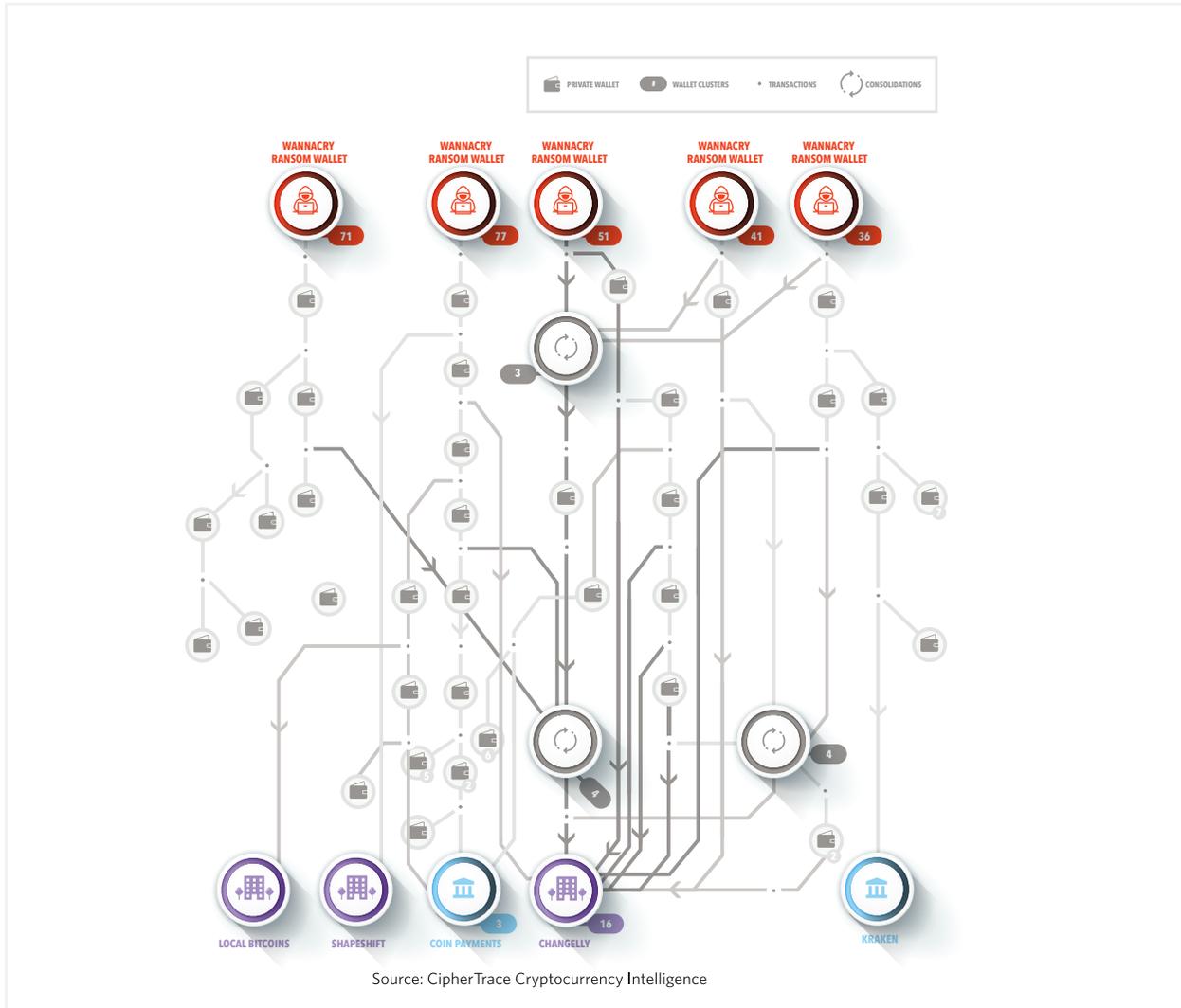


Figure 6 Tracing the Flow of North Korean Ransomware to Money Mixing Services.

CipherTrace tracked funds from 280 North Korean ransomware wallets through numerous transactions, which then consolidated flowed into mixers and risky exchanges before seeking and off ramp into fiat. This clearly demonstrates how banks and exchanges can not only avoid compliance risks but also help to reduce eCrime by deploying advanced blockchain forensics tools.

Thefts, Scams and Fraud

Canadian Einstein Exchange Lost US\$12 Million

A November 18 British Columbia Supreme Court filing revealed Vancouver-based Einstein Exchange—which was shut down on November 1 amid allegations that it owes its clients up to US\$12 million—had only about US\$34,000 in crypto and fiat assets remaining.

The B.C. Securities Commission (BCSC) took this action after investigating numerous complaints from customers who were unable to access their fiat or crypto assets. The Supreme Court of British Columbia assigned Grant Thornton Limited as the receiver to seize Einstein's assets and return the allegedly missing funds to clients.

Although most of Einstein's assets were made up of cryptocurrency, according to a November 18 Supreme Court filing, "a very limited review of Einstein Groups' books and records" revealed all that remains are about US\$11,000 in cryptocurrency assets and US\$23,000 in fiat—a far cry from the US\$12 million it owes customers. Einstein has informed Grant Thornton that it estimates its clients are owed between US\$6 million and US\$7.5 million and not the US\$12 million the BCSC had calculated.

The BCSC has been investigating the platform since May 2019 amid customer complaints and potential money laundering concerns coming from within the company, according to an affidavit issued by investigators. On October 9, the BCSC demanded to see evidence of where the exchange was holding its crypto assets. Einstein told the BCSC that they had planned to shut down in 30 to 60 days after negotiations to sell the business to a U.S. company collapsed. However, Einstein still claimed to have sufficient crypto assets on hand to satisfy withdrawal requests.

To verify this claim, on October 31, BCSC asked Einstein's lawyers to tell them where the fiat and cryptocurrency balances were kept. Einstein's counsel responded by claiming they no longer represented Einstein. The next day, the BCSC ordered the Einstein exchange to cease all operations. According to Einstein CEO Micheal Gokturk's testimony regarding the funds, most of their funding was stored via crypto assets. Gokturk had used both hardware wallets and other cryptocurrency exchanges to store Einstein funds.

It is still unclear what happened to the missing funds, but the BCSC says it plans to continue its investigation.

IDAX Exchange Experiences Withdrawal Issues After CEO Disappears

On November 28, after experiencing withdrawal problems, the China-based IDAX exchange announced that it had lost contact with its CEO, Lei Guorong, along with access to its cold storage.

The official announcement states, "IDAX Global CEO have gone missing with unknown cause and IDAX Global staffs were out of touch with IDAX Global CEO. For this reason, access to Cold wallet which is stored almost all cryptocurrency balances on IDAX has been restricted so in effect, deposit/withdrawal service cannot be provided." The announcement came four days after the company said it would no longer provide services for users in China due to an official policy that makes exchanges illegal in the country. IDAX has since recommended that all users "refrain from using our all [sic] platform services."

Guorong's disappearance quickly led to speculation of another possible Quadriga-esque exit scam as the company's statements revealed that IDAX was also being controlled by a single person, as in the case of QuadrigaCX, who held all the private keys. It is currently unclear how many crypto assets were held in cold storage, or if any still remain.

Upbit Hack Costs 342,000 ETH Worth \$52 Million USD

In a November 27 post to their website, Upbit CEO Lee Seok-woo announced that the exchange was hacked for 342,000 ETH (approximately US\$52 million at the time). The Ethereum was moved from the company's hot wallet to 0xa09871AEadF4994Ca12f5c0b6056BBd1d343c029. In response, the company transferred all cryptocurrencies in their hot wallet to cold wallet storage, and stated they will cover any stolen customer funds with Upbit assets.

On December 3, one of the addresses where the hacker was storing the stolen ETH began to show signs of life as eight transfers to four different addresses occurred between December 3 and December 6. On December 23, the address sent an additional 2,000 ETH to a new address. CipherTrace will continue to monitor the situation for signs of movement into any exchanges, where the funds can be frozen and returned to Upbit. Some exchanges, such as Binance, have already pledged to ensure any hacked funds will be immediately frozen if they enter their exchanges.

QuadrigaCX Update – Victims Demand Authorities Exhume Former CEO's Body

As an update to the unfortunate QuadrigaCX saga, on December 13 the defunct exchange's victims demanded the exhumation of the recently deceased QuadrigaCX founder, Gerald Cotten. He mysteriously died while on honeymoon in India, taking the private keys and access to all the exchange funds with him. The victims' lawyers claim that the publicly available information related to the situation highlights the need for certainty on whether Cotten is in fact deceased, and what the cause of death was, especially given the questionable circumstances. Given decomposition concerns, the law firm has requested the process be completed by spring.

Near Crypto Crimes

BitClub Network – Four Arrested in US\$722 Million “Cryptocurrency Mining” Ponzi Scheme

On December 10, three men were arrested in the US in connection with a cryptocurrency mining scheme that defrauded investors of US\$722 million. A fourth was arrested in Germany soon after, and a fifth remains on the run.

From April 2014 to December 2019, the defendants operated BitClub Network—a Ponzi scheme that solicited money from investors in exchange for shares of purported cryptocurrency mining pools. Investors were encouraged to recruit new investors, with their website reading “earn daily profits from all of the Bitcoin being earned by your entire team.” BitClub Network provided false and misleading figures that were purportedly generated by the BCN bitcoin to its investors. According to the indictment, BitClub Network never owned any pools and email between BCN leadership called investors “dumb” and “sheep,” and claimed BCN was built “on the backs of idiots.” According to U.S. Attorney Carpenito, “What they allegedly did amounts to little more than a modern, high-tech Ponzi scheme that defrauded victims of hundreds of millions of dollars.”

NOTE: As it appears the perpetrators never actually mined any cryptocurrency, this Ponzi/pyramid scheme was not included this report’s Thefts, Hacks, and Scams total.

OneCoin – Widely Publicized Faux Cryptocurrency Ponzi Scheme

As of November 30, the website for “cryptocurrency” Ponzi scheme OneCoin has gone offline—nine months after the US authorities indicted one of its founders for the multibillion-dollar financial fraud.

According to the March 8th indictment, Konstantin Ignatov was arrested for his role as leader of international pyramid scheme that involved the marketing of a fraudulent cryptocurrency called “OneCoin.” The indictment also charged Konstantin’s sister Ruja, the original leader of OneCoin, aka the “Crypto Queen.” Ruja’s whereabouts are currently unknown, and Konstantin is actively working with authorities to find her. The indictment claims OneCoin’s faux cryptocurrency defrauded investors out of billions of dollars worldwide.

NOTE: Because OneCoin is not a real cryptocurrency, attached to any blockchain, CipherTrace considers this a “near crypto crime and thus it has not been included this report’s Thefts, Hacks, and Scams total.

Potential Blockchain Vulnerabilities

Maker DAO Vulnerability Could Have Frozen \$100M DAO

On May 9, security audit firm Zeppelin released a disclosure outlining how their discovery of a Maker DAO contract vulnerability that could have been used to move user tokens and lock them permanently within the MakerDAO voting contract, effectively freezing \$100 million worth of MKR tokens. In partnership with Coinbase and Zeppelin, the Maker Foundation had participated in a round of audits for the Maker Voting Contract between April 22 and 26, when the vulnerability was first discovered. The MakerDAO team was informed immediately and has since patched the vulnerability.

The audit was contracted by Coinbase as part of the company's due diligence process to support the MakerDAO voting capability within the Coinbase Custody product, according to a Coindesk interview with Alan Leung, head of security for Coinbase Custody. Now that the vulnerability has been patched, Leung affirmed Coinbase's continued intention to launch MKR voting capability on Coinbase Custody.

MimbleWimble Transaction Privacy Proven Vulnerable

Mimblewimble—a privacy protocol currently being considered for integration by Litecoin—has currently captured the spotlight for potential security flaws. On November 18, Ivan Bogatyy, a venture capitalist with Dragonfly Capital, published a report that revealed a security flaw in MimbleWimble's privacy model that allowed him to trace 96% of all Grin transaction sender and recipient addresses in real time.

According to Bogatyy, "The problem is inherent to Mimblewimble, and I don't believe there's a way to fix it. This means Mimblewimble should no longer be considered a viable alternative to Zcash or Monero when it comes to privacy." While the exploit does not allow attackers to determine the amounts that people are exchanging, Bogatyy claims it does reveal who paid whom.

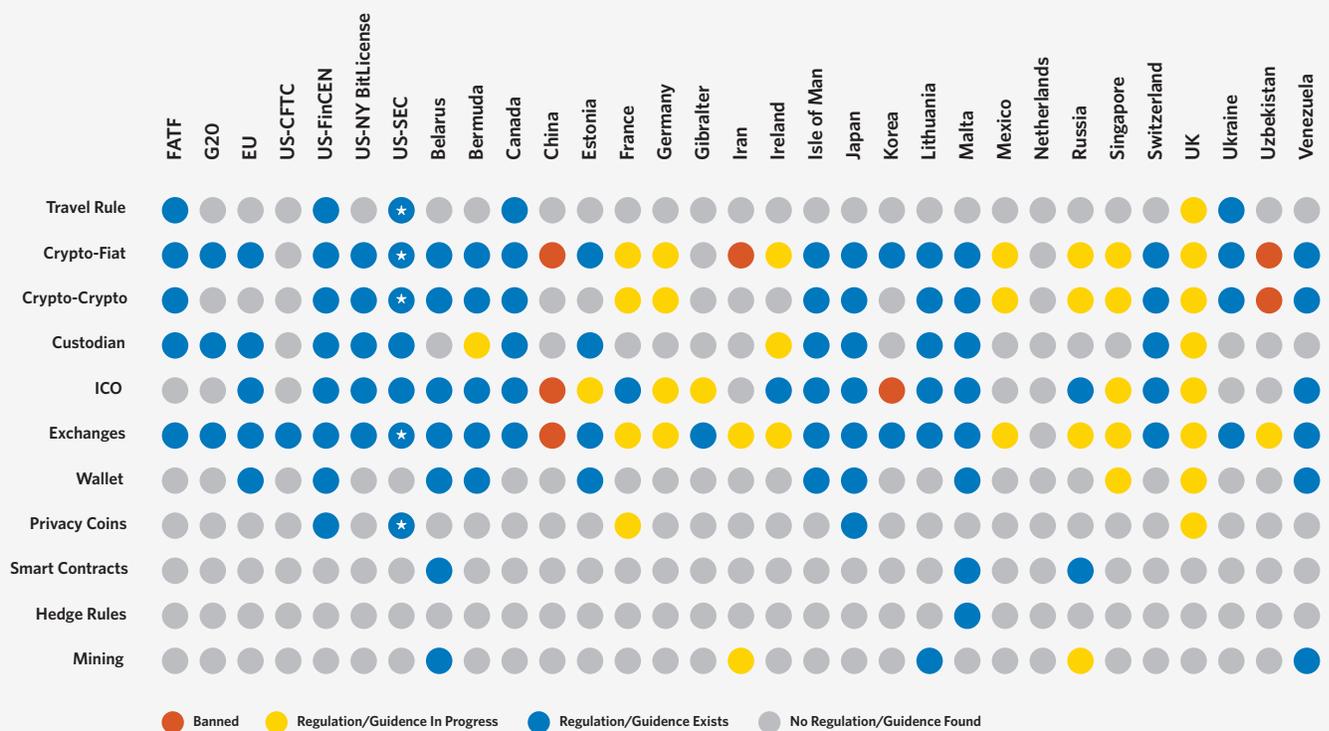
The creator of Litecoin, Charlie Lee, responded to Bogatyy on Twitter, stating "this limitation of MimbleWimble protocol is well known. MW is basically Confidential Transactions with scaling benefits and slight unlinkability. To get much better privacy, you can still use CoinJoin before broadcasting and CJ works really well with MW due to CT and aggregation." On December 11, Grin, the privacy coin based on MimbleWimble, responded to Bogatyy's claims in a Medium article stating the Mimblewimble attack is "factually inaccurate" and could not link identities to addresses.

Changes in the Global Regulatory Environment

The State of Cryptocurrency Anti-Money Laundering Legislation

Figure 7 shows the widely varying levels of maturity and sophistication in AML/CTF regimes around the globe. The gaps in these regulations present risky avenues that can be exploited by money launderers and terrorist organizations. Specifically, the money laundering risks of crypto-to-crypto exchanges, privacy coins, and anonymizing services are not well addressed by lawmakers attempting to regulate blockchain technology assets based on the physics of fiat currency.

Current Implementation of AML/CTF Regulations Globally



Source: CipherTrace Cryptocurrency Intelligence
 * If securities are traded

Figure 7

Which US Agencies Regulate and Enforce Regulation on Blockchain Entities and Activities

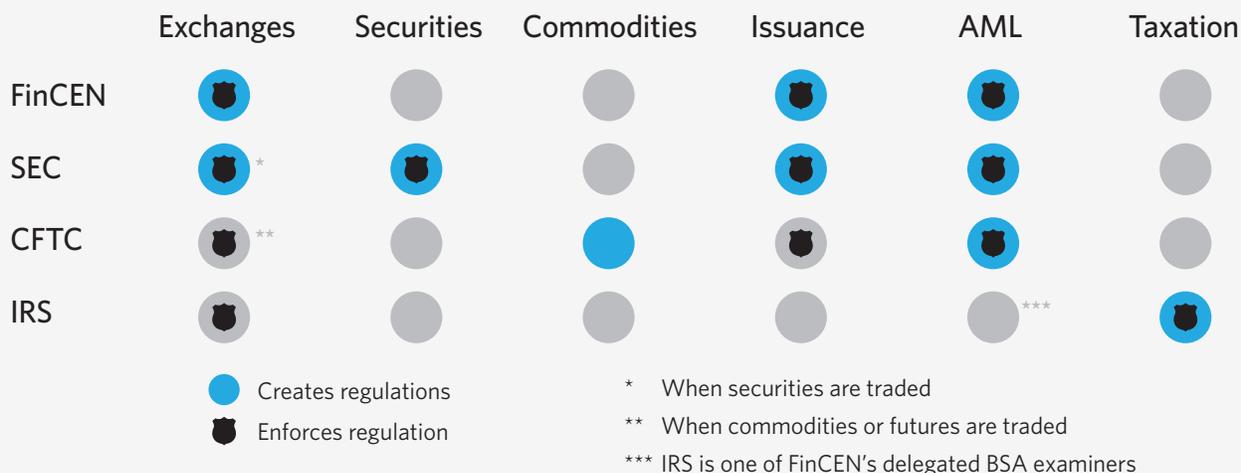


Figure 8

Leaders of FinCEN, CFTC, and SEC Clarified Areas of Authority

On October 11, FinCEN, the Commodity Futures Trading Commission (CFTC) and the Securities and Exchange Commission (SEC) issued a joint statement to remind persons engaged in activities involving digital assets of their AML/CFT obligations under the BSA. This clarification includes MSBs as defined by FinCEN, futures commission merchants, and introducing brokers obligated to register with the CFTC and broker-dealers and mutual funds obligated to register with the SEC.

The joint statement clarifies the label or terminology market participants use—e.g., “exchange”—is not of primary importance. What matters are “the facts and circumstances underlying an asset, activity or service, including its economic reality and use (whether intended or organically developed or repurposed), that determines the general categorization of an asset, the specific regulatory treatment of the activity involving the asset, and whether the persons involved are ‘financial institutions’ for purposes of the BSA.”

If a person does fall under the definition of a “financial institution,” its AML/CFT obligations under the BSA could be overseen by one or more of these agencies, depending on its activities. For example, a futures commission merchant’s AML/CFT obligations would be overseen by the CFTC and FinCEN, as well as the National Futures Association (NFA). Likewise, a broker-dealer in securities would be overseen by the SEC and FinCEN, as well as the Financial Industry Regulatory Authority (FINRA). Likewise, broker dealers dealing in privacy coins or stable coins would also be regulated by the SEC due to their underlying engagement in the business of trading securities. See Figure 8.

Basel Committee on Banks' Crypto-Asset Risk Exposure

The Basel Committee on Banking Supervision (BCBS) acts as a global standard setter for the prudential regulation of banks. Its 45 members comprise central banks and bank supervisors from 28 jurisdictions. The Committee seeks the views of stakeholders on a range of issues related to the regulatory treatment of crypto-assets, including:

- Features and risk characteristics of crypto-assets that should inform the design of a prudential treatment for banks' crypto-asset exposures
- General principles and considerations to guide the design of a prudential treatment of banks' exposures to crypto-assets, including an illustrative example of potential capital and liquidity requirements for exposures to high-risk crypto-assets

In a statement released in March 2019, the BCBS provided guidance to financial institutions about the dangers it believes crypto assets pose to the global financial system. It also detailed steps banks need to take to manage exposures to this new asset class.

In its initial statement, the BCBS cautioned banks about acquiring exposures to crypto-assets or providing related services, saying "the continued growth of crypto-asset trading platforms and new financial products related to crypto-assets" could raise concerns about financial system stability. In addition to extreme price volatility, the committee claimed cryptocurrencies specifically pose liquidity, credit, market, and operational risks, including fraud and cyber risks. It further cited money laundering and terrorist financing risks as well as legal and reputational risks.

These findings are especially significant because compliance with the U.S. Bank Secrecy Act (BSA) funds Travel Rule requires financial institutions to clearly identify the MSBs with which they transact. Based on new FATF guidance, governments around the world are required to enact a similar rule by June 2020. Nonetheless, most banks are currently ill-equipped to identify and monitor cryptocurrency exchanges and other virtual asset service providers as MSBs, which is required under these two Travel Rules.

While the BCBS believes banks have limited crypto-asset exposure, the discussion paper seeks clarity on one question: "Are there additional channels other than those listed above by which banks could be directly or indirectly exposed to crypto-assets?"

This is especially significant since compliance with the (BSA) funds Travel Rule requires financial institutions to clearly identify the MSBs they facilitate, a topic not covered by the Discussion Paper. With the large number of hidden crypto transactions coming to and from banks, CipherTrace research demonstrates that most banks are ill-equipped to identify and monitor cryptocurrency exchanges and other virtual asset service providers as MSBs, which is required under the BSA as well as new FATF guidance that will soon become law in G20 nations.

Joint Statement by the EU Council and the Commission Regarding Stablecoins

A December 5 press release by the EU Council and the Commission stated that, although stablecoins may present opportunities in terms of cheap and fast payments, they also pose multifaceted challenges and risks related to:

- Consumer protection
- Taxation
- Operational resilience
- Terrorism financing
- Governance
- Privacy
- Cyber security
- Money laundering
- Market integrity
- Legal certainty

These risks are amplified when the stablecoin has the potential to reach a global scale—as would be the case with Facebook’s Libra—posing potential risks to monetary sovereignty, monetary policy, and overall financial stability.

Despite these risks, the Council and Commission also reaffirmed their willingness to appropriately tackle the challenges raised by stablecoins, as long as they don’t “undermine existing financial and monetary order as well as monetary sovereignty in the European Union.”

The statement further goes on to emphasize that no global stablecoin should begin operating in EU until all legal, regulatory and oversight challenges and risks have been adequately identified and addressed.

US – IRS Increases Focus on Cryptocurrencies

While FinCEN may set AML regulations for crypto-asset MSBs, the IRS examines VASPs to ensure they are in compliance. Recent developments show the IRS is increasing its interest in the blockchain sphere. For example, a question at the top of the 2019 Form 1040 for Additional Income reads, “At any time during 2019, did you receive, sell, send, exchange, or otherwise acquire any financial interest in any virtual currency?” While at first glance this may appear to simply be a sign that the IRS will begin to monitor cryptocurrency trading gains more closely, the overall role of the IRS in enforcing AML compliance may provide insight into where their focus will be in 2020. The “Internal Revenue Service Progress Update Fiscal Year 2019” report also names crypto as a new and emerging compliance area that requires attention and affirms cryptocurrency “will remain an important focal point for the IRS in 2020.” According to a December 5 Accounting Today interview with IRS Criminal Investigation Chief Don Fort, the division expects to hire more agents as it intends to pursue more cryptocurrency-related cases.

SCHEDULE 1
(Form 1040 or 1040-SR)

Department of the Treasury
Internal Revenue Service

Additional Income and Adjustments to Income

► Attach to Form 1040 or 1040-SR.
► Go to www.irs.gov/Form1040 for instructions and the latest information.

OMB No. 1545-0074

2019
Attachment
Sequence No. **01**

Name(s) shown on Form 1040 or 1040-SR _____ Your social security number _____

At any time during 2019, did you receive, sell, send, exchange, or otherwise acquire any financial interest in any virtual currency? Yes No

1 Taxable refunds, credits, or offsets of state and local income taxes 1

2a Alimony received 2a

b Date of original divorce or separation agreement (see instructions) ► _____

3 Business income or (loss). Attach Schedule C 3

Figure 9 As of 2019, the IRS now requires disclosure of any cryptocurrency financial interest.

US – Cryptocurrency Act of 2020

On December 17, a draft of the Crypto-Currency Act of 2020 was introduced in the U.S. Congress. The bill seeks to clarify which Federal agencies regulate which digital assets, and will require those agencies to notify the public of any Federal licenses, certification, or registrations related to each asset.

According to the draft legislation, three agencies are assigned the title “Federal Digital Asset Regulator” or “Federal Crypto Regulator.” These are the CTFC, the SEC, and FinCEN. The proposed legislation also splits digital assets into three categories, each regulated by a different Federal Crypto Regulator. It clarifies enforcement responsibilities as follows: FinCEN oversees cryptocurrencies, while the CFTC monitor crypto-commodities and the SEC has regulatory responsibility for crypto-securities.

While that clarification may not have been news to most people operating in this sphere, the bill also requires the Secretary of the Treasury to issue rules to require each cryptocurrency to allow for the tracing of transactions. This requirement includes “synthetic stablecoins” (stablecoins not backed one-to-one by a reserve).”

US – House Bill Would Classify Stablecoins as Securities

On October 18, the U.S. House of Representatives introduced the “Stablecoins Are Securities Act of 2019” to the House Financial Services Committee. If passed, the bill will amend the statutory definitions of the term security to include “managed stablecoins,” giving the SEC authority over all stablecoins and any stablecoin issuers wishing to deal with U.S. persons.

AMLD5 Effective Across EU after January 2020

The EU's Fifth Anti-Money Laundering Directive (AMLD5) came into force on January 20, 2020. As a result, VASPs and regulators in EU member states will operate under a new regulatory regime that includes the following:

- Crypto-to-fiat exchanges and custodian wallet providers must comply with relevant AML/CFT requirements under AMLD4.
- Crypto-to-fiat exchanges and custodian wallet providers must be registered.
- "Competent authorities" can monitor the use of virtual currencies for the purposes of AML/CFT.
- National Financial Intelligence Units (FIUs) can obtain information allowing them to associate virtual currency addresses to the identity of the virtual currency owner.
- Crypto-to-fiat exchanges and custodian wallet providers must keep customer due diligence (CDD) records for five years after the end of a business relationship or occasional transaction.

Of note, however, crypto-to-crypto controls are not included in AMLD5. As discussed in the CipherTrace Q2 2019 Crypto currency Anti-Money Laundering Report, this constitutes a critical weakness in the effectiveness of AMLD5 in stopping money laundering and terrorism financing. Member states are nonetheless free to adopt stronger regulations.

In order to comply with the Directive, member states are required to make changes to their national legislation if they currently do not comply. If a member state fails to pass AMLD5 laws into its national legislation, the European Commission may initiate legal action against the member state in the European Court of Justice.

In anticipation of AMLD5 enforcement, several crypto-asset and blockchain firms have already shut down. Cryptocurrency mining pool Simplecoin and bitcoin gaming platform Chopcoin, both of which were founded by the same individual, shut down in January 2020, citing upcoming AMLD5 regulations. A notice on Simplecoin's website read, "When the laws come into effect, we would be forced to require you, the users, to identify yourselves for anti-money-laundering purposes. Mining should be available to anyone and we refuse to jeopardize our users' privacy."

However, miners are not "obliged entities" under the AMLD5. "When we look at the key players in cryptocurrency markets, we can see that a number of those are not included in AMLD5, leaving blind spots in the fight against money laundering, terrorist financing and tax evasion," concludes the European Parliament's Study on Cryptocurrencies and Blockchain. "The examples are numerous and include miners, pure cryptocurrency exchanges that are not also custodian wallet providers, hardware and software wallet providers, trading platforms and coin offerors. Persons with malicious intent could look up these blind spots."

Germany Adopts AMLD5 Regulation into National Law

A draft bill for the implementation of AMLD5 became effective in Germany on January 1, 2020. According to the bill, crypto-assets now qualify as financial instruments under the German Banking Act (KWG). As a result, any person wishing to provide crypto-related financial services, either commercially or on a scale that requires commercially organized business operations, will need authorization from the Federal Financial Supervisory Authority (BaFin)—Germany’s financial regulatory authority.

The bill also introduced an “exclusive” licensure requirement for crypto custody businesses, which means firms that are already authorized to provide financial or banking services cannot apply for an additional license covering a “crypto custody business.” Instead, firms must separate such business from their other financial service or banking business.

While this licensure requirement goes beyond what is technically required to fulfill AMLD5 obligations—AMLD5 simply lays out the minimum requirements for compliance—stricter national regulations are still possible. A similar expansion on AMLD5 regulations was seen in the UK’s adoption of AMLD5 regulations in Q2, where, in addition to fiat-to-crypto exchanges, its national law also included crypto-to-crypto exchanges, P2P exchanges, and bitcoin ATMs.

Current custodian businesses must announce their intention to get a license before April 1, 2020, and submit an application before November 1, 2020. However, at the time of this report, BaFin has yet to release final regulations around licensure. Many German custodian businesses are allegedly waiting for final regulations before deciding if they intend to apply for a license or not.

Ukraine – New Crypto AML Regulations Based on FATF Guidelines

Ukraine’s legislative body has approved a law based on FATF recommendations for the regulation of VASPs. This includes a new Travel Rule compliance regulation that dictates transactions in excess of 30,000 hriven (approximately US\$1300) will require the transmittal of sender and receiver information as well as verification of the nature of the business relationship.

Binance has been working with the government of Ukraine on its new cryptocurrency AML regulations. Binance CEO Changpeng Zhao (CZ) said in November that the legalization of cryptocurrencies and the adoption of progressive legislation can play a key role in bringing positive growth to the economy. It can also attract additional investments, according to the official announcement on the Binance website.

Russia Enacts New Crypto Law for Smart Contracts

On October 1, Russia enacted the law “On Digital Rights.” This new legislation formally establishes smart contracts and security tokens into Russian civil law. The legislation defines “digital rights” as securities or a set of contractual rights to which a holder is entitled, making the term analogous with security tokens. The law also outlines how users can exercise and transfer these “digital rights.” It requires information systems to be able to identify a digital rights owner as well as the participants of a transaction and to allow reproduction of the terms of the agreement.

Russia - “Crowdfunding” Law Takes Effect

On January 1, 2020, Russia’s law “On Attracting Investments Using Investment Platforms,” also known as the “law on crowdfunding,” came into force. According to the legislation, entities wishing to use investment platforms must register with the Central Bank of Russia (CBR). In addition, to mitigate potential risks, “unqualified investors” are limited by yearly investment caps of 600,000 rubles (US\$9,000). Although the law does not explicitly name Initial Coin Offerings (ICOs), many legal experts agree that the regulations should theoretically apply to ICOs. Nevertheless, getting the CBR to approve an ICO registration may turn out to be easier said than done as the Central Bank of Russia famously supported a crypto ban back in November.

Sanctioned Countries

North Korean Crypto Conferences Help Fortify Regime's Crypto Laundering Efforts

From April 18-25, 2019, North Korea held its inaugural Pyongyang Blockchain and Cryptocurrency Conference. While not much is publicly known about who attended or what was discussed—the official website's agenda simply stated "Blockchain and Crypto Conference" in any time slot referencing the conference—on November 29, the U.S. Attorney for the Southern District of New York and the FBI announced they had arrested and charged one attendee, Virgil Griffith, for violating U.S. economic sanctions laws.

Griffith, an Ethereum research scientist, allegedly travelled to Pyongyang in April after being denied permission by the State Department. Once there, authorities allege he "provided highly technical information to North Korea, knowing that this information could be used to help the DPRK launder money and evade sanctions." At the time of his arrest in 2019, Griffith was a resident of Singapore and was allegedly investigating the possibility of renouncing his U.S. citizenship.

During his speech and in discussions afterward, Griffith provided information about how North Korea could use cryptocurrency to "achieve independence from the global banking system," the complaint claims. He also later made plans "to facilitate the exchange" of a digital currency between North and South Korea.

"In allegedly doing so, Griffith jeopardized the sanctions that both Congress and the president have enacted to place maximum pressure on North Korea's dangerous regime," said U.S. Attorney Geoffrey S. Berman.

Ethereum cofounder Vitalik Buterin defended the 36-year-old American citizen and personal friend in a series of tweets. Vitalik claims he doesn't believe that Virgil actually helped the DPRK in doing anything bad—i.e., he simply delivered a presentation based on public information about open source software, without any "weird hackery (sic) advanced tutoring." Vitalik also claimed, "Geopolitical open-mindedness is a *virtue* [sic]. It's *admirable* [sic] to go to a group of people that one has been trained since childhood to believe is a Maximum Evil Enemy, and hear out what they have to say. The world would be better if more people on all sides did that."

However, it is hard to imagine how blockchain and cryptocurrency technology could help average North Korean citizens because only top party members have access to the global internet. With this in mind, cryptocurrency would be useless to anyone but the regime, providing it with new ways to launder illicit gains and fund its weapons of mass destruction (WMD) and ballistic missile programs. According to an August 2019 U.N. Security Council North Korea sanctions committee report, the DPRK has already raised over US\$2 billion dollars in illicit crypto funds for its WMD program to date.

The DPRK's next conference is slated to take place from February 22 to February 29, 2020. While the conference's official website has since been taken down, an archive of the site shows the conference program is just as cryptic as the previous one, having time slots simply filled with the description "Blockchain and Cryptocurrency conference."

The website also states that any interested person can attend, unless your passport is from South Korea, Japan or Israel, and “to preserve the confidentiality of the participants, foreign and local companies involved,” journalists are not allowed to attend. While the site also claims the regime will not stamp visitors’ passports, sanctions experts at the UN are still warning people not to attend the conference or risk facing penalties for violating sanctions.

Iran – Rouhani Calls for Muslim Cryptocurrency

In a speech given during the opening ceremony of a December 2019 Islamic conference in Malaysia, Iranian President Hassan Rouhani said Muslim nations need their own cryptocurrency to fight against American economic hegemony and cut reliance on the US dollar. US economic sanctions currently limit how Iranian institutions conduct transactions due to their restricted use of the US dollar, the world’s reserve currency. Sanctions coupled with inflation of the Iranian rial has led many in the country to turn to cryptocurrency for relative stability and to keep their financial dealings private.

In September, the financial analytics firm Gate Trade surveyed 1,650 Iranian bitcoiners in Persian Telegram groups and found that 25 percent of them earned US\$500 to US\$3,000 a month from cryptocurrency. This income stream breaks down as follows: 35 percent from mining, 58 percent through trading on regulated exchanges or peer-to-peer marketplaces, and 7 percent from undisclosed sources. Economic sanctions prevent most global exchanges from onboarding or trading with Iranian customers. However, in an interview with CoinDesk, Gate Trade representatives said many Iranians use VPNs and foreign ID cards purchased on the black market to circumvent the KYC policies of global exchanges.

Iran – Crackdown on Illicit Crypto Mining Escalates

On November 13, Mostafa Rajabi, a spokesman of Iran’s Energy Ministry announced a bounty to anyone who discloses illicit mining operations in the country. Rajabi also announced new electricity pricing for crypto miners, charging miners the same price as exported electricity and banning operations during peak consumption hours.

Venezuela – Maduro Continues to Force Petro on Citizens

Thus far, Venezuela’s answer to bitcoin, the petro (PTR), has not been a big hit with the locals. That has prevented Venezuela president Nicholas Maduro from continuing to press citizens and companies to adopt the country’s national cryptocurrency. For instance, in both 2018 and 2019, the Venezuelan regime paid out pensioners’ bonuses for the year in PTR, requiring the citizens to download the petro-app if they wish to receive their funds.

Then on January 14, 2020, Maduro said Venezuela will sell its oil for the petro rather than the U.S. dollar in an attempt to decrease the dollar’s importance in the oil market. The president also decreed that the sale of all fuel sold by Petróleos de Venezuela, S.A. (PDVSA)—Venezuela’s state-owned oil company—for planes operating international routes will now be made in petros.

But even as inflation continues to erode the value of the Venezuelan bolivar, the petro is purportedly still not widely used in the country. This poor adoption may relate to a lack of trust in the true value of the cryptocurrency. As a result of November 2019 US sanctions against PDVSA, Maduro purportedly cut the petro's backing to 30 million barrels of oil, despite announcing the coin would be pegged to five billion barrels at the time of the petro launch in February 2018.

Even with the discrepancy, the petro is still worth approximately the price of one barrel of oil, roughly US\$60. Yet, it has been reported that many Venezuelans can be found selling the coin on peer-to-peer marketplaces such as Localbitcoins for half that amount.

The screenshot shows a LocalBitcoins.com listing for selling bitcoins using PETROS (PTR) with Venezuelan Bolívar (VES). The listing includes the following details:

- Price:** 625,856,015.49 VES / BTC
- Payment method:** PETROS (PTR)
- User:** gilbertorb (feedback score 100 %, see feedback)
- Trade limits:** 100,000 - 12,535,143 VES
- Location:** Venezuela
- Payment window:** 4 hours 30 minutes

The terms of trade section includes:

- Vendo Petros PTR**
- Forma de pago:** -BTC
- La cantidad ofertada de BTC será calculada a través de la calculadora**
- https://petro.gob.ve/calculadora.html**
- Si no me ves en línea escribe al Telegram: gilbertorb**
- Nota: Hasta 3 PTR tengo disponible**

At the bottom left, there is a sign-up section with the text "Sign up and sell bitcoins instantly." and a "Sign up free" button. Below the button, it says "Signing up is free and takes only 30 seconds."

Figure 10 Websites selling petros at half their official value shows a lack of trust in Venezuela's crude oil backed national cryptocurrency.

Notably, Venezuelans' lack of excitement for petro does not correlate to a lack of excitement for crypto. They constantly search for solutions to the country's hyper-inflation, and crypto provides an alternative to the weakening Venezuelan bolivar. According to a tweet by Mark Mason, Director of Media and PR at Dash, between May and December 2019 there was a 562% increase in active Android devices using the Dash wallet app in Venezuela. Even Burger King Venezuela declared in a December 30 tweet that a branch in Caracas now accepts Bitcoin, Ethereum (ETH), Litecoin (LTC), Binance Coin (BNB), Dash (DASH), and Tether (USDT). The petro did not make it onto the list of accepted digital currencies.

Further pushing to promote Petro, on January 17 Maduro authorized the operations of a crypto casino that will operate out of the Humbolt Hotel in Caracas. While the casino accepts a variety of fiat currencies and cryptocurrencies, bets can only be placed in petros, so patrons must convert their funds before playing. According to the announcement, all funds raised will be allocated to social investments in areas such as health and education. At the time of this report's publication, the casino's opening day had not been released.

Russia – Largest Russian Dark Market Launches ICO to Fund Western Expansion

Russia's largest darknet marketplace, Hydra, recently announced a US\$146 million token offering via an "investment memo" on its website. According to the memo, Hydra plans to use the funds to build out a new service called "Eternos," which combines encrypted messaging services, a new privacy-focused browser, automated dispute resolution and an over-the-counter marketplace and crypto exchange.

Hydra claims this year's liquidation of major foreign dark markets has created a "vacuum" in international black-market trade. The memo attributes these recent takedowns to technical vulnerabilities of the TOR network, marking "a clear need for a technologically advanced and secure, high-level international platform similar to the HYDRA project."

Hydra's website claims to process over 100,000 transactions a day for its more than three million users. While, at first glance, it may look like any other dark marketplace selling illicit drugs, stolen credentials, forged documents and the like, Hydra's unique business operations set it apart from other marketplaces. Dark markets typical use a sell-and-ship model that leaves law enforcement and investigators multiple breadcrumbs for potential tracking. Hydra instead uses couriers that deliver purchased goods to designated, concealed spots in public spaces to be collected later by the client. Neither buyer, seller nor courier ever cross paths in person.

The operators of the marketplace have ambitions to roll out their model of anonymized rogue trading for illicit substances at a massive scale. The start of the project is scheduled for September 1, 2020.

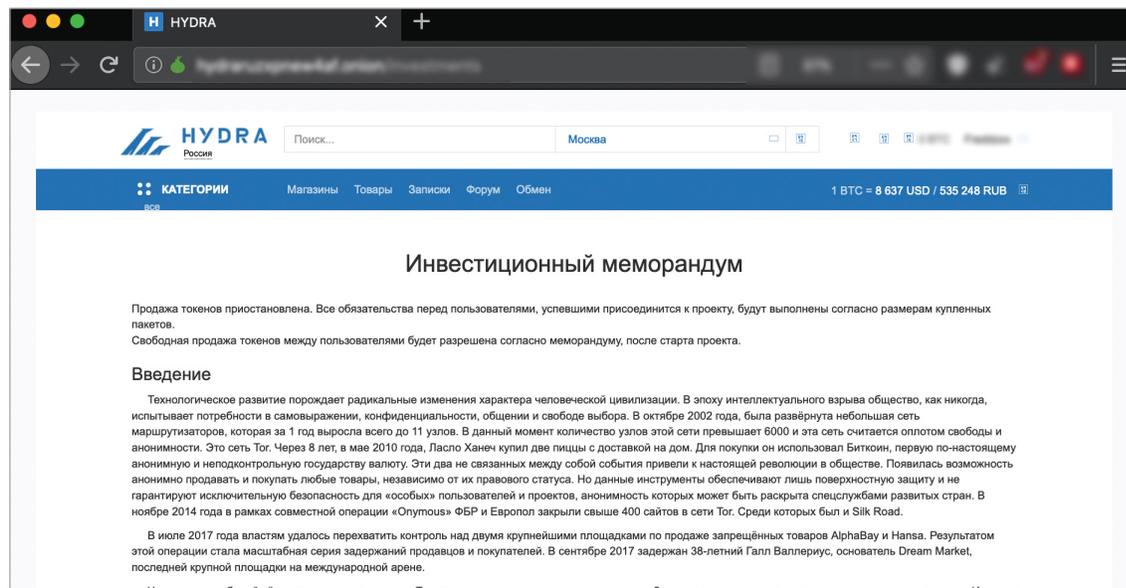


Figure 11 An investment memorandum on the Hydra website, accessible only via dark web browsers like Tor, claims the platform's global expansion "will start a new era in the West" at a scale that is "hard to imagine."

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**

Managing Editor, **Kevin Mitchell**

Financial Crime Analyst, **Julio Barragan**