CIPHERTRACE
mastercard

Cryptocurrency crime and anti-money laundering

REPORT

JUNE 2022

Contents

Foreword

The last seven months have been thrilling for CipherTrace. In October 2021, we were acquired by Mastercard, accelerating our joint efforts to ensure that the crypto economy is instilled with the same trust and peace of mind that consumers currently experience with more traditional payment methods.

Now that we're part of the Mastercard family, we're continuing to produce our cryptocurrency crime and anti-money laundering report (CAML), but taking the opportunity to infuse a new flavor into it. You'll see the design is fresh and content is slimmed down to provide our key findings from 2021 and Q1 2022.

Our hope with this report is that it will give you valuable insight into this explosive, ever-changing market. Additonally, we can offer ways to protect your business and customers as the crypto market evolves; we're here to help when you need us.

Dave Jevans
CEO, CipherTrace, a Mastercard company

Executive summary

~3.5%

illicit cryptocurrency transactions (% of overall) in 2019 mostly from large, isolated activities

1,456%

growth in the cryptocurrency market in three years from $135B on Jan 1, 2019 to $2.1T on Mar 31, 2022

The virtual asset ecosystem continues to exhibit rapid growth, particularly in 2021, compared to prior years. The cryptocurrency market cap went from approximately $135 billion on January 1, 2019, to just under $2.1 trillion on March 31, 2022, which is an increase of 1,456 percent. That cryptocurrency market cap peaked in November 2021 at almost $3 trillion, at which time Bitcoin hit its all-time-high of $68,790. The total dollar amount associated with cryptocurrency transactions in 2021 boomed compared to that in 2020. CipherTrace previously reported that total activity for 2020 was around $4.3 trillion; CryptoCompare (a partner of CipherTrace)[1] was cited by the World Bank Group when it stated there was approximately $16 trillion of total activity, alone, in the first half of 2021.

While illicit cryptocurrency activity in 2021 is a much larger dollar value compared to prior years, it is important to note that it continues to decline as a percentage of overall activity. CipherTrace estimates the total percent for 2021 illicit activity was between 0.10 and 0.15 percent of overall cryptocurrency activity compared to between 0.62 and 0.65 percent of overall cryptocurrency activity in 2020. Nonetheless, shifts in illicit activity characteristics have been noticeable year-over-year. The key trends identified in this report for 2021 and year-to-date 2022 are:

- Increase in DeFi hacks and fraud
- DeFi and NFTs as potential money laundering schemes
- Next generation mixing services
- Ransomware double-extorsion events
- Continued global evolution and roll-out of regulations
- Increase crypto-currency related sanctions

$3.5B

cryptocurrency seizures in 2021 by IRS-CI

Decentralized finance has boomed, in more ways than one, since the start of 2021. Many DeFi platforms serve a distinct purpose of connecting users with excess funds and users with funding shortfalls. User interactions leverage smart contract technology. While this offer has benefits, there are still limitations with smart contracts when compared to traditional contracts. Overall DeFi market values quickly surpassed $100 billion in the first half of 2021; however, the two largest hacks in virtual asset history occurred not too far after that exponential growth. The Poly network hack of $610M occurred in August 2021, while the Ronin hack of $625M occurred in March 2022. Both benefits and threats exist in this rapidly evolving and growing space, and CipherTrace expects this will be a focus of regulatory efforts, globally.

Law enforcement, law makers, legislatures, and regulatory agencies have been active in 2021 and 2022. Per its 2021 annual report (Publication 3583), Internal Revenue Service (IRS) Criminal Investigations (CI) announced $3.5 billion in cryptocurrency seizures, which accounted for 93 percent of all IRS-CI seizures in 2021. While accessing seized cryptocurrency and virtual assets can sometimes be difficult, law enforcement announcements of seizures were plentiful in 2021 and 2022. One of the most recent involved the German Federal Criminal Police Office (Bundeskriminalamt – BKA) seizing $25M in bitcoin after shutting down servers for the dark-market, Hydra. Very quickly after this, OFAC announced sanctions related to Hydra, Garantex, and over one hundred virtual addresses.

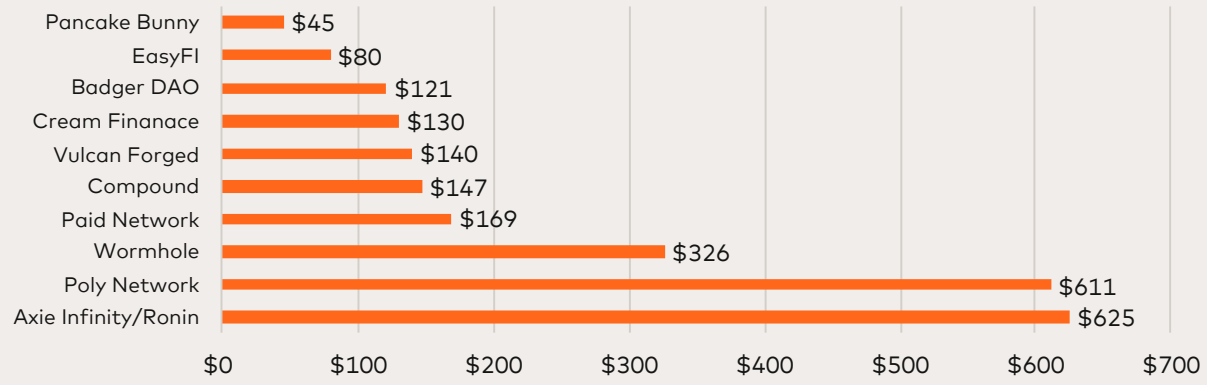
Regulatory agencies and lawmakers, globally, have been moving swiftly to coordinate oversight of the rapidly growing sector of virtual assets. The Financial Action Task Force (FATF) issued updated guidance on risk-based approaches to virtual assets (VAs) and virtual asset service providers (VASPs); this expanded what might constitute a VA or VASP as technology changes have been abundant since its initial guidance on virtual currencies in 2015 and its first iteration of VA/VASP guidance in 2018. The United States has been active with an Executive Order instructing various agencies to coordinate their approaches. There have also been various regulatory communications and guidance by the US Federal Banking Agencies, the US Securities and Exchange Commission (SEC), and Commodity Futures Trading Commission (CFTC). Legislation (enacted and new drafts) and regulatory communications touching on topics from consumer protection to economic stability were abundant in the United Kingdom, Europe, Chile, Brazil, and numerous other regions and countries around the world. While some jurisdictions are farther than others, it's clear that the legislative and regulatory frameworks are still in early stages.

Major hacks, thefts, and fraud – focus on the continued rise of decentralized finance (DeFi)

2021 was a year of turmoil for DeFi related hacks. On average, there was almost one significant reported attack per week. These attacks were either an exploit of a system or contact and in other cases were intentional fraudulent acts. Significant losses (in the billions) for victims around the world cannot be ignored and serves as a call to action for everyone in the crypto industry to take notice. As 2021 went on, more DeFi attacks took place, peaking with the August Poly Network attack of over $610M. The increase and frequency of the attacks is a demonstration of the increased capabilities and willingness of the wrongdoers to carry out such attacks.

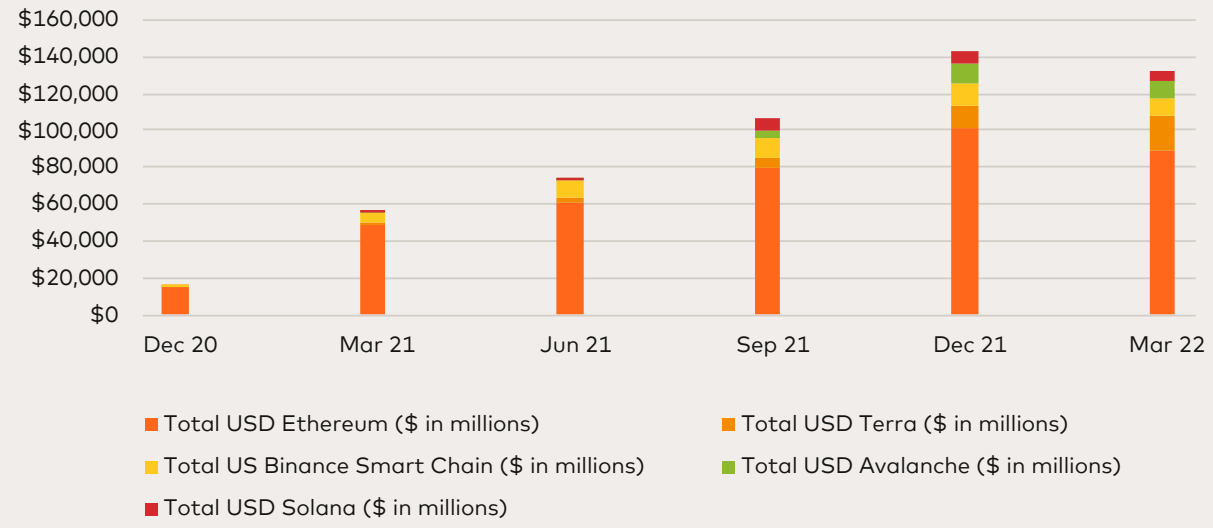
Review and analysis of the attacks of 2021 is necessary to not only stop the attacks and their frequency, but also to prepare for what is to come. Repeatedly successful attacks do not serve to deter illicit activity, but rather as an invitation to continue engaging in such behavior. It is easy to comment with the benefit of hindsight, but investigations and intelligence are designed to evaluate what happened, address the issues, and determine an appropriate response. In August of 2021, the CipherTrace CAML Report detailed $681M dollars' worth of thefts, hacks and frauds related to cryptocurrency to that point of the year. Graphic 1 illustrates the top 10 DeFi hacks (including losses from smart contract errors) of 2021 and 2022 (through Q1) account for $2.4 billion. While Ethereum continues to be the most widely used blockchain for DeFi, Graphic 2 illustrates a declining trend on its dominance in use.

Graphic 1: Top 10 DeFi hacks ($M) 2021–2022



Source: CipherTrace. Values subject to fluctuation.

Graphic 2: Quarterly DeFi volume for top 5 chains



Source: CipherTrace

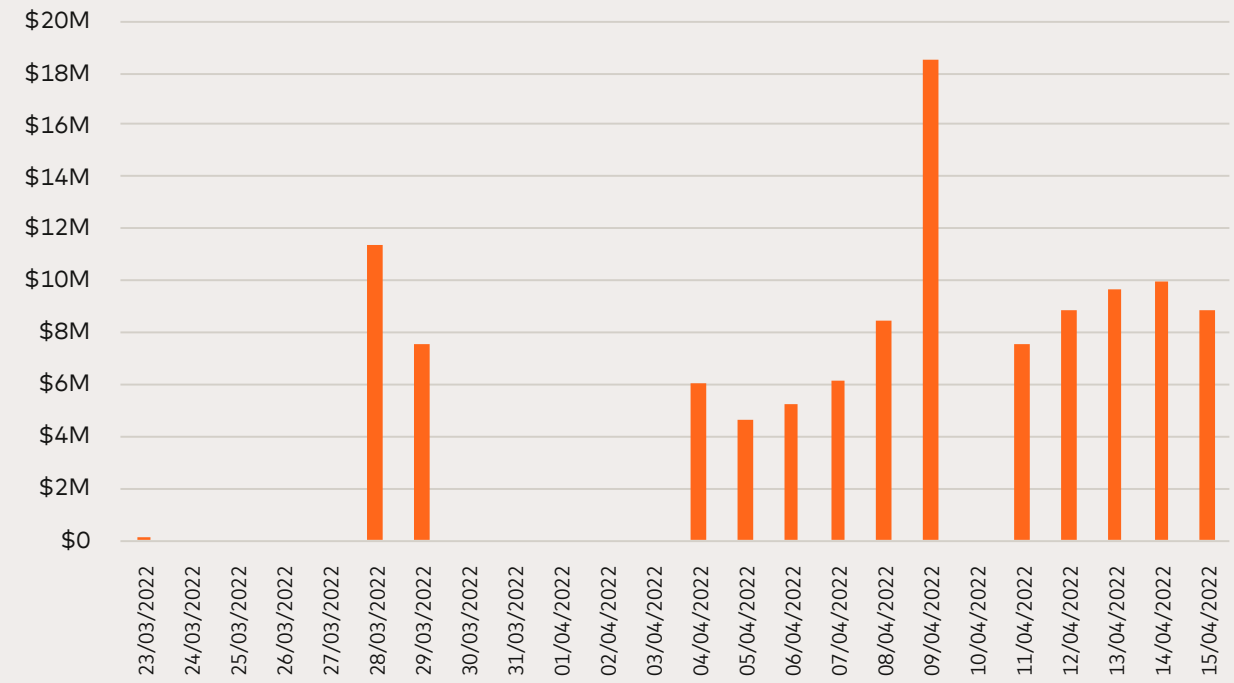
DeFi hacks, theft, and fraud trends clearly calls for increased efforts in intelligence, training/education and proactive problem solving to prevent continued attacks. Additional examples are noted below:

Ronin and Axie Infinity

Axie Infinity is a decentralized gaming universe with millions of users around the globe. Users collect 'Axies', which are essentially a virtual form of a pet. Gameplay allows for users to play in various ways, most of which includes tactical practices and head-to-head competition. Players could benefit from rewards when they reach certain skill levels. Axies are purchased with Axie Infinity Shards (AXS); the AXSs are ERC-20 governance tokens. CipherTrace defines ERC-20 as a technical standard used to implement smart contracts on the Ethereum blockchain; ERC-20 tokens follow the ERC-20 standard on the Ethereum blockchain. Ronin is a sidechain linking to the Ethereum blockchain; it was specifically created for Axie Infinity. This bridge allows a user to exchange tokens from the game for ether and other cryptocurrencies.

The Ronin network was the source of an approximate $625M hack in March 2022. The Ronin network has stated that it was hacked in November 2021, but initial withdrawal of funds started on March 23, 2022. As a result of the substantial size of the userbase in November 2021, security protocols were loosened. Hackers gained access to validators' private keys on the network somewhere between November 2021 and March 23, 2022. With control over validation, perpetrators were able to execute phony withdrawals. As of March 30, 2022, the hack was said to contain 173,600 eth and 25.5M USD Coin. Most of the funds remain in the hacker's address; however, as shown below, some funds were transferred to exchanges.

Graphic 3: Daily USD sent from sanctioned Eth address



Source: CipherTrace

On April 14, 2022, this story took another turn. Ronin's newsletter[2] noted that the Federal Bureau of Investigation (FBI) tied an address to North Korea's Lazarus Group. OFAC sanctions are in place with both North Korea and Lazarus Group; an associated Ethereum address was added to OFAC's Specially Designated Nationals (SDN) list within the Lazarus Group's listing. Utilizing CipherTrace tools, Graphic 3 illustrates eth transactions that were to/from the sanctions Ethereum address from March 23 through April 15, 2022.

Smart contract hacks

A smart contract has many similarities to a traditional contract. Both outline the terms or an arrangement or agreement. A smart contract differs in that it is written in code instead of everyday language. The smart contract is enacted as the code runs on a blockchain. The most common blockchain for running smart contracts continues to be Ethereum. Because smart contracts on Ethereum can be read by anyone, hackers have unparalleled visibility into detecting coding errors that can allow them to take control of funds controlled by a contract. Their level of sophistication grew significantly in 2021 and shows no signs of slowing down in 2022. Many DeFi projects release their code publicly on GitHub. This can be a problem if a security vulnerability is identified and fixed in the publicly viewable code, before it is released into production form, thus giving hackers a clear indicator of the vulnerability and how to exploit it.

February 2022: The Wormhole token bridge was hacked and 120,000 wrapped ether was lost (approximately $322M USD). The attacker found a vulnerability in the Wormhole smart contracts and issued transactions on the Wormhole smart contract to avoid signature validation checking.

Flash loan attack

A flash loan is a transaction in which a specific quantity of liquidity is borrowed and repaid in the same transaction or block. Malicious actors can find certain vulnerabilities and exploit the smart contract. The exploits often target a lack of security protocols in the contract.

February, August, and October 2021: Cream Finance was hacked three times: February $37M, August $29M, October $130M. These appear to be attacks on a vulnerability in Cream's DeFi flash loan system. CipherTrace analysts identified breakdowns in the Cream Finance attacks.

Cryptocurrency exit scam and DeFi rug pull

An exit scam occurs when the creators/promotors of a cryptocurrency build up a pool of investors during a coin offering. The creators/promotors leave by taking investors' funds during or shortly after that offering. A DeFi rug pull is a type of exit scam; however, this more specifically occurs when a project is abandoned all together. The creators/promotors then leave with the funds. Rug pulls accounted for nearly 40 percent of DeFi fraud in 2021.

November 2021: Building on the popularity of the Netflix show, Squid Games, the squid game token was created in 2021. The token's value went above $2,850, only to lose 99.9 percent of its value almost instantaneously in November 2021. Estimated losses are around $12M.

December 2021: MetaDAO (approx. $3M) and MetaSwap MGAS (approx. $600,000) were examples of rug pull scams. In both cases, stolen funds were sent through Tornado.cash.

Phishing and 'ice phishing'

Most people know phishing as fraudulent emails attempting to steal a users' private information (i.e., credentials, account information, etc.). A type of phishing attempt to steal crypto usually targets a user's private key. This is like attaining log in information to a user's bank account in traditional finance. Phishing in DeFi will have a similar entry point by way of fraudulent emails, social media posts, or other methods to get a user to click on a phishing website; however, the fraud occurs when the perpetrator's actions result in the user approving a smart contract that delegates authority to the perpetrator. Ultimately, the perpetrator can approve the sending of the user's tokens. Microsoft is one of the firms that has associated the term Ice Phishing[3] with this type of attack. In late 2021 and now in Q1 2022, these phishing methods have increased in DeFi services. These are particularly difficult to defend against, as there is no centralized IT infrastructure that can dynamically detect and prevent phishing or the use of phished wallets. This is unlike centralized payment services, where many behavioral and historic patterns can be used to detect account takeovers in real-time.

February 2022: Users of the OpenSea NFT exchange received a legitimate support email from OpenSea instructing them to move their funds to a new contract due to upgrades. Phishers then sent out a copy of that email and modified it to take users to a hostile web page rather than the legitimate OpenSea page. Users were tricked into signing a malicious payload resulting in theft of ether and numerous NFTs.

Ransomware double-extorsion attacks grow exponentially

Ransomware continues to be a major cybersecurity challenge that impacts us all – from big industry to small businesses to individuals. In 2021, we analyzed trends in ransomware usage and bottled those up in our latest Current Trends in Ransomware Report. Here's a snapshot of what you'll find in the report:

- Double extortion ransomware increased nearly 500% in 2021
- Bitcoin (BTC) remains the preferred payment system, but Monero (XMR) has jumped sharply in adoption by ransomware groups
- The first six months of 2021 saw payments to ransomware groups of $590M, an increase of 42% over the whole of 2020

As the digital economy grows, cyberattacks are increasing. It's crucial for businesses and governments to have a disaster preparedness plan in place for cyberattacks and security breaches to mitigate risk and limit their liability. Backups are not enough.

Money laundering themes and schemes

The FATF's September 2020 Report, 'Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing', continues to be a reference point for typologies and characteristics indicative of money laundering. A summary can be found on the CipherTrace blog. Below are examples that mimic red flags, including but not limited to: mixing services, lax or nonexistent KYC protocols, converting virtual assets at a loss, and conducting activity on peer-to-peer platforms.

NFT loss and wash sales

An NFT is a unit of data on a blockchain that is not interchangeable. These unique assets continued to gain popularity in 2021 and 2022. NFTs can be bought, sold, and resold. These could be resold amongst related-parties or even the same underlying party, which can artificially inflate the value of the asset. Meanwhile, buying and quickly selling at a break-even point or at a loss could be indicative of money laundering. CipherTrace analysts regularly see stolen cryptocurrencies being used to purchase NFTs. Much like tangible physical assets (i.e., artwork and luxury goods), NFTs also have an aura of legitimacy, and there is typically much less application of AML controls on NFTs as compared with cryptocurrencies.

February 2022: OpenSea phishers stole and sold NFTs worth 1,200 ether ($3.4M) and laundered the funds through Tornado.cash on February 22, 2022. The NFTs were stolen when users signed a malicious payload. Malicious payloads are the element of the attack causing harm (i.e., data theft, monitoring activity, etc.).

Mixing services

In the past, mixing services were primarily oriented toward mixing Bitcoin transactions. Multiple people would send funds to a mixer, which gathers up those funds; the mixer then distributes funds back out in an output transaction in a manner that obfuscates ownership. The mixing service takes fees that may range up to five percent. By definition, a mixing service is a virtual asset service provider (VASP). Tornado.cash is a mixer for Ethereum tokens, which grew substantially in 2021.. This is a non-custodial (meaning users are the only party with access to their private key(s)), decentralized solution that operates on the Ethereum blockchain. It allows users to deposit ERC-20 tokens and ether to the mixing service; the user then withdrawals to a new address that would not be traceable.

Tornado.cash was created in 2019, but in May 2020, the creators ran a contract update that led to a fully decentralized method of control. The sender of funds can retrieve an audit showing which address they sent the funds to through Tornado.cash, but this log does not exist anywhere except with the sender.

February 2022: Finance Build exploiter laundered 163 ether ($495,000) and the Ariva coin rug pull sent 1,710 BNB ($600,000) through Tornado.cash.

August 2021: Helix functioned as a bitcoin mixer from 2014 through 2017. It was operated by Larry Harmon, who admitted to conspiring with darknet vendors to launder Bitcoin derived from drug and other illicit activity proceeds through Helix's mixing capabilities. He pled guilty to laundering over $300M on August 18, 2021[4].

Refer to additional examples in Cryptocurrency exit scams and DeFi rug pull and NFT loss and wash sales sections above for Q4 2021 examples.

Changes in global regulation

Financial Action Task Force (FATF)

The FATF has released numerous publications pertaining to virtual assets (VAs) and VASPs as early as 2014. FATFs global influence is significant; the guidance and publications have been and will continue to contribute to countries' CFT/AML legislative and regulatory oversight of VAs/VASPs. The graphic below depicts key items published in this space:

JUN 2014
Virtual Currencies: Key Definitions and Potential AML/CFT Risks (link)

JUN 2015
Guidance for a Risk-Based Approach to Virtual Currencies (link)

JUN 2019
Guidance for a Risk-Based Approach – Virtual Assets and Virtual Asset Service Providers (link)

JUL 2020
12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers (link)

SEP 2020
Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing report (link)

JUL 2021
Second 12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers (link)

OCT 2021
Guidance for a Risk-Based Approach – Virtual Assets and Virtual Asset Service Providers (link)

FATF's *Guidance for a Risk-Based Approach – Virtual Assets and Virtual Asset Service Providers* is its most recent issuance on October 28, 2021. This will establish an updated global standard for CFT/AML and highlights risk-based approaches for VAs and VASPs. The publication's primary focus was on the following: "*Clarification of the definitions of VAs and VASPs; Guidance on how the FATF Standards apply to stablecoins; Additional guidance on the risks and the tools available to countries to address the money laundering and terrorist financing risks for peer-to-peer transactions; Updated guidance on the licensing and registration of VASPs; Additional guidance for the public and private sectors on the implementation of the "travel rule"; and Principles of information-sharing and co-operation amongst VASP Supervisors.*"

This publication discusses the nuanced nature of decentralized applications (dApps), DeFi, NFTs, and stablecoins. Each of these may be considered as VAs or VASPs, depending on certain characteristics. FATF suggests that fitting into VA/VASP categories is less about the terminology and technology and more about the specific use case.

Changes in regional and country regulation

Our crypto-asset advocacy begins from a recognition that regulators and policymakers from different traditions may have very different starting positions – with some potentially viewing crypto-assets as a fundamental threat to national security and others deeply invested in their potential to drive innovation. Consequently, we focus on the principles that should guide governments in establishing their regulatory frameworks for crypto-assets, rather than prescribing the specific policy outcomes they should reach. Our key principles include:

Clarity
We welcome additional clarity around the regulatory treatment of various types of crypto-assets and related activities, particularly in payments.

Consistency
We support consistency in the regulatory treatment of crypto-assets and activities across different markets, industries, and business models to reinforce a level playing field and prevent regulatory arbitrage.

Proportionality
We support a principled and risk-based approach to crypto-asset regulation, with the aim of achieving the same regulatory outcomes for the same risk (not necessarily the same exact rules), while providing sufficient regulatory flexibility to adapt as technology evolves.

Security/resiliency
We support the implementation of robust security and resiliency safeguards for any payment system, including those involving crypto-assets and blockchain technology, to preserve and reinforce trust in payments.

Consumer protection
We support regulations that seek to ensure strong consumer protections, including the safety and reliability of payments, and protections against loss in certain circumstances.

Responsible innovation
We believe that crypto regulation should balance preventing consumer harm and financial instability with the fostering of innovation, for example by providing clear rules, expectations, safe harbors, and/or risk management frameworks.

How to understand regulations and take action

Legislation and regulations continue to rapidly evolve in the virtual asset space. While there is global leadership and guidance from FATF for combatting money laundering and terrorist financing, there are still varying approaches across the globe with regards to virtual assets. CipherTrace monitors these changes on a regular basis for the following regions: North America, Latin America (LATAM), Europe, Middle East, and Africa (EMEA), and Asia-Pacific (APAC). Within the United States, we also actively monitor state level legislation and statutes. Additionally, CipherTrace offers Armada, which is a tool used by clients to better understand risks for more than 1,200 VASPs around the world. The Armada product contains applicable regulatory information by country, which allows for ease of reference when clients are utilizing the platform and often navigating between VASPs with different regulatory considerations. Later in the year, Mastercard will deploy a new product which will provide financial service organizations with frequent updates on new and evolving regulatory requirements to which they are subject.

Sample of significant legislative and/or regulatory topics

U.S. – The White House

President Biden signed 'Executive Order on Ensuring Responsible Development of Digital Assets' on March 9, 2022, (EO link and factsheet link). The Executive Order will require the Administration, Congress, and various agencies across the federal government to work towards establishing policies and regulations that will guide the ongoing development of digital assets. While numerous government and regulatory agencies have been working to understand and oversee activities associated with digital assets, this executive order placed clear deliverables and timelines to completing these various steps. The Executive Order also ensures better coordination of these efforts by outlining guiding principles that must be achieved through a balanced approach. These items include the following: protect US consumers, investors, and businesses; protect US and Global financial stability; mitigate illicit finance and national security risks; reinforce US leadership in the global financial system and in technological and economic competitiveness; promote access to safe and affordable financial services; and support technological advances that promote the responsible development and use of digital assets. In early April, Secretary of the Treasury, Janet Yellen, and head figures for various agencies began to reference the key themes within the Executive Order as they discuss their agency's role. There is much work to be done, but this coordination effort was needed to outline a path that will bring digital, virtual, and crypto assets into a regulated and trusted environment for longer-term stability.

EMEA – European Union (EU) Parliament
EU Committees on Economic and Monetary Affairs and on Civil Liberties, Justice and Home Affairs Voted on measures to apply AML requirements to crypto on March 31, 2022 (EU Parliament link). This vote is not final and would require an announcement at EU Parliament plenary sessions where it could be challenged. The proposal would apply AML requirements for gathering pertinent information on all crypto transactions and amends the existing regulation to comply with information accompanying the electronic transfer of funds (EU 2015/847). While there are several measures within the proposal, two items are notable:

1. The European Supervisory Authority (European Banking Authority) would be required to create and maintain a "public register of entities, crypto-asset services, and wallet addresses that are higher risk of money-laundering, terrorist financing, or other criminal activities"[5]
2. Providers of crypto-asset transfers are required to attain information on a sender/beneficiary for un-hosted wallet transactions and confirm the accuracy of information provided by their client for said transactions.

This EU proposal exhibits some contrast to the US' Executive Order from early in the month. While both seek to promote a more regulated and trusted ecosystem for digital, virtual, and crypto assets, EU's proposal focuses more pointedly on the topic of illicit activity. Should the amendments become final, Ciphertrace's Inspector and Traveler products could play key roles in helping firms comply.

EMEA – Dubai
On February 28, 2022, a law (Law No. 4 of 2022) on the Regulation of VAs in the Emirate of Dubai was passed (United Arab Emirates (UAE) link). This law establishes a Virtual Assets Regulatory Authority (VARA) as the primary regulator of VAs. VASPs will need to meet licensure requirements, and the VARA will be tasked with oversight to increase transparency, mitigate illegal activity, and develop a formal oversight framework. The VARA is also specifically charged with ensuring beneficiaries' personal data remains safe, organizing the issuance and trading of VAs, and preventing price manipulation for VAs. Lastly, the VARA will be required to closely coordinate with the UAE Central Bank on topics that will help ensure financial stability. While much work is left, there are positives here to promote growth in the digital, virtual, and crypto asset ecosystem in a regulated manner. As regulatory and government agencies' roles become clearer, the industry can better operate within its applicable regulation.

LAC – Brazil

Brazilian lawmakers proposed a bill in February 2022 to establish the groundwork to regulate its cryptocurrency market. The proposed bill defines virtual assets and crypto service providers; it also focuses on mitigating criminal activity by proposing virtual asset service providers maintain AML programs to monitor for illicit activity. This is still proposed legislation at this time, but it is a meaningful start for a country that continues to see rising use of digital, virtual, and crypto assets. A push for a more regulated ecosystem will continue to be critical to mitigate illicit finance and protect consumers.

AP – Hong Kong Monetary Authority (HKMA) and Securities and Futures Commission (SFC)

The HKMA and SFC issued a joint circular and appendix on January 28, 2022, which focused on VA related activity for intermediaries. The content within the joint circular is focused heavily on investor protections and mitigating illicit activity. Specific requirements are outlined for licensed intermediaries that provide VA services. The HKMA also issued a circular on January 28, 2022, titled Regulatory approaches to Authorized Institutions (AIs) interface with VAs and VASPs. This outlined various measures specific to AML/CFT program expectations when AIs provide services for VASPs or other client VA activities. Additionally, the HKMA stated, "AIs intending to engage in VA activities should discuss with HKMA (and other regulators where appropriate) and obtain the HKMA's feedback on the adequacy of the institution's risk-management controls before launching relevant products or services"[6]. This approach is consistent with current views of the Office of Comptroller of the Currency (OCC link) and the Federal Deposit Insurance Corporation (FDIC link). The HKMA and SFC are prioritizing regulation to protect consumers/investors and mitigate illicit finance. These regulatory considerations promote additional transparency and trust for the ecosystem.

Enforcement actions and law enforcement activity

Tether and Bitfinex ordered to pay $42.5M in fines

In October, the CFTC filed charges against Tether and Bitfinex, requiring Tether to pay a fine of $41M, and Bitfinex to pay a $1.5M civil monetary penalty. Tether was fined for its omissions of material facts, making misleading statements regarding the US dollar tether token (USDT). In simultaneous filings, the CFTC filed charges against Bitfinex, for engaging in illegal, off-exchange retail commodity transactions with US persons on their Bitfinex trading platform, while operating as a futures commission merchant (FCM) without registering as required.

German authorities shut-down Hydra servers

On April 5, 2022, the Federal Criminal Police Office (BKA) and the Central Office for Combating Cybercrime (ZIT) announced they closed the darknet marketplace, Hydra. This occurred after they acquired the server infrastructure in Germany. Along with this, law enforcement seized 23M Euros (approx. $25.6M USD). Hydra has operated since 2015 and is considered one of the largest darknet marketplaces. Per ZIT and BKA, Hydra accounted for sales of 1.23 billion Euros (approx. $1.35 billion USD) in illegal goods such as narcotics, false identification documents, and stolen credit card data. This is tied to OFAC sanctions issued on April 5, 2022.

Polymarket fined $1.4M for unregistered swaps

In January 2022, the US Commodity Futures Trading Commission (CFTC) ordered the event-based options markets operator, Polymarket, to pay a $1.4M fine for conducting unregistered swaps. Polymarket was offering off-exchange event-based binary options contracts and failed to obtain a designated contract market or register as a swap execution facility. The CFTC also ordered it to provide refunds on charges from unregistered activities and cease operations. Polymarket had cooperated with the investigation and the fine was part of a settlement. It shut down three markets in January 2022.

Bitcoin scheme leader arrested in Brazil

On December 30, 2021, Johann Steynberg, the executive director of Mirror Trading International was arrested by the Federal Police of Brazil. Steynberg was wanted by various entities, including Interpol and the Federal Bureau of Investigations (FBI). Steynberg was the CEO of a South African-based trading platform, which at one time had over 165 thousand clients globally. He was able to syphon funds through several investment platforms by using cryptocurrencies. South African authorities warned Steynberg that he was conducting an illegal operation which misled clients, and that MTI did not have the necessary permits to offer financial services with cryptocurrencies.

Conclusion

It's certainly fair to say that the world of cryptocurrency saw enormous growth in 2021 and that brought with it an increase in illicit activity too. Early indications are that 2022 is going to continue this trend, but as noted in our sections on legislation and enforcement, the world's governments are starting to take decisive action to ensure that the space isn't just a modern-day wild west. With big fines, like Tether's $41M penalty, these organizations are going to have a very real incentive to shape up or face more heavy losses at the hands of government.

For those reading this in VASPs, banks, payment processors and both federal and local law enforcement, CipherTrace has considerable expertise and tools to help monitor the movement of cryptocurrency and can assist – get in touch with us at ciphertrace.com. Sign up for email alerts and we'll keep you up-to-date on trends, our latest reports and significant changes to the industry.

1. CryptoCompare. 2021, October. CryptoCompare Exchange Review October 2021. https://www.cryptocompare.com/media/38554107/cryptocompare_exchange_review_2021_10.pdf
2. Ronin Network. (2022, April 14). Community Alert: Ronin Validators Compromised. Ronin Newsletter. https://roninblockchain.substack.com/p/community-alert-ronin-validators?s=w
3. Microsoft 365 Defender Research Team. (2022, February 16). 'Ice Phishing' on the Blockchain. Microsoft. https://www.microsoft.com/security/blog/2022/02/16/ice-phishing-on-the-blockchain/
4. US Department of Justice. (2021, August 18). Ohio Resident Pleads Guilty to Operating Darknet-Based Bitcoin 'Mixer' that Laundered Over $300 Million. https://www.justice.gov/opa/pr/ohio-resident-pleads-guilty-operating-darknet-based-bitcoin-mixer-laundered-over-300-million
5. EU Parliament. (2022, March 31). Proposal for a regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets. https://www.europarl.europa.eu/doceo/document/A-9-2022-0081_EN.html
6. HKMA. (2022, January 28). Regulatory approaches to Authorized Institutions' interface with VAs and VASPs. https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2022/20220128e3.pdf

Designed by Mastercard Creative Studio