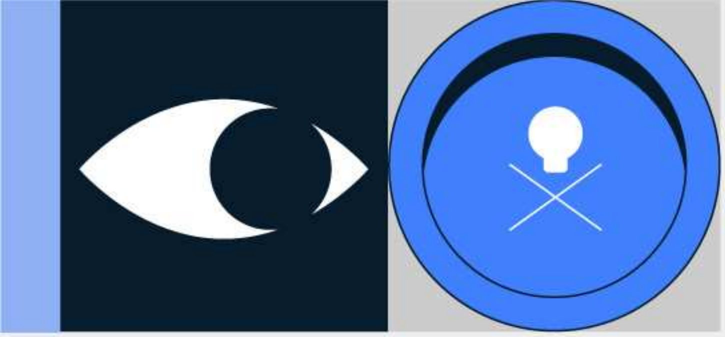
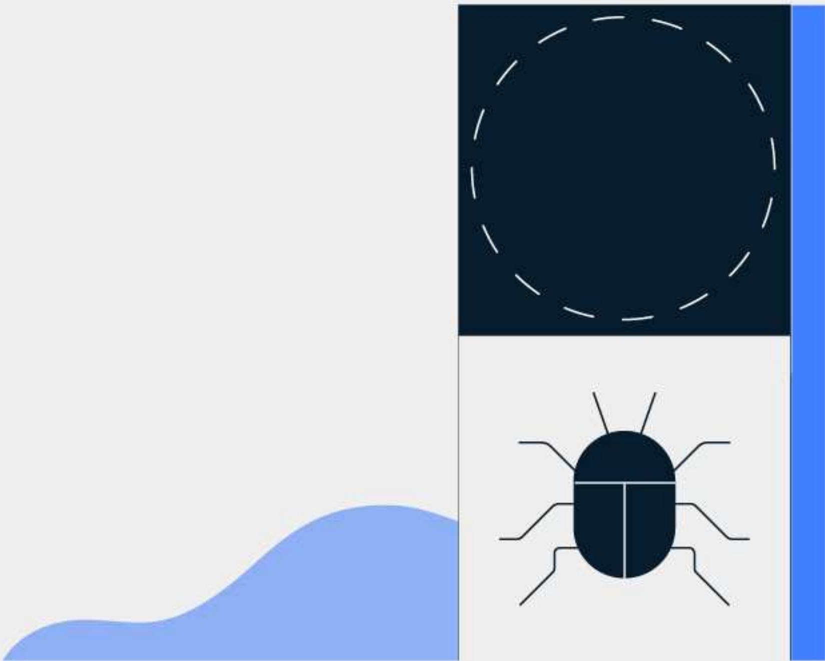


TRM

Illicit Crypto Ecosystem Report

A Comprehensive Guide to Illicit Finance Risks in Crypto

June 2023



Part I

Illicit Crypto

Part II

Money Laundering

Introduction

Confounding expectations, the collapse in cryptocurrency prices since 2021 had no meaningful impact on the dollar value of crypto-related crime in 2022. Indeed, TRM data reveals at least USD 7.8 billion paid into Ponzi or pyramid schemes, USD 1.5 billion spent on darknet markets specializing in illegal drugs, and USD 3.7 billion stolen through hacks and exploits, based on TRM Labs data.

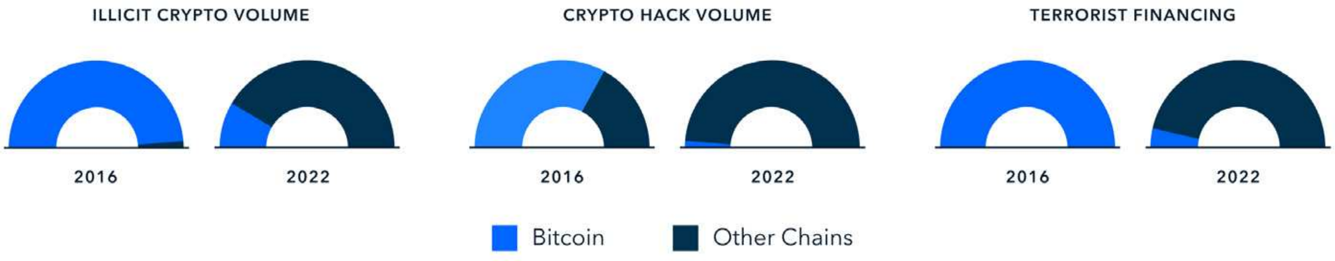
Among the possible reasons behind this resilience is crypto's qualitative leap away from Bitcoin domination towards a new multi-chain reality that has given rise to novel threats.

For example, in 2022, approximately USD 2 billion was stolen through attacks on cross-chain bridges, which enable cryptocurrency to pass from one blockchain to another. Criminals also increasingly rely on chain-hopping, or moving funds through various blockchain networks, as part of their money laundering strategies to obscure the source and destination of ill-gotten gains.

The multi-chain era has had a sweeping impact on the distribution of illicit crypto volume as a whole, where Bitcoin's share plummeted from 97% in 2016 to 19% in 2022. In 2016, two thirds of crypto hack volume was on Bitcoin; in 2022, it accounted for just under 3%, with Ethereum (68%) and Binance Smart Chain (19%) dominating the field. And while Bitcoin was the exclusive currency for terrorist financing in 2016, by 2022 it was all but replaced by assets on the TRON blockchain, with 92%.

Yet until now, there has been no systematic attempt to create a holistic overview of this new illicit crypto ecosystem. In the first guide of its kind, TRM Labs has identified, studied and classified over 40 types of criminal activity, from espionage to SIM swapping and pump and dump schemes.

QUICK LINKS

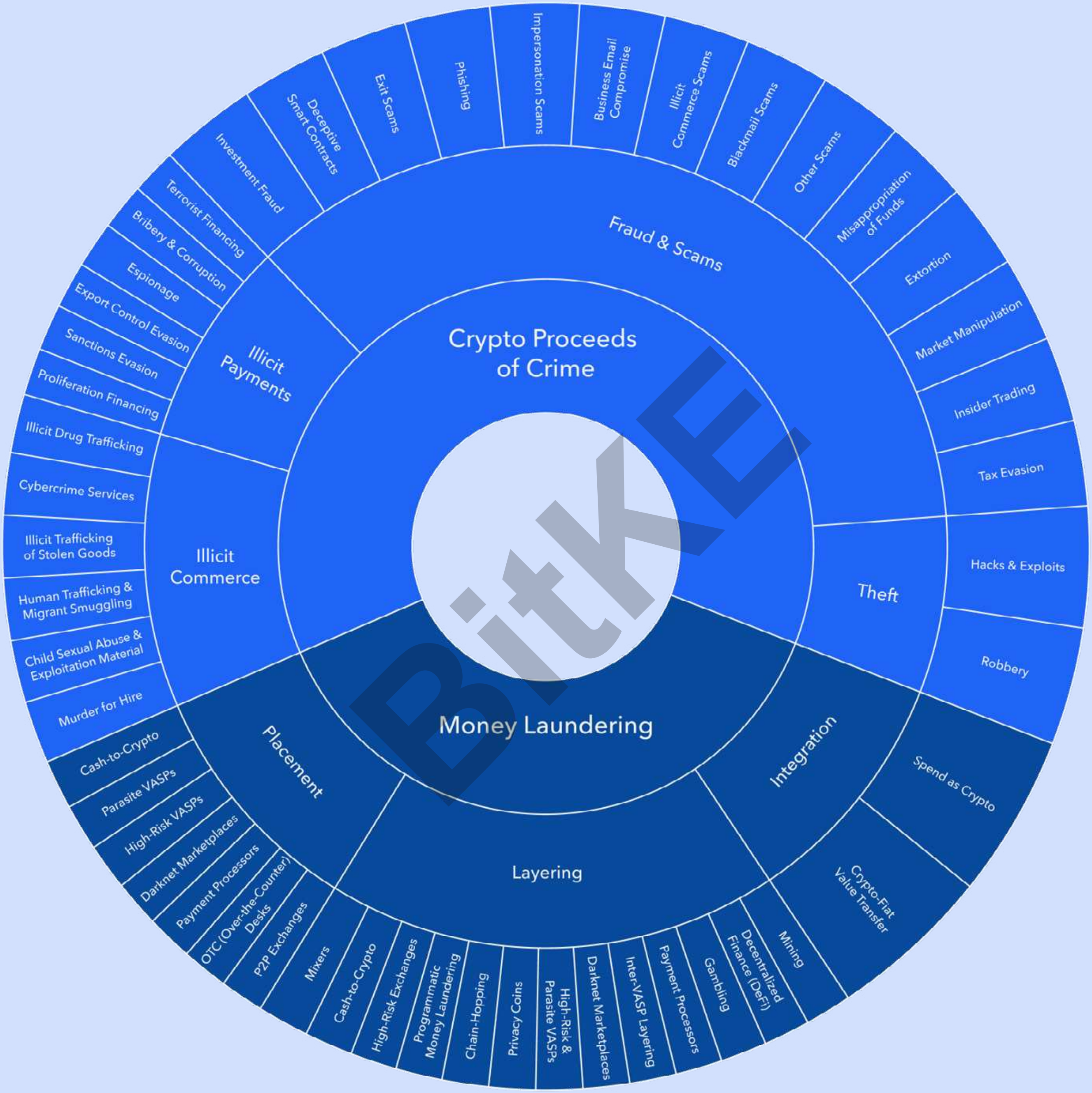


This landmark report spans over 20 blockchains and covers all major known forms of crypto-mediated illicit finance, as well as the use of cryptocurrency to launder the proceeds of crime.

The first section maps out criminal activities that generate crypto proceeds of crime including illicit commerce, illicit payments, fraud, and theft. The second section catalogs the way the crypto ecosystem is used in laundering proceeds of crime, whether fiat or crypto.

Through original research, case studies and an analysis of specific risks, this report offers insights into the complex dynamics of the illicit crypto ecosystem and contributes to a better understanding of the challenges faced by regulators, law enforcement agencies and industry stakeholders.

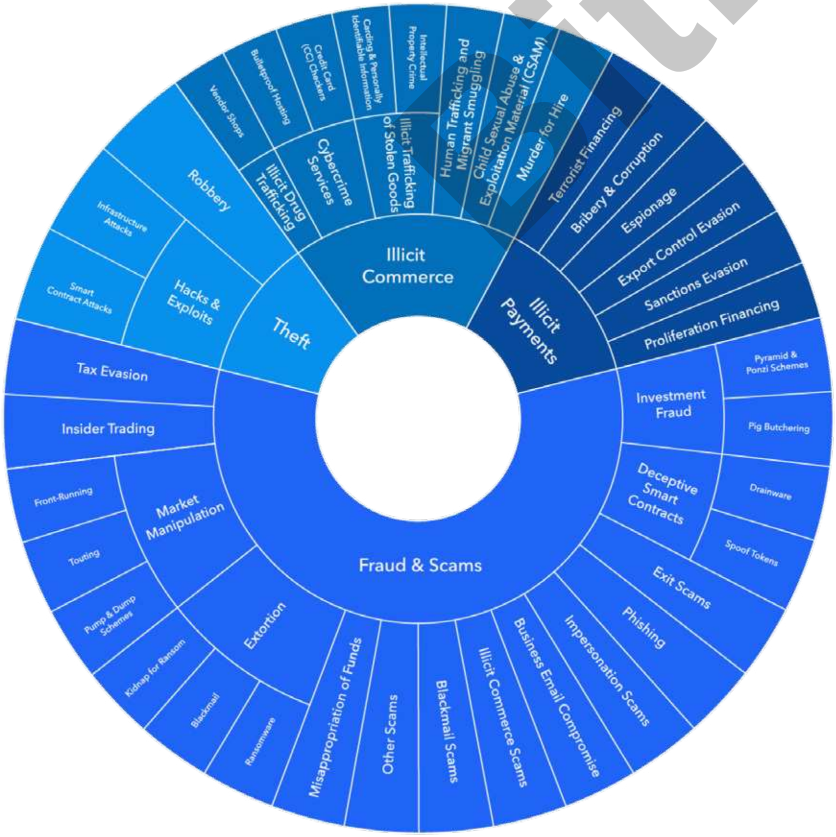
Understanding these risks is crucial for law enforcement to combat wrongdoing, for financial institutions and businesses to ensure that their platforms are not used to launder illicit funds, and for policy makers and regulators to assess, respond to, mitigate and prevent the full gamut of blockchain-mediated illicit activity.


Crypto Proceeds of Crime
Money Laundering
Fraud & Scams
Theft
Illicit Payments
Illicit Commerce
Placement
Layering
Integration
Investment Fraud
Deceptive Smart Contracts
Exit Scams
Phishing
Impersonation Scams
Business Email Compromise
Illicit Commerce Scams
Blackmail Scams
Other Scams
Misappropriation of Funds
Extortion
Market Manipulation
Insider Trading
Tax Evasion
Hacks & Exploits
Robbery
Terrorist Financing
Bribery & Corruption
Espionage
Export Control Evasion
Sanctions Evasion
Proliferation Financing
Illicit Drug Trafficking
Cybercrime Services
Illicit Trafficking of Stolen Goods
Human Trafficking & Migrant Smuggling
Child Sexual Abuse & Exploitation Material
Murder for Hire
Cash-to-Crypto
Parasite VASPs
High-Risk VASPs
Darknet Marketplaces
Payment Processors
OTC (Over-the-Counter) Desks
P2P Exchanges
Mixers
Cash-to-Crypto
High-Risk Exchanges
Programmatic Money Laundering
Chain-Hopping
Privacy Coins
High-Risk & Parasite VASPs
Darknet Marketplaces
Inter-VASP Layering
Payment Processors
Gambling
Decentralized Finance (DeFi)
Mining
Crypto-Fiat Value Transfer
Spend as Crypto

Part I

Illicit Crypto

This section presents an analysis of criminal activities that may generate proceeds in cryptocurrency. While fiat currencies, particularly the US dollar, dominate illicit transactions, the utilization of crypto in illicit activity offers critical benefits in the fight against financial crime. The transparent and traceable nature of crypto transactions facilitates two unique benefits: (1) the systematic measurement of illicit activity, leading to insights into criminal networks and typologies, (2) an ability to "follow the money" in criminal investigations that is faster and more effective than following the money in cash. By leveraging the transparency and traceability of crypto transactions, we not only gain valuable tools for measuring illicit activity and understanding criminal networks but also contribute to the development of a more resilient and secure financial ecosystem.



QUICK LINKS

Part I – Illicit Crypto

1. Illicit Commerce

2. Illicit Payments

3. Fraud and Scams

4. Theft

1. Illicit Commerce

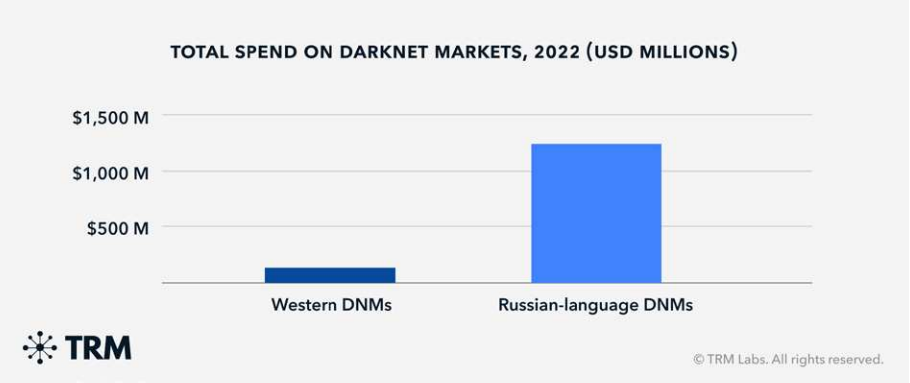
Illicit commerce involves the trade of illegal goods and services. While the vast majority of illicit commerce continues to use fiat currency such as the US dollar, cryptocurrency is the preferred medium of exchange on darknet marketplaces, cybercrime forums, and on CSAM sites.Darknet markets (DNMs), which specialize in selling drugs and also offer personally identifiable information (PII), are the biggest drivers of illicit commerce using cryptocurrency. A smaller and more elusive subset of illicit commerce concerns child sexual abuse materials (CSAM).

Illicit Drug Trafficking

The crypto-mediated illicit drugs trade mostly takes place on DNMs - multi-vendor online illicit global commerce platforms located on the "darknet", an encrypted section of the internet neither accessible from standard internet browsers nor indexed by search engines.

An established form of transnational organized crime, DNMs combine anonymization networks and cryptocurrencies with encryption technologies. They are distinct from independent single-vendor shops that also sell illicit drugs, and from other types of fraud stores.

As much as USD 1.49 billion was spent on DNMs in 2022, according to TRM Labs research. Over 80% of this was spent on Russian-language DNMs. By contrast, the largest Western Bitcoin DNM currently in existence – ASAP Market – accounted for less than 10% of global DNM market share. Most Russian-language DNMs only support Bitcoin, with no privacy coin options available. This may reflect their lower perceived risk of being taken down by the authorities. By contrast, Western DNMs employ more on-chain operational security measures and either offer Monero only or Monero alongside Bitcoin.



QUICK LINKS

Vendor Shops

Also known as single-vendor markets, vendor shops are online platforms that host illicit drug sales for a particular vendor only. These independent vendors use a range of online services, from darknet websites such as onion sites on the Tor network and eepSites on the I2P network, to automated Telegram bots, direct interactions on encrypted communication applications, and encrypted email services. Many vendor shop owners also trade simultaneously on DNMs.

Generally offering a limited range of products, sometimes only one or two types of drug, vendor shops first gained prominence in the wake of Operation Onymous in 2014. That international law enforcement action shut down several large DNMs, leading customers to seek alternative sources of supply. TRM Labs data indicates that in 2022 vendor shops received more than USD 230 million.

Engaging directly with vendor shops carries greater risks for customers than dealing with vendors on DNMs due to the absence of the neutral third-party which provides the escrow service, manages transactions and mediates disputes.

Cybercrime Services

Cybercrime services are illicit services such as bulletproof hosting, DDOS attacks, exploits-as-a-Service, compromised accounts, credit card (CC) checkers, botnet-as-a-service, flood attacks, spam attacks and online forums dedicated to cyber crime activity, typically sold through darknet forums. These forums play a significant role in connecting and driving cybercrime. Cybercrime forums derive their income from registration fees, advertisements, escrow services and account status upgrades.

Two prominent examples of such forums studied by TRM Labs are Exploit.in and Cracked.io. Exploit is a Russian cybercrime forum established in 2005. Discussions on the forum focus on sharing exploits and vulnerabilities of various computer systems. Exploit is also a marketplace for initial accesses, digital goods, malware and so-called zero-day vulnerabilities – security flaws in a software application or system that are unknown to the vendor or developer and for which no patch or fix has been released.

Cracked is a well-known English-language hacking forum, with more than 3.5 million users and 22.6 million posts on hacking, cracking, leaks and related topics. Cracked also includes a marketplace for illicit products. This platform periodically changes its cryptocurrency wallets.

Bulletproof Hosting

Bulletproof hosting services (BPHS) facilitate illicit threats such as botnets, malware, CSAM content, cybercrime forums and ransomware while providing secure anonymous hosting for malicious content and activity. Not all BPHS are illicit: many DDOS protection services also use the term bulletproof in their advertisements. TRM Labs tracks only entities that allow illicit threats or content to be hosted, and which ignore abuse requests.

Bulletproof hosting providers may ignore abuse requests and other legal requests because they are often based in countries that lack strict internet regulations. Additionally, these providers may take steps to protect the anonymity of their customers and prevent their identities from being revealed. Some bulletproof hosting providers may also require little or no identifying information from customers, making it difficult for authorities to track down the owners of illicit websites. These services are also central to illicit actors layering their identities online to obfuscate their illicit activity.

Most major BPHS entities require manual setup, including, for example, a mass-scan of a network. Some entities also advertise the offerings on their websites, allowing users to choose the configurations for their server from a catalog, and pay in crypto at checkout. BPHS websites such as these often use payment processors.

Credit Card (CC) Checkers

CC checkers are illicit darknet services used to validate compromised payment cards by conducting unauthorized micro-transactions at specific online stores. They are also used to check whether a credit card number is valid according to the rules for that card type, and whether the expiration date and CVV code match the information held by the issuing bank. Some CC checkers may also provide additional information about the card, such as the type of card and the name of the issuing bank.

CC checkers are fully automated in terms of accepting payments. They usually have their own websites and telegram bots, and can also work as built-in checkers within carding shops, by providing their API (application programming interface) to the carding shop. Unlike cybercrime forums or BPHS, CC checkers incur no fixed overhead expenses, which maximizes their profit margins.

4check, a prominent CC checker, raised USD 2.8 million worth of cryptocurrency from 16 Carding/PII (personally identifiable information) shops between January 2016 and October 2022. An on-chain investigation found that the carding shops likely used 4check as a built-in CC checker. Two carding shops, Bypass and Ferum, were 4check's biggest customers, having paid a total of USD 1.2 million each.

Illicit Trafficking of Stolen Goods

Cryptocurrency has long been linked to the receipt and trafficking of stolen goods. The darkweb is replete with illicit marketplaces that accept cryptocurrency in exchange for stolen credit card details, personally identifiable information (PII), counterfeit goods and other products. There have also been reports of darknet-enabled illicit commerce involving antiquities and other significant cultural artifacts.

Carding and Personally Identifiable Information (PII)

Carding and PII shops are entities associated with buying, selling or distributing payment card data and PII using cryptocurrencies. They range from illicit marketplace platforms that act as brokers connecting buyers and sellers of the compromised payment cards and PII data, to individual vendor shops that sell payment card and PII data.

Intellectual Property Crime

Counterfeit products account for between 1.5% and 2.5% of all listings on DNMs, according to Europol estimates. Most of that comprises counterfeit banknotes and fake IDs. Other products available on the darknet that infringe on intellectual property rights include:

- Clothes, textiles and accessories
- Electronics including mobile phones
- Jewelry
- Pirated software
- Pirated e-books
- Pharmaceutical products (especially lifestyle medicines, steroids and hormones)
- Subscriptions to TV channels, music platforms and online game accounts
- Watches

Human Trafficking and Migrant Smuggling

Despite claims that crypto is used as a means of payment for human trafficking, TRM research suggests that the most prominent nexus between crypto and human trafficking is the use of human trafficking to prop up cryptocurrency scams and frauds.

For example, human trafficking victims have been found to be working in illegal call centers run by Chinese criminal syndicates operating cryptocurrency pig butchering scams. These scams rely on psychological manipulation

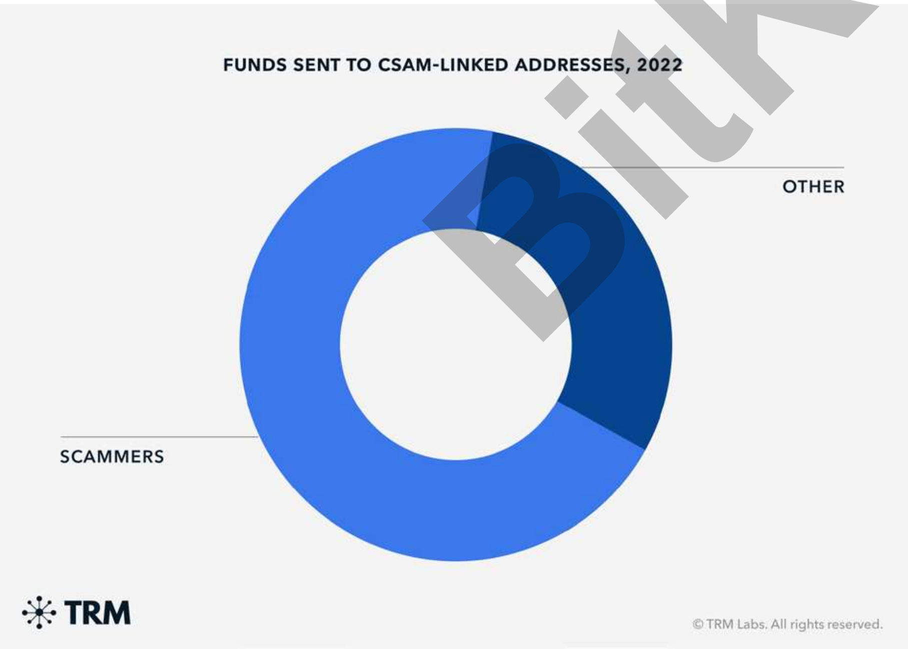
QUICK LINKS

to wipe out victims' life savings on the promise of making large returns on their investments. According to the FBI, people lured by false job advertisements offering lucrative pay later have their passports confiscated and are coerced into committing crypto fraud. More recently, authorities in the Philippines reportedly rescued victims who had allegedly been trafficked to work in a crypto scam call center based in Cambodia.

Child Sexual Abuse and Exploitation Material (CSAM)

CSAM includes imagery or videos that show a child engaged in or depicted as being engaged in explicit sexual activity.

TRM has analyzed over USD 3 million sent to cryptocurrency addresses involved in CSAM activities online in 2022. More than two thirds of those payments appear to have been made to CSAM scammers, who attempt to convince would-be buyers of CSAM images to pay for images or VIP access to galleries that turn out not to exist.



The disproportionate share of funds received by CSAM scammers, who advertise widely on the darknet and deal almost exclusively in cryptocurrency, can be explained at least in part by the fact that true CSAM vendors seldom publicly promote their activity and continue to favor traditional finance channels.

QUICK LINKS

By studying the properties and behaviors of CSAM actors, blockchain intelligence can allow investigators to identify international CSAM networks, profile persistent CSAM customers, and expose vendors that impersonate scammers in order to evade law enforcement attention by hiding in plain sight.

Murder for Hire

The past few years have witnessed a rise in the attempted use of cryptocurrency to pay for contract killings. It should be noted that there have been no publicly documented examples of a completed murder-for-hire scheme paid for in cryptocurrency at the time of publication. However, there is evidence of demand for such services, as shown by the prosecution of several individuals who have attempted to pay for contract killings with cryptocurrency.

In 2022, a Los Angeles man pleaded guilty to a federal murder-for-hire charge after sending USD 13,000 worth of bitcoin to a darknet website to hire a hitman to kill a woman who had rebuffed his advances.

Other instances of people accused of using cryptocurrency to pay hitmen have been reported elsewhere. In 2022, a Mississippi resident received a 10-year prison sentence for attempting to have her husband killed for a USD 10,000 fee in bitcoin.

Such events have not been confined to the US. In 2021, Europol and the Italian police collaborated to arrest a man suspected of paying EUR 10,000 in bitcoin to hire an assassin to kill his ex-girlfriend. In that instance, the virtual asset service provider (VASP) involved in the transfer of the bitcoin to the would-be killer cooperated with authorities in providing details of the suspect.

2. Illicit Payments

Cryptocurrency has been used to evade capital controls and make illicit payments to terrorist groups, corrupt officials or sanctioned jurisdictions and individuals. “More crypto usage is empirically associated with higher perceived corruption and more intensive capital controls,” stated a 2022 working paper from the International Monetary Fund. It found that “countries with weaker control of corruption (more corruption) and lower degree of capital openness (more capital controls) tend to have a larger share of crypto adoption, suggesting that crypto assets may be used to transfer corruption proceeds or circumvent capital controls.”

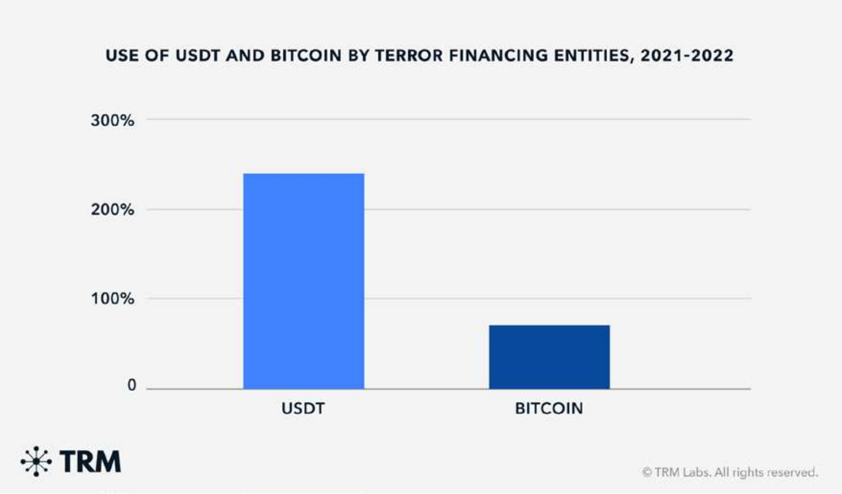
Terrorist Financing

Terrorist financing refers to the provision of financial support to terrorist organizations and individuals involved in terrorist activities. Cryptocurrency has been for terrorist financing due in part to its perceived anonymity and ease of cross-border transfers.

Fundraising campaigns for ISIS families held in internment camps in northeastern Syria has been a significant driver of cryptocurrency usage among ISIS and its supporters. TRM Labs identified dozens of fundraising campaigns that accepted cryptocurrency in 2022, raising between a few dollars to tens of thousands.

TRM Labs also identified multiple pro-ISIS groups in Pakistan and Tajikistan raising tens of thousands of dollars in cryptocurrency to spread propaganda and recruit fighters. Over the course of 2022, TRM Labs has observed a significant increase in the use of the TRON blockchain among terrorist groups and associated fundraising campaigns, with some using it exclusively. The overwhelming majority of those actors collected donations in the stablecoin Tether (USDT). Among the terror financing entities tracked by TRM Labs in 2022, there was a 240% year-on-year increase in the use of Tether - against a mere 78% rise in Bitcoin use.

QUICK LINKS



In 2022, multiple terror financing entities, including Syria-based cryptocurrency exchanges involved in terror financing campaigns, began experimenting with decentralized exchanges. Decentralized exchanges (DEXs) are peer-to-peer marketplaces where individuals can trade cryptocurrencies in a non-custodial manner.

Bribery and Corruption

There have been several high-profile cases of proven or alleged bribery involving crypto. In 2021, FTX founder Sam Bankman-Fried allegedly gave a USD 40 million cryptocurrency bribe to Chinese officials in exchange for unfreezing company accounts containing over USD 1 billion worth of cryptocurrency.

In 2022, the US Department of Justice accused two Chinese intelligence officers of allegedly attempting to bribe a US government employee with USD 61,000 in bitcoin to steal documents related to an investigation into Chinese tech giant Huawei.

Cryptocurrencies can also be used to influence voters during election campaigns. In 2019, a gubernatorial candidate in St Petersburg, Russia, handed out crypto tokens to voters on the campaign trail.

Espionage

Espionage activities can involve the covert transfer of funds to support intelligence gathering or other covert operations. Cryptocurrencies can provide a discreet and secure means of transferring funds, making them an attractive option for state or non-state actors engaged in espionage.

In November 2022, US nuclear engineer Jonathan Toebbe and his wife Diana were sentenced to 18 and 21 years in prison respectively for attempting to pass secret nuclear propulsion technology to a third country. In their exchanges with FBI agents posing as foreign officials, the couple requested payment in the Monero privacy coin.

The use of privacy-focused cryptocurrencies or mixing services can further enhance the anonymity of transactions, making it more difficult for authorities to trace the source or destination of the funds. In December 2022, Iran executed four alleged Israeli spies who were accused of receiving payment in cryptocurrency. That same year, South Korea arrested two of its nationals for allegedly accepting cryptocurrency to spy on behalf of North Korea.

Export Control Evasion

Export control evasion involves using cryptocurrencies to bypass state capital controls and restrictions on the export of certain goods or technology. Individuals can use digital assets to facilitate payments for prohibited items, circumventing traditional financial systems that might flag or block such transactions. A 2019 study by researchers at the Chinese University of Hong Kong, Deakin University and the University of Technology Sydney found that cryptocurrency was being widely used by traders in China to circumvent capital controls.

Sanctions Evasion

US officials have long warned that North Korea, Iran and Russia could use cryptocurrency to evade sanctions. The European Union has also taken steps to prevent crypto from being used by Russia to evade international sanctions imposed after its invasion of Ukraine in 2022.

On-chain analysis has yet to show this happening to a significant degree today. Experts believe this is likely to be due to crypto's current lack of liquidity relative to a country's economy.

Nevertheless, Russia, Iran and North Korea have been observed using crypto to offset the impact of international sanctions by conducting cyberattacks and mining bitcoin: both practices generate revenues that help make up for lost trade and investment. In 2022, the US Treasury Department's Office of Foreign Assets Control (OFAC) sanctioned a Russian cryptocurrency mining company in order to prevent mining from becoming a "mechanism for the Putin regime to offset the impact of sanctions".

OFAC has also sanctioned cryptocurrency addresses related to facilitators of North Korean weapons proliferation and Russian paramilitary groups. Additionally, the US Treasury has used sanctions to target money laundering linked to sanctions evasion. For example, in 2022, OFAC sanctioned Ethereum-based mixing service Tornado Cash for its involvement in laundering hacked and stolen funds by North Korea.

Proliferation Financing

Proliferation financing involves the use of cryptocurrencies to fund the development or acquisition of weapons of mass destruction (WMD) or related materials. By using digital assets, parties involved in proliferation activities can avoid the scrutiny of traditional financial systems and evade international non-proliferation regimes. In April 2023, the US, Japan and South Korea accused Pyongyang of funding its WMD programme using stolen cryptocurrency.

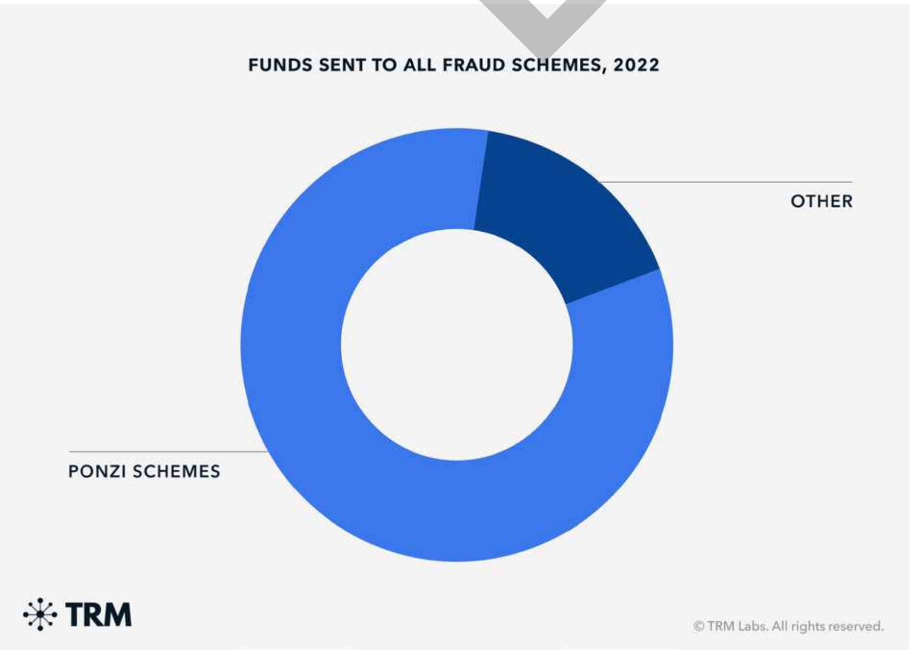
3. Fraud and Scams

Cryptocurrency fraud and scams include investment fraud such as pyramid schemes, insider trading, phishing attacks geared towards stealing private keys and exchange credentials, pig butchering and impersonation-based scams such as business email compromise (BEC). Scammers also resort to attempts at blackmail, in which they claim to possess sensitive or damaging information and demand cryptocurrency payment for its return or suppression.

Although "fraud" and "scam" are often used interchangeably, the cryptocurrency community typically refers to "scams" . Generally, the concept refers to people being deceived into sending cryptocurrency and other digital assets (or clicking on something that enables the transfer) to somewhere that they would otherwise not have done had they known the truth.

Many types of fraud can coexist within the same scheme. For example, a pig butchering scheme can involve a romance scam, an investment scam, an advance fee scam and an asset recovery scam. Equally, an investment scheme operating around a new token can involve market manipulation, a pyramid scheme and an exit scam.

TRM Labs identified about USD 9.04 billion being sent to various types of fraud schemes in 2022, with the large majority going to apparent Ponzi and/or pyramid schemes.



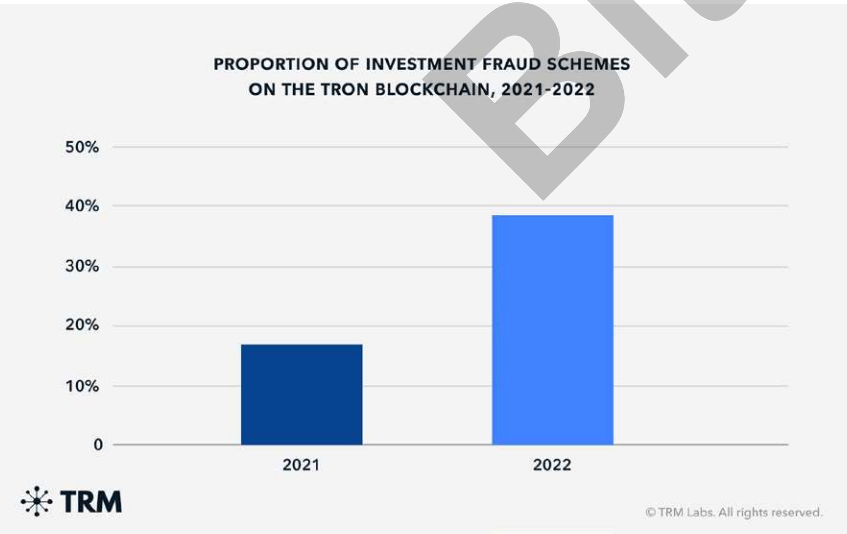
Investment Fraud

Investment fraud centers on the solicitation of funds for fraudulent investments or projects. In the cryptocurrency space, these often involve fake initial coin offerings (ICOs), unregistered securities or fraudulent investment platforms. Investment fraud involving cryptocurrency rose by nearly 200% from USD 907 million in 2021 to USD 2.57 billion in 2022, according to the FBI's annual Internet Crime Report.

Pyramid and Ponzi Schemes

Pyramid and Ponzi schemes are fraudulent investment schemes that rely on the constant recruitment of new investors or investments to generate returns for earlier investors. These schemes often collapse when it becomes impossible to recruit enough new investors or investments to maintain payouts.

TRM Labs identified at least USD 7.78 billion in incoming volume in 2022 related to these types of schemes. Ten of the largest schemes accounted for about 54% of the total amount. Just under 40% of total incoming volume for all investment fraud schemes active in 2022 was on TRON, mostly via USDT, more than double the 17% observed in 2021.



Several major cryptocurrency-based Ponzi schemes were prosecuted in 2022. Two of the largest were Forsage and the Trade Coin Club, while the Bitconnect founder was indicted by the US Department of Justice (DOJ) following charges from the Securities and Exchange Commission (SEC) in 2021.

According to the SEC, Forsage was a cryptocurrency-based Ponzi and pyramid scheme that lured investors with promises of high returns through several smart contracts on Ethereum and BNB Chain in what TRM Labs calls a decentralized investment fraud scheme. TRM Labs research found that the scheme has received nearly USD 400 million since 2020. The apparent successor to Forsage, Meta Force, received about USD 574 million in 2022.

The Trade Coin Club was a Ponzi scheme that claimed to offer high returns through a cryptocurrency trading platform. The platform's operators used new investors' funds to pay returns to earlier investors, and the scheme ultimately collapsed, resulting in significant losses for many participants. The Trade Coin Club raised more than BTC 82,000 – valued at USD 295 million at the time – from more than 100,000 investors between 2016 and 2018, according to charges filed by the SEC in November 2022.

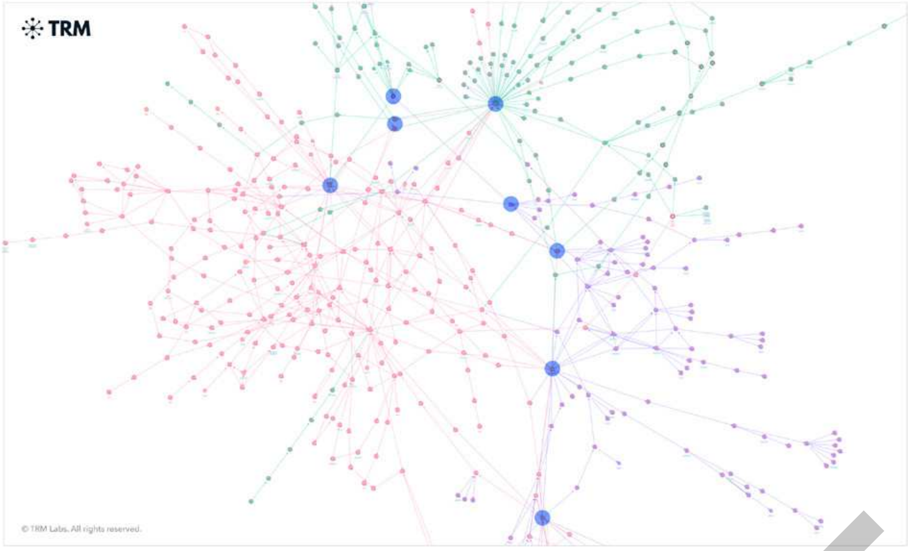
Pig Butchering

Pig butchering scams rely on psychological manipulation and social engineering to wipe out victims’ life savings on the promise of making large returns on their investments. Such scams often include the widespread use of Tether by scammers, significant interconnectivity between individual pig butchering scams, and links to transnational organized criminal groups. Because scams in general are significantly under-reported by victims, it is difficult to quantify the scale of pig butchering globally.

Once cryptocurrency reaches a scammer’s wallet, it is typically shuffled from wallet to wallet in a complex web of transactions between scammers and money launderers (sometimes the same people), with each wallet accumulating funds from additional victims along the way. Funds often move circuitously, making it difficult for investigators to follow the money and to separate victim funds from other tokens.

TRM Labs data indicates that cryptocurrency wallets that receive victim funds from individual pig butchering scams are also often associated with other scams. Over half of the pig butchering schemes studied by TRM Labs up to December 2022 exhibited apparent links to large transnational organized crime groups.

The graph below, of a pig butchering scheme studied by TRM Labs, shows multiple interconnected scams operated by the illicit actors either in succession or simultaneously. In addition, the scammers appear to have relied on a single money laundering network, with the same addresses appearing in multiple cases.



Deceptive Smart Contracts

Deceptive smart contracts are intentionally designed to trick users into transferring funds or granting permissions to them. The most notable example of this is drainware – smart contracts that, upon interaction, grant the attacker permission to move funds from the victim's wallet. Spoof tokens are another form of deceptive smart contracts.

Drainware

Drainware is a type of malicious smart contract that has been referred to as "drainers", "sweepers" and "wallet drainers." Drainware attacks operate by draining cryptocurrency and NFTs (non-fungible tokens) directly from a user's wallet after they unknowingly sign a transaction to purchase and mint an NFT, or interact with a phishing website.

Until its creator shut it down in 2023, Monkey Drainer was one of the latest major drainware tools targeting the crypto industry en masse. The malicious contract required users only to approve and sign transactions, making it simpler than many traditional attack methods. Most of the stolen cryptocurrency from Monkey Drainer was laundered through Tornado Cash. In some cases the fraudsters used intermediary wallets before attempting to cash out stolen funds at three centralized exchanges. Since the demise of Monkey Drainer, others, such as Venom Drainer, have filled the niche.

This dramatic rise in drainware attacks has even led to the emergence of Drainer Templates as a Service (DTaaS), providing ready-to-launch pre-built templates and enabling attackers to launch malicious contracts at scale, as

QUICK LINKS

Part I – Illicit Crypto
3. Frauds and Scams
Investment Fraud
Deceptive Smart Contracts
Exit Scams
Phishing
Impersonation Scams
Business Email Compromise
Illicit Commerce Scams
Blackmail Scams
Other Scams
Misappropriation of Funds
Extortion
Market Manipulation
Insider Trading
Tax Evasion

seen during the 2021 NFT boom. Some drainers also attempt to scam their criminal users, for example by sending high value NFTs or tokens to the original creator of the malicious contract and less valuable tokens to the actor wielding the drainer. This has led to the rise of an entire "scam-as-a-service" industry, offering entire malicious packages complete with a phishing website, discord server bot and smart contract.

Spoof Tokens

SSpoof tokens are crypto tokens – whether new coins or NFTs – set up by scammers who manipulate the tokento make it look like they have been sent from addresses associated with celebrities, high-profile influencers, companies, or specific projects.. Believing them to be popular potentially lucrative, investors are deceived into buying these tokens, when in fact they have no value.

To manufacture spoof tokens, scammers create a new token smart contract and give it a name related to what they are spoofing. They may also modify the smart contract code to enable the scammer to send the token on behalf of other addresses, making it appear that those addresses initiated the transfer.

A recent example of a spoof token was the "Peaceful World" token which purported to be a token airdropped by the Ukrainian government.

Exit Scams

Exit scams, also known as rugpulls, occur when the operators of a project – one often related to investments or a new token – stop developing the project and withdraw user funds for themselves. They can either happen abruptly where project devs and funds suddenly disappear, or they can occur more slowly, where money is siphoned off a bit at a time and devs get less and less active. Sometimes, projects are called rugpulls by the community when they overpromise and underdeliver, though this is more difficult to outright label as fraud.

Often they target decentralized finance (DeFi) projects. In a rugpull related to a new token, the project creators can withdraw liquidity from the trading pool, causing the value of the associated tokens to plummet. Investors are left with worthless tokens and no way to recover their funds. Many pyramid and Ponzi schemes end in exit-scam-like behavior, where payouts stop being made to investors and the creators of the scheme take the remaining funds and disappear.

In June 2022 the US Department of Justice charged a Vietnamese national with one count of conspiracy to commit wire fraud and one count of conspiracy to commit international money laundering. Le Ahn Tuan had created an NFT project called Baller Ape Club, which sold NFTs of cartoon monkeys. According to the indictment, once Tuan and his co-conspirators had collected some USD 2.6 million from investors, they carried out a rugpull, ending the purported investment project, deleting its website, and stealing the investors' money.

Frosties NFT was another NFT project that promised exclusive digital art and collectibles. However, shortly after the project's launch the two 20-year-old creators shut down its website and Discord servers, removed the liquidity from the trading pool and disappeared with USD 1.1 million of investors' funds. According to the DOJ complaint, the duo transferred the proceeds from the scheme to various cryptocurrency wallets under their control in multiple transactions designed to obfuscate the original source of funds. They were later arrested and charged with wire fraud and conspiracy to commit money laundering.

Phishing

Phishing involves the use of fraudulent emails, websites, or messages to trick users into revealing sensitive information, such as private keys or login credentials. In the cryptocurrency space, phishing attacks may target users of digital wallets or exchanges, leading to the theft of funds.

Crypto-related phishing attacks grew in prominence during the 2017 Initial Coin Offering (ICO) boom. Victims targeted in these phishing attacks would only lose the amount of cryptocurrency they sent to the wrong address in error. As NFTs entered the mainstream, attackers began to target novice NFT investors by exploiting the "FOMO" – fear of missing out – and hype surrounding the NFT world.

TRM Labs has observed hundreds of phishing attacks over the last year targeting NFT projects, where real-time messaging across multiple platforms has enabled attackers to target NFT investors by publishing phishing website links at a rapid pace. Phishing attacks linked to NFT minting scams deployed through compromised Discord accounts grew rapidly in 2022. A review of more than 15 notable Discord compromises targeting NFT servers and analysis of on-chain and off-chain data by TRM investigators suggest that dozens of these recent account compromises are likely related.

"Address poisoning", a relatively new type of phishing, rose to prominence in 2022. It involves the scammer creating an address that resembles one to which the intended victim had previously sent funds. The scammer then sends a small amount of cryptocurrency to the target in the hope that they will unwittingly make a future payment to that scam address in place of their intended recipient.

Impersonation Scams

Related to phishing, impersonation scams involve criminals posing as well-known individuals or organizations to deceive victims into sending funds or revealing sensitive information. In the cryptocurrency space, impersonation scams may involve criminals pretending to be representatives of exchanges, wallet providers or celebrities to trick users into sending cryptocurrencies to fraudulent addresses or divulging sensitive information.

Scammers can create fake websites or social media accounts that resemble legitimate crypto exchanges or wallet providers. They impersonate customer support agents and reach out to unsuspecting users, offering assistance with technical issues or account problems. The users are persuaded to share their login credentials, private keys, or sensitive information, allowing the scammers to steal their funds.

Similarly, scammers also create fraudulent websites, social media accounts, or email campaigns to impersonate legitimate crypto projects. Unsuspecting users send their cryptocurrencies, but the scammers disappear with the funds, leaving investors with nothing.

Business Email Compromise

Business email compromise (BEC) is a type of scam where criminals impersonate a legitimate business or organization to trick employees or partners into transferring funds or revealing sensitive information.

BEC scams may involve the compromise of email accounts belonging to employees of exchanges, wallet providers, or other organizations, leading to the theft of funds or sensitive data. In 2022, BEC accounted for USD 2.7 billion (crypto and fiat) in losses reported by victims to the FBI's Internet Crime Complaint Center (IC3).

Illicit Commerce Scams

For almost every type of illicit commerce or activity in the crypto space, there is a scam version of it, sometimes found on the dark web. TRM Labs has found scam money laundering services, carding shops, drug vendors, murder-for-hire providers, weapons dealers, CSAM sellers, hacking services, market manipulation services, scam-as-a-service providers and ransomware sellers.

Blackmail Scams

Blackmail scams typically involve the scammer sending threatening emails to random recipients, claiming knowledge of infidelity, pornography use or other potentially embarrassing personal details that would be released publicly unless a cryptocurrency payment was made.

In many cases, the scammer does not in fact have the information in question. The most common type appears to be "sextortion", where the scammer emails hundreds or thousands of people claiming to have installed malware on their computer or phone that recorded the recipient viewing pornographic sites. They then instruct the intended victim to send cryptocurrency – usually bitcoin – to the scammer in order not to have the videos sent to their friends and family.

Other Scams

Scammers are creative and can make a scam version out of nearly any activity. As such, there are many other types of scams than those mentioned in this paper. They include asset recovery scams, overpayment scams, money mule scams, different variations of the advance-fee scam, and the basic scam of simply not giving the buyer what they purchased.

Misappropriation of Funds

Misappropriation of funds often occurs as part of many of the other frauds and scams mentioned here, though it can also occur independently. It is related to, but in some jurisdictions is a separate crime from, embezzlement.

Misappropriation of funds frequently accompanies investment fraud schemes, where, instead of investing customer funds as promised, the operator of the scheme instead diverts them either for personal use – such as to buy luxury goods – or for other business purposes. For example, the SEC alleges that the former CEO of Alameda Research "used misappropriated FTX customer funds for Alameda's trading activity."

In 2021, a Microsoft employee was arrested for allegedly misappropriating USD 10 million in company funds by secretly creating thousands of official XBox gift card codes that he then sold at a discount online in exchange for cryptocurrency.

Extortion

Crypto extortion can take many forms. At its most basic, it involves individuals threatening their victims and demanding payment in cryptocurrency. It can also involve the use of malicious software known as ransomware. As such, it is often prosecuted in the US under fraud statutes.

In May 2023 a former employee of a public New York-based technology company was sentenced to six years in prison for stealing company files and demanding nearly USD 2 million for their return. In 2019, a group of Russian secret service agents were reported to have extorted a media mogul in exchange for USD 670,000 worth of bitcoin.

Other variations of extortion begin with the scammer using phishing techniques to take control of the victim's Instagram profile. The criminals then force the victims into filming videos instructing their followers to participate in fraudulent get-rich-quick Bitcoin schemes.

Yet by far the biggest driver of crypto extortion is ransomware, which has also increasingly been adopted by groups targeting countries' national security infrastructure (see below).

Ransomware

Ransomware is a type of malicious software that encrypts a victim's files or data, rendering them inaccessible. The attacker then demands a ransom, usually in cryptocurrency, in exchange for the decryption key. Ransomware has become a significant threat to individuals, businesses, and even governments, with high-profile attacks making headlines.

Two of the most significant ransomware syndicates in recent years have been LockBit and Conti. LockBit largely focused on government facilities, healthcare and public health, and the financial services sector. Conti most frequently targeted critical manufacturing, commercial facilities, and the food and agriculture sectors. Lockbit, the most prolific ransomware group, has received at least USD 100 million in payments since its inception, and USD 44 million in 2022 alone, according to TRM Labs analysis of on-chain data.

The Russian invasion of Ukraine led to significant changes in the Russian-speaking ransomware ecosystem. TRM Labs analysis of on-chain transactions, open source reporting, and proprietary information indicates that LockBit and Conti restructured, probably to avoid sanctions by Western countries. Conti shut down its operations and rebranded into at least three smaller groups – Black Basta, Karakurt, and BlackByte.

QUICK LINKS

Part I – Illicit Crypto

3. Frauds and Scams

Investment Fraud
Deceptive Smart Contracts
Exit Scams
Phishing
Impersonation Scams
Business Email Compromise
Illicit Commerce Scams
Blackmail Scams
Other Scams
Misappropriation of Funds
Extortion
Market Manipulation
Insider Trading
Tax Evasion

Blackmail

Blackmail can be perpetrated by outside hackers or disgruntled employees with access to corporate information. For example, in 2022 a former worker at an internet provider in the UK was sentenced to two years and four months in prison for attempting to blackmail a senior manager whose hard drive he had hacked into, transferring him GBP 40,000 worth of bitcoin.

Scammers can also use the empty threat of blackmail to convince victims to transfer cryptocurrency to them – that practice is known as crypto blackmail scams.

Kidnap for Ransom

Kidnap-for-ransom schemes involve the abduction of individuals and the subsequent demand for a ransom in exchange for a victim's release.

The use of cryptocurrency in kidnappings has been reported all over the world. In 2020, an armed gang kidnapped a lawyer in Mexico city and demanded nearly USD 100,000 in bitcoin to secure her freedom, while criminals in India set a USD 2.3 million ransom for the release of a kidnapped boy. Both incidents followed the 2019 kidnapping of a wealthy Norwegian woman by captors who reportedly sought over USD 10 million in cryptocurrency.

Market Manipulation

Market manipulation in the cryptocurrency space can involve various schemes designed to artificially influence the price of a cryptocurrency or token. These schemes can include pump and dump schemes, scalping, touting, and front-running.

One of the most prominent recent examples of this practice took place in October 2022, when the Solana-based platform Mango Markets lost around USD 115 million when a group manipulated its price oracle, the authority that determines a token's value. The hackers' self-proclaimed leader, Avraham Eisenberg, later revealed his identity and characterized his team's activities as a "highly profitable trading strategy" rather than a hack.

Eisenberg initially reached an agreement with Mango Markets to return around USD 70 million in exchange for a promise not to pursue criminal charges against him. Nevertheless, he was arrested by US officials in December 2022 and charged by the SEC with violating anti-fraud and market manipulation provisions of the securities laws. Eisenberg was later also sued by Mango Markets to return his remaining USD 47 million plus interest.

QUICK LINKS

Part I – Illicit Crypto

3. Frauds and Scams

Investment Fraud

Deceptive Smart Contracts

Exit Scams

Phishing

Impersonation Scams

Business Email Compromise

Illicit Commerce Scams

Blackmail Scams

Other Scams

Misappropriation of Funds

Extortion

Market Manipulation

Insider Trading

Tax Evasion

Also in December 2022, the SEC charged leaders of Alameda Research and FTX with manipulating the price of FTX's FTT Token "by purchasing large quantities on the open market to prop up its price."

Pump and Dump Schemes

Pump and dump schemes involve the coordinated buying of a cryptocurrency or token to inflate its price artificially, followed by a coordinated sell-off once the price has reached a certain level. This results in the price crashing, leaving unsuspecting investors with significant losses. These schemes are often organized through online forums or social media groups and can involve the use of misleading or false information to entice new investors.

Thousands of online chat rooms in the deep and dark web as well as public chat channels on Telegram are dedicated to pump and dump schemes, some with as many as four million subscribers in a single room.

Researchers at the Centre for Blockchain Technologies at University College London (UCL) studied data from almost five million deep and dark web messages gathered by Cloudburst Technologies, a crypto market monitoring company, relating to cryptocurrency price manipulation fraud. The researchers found that pump and dump schemes amounted to as much as USD 120 billion in annual crypto volumes. Geolocation-aided analysis found that the US was the leading source of pump and dump, followed by Iran, Iraq, Yemen, Pakistan, Egypt, Saudi Arabia, the United Arab Emirates, Turkey and Russia.

Many pump and dump schemes also exhibit the characteristics of scams. For example, organizers and higher-ranking members of a Telegram group may provide trading signals to other group members several minutes after they have already traded. This helps the leaders of the group profit at the expense of the other members, who are misled to believe that they will profit by buying or selling the relevant token at the organizers' direction.

Touting

When an individual promotes a cryptocurrency or other digital asset defined as securities without disclosing that they are being paid by their issuers, that is known as touting - an illegal practice under US federal securities laws. Over the past five years, several celebrities have been sanctioned by the SEC for violating touting laws when promoting Initial Coin Offerings (ICOs).

In one particularly high-profile case, in October 2022, the SEC charged Kim Kardashian West for touting on social media a “crypto asset security” offered and sold by EthereumMax without disclosing that she was paid USD 250,000 to do so. Kardashian paid USD USD 1.26 million in penalties, disgorgement, and interest to settle the charges.

In March 2023, the SEC charged eight other celebrities, including Lindsay Lohan and YouTube influencer Jake Paul, with touting. Most of the defendants paid to settle the charges.

Front-Running

Front-running involves individuals or groups exploiting their access to information or trading systems to profit from upcoming trades. This can involve using privileged access to exchange order books or exploiting the latency of decentralized exchanges to execute trades before other users. Front-running can lead to price manipulation and undermine the integrity of the market. However, unlike insider trading (see below), in the crypto world front-running may not necessarily be illegal.

A 2022 paper by academics at the University of Technology Sydney found that up to a quarter of new crypto listings at a major US exchange between September 2018 and May 2022 were affected by front-running. Such activity generated up to USD 1.5 million in profits for those involved.

One example is the popular use of Maximal Extractable Value Bots (MEV Bots), which operate based on publicly available blockchain information. MEV Bots can have extremely high amounts of activity and have played a role in several large scale exploits, including Nomad.

Insider Trading

Crypto insider trading entails the use of non-public information to purchase cryptocurrency or other digital assets ahead of exchange listing announcements and profiting from the price surge that follows an announcement. As much as USD 24 million worth of ERC20 tokens was linked to insider trading in 2022 alone, generating at least USD 5.5 million in profit for the traders, according to proprietary research by Argus Inc, a blockchain insider trading and front-running analytics firm. Many of these wallets have continued to be active into 2023.

QUICK LINKS

In June 2022 a former employee of an NFT marketplace became the first individual to be charged with wire fraud and money laundering in connection with a scheme to commit insider trading in NFTs by using confidential information about what NFTs were going to be featured on the exchange's homepage. Others have since faced similar charges.

Tax Evasion

Cryptocurrency "poses a significant detection problem by facilitating illegal activity broadly including tax evasion", according to a US Treasury report released in 2021. High net worth individuals may shift taxable assets into the crypto economy to avoid tax, as governments may not be able to trace crypto income or transactions if they go unreported by exchanges, businesses and other third parties.

A 2022 study found that crypto investors were likely paying less than half the taxes they owed. In response to these tax evasion concerns, in 2022 the European Commission proposed an amendment to the Directive on Administrative Cooperation (known as DAC8) that would widen tax reporting and information sharing requirements relating to holders of crypto and some NFTs. The new rules are likely to come into force in mid-2023.

4. Theft

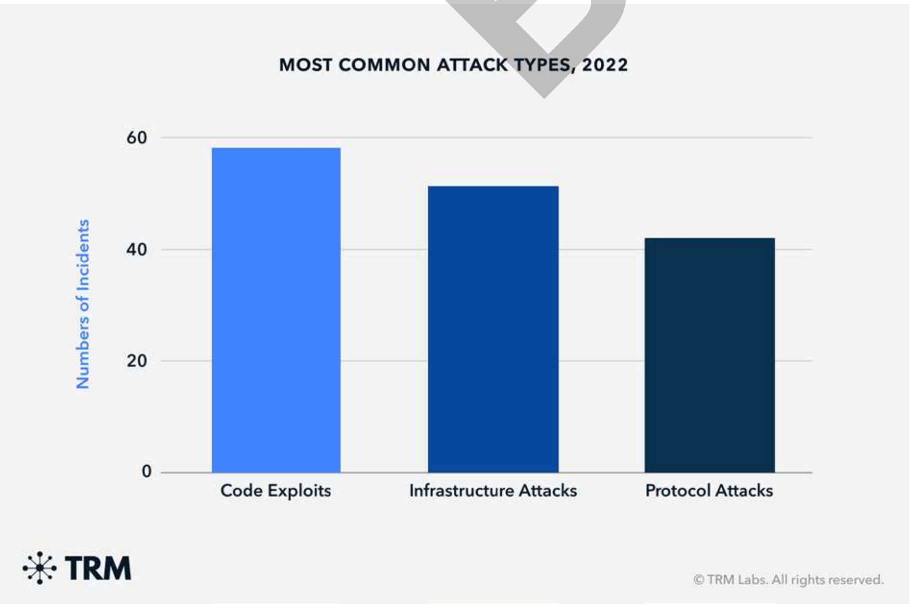
Theft is the biggest driver of crypto crime. It comprises a wide array of malfeasance, from hacks and exploits to robbery. In total, nearly USD 4 billion was stolen in 2022 through the main types of crypto theft studied by TRM Labs.

Hacks and Exploits

The year 2022 was the biggest on record for cryptocurrency hacks and exploits, with about USD 3.7 billion stolen across over 175 incidents, according to a review of attacks by TRM Labs. The average hack was over USD 20 million per incident.

Hacks and exploits can be divided into smart contract and infrastructure attacks. The former group encompasses code exploits and protocol attacks; the latter includes private key theft and SIM swapping, among others.

Nearly 90% of the USD 3.7 billion stolen last year was through infrastructure attacks and code exploits, with most of the remaining value stolen from protocol attacks. The most common attack type in 2022 were code exploits, at 57 incidents, followed by infrastructure attacks (52) and protocol attacks (45). There were nearly 15 attacks per month on average in 2022, roughly one hack every two days.



QUICK LINKS
Part I – Illicit Crypto
4. Theft
Hacks and Exploits
Robbery

Attacks against DeFi projects were more common and damaging than attacks against CeFi targets in 2022, with approximately 80% of all stolen funds, or USD 3 billion, involving DeFi victims and nine of the ten largest attacks occurring against DeFi projects. Flaws in smart contracts, a key component of DeFi that facilitate automation and transparency, provide attackers a seemingly endless supply of bugs to exploit.

Smart Contract Attacks

Smart contracts are self-executing computer programs that are stored on a blockchain and are used to automate the execution of transactions. In a smart contract attack, hackers target bugs or vulnerabilities in smart contracts to steal funds, manipulate data, or disrupt the functionality of the service. Code exploits and protocol attacks are types of smart contract attacks.

Code Exploits

Code exploits target a project's smart contract code and allow an attacker to remove funds from DeFi protocols without authorization. Code exploits are facilitated by coding mistakes and errors, such as unchecked external calls, access control issues, and logic bugs. Of the USD 1.4 billion stolen via code exploits in 2022, authentication issues, improper validation, and signature verification issues accounted for about 90% of the amount stolen.

In February 2022, Solana's Wormhole bridge was targeted in a hack resulting in over USD 300 million being removed from the DeFi protocol. According to the Wormhole team, the hacker managed to exploit the Solana VAA verification and mint tokens. The hacker then utilized the Wormhole bridge to hop chains to Ethereum.

Protocol Attacks

Protocol attacks target weaknesses in the underlying protocol or business logic of a cryptocurrency system. Although this was one of the most common attack types in 2022, the average protocol attack was only half as damaging as the average hack. Over 50% of the total amount stolen from protocol attacks came from price manipulation techniques, such as oracle issues and flash loans. It is common for attackers to combine attack techniques in protocol attacks to achieve the desired result, such as leveraging flash loans and governance attacks.

In October 2022, Sovryn, allegedly the first DeFi protocol on Bitcoin, was attacked resulting in an approximate loss of USD 1 million. In the attack, the hacker utilized a vulnerability in pricing and executed a flash loan. Despite a majority of the funds being returned, the attacker managed to use ThorSwap to hop chains to Bitcoin.

Governance attacks are a type of protocol attack where a hacker manipulates a blockchain project that uses decentralized governance by gaining enough voting rights to reshape the rules. A DeFi credit-based stable coin protocol known as Beanstalk was attacked in April 2022 resulting in a loss of USD 182 million. The attacker utilized a flash loan to exploit the DeFi protocol's governance. With the USD 182 million, the attacker gained controlling ownership in the protocol providing the ability to influence votes.

Infrastructure Attacks

Infrastructure attacks target the systems, platforms, or services that support the creation, exchange, or storage of cryptocurrencies. These types of attacks are often facilitated by traditional cyber attacks or exploits. Techniques include private key or seed phrase theft and SIM swapping.

Private Key Theft

The most damaging type of infrastructure attacks in 2022 were private key or seed phrase thefts, which allow an attacker to commandeer and drain a victim's wallet. Private key or seed phrase compromises accounted for nearly USD 1.5 billion in stolen funds, or 85% of all infrastructure attacks, in 2022. Other types of infrastructure attacks, such as front-end compromises and DNS hijacking, accounted for about USD 250 million in stolen funds in 2022.

In March 2022, Ronin Bridge was attacked, leading to a loss of over USD 600 million. According to a post mortem from Ronin, the attacker was able to drain 173,600 Ethereum and USD 25 million USDC by stealing private keys to forge fake withdrawals. In April 2022, the FBI publicly attributed the attack to Lazarus Group and APT38, cyber actors associated with North Korea.

SIM Swapping

SIM swapping involves the hijacking of a victim's phone number in order to fraudulently authenticate the movement of funds out of their account. In 2022 a Florida man was sentenced to 18 months in prison for a 2018 SIM swap attack that allowed his co-conspirators to hijack the victim's phone number and fraudulently transfer over USD 23 million in cryptocurrency away from his crypto wallet.

Robbery

Cryptocurrency robberies involve the use of force, coercion, or threats to physically steal cryptocurrencies from victims. Sometimes known as "five dollar wrench attacks", such robberies can occur during in-person transactions, such as buying or selling cryptocurrencies, or in more sophisticated and organized criminal operations.

In 2022, police in Sweden were called to an incident involving an assault on a couple by armed strangers who broke into their home, tied them up, and forced them to transfer their cryptocurrency at gunpoint. During the same year, a Canadian man was held at gunpoint, tied up and assaulted during an in-person deal to exchange bitcoin for cash.

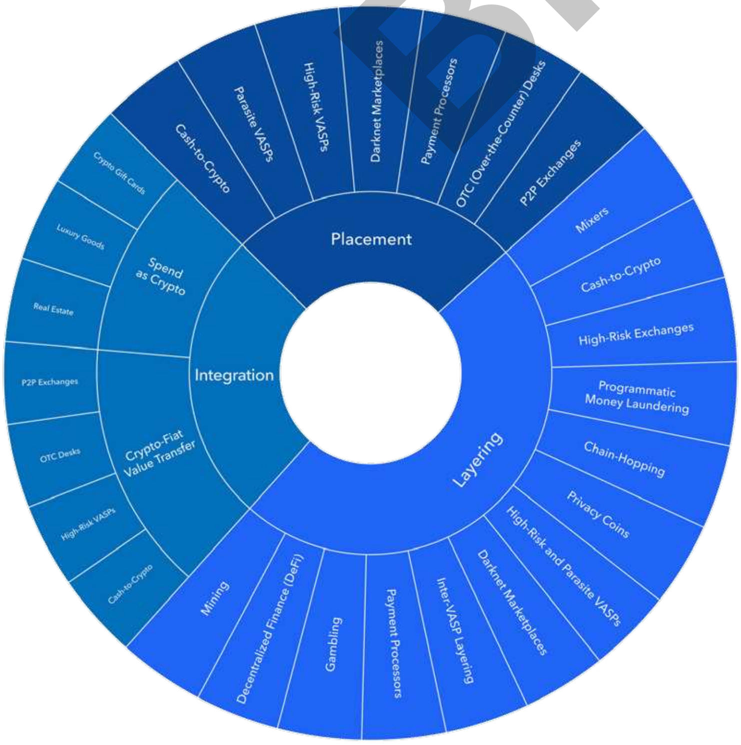
Part II

Money Laundering

Money laundering amplifies the total amount of illicit activity in the ecosystem because all transactions made to try to launder funds are themselves illicit. It involves processing the criminally-derived funds in order to disguise their illicit origin. This is done largely through the abuse of otherwise legitimate tools, such as privacy coins and cash-to-crypto services. However, money launderers also leverage darknet markets and cybercrime services, creating a multiplier effect on total illicit activity.

Cryptocurrency services are attractive to money launderers for many of the same factors appreciated by regular consumers: fast transfers, pseudo-anonymity and convenience. Criminals are interested in collecting funds via a non-reversible format that is nearly instantaneous.

Money laundering involving cryptocurrency largely follows the same path as its conventional counterpart, starting with placement, followed by layering and integration. This section maps the key mechanisms for money laundering within the crypto ecosystem.



QUICK LINKS

- Part II – Money Laundering
- 1. Placement
- 2. Layering
- 3. Integration

1. Placement

During this initial stage of money laundering, criminals can use the profits obtained through illegal activity to purchase cryptocurrencies. In cases where the initial funds are received in cryptocurrency, for example from theft, extortion or illicit commerce, placement involves obscuring their origins and converting them into more widely-accepted or less traceable forms.

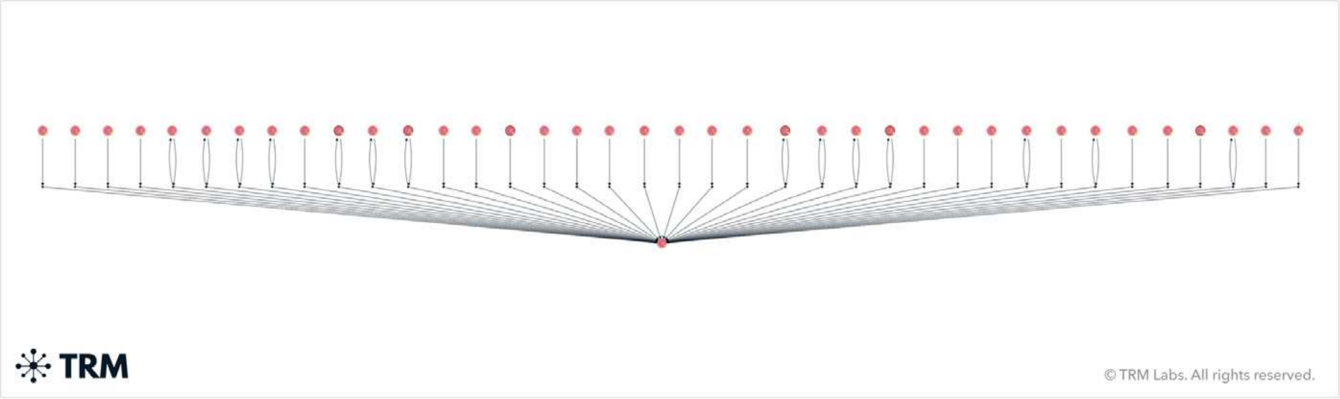
The form that placement takes depends on the type of predicate crime and the service used. In cases of fraud, particularly pig butchering and romance scams, victim funds often enter the crypto ecosystem through cash-to-crypto services. Ransomware perpetrators, on the other hand, tend to require victims to use a third-party service or VASP in order to make a payment.

Cash-to-Crypto

Among the fastest ways to convert fiat currency into cryptocurrency and vice-versa is through cash-to-crypto services. Of these, crypto ATMs are the most popular. These kiosks allow customers to insert banknotes, buy cryptocurrency and send it directly to a wallet without needing an exchange or even a bank account. There are over 30,000 crypto ATMs around the world, over 90% of which are located in North America.

Crypto ATMs and other cash-to-crypto services are not illegal; however, they can be an appealing payment method for cybercriminals and other illicit actors. In 2022, over USD 40 million was sent to known scam addresses via cash-to-crypto services, according to research by TRM Labs. These addresses were linked to perpetrators of romance scams, investment scams, impersonation scams and others as neutral platforms enabling payment by victims.

QUICK LINKS
Part II – Money Laundering
1. Placement
Cash-to-Crypto
Parasite VASPs
High-Risk VASPs
Darknet Marketplaces
Payment Processors
OTC (Over-the-Counter) Desks
P2P Exchanges



In the case shown above, a single exchange address received funds from 40 different cash-to-crypto services ATMs located all over North America. The same address was reported in multiple public reports and investigations as being used by scammers as an aggregator and off-ramp for stolen funds. In this case, the significant number of transfers from multiple cash-to-crypto service locations to the same address served as the trigger for investigators to identify the suspicious destination address.

As a reflection of the use of cash-to-crypto services by illicit actors, state and local police departments regularly receive reports of victims being coerced into sending cryptocurrency to fraudsters through crypto ATMs. These victim payments are often representative of placement in the money laundering context.

In March 2023, authorities in New York arrested a man accused of helping to launder over USD 1 million in fraudulently-obtained small business loans which were offered as part of the US government's COVID-19 relief strategy. He allegedly converted some of the funds to bitcoin and "used a portion of the rest to start his own lucrative cryptocurrency ATM business."

Parasite VASPs

Parasite VASPs rely on the architecture of a larger exchange to provide digital assets trading services to users, often without the knowledge or consent of the host exchange. Criminals and sanctioned individuals may use parasite VASPs to move their illicit proceeds through the crypto ecosystem to make the transactions appear legitimate. Parasite exchanges usually have weak to non-existent Know-Your-Customer (KYC) and AML requirements, which can make them a preferred vehicle of cybercriminals and money launderers for moving funds.

Parasite exchanges facilitate as much as 100 times more illicit on-chain activity than their mainstream counterparts, according to research by TRM Labs. Funds linked to sanctioned entities account for over half of the illicit volume processed by parasite exchanges. This is partly because nearly two-thirds of parasite exchanges appear to be based in Russia and Iran, with the Iranian exchanges being sanctioned based on their jurisdiction. SUEX, a crypto exchange and OTC broker sanctioned by OFAC in 2021, operated as a parasite exchange and was complicit in laundering millions of dollars for Russian ransomware groups.

Parasite exchanges were also found to play an important role in the Russian darknet market ecosystem, resulting in significant exposure to Hydra - the world's largest DNM until its sanctioning by OFAC in April 2022. Even controlling for sanctions exposure, TRM Labs research found parasite exchanges to carry 45 times more illicit exposure than compliant exchanges, as a percentage of their volume.

QUICK LINKS

Part II – Money Laundering

1. Placement

Cash-to-Crypto

Parasite VASPs

High-Risk VASPs

Darknet Marketplaces

Payment Processors

OTC (Over-the-Counter) Desks

P2P Exchanges

High-Risk VASPs

High-risk exchanges and other VASPs are characterized by lax compliance controls or are located in jurisdictions with weak regulatory oversight, which makes them attractive channels for money laundering activities. Over the course of 2022, TRM Labs tracked more than 500 active high-risk exchanges that together transferred tens of billions of dollars in value.

High-risk VASPs share a combination of the following characteristics:

- Exhibit elevated counterparty risk exposure to darknet marketplaces, scams, cybercrime services and other incidence of illicit on-chain activity such as money laundering
- Facilitate transactions using accounts of other exchanges without having a contractual relationship with them
- Use multiple accounts registered under fake or stolen identities to distribute their trading activity, making it harder for the host exchange to detect them
- Have inadequate KYC and AML procedures as well as weak or non-existent identity verification processes, making it easier for criminals to use these platforms for illegal activities
- Offer services that allow users to directly convert cryptocurrencies to cash or vice-versa, which helps to anonymize funds and avoid detection of illicit activities by authorities
- Operate from sanctioned jurisdictions or those listed on FATF Black and Grey lists

Darknet Marketplaces

In addition to their primary role in crypto crime – the sale of illicit drugs – darknet markets (DNMs) are also involved in the laundering of proceeds from crime. Over the course of 2022, TRM Labs has witnessed a rise in international criminals using Russian-language DNMs to launder money.

Payment Processors

Cryptocurrency payment processors are legitimate services that help individuals and businesses accept cryptocurrency as payment. These payment processors create payment addresses for customers and provide services that allow them to accept payments directly from their own websites, such as via an API, in return for a small percentage of the transaction value.

Payment processors can be abused by criminals seeking to launder money, most commonly in placement and layering. Lightly regulated, they often have little to no KYC. By allowing users to create new addresses for every payment – or in some cases, reuse addresses for different actors – payment processors can make it more difficult for investigators to follow the flow of funds.

OTC (Over-the-Counter) Desks

OTC desks allow users to exchange crypto for fiat and vice-versa without a centralized exchange or broker. They tend to specialize in larger sums. Although some established exchanges have proprietary OTC operations that are subject to stringent oversight, many private OTC brokers do not perform KYC or source of wealth checks on their customers. As a result, such OTC brokers are vulnerable to abuse by criminals seeking to cash out illegally-derived cryptocurrency.

P2P (Peer-to-Peer) Exchanges

P2P exchanges operate on the same principle as OTC desks: they enable users to change between cryptocurrencies and fiat. However, unlike OTC desks that are manned by brokers, P2P exchanges operate as fully automated DeFi entities. They operate by connecting trading partners seeking to buy or sell cryptocurrency without a third party intermediary. Some of these transactions can be arranged using cash or other non-crypto payment methods via the P2P platform.

2. Layering

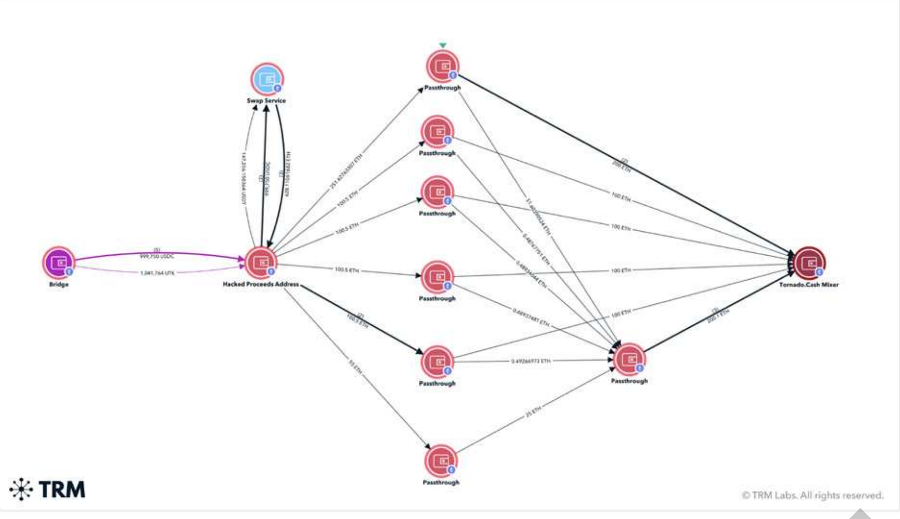
Layering is designed to make the tracing of illicit assets more difficult by putting them through a series of transactions and by using a variety of tools. Mixers, bridges, swap services, and coin-joins – individual transactions where multiple senders combine funds to obfuscate their source – are commonly used for layering as they are designed to enhance privacy and make it more difficult for investigators to trace the flow of funds. While some will simply funnel funds to exchanges in order to cash out quickly, advanced launderers may incorporate programmatic money laundering techniques.

Data science models that can identify different types of money laundering patterns (called Signatures) are an essential toolkit for money laundering investigators, as is the ability to demix transactions from mixers and automatically trace through cross-chain bridges.

Mixers

Mixers, also known as tumblers, are services that blend multiple cryptocurrency transactions, making it difficult to trace the origin and destination of funds. According to the US Treasury's National Money Laundering Risk Assessment from 2022, mixers and tumblers "help criminals hide the movement or origin of funds, creating additional obstacles for investigators."

Mixers are not illegal; nor are they used exclusively for illicit activity. For example, many mixers advertise themselves as means to increase privacy and anonymity online. However, mixers are also frequently used by cybercriminals as a layering technique to disguise the source of illicit funds. The graph below shows an illicit actor using the Ethereum-based mixer Tornado Cash to obfuscate around USD 1 million of proceeds from a hack. After migrating the funds to the Ethereum blockchain and swapping them from USDC to ETH, the actor sends them to various wallets before depositing them into Tornado Cash.



© TRM Labs. All rights reserved.

In August 2022, OFAC sanctioned Tornado Cash, which has been used by North Korean cyber-criminals and other threat actors to launder the proceeds of hacks and other illicit activity. TRM Labs showed that North Korean cyber actors used Tornado Cash to launder over USD 1 billion of stolen funds in at least ten major cryptocurrency heists.

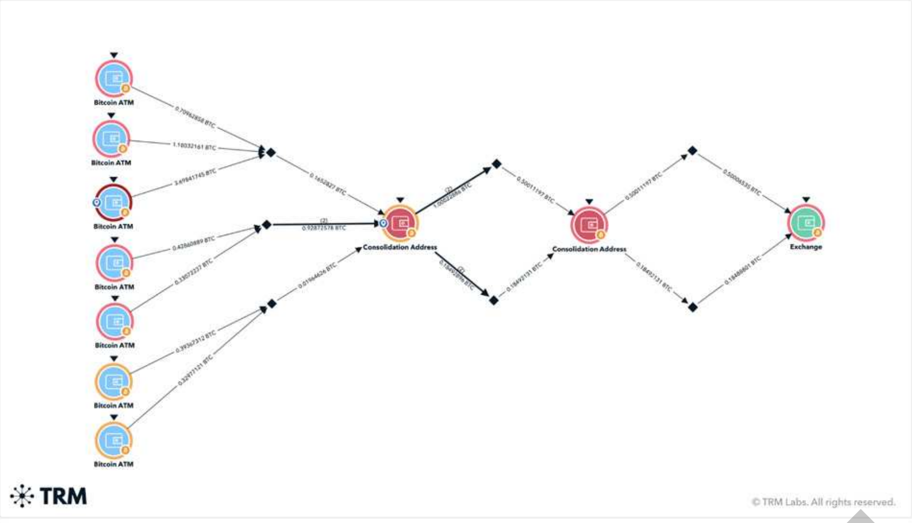
In March 2023, German and US authorities, supported by Europol, announced the shutdown of ChipMixer, a cryptocurrency mixing service that facilitated international money laundering. During the operation, officials seized four servers and nearly USD 44.2 million in cryptocurrency. Research by TRM Labs confirms that ChipMixer was widely used by prominent ransomware syndicates to launder illicit proceeds. Among them were Karakurt, SunCrypt, REvil, Conti, LockBit, Ragnar Locker, and Royal. TRM Labs research also found at least 20 darknet marketplaces (DNMs) that sent funds to ChipMixer during the mixer's nearly six years of activity.

Cash-to-Crypto

Cash-to-crypto services can be used for layering through a laundering technique called money muling or smurfing. This entails the transfer of stolen funds by individuals unconnected to the original crime.

In the example below, in August 2022 a money laundering group deposited illicitly-obtained cash from into several crypto ATMs. From there, the funds, now in bitcoin, were sent to a consolidation wallet before being deposited at a large exchange.

QUICK LINKS
Part II – Money Laundering
2. Layering
Mixers
Cash-to-Crypto
High-Risk Exchanges
Programmatic Money Laundering
Chain-Hopping
Privacy Coins
High-Risk and Parasite VASPs
Darknet Marketplaces
Inter-VASP Layering
Payment Processors
Gambling
Decentralized Finance (DeFi)
Mining



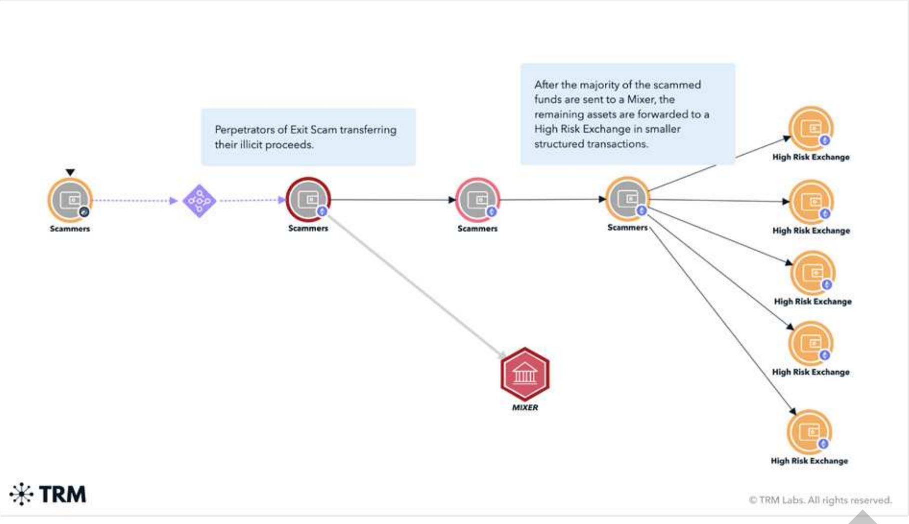
In April 2023, a Missouri woman was arrested on charges of assisting with the movement of stolen funds. The suspect used cashiers checks and cryptocurrency ATMs to transfer USD 565,000 on behalf of the criminals that committed fraud in order to steal the victim's funds. As smurfing can take place by unwitting third parties, it is often difficult to identify as the person committing the layering activity may not be aware of the source or destination of the funds.

High-Risk Exchanges

High-risk exchanges are significantly more exposed to illicit counterparties than regulated exchanges, according to TRM Labs research. Some high-risk exchanges also operate as parasite exchanges, and usually have lax or non-existent KYC and AML processes. This makes them attractive platforms for cybercriminals who want to launder money or fund illicit activities. Administrators of such exchanges claim to earn 0.5%-1.0% commission on the transaction volume, depending on the share of revenue allocated to advertising and affiliate marketing necessary to drive traffic to their exchange.

In the example below, after hopping chains and diverting some of their stolen funds to a mixer, a scammer sends the remainder of the ill-gotten proceeds to a series of accounts at a Russia-based high-risk exchange.

QUICK LINKS



Perpetrators of Exit Scam transferring their illicit proceeds.

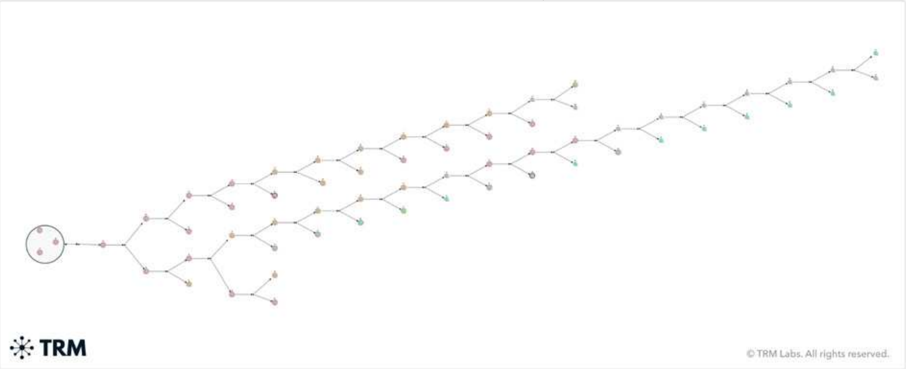
After the majority of the scammed funds are sent to a Mixer, the remaining assets are forwarded to a High Risk Exchange in smaller structured transactions.

© TRM Labs. All rights reserved.

Programmatic Money Laundering

Programmatic money laundering (PML) includes using software to quickly move funds through hundreds or thousands of transactions, in an attempt to obfuscate the illicit origin.

In the example below, a criminal sent illicit funds from a mixer through a series of peel chains to "peel off" small amounts of BTC (represented by the green nodes) that are then sent to an exchange. One of the most high-profile examples of cryptocurrency-based PML involved the North Korean Military in 2021.



© TRM Labs. All rights reserved.

QUICK LINKS

Chain-Hopping

Chain-hopping refers to the practice of moving cryptocurrency from one blockchain to another.. While chain-hopping is not inherently illicit, it can be used by money launderers to obfuscate the transaction trail.

For example, Bitfinex, a cryptocurrency exchange, fell victim in 2016 to a breach that resulted in the theft of nearly BTC 120,000. In 2022, the US Department of Justice (DOJ) used on-chain analytics to charge the two suspects in the case with fraud and money laundering. The money launderers conducted chain-hopping from Bitcoin to other blockchains, including swaps to anonymity-enhanced cryptocurrencies like Monero, before the funds were deposited into traditional financial accounts.

TRM Labs research has also found bridge-hopping to be a favored money laundering methodology used by CSAM actors.

Privacy Coins

Privacy coins such as Monero, Zcash, and Dash provide enhanced privacy and anonymity features compared to standard cryptocurrencies like Bitcoin. Although privacy coins are not illegal, their ability to render transactions difficult to trace make them attractive for criminals seeking to launder illicit proceeds.

Several countries have cracked down on their use. Australia and South Korea have banned exchanges from offering privacy coins, while Japan banned them entirely in 2018. The use of blockchain intelligence tools to monitor crypto services that offer privacy coins helps law enforcement and regulators to identify on-ramps and off-ramps involving these protocols.

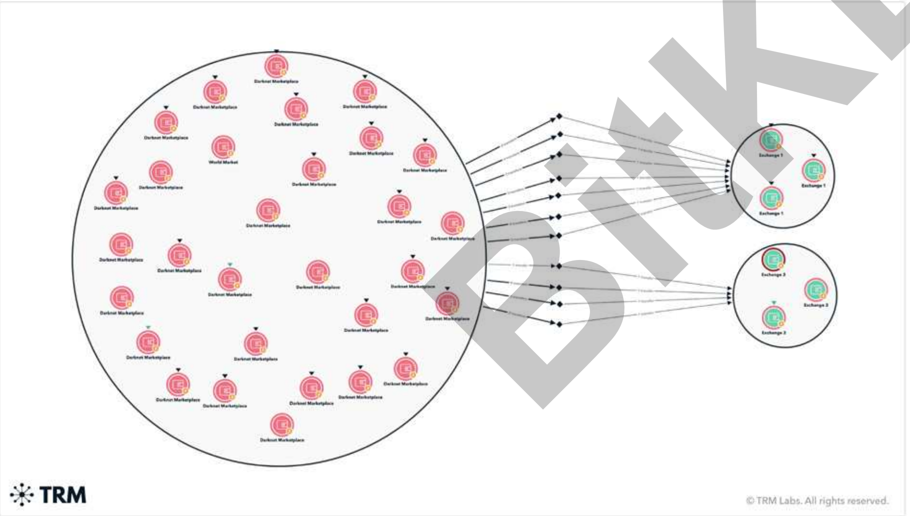
One challenge for such on-chain surveillance is that criminals frequently cash out using brokers who exchange physical banknotes for privacy coins deposited to their receiving address. The cash is then smuggled across borders while the cryptocurrency is traded on exchanges.

High-Risk and Parasite VASPs

Because high-risk VASPs and parasite VASPs usually have weak to non-existent KYC and AML requirements, they are a preferred vehicle of cybercriminals and money launderers for moving funds as part of the layering process. These exchanges are sometimes referred to as swap services, because they allow criminals to pass funds through the service by exchanging one type of cryptocurrency for another, making tracing more difficult. Cybercriminals can also use these services to cash out into the traditional financial system.

Darknet Marketplaces

Darknet markets (DNMs) are also used for layering illicit funds. The below example shows a drug vendor cashing out their profits from the DNM (represented by the red nodes) and sending the funds to addresses controlled by them at two separate exchanges.



The collapse in cooperation between Russia and the West on cybercrime matters since the start of the Ukraine war has created the perception among criminals that Russian-language DNMs have become a safe-haven from US and European law enforcement. As such, a wide range of criminals – including CSAM threat actors – have been observed depositing cryptocurrency to DNMs in order to obscure their original source: once crypto funds are withdrawn from DNM's escrow accounts, they are no longer the same coins as those originally deposited.

QUICK LINKS

Part II – Money Laundering

2. Layering

Mixers

Cash-to-Crypto

High-Risk Exchanges

Programmatic Money Laundering

Chain-Hopping

Privacy Coins

High-Risk and Parasite VASPs

Darknet Marketplaces

Inter-VASP Layering

Payment Processors

Gambling

Decentralized Finance (DeFi)

Mining

Inter-VASP Layering

Inter-VASP layering involves the use of several exchanges or other VASPs to break up and move funds during the money laundering process in order to make it more difficult for investigators to trace. Inter-VASP layering mirrors traditional money laundering techniques, whereby criminals use multiple banking services to obfuscate the source of funds; it is particularly difficult to trace funds through VASPs that settle transactions off-chain.

Although blockchain forensics tools can assist with identifying the transactions that reach the VASP, investigators are required to apply for legal data access to obtain the necessary transaction data to identify the off-ramps.

Payment Processors

Payment processors can be abused by a variety of criminals and threat actors, including extremist and militant groups, to layer their funds. TRM Labs has identified numerous investment fraud schemes that have used mainstream payment processors. Violent extremist groups, including US-based neo-Nazi actors, have used payment processors to generate dynamic addresses, typically for the exchange of goods, services, or subscriptions. Following seizures by the Israeli government, Hamas and other Gaza-based militant groups stopped publicly publishing their cryptocurrency donation addresses and instead turned to payment processors, typically embedding them in their websites' fundraising pages.

Gambling

Although gambling is legal and socially acceptable in many jurisdictions, it has long been a useful method of laundering funds from illicit activity. The gambling process involves customers paying money into a casino or bookmakers' and later cashing out any winnings along with the remaining funds and an official receipt. This gives money launderers the opportunity to claim that their illicitly-obtained funds are merely gambling profits.

Cryptocurrency-based gambling platforms make it difficult to trace funds through the service. However, they are increasingly subject to compliance regulations. This means that casinos must perform KYC and source of wealth checks on customers seeking to deposit large amounts. Later, should a suspected criminal claim gambling winnings as the source of their funds, the online casino in question can be subpoenaed by local law enforcement to release records relating to that user.

QUICK LINKS

Part II – Money Laundering

2. Layering

Mixers

Cash-to-Crypto

High-Risk Exchanges

Programmatic Money Laundering

Chain-Hopping

Privacy Coins

High-Risk and Parasite VASPs

Darknet Marketplaces

Inter-VASP Layering

Payment Processors

Gambling

Decentralized Finance (DeFi)

Mining

Decentralized Finance (DeFi)

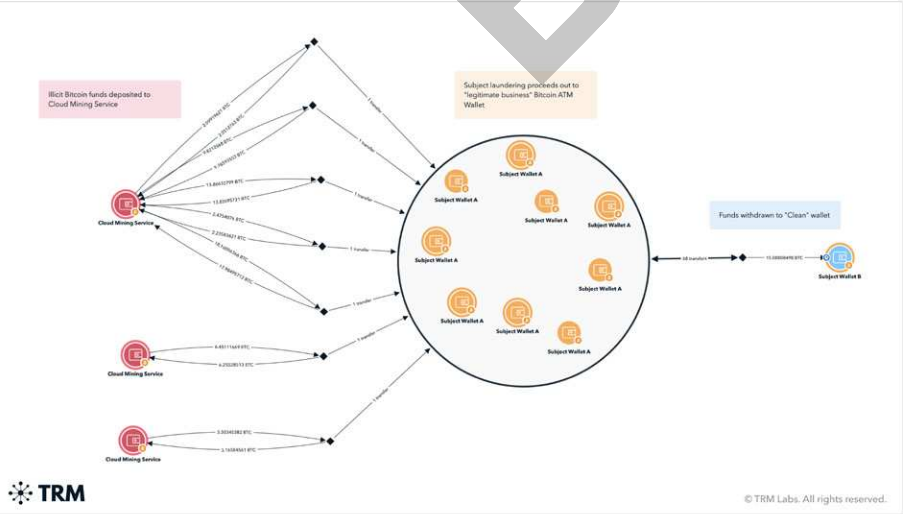
Decentralized finance (DeFi) is at risk of abuse by money launderers. While DeFi has the potential to increase financial inclusivity and provide more accessible and transparent services, it can also be exploited by those seeking to engage in illicit activities.

It is important to note that many DeFi platforms are actively implementing measures to enhance security, compliance and transparency. Regulatory authorities are also working on frameworks to address money laundering risks in the context of DeFi.

Mining

Cryptocurrency mining has been abused for laundering funds by ransomware groups, such as APT43, and other illicit actors. The coins minted on mining equipment acquired with illicit funds have no apparent ties to criminal activity, allowing criminals to cash out without leaving a traceable path on the blockchain.

For example, TRM Labs has identified a DNM vendor using illicit funds made from the sale of drugs to purchase cloud mining accounts. The outputs from the mining transactions were then laundered through a Bitcoin ATM business controlled by the vendor, which provided a front for the illicit activity. From there the funds were withdrawn to a personally-held wallet.


Illicit Bitcoin funds deposited to Cloud Mining Service
Subject laundering proceeds out to "legitimate business" Bitcoin ATM Wallet
Funds withdrawn to "Clean" wallet
Cloud Mining Service
Cloud Mining Service
Cloud Mining Service
Subject Wallet A
Subject Wallet B
1 transfer
TRM
© TRM Labs. All rights reserved.

QUICK LINKS

Part II – Money Laundering

2. Layering

Mixers

Cash-to-Crypto

High-Risk Exchanges

Programmatic Money Laundering

Chain-Hopping

Privacy Coins

High-Risk and Parasite VASPs

Darknet Marketplaces

Inter-VASP Layering

Payment Processors

Gambling

Decentralized Finance (DeFi)

Mining

3. Integration

QUICK LINKS

Part II – Money Laundering

3. Integration

Crypto-Fiat Value Transfer

Send as Crypto

Integration is the final stage of money laundering, during which the laundered proceeds are re-introduced into the legitimate economy. This is done by funneling the funds to legitimate channels so that the source of funds can plausibly be explained.

The key purpose of integration is to convert the tainted crypto funds into fiat currency or stablecoins which are then off-ramped through VASPs such as payment processors, exchanges, OTC desks, cash-to-crypto services and peer-to-peer (P2P) services. Criminals may also use their crypto proceeds directly to purchase goods and services such as NFT artwork, computers, airline tickets and clothing. Dozens of mainstream retailers already accept payment in cryptocurrency.

Transaction analysis of declared wallets – incorporating both direct and indirect risk exposure – belonging to accused criminals can help investigators to identify the true source of funds .

Crypto-Fiat Value Transfer

There are numerous options for transforming criminally obtained crypto into fiat currency. Bitcoin, Ethereum, and a range of other assets can be used online to buy gift vouchers, prepaid debit cards, or iTunes vouchers – without undergoing KYC or source of wealth checks. Unscrupulous OTC ("over the counter") traders and P2P exchanges also offer cash-changing services with minimal scrutiny while maintaining client anonymity.

This transaction mechanism is often seen as part of the integration process for launders. Often they will engage services or peer traders that will not ask any questions about the source of funds so that the transfer is not subject to scrutiny.

Cash-to-Crypto

Cash-to-crypto services can be used to cash out the illicit proceeds of crime during the integration stage. TRM Labs has tracked the use of crypto ATMs by suspected perpetrators of severe illicit activity, including terrorist financing and CSAM. It is likely that criminals use such ATM kiosks due to the relatively loose KYC policies implemented by many such services.

High-Risk VASPs

Due to their lack of KYC requirements, unregulated status and domicile in opaque jurisdictions, high-risk VASPs are frequently used to cash out illicit cryptocurrency earnings. The obtained fiat currency can then be spent on a variety of goods and services.

OTC Desks

OTC services can be used for all three stages of laundering, where criminals need to place cash into the financial, or wish to transfer funds across borders quickly without oversight as a method of layering, and finally as a way of cashing out their funds during the integration process. In 2021, SUEX, a Russian-language OTC broker, was sanctioned by OFAC for facilitating financial transactions for ransomware actors.

P2P Exchanges

Although most P2P exchanges are technically governed by AML rules – for example, business transactions of over USD 600 involving US persons must be reported under US informational reporting rules – many flout such requirements.

Spend as Crypto

It is possible for criminals to integrate their crypto-based wealth without resorting to fiat currency off-ramps. Over the past five years, an increasing array of goods and services has become available for purchase directly using cryptocurrency. This ranges from digital goods such as NFTs and in-game purchases to luxury goods and even real estate. These purchases may also be seen as stores of value, depending on how the criminal intends to use the asset in the future.

Real Estate

In 2022, Portugal became among the first countries to allow the sale of a house using crypto. Most high-value real-world transactions involving crypto require KYC and source of wealth checks, which poses challenges for criminals. However, there remain myriad ways for illicit actors to evade such guardrails - often through the use of shell companies and cybercrime services.

QUICK LINKS

Part II – Money Laundering

3. Integration

Crypto-Fiat Value Transfer

Send as Crypto

Luxury Goods

Luxury goods such as supercars, jewelry, and designer bags are frequently bought with the proceeds of illicit crypto activities. Some luxury goods can be purchased directly with cryptocurrency: for example, the German fashion designer Philipp Plein allows the use of cryptocurrency in his online boutiques.

Luxury goods are often found during police raids on crypto criminals. In March 2022, a series of raids by Brazilian police on a gang accused of running a EUR 780 million illegal cryptocurrency scheme. Despite promising investors healthy returns, the criminals used investor funds to buy real estate, jewelry, cars, boats, and luxury clothing.

Crypto Gift Cards

As prepaid gift cards can be purchased using cryptocurrency, they can also be abused by criminals to cash out illicit funds. After buying gift cards from an online service with proceeds from crime, an illicit actor can then use the cards to acquire a wide range of consumer goods from mainstream e-commerce platforms and physical stores. For example, one of the accused parties behind the Bitfinex hack allegedly spent a portion of the stolen funds on a USD 500 Walmart gift card.

Gift cards can also be acquired by scammers posing as crypto traders who convince would-be investors to send them gift cards as sources of value to make crypto investments on their behalf. The scammers then run off with the gift cards.

Methodology

The taxonomy development process followed a systematic and iterative approach, incorporating various data sources and expert input to include the most comprehensive range of predicate offenses.

Initially, a preliminary list of illicit activities associated with cryptocurrency was compiled through a literature review and expert interviews. This included analyzing predicate offenses defined by the FATF Recommendations, examining criminal investigations involving cryptocurrency, and consulting with private and public sector partners globally. The activities were categorized into themes and subcategories, considering the nature of the activities, the actors involved, and prosecution across jurisdictions. For instance, ransomware was classified under extortion and fraud due to its frequent prosecution in the United States under the Computer Fraud and Abuse Act (CFAA) - 18 U.S.C. § 1030.

To gather data, historical transaction data from 20 public blockchains was indexed. Open-source intelligence, active intelligence collection, and pattern recognition algorithms were used to collect information on blockchain addresses and transactions associated with illicit activity.The absolute volume of a specific category ($X) was measured by aggregating the USD value of incoming transfers to relevant addresses, considering the USD price of the asset on the transfer date.

Several limitations should be acknowledged in this report. First, reported volume for specific categories may be underestimated if TRM lacks attribution for addresses or transactions within those categories. Certain categories like darknet marketplaces and investment schemes are more likely to be comprehensively measured due to their inherent visibility and the presence of platforms like Chainabuse that facilitate victim reporting. The transparency of the blockchain allows for an estimation of the upper bound of illicit activity by subtracting known volume associated with legitimate activity such as trading from total crypto volume. Second, this report does not measure fiat proceeds of crime converted into crypto. Virtual asset service providers (VASPs) and financial intelligence units (FIUs) play a critical role in detecting the conversion of fiat proceeds of crime into cryptocurrency and digital assets for money laundering.

As TRM continues to collect more data, it is possible that the reported numbers may increase over time, improving the accuracy and completeness of the report. These limitations are essential to consider in interpreting the findings and recognizing the potential for further refinement and expansion of the taxonomy in the future.

Conclusion and Recommendations

Despite only existing in mainstream use for around a decade, cryptocurrencies have embroidered themselves into every typology of crime, from the purely digital theft enabled by hacks to drugs trafficking, extortion, terrorist financing and espionage. Crypto did not introduce these criminal forms; nor has it (yet) come to dominate them. Indeed, fiat currencies and even older forms of finance such as *hawala* remain the default means by which illicit activity is financed and its proceeds are laundered.

The "crypto winter" of 2022 did little to erode the use of crypto in illicit activity and in money laundering. The year saw as much as USD 2 trillion worth of cryptocurrency assets wiped out from investors' balance sheets, according to World Economic Forum estimates. Yet the fall in crypto's value does not appear to have dissuaded criminals from using and exploiting crypto.

This has been particularly true regarding DeFi, with hacks on DeFi targets and cross-chain bridges resulting in USD 3.7 billion stolen – an average of over USD 20 million per incident. Illicit investment schemes, too, have seen significant activity, with at least USD 7 billion in volume linked to such addresses.

The continued proliferation of cryptocurrencies and blockchain technology suggests that they will retain a significant place in the criminal arsenal. The good news for investigators, law enforcement and regulators is that cryptocurrencies can provide granular visibility into the structure, operations and, most of all, interconnectivity between different criminal actors and enterprises.

As this report shows, the various kinds of crypto crime and their perpetrators do not operate in silos; rather, they are highly intertwined.

Seemingly unrelated pig butchering incidents were found to be linked to major international crime groups; cryptocurrency ATM scams have been alleged to fuel people trafficking syndicates; Russian-language DNMs specializing in drugs are also used by CSAM actors to launder funds; the sanctioned mixing service Chipmixer was facilitating the work of Royal, a notorious ransomware syndicate that targets US national security infrastructure.

Over the last two years, the US Treasury Department's Office of Foreign Assets Control (OFAC) has sanctioned non-compliant VASPs, darknet markets and other parts of the illicit crypto ecosystem for facilitating ransomware, sanctions evasion, and other activity.

In January 2023, the US Department of Justice and the US Treasury Department announced a coordinated action against non-compliant Hong Kong-registered cryptocurrency exchange Bitzlato. Its owner was arrested for "conducting a money transmitting business that transported and transmitted illicit funds and that failed to meet US regulatory safeguards, including anti-money laundering requirements."

Disrupting these criminal enterprises depends on understanding not just the ways in which they connect but also on the ability to overcome their attempts at obscuring the origin and flow of their cryptocurrencies across blockchains. As the number of blockchains continues to proliferate, tracking these financial flows becomes ever more technically demanding.

As the first blockchain intelligence platform designed for the multi-chain era, TRM Labs has pioneered tracing support for new blockchains, including all assets on Ethereum (2019), TRON (2019) and Solana (2021). Today, TRM Labs can trace over 28 blockchains and over a million assets including all derivative assets, wrapped assets, stablecoin and NFTs, enabling historical replay of 99% of crypto volume.

TRM Labs was the first to launch state-of-the-art capabilities including automated cross-chain tracing, automated demixing, NFT tracing, nested entity analytics, and mobile-first forensics. TRM Labs offers one-click tracing through 50 blockchain pairs and over 10 million cross-chain swaps.

Blockchain intelligence represents a transformative leap forward in the ongoing fight against illicit finance. Previously, law enforcement agencies, regulators and the broader private sector lacked a real-time understanding of illicit economies, their size, how their assets are transferred and how they are overlapping with other illicit networks.

Approaching crypto crime in a systematic way allows for a holistic view that can inform a broad strategy for dealing with crypto crime risks. Any such strategy should consider the following questions:

- How detailed is our understanding of crypto crime and money laundering, and do we need to adjust our frameworks to mirror a more granular risk taxonomy?
- Are we overly focused on activity involving bitcoin to the detriment of other emerging chains showing increased involvement in illicit activity?
- Have we conducted a coverage assessment against these risks to better understand our exposure to the various illicit risk categories?
- Are our resources (both technological and human) well positioned to identify not just a singular risk and typology but multiple illicit activities interacting within one connected scheme?

Such an approach can help equip law enforcement and compliance professionals with a more comprehensive, granular and targeted view of where to allocate their surveillance, investigative and technological resources.