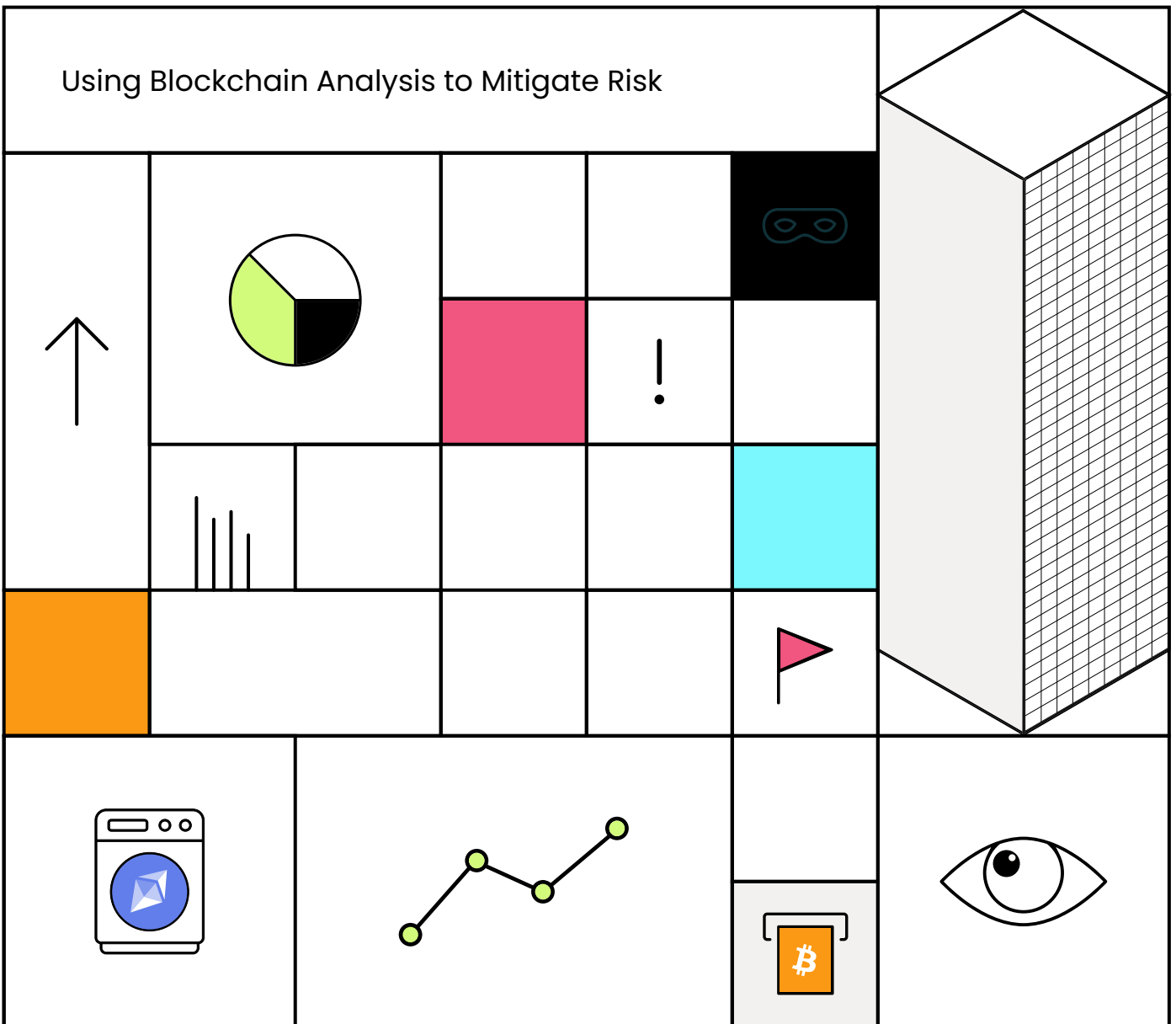


# Preventing Financial Crime in Cryptoassets



<b>Introduction</b>	<b>7</b>
<b>Part I: Money Laundering</b>	<b>10</b>
<b>1. Cryptoasset Exchanges</b>	<b>11</b>
1.1. Use of Non-compliant or Unlicensed Exchanges	11
1.2. Use of Exchanges in High-risk Jurisdictions	17
1.3. Use of Money Mules or Fraudulent Documents at Legitimate Exchanges	23
<b>2. Mixers and Privacy Wallets</b>	<b>29</b>
<b>3. Decentralized Finance (DeFi) and Cross-chain Crime</b>	<b>37</b>
3.1. Money Laundering Through DEXs	38
3.2. Money Laundering Through DeFi Mixers	41
3.3. Money Laundering Through Cross-chain Bridges	45
<b>4. Tokens and Stablecoins</b>	<b>49</b>
4.1. Tokens & Stablecoins Used to Clean Illicit-origin Funds	50
4.2. Laundering of Proceeds From Scams	51
4.3. Laundering of Hacked Tokens and Stablecoins	54
<b>5. Privacy Coins &amp; Chain Hopping</b>	<b>57</b>
5.1. Use of Privacy Coins to Layer Illicit Proceeds	57
5.2. Laundering Illicit-origin Privacy Coins	59
<b>6. Wallet-specific Behaviors</b>	<b>63</b>
6.1. Chain Peeling	63
6.2. Multi-customer Cross-wallet Activity	66
<b>7. Cryptoasset ATMs</b>	<b>68</b>
7.1. Facilitation of Illicit Transfers	68
7.2. Money Mule Activity	73
7.3. Victims of Scams Send Funds via Cryptoasset ATMs	75

<b>8. Cards</b>	<b>79</b>
8.1. Use of Cryptoasset Prepaid Cards to Layer Criminal Proceeds	79
8.2. Dirty Cryptoassets Used to Purchase Fiat Cards For Laundering	82
8.3. Fiat Cards Used to Purchase Cryptoassets For Illicit Purposes	85
<b>9. Banks and Indirect Exposure to Cryptoasset Risks</b>	<b>87</b>
9.1. Indirect Exposure Through Processing VASP Transactions	87
9.2. Indirect Exposure Through Correspondent Relationships	89
<b>10. Non-fungible Tokens (NFTs)</b>	<b>91</b>
10.1. NFTs and Money Laundering	92
10.2. NFTs and Fraud	93
10.3. NFTs and Theft	96
<b>11. Metaverse-related Laundering</b>	<b>100</b>
11.1. Use of Metaverse Services to Launder Illicit-origin Cryptoassets	100
11.2. Laundering the Proceeds of Metaverse Crimes	101
<b>12. Multi-technique and Multi-service Typologies</b>	<b>103</b>
12.1. The Bitfinex Hack	103
12.2. Operation Argenti	106
12.3. Russia Hacking	106
12.4. Dark Web Laundering	109
12.5. Ransomware: the Colonial Pipeline Attack	110
12.6. Other Examples	111
<b>Part II: Terrorist Financing</b>	<b>112</b>
<b>13. TF Involving Crowdfunding Through Charities and Other Organizations</b>	<b>114</b>
<b>14. TF Involving Individuals or Small Cells</b>	<b>119</b>

<b>Part III: Key Trends: Criminal and Threat Actors</b>	<b>121</b>
15. Hackers and Cybercriminals	123
16. Dark Web Vendors	124
17. Fraudsters	125
18. Professional Money Launderers	129
19. Street Drug Dealers	130
20. Human Traffickers and Sex Trade Perpetrators	131
21. Tax Evaders	132
23. State Actors and Sanctions Evaders	134
24. Terrorists and Political Extremists	143
Index	144

# Executive Summary to the 2023 Edition

It's only been a year since we published the 2022 version of Elliptic's Typologies Report, but in that short time, cryptoasset businesses and financial institutions have faced a rapidly changing landscape that places growing demands on compliance teams to adapt.

The collapse of the FTX crypto exchange in November 2022 has catalyzed a flurry of regulatory activity that has seen regulators tighten requirements for firms operating globally.

Emerging regulatory frameworks in jurisdictions such as Hong Kong, Dubai, the United Kingdom and the European Union help to provide clarity about the rules of the road. However, they also come with significant new requirements that create operational challenges for compliance teams. Efforts by regulators in the United States to enforce regulations have intensified significantly, and the increased use of policy tools such as financial sanctions directed at crypto-related activity places further demands on businesses' compliance operations.

As this regulatory change has unfolded at a relentless pace, the past year has also seen new developments in the financial crime risk landscape impacting cryptoassets. For example:

- Threat actors such as North Korean cybercriminals and ransomware gangs now look routinely to decentralized finance (DeFi) services to engage in "chain-hopping" typologies of money laundering.
- Financial sanctions have been imposed on mixing services – such as the Tornado Cash and Blender mixers – leading to severe consequences if businesses facilitate transactions with them.
- Fraud schemes such as "pig butchering" investment scams have proliferated as fraudsters attempt to take advantage of a volatile market.
- Hacks, scams and other crimes have increasingly spilled over into new, emerging environments, such as the world of non-fungible tokens (NFTs) and the metaverse.
- Criminals are increasingly able to launder funds between the worlds of traditional finance (TradFi) and the crypto ecosystem, which in turn creates additional challenges of detection and monitoring.

This combination of an intensifying regulatory environment and evolving threat landscape means that compliance teams face greater challenges than ever before to ensure they can detect and mitigate financial crime risks efficiently and effectively.

Our aim with this report is to equip your compliance team with the practical insights needed to ensure your business is able to scale its ability to detect new financial crime risks with success. Therefore, we've designed the 2023 version of this report to reflect the changing landscape. For example, we've:

- provided additional insights into the use of DeFi, stablecoins and other related innovations that are involved in cross-chain laundering typologies;
- described in further detail the evolving money laundering techniques of ransomware gangs and their support networks;
- offered further insights into the proliferation of crimes such as pig butchering, and their use in money laundering typologies involving services such as Bitcoin ATMs;
- included a chapter on metaverse-related money laundering activity; and
- provided updated case studies and illustrations throughout the report to give insights into the latest regulatory and law enforcement actions impacting the crypto space.

In addition to describing key risks, throughout the report we provide concrete examples of compliance controls your team can implement to address specific financial crime typologies you encounter. This includes examples of how Elliptic's Holistic Screening capabilities can be used to detect "chain-hopping" typologies of money laundering at scale by enabling the detection of illicit activity even where illicit funds are swapped through various DeFi services.

Additionally, this year we have produced a separate Cryptoasset Risk Assessment Matrix supplement. This will assist your compliance team in practically ensuring that you have the monitoring controls needed in place to manage the risks outlined in this report.

It is more important than ever for compliance professionals to understand the evolving nature of financial crime typologies in the crypto space, so that they can scale their operations to ensure the effective detection and disruption of risks. At Elliptic, we have always been committed to equipping compliance teams with the insights and capabilities needed to navigate a rapidly evolving landscape.

We hope this guide provides you with the insights needed to ensure successful financial crime compliance and risk management.

**David Carlisle**

**Vice President of Policy and Regulatory Affairs**

# Introduction

The public discussion around cryptoassets frequently mentions their use in money laundering, terrorist financing and other financial crime. It is often anecdotal and of little practical use to compliance officers, law enforcement agents, regulators and other stakeholders responsible for disrupting illicit activity.

This detailed guide to money laundering and terrorist financing typologies details the true impact of crime in cryptoassets. Elliptic's intention is for this study to provide a meaningful contribution to the public and private sectors as they work to root out illicit actors.

This report is designed to equip financial crime analysts and investigators with the knowledge and insights needed to proactively and practically:

- identify specific money laundering and terrorist financing risks;
- investigate cases of suspected crime involving cryptoassets;
- develop anti-money laundering and counter-terrorist financing (AML/CTF) responses;
- evolve their responses to manage risk to businesses, consumers and society;

In compiling this report, Elliptic has drawn from multiple sources:

- Data insights drawn from Elliptic's continuous research and analysis of blockchains.
- Consultations with compliance officers at cryptoasset businesses about the typologies they face and risks they encounter on a day-to-day basis.
- Publicly available reports, indictments and literature produced by law enforcement agencies (LEAs), national financial intelligence units (FIUs), organizations such as the Financial Action Task Force (FATF) and other publicly available court documents.
- Other public records such as press reporting.

Bad actors continue to find new ways to support their criminal activities. Between editions of this report, you will find **the latest insights and trends related to money laundering and terrorist financing** using cryptoassets on our website.

As we work in partnership to make crypto safe to use, please share any emerging typologies identified through your daily work with your Elliptic contact. Our Research & Intelligence Team will use these inputs – together with Elliptic’s bespoke monitoring and analysis techniques – to uncover new typologies and bad actors, ensuring you can rely on the most accurate and up-to-date blockchain analytics capabilities.

## How to Use This Report

This report is designed to be a desk guide to complement Elliptic’s blockchain analytics solutions for analysts and investigators. It can be studied top to bottom so you can become familiar with money laundering red flags in crypto, or you can use it as a reference as and when suspicious activity emerges.

Elliptic’s crypto AML/CFT risk management and investigative solutions enable compliance teams, LEAs, regulators and FIUs to efficiently and effectively:

- Automate AML/CTF and sanctions compliance checks.
- Identify address clusters associated with illicit actors and take action.
- Illustrate the flow of Bitcoin from address to address to support investigations.
- Monitor movement related to criminal activity involving dark web markets, ransomware attacks, cryptoasset exchange hacks and other crimes.

This guide deep dives into financial crime typologies using cryptoassets to arm you with a comprehensive set of red-flag indicators that describe:

- Illicit activity involving cryptoassets.
- Examples of how these indicators fit into broader criminal behaviors.
- Context on how criminals engaged in these activities are cleaning their illicit funds.
- How money laundering methods are evolving, assuming some basic knowledge of these crime types.



This document catalogs identified typologies into three parts for easy reference.

## Part I: Money Laundering

An outlook of key money laundering typologies Elliptic has identified and their impact on specific cryptoasset products and services.

## Part II: Terrorist Financing

An overview of identified terrorist financing cases involving cryptoassets.

## Part III: Key Trends: Criminal and Threat Actors

A summary view of how specific sets of illicit actors make use of the specific laundering techniques identified throughout the guide.

Look out for these indicators which evidence the typologies described and inform actions you need to take.

### Red Flags

Indicators of risk that might not clearly pinpoint illicit activity as a standalone. But, when they appear in conjunction with other indicators, it may suggest suspicious activity is at play.

### Diagrams and Flowcharts

Illustrations, diagrams, graphs and charts are included throughout to help you visualize a typology and, where possible, give a relative view.

### Case Studies

Wherever possible, real-life examples of how criminals are exploiting the typologies Elliptic has examined are included to evidence how the typology is played out.

### Warning Signals

Warnings describe significant issues and trends in criminal behavior that are worth highlighting in their own right and can indicate suspicious activity or require extra attention.

### Key Controls & Best Practices

These summarize solutions and approaches that can enable the detection and prevention of the typologies described in this report.

→ 01.

# Money Laundering

# 1. Cryptoasset Exchanges

Cryptoasset exchanges provide essential liquidity to crypto markets, acting as vital gateways between the fiat and cryptoasset ecosystems. Thus, exchanges inevitably feature heavily in cryptoasset-related money laundering activity.

A report by the Financial Action Task Force (FATF) in September 2020 on cryptoasset red flags highlights the specific risks coming from unregulated exchanges, or those that don't have AML/CTF controls. The FATF noted that "criminals have exploited the gaps in AML/CTF regimes [...] by moving their illicit funds to VASPs domiciled or operated in jurisdictions with non-existent or minimal AML/CTF regulations [...]."<sup>1</sup>

Unlicensed and non-compliant exchanges present significant money laundering risks. Legitimate and well-intentioned exchanges may also be targeted in money laundering schemes. Those exchanges that hold KYC information on users can often provide law enforcement with vital insights that help to connect the dots between the transaction trail on the blockchain and information about the identities of illicit actors.

This section highlights three major money laundering typologies related to criminal abuse of cryptoasset exchanges.

## 1.1. Use of Non-compliant or Unlicensed Exchanges

### The Problem

Criminals deliberately seek out exchanges they know they can exploit with little or no obstruction when moving between fiat and cryptoasset, or from cryptoasset-to-cryptoasset.

This may include:

- exchanges that deliberately flaunt regulation and registration requirements;
- those that allow customers to set up accounts with little or no identifying information; and
- exchange services that do not require customers who open accounts to comply with regulation in any jurisdiction.

Considering that unlicensed and non-compliant exchanges often do not require any KYC or customer due diligence (CDD) information from users, criminals can operate under a veil of additional anonymity beyond that already afforded by the pseudonymous or anonymous nature of certain cryptoassets.

In addition, some – though certainly not all – non-compliant and unlicensed exchanges have themselves been criminal enterprises and deliberately facilitated illicit activity.

Non-compliant and unlicensed exchanges present significant systemic risks within the cryptoasset ecosystem, because they enable a wide range of illicit actors to engage in large scale money laundering.

Legitimate crypto exchanges should be on the alert for customers whose cryptoasset transaction histories include frequent interactions with unregulated or non-compliant exchanges.

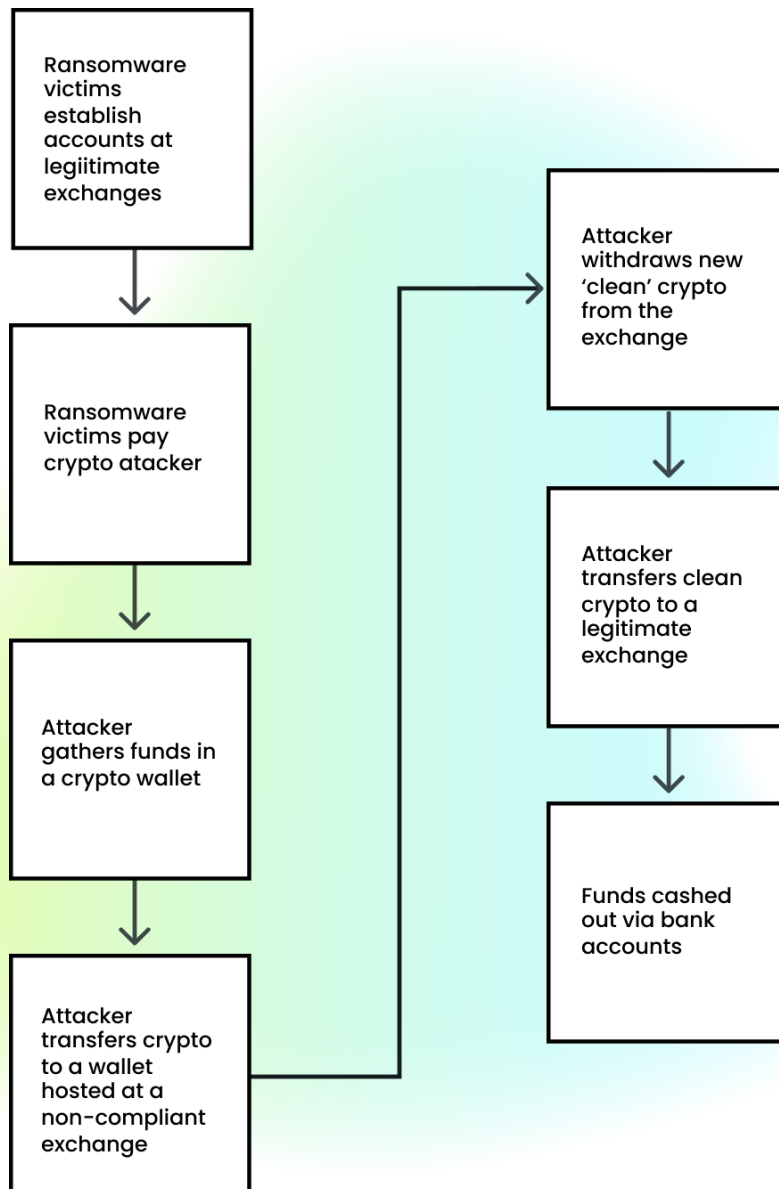
Similarly, legitimate exchanges and digital asset businesses – such as cryptoasset brokerages – that provide services to other exchanges must be alert to the risks of dealing with unlicensed and non-compliant exchanges.

## The Typology<sup>2</sup>

A common method of abusing unlicensed and/or non-compliant exchanges works as follows:

1. A criminal – for example a ransomware perpetrator – is in possession of illicitly obtained cryptoassets and requires a source to make the dirty cryptoassets appear clean.
2. The criminal establishes an account with an unlicensed or non-compliant exchange to swap their cryptoassets, sometimes using a mixing or tumbling service. They can set up accounts with complete anonymity, or by using aliases (such as “Mickey Mouse”), or false identifying information (such as listing residential addresses at “123 Main Street”).<sup>3</sup>
3. The criminal swaps their dirty cryptoassets for fiat currencies, or for other cryptoassets.
4. The criminal can then “cash out” from the exchange, having their funds routed directly to a bank account. Other options could be via WebMoney, Perfect Money or other value transfer services, including through the banking system. Often, any messages accompanying related funds transfers may include information or references that are deliberately meant to conceal that they are related to cryptoassets.
5. Alternatively, the criminal may first move new “clean” cryptoassets to a legitimate exchange, from which it can then cash out. Often, this includes swapping transparent cryptoassets – like Bitcoin, Ethereum and Litecoin – for privacy coins, such as Monero.

The diagram below offers a simple illustration of how a criminal may move dirty cryptoassets through non-compliant exchanges.



## Red Flags

Common red-flag indicators and risk factors associated with non-compliant and unlicensed exchanges include:

- the exchange requires no KYC/CDD information;
- customers can establish an account, or access services with only basic information, such as an email address and password;
- the exchange is either unable to produce AML policies and procedures when requested to do so, or its documented AML policies are of a poor standard;
- the exchange does not place any limits or restrictions on customers' volumes and values of permissible trading activity;
- the exchange permits customers to fund their account even if they have received cryptoassets directly from mixers/tumblers;
- there is no meaningful information about its compliance practices, management structure or business registration on the exchange's website;
- customers regularly do business with other non-compliant and/or opaque exchanges;
- the exchange is associated with high percentages of cryptoasset transfers coming from addresses associated with criminal sources, such as ransomware attacks and dark web markets (for instance, 50-60% or more of the exchange's business may come from or go to criminal sources);
- the exchange's website warns customers not to make mention of Bitcoin or cryptoassets when talking to external parties such as banks;
- the exchange may instruct customers to put vague or misleading information into wire transfer message fields when transferring fiat funds to or from a bank;
- the exchange may have only recently registered and possibly has no prior established history of cryptoasset trading;
- association with open discussions among criminals on the dark web;
- the exchange is associated with open discussions among criminals on its user chat rooms, internet message boards – such as Reddit – or other surface web sources; and
- the exchange advertises that it allows customers to exchange cash for cryptoassets.



## SUEX, Chatex, Garantex and the Laundering of Ransomware Proceeds

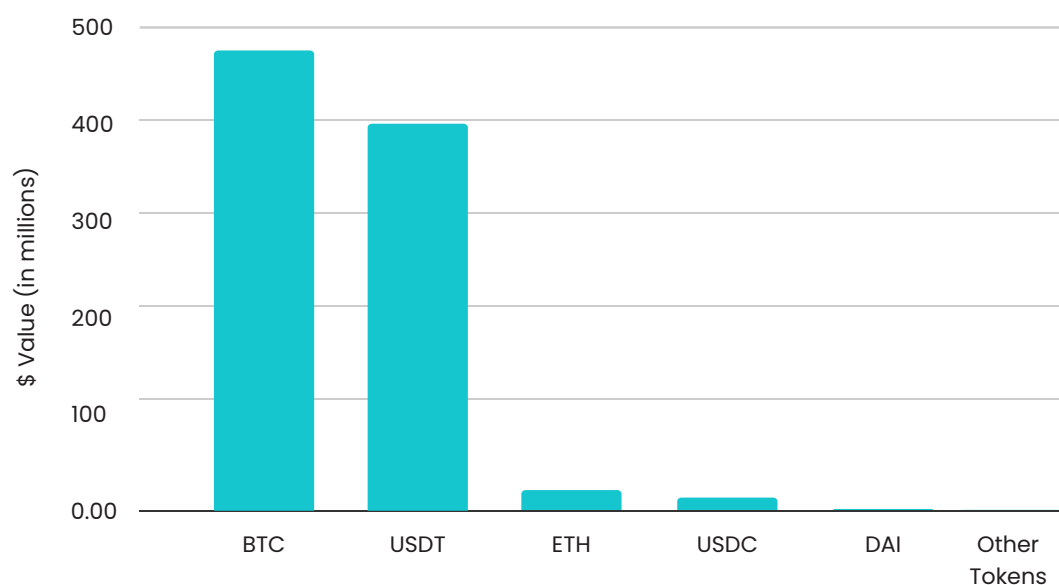
In September 2021, the US Treasury's Office of Foreign Assets Control (OFAC) undertook a sanctions action that highlighted the pivotal role that unregulated cryptoasset exchanges that fail to apply AML/CFT controls play in facilitating illicit finance.

That month, OFAC placed sanctions on SUEX OTC, S.R.O., a cryptoasset trading business registered in the Czech Republic and with operations in Russia. SUEX had a limited online presence, advertising boutique services for a largely Russian clientele, including enabling users to buy cryptoassets with credit cards online, or in-person in cash. To the average person, SUEX would have appeared to be an inconsequential and small cryptoasset business of little relevance.

However, SUEX was in fact a linchpin in the ransomware ecosystem, enabling ransomware perpetrators to launder their ill-gotten gains. According to OFAC, SUEX facilitated money laundering activity related to at least eight ransomware strains, and as much as 40% of its overall business was related to illicit activity.<sup>4</sup>

Elliptic's research indicates that from 2018 onward, SUEX engaged in cryptoasset transactions totalling more than \$934 million, as indicated in the chart below. This suggests that it processed more than \$370 million in illicit transactions in the course of just three years – a substantial sum for a seemingly small exchange service.<sup>5</sup>

### Value of Cryptoassets Received By SUEX Addresses Listed By OFAC



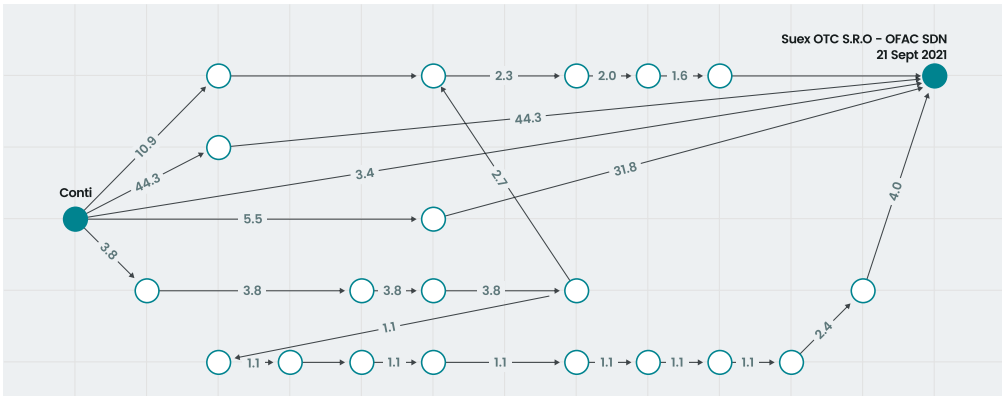
As part of its sanctions action targeting SUEX, OFAC included 25 Bitcoin, Ethereum and Tether addresses that it controlled to enable the private sector to block transactions with SUEX. Because SUEX operated an over-the-counter trading service by opening accounts at larger exchange businesses, the OFAC sanctions come with real impact: other exchanges need to cut off business with SUEX or risk violating OFAC's restrictions.

In November 2021, the agency followed the SUEX action by placing sanctions on another exchange – Chatex – which was also a key facilitator of ransomware payments. Registered in St. Vincent and the Grenadines, Chatex shared common owners and controllers with SUEX and serviced a largely Russian clientele.

According to OFAC, up to 50% of Chatex's transaction history involved illicit activity, and Elliptic's own analysis indicates that in addition to facilitating ransomware transactions, Chatex was also a major facilitator of transactions involving the Russia-based Hydra dark web market. Press reporting from December 2021 indicated that Chatex and its users were facing an inability to move their funds off of the exchange as a result of the OFAC sanctions.<sup>6</sup>

In April 2022, OFAC sanctioned yet another Russia-linked crypto exchange when it targeted Garantex, an Estonia-registered exchange also accused of facilitating activity on behalf of Russian ransomware gangs.<sup>7</sup>

The OFAC sanctions targeting SUEX, Chatex and Garantex send a powerful message: the US government is prepared to disrupt the financial networks that sustain crimes such as ransomware, and it will target those cryptoasset exchanges at the heart of these illicit networks.



*This image from Elliptic Investigator above illustrates the flow of funds from a Bitcoin wallet belonging to the Conti ransomware gang (represented by the green circle on the left) to the SUEX crypto exchange (represented by the green circle on the right). The funds pass through intermediary wallets prior to being deposited at SUEX.*



## 1.2. Use of Exchanges in High-risk Jurisdictions

### The Problem

Criminals will often look to exchanges that are in high-risk jurisdictions during the money laundering process. For cryptoasset-laundering purposes this can include:

- countries and regions that are generally high risk for money laundering and terrorist financing purposes. These could be in Africa, Eastern Europe or the Middle East;
- countries subject to international financial sanctions, embargoes and other restrictions;
- countries on the FATF's list of High Risk and Non-Cooperative Jurisdictions; and
- countries with no AML/CTF regulation around cryptoassets, or with ineffective regulatory frameworks.

This latter category can include countries and regions that in other contexts might not be regarded as high risk, but should be considered higher risk for crypto-laundering purposes.

### The Typology

This typology will generally mirror that described in section 1.1, with additional red flags described below.

#### Red Flags

Common red-flag indicators associated with cryptoasset exchanges in higher-risk jurisdictions are listed below:

- limited or no information available from any source about the location of the exchange;
- ownership structure may be opaque and involves the presence of shell companies in multiple jurisdictions – such as the Seychelles, Belize and the Marshall Islands – associated with easy and non-transparent company formation;
- information on registration or legal status is unclear or contradictory with no available explanation (headquartered in Bulgaria but subject to the laws of Cyprus, for instance);
- the exchange is headquartered in a jurisdiction with no AML regulation around cryptoassets, and its website suggests it does not voluntarily apply AML/KYC in the absence of regulation;
- No KYC/AML policies in place at the exchange and it is also located in a country associated with high levels of organized criminal activity (such as Russia or Colombia);

- overseas registration – for example, in the Caribbean – even though nearly all its customers are located elsewhere (for instance, 75% or more are located in the EU);
- the exchange provides fiat currency trading pairs that are illogical or do not make business sense (for example, an exchange in Finland offers high value trading in Colombian pesos,<sup>8</sup> or an exchange in Cyprus offers trading in Russian rubles);
- registration in a jurisdiction associated with international sanctions (such as Venezuela or Iran);
- the exchange engages in high-volume trading involving fiat currencies associated with sanctioned jurisdictions (such as the Iranian rial);
- the exchange claims to offer trading in a state-issued cryptoasset (such as the Venezuelan petro);
- the exchange has been explicitly licensed by a sanctioned jurisdiction to offer services in a state-owned cryptoasset (for example, the exchange is a Venezuelan exchange authorized by the Venezuelan government to facilitate trading in the Venezuelan Petro);<sup>9</sup>
- the exchange may be registered in a lower-risk jurisdiction but has directors and beneficial owners who are from, and reside in, higher-risk jurisdictions (for instance, the exchange is a UK-registered limited company but whose owners reside in the Ukraine);
- in some cases, the beneficial owners of the exchange may be subject to adverse media or may be Politically Exposed Persons;
- the exchange has a phone number in a higher-risk country – such as Russia – and is owned by registered companies located in other jurisdictions with no clear rationale (for instance, the British Virgin Islands);
- reliance on payment processors in higher-risk jurisdictions to process customers' fiat payments for no apparent reason (a US-based exchange uses an Azerbaijani payment processor, for instance);<sup>10</sup>
- representatives of the exchange use web domains in high-risk jurisdictions with no clear connection to its publicly stated place of business; and
- trading addresses, phone numbers and other business information change frequently and for no apparent reason.



BTC-e remains the most notorious example of a non-compliant, unlicensed exchange that operated with many high-risk geographical indicators while readily facilitating illicit activity.

Established in 2011 by Alexander Vinnik – a Russian national – BTC-e was the preferred exchange for criminals using cryptoassets until Vinnik’s arrest in Greece, in mid-2017. By some estimates, as much as 95% of all Bitcoin-denominated ransomware payments were cashed out via BTC-e<sup>11</sup>. According to US authorities, BTC-e engaged in a wide array of crimes which included “computer hacking and ransomware, fraud, identity theft, tax refund fraud schemes, public corruption, and drug trafficking”.<sup>12</sup>

BTC-e provided cryptoasset trading services to US persons without ever registering as a Money Service Business (MSB). This led the US Financial Crimes Enforcement Network (FinCEN) to impose a civil monetary penalty of \$110 million on Vinnik and BTC-e. According to FinCEN: “BTC-e allowed its customers to open accounts and conduct transactions with only a username, password, and an email address. The minimal information collected was the same regardless of how many transactions were processed for a customer or the amount involved”. BTC-e also allowed customers to transact after using mixers and gave them access to privacy coins such as Dash.

BTC-e worked to conceal the nature of its activities by operating through a web of corporate structures. It also provided incomplete and contradictory information on its whereabouts and the location of its activities. BTC-e’s ownership structure involved numerous shell companies, including the UK-registered Always Efficient LLP, which in turn had nominee directors based in the Marshall Islands and the Seychelles.<sup>14</sup>

The US indictment of Vinnik alleges that “BTC-e’s own website stated that it was located in Bulgaria, yet simultaneously stated it was subject to the laws of Cyprus. Meanwhile, BTC-e’s managing shell company Canton Business Corporation was based in the Seychelles but affiliated with a Russian phone number, and its web domains were registered to shell companies in Singapore, the British Virgin Islands, France and New Zealand”.<sup>15</sup> BTC-e also relied on offshore bank accounts in the names of various shell companies to process fiat transactions with its customers.

In July 2018, FinCEN Director Kenneth Blanco described how Suspicious Activity Reports (SARs) helped FinCEN to detect BTC-e’s evasive behavior, noting that “SAR filings played a critical role in the investigation of that case. It was filings by both banks and other virtual currency exchanges that provided critical leads for law enforcement.

This information included beneficial ownership information, additional activity attributed to the exchange of which we were previously unaware, jurisdictional information, and additional financial institutions we could contact for new leads. All of this was obtained through SARs and the supporting documents filed by financial institutions.”<sup>16</sup>

BTC-e was, for a time, reconstituted under a new name – WEX – and registered in Singapore. Vinnik remains in custody in Greece, with the US, France and Russia all seeking his extradition.



#### Bitzlato – a Primary Money Laundering Concern

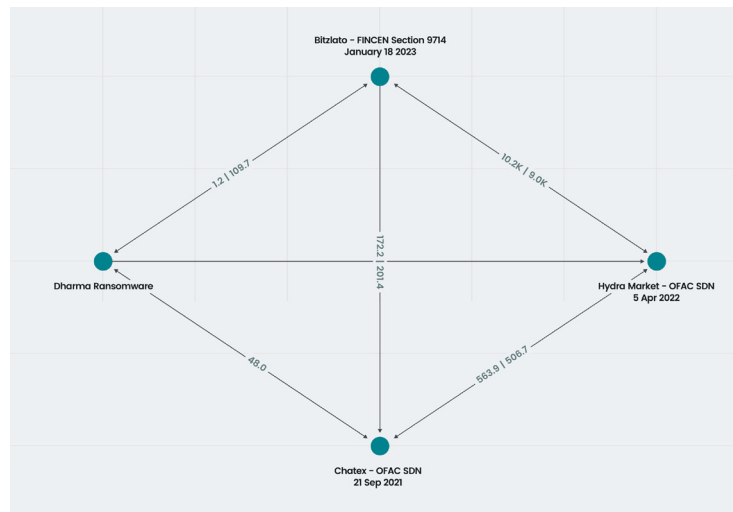
In January 2023, FinCEN took action against another Russia-linked crypto exchange it accused of facilitating widespread money laundering activity.

On January 18th, FinCEN identified Bitzlato – a Hong Kong-registered exchange owned by individuals from Russia – as a “primary money laundering concern”. The designation was made under section 9714 of the Combatting Russian Money Laundering Act, and marked the first time FinCEN applied the “primary money laundering concern” label to a crypto exchange. FinCEN had previously used authorities under the USA PATRIOT act to apply the label to approximately two dozen financial institutions it had accused of egregious money laundering activity, which puts Bitzlato among notorious company.

Specifically, FinCEN alleges that Bitzlato laundered hundreds of millions of dollars worth of cryptoassets on behalf of Russia-based illicit actors, including users of the Hydra darknet market, numerous ransomware campaign and the OFAC-sanctioned Chatex crypto exchange.

As a result of the action, US crypto exchanges and financial institutions must not engage in transactions with Bitzlato, and must ensure that they reject or block incoming funds transfers with Bitzlato and its successor entities.<sup>17</sup>

The image from Elliptic Investigator shows transactional links between the Bitzlato crypto exchange, the OFAC sanctioned entities Hydra Market and Chatex, and the Dharma Ransomware campaign.



## ✔ Dealing with Unlicensed, Non-compliant Exchanges (Including Exchanges in Higher-risk Jurisdictions)

Below are some of the controls that can be used to assist in the detection of unlicensed and non-compliant exchanges, including those in higher-risk jurisdictions:

- Elliptic Lens and Elliptic Navigator – to identify where a cryptoasset address or transaction is associated with an entity that is located in a high risk or sanctioned jurisdiction;
- Elliptic Investigator – to follow the flow of funds through the blockchain to identify if they originate from, or are deposited into, high-risk exchanges; determine if the exchange is associated with significant levels of transactions with illicit entities.
- Elliptic Discovery – to identify where an exchange is unlicensed, whether it lacks KYC requirements or AML policies, or presents other high-risk factors;
- consulting information on an exchange’s website to determine whether it requests KYC information of its users and, or imposes meaningful limits and restrictions on trading activity;
- requesting that an exchange provide copies of its AML policies and procedures;
- in some cases, asking an exchange to provide additional information about the size, location and nature of its customer base;

- obtaining corporate due diligence reports and searching open-source beneficial ownership registries – such as Companies House in the UK – to obtain information about an exchange’s ownership and control structure;
- requiring that exchanges seeking corporate cryptoasset services are subject to questions contained in enhanced due diligence forms; and
- screening the name of an exchange and its beneficial owners for evidence of adverse media or the presence of Politically Exposed Persons (PEPs).



#### OTC Traders Operating on Exchanges

Over-the-Counter (OTC) brokers play an important role in the cryptoasset ecosystem. They facilitate large trades between liquidity providers, often at lower prices than those available on exchanges. It is estimated the size of cryptoasset OTC markets are likely to total between \$2 billion to \$20 billion per day.

Where they maintain accounts at exchanges to facilitate their trading, OTC desks can act as an attractive avenue for money laundering. Their large trades offer a convenient cover for the introduction of illicit funds. This is particularly true of Chinese OTC brokers, who frequently maintain accounts at exchanges located in Asia and have been associated with large money laundering operations.

By maintaining nested accounts at larger exchange businesses, illicit OTC brokers can conceal themselves in the larger cryptoasset ecosystem with a veneer of legitimacy. This was the operating model of the SUEX and Chatex exchange service sanctioned by OFAC in September and November 2021, respectively, for facilitating ransomware laundering.

US law enforcement agencies have stated that Chinese cryptoasset brokers are involved in laundering funds on behalf of Mexican drug cartels.<sup>18</sup> Chinese authorities also undertook a major crackdown on OTC traders across 2020, responding in part to their potential involvement in money laundering.<sup>19</sup>

These OTC services may also offer crypto-to-cash swaps for users. Services such as SUEX and Chatex enabled users to swap Bitcoin for Russian ruble cash notes. Research by Transparency International (TI) also indicates that Russia-based OTC brokers allow users in the UK to swap stablecoins such as Tether for cash. According to TI, these services do not seek KYC information of users.<sup>20</sup> (See more information about money laundering using stablecoins in section 4 of this report).

## 1.3. Use of Money Mules or Fraudulent Documents at Legitimate Exchanges

### The Problem

Using regulated and compliant exchanges can add a veneer of legitimacy to a criminal's otherwise illegitimate behavior. Legitimate exchanges can have a "mixing" effect for criminals. They can obtain new, untainted coins or cash out with fiat so that their otherwise tainted trail of activity appears clean.

Regrettably, criminals sometimes succeed in abusing legitimate exchanges. The use of fraudulent KYC documents is attractive to money launderers seeking to deceive legitimate exchanges because the cryptoasset industry is online, and not face-to-face.

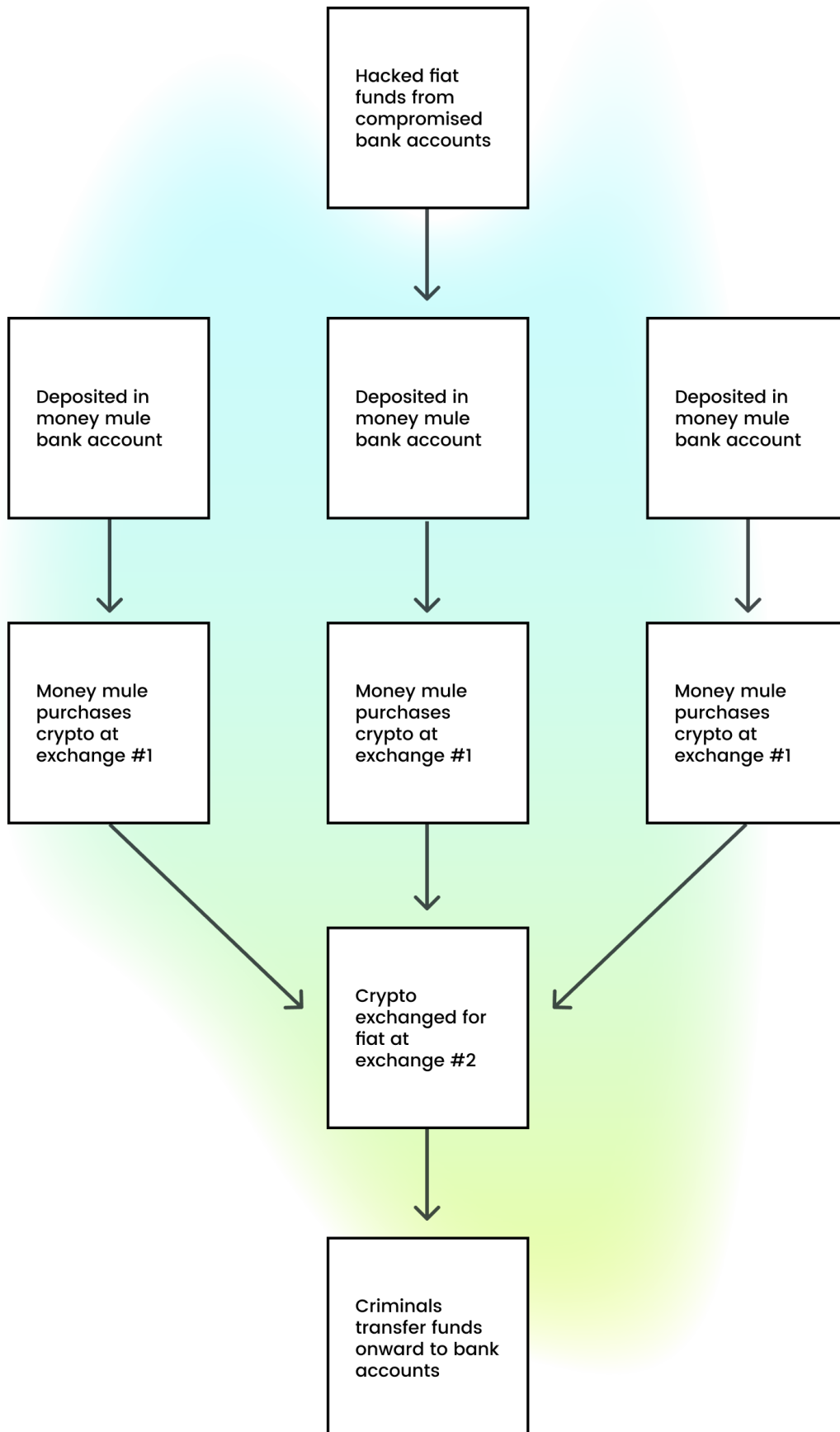
Criminals often rely on fraudulent documents to open accounts in their own names, or in the names of other individuals. One method involves employing money mules – individuals who are used to open accounts and move funds on behalf of the criminal network.

### The Typology

A common method of employing money mules at legitimate exchanges works as follows:

1. A group of individuals – often of common nationality and similar residential addresses – establish accounts at a cryptoasset exchange, generally within a short time period of one another.
2. The new customers provide full identity details and supporting documentation, including passports and driving licences. They may even supply selfies when prompted to do so by the exchange's mobile app.
3. The new customers are provided with accounts at the exchange.
4. In one such set up, the mule accounts transfer in, or out, illicit funds to or from external sources – such as bank accounts – that are also registered in the names of the mules. The mules may operate the accounts themselves and facilitate transfers.
5. Alternatively, the criminals will operate the mule accounts manipulating them for their own ends. This could mean transferring funds to external sources, such as banks, money transfer services or other cryptoasset exchanges.

The diagram below provides a general illustration of how a money mule operation can work.







### Students Used as Money Mules in the UK

In October 2021, *The Guardian* reported on a money muling scheme targeting university students and relying on cryptoassets to launder illicit funds.<sup>21</sup>

In this scheme, university students responded to job advertisements on social media offering between £500 and £1,000 per week to act as brokers for cryptoasset transactions. Students who responded to the job posting were told by agents of a criminal organization posing as job recruiters to provide their personal information and ID documents. The criminal organization then instructed the students to open accounts at cryptoasset exchanges using their identity details and documents.

The criminal organization would then transfer fiat currency funds into the students' bank accounts in round value denominations of £700. The students were instructed to transfer the funds – which were derived from online fraud – to cryptoasset exchanges and buy cryptoassets with the proceeds of crime.

The student money mule accounts therefore acted as a way for criminals to launder the proceeds of fraud using crypto exchange accounts in the names of other individuals.



### DoJ Takes Down International Crypto Money Laundering Ring

In November 2022, the US Department of Justice (DoJ) announced criminal charges against 21 individuals involved in using cryptoassets to launder funds stolen from US-based victims of online scams, such as romance scams, technical support schemes, and other forms of fraud, as well as from crimes such as dealing narcotics. Those charged acted as money mules on behalf of members of fraud and drug rings.

For example, one of the accused was Zenobia Walker of Maryland, who received cash and checks in US dollars from victims of romance scams. After depositing the funds in her personal bank account, she would then convert the funds into cryptoassets to send to members of a fraud ring.<sup>22</sup>

## Red Flags

Common red-flag indicators associated with money mule activity impacting legitimate exchanges include the following:

- accounts are opened by numerous individuals within a short period of time using shared addresses, mobile devices, IP addresses and other common identity indicators;
- presentation of documents that appear to be forged, falsified or stolen;
- sometimes documents that are forged or stolen may be almost impossible to distinguish from legitimate documents (see the text box on KYC kits below);
- large numbers of accounts may be opened simultaneously by groups of foreign nationals. They may be exploited for the purposes of opening accounts and have no clear link to the country where the exchange operates. For example, it could be groups of Vietnamese nationals opening accounts in Japan, or nationals from Baltic states opening accounts at exchanges in Spain;
- inconsistencies between the customer's stated identity information and other data they provide, or activity they undertake. This could be a customer with an address in a poor rural region of Africa who may have an email address, or IP addresses associated with China. They could make frequent large value cash-outs to exchanges in Hong Kong, suggesting a Chinese individual has stolen or purchased the mule IDs;
- multiple customers make high-value onward transfers to common accounts in high-risk jurisdictions with no clear apparent purpose. A customer can purchase cryptoassets in euros at a Finland exchange, quickly swap them for Colombian pesos and then request immediate transfers onward to banks in Colombia;
- cryptoassets pass through tumblers or mixers before eventually being transferred to the mule's wallet. Funds are promptly cashed out from the exchange to bank accounts belonging to money mules;
- fiat funds may be sent to the exchange from corporate bank accounts – suggesting an online banking compromise – with requests to make rapid high-value transfers into cryptoassets;
- frequent transfers are made to or from the customer's account at the exchange, to or from individual third-party bank accounts – for instance, the mule is transferring funds to other mules or to criminals;
- the account holder may not have any understanding of what the funds in the account are being used for when questioned. In a case of stolen identity, they may not even be aware that an account was opened in their name;

- mule accounts may feature randomly generated email addresses that just have a string of random numbers and letters; and
- some mules may suggest that they have responded to ads on social media platforms offering money to open an account at the exchange.



A common practice to enable money muling is the availability of “KYC kits”. Sold on the dark web, KYC kits provide criminals with stolen identity details of victims that can be used to open accounts and bypass AML controls.<sup>23</sup> KYC kits can include a significant amount of information about the victim, such as:

- full name, date of birth, residential address and other identifying details;
- images of the individual’s ID documents, including passports, national ID cards or driving licences;
- selfies taken using a mobile device during online account opening; and
- logins and passwords for online bank accounts and other sites.

Elliptic’s investigations have revealed more criminals are willing to use legitimate, compliant exchanges to launder funds because they can employ KYC kits. The image below shows an advertisement from the now-defunct Dream Market dark web market for KYC kits complete with selfies, ID documents and utility bills.

**Selfie holding ID Serbia + ID photo +utility bill**

**Vendor** CardPass (2950) (4.85★) (📧 146/4/9)

**Price** ₪0.00913 (€52)

**Ships to** Worldwide

**Ships from** Worldwide

**Escrow** Yes



**Product description**

Selfie holding ID + ID photo + utility bill Serbia.

You will get:

- selfie holding ID
- ID photo both sides
- utility bill no older than 3 months

All documents are valid. You can choose male or female.

## Dealing With Money Mules

The following are controls used to assist in the detection of money mules:

- using cryptoasset transaction monitoring software like Elliptic Navigator to identify transactions among exchange customers that demonstrate patterns of money mule activity, such as repeated low-value transactions that ultimately derive from or flow to an illicit source of funds;
- using Elliptic Investigator to trace and visualize the flow of funds to or from an exchange that reveal patterns of transactions associated with money muling;
- monitoring customer logins and using mobile device fingerprinting to determine if the customer is active where they claim to be resident;
- using third-party identity document scanning solutions to assess the reliability of passports and other IDs;
- monitoring customer devices to identify whether multiple customers are using the same mobile device to access their accounts;
- following customer IP addresses to identify customers who may be accessing accounts from the same location;
- searching customer accounts for signs of emails registered to foreign domains inconsistent with their residential addresses;
- obtaining third-party due diligence reports on customers of concern in case they have other phone numbers or addresses associated with their name in addition to those listed on their account;
- imposing limits or prohibitions on customers to transfer funds to – or receive funds from – third-party accounts.

## 2. Mixers and Privacy Wallets

Cryptoasset mixing services add an element of privacy and opaqueness to the otherwise highly transparent crypto ecosystem. By collating and redistributing cryptoassets among numerous users, these services break the chain of end-to-end traceability around transactions on cryptoasset blockchains.

Mixers play a vital role in cryptoasset laundering due to their ability to obscure transaction flows. Illegal mixing services have generally been associated with a small number of mixers, whose creators in some cases advertise to dark web vendors, cybercriminals and other illicit actors.

Among the most prolific mixers to date was the Helix mixer, which went offline in early 2018 but operated as a significant money laundering vehicle for criminal actors. In February 2020, its founder Larry Dean Harmon was arrested and charged with laundering over \$300 million via the Helix mixer on behalf of criminals.<sup>24</sup>

In October that year, FinCEN announced a \$60 million penalty against Harmon for operating an unlicensed MSB. In April 2021, the US Department of Justice (DoJ) announced the arrest of Roman Sterlingov, the alleged operator of Bitcoin Fog, another widely used mixing service that processed hundreds of millions of dollars in transactions for dark web markets.<sup>25</sup>

Transactions with mixers also increasingly present sanctions risks. The US Treasury has begun targeting mixers with its sanctions powers, as we describe in one of the case studies below.

### The Problem

Mixing services are generally used in coordination with other money laundering typologies outlined in this report, some of which we've covered throughout (we also note some specific cases that have emerged recently in Chapter 13 on multi-service typologies).

Over the past two years, privacy wallets have also become an increasingly important money laundering vehicle for criminals. Privacy wallets such as Wasabi Wallet and Samurai use built-in anonymization techniques like CoinJoin to achieve a mixing effect that hides a users' ultimate source of funds. As the graph below demonstrates, privacy wallets have overtaken mixers as a preferred avenue for laundering illicit funds.

Fortunately, despite their opaque properties, mixing services and privacy wallets are detectable using Elliptic's blockchain analytics software – enabling cryptoasset businesses to identify related suspicious activity.

## The Typology

1. A hacker, ransomware attacker, darknet market vendor or other criminal obtains cryptoassets.
2. The perpetrator transfers the funds through multiple wallets, potentially using chain-peeling techniques (see chapter 6), before sending the funds to a mixer or privacy wallet.
3. The criminal may also send funds through other conversion services, such as DEXs (see chapter 3.2), prior to sending them to the mixer or privacy wallet.
4. After receiving new, “clean” cryptoassets from the mixer or privacy wallet, the criminal will send the funds to a centralized exchange service to convert the funds into fiat. The funds may be sent through multiple intermediary wallets before arriving at the exchange.

### Red Flags

Red-flag indicators associated with cryptoasset laundering using mixing services and privacy wallets include the following:

- a customer has received a large amount of funds from a mixing service or privacy wallet and cannot provide further evidence of the ultimate source of funds;
- a customer’s account shows frequent transactions to or from a mixing service or privacy wallet in a short amount of time, with only a vague explanation; and
- a customer is evasive about their reason for using a mixing service or privacy wallet.

Elliptic’s software can generally identify known mixers and privacy wallets, and below are other indicators of Bitcoin addresses that could represent unidentified mixing services on the blockchain:

- the address involves very large volumes and values of Bitcoin inputs and outputs – it can be more than 20,000 – and has been highly active;
- at any given time, the address has a very low balance, which would distinguish it from an exchange or other conversion service managing customer orders; and
- the address suddenly stops transacting after having processed large volumes of payments – suggesting it has been abruptly shut down.



## July 2020 Twitter Hack

The July 2020 Twitter hack is one of the best examples to date of how blockchain analytics enabled the real-time detection of criminals. It also illustrated the role of mixing services and privacy wallets in illicit transfers.

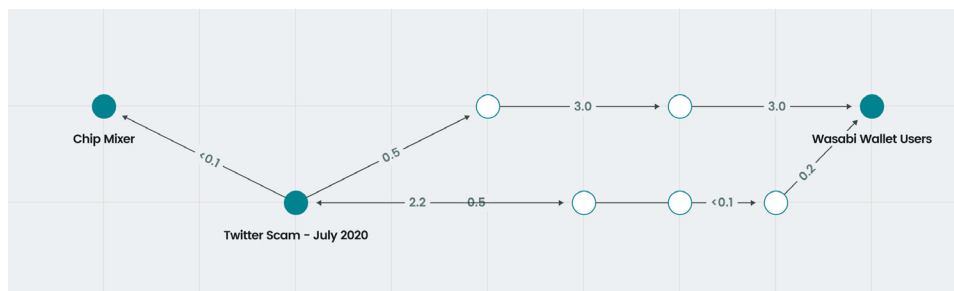
On July 15th 2020, Twitter suffered a major breach which allowed hackers to post fraudulent tweets through 130 compromised accounts owned by a range of well-known individuals and corporations. The attack started with a phone scam known as spear-phishing – targeting Twitter employees.

The compromised accounts were used to defraud around 400 victims of \$121,000 in Bitcoin, by way of a common fraud technique known as a “giveaway scam”. Once the hackers received funds from the victims, they undertook an elaborate series of transactions in an attempt to launder the Bitcoin. Approximately half of the stolen funds were sent via ChipMixer and Wasabi Wallet, while much of the remainder was sent to cryptoasset exchanges.

While the use of ChipMixer and Wasabi Wallet added a layer of obfuscation to the hackers’ funds transfers, cryptoasset businesses were not completely in the dark.

Elliptic’s capabilities enable its customers to determine whether a crypto transaction originated from specific mixing services such as ChipMixer or Wasabi Wallet. Knowing that these specific mixers were used by the scammers, cryptoasset exchanges in receipt of funds from those services could initiate further due diligence and identify whether their customers deposit proceeds of this scam.

The hackers – three US and UK teenagers – were arrested on July 31st 2020, which was only 16 days after the cyberattack. Blockchain analytics and information obtained by cryptoasset businesses and supplied to law enforcement played a pivotal role in apprehending them.



The above image from Elliptic Investigator shows the flow of funds between a Bitcoin wallet belonging to the July 2020 Twitter scammers and the obfuscating services Wasabi Wallet and ChipMixer.



US legal and regulatory action against Larry Dean Harmon – the founder of the Helix and Coin Ninja mixing services – reveals the scale and nature of illicit activity that mixing services can achieve.

FinCEN discovered that Harmon offered his mixing services to criminals – especially vendors on the dark web market Alphasay. Over a three-year period, he processed more than one million transactions worth \$311 million.<sup>26</sup>

Harmon ran Helix on the Grams darknet.onion site<sup>27</sup> and advertised his services on both the surface web and dark web, claiming that Helix could allow users to avoid law enforcement detection. He argued that by providing users with fresh cryptoasset addresses with no trading history, Helix made transactions less susceptible to blockchain monitoring<sup>28</sup>. From April 2014 to December 2017, Helix was the mixer of choice for dark web vendors on Alphasay, Agora Market, Nucleus, Dream Market and others.<sup>29</sup> Harmon also facilitated transactions on behalf of child exploitation sites, neo-Nazi groups, Iran-based users and conducted approximately \$900,000 of transactions involving BTC-e.<sup>30</sup>

FinCEN provided the following detailed account describing how Helix transactions worked:

- a. customers would send Bitcoin to a wallet associated with their Grams account;
- b. customers would then complete a Helix withdrawal form, which included the amount to withdraw, a destination address and the ability to set a time delay for the transactions;
- c. Helix would transmit the Bitcoin deposited into their wallet to one of numerous accounts held at different exchangers of convertible virtual currency;
- d. Helix would take Bitcoin from a different account it held and transmit that Bitcoin to a different Bitcoin address;
- e. from this Bitcoin address, Helix would then transmit Bitcoin to the customer – minus a fee – into the previously provided customer destination address;
- f. Helix asserted that it deleted customer information after seven days, or allowed customers to delete their logs manually after a withdrawal.<sup>31</sup>

In addition to running Helix, Harmon set up a Delaware company called Coin Ninja in July 2017. The latter also operated a mixing service “allowing customers to accept and transmit Bitcoin through text messages or Twitter handles”.<sup>32</sup>



## Preventing Abuse of Mixers and Privacy Wallets

Controls to mitigate or prevent the risk of money laundering using mixing services and privacy wallets include:

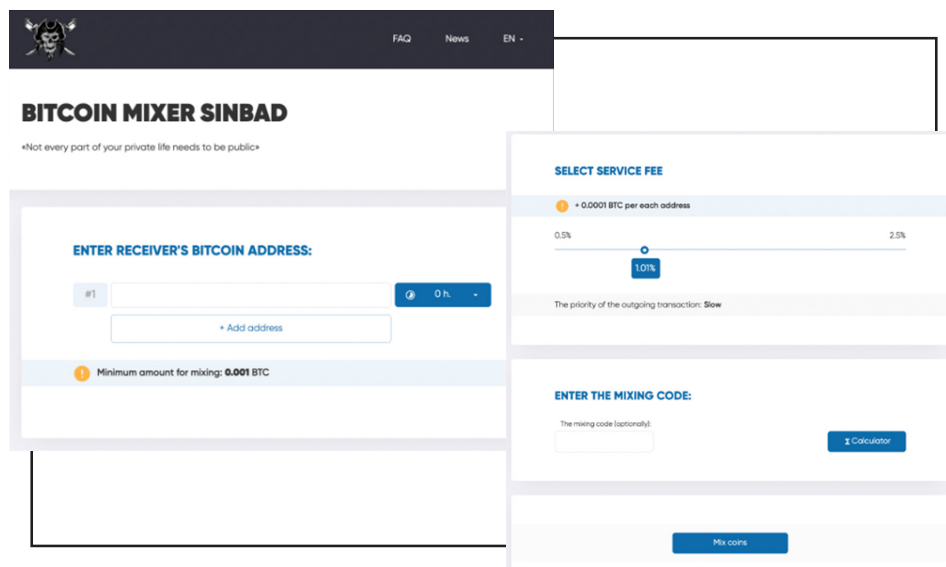
- utilizing wallet screening solutions – such as Elliptic Lens – to identify attempted customer withdrawals to wallets associated with mixers and privacy wallets;
- utilizing transaction monitoring solutions like Elliptic Navigator to identify transactions with exposure to mixers and privacy wallets;
- establishing policies and procedures to ensure enhanced due diligence is conducted around higher-risk scenarios involving mixers and privacy wallets. This includes seeking additional information from the customer about the purpose and ultimate source or destination of funds.



### Sanctions and Mixers

Since early 2022, OFAC has begun imposing sanctions on mixing services that have facilitated illicit activity.

In May that year, OFAC sanctioned Blender – a mixing service that was used to launder Bitcoin by North Korea’s Lazarus Group – a sanctioned cybercrime organization.



The screenshot displays the Bitcoin Mixer Sinbad website. At the top, there is a navigation bar with a skull icon, 'FAQ', 'News', and 'EN'. Below the navigation bar, the title 'BITCOIN MIXER SINBAD' is prominently displayed, followed by the tagline '«Not every part of your private life needs to be public»'. The main interface is divided into several sections: 1. 'ENTER RECEIVER'S BITCOIN ADDRESS:' with a text input field containing '#1', a '0 h.' timer, and an '+ Add address' button. 2. A notification bar stating 'Minimum amount for mixing: 0.001 BTC'. 3. 'SELECT SERVICE FEE:' section featuring a slider from 0.5% to 2.5% with a '10%' marker and a '10%' button. Below the slider, it says 'The priority of the outgoing transaction: Slow'. 4. 'ENTER THE MIXING CODE:' section with a text input field and a 'Calculator' button. 5. A 'Mix coins' button at the bottom.

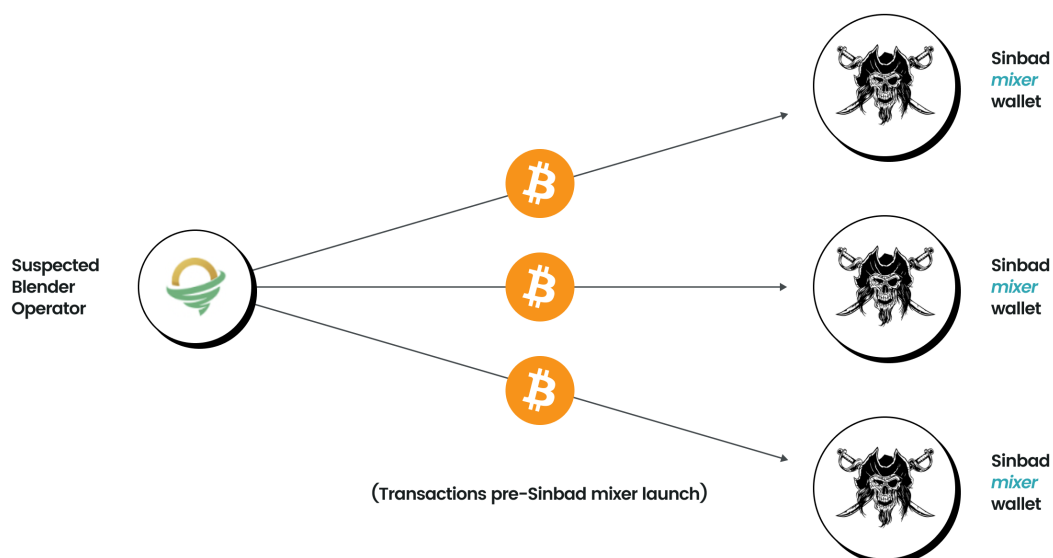
*The Sinbad website.*

Analysis of the blockchain indicates that the Lazarus Group laundered Bitcoin worth more than \$20.5 million through Blender following the March 2022 hack of the Ronin Bridge, a decentralized finance (DeFi) service related to the *Axie Infinity* blockchain-based gaming platform, which resulted in the theft of more than \$540 million on cryptoassets.

By imposing sanctions on Blender, OFAC prohibited US persons – including US crypto exchanges – from processing transactions with the mixer, which shut down around the time of the sanctions.

In researching Sinbad, Elliptic determined that the new service appeared to be acting as a replacement for Blender following the OFAC sanctions. Analysis of Bitcoin transactions indicated that Sinbad's activity was closely tied to Blender's through common transactions, and showed that a disproportionate number of transactions for such a new mixing service appeared to be related to facilitating transactions with the Lazarus Group.

Cryptoasset businesses and financial institutions therefore face a range of sanctions risks when it comes to mixers and other privacy-enhancing services.



*Analysis of blockchain transactions shows clear links between Blender and Sinbad.*

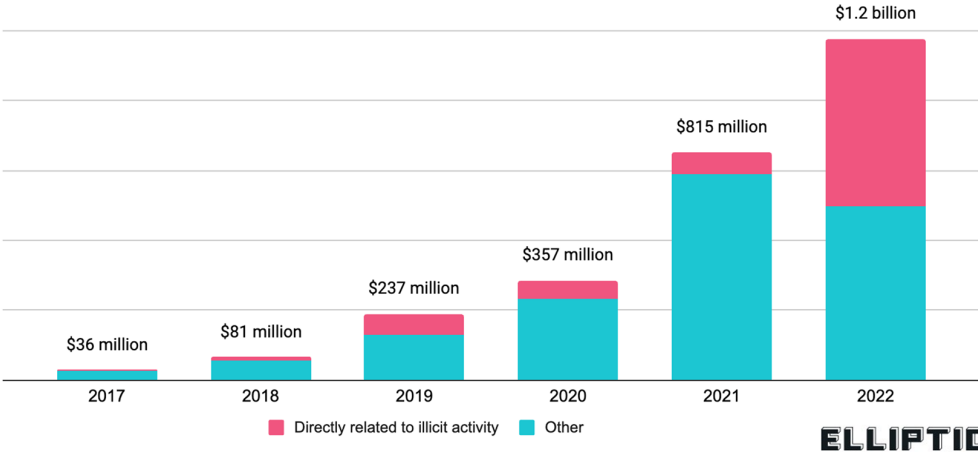


In total, more than \$2.7 billion in Bitcoin was sent through ChipMixer since it was established in May 2017.

As part of the operation, law enforcement were able to seize \$47.5 million in Bitcoin from the mixer.

The US Justice Department also announced that 49-year-old Minh Quoc Nguyen of Hanoi, Vietnam, was charged with money laundering, operating an unlicensed money transmitting business and identity theft, connected to the operation of ChipMixer.

### Over \$1 Billion in Bitcoin was Sent Through ChipMixer in 2022 - Half Linked to Criminal Activity



### 3. Decentralized Finance (DeFi) and Cross-chain Crime

Decentralized finance (DeFi) has been one of the most significant areas of cryptoasset growth and investment over the past couple of years. DeFi involves the use of “smart contracts” – or programmable, self-executing protocols – to enable users to have disintermediated access to financial services that have historically only been available through centralized financial institutions. Using the Ethereum network – as well as other emerging blockchains – innovators have launched new DeFi apps (Dapps) for use cases such as:

- lending;
- stablecoins;
- derivatives trading;
- prediction markets;
- asset management; and
- decentralized exchange services (DEXs).

The growth in the DeFi space in recent years has been truly explosive. The total value of capital locked in Dapps grew 1,700% during 2021 to reach \$247 billion, and monthly trading volumes on DEXs hit \$300 billion. While DeFi trading volumes declined off their highs during 2022 as crypto markets faced turbulence, DeFi innovations remain at the forefront of developments in the crypto space. This incredible rate of innovation has started to gain the attention of banks and other financial institutions, which are considering how they can leverage DeFi innovations to provide their clients with new products and services.

However, innovation in the DeFi space brings risk as well as opportunities. DeFi protocols and apps, for example, are frequently targeted by cybercriminals, who steal funds from them. Elliptic’s research indicates that approximately \$3.3 billion was stolen from exploits of these protocols in 2022.

What’s more, criminals are able to use the DeFi ecosystem to launder the proceeds of crime. Users of Dapps can generally access these services without having to provide KYC/CDD information, which makes the DeFi ecosystem an attractive conduit for cybercriminals and others seeking to launder stolen cryptoassets.

Furthermore, DeFi allows users to move funds seamlessly across different cryptoassets and blockchains. This enables the acceleration of “chain-hopping” typologies of money laundering, whereby criminals attempt to break the funds trail on the blockchain by swapping their ill-gotten funds into other assets or coins. In a report it issued in June 2022, the FATF noted that “DeFi protocols can be used to perform ‘chain-hopping’ which can make the transactions more difficult to trace”.

We've outlined these risks and challenges in detail in our separate "State of Cross-Chain Crime" report. The rise of this type of crime also prompted Elliptic to update our blockchain analytics solutions suite across 2023 to enable the detection of these risks, including by pioneering our unique Holistic Screening capabilities, which enable the instantaneous identification of funds being swapped through cross-chain and cross-asset services.

Below, we summarize three of the primary DeFi money laundering typologies that enable cross-chain crime, and tips for how you can spot them.

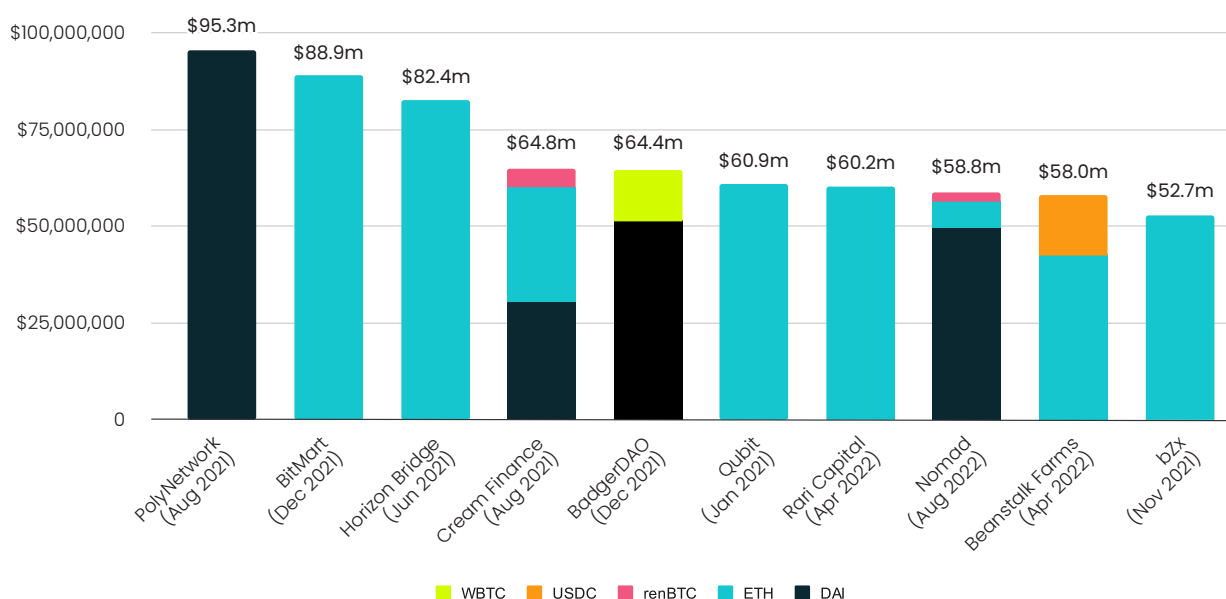
### 3.1. Money Laundering Through DEXs

Unlike centralized exchange platforms – which are custodial services that take possession of users' funds – DEXs built on Ethereum and other blockchains utilize smart contracts to enable users to undertake peer-to-peer (P2P) cryptoasset swaps exchanges in real time.

DEX trading volumes have exploded in recent years, hitting highs of more than \$30 billion per month at their height. Major DEXs such as Uniswap are now competing with large centralized exchanges in overall trading volumes. This increase in liquidity on DEXs has also made them increasingly vulnerable to exploitation by money launderers, who can layer large volumes of funds through these increasingly active platforms.

Elliptic's research has shown that to date, hackers have laundered more than \$1.2 billion of funds stolen from hacks of DeFi protocols through DEXs in an effort to throw investigators off the trail. The chart below illustrates the largest hacks where funds were laundered through DEXs after the attack.

Top 10 Exploits By Assets Swapped Through DEXs



## The Problem

DEXs can offer criminals the advantage of bypassing compliance controls – much in the manner of dealing with non-compliant exchanges like SUEX, Chatex or BTC-e. Simultaneously offering another advantage, they lack a central administrator with active oversight of user accounts, records, identities or activities.

In many jurisdictions, it is still unclear whether DEXs fall within the scope of AML/CTF regulation. DEXs provide a useful mechanism for the laundering of criminal proceeds. In particular, for undertaking cryptoasset-to-cryptoasset swaps – while avoiding exposure to regulators or law enforcement.

DEXs may also prove attractive to more sophisticated illicit cryptoasset users – such as cybercriminals – who can use them with ease. North Korea’s cybercriminal organization the Lazarus Group made frequent use of DEXs across 2022, in an effort to hide hundreds of millions of dollars it stole from hacks of crypto platforms.

The explosion in DeFi has also led to a corresponding ecosystem of tools that enable hiding Ether transactions – such as the Tornado Cash mixing services. Criminals can use these in conjunction with DEXs.

More importantly, laundering via DEXs is not impervious to AML controls. Unlike centralized exchanges – which are a dead-end when it comes to trying to trace flows of funds through them – DEXs offer tremendous transparency when it comes to blockchain analytics. All DEX crypto-to-crypto swaps are recorded in smart contracts on the blockchain, which makes these swaps visible. This, therefore, allows users of Elliptic’s solutions to see if funds they’ve received are of illicit origin even where DEXs are used in the laundering process.

## The Typology

A money laundering typology involving DEXs works as follows:

1. a criminal obtains Ether or Ethereum-based tokens, for example by hacking an exchange;
2. the criminal moves the funds to a wallet they use at a DEX;
3. the Ether or Ethereum-based tokens are swapped at the DEX for new tokens; and
4. the new tokens are deposited at a legitimate exchange, and cashed out for fiat.

## Red Flags

Red flags associated with money laundering involving DEXs may include the following:

- a customer suddenly receives a large amount of cryptoassets directly from a DEX-associated account and attempts to cash out immediately;
- the customer can not provide any evidence or logical explanation for their source of funds and why they were engaged in dealings through a DEX; and
- the DEX in question may be associated with relatively high volumes of illicit activity involving dark markets, exchange hacks and other crimes such as ransomware attacks.



### The Axie Infinity Ronin Bridge Hack

On March 29th 2022, the Ronin Network announced that 173,600 Ether (ETH) and 25.5 million USD Coins had been stolen from the Ronin cross-chain bridge six days earlier. The total value of the stolen cryptoassets at the time of the theft was \$615 million.

On April 14th, the US Treasury's Office of Foreign Assets Control (OFAC) announced new sanctions against the thief's Ethereum address and listed the owner of this address as the Lazarus Group – the North Korean state hacking organization. The sanctions prohibit US persons and entities from transacting with this address to ensure the state-sponsored group can't cash out any further funds they continue to hold onto through US-based crypto exchanges.

The incident occurred six days before the exploit was announced by Ronin. Amid confusion over the delayed response, it announced that the exploit was only discovered after a 5,000 ETH withdrawal attempt from one of their users failed.

According to a postmortem published by Ronin, the theft came as a result of an attacker hacking the "validator nodes" of the Ronin bridge. Funds can be moved out if five of the nine validators approve it. The attacker managed to get hold of the private cryptographic keys belonging to five of the validators, which was enough to steal the cryptoassets.

Elliptic's internal analysis indicates that the attacker had managed to launder 18% of their stolen funds as of April 14th.

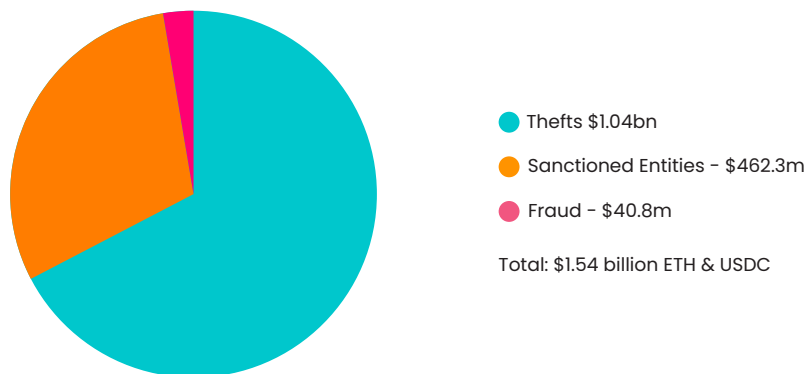
First, the stolen USDC was swapped for ETH through decentralized exchanges (DEXs) to prevent it from being seized. Tokens such as stablecoins are controlled by their issuers, who in some cases can freeze tokens involved in illicit activity.





Since being designated by OFAC, Tornado Cash’s transaction volumes have declined by more than 50%, which renders it less effective as a mixing service. However, the same typology that criminals have used in laundering funds through Tornado Cash is one that can apply to other, smaller Ethereum mixers.

## Proceeds of Crime Laundered Through Tornado Cash



## The Typology

A money laundering typology involving DEXs works as follows:

1. a criminal obtains Ether or Ethereum-based tokens, for example by hacking a DeFi lending platform;
2. the criminal sends the stolen funds to a Tornado Cash address;
3. the criminal receives new “clean” tokens from Tornado cash; and
4. the new tokens are deposited at a centralized exchange platform, and cashed out for fiat.

## Red Flags

Red flags associated with money laundering involving DeFi mixers may include the following:

- a customer receives frequent inbound transfers from a DeFi mixer such as Tornado Cash, and is unwilling or unable to give information about the ultimate source of funds;
- a customer makes frequent transfers to Tornado Cash or other DeFi mixers without a reasonable explanation for this activity; and
- a customer whose activity involves frequent interactions with DEXs also engages in transactions with mixing services such as Tornado Cash.



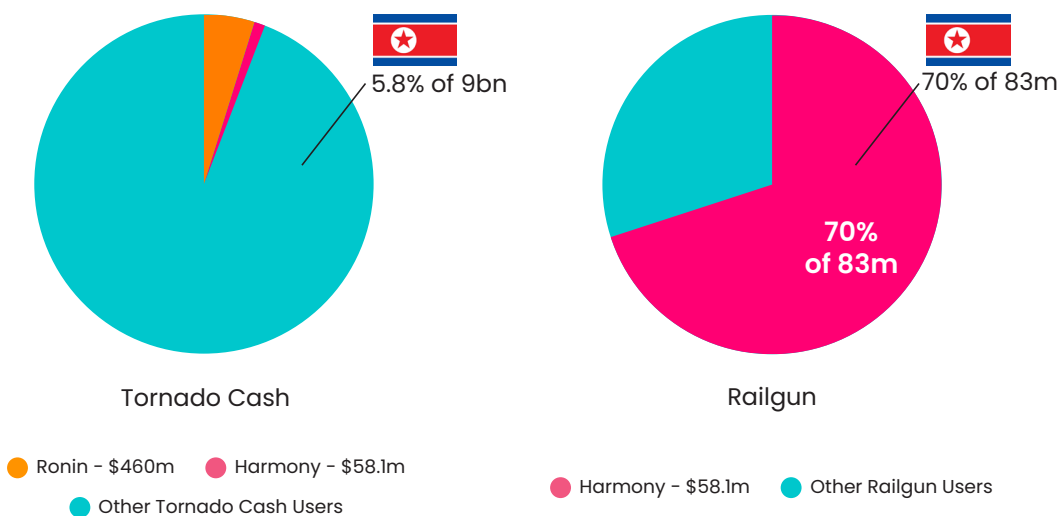
Horizon – a cross-chain bridge servicing the Harmony blockchain – was exploited on June 24th 2022 for \$99.7 million. Concerns had previously been raised that the bridge was over-centralized, meaning that it was particularly vulnerable to social engineering attacks, which is a common attack vector for the Lazarus Group. Similar issues resulted in the criminal organization stealing over \$540 million in the aforementioned Ronin attack earlier in March 2022.

After stealing the funds from Horizon, the Lazarus Group then programmatically structured transactions through Tornado Cash, which is a decentralized Ethereum-based mixer. Elliptic researchers identified that the laundering methods employed mirrored those the Lazarus Group had used when attempting to conceal funds from the Ronin Bridge hack, which had also been sent through Tornado Cash.

Tornado Cash was subsequently sanctioned by the US Treasury in August 2022, with Secretary of State Anthony Blinken citing its prolific use by the Lazarus Group to launder funds from its past hacks.

Elliptic's research suggests that the Lazarus Group sent more than \$555 million through Tornado Cash from these hacks, including more than \$468 million from the Ronin hack and \$96 million from the Harmony hack. This North Korea-linked activity accounts for approximately 5.8% of the nearly \$9 billion in total funds sent through the Tornado Cash mixer to date.

### Proportion of Funds DeFi Obfuscating Services Have Received From North Korean Hacks



Elliptic has traced the stolen funds from the Horizon hack through Tornado Cash. Our forthcoming briefing note will break down the methodology we used and how it ultimately aided the eventual attribution of the exploit to the Lazarus Group. The post-Tornado withdrawals were initially placed into several addresses, where they remained dormant until January 2023.

That month, Lazarus began structuring the funds into several deposits into a privacy-based DeFi protocol called Railgun, which functions similar to a mixer. Elliptic has previously identified Railgun as a prime alternative to Tornado Cash following sanctions against the latter. You can read more about Railgun – and other Ethereum-based privacy-enhancing solutions – in our Tornado Cash Alternatives briefing note.

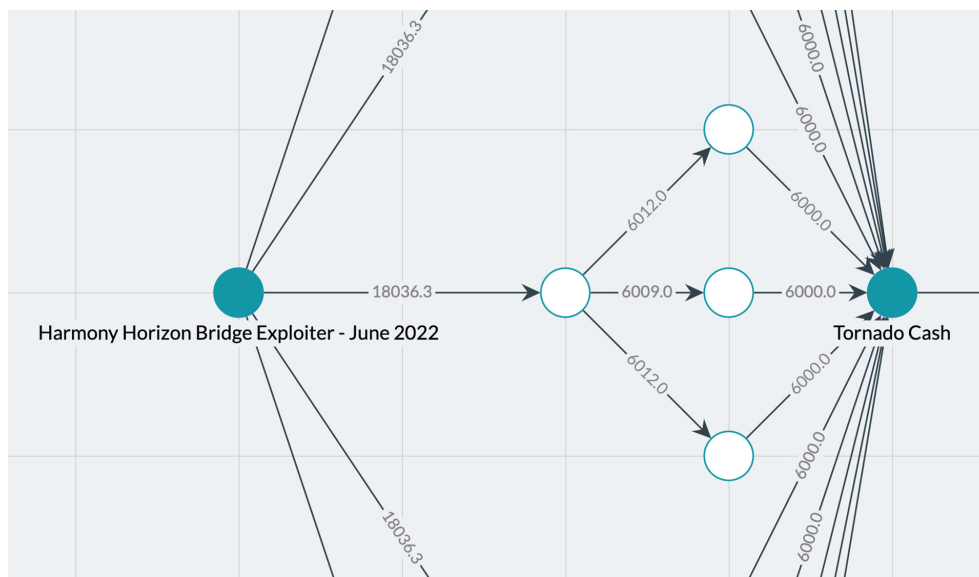
Elliptic's research suggests that a significant portion of funds – estimated at around 70% – that has been sent through Railgun to date are funds from the Harmony hack. This suggests that since the OFAC sanctions on Tornado Cash, North Korea may be turning to lower obfuscating services as an alternative. However, the fact that funds from the Harmony hack comprised such a substantial volume of the Ether passing through Railgun renders the mixing ineffective.

As an analogy, imagine if you threw five pennies into a jar full of 100 pennies, it would be extremely difficult for someone to determine which pennies were yours. However, if you threw 70 pennies into a jar with only 30 other pennies in it, then there would be a higher chance of linking those 70 specific pennies back to you. Mixers work in a similar way: when the anonymity set or volume of other funds in the mixer is low, it makes the mixer less effective at concealing disproportionately large funds transfers.

On-chain data shows that after sending the funds through Railgun, the Lazarus Group has since deposited funds into three cryptoasset exchanges. Two of them – namely Binance and Huobi – have announced that they have identified, blocked and seized a portion of the funds.

This case demonstrates the importance of cryptoasset exchanges utilizing blockchain analytics solutions to identify transactions involving mixing services abused by sanctioned actors such as North Korea. Elliptic's Holistic wallet and transaction screening solutions enable our customers to identify and block transactions involving these mixing services, including where there may be sanctions implications – such as links to North Korean-perpetrated hacks.

A screenshot from Investigator, Elliptic's multi-asset crypto investigations software – showing the stolen funds being sent through Tornado Cash, to several new wallets.



A screenshot from Investigator - Elliptic's multi-asset crypto investigations software - showing the stolen funds being sent through Tornado Cash, to several new wallets.

### 3.3. Money Laundering Through Cross-chain Bridges

One inherent limitation of DeFi ecosystems is that transactions within a particular DeFi network – such as Ethereum – are limited to tokens based on that blockchain. In other words, blockchains are not interoperable, and a user cannot use Bitcoin for transactions with Ethereum-based Dapps. This limits the practical utility of DeFi for many users, who may wish to move funds across numerous blockchains.

A solution to this problem are cross-chain bridges, which allow for an asset on one blockchain to be represented as a token on another. Popular cross-chain bridges have included RenBridge, VoltSwap and WanBridge. Rather than relying on a centralized exchange to swap Bitcoin for Ether, users can send their BTC to a cross-chain bridge to obtain Ethereum-based tokens, but avoid having to surrender custody of their cryptoassets or undergo KYC, as would be required if transacting through a centralized exchange.

#### The Problem

This ability to swap cryptoassets in and out of the DeFi ecosystem without having to undergo KYC presents obvious benefits for criminals, who may look to launder the proceeds of crime derived in one cryptoasset – like Bitcoin – for others, such as Ethereum-based tokens. This cross-chain movement of funds can present challenges for compliance analysts or investigators seeking to follow the funds trail.

## The Typology

1. A criminal obtains Bitcoin from an illicit source, such as launching a ransomware attack, or selling narcotics on the darkweb.
2. The criminal sends the illicit-origin Bitcoin to a cross-chain bridge.
3. The criminal receives new “clean” tokens from the cross-chain bridge in return for their Bitcoin.
4. The new tokens may be sent onward and further swapped at DEXs, or traded for fiat currencies at centralized exchange services.

## Red Flags

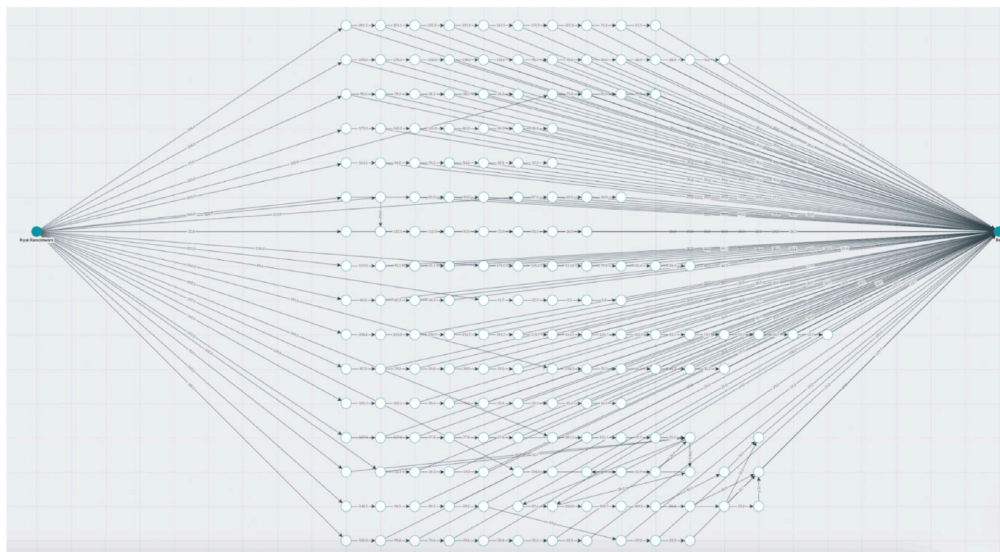
Red flags associated with money laundering involving cross-chain bridges may include the following:

- A centralized exchange’s customer receives frequent deposits of Ethereum-based or other DeFi tokens from addresses associated with cross-chain bridges, and cannot explain the reason for these transactions. Blockchain analytics screening shows that some of these funds are traceable back to illicit sources, such as wallets associated with ransomware or the darknet.
- A centralized exchange’s customer makes a high number of frequent withdrawals to bridges in a manner that appears abnormal.



## Laundering Conti Ransoms Through Cross-chain Bridges and Using Holistic Screening to Identify the Risks

Using crypto tracing forensics capabilities such as Elliptic Investigator, analysts can trace a ransomware gang's attempts to engage in money laundering with cross-chain bridges and other related services, as illustrated in the image below.



*A screenshot from Elliptic Investigator, showing the flow of Bitcoin from wallets associated with Ryuk cybercrime group (far left) to RenBridge (far right).*

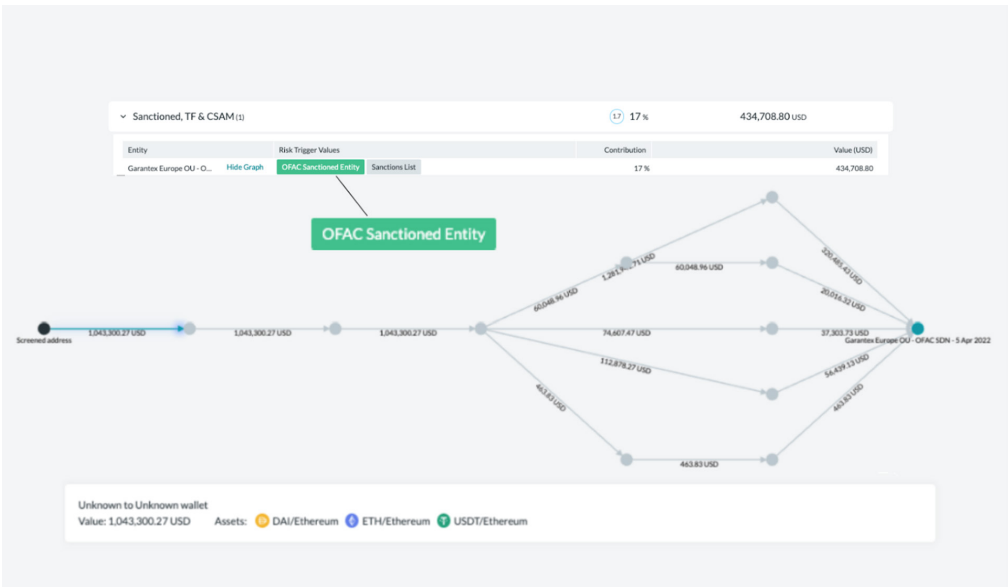
Once attackers swap their funds from Bitcoin into Ether through a bridge, they often then attempt to further launder the funds by swapping the new "clean" Ether for other tokens on the Ethereum network, including by swapping the funds at DEXs. As the FATF notes, this can involve swapping the funds for stablecoins.

In a detailed briefing note we published describing an Elliptic investigation into Conti's money laundering activity, our researchers identified a case of cross-chain and cross-asset laundering to try and conceal the proceeds of crime. In that case, Conti received 75 Bitcoin from a ransomware victim.

The Bitcoin was then sent through RenBridge and swapped for Ether. After obtaining the latter, Conti then swapped the funds for other Ethereum-based tokens, such as DAI and Tether, which are two stablecoins. These were then sent onwards to cryptoasset exchanges, including a crypto exchange in Estonia known as Garantex, that was sanctioned by the US Treasury in April 2022 for providing support to ransomware gangs.

Blockchain analytics can be used to screen the associated transactions in a case like this to identify where funds have been swapped through cross-chain and cross-asset services. As illustrated in the image below from Elliptic Navigator – our transaction screening solution – analysts can visualize the flow of funds through these services and across different assets.

This enables the identification of suspicious activity related to ransomware attackers' funds flows, and can enable the seizure and disruption of their assets where funds are deposited at cryptoasset exchanges. Elliptic's unique Holistic Screening capabilities allow analysts to identify these cross-chain and cross-asset funds transfers seamlessly and efficiently.



*This image from Elliptic Navigator shows the flow of funds from a ransomware attacker's Ethereum address (the black circle on the left) and the subsequent trail after the funds were converted for DAI and Tether, before being deposited at Garantex, an OFAC-sanctioned exchange (represented by the green circle on the right).*



## 4. Tokens and Stablecoins

One of the most important innovations in cryptoassets is the ability to launch new tokens with ease.

The emergence of token protocols such as ERC-20<sup>33</sup> has been instrumental in allowing innovators to launch new tokens that can fund the creation of new blockchain-based services and support the development of new cryptoasset or cryptoasset-powered platforms.

Tokens have also featured in emerging money laundering and fraud typologies. Most famously, they were associated with 2017's initial coin offering (ICO) bubble that featured widespread fraud. While that craze simmered down, tokens continue to flourish and can offer advantages to criminals, particularly where they are traded on DEXs that do not require KYC information.

In a related development, 2018 onwards has revealed the emergence of stablecoins, which are cryptoassets designed to avoid price volatility by pegging their value to fiat currencies or commodities. USDC, Tether, PAX Standard, DAI and others play a vital role in the cryptoasset ecosystem. Their price stability allows stablecoins to act as an effective on-and-off ramp between fiat currencies and more volatile cryptoassets such as Bitcoin.

The rapid rise of stablecoins has led to inevitable concerns about their role in financial crime. Indeed, in June 2020, the FATF published a report dedicated to the risks posed by them.<sup>34</sup>

The FATF asserts that there are several features associated with stablecoins that can create money laundering and terrorist financing risks:

- anonymity: enabling P2P transactions via the use of unhosted wallets, stablecoins can present elevated risks;
- global reach and potential for mass adoption: like other cryptoassets, stablecoins are globally accessible and unconstrained by borders. Unlike fully decentralized cryptoassets, stablecoin projects embedded in existing social and financial networks can potentially achieve mass scale rapidly, presenting systemic risks; and
- layering: price stability of stablecoins can make an attractive way to layer proceeds of crime derived from more volatile cryptoassets.

Elliptic's research and concurrent law enforcement and press reporting suggests that stablecoins appear increasingly in cases of money laundering, owing to these certain features. However, stablecoins often possess a feature that can mitigate the risks unlike most censorship-resistant cryptoassets like Bitcoin. Stablecoin transactions are reversible and allow their issuers to recover funds readily in cases of identified fraud or other criminality. This has enabled the seizure of stablecoins in instances of criminality.

## 4.1. Tokens & Stablecoins Used to Clean Illicit-origin Funds

### The Problem

Tokens and stablecoins can be rapidly traded for other more volatile cryptoassets, making them a useful conduit in the “layering” phase of money laundering.

Illicit actors may attempt to swap illicit-origin Bitcoin, Ether or other volatile cryptoassets for stablecoins, which they may then transfer onwards to exchanges or other services to cash out into fiat currencies. Criminals may also purchase stablecoins with illicit origin funds derived in fiat currencies from crimes such as drug trafficking and illegal online gambling, laundering the funds onwards to obscure their illicit origin.

### The Typology

1. A criminal actor has illicit-origin funds denominated in cryptoassets or fiat currencies.
2. If denominated in cryptoassets, the funds are swapped at centralized exchanges or DEXs for stablecoins. If denominated in fiat currencies, the perpetrator sends the funds from their bank account to an exchange, where they purchase stablecoins.
3. Having obtained new, “clean” stablecoins, the perpetrator sends the funds to another exchange service.
4. The criminal swaps their stablecoins for fiat currencies at the exchange, and proceeds to launder the new “clean” fiat currencies through the banking system.

### Red Flags

Red flag indicators associated with token-based laundering include the following:

- a customer of an exchange suddenly wishes to exchange a large volume of funds for stablecoins with no clear rationale;
- the funds are converted into stablecoins at unregulated or non-compliant exchange services, or through non-compliant OTC brokers; and
- blockchain analytics indicates a connection between the individuals involved in the transfers and ultimate sources of funds related to crimes such as drug trafficking, hacking, ransomware and illegal online gambling.



Law enforcement cases from China and the US have highlighted the use of stablecoins in facilitating illegal online gambling, as well as the movement of funds related to narcotics trafficking.

According to news reports,<sup>35</sup> law enforcement agencies in China unearthed a complex online gambling scheme that leveraged Tether for money laundering. In that scheme, members of illicit online gambling syndicates across China would collect funds from gamblers through mobile payments using QR codes. They used student money mule accounts and false websites to obscure the illicit renminbi transfers and consolidate them in accounts for onward transfer to the gambling site operators.

At this stage, the criminal network would convert the renminbi into Tether on cryptoasset exchanges. They would then transfer the Tether back into renminbi, thereby receiving new, “clean” funds.

In another case reported in the press in February 2023, the crypto exchange Binance collaborated with law enforcement to disrupt a Mexican drug cartel’s use of Tether to launder the proceeds of drug trafficking.<sup>36</sup> Under the scheme, drug dealers associated with the cartel and located in the US sold cocaine and methamphetamines, generating cash proceeds. These were deposited into the banking system, and the funds used to purchase Tether on the exchange. The drug dealers then transferred the Tether they’d purchased to a crypto wallet controlled by the drug cartel members in Mexico.

Binance’s collaboration with law enforcement on the case enabled the seizure of \$1.8 million from six accounts belonging to the cartel members.

## 4.2. Laundering of Proceeds From Scams

### The Problem

Some token projects have been outright scams. By some estimates, as many as 80% of ICOs launched during the 2017 craze were frauds and scams, and scams involving new tokens continue to flourish today.<sup>37</sup> Individuals – especially the financially vulnerable – are at risk of being coerced by fraudsters in this environment.

As described below, some cases of token scams may involve the laundering of cryptoassets obtained from innocent victims.

## The Typology

1. Victims are contacted by fraudsters or respond to ads on social media regarding new token projects promising large returns.
2. The victims are told to pay the fraudsters – posing as legit token founders – in Bitcoin or other cryptoassets.
3. The victims open accounts at exchanges and purchase cryptoassets.
4. The victims transfer cryptoassets to a wallet belonging to the fraudsters.
5. The fraudsters move the cryptoassets between multiple wallets.
6. The fraudsters use the stolen cryptoassets to cash out at exchanges, purchase property and luxury items, or use other available methods to launder their proceeds.



### Thailand Dragon Coin Scam

A case in Thailand involved a token scam that was used to launder Bitcoin worth nearly \$35 million.<sup>38</sup>

Fraudsters claiming to represent founders of the Dragon Coin ICO – an actual ICO launched in Macau to fund casino operations – contacted potential investors, including a wealthy individual in Finland, and asked them to provide Bitcoin to fund the project. The wealthy Finnish investor – believing the fraudsters were genuinely connected to the Dragon Coin ICO – sent Bitcoin worth \$35 million to the fraudster’s Bitcoin addresses.

The fraudsters then laundered the Bitcoin in part by using it to purchase property in Thailand. The remaining funds were transferred among multiple Bitcoin addresses and eventually cashed out for fiat currency at an unnamed exchange. The criminals then moved the remaining fiat into 51 bank accounts across Thailand. Some of the accounts belonged to family members of the suspected fraudsters.<sup>39</sup>



## Tokens and Stablecoins Involved in Fraud and Hacking

Several hacking incidents have involved the theft of tokens and stablecoins from cryptoasset exchanges.

The largest hack of tokens to date involved the theft of over \$400 million NEM tokens from the Japanese exchange Coincheck.<sup>40</sup> Hackers stole the funds from Coincheck's hot (or online) wallet, but the team behind NEM tokens resisted calls to recover the funds – ultimately leaving Coincheck on the hook to refund customer losses.

The September 2020 KuCoin hack (see Chapter 3 for a detailed description) also involved stolen tokens and stablecoins, but the token issuers opted for a different approach. After hackers stole more than \$150 million worth of tokens and stablecoins, token issuers such as Ocean Protocol and Tether began to freeze balances or forcibly move funds, so that KuCoin could retrieve the stolen assets.

In April 2020, the token issuer Tether froze \$300,000 of its eponymous asset in response to a case of fraud. This case involved an individual who had purchased Tether from a cryptoasset exchange and had some of the funds stolen by a hacker after moving it to his personal wallet. On learning that the funds had been reported stolen, Tether froze them and assisted law enforcement with their investigation into the alleged fraud.<sup>41</sup>



## Red Flags

Red flag indicators associated with token scams include:

- new customers to an exchange demonstrate little or no understanding of cryptoassets and indicate they are responding to an ad for a token;
- defrauded customers of an exchange may attempt to purchase relatively significant amounts of cryptoassets as a one-off, despite their limited understanding of the technology; and
- the ostensible token may feature on websites or social media – promising huge returns and promises that investors will get rich quickly.

## 4.3. Laundering of Hacked Tokens and Stablecoins

### The Problem

As tokens and stablecoins become more widely available for trading, they are increasingly attractive to cybercriminals. Hackers can steal tokens and stablecoins from exchanges, and then launder the funds by trading them for other cryptoassets on both centralized exchanges and DEXs.

### The Typology

1. Hackers steal a large quantity of tokens and/or stablecoins from a cryptoasset exchange.
2. The hackers move the funds to their own wallets.
3. The funds are then transferred to centralized exchanges and, or DEXs, where they are converted into other cryptoassets.
4. The new “clean” cryptoassets are sent onward for further laundering, typically with the aim of cashing out into fiat currencies.

### Red Flags

Red-flag indicators associated with the laundering of stolen tokens and stablecoins may include the following:

- a customer is in possession of a large volume of tokens and stablecoins with an obscure explanation for how they were obtained;
- blockchain analytics indicates that a customer is in possession of tokens and stablecoins that have been exposed to a known exchange hack; and
- a customer suddenly begins sending or receiving tokens and stablecoins to or from DEXs frequently, with no real explanation.



## Preventing Abuse of Tokens and Stablecoins

Controls that can be used to mitigate the risk of money laundering using tokens and stablecoins include:

- blockchain analytics solutions: Elliptic Lens and Elliptic Navigator, that ensure adequate coverage of different stablecoins and tokens;
- setting transaction monitoring risk rules to detect token and stablecoin transactions from DEXs; and
- seeking additional evidence on the source or destination of funds from customers whose account activity involves frequent use of many tokens and stablecoins.



### Ponzi Schemes

Ponzi schemes have long preyed on the cryptoasset space, with fraudsters exploiting the public's lack of knowledge and victims' desire to get rich quickly.

Some Ponzi schemes may be relatively sophisticated and large in scale. The OneCoin scam resulted in fraudsters robbing victims around the world of funds totaling several hundred million dollars.<sup>42</sup> Other Ponzi schemes are more unsophisticated frauds peddled through social media sites such as Twitter and Facebook.

Many cryptoasset businesses – especially exchanges – have been exposed to Ponzi schemes and have encountered victims of these frauds. An exchange may find that many customers sign up for accounts within a short period of time.

When the exchange asks the customers the reason for establishing accounts, many of them could be victims who have been told to open accounts at the exchange by scammers in order to transfer cryptoassets to the Ponzi scheme perpetrators. Digital assets from these customers may funnel to the wallet of a perpetrator – either at the same exchange or elsewhere.

Alternatively, victims may contact an exchange stating that an account was opened on their behalf by the founders of an investment scheme, and they will receive a cryptoasset-payout. No account exists, and the exchange must inform the victim they have been defrauded.

As noted earlier, non-compliant exchanges such as Payza have also assisted Ponzi scheme operators in laundering the proceeds of their crimes.

The following are steps that compliance officers take to mitigate the risks of exposure to Ponzi schemes:

- maintaining internal blacklists of known Ponzi schemes and alerting compliance staff to this information;
- searching customer details such as email addresses, to determine whether any contain the names of known Ponzi schemes, and exiting those customer relationships;
- monitoring vulnerable customers – individuals over 65 years old, or customers who may be financially distressed and can be easily targeted by Ponzi schemes.



## 5. Privacy Coins & Chain Hopping

Cryptoassets such as Monero, Dash, and Zcash are viewed by some cryptoasset enthusiasts as providing advantages over Bitcoin's relative lack of privacy.

Privacy coins<sup>43</sup> have featured recently in some significant cases of criminal activity. The now-defunct Alphabay dark web marketplace began allowing Monero payments in addition to Bitcoin. Elliptic's research highlights that most new dark web markets now accept Monero. Recent sanctions actions undertaken by OFAC in the US also highlight how cybercriminals are looking to privacy coins as part of their operations.

The use of privacy coins for laundering purposes is also heightened where the exchanges that criminals attempt to exploit are unlicensed and non-compliant. The FATF's report on cryptoasset red flags draws special attention to unlicensed and non-compliant exchanges that offer privacy coins as an area of specific and significant risk.

Not all privacy coins present the same risks. Those such as Monero remain imperious to AML solutions, while others such as Zcash are not. Since Zcash transactions do not provide default privacy like Monero does, users of Elliptic's blockchain analytics solutions can screen unshielded Zcash transactions for traces of illicit activity, just as they would with Bitcoin.

In addition to privacy coins, criminal actors may also attempt to move between cryptoassets such as Litecoin, Bitcoin Cash and others, as a way of hiding the flow of funds by switching between blockchains – a process known as “chain hopping”. This activity has been given a major boost in recent years through the proliferation of dedicated “coinswap” services, or P2P exchange platforms that require little or no KYC for crypto-to-crypto traders.

Below are examples of how privacy coins and chain hopping are used in the laundering process for criminal purposes.

### 5.1. Use of Privacy Coins to Layer Illicit Proceeds

#### The Problem

Owing to its relatively high liquidity, Bitcoin remains by far the favored choice for criminal actors using cryptoassets.

Bitcoin remains highly traceable. Criminals may seek to exploit privacy coins in the same manner that they take advantage of mixers by using privacy coins to break up the Bitcoin transaction trail.

Privacy coins provide a layering mechanism in the money laundering process – helping to hide the link between the illicit source and ultimate destination of funds.

## The Typology

1. Bitcoin is received into a wallet from an illicit source, such as ransomware.
2. The criminal engages in a pattern of “chain-peeling” (see section 10.1 above), moving the Bitcoin across numerous wallets.
3. After this process, the criminal then swaps the Bitcoin for Monero, Dash or other similar privacy coins at an exchange offering them.
4. The criminal deliberately uses non-compliant and unregulated exchanges as part of this conversion process.

### Red Flags

Red flags associated with criminals’ use of privacy coins to layer funds may include the following:

- Bitcoin known to be associated with a large-scale criminal event – such as a hack or ransomware – is cashed out at an exchange that provides access to privacy coins;
- Bitcoin associated with high-risk address clusters move through a complex process of chain-peeling before being cashed out at an exchange that provides privacy coins; and
- the exchange in question may be unregulated or non-compliant, or located in a high-risk jurisdiction (see sections 1.1 and 1.2 above for indicators of these types of exchanges).



#### WannaCry

In May 2017, hundreds of thousands of computers around the world were infected with the WannaCry ransomware virus, which demanded that victims pay small sums of Bitcoin to specified wallets belonging to the cybercriminals.

The attack was launched by members of the Lazarus group, the North Korean-sponsored cyber criminal outfit that the country had used in other cyber-attacks targeting banks around the world. Though in launching the WannaCry attack, the cyber criminals made a critical mistake. They only generated three Bitcoin addresses for the receipt of funds – allowing the world to watch as victims made ransom payments totaling approximately \$140,000 into the three wallets.<sup>44</sup>

The hackers began to move the Bitcoin from the three wallets – first transferring funds across multiple wallets. Once completed, they transferred a portion of the funds to the ShapeShift exchange, where they swapped the Bitcoin for Monero.

## 5.2. Laundering Illicit-origin Privacy Coins

### The Problem

Criminals may obtain privacy coins directly from illicit sources, as well as using them to obscure illicit Bitcoin or other transparent cryptoassets. For example, perpetrators of “crypto-jacking” campaigns have used victims’ hacked computers to mine Monero – providing criminals with newly minted Monero that appears clean.

In this context, privacy coins may present criminals with specific advantages over Bitcoin. This is because the flow of funds related to ransomware, hacking and other illicit activities are highly visible on the Bitcoin blockchain. Obtaining illicit-origin privacy coins allows the criminal a greater degree of anonymity during the early stages of the money laundering process.

Monero and other privacy coins generally lack sufficient liquidity to enable their ready conversion into fiat currency in significant values and volumes. Criminals often need to convert them into Bitcoin before cashing out. When criminals convert privacy coins into Bitcoin or other more transparent cryptoassets, they become vulnerable to identification, tracing and detection.

### The Typology

1. In a variation of the typology outlined in 10.1, a criminal comes into possession of Monero that is illicit in nature – it was mined through crypto-jacking, for instance.
2. The criminal approaches an exchange that accepts privacy coins and swaps the funds for Bitcoin. This may often occur through unlicensed and non-compliant exchanges.
3. The criminal can either immediately attempt to cash out, or transfer the Bitcoin on to other exchanges or wallets before eventually cashing out.

### Red Flags



Red flags associated with the use of privacy coins to layer funds may include the following:

- legitimate exchanges experience such activity where a customer transfers in a large volume of Bitcoin from an exchange that offers privacy coins;
- the customer engages in frequent transactions involving unregulated coinswap services; and
- a customer is unwilling or unable to provide information about the source of privacy coins they once held.



## Sanctioned Russian Cybercriminals Using Privacy Coins

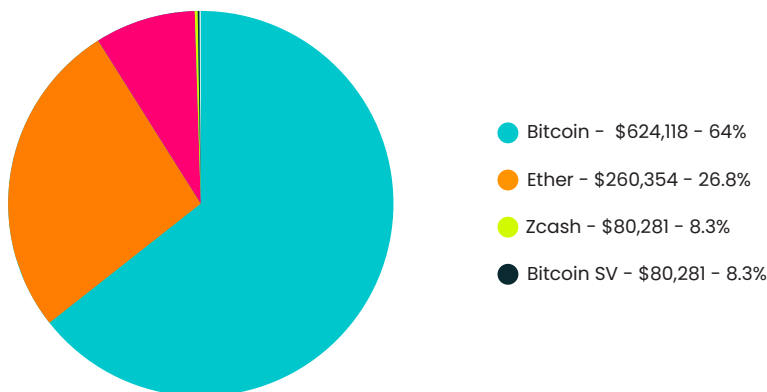
In two September 2020 sanctions actions, OFAC outed Russian cybercriminals and election hackers who rely on privacy coins.

According to OFAC, Danil Potekhin and Dimitri Karasadivi hacked cryptoasset exchanges and undertook complex money laundering operations to clean the funds. This included using numerous accounts at several cryptoasset exchanges to swap the funds for multiple cryptoassets – an example of chain-hopping in action. As part of its sanctions action against them, OFAC listed cryptoasset addresses belonging to the two criminals – including Monero, Dash and Zcash addresses belonging to Karasadivi.

KARASAVIDI, Dmitrii (Cyrillic: КАРАСАВИДИ, Дмитрий) (a.k.a. KARASAVIDI, Dmitriy), Moscow, Russia; DOB 09 Jul 1985; Email Address 2000@911.af; alt. Email Address dm.karasavi@yandex.ru; Gender Male; Digital Currency Address - XBT 1Q6saNmqKkyFB9mFR68Ck8F7Dp7dTopF2W; alt. Digital Currency Address - XBT 1DDA93oZPn7wte2eR1ABwcFoxUFxkKMwCf; Digital Currency Address - ETH 0xd882cfc20f52f2599d84b8e8d58c7fb62cfe344b; Digital Currency Address - XMR 5be5543ff73456ab9f2d207887e2af87322c651ea1a873c5b25b7ffae456c320; Digital Currency Address - LTC LNwgtMxcKUQ51dw7bQL1yPQjBVZh6QEqs; Digital Currency Address - ZEC t1g7wowvQ8gn2v8jrU1bijJ26sieNqNsBJy; Digital Currency Address - DASH XnPFsRWTaSgiVauosEwQ6dEitGYXgwznz2; Digital Currency Address - BTG GPwg61XoHqQPNmAucFACuQ5H9sGCDv9TpS; Digital Currency Address - ETC 0xd882cfc20f52f2599d84b8e8d58c7fb62cfe344b; Passport 75 5276391 (Russia) expires 29 Jun 2027 (individual) [CYBER2].

During the same month, OFAC sanctioned four Russian-linked individuals for interfering in the US election. According to the agency, Artem Lifshits, Anton Andreyev and Darla Aslanova supported the activity of a Russian agent – Andrii Derkach – by facilitating cryptoasset transactions that furthered Derkach’s attempts to subvert the 2020 US election online. OFAC listed Zcash and Dash addresses belonging to Lifshits and Andreyev – as well as Bitcoin, Litecoin and other cryptoasset addresses they controlled.

Elliptic’s analysis of their activity indicated that they had engaged in Zcash transactions totalling approximately \$80,000.



## Privacy Coins and Chain Hopping

Controls that can mitigate the risk of money laundering and terrorist financing via privacy coins and chain hopping include:

- solutions such as Elliptic Discovery to identify cryptoasset exchanges that offer privacy coin trading;
- blockchain analytics solutions: Elliptic Lens and Elliptic Navigator screen unshielded Zcash transactions, and identify shielded Zcash transactions; and
- setting transaction monitoring risk rules to ensure the detection of transactions involving coin-swap services involved in potential chain hopping.



### Coinswap Services Used For Chain Hopping With Privacy Coins

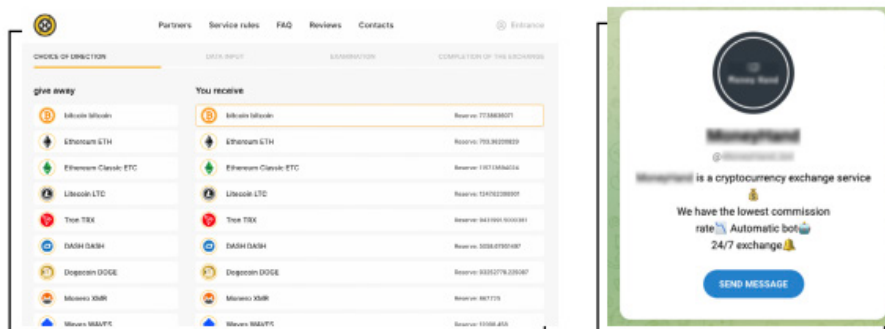
Coinswap services – specifically those based in post-Soviet states – are a preferred avenue of money laundering for cybercriminals and dark web vendors, allowing them to achieve a mixing effect. These crypto-to-crypto services do not require KYC information, and they often advertise this as a compelling feature to attract users, often advertising themselves exclusively to a cybercriminal audience.

These services allow users to swap crypto-for-crypto and enable trading in both transparent cryptoassets – as well as privacy coins. Users can often also trade cryptoassets for Perfect Money and other online digital payment mechanisms. Criminals can send illicit-origin digital assets to these services and readily obtain other “clean” cryptoassets, which they may send on to exchanges.

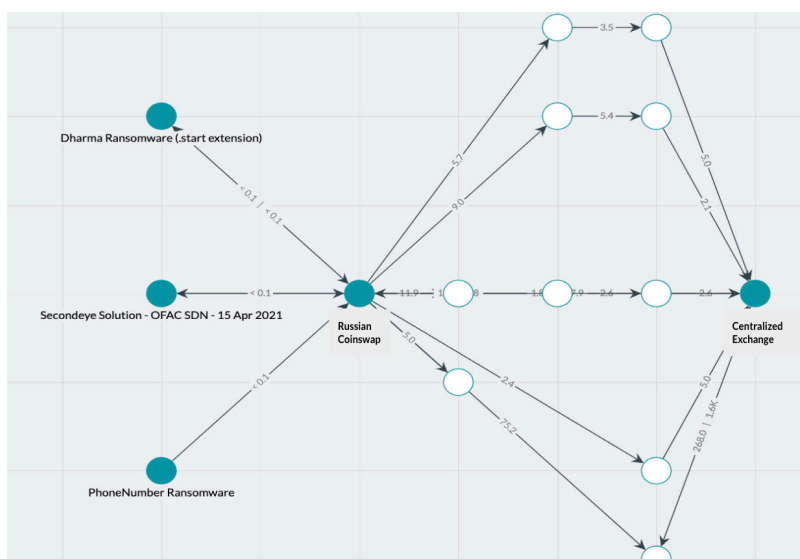
Besides being anonymous and offering anonymous swaps, coin swap services advertised on cybercrime forums have a number of other common characteristics:

- They are predominantly Russian speaking.
- Countries and currencies for which many of these services offer support include Russia, Ukraine and Kazakhstan. Besides rubles and hryvnia, many also provide euro and USD cash outs.
- Their crypto reserves are often lower than mainstream exchangers due to the specific nature of their clientele, meaning commission fees are typically high.

- They sometimes offer conversion services to Monero or other privacy coins.
- They often use a similar site template or operate on Telegram.



An example of a coin swap service as a website (left) and Telegram bot channel (right).



The image above from Elliptic Investigator demonstrates the inflow of illicit funds from ransomware campaigns and a US-sanctioned entity to a Russian coinswapping service, and outbound flows destined for a major cryptoasset exchange business.

## 6. Wallet-specific Behaviors

The transparency of the Bitcoin blockchain makes it possible to readily identify associated addresses linked to the same entity or individual. Elliptic's software makes it possible to identify these clusters of addresses and associated wallets. As a result, it offers an incredibly powerful tool for detecting and monitoring suspicious activity.

Criminals will still take specific steps to try and mask the connection between the Bitcoin addresses they are using – avoiding the clustering of addresses as a method for laundering.

In addition, groups of customers may engage in patterns of wallet activity that are highly unusual, like swapping Bitcoin among one another with a frequency that has no explainable legitimate purpose.

These behaviors are described below. While the examples given involve activity occurring in Bitcoin, similar techniques could in theory be employed by criminals seeking to hide activity in other cryptoassets.

### 6.1. Chain Peeling

#### The Problem

Criminals leave themselves vulnerable to detection where they rely on static addresses or repeatedly recycle the same few addresses.

“Chain-peeling” is one method criminals can use to reduce this vulnerability. It refers to the process of a user avoiding address re-use by repeatedly distributing unspent Bitcoin among brand new addresses in small amounts – thereby hiding the connection back to an original address that held illicit cryptoassets.

A peeling chain may involve an actor making up to dozens of hops between newly generated addresses, before attempting to cash out through exchanges and other conversion services.

Peeling chains tend to feature in very high value cases of illicit activity – such as hacks of major exchanges and large-scale ransomware campaigns. If conducted effectively, peeling chains can make it difficult for an exchange to readily identify that the cryptoassets it has received from multiple addresses are ultimately controlled by the same user.

Fortunately, Elliptic's solutions facilitate the detection of peeling chains, as described here.

## The Typology

1. An address is in receipt of a very large volume of criminal proceeds – for example Bitcoin resulting from the hack of an exchange.
2. The criminal sends a small portion of the stolen cryptoassets to an exchange address and then transfers the remaining unspent cryptoassets to a newly-generated address.
3. The criminal subsequently repeats this process, making dozens of individual transfers to the same exchange – or possibly multiple exchanges – and then transferring any unspent coins onward to several more newly-generated addresses.
4. If the criminal has conducted the chain peeling effectively, the exchange will only see that numerous individual small or moderate value cryptoassets deposits have been made, with a large number of new wallets involved in the transaction chain. The connection back to the original address that received the illicit funds remains hidden.

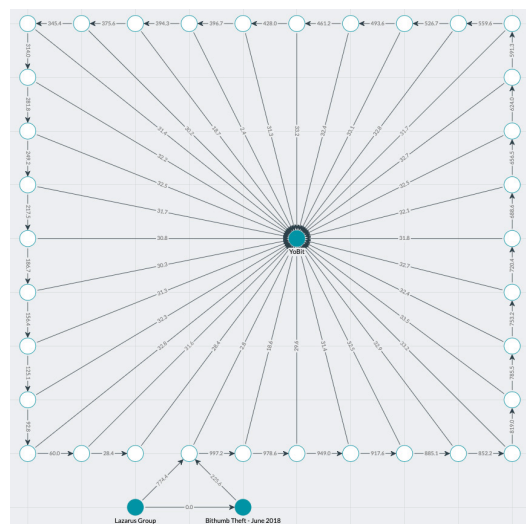




In June 2018, the South Korean cryptoasset exchange Bithumb was the target of a hack which resulted in the loss of cryptoassets worth over \$30 million. This included Bitcoin worth more than \$13 million.<sup>45</sup>

Elliptic's research reveals that after stealing the Bitcoin, the hackers – who some analysts suggest may be the North Korea-linked Lazarus Group – moved the funds into a Bitcoin wallet containing over 70 addresses. The funds remained in this wallet until early August 2018, when the hackers transferred the funds to the Russian-based cryptoasset exchange YoBit. The criminals employed a chain-peeling technique – engaging in a total of 68 transactions to deposit 1,993 BTC at YoBit.

The diagram below illustrates the process of a peeling chain as it transpired in the Bithumb hacking case, with the funds deposited in dozens of separate transactions at YoBit.



## Red Flags

Red-flag indicators associated with the use of chain peeling may include the following:

- a single customer receives cryptoassets at an exchange, with blockchain data indicating a large number of hops – for example, 20 or greater – through multiple new wallets within a very short period – several hours, for instance;
- in some cases, the cryptoassets associated with the new addresses may be deposited into numerous mule accounts;

- each individual transaction associated with the new wallets will tend to occur in a very short period of time, with all transactions part of the same block or separated by only one or two blocks; and
- the activity in question may be identified very shortly after a known exchange hack or other major criminal event has occurred involving large amounts of cryptoassets.

## 6.2. Multi-customer Cross-wallet Activity

### The Problem

Numerous individuals who are part of a criminal network may work in a coordinated fashion to use hosted or custodial wallets from the same exchange or wallet provider. They transfer illicit funds between one another's wallets frequently. Exchanges only record these internal transfers on their books – resulting in no transactional information appearing on the Bitcoin blockchain.

Sometimes, this activity may resemble legitimate behavior – for instance, members of a family in different countries who all have accounts at an exchange may transfer remittances to one another – but when associated with other red flags, this cross-account activity among countless users can be a sign of suspicious behavior.

### The Typology

1. Multiple customers who signed up within a short period of one another begin sending cryptoassets between their accounts in high volumes and at high velocity. For instance, several individuals may move funds between one another's accounts several times a day, every day, and within very short time periods.
2. Some or all of the colluded users' wallets may ultimately link to high-risk clusters – such as dark web markets, offshore gambling sites or similar.
3. Alternatively, some of the linked users attempt to cash out rapidly via exchanges, cryptoasset ATMs or other conversion services immediately after engaging in unusual cross-wallet activity.

### Red Flags

Red flags that may accompany multi-customer cross-account activity include the following:

- multiple customers – sometimes in large numbers in excess of 15 or 20 customers – with shared addresses, mobile devices or other common indicators create accounts at the same time. They begin sending funds on a continuous basis – daily, for example – with volumes or values that don't appear to have any legitimate purpose;

- a customer in one jurisdiction – Europe, for instance – transfers funds from his or her wallet to that of another customer in a different jurisdiction such as South America. The funds are immediately cashed out at an exchange or ATM in short succession, with a velocity that appears unusual;
- the individuals in question may have different surnames or nationalities so are unlikely to be family members; and
- the relevant customers are unable or unwilling to provide information about their source of funds and the purpose of their repeated transfers.

## 7. Cryptoasset ATMs

Cryptoasset ATMs have played an important role in the digital asset ecosystem. They provide a reliable method for rapidly transferring digital assets into fiat – or vice versa. Crypto ATMs offer a useful avenue for moving cash from one counterpart to a wallet, to another person located elsewhere. Proponents view them as playing a critical role in furthering financial inclusion and broader cryptoasset adoption.

There are more than 33,000 cryptoasset ATMs located around the world<sup>46</sup>, most of these in the US, and many provide access to a growing range of cryptoassets: Ether, Litecoin, Dash, Zcash, Monero and others.

Major crypto kiosk operators such as Coinsource, CoinFlip and Digital Mint are regulated in the US and have demonstrated a commitment to compliance and work to apply AML/CFT controls, such as blockchain analytics. Unfortunately, certain other crypto ATM providers have deliberately avoided compliance with regulation, and in some cases, these noncompliant services may be aware of or even complicit in illicit activity of their users.

The availability of these non-compliant kiosk services where users can swap cash for crypto with no AML/CFT controls has resulted in organized criminal networks abusing these services for purposes such as drug trafficking. It has also resulted in these kiosks featuring increasingly in crimes such as pig butchering – a variety of investment fraud in which victims are fooled into transferring their funds to perpetrators and sometimes lose thousands or even millions of dollars in the process.

### 7.1. Facilitation of Illicit Transfers<sup>47</sup>

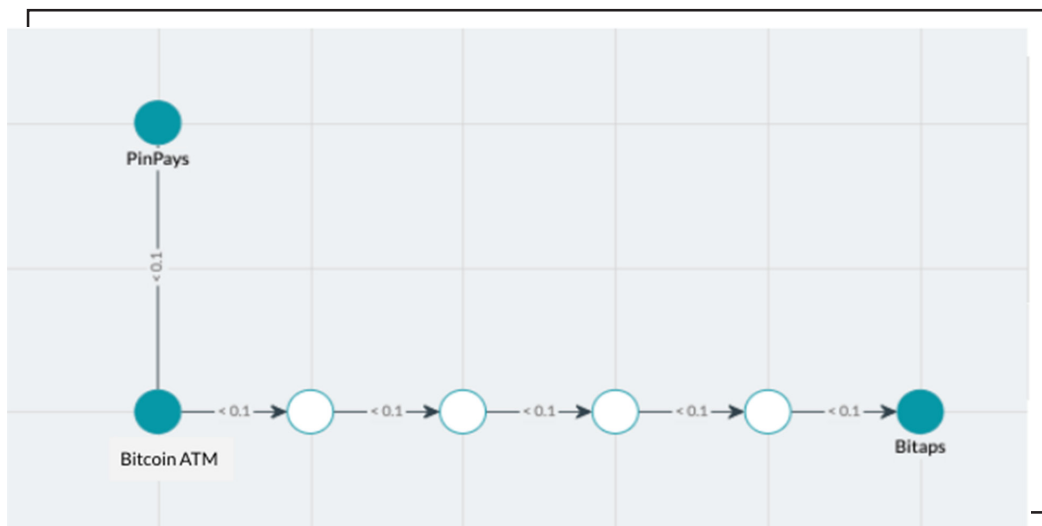
#### The Problem

Criminals seek to take advantage of how easy it is to use cryptoasset ATMs. They particularly explore how to convert dirty fiat into cryptoassets – or vice versa – and move their illicit proceeds to other members of a criminal network.

Criminals can do this domestically or internationally, which allows them to bypass contact with the formal financial system during various certain stages of the money laundering process. Cryptoasset ATMs are then used to convert illicit fiat into digital assets for onward laundering as described in the examples below, or to convert illicit cryptoassets – for example from ransomware or the dark web – into cash.

## The Typology

1. Members of a criminal network deposit large volumes of illegally-obtained cash from drug sales into cryptoasset ATMs.
2. The fiat funds are converted into cryptoassets and transferred to wallets belonging to other members in the same criminal network.
3. Members of the network on the receiving end of the transfers cash out the funds at an exchange, or withdraw the funds in cash at other cryptoasset ATMs.
4. The fiat funds are further laundered onward through wire transfers or cash deposits at banks and other financial institutions.



*The above image from Elliptic Investigator shows funds being transferred from a Bitcoin ATM service to two dark web services used to buy and sell stolen credit card details: PinPays and Bitaps.*



## The Europe-Colombia Drug Connection

Europol has described how drug dealers across the continent have exploited the unregulated status of cryptoasset ATMs in the EU to funnel criminal proceeds to narco-traffickers in Colombia.<sup>48</sup>

Drug dealers on the streets of Europe take their cash euro proceeds to cryptoasset ATMs that are often located at cafes and stores potentially owned by criminals. Alternatively, the criminals may seek to exploit cryptoasset ATMs they know to have lax or no KYC measures.<sup>49</sup>

The dealers deposit the funds in round-value increments such as 1,000 euros (\$1,075) – usually operating below the ATM's maximum deposit value – and often using large denomination notes. The dealers will use many ATMs in several locations. According to Europol, one identified criminal network deposited as much as 200,000 euros (\$215,000) per month into a single cryptoasset ATM.

Once deposited in the cryptoasset ATMs, the funds are sent to the Bitcoin wallets of money launderers in Europe. These individuals then transfer the funds to launderers' wallets in Colombia.

The Colombian launderers will immediately exchange the funds to pesos at a domestic cryptoasset exchange. The funds are further laundered through a complex layer of accounts at banks and MSBs across Colombia, and onward to accounts belonging to the drug cartel.<sup>50</sup>

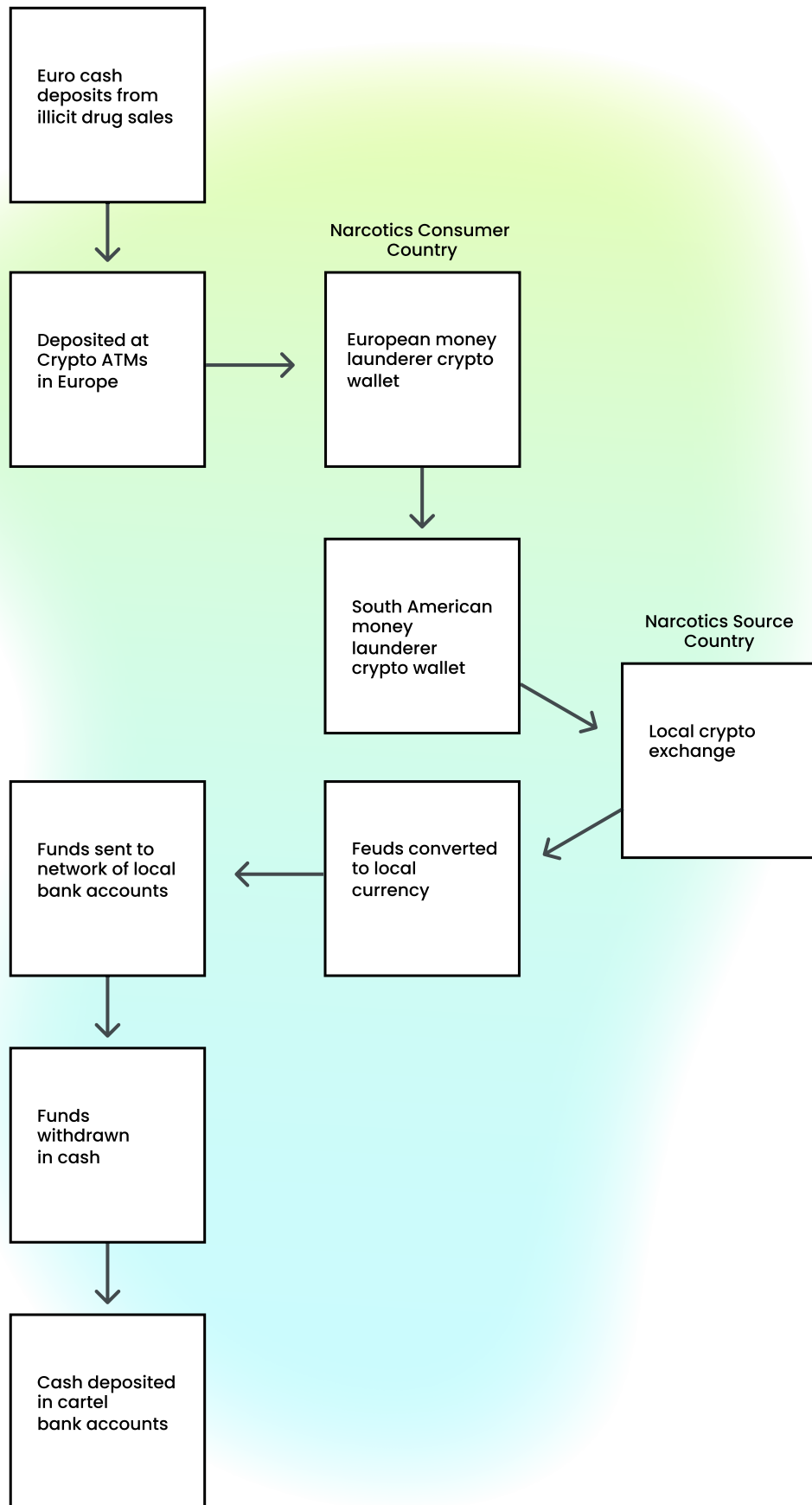


## Criminals Owning and Operating ATMs

Some criminals have obtained their own cryptoasset ATMs to carry out crimes.

In May 2019, Europe announced the arrest of a Spanish criminal organization engaged in money laundering as a service.<sup>51</sup> The criminals took cash proceeds from drug dealers and converted it into cryptoassets for onward laundering. The launderers owned and operated two Bitcoin ATMs. By feeding cash into the machines, they could convert them directly into Bitcoin. The new "clean" cryptoassets were then transferred to wallets controlled by the drug dealers.

The diagram below offers a simple illustration of how criminals may attempt to launder funds through cryptoasset ATMs.



## Red Flags

Red-flag indicators associated with laundering illicit proceeds via cryptoasset ATMs include:

- large denomination notes – such as 50, 100 or 500 euros – used to make frequent and ongoing fiat deposits into Bitcoin ATMs by the same users, possibly re-using only a small number of cryptoasset wallets;
- the cryptoasset ATMs used by the criminals are located in regions or neighborhoods associated with high concentrations of criminal and gang activity;
- funds are sent to or collected from cryptoasset ATMs in jurisdictions with little or no regulation around cryptoassets, and, or involving cryptoasset ATM providers that do not require KYC/CDD information;
- the cryptoasset ATMs are located at physical addresses associated with what appear to be front businesses, and which may themselves be owned by criminals complicit in the illegal activity;
- in some cases, a single front business may operate numerous Bitcoin ATMs, all of which have turnover levels that are implausibly high. This could include, for example, a single ATM used to process as much as 200,000 euros (\$215,000) per month in areas or regions that are not known to have exceptionally high cryptoasset adoption.





### Unlicensed and Unregistered Crypto Kiosks

Transactions involving unlicensed and unregistered Bitcoin ATM services are especially high risk. Because these services do not comply with AML/CFT requirements, they are especially vulnerable to illicit activity, and they may even be complicit in it.

Regulatory and law enforcement agencies have been warning increasingly about the risks from these unlicensed kiosk operators, and have been taking actions to shut them down. In early 2023, the UK's Financial Conduct Authority (FCA) indicated that it was investigating sites in London and Leeds suspected of hosting unregistered crypto ATMs.

In March 2023, the US Secret Service collaborated with law enforcement in Ohio to arrest the founders of Bitcoin of America, an operator of more than 2,000 kiosks across the US that authorities alleged knowingly facilitated crimes such as romance and investment scams. The law enforcement action resulted in the seizure of 52 kiosks operated by Bitcoin of America.<sup>52</sup>

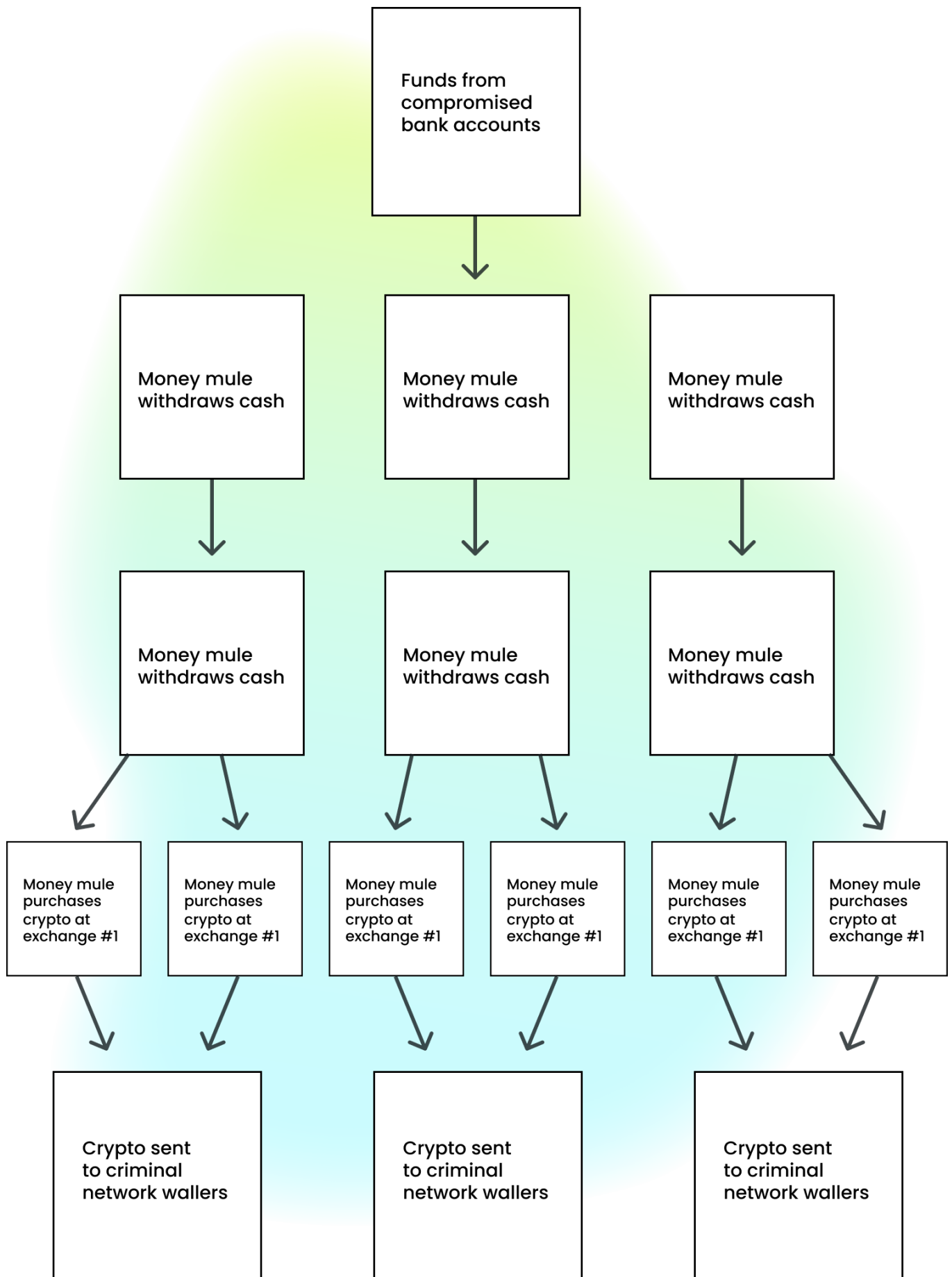
## 7.2. Money Mule Activity

### The Problem

Along with targeting standard cryptoasset exchanges, criminals may also rely on mules to funnel illicit funds through cryptoasset ATM networks. The use of widespread and complex money mule networks can create added challenges of detection and prevention for cryptoasset ATM operators – especially where false or stolen identifying information is used. Europol has observed the growing use of money mules at cryptoasset ATMs across Europe, as described below and illustrated in the accompanying diagram.

### The Typology<sup>53</sup>

1. Criminals come into possession of illicitly obtained fiat currency – for instance, through online bank accounts that have been compromised.
2. Money mules receive illicit funds into bank accounts belonging to them.
3. The mules withdraw the funds in person at bank branches, or at fiat ATMs.
4. The mules deposit the cash funds into cryptoasset ATMs.
5. The funds are transferred to wallets belonging to members of the criminal network, who launder the funds onward.



## Red Flags

Red-flag indicators associated with mule activity involving cryptoasset ATMs may include:

- a single individual making multiple fiat deposits at a cryptoasset ATM each day up to the standard deposit limit – under \$3,000, for instance – or at frequent intervals for amounts consistent with “smurfing” activity;
- a single individual accesses multiple cryptoasset ATMs in different locations over a short period of time for unexplained reasons;
- accounts are opened by university students or other young individuals. When questioned, some may imply that they were targeted by job adverts via Twitter or other social media platforms offering a fee for transferring Bitcoin via ATMs. The related job adverts may pose under the guise of IT consulting firms or similar businesses;<sup>54</sup>
- false identity documents used to undertake transactions and pass KYC where it is required – including use of earlier described KYC kits;
- numerous individuals with common addresses, mobile devices, nationalities or other identity indicators sign up for accounts in a short time period for ambiguous reasons;
- high-value funds are sent from multiple cryptoasset addresses via ATMs to a single recipient wallet address over a short period; and
- inconsistent or improbable reasons customers provide – for instance, to buy furniture or other ordinary items – for the large value transfers given the sums involved.

### 7.3. **Victims of Scams Send Funds** via Cryptoasset ATMs

#### The Problem

Public reporting points out a growing number of scams involving cryptoasset ATMs. Victims are duped into depositing fiat funds into cryptoasset ATMs for onward transfer to cryptoasset wallets belonging to criminals. These individuals then launder the funds forward via exchanges or other conversion services.

## The Typology

1. The victim is contacted by scammers – mostly by email or phone – and instructed to make payments for a genuine service that requires funds to be transferred via cryptoasset ATMs.
2. Common guises for the fraud may include tax scams, romance or employment scams – see case study below.
3. Scammers give the victim essential information to use the cryptoasset ATMs, such as QR codes and instructions for sending the funds to the appropriate cryptoasset wallet which they control.
4. The victim withdraws funds from his or her fiat bank account, and deposits the funds in a cryptoasset ATM.
5. The scammers receive cryptoassets in their wallets and can transfer the funds onward to cryptoasset exchanges or P2P exchanges.



### Tax and Utilities Collection Scams Use Cryptoasset ATMs

Recent cases have implied that fraudsters posing as employees of public sector agencies have conned victims into parting with their funds via Bitcoin ATMs.

One scam reported in Canada, the US and Australia<sup>55</sup> involved a tax collection scam. Around tax filing day, victims are contacted by fraudsters claiming to represent the official tax revenue office. The victims are told that they owe additional taxes and must make payment by depositing cash at a Bitcoin ATM.

The fraudsters are often aggressive and threaten the victims with a penalty from the tax authorities for non-payment. The victim will be instructed to make multiple payments in values just under the ATM's maximum deposit thresholds, then transfer the funds to Bitcoin addresses controlled by the fraudsters.

A similar scam was reported in Hawaii in 2018.<sup>56</sup> Fraudsters posing as employees of local energy utility providers called victims and told them to pay outstanding bills or risk having their electricity cut off. The victims were instructed to deposit cash at Bitcoin ATMs and to transfer the funds to the fraudsters' Bitcoin wallets.

## Red Flags

Some red-flag indicators associated with cryptoasset ATM scams include:

- victims may be elderly individuals who do not understand cryptoassets and may appear confused when questioned about their activity;
- victims may sound panicked and frightened if contacted by the cryptoasset ATM operator – especially if threatened by fraudsters. The financially vulnerable may have been targeted as part of an apparent employment or work-from-home scam; and
- victims may have been instructed to make multiple cash deposits at the cryptoasset ATM just under the single maximum deposit threshold.

## Preventing Abuse of Cryptoasset ATMs

Controls used by compliance officers to prevent money launderers from abusing cryptoasset ATMs include:

- a requirement that customers provide KYC information and documentation before undertaking their first transaction;
- setting strict limits on maximum single transaction thresholds, as well as limits on the maximum number and value of transactions permitted daily;
- questioning customers who make multiple daily ATM transactions or who frequently access ATMs in different locations;
- monitoring customers with shared addresses and other common indicators, who may be accessing the same ATM within a very short period of time;
- monitoring customers with shared phone numbers who attempt to access ATMs repeatedly using the same mobile device;
- making use of live camera footage to monitor unusual customer behavior when using an ATM.



## The Use of Bitcoin ATMs in Pig Butchering

On October 3rd 2022, the US Federal Bureau of Investigation (FBI) warned of the growing use of Bitcoin ATMs in pig butchering – a rapidly proliferating form of investment fraud.

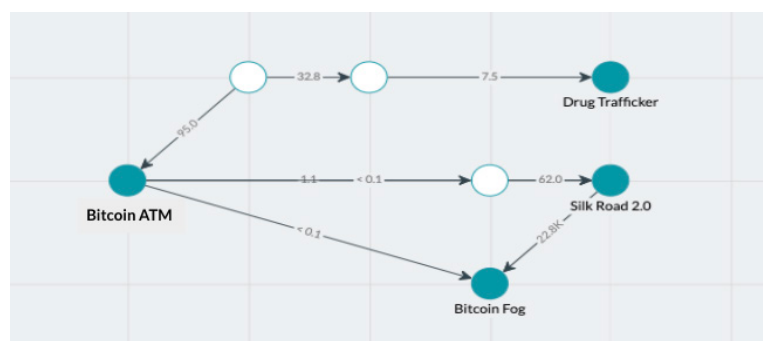
Pig butchering scams involve fraudsters luring their victims to financial ruin. In pig butchering frauds, criminals will often use romance scam techniques to establish a relationship with their victims, posing as a potential love interest who also happens to be a successful and wealthy crypto investor.

Having established a relationship with the victim, the fraudster encourages them to participate in crypto investing with the promise of potential riches. The criminals direct the victims to purchase crypto and deposit the funds through fake websites designed to look like legitimate crypto trading platforms and duping them into thinking they are earning large investment returns – though the funds are in fact sent to crypto wallets belonging to the fraudster.

Slowly, over the course of weeks or months, the fraudster will encourage the victim to part with more and more of their funds, in many cases draining them of their entire life savings and leaving them penniless.

Pig butchering scams have proliferated since 2021. While their exact value is very difficult to determine given the number of unreported cases, estimates suggest that total fraud losses from pig butchering range in the hundreds of millions to low billions of dollars.

According to the FBI's notice of October 2022: "The use of [...] cryptocurrency ATMs is also an emerging method of payment"<sup>57</sup> in these pig butchering scams. It is therefore important to be alert to red flags of crypto ATMs scams noted above as part of efforts to detect and disrupt pig butchering.



The above image from Elliptic Investigator shows transactions between a Bitcoin ATM service and illicit actors, including a drug trafficker, the Silk Road 2.0 dark web market, and the Bitcoin Fog Mixing Service.

## 8. Cards

Cryptoasset prepaid cards allow crypto users to purchase real-world goods and services seamlessly. This is a convenient, portable method for transferring and spending cryptoassets. Users can simply load their prepaid accounts with digital assets and then spend the funds at any retailer, rather than having to find vendors who accept cryptoassets.

Some law enforcement cases suggest criminals have taken advantage of the convenience of cryptoasset prepaid cards to move dirty funds quickly.

Similarly, criminals can use cryptoassets to purchase fiat prepaid cards or stolen card details, and then use those cards as a way of further laundering their illicit funds.

These typologies are described below.

### 8.1. Use of Cryptoasset Prepaid Cards to Layer Criminal Proceeds

#### The Problem

Cryptoasset prepaid cards can offer a useful “layering” vehicle for moving illicit proceeds – allowing criminals to do the following:

- deposit illicit cryptoassets – from ransomware or the dark web, for example – into their prepaid account for rapid conversion into fiat;
- swap illicit fiat – from a compromised online bank account or stolen card – for cryptoassets, which they can then transfer onward or spend on their prepaid card.

#### The Typology

1. A ransomware perpetrator or other criminal receives a large amount of cryptoassets from victims.
2. The perpetrator transfers the funds to wallets at exchanges and custodial wallet services offering a prepaid card.
3. The criminal may employ mules to open numerous accounts connected to many prepaid cards.
4. The cryptoassets are then transferred onward to other wallets or spent using the prepaid cards. The funds can purchase high-value luxury goods and services. Funds can also be withdrawn via ATMs so that the criminals have access to untraceable cash.



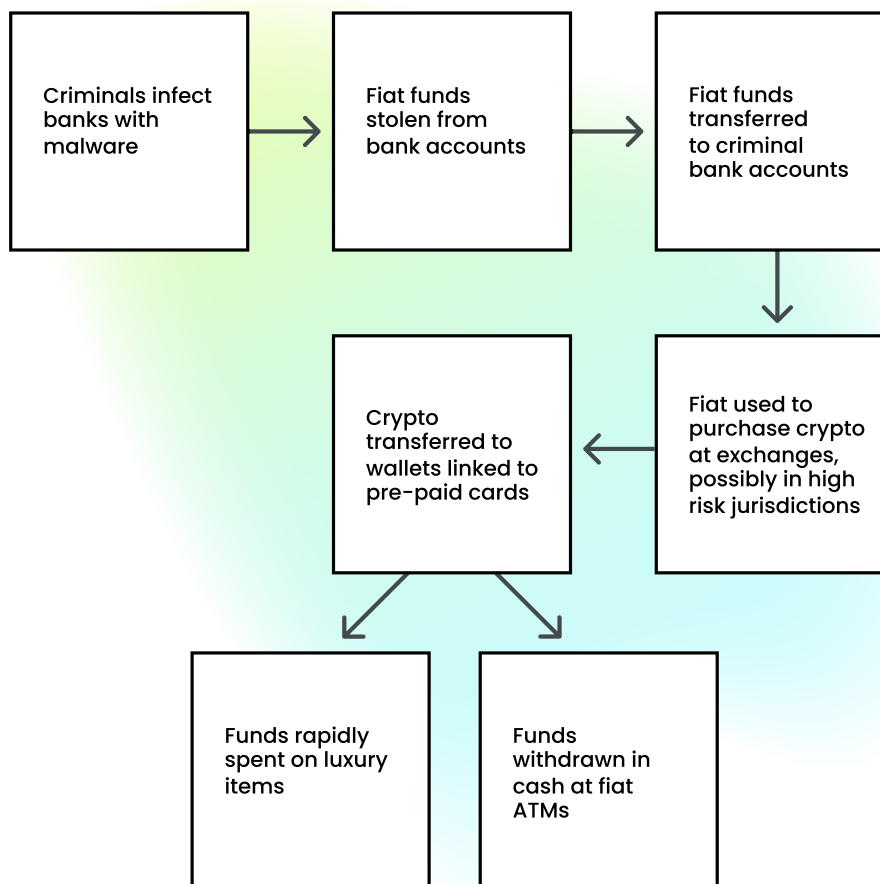
## The Carbanak and Cobalt Cyber Crime Syndicate

In March 2018, Europol arrested the head of the cybercrime group that developed the Carbanak and Cobalt malware strains used to attack dozens of global banks. This criminal organization laundered up to \$1 billion and relied heavily on cryptoassets.

The malware strains they deployed allowed them to compromise bank accounts and transfer funds to their own overseas banks accounts. The malware also allowed the thieves to compromise bank ATMs and empty them of cash.

The criminal network moved these stolen funds through numerous fiat bank accounts using money mules in countries such as Taiwan, Spain and Belarus.<sup>58</sup> They eventually converted the funds into cryptoassets through exchanges and wallet service providers offering prepaid card services. According to Europol, the prepaid cards were used to buy luxury items such as houses and cars.<sup>59</sup>

The following diagram provides a simple illustration of how schemes like the Carbanak/Cobalt case work:





## Red Flags

Red-flag indicators associated with the illicit use of cryptoasset prepaid cards include:

- moving funds directly from an illicit source – ransomware, dark web drug proceeds – to a cryptoasset prepaid card provider to use for rapid conversion into fiat, or to purchase physical goods and services;
- using large incoming transfers from bank accounts to top-up cryptoasset prepaid balances rapidly and spending on high value items at merchants associated with luxury goods;
- the cards may feature sudden spurts of high volume and high-value spending at a single merchant for no obvious purpose;
- mules who in some cases can be used to open numerous accounts and obtain prepaid cards using genuine or fake IDs, common addresses, mobile devices or IP addresses;
- criminals who may open accounts at prepaid card providers that are unregulated, non-compliant or with weak KYC or CDD measures in place;
- fiat funds transferred to cryptoasset prepaid card providers arrive from bank accounts in high-risk countries, such as Ukraine, Belarus and Russia;
- criminals setting up numerous accounts at a single prepaid provider and attempting to use multiple cards just below the authorized transaction limits to avoid detection on each account;
- the criminal attempting to top-up stolen fiat debit or credit cards where the prepaid card allows a “top-up” with debit or credit cards, which they then convert into cryptoassets for further onward laundering;
- large volumes of inbound fiat wire transfers may be associated with social engineering frauds that exploit Facebook or other social media platforms to obtain funds from victims and then convert them to cryptoassets for more laundering;
- criminals may attempt to make purchases on online platforms that convert cryptoassets directly into holdings in commodities such as gold and other precious metals;<sup>60</sup> and/or
- criminals targeting providers of prepaid cards that are unlicensed or non-compliant.



### The Use of Luxury Goods to Conceal Illicit Proceeds

As demonstrated in the Carbanak and Cobalt case, criminals can abuse cryptoassets by purchasing high-value goods where large amounts of illicit funds can be concealed.

A growing range of luxury goods and services are available to cryptoasset holders to purchase – including houses and other property, vehicles, artwork, watches and jewelry.

Customers making high-value cryptoasset transfers to dealers in expensive goods, and specifically to certain services such as estate agents, auto-dealers, jewelers and auction houses may warrant enhanced scrutiny, particularly where these activities involve higher-risk jurisdictions.

In the US, a 19-year-old hacker hijacked phone numbers of cryptoasset users and managed to steal Bitcoin worth approximately \$1 million from victims at US exchanges. He used the Bitcoin in part to purchase a McLaren sports car, which can be worth hundreds of thousands of dollars.<sup>61</sup>

## 8.2. Dirty Cryptoassets Used to Purchase Fiat Cards For Laundering

### The Problem

Stolen card details are widely available on the dark web – including on Tor-based sites that act as underground emporiums for carders. Criminals can purchase stolen card information – alongside accompanying KYC kits – to help mask the proceeds of illicit funds.

Furthermore, criminals may attempt to use cryptoassets to purchase fiat prepaid or gift cards from legitimate vendors that accept digital assets for cards.

Whether the fiat-denominated cards are stolen or legitimate, the intention is the same – to enable the criminal to break the transaction chain between their illicit-origin cryptoassets and spending they undertake in fiat currency.

## The Typology

1. A criminal has illicit cryptoassets – for instance, derived from ransomware – and purchases stolen card details from a Tor-based vendor of compromised cards.
2. The criminal purchases KYC kits along with the compromised cards, and this gives them access to the victim’s identifying information and supporting ID documents.
3. The criminal uses the compromised cards to spend at a variety of vendors – allowing them to have newly acquired “clean” goods.
4. The criminal may try to set up accounts at banks using the KYC kits, making purchases and ATM withdrawals so that their once dirty cryptoassets now appear as “clean” goods or cash.

### Red Flags

Red-flag indicators associated with cryptoasset laundering using fiat cards – both legitimate or stolen cards – may include the following:

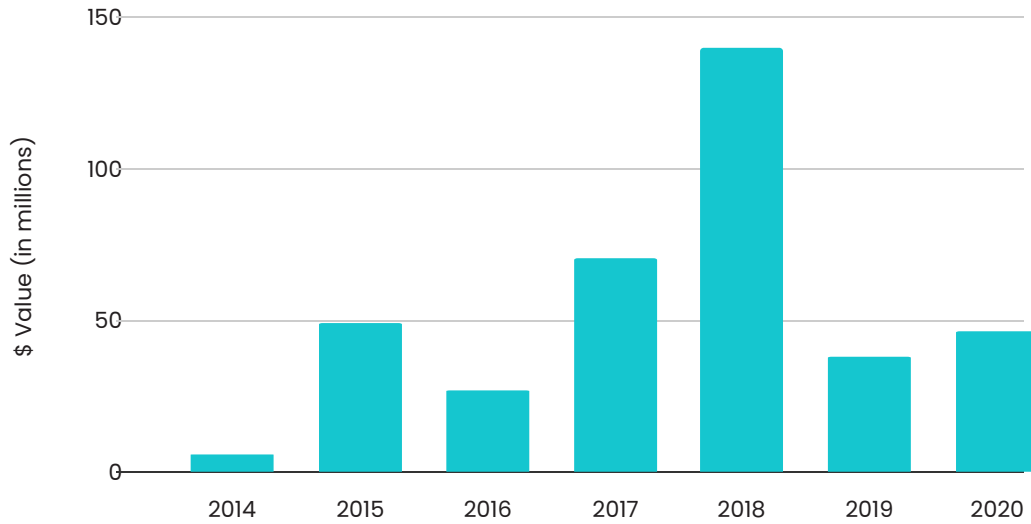
- a customer purchases a large amount of cryptoassets and makes an immediate onward transfer to a dark web carding site;
- a customer purchases a large amount of cryptoassets and immediately uses the funds to make frequent or high-value purchases at mainstream vendors that offer the purchase of fiat-denominated prepaid and, or gift cards with cryptoassets.



#### Joker’s Stash: the Largest Carding Market Retires

For several years, the most popular website for criminals to buy stolen credit and debit card details using cryptoassets was Joker’s Stash. Established in 2014, Joker’s Stash was a massive online carding emporium, where criminals could buy stolen card details for \$1 to \$150 per card using Bitcoin. While these amounts may seem small, the total trade in stolen cards that took place on Joker’s Stash was staggering: Elliptic’s research indicates that it received more than \$400 million in Bitcoin payments between 2014 and 2020, as indicated in the chart on the next page.

## Value of Bitcoin payments received By Joker's Stash, By year



In February 2021, the operators of Joker's Stash announced their retirement and closed the site. Their illicit business earned them huge profits; the Bitcoin they acquired would have had a value of approximately \$2.5 billion by early 2021.<sup>62</sup> While Joker's Stash is no longer in existence, the significant revenues it generated demonstrate that there is widespread demand among for stolen credit card details, and that these transactions are often facilitated by using cryptoassets.

ID	BIN	Bank	Level	Credit?	Country	State	City	ZIP	DOB?	SSN?	E-mail?	Phone	Address	F. Name	Exp.?	Price	
3004	459981 [-]	Banco Cooperativo E...	Electron	Debit	ES		Cabrera	37180 [-]						Gen...	Class	Yes	\$25.00
3004	468879 [-]	Bendito Bank FC	Classic	Debit	GB		Arenley Road						Red St	Primo	Yes	\$25.00	
3004	413388 [-]	Eto Blanco, S.A.	Electron	Debit	ES		Las Palmas	35007 [-]					9558	Gen...	Master	Yes	\$25.00
3004	316675 [-]	Az Mexico Giobetter	Gift	Credit	MX		Puebla	32000 [-]						Gen...	Master	Yes	\$25.00
3004	525678 [-]	Banco Nacional de...	Standard	Debit	MX		Itzamal, Yucatan	34000 [-]						Gen...	Master	Yes	\$25.00
3004	403948 [-]	La Banque Postale	Classic	Debit	FR		Ikos Colombee	93070 [-]						Gen...	Master	Yes	\$25.00
3004	527533 [-]	Erste Bank A.d. Pbd...	Standard	Debit	SE		Indragiri	81000 [-]					8028	Gen...	Master	Yes	\$25.00
3004	52729 [-]	Commonwealth Ban...	Standard	Debit	AU		Calder	30070 [-]					61 00	Gen...	Master	Yes	\$25.00
3004	462765 [-]	Erste Bank Slovake...	Electron	Debit	SK		Serebtor	30000 [-]						Gen...	Master	Yes	\$25.00
3004	466254 [-]	Hong Leong Bank B...	Classic	Debit	MY		Klang	41000 [-]					7430	Gen...	Master	Yes	\$25.00
3004	438312 [-]	Malayan Banking B...	Classic	Debit	MY		Arang						6196	Gen...	Master	Yes	\$25.00
3004	483561 [-]		Classic	Debit	NZ		Nelson	41000 [-]					540 A	Gen...	Master	Yes	\$25.00
3004	454313 [-]	Nationwide Building	Classic	Debit	GB		Sunderland	NE5 1YU [-]					8152	Gen...	Master	Yes	\$25.00
3004	525678 [-]	Banco Nacional de...	Standard	Debit	MX		Quilichavan	35000 [-]					4066	Gen...	Master	Yes	\$25.00
3004	517041 [-]	Turkiye Garanti Bank...	Standard	Debit	TR		Stambul	34000 [-]						Gen...	Master	Yes	\$25.00
3004	52729 [-]	Commonwealth Ban...	Standard	Debit	AU		Bogota	10000 [-]						Gen...	Master	Yes	\$25.00
3004	454075 [-]	Banco Frances, S.A.	Classic	Credit	AR		General Pueyrredon	81000 [-]						Gen...	Master	Yes	\$25.00
3004	453268 [-]	State Bank of India	Global	Debit	IN		Nagpur	44000 [-]					9028	Gen...	Master	Yes	\$25.00
3004	524182 [-]	SBI Cards & Paymen...	Titanium	Credit	IN		99, Nagar Chemical	40000 [-]					5241	Gen...	Master	Yes	\$25.00
3004	451564 [-]	Banco Mercantil del...	Electron	Debit	ES		Guadalupe	46070 [-]						Gen...	Master	Yes	\$25.00
3004	518815 [-]	Swedbank AB	Standard	Debit	SE		Huskvarna	30000 [-]						Gen...	Master	Yes	\$25.00
3004	548901 [-]	Banco Santander, S.A.	Standard	Debit	ES		Leon	24000 [-]						Gen...	Master	Yes	\$25.00

A screenshot from Joker's Stash, showing individual payment cards for sale together with details of the cardholder.

## 8.3. Fiat Cards Used to Purchase Cryptoassets For Illicit Purposes

### The Problem

The growing availability of both fiat prepaid cards and cryptoassets means criminals can readily leverage both technologies in their operations.

Criminals can obtain prepaid cards – or credit or debit cards – to buy cryptoassets at exchanges, with the aim of using the digital assets to purchase illicit goods and services. This can include the use of both new cards, as well as stolen card details.

### The Typology

1. Criminals obtain prepaid, credit or debit cards.
2. They use the new cards to purchase cryptoassets from exchanges or P2P platforms.
3. The cryptoassets may be used to purchase illicit goods and services.
4. Alternatively, the cryptoassets may be sent to other members of the criminal network, who use them for illicit purposes.

### Red Flags

Red-flag indicators associated with the use of fiat cards – both legitimate or stolen cards – to purchase cryptoassets for illicit purposes include the following:

- a customer makes numerous purchases of cryptoassets using prepaid cards with a frequency that can't be legitimately explained;
- the customer uses countless different cards to make purchases of cryptoassets;
- after purchasing digital assets using prepaid cards, the customer immediately transfers the cryptoassets to high-risk sites. These could be dark web markets or sites associated with prostitution or similar activities.



## Using Fiat Cards to Purchase Cryptoassets For Illicit Purposes

Law enforcement agencies in the US have identified instances of human traffickers and terrorist supporters using fiat cards to purchase cryptoassets for use in their crimes.

According to FinCEN, in one case, US law enforcement in Texas arrested William Harris and Dean Hall, who were involved in trafficking women into prostitution. In recovering firearms from the men, law enforcement learned that Harris had purchased prepaid Vanilla Visa credit cards. He used these cards to purchase Bitcoin on a popular P2P website, and then used the Bitcoin to purchase ads on the Backpage.com prostitution site.<sup>63</sup>

In another US case, a New York woman was sentenced to 13 years in prison for her part in a campaign to fund the terrorist organization ISIS. According to the Department of Justice, Zoobia Shanaz fraudulently obtained a \$22,500 loan. She also used over a dozen fraudulently-obtained debit and credit cards to purchase cryptoassets totaling \$62,500. Shanaz eventually transferred funds to ISIS front entities in Pakistan, China and Turkey.<sup>64</sup>



## Preventing Abuse of Cryptoasset Prepaid cards

Controls to mitigate or prevent the risk of money laundering using cryptoasset prepaid cards include:

- placing significant limits on both one-off and accumulated spending using the card;
- insisting on customers completing an enhanced due diligence process before raising their spending limits;
- observing spending at high-risk merchant types, such as estate agents, vehicle dealerships and jewelry shops to name a few;
- establishing transaction monitoring rules to check for large inbound top-ups followed by immediate outbound transfers, withdrawals or spending;
- developing lists of high-risk countries and tracking customer card spending in those jurisdictions;
- using address verification checks and card blacklisting to monitor for signs that a customer is topping up stolen debit or credit cards; and
- monitoring for proof – common email addresses, residential addresses, mobile devices and logins – that a single user or group of linked users are attempting to set up multiple accounts and obtain more than one debit card.

## 9. Banks and Indirect Exposure to Cryptoasset Risks

It is not only crypto-native businesses such as exchanges and ATMs that are impacted by the typologies and financial crime activities outlined in this report. Banks and other financial institutions are also significantly impacted by financial crime activity in cryptoassets.

A growing number of banks offer cryptoasset products and services – such as custody and exchange services – and these financial institutions will consequently face direct exposure to all of the typologies outlined in this report. However, even financial institutions that do not themselves offer cryptoasset products and services can be profoundly impacted by financial crime in cryptoassets where they have indirect exposure to digital asset activity.

In this section, we describe two primary ways in which banks may face indirect exposure to financial crime activity in cryptoassets.

### 9.1. Indirect Exposure Through Processing VASP Transactions

#### The Problem

Banks can be exposed to financial crime risks where they process fiat currency transactions on behalf of virtual asset service providers (VASPs) – such as exchanges, ATMs and other platforms. In some cases, banks may knowingly maintain relationships with VASPs and can therefore apply risk management controls to monitor those VASP accounts.

However, in many instances a bank may have exposure to VASPs that is less obvious. Indeed, a bank might process transactions for VASPs and their customers that on the surface do not appear to have any obvious connection to digital assets. Without sufficient controls in place to detect this type of activity, the bank could face significant exposure to cryptoasset-related risks.

#### The Typology

1. A money mule acting on behalf of a criminal organization receives multiple online transfers into their bank account in round value amounts like \$500 or \$750. These transfers represent the proceeds of online fraud or cybercrime activity.
2. The money mule immediately transfers the funds from their bank account to an entity called ABC Limited, which is a small cryptoasset exchange service located in a high-risk jurisdiction.

3. The funds are used to purchase Bitcoin or other cryptoassets at ABC Limited.
4. The money mule then sends the funds to crypto wallets controlled by the criminal organization, which then further launders the funds using techniques outlined in this report.

## Red Flags

Red-flag indicators associated with banks' indirect exposure via transactions involving VASPs include:

- a customer repeatedly sends funds to a VASP from their bank account immediately after receiving inbound transfers whose purpose is unclear or can't be explained;
- a customer repeatedly transacts with a VASP in a high-risk jurisdiction;
- a customer repeatedly transacts with a VASP that offers trading in privacy coins;
- a customer repeatedly transacts with a VASP that does not require KYC information of users; and
- a customer's transactions that include the above characteristics also include frequent payment references to cryptoasset-related terminology – such as "Bitcoin" or "crypto".



### North Korean Money Launderers

In March 2020, OFAC sanctioned two individuals connected to North Korea's cybercrime operations. Their activity demonstrates the scale and complexity of emerging sanctions evasion techniques in cryptoassets.

According to the enforcement agency, two Chinese nationals called Tian Yinyin and Li Jaidong undertook an elaborate cryptoasset laundering scheme on behalf of the Lazarus Group.<sup>65</sup> In April 2018, the organization stole cryptoassets worth more than \$250 million from an exchange that it had hacked through a phishing campaign. Yinyin and Jaidong laundered \$91 million of the stolen funds using a variety of techniques.

They engaged in "chain peeling" transfers in an attempt to hide the funds' origin before depositing them at four other cryptoasset exchanges. From there, at least \$34 million was sent to Yinyin's Chinese bank account.

Yinyin also used some of the stolen Bitcoin to purchase Apple iTunes prepaid cards worth \$1.4 million.



## 9.2. Indirect Exposure Through Correspondent Relationships

### The Problem

Banks can also face indirect exposure to cryptoasset-related risks through their correspondent relationships. Where a bank facilitates currency clearing or provides other services on behalf of counterparty financial institutions, it may be exposed to risks where those financial institutions maintain relationships with VASPs or other cryptoasset businesses.

### The Typology

1. Bank A – which is based in the United States – receives a request from Bank B in Europe to facilitate a US dollar transfer to Bank C in Asia.
2. Payment details included on the payment message indicate that Bank B's customer is ABC Limited.
3. ABC Limited is a small cryptoasset exchange registered in a high-risk jurisdiction that has processed large volumes of Bitcoin transactions on behalf of cybercriminals.

### Red Flags

Red-flag indicators associated with banks' indirect exposure to cryptoasset risks via correspondent relationships include:

- repeat transactions processed through a correspondent account for the ultimate benefit of a VASP or other cryptoasset business;
- transactions that involve VASPs or other cryptoasset business with high-risk characteristics – such as registration in a high-risk jurisdictions and a lack of KYC controls; and
- VASPs or other cryptoasset businesses featured in the transactions may have legal names that do not clearly indicate their involvement with cryptoassets, which only becomes apparent after further investigation.



## Preventing Indirect Exposure to Cryptoasset Risks

Controls that banks can use to mitigate the risk of indirect exposure to cryptoasset risks include:

- using VASP due diligence solutions – such as Elliptic Discovery – to identify and assess VASP risk profiles prior to approving transactions or establishing relationships with them; and
- feeding data contained in VASP due diligence solutions – like entity legal names, addresses and other identifiers – to enrich transaction monitoring data to assist in the detection of VASP transactions that might otherwise not be apparent.

## 10. Non-fungible Tokens (NFTs)

Few innovations in the cryptoasset space are gaining more attention than non-fungible tokens (NFTs). Put simply, NFTs are a manner of representing ownership in unique digital assets, such as a piece of digital art, sports collectibles, goods and property purchased in online gaming and others.

NFTs are spawning new possibilities for the mainstream adoption of cryptoassets. By tying the infrastructure underpinning digital assets to visible products and a wide range of use cases, NFTs are enabling increasing numbers of people to engage with the cryptoasset ecosystem.

Companies in the NFT space – such as Dapper Labs and Open Sea – have been among the fastest growing companies in the entire cryptoasset industry. During 2021, the NFT market achieved a total estimated value of approximately \$11 billion<sup>66</sup> – a staggering increase of more than 704% on the previous quarter – though this value decreased substantially during the market downturn of 2022.<sup>67</sup>

NFTs are also helping innovators to reimagine the possibilities for Web3, or the metaverse: the ability to trade digital art, buy land in an online game, and other NFT use cases opens up the prospect of new and rich virtual worlds accessible to the average individual.

These incredible new possibilities also present risks. The ability to buy and sell digital art and goods presents new opportunities for fraud, money laundering and sanctions evasion. NFT markets are also characterized by uneven regulatory oversight: while some markets may be captured by AML/CFT requirements for art dealerships, securities brokerage, or other regulated activities, regulatory clarity around the NFT space has been lacking, and regulatory approaches are only emerging. This adds an additional layer of vulnerability to NFT markets, where criminals may attempt to exploit that lack of consistent oversight.

Elliptic's research has indicated a number of trends related to the use of NFTs in crime, including:

- Over \$8 million of illicit funds has been laundered through NFT-based platforms since 2017 – representing 0.02% of trading activity originating from known sources.
- However, a further \$328.6 million (0.81%) originates from obfuscation services such as crypto mixers. A proportion of this may reflect proceeds from illicit activity.
- Over \$100 million worth of NFTs were publicly reported as stolen through scams between July 2021 and July 2022, netting perpetrators \$300,000 per scam on average. July 2022 saw over 4,600 NFTs stolen – the highest month on record – indicating that scams have not abated despite the crypto bear market.
- May 2022 saw the highest confirmed value of NFTs stolen through scams, at just under \$24 million. However, actual numbers are likely to be higher, as thefts are not always publicly reported.

Social media compromises – particularly of NFT project Discord servers – surged in 2022, accounting for 23% of all NFTs (close to 5,000, worth around \$20 million) stolen that year. The growing availability of tailored malware that can bypass multi-factor authentication is likely to be partially responsible.

Below, we describe three financial crime typologies involving NFTs.

## 10.1. NFTs and Money Laundering

### The Problem

NFT markets are highly liquid and assessing a fair value to NFTs can be challenging – or nearly impossible. Some NFTs are selling for staggering sums, such as the NFT “Everydays: the First 5000 Days” by the graphic artist Beeple, which sold for more than \$69 million in March 2021.

NFT markets may be vulnerable in particular to money laundering schemes reflective of trade-based money laundering (TBML), which involves using the purchase of goods and services as a manner of layering illicit proceeds. TBML schemes have been rife in the physical art and antiques world, and the NFT space is also vulnerable to similar risks.

The prospect for TBML typologies in the NFT space is also enhanced by the close intersection of NFTs and DeFi. Because NFTs are traded on the Ethereum blockchain using the ERC721 token standard, traders can buy and sell NFTs with Ether and Ethereum-based tokens used in Dapps.

This can also include making use of DeFi mixers prior to buying or selling an NFT. Elliptic’s research indicates that many large value NFT purchases involve the use of Tornado Cash – the largest NFT mixing service. For more information on Tornado cash, see Chapter 3.2; for more general information on mixing services, see Chapter 2.

### The Typology

1. A criminal has illicit cryptoassets derived from an activity such as hacking a centralized cryptoasset exchange.
2. The criminal uses Tornado Cash to launder any stolen Ether or Ethereum-based tokens, receiving “clean” funds in return.
3. The criminal transfers the new, clean Ether to an NFT marketplace and purchases an NFT.
4. Now in possession of an NFT, the criminal may attempt to resell it, potentially for increased value. The receipt of the NFT sales allows them to demonstrate an NFT sale as their source of funds.

## Red Flags

Red-flag indicators associated with TBML using NFTs may include the following:

- when asked about their source of funds, a customer claims that they are generating large amounts of money from selling NFTs, but they are unable to explain where they got the funds to purchase those high value NFTs in the first place;
- a customer's transactional activity suggests they always send funds through Tornado Cash or other mixers before purchasing NFTs.

## 10.2. NFTs and Fraud

### The Problem

Online NFT marketplaces are ripe for fraud. Criminals can take advantage of the non-face-to-face nature of digital art marketplaces to scam other users, and the frothy prices for which many NFTs sell act as a convenient front for fraudsters. Unsuspecting buyers are vulnerable to scams on NFT markets and may often lack the education necessary to avoid becoming victims. NFT markets are easy targets for “rug pulls” – scams in which an NFT seller flees with money from the purchaser while failing to provide them with the NFT the buyer was promised. In other cases, the NFTs may actually exist, but may not be what they appear.

### The Typology

1. A criminal posts a listing for an NFT on a popular marketplace, posing as a well-known artist or personality.
2. The criminal sells the NFT for a large-value sum – potentially even six or seven figures – to an unsuspecting victim, who believes they are obtaining a work of art produced by a famous person.
3. The criminal receives cryptoassets from the victim, who is left with a worthless NFT.
4. The criminal goes on to launder the proceeds of the fraudulent sale using the techniques described elsewhere in this report.

## Red Flags

Red-flag indicators associated with fraud in NFT market places may include:

- a customer deposits funds into their exchange account that ultimately derive from an addresses associated with known cases of NFT fraud;
- a customer indicates that their primary source of income is selling art on NFT markets, but this is inconsistent with known information about their employment; and

- a customer’s activity suddenly changes to include frequent high value NFT-related transactions that are not explainable from known information about their income.



## Fraud and NFTs

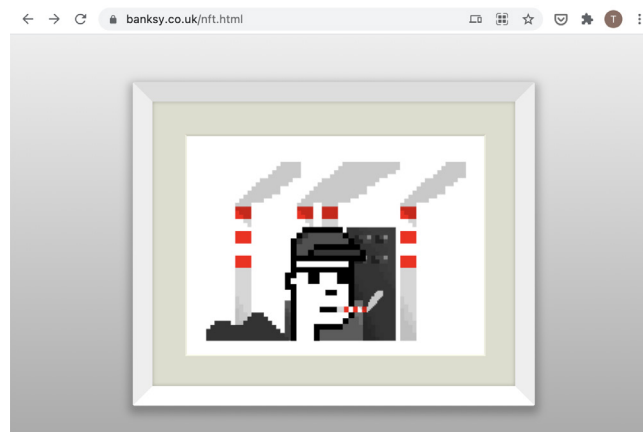
A case that Elliptic identified in August 2021 demonstrates the vulnerability of the NFT market to fraud.

On the morning of August 31st 2021, a new page appeared on the website of the famous British artist Banksy showing an image of an NFT entitled: “Great Redistribution of the Climate Change Disaster”. The image linked to a page on an NFT marketplace called OpenSea – where an NFT featuring the same image was listed for auction. Several bids were soon placed, with the highest being 100 Ether (\$336,000). By 11:00am that morning the image had sold to the bidder willing to pay \$336,000 for the image.

However, Banksy’s representatives later denied that he had created the NFT, and the link to it was abruptly removed from his website. A hacker appears to have gained access to Banksy’s website and used it as a front for duping bidders into paying for a supposed original piece of work by the artist.

Elliptic’s analysis of the Ethereum blockchain indicates that the fraudulent NFT was originally created using funds from an Ethereum account that has been active for just over eight months. It has previously transacted with a major exchange, a gambling service, DEXs and Tornado Cash – a mixing service used to prevent tracing of funds.

Because this case was identified by Elliptic in real-time and garnered significant public attention, the fraudster eventually returned the funds to the victim who had purchased the NFT. However, the case nonetheless reveals how fraudsters can exploit online NFT markets and steal funds from unsuspecting victims.<sup>68</sup>

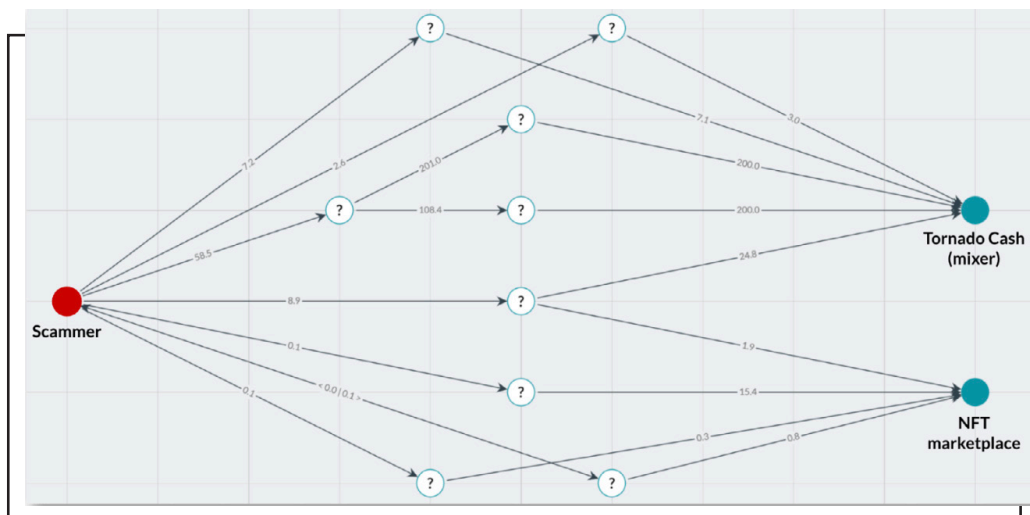


*The “NFT” page on the Banksy website, before it was removed.*



Elliptic actively tracks, verifies and labels addresses implicated in scam reports within its wallet screening and transaction monitoring tools. Scam reports may originate from numerous sources, meaning that NFT marketplaces and cryptoasset exchanges will be alerted and able to block scam addresses identified from different platforms. This is crucial for ensuring that scammers have minimal avenues for cashing out their stolen assets, increasing the incentive – as has previously been observed – to negotiate their return back to victims.

Improving scam response capabilities can have a wider effect of increasing market confidence and dissuading scam attempts – especially if perpetrators observe a reduction in their chances of successfully cashing out.



*This image from Elliptic Investigator shows the flow of funds as a scammer who stole \$325,000 worth of NFTs from 29 victims transfers funds through Tornado Cash and by purchasing other NFTs through a prominent marketplace using intermediary hops.*

Elliptic's tracing capabilities also cover illicit and dark web entities, such as stolen data vendors and identity spoofing services, that are often used by more sophisticated NFT scammers to facilitate their illicit activity, including social media compromises or impersonation scams.

## 10.3. NFTs and Theft

### The Problem

An increasingly common typology Elliptic has observed involves criminals stealing NFTs from collectors. Criminals have succeeded in devising sometimes sophisticated scams that enable them to persuade collectors to part with their NFTs, which the criminals then attempt to sell onwards for their own profit.

These thefts are often perpetrated by criminals establishing phishing websites that can deceive NFT collectors into thinking they are transacting in legitimate marketplaces. Criminals may also pretend to be customer support staff from real NFT markets, duping collectors into providing them with sensitive information or providing them with access to their computers – in order to steal from those users.

### The Typology

1. A criminal establishes a website designed to look like an NFT marketplace, where users are prompted to provide cryptoasset wallet information in order to buy NFTs. The criminal may draw users to the site by publishing advertisements for NFT minting campaigns or discounts on Twitter, Reddit or other popular social networking sites.
2. The unsuspecting user provides their cryptoasset wallet information in response to the website prompt.
3. The criminals are able to use this information to obtain the user's private keys to their cryptoasset wallet.
4. The thieves then steal NFTs in the wallet, and they may also steal other cryptoassets in the wallet, such as Ether or ERC-20 tokens.
5. They then attempt to sell any stolen NFTs on other, legitimate marketplaces, and will also attempt to launder cryptoassets stolen – potentially using DeFi mixing services such as Tornado Cash.

### Red Flags

Red-flag indicators associated with NFT theft include:

- a customer deposits funds into their exchange account that ultimately derives from an address identified as associated with an NFT theft;
- when asked about their source of funds, a customer points to NFT sales on a website that appears to be new and does not have a long history of facilitating NFT sales – suggesting it may be fraudulent.



## Preventing Financial Crime Involving NFTs

Controls that financial institutions can use to mitigate the risk of financial crime involving NFTs include:

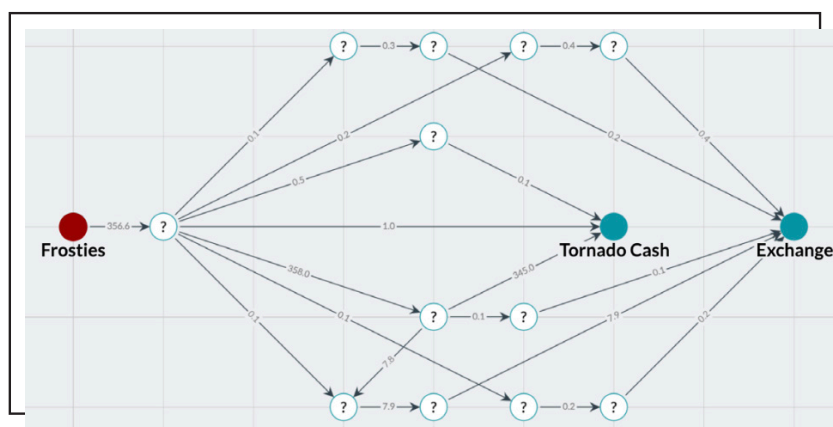
- using wallet screening solutions – such as Elliptic Lens – to determine if a wallet is linked to NFT thefts;
- using transaction monitoring solutions – like Elliptic Navigator – to identify transactions involving NFT thefts;
- blacklisting addresses known to be associated with stolen NFTs, so that they can't be sold on popular marketplaces; and
- educating compliance staff on NFT fraud and scam techniques to enable them to identify situational red flags.



### US Investigators Bust the “Frosties” Rug Pull Scammers<sup>70</sup>

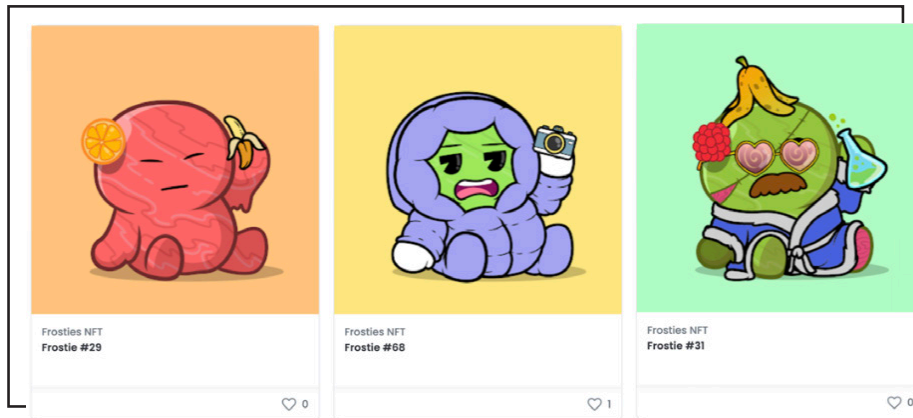
The January 2022 “Frosties” scam NFT project is particularly well known due to its case being potentially the first in the NFT space to lead to real-world charges. Made up of 8,888 trendy cartoons, the Frosties website and social media boasted upcoming metaverse capabilities and other such features typical for NFT projects.

Shortly after the NFTs were minted, the project shut down its social media servers and disabled its website, posting one short-lived tweet before its Twitter account was deactivated – reading “I’m sorry”. The project made \$1.1 million in ETH, 94% of which was laundered through Tornado Cash and the remaining 7% through centralized exchanges.



*Elliptic's Investigator software shows the Frosties scammers laundering their \$1.1 million rug pull proceeds.*

On March 24th 2022, the US Department of Justice announced that two 20-year-old individuals had been arrested in connection to the Frosties rug pull. They faced wire fraud and conspiracy to commit money laundering charges – carrying a sentence up to 20 years in prison. Investigators successfully matched their IP addresses to cryptoasset exchange accounts that had received the proceeds of the funds. The pair had been preparing to launch a new \$1.5 million NFT rug named “Embers” just two days after the announcement.



Some of the 8,888 Frosties NFTs.



#### NFTs and Sanctions

In addition to money laundering and fraud risks described above, NFTs may also present sanctions risks.

Sanctioned actors – such as OFAC-listed cybercriminals and nation states – might attempt to exploit NFTs to raise funds. Cryptoasset businesses or financial institutions that facilitate transactions related to the buying or selling of NFTs involving a sanctioned person could face sanctions violations.

An OFAC action in November 2021 underscored the nature of these sanctions risks. In a sanctions action it took against the Chatex cryptoasset exchange on November 8th 2021 (see more about the sanctions against Chatex in Chapter 1 of this report), OFAC listed several dozen cryptoasset addresses belonging to the platform, which had facilitated millions of dollars of transactions on behalf of ransomware gangs.

Among Chatex's addresses that OFAC listed was an Ethereum address containing NFTs. Elliptic's research revealed that these NFTs were listed on a popular NFT marketplace and had a collective value of approximately \$531,000. The NFTs collected by this account include digital magazine covers, superhero figures and powers, digital land parcels and relatively little-known digital art collections. It has also interacted with the native GHST tokens of the popular NFT gaming collectibles "Aavegotchi". The account has also minted – or created – four of its 42 NFTs itself.<sup>71</sup>

US persons interacting with this Chatex address by buying NFTs it holds could risk running afoul of OFAC sanctions.

# 11. Metaverse-related Laundering

## 11.1. Use of Metaverse Services to Launder

### Illicit-origin Cryptoassets

One of the most exciting developments related to cryptoassets is the emergence of the crypto-enabled metaverse – or immersive virtual reality environments where users interact through avatars. *Decentraland* and *The Sandbox* are two gaming platforms built atop the Ethereum network that utilize their own ERC-20 tokens to enable users to access an increasingly rich variety of experiences online.

In these environments, users can buy plots of land, purchase and collect “wearables”, or virtual clothing, and other items that are created and recorded on the blockchain as NFTs. Users can also utilize DeFi services – such as lending protocols – in the metaverse.

While the number of users operating in the crypto-enabled metaverse is still small, user engagement in the metaverse more generally is expected to grow substantially. Corporates such as adidas, Gucci, J.P. Morgan, Samsung and others have begun launching brand campaigns in the metaverse, and Citi estimates that the metaverse could ultimately present a \$13 trillion opportunity for those firms willing to get immersed in it.<sup>72</sup>

However, the emergence of the metaverse also presents financial crime risks. While instances of metaverse-related crime remain relatively small, as the metaverse grows, so do the risks that illicit actors could launder money through the virtual space, or can commit crimes – such as cybercrime and fraud – in the metaverse, and then launder the proceeds through the crypto ecosystem.

We provide detail on these and other risks in our “Future of Financial Crime in the Metaverse” report.

### The Problem

Criminals can potentially exploit the metaverse to launder the proceeds of crimes. As metaverse environments become increasingly complex, it opens up avenues for criminals to swap their illicit-origin crypto for ERC-20 tokens used in the virtual space, or to purchase digital items in the metaverse with tainted funds in an effort to conceal their ultimate origin.

### The Typology

1. A criminal has possession of Ether that they’ve generated from a crime such as hacking or scams.

2. The criminal swaps the funds at a DEX and obtains ERC-20 tokens that they can trade in a metaverse environment.
3. The criminal uses the ERC-20 token to purchase items in the metaverse, such as land or wearables.
4. The criminal then sells these digital items for units of the ERC-20 token, receiving new “clean” tokens.
5. The criminal then swaps the ERC-20 tokens for Ether at a DEX.
6. They then swap the Ether for fiat currencies at a centralized exchange.

## Red Flags

Potential red-flag indicators associated with laundering through the metaverse include:

- funds are swapped at DEXs for ERC-20 tokens used in metaverse gaming environments, and transaction screening shows that the funds ultimately originate from an illicit source.
- a user has generated large proceeds of ERC-20 tokens from the sale of metaverse-related items – such as land or wearables – that can’t be explained by their known income or other financial activity.

## 11.2. Laundering the Proceeds of **Metaverse Crimes**

### The Problem

As the metaverse evolves, there will also be increasing opportunities for criminals to exploit users in these environments, and to generate illicit proceeds from a variety of crimes, including:

- Scams: fraudsters can perpetrate scams against users in the metaverse, for example by creating phony NFTs.
- Hacking: cybercriminals can steal users’ virtual goods – such as land or wearables – and can also exploit DeFi protocols used in the metaverse.
- Ransomware: ransomware gangs can encrypt users’ NFTs and demand payment in return.
- Drug dealing: darknet market vendors could set up illicit storefronts in the metaverse to sell drugs, or other illicit items such as stolen credit card data.
- Terrorist financing: terrorist and extremist organizations could establish a presence in the Metaverse to raise funds, including by buying and selling digital items.

As these, and potentially other, crimes emerge in the metaverse, illicit actors will face a pressing need to launder the funds from these activities, likely leveraging the DeFi laundering ecosystem we describe in Chapter 3 of this report.

## The Typology

1. A criminal generates illicit-origin ERC-20 tokens – for example, from a scam, hack or ransomware attack the launch in the metaverse.
2. The criminal swaps the ERC-20 tokens for Ether at a DEX.
3. The criminal sends the Ether through a DeFi mixing service.
4. The criminal then takes the new “clean” Ether and swaps it at a centralized exchange for fiat currency.

## Red Flags

Red-flag indicators associated with laundering the proceeds of metaverse-generated crimes could include:

- large volumes or values of ERC-20 tokens associated with metaverse environments are sent into DEXs, and transaction screening indicates that they are associated with an illicit source;
- after converting funds from ERC-20 tokens to Ether or other cryptoassets, the funds are sent through mixers or other obfuscating services.

## Identifying Metaverse-related Laundering

Controls that can enable the detection of metaverse-related laundering include:

- Using wallet and transaction screening solutions – such as Elliptic Lens and Elliptic Navigator – to identify ERC-20 tokens associated with the metaverse that come from an illicit source, and using Holistic Screening to identify where these have been sent through cross-chain or cross-asset services.
- Using Elliptic Investigator to follow and visualize the flow of funds from multi-asset metaverse-related laundering.

## 12. Multi-technique and Multi-service Typologies

Some criminal networks have been observed utilizing several of the money laundering methods described above – using numerous cryptoasset services to profit from their exploits.

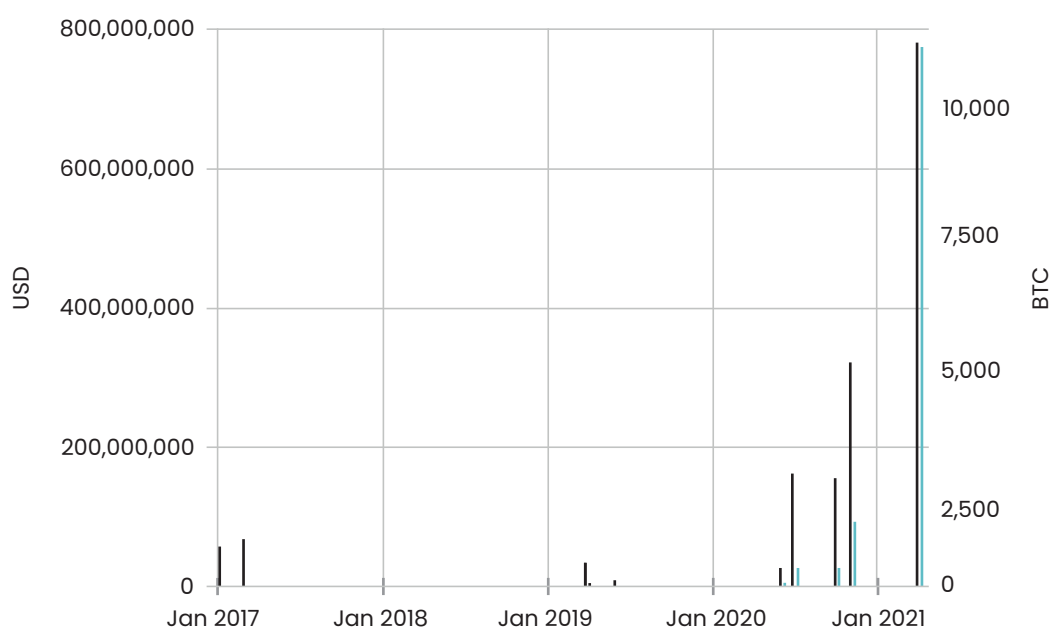
The case studies below describe some of these multi-technique or multi-service typologies.

### 12.1. The Bitfinex Hack

In February 8th 2022, the US Department of Justice announced the arrest of Ilya Lichtenstein and Heather Morgan, a husband and wife couple who the US alleges laundered funds stolen from the August 2016 hack of the Bitfinex crypto exchange. Those funds were worth \$72 million at the time of the theft, but they grew in value more than \$7 billion by late 2021, just before the pair were arrested.

Around 21% of the Bitcoins stolen from the hack were moved and laundered over the past five years – a process that Elliptic has tracked through blockchain analytics.

The 2016 Bitfinex Theft: Value of Outflows From the Thief's wallet



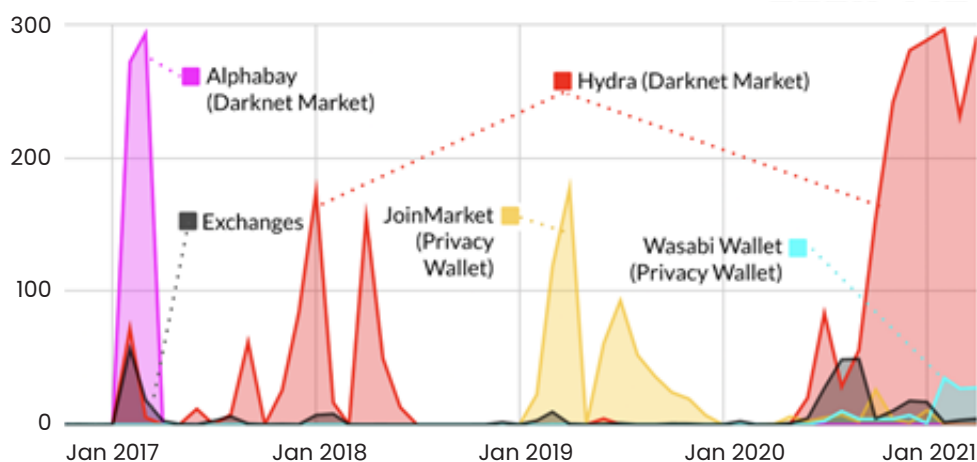
*Monthly outflows from the wallet that received the Bitcoin stolen from Bitfinex. Figures in BTC and USD (using the BTC/USD exchange rate at the time of the outflow).*

On February 8th, the DoJ confirmed Elliptic’s findings that the stolen cryptoassets were laundered using a variety of techniques, including:

*“utilizing computer programs to automate transactions, a laundering technique that allows for many transactions to take place in a short period of time; depositing the stolen funds into accounts at a variety of virtual currency exchanges and darknet markets and then withdrawing the funds, which obfuscates the trail of the transaction history by breaking up the fund flow”.*

Elliptic’s analysis showed that a wide variety of money laundering techniques were used – including sending the funds through darknet markets such as Alphabay and Hydra. The Wasabi Wallet privacy wallet was used to attempt to hide the blockchain money trail. The indictment against the pair also indicates that they used techniques such as peeling chains, chain-hopping by swapping Bitcoin for Monero, and withdrawing funds from Bitcoin ATMs to try and conceal the funds flow.

### Destination of Bitcoins From the 2016 Bitfinex Hack



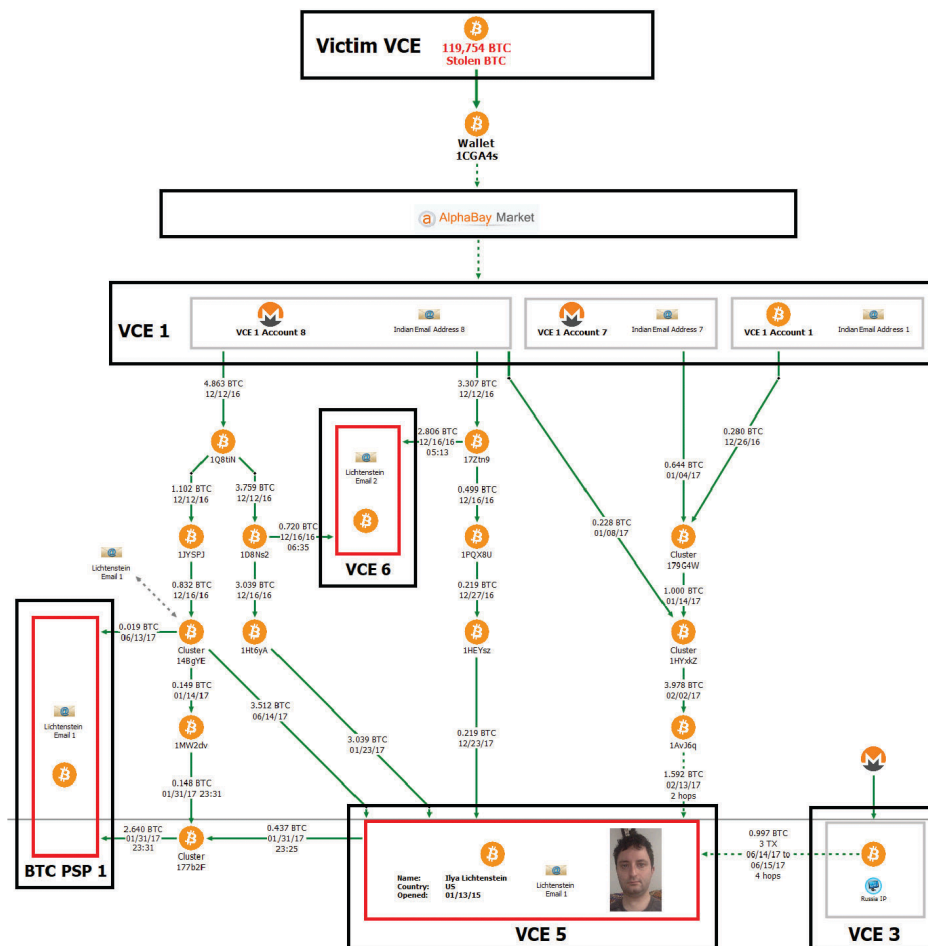
*Number of Bitcoins from the Bitfinex hack received each month by the largest destinations.*

*A significant amount of time can elapse between the funds leaving the theft wallet, and reaching one of these destinations.*

The arrest warrant describes exactly how the suspects were identified. As described above, in January 2017 a small portion of the stolen Bitcoins were moved, and sent through Alphabay – a darknet marketplace. This was likely done in order to hide the blockchain trail. Services such as Alphabay pool all user funds together, making it impossible for anyone other than the platform to link incoming Bitcoin transactions with outgoing ones. Therefore, the launderers effectively used Alphabay as a “mixer”.



However, in July 2017 Alphabay was seized and shut down by law enforcement. This likely allowed them to access Alphabay’s internal transaction logs, which would enable them to trace the stolen Bitfinex funds through Alphabay. The warrant shows exactly this being done – the funds are traced out of Alphabay, and on to a cryptoasset exchange account in the name of Lichtenstein.



A diagram from the arrest warrant, showing how the stolen Bitcoins were traced through Alphabay and another exchange – and onwards to a further exchange account in the name of Lichtenstein.

The remainder of the stolen funds – now worth \$4.1 billion – were moved to a new wallet controlled by law enforcement, who seized the funds when they arrested the couple.

This demonstrates that even when sophisticated money laundering techniques are used, blockchain records still allow law enforcement to link criminal activity to individuals, and bring them to justice.

## 12.2. Operation Argenti

Europol has described<sup>73</sup> the takedown of a criminal network that exploited money mules at cryptoasset exchanges while also using mixers to launder funds.

In a case known as Operation Argenti, criminals had perpetrated ransomware attacks and used fraudulent money mules to open accounts at cryptoasset exchanges throughout Europe and in Spanish banks. Some of the mules were from the Baltic countries and were used simply to open accounts, which were handed over to the criminals to use. Other accounts were opened using entirely false identity documents.

After engaging in cyber crime and fraud, the criminals first moved the dirty Bitcoin through tumblers and mixers. The new Bitcoin obtained from the mixers was then deposited in the mule accounts at numerous European exchanges.

At the exchanges, the funds were converted into euros, which were then transferred to the accounts opened in the names of the Baltic-national money mules in Spain. The bank accounts were typically opened for only a short period before being emptied through cash withdrawals at bank ATMs or through further onward bank transfers.

## 12.3. Russia Hacking

In July 2017, the US unsealed an indictment outlining hacking and money laundering charges against Russian military intelligence officers who worked to undermine the 2016 US Presidential election. This indictment details how state-backed actors can exploit multiple methods of cryptoasset activity to perpetuate illicit behavior.

Officers from Russian intelligence agency Main Intelligence Directorate (GRU) mined Bitcoin to purchase online services and infrastructure such as VPNs and web domains. They did so to carry out their hacking activities against the Democratic National Committee (DNC) and other political organizations. The newly-mined coins had no transaction history on the Bitcoin blockchain; they were transferred to web hosting and other online services via cryptoasset payment processors.

The GRU hackers also managed to conceal their identities and evade detection in many ways. These included:

- false and stolen identity documents to register accounts at legitimate and reputable cryptoasset exchanges in the US;
- relying on P2P exchanges to purchase Bitcoin without having to provide KYC information;

- using third-party individual cryptoasset brokers to launder funds through various unregulated and non-compliant exchanges;
- exchanging funds at a Slovak cryptoasset exchange with lax KYC standards; and
- swapping Bitcoin for other cryptoassets to mask the flow of funds.<sup>74</sup>



#### Using Cryptoassets to Purchase Web Hosting and Other IT Services

This is a common occurrence, and in most cases it is likely to be entirely legitimate. However, illicit actors have also used Bitcoin to purchase online services for illegal activities.

Russian hackers have used cryptoassets to purchase web hosting and other online services including VPNs to facilitate their crimes. Part II below implies that at least one group of jihadist actors may have used Bitcoin to purchase web hosting services in support of a propaganda campaign.

Companies that provide online services can serve as a convenient front for criminal actors. That's because they can justify having a limited physical presence and high turnover and can present a high money laundering risk.

Possible red flag indicators that might be associated with the use of cryptoassets to purchase web hosting and other online services for illegal purposes include the following:

- a customer makes frequent and/or rapid cryptoasset deposits and onward transfers via payment processors to web hosting or similar services. They refuse to provide information about the source of funds to purchase those services, or the intended use of those services;
- a customer uses cryptoassets to buy web hosting services in high-risk jurisdictions, or in jurisdictions that have no logic given the customer's physical location; and
- a customer attempts to purchase services through a cryptoasset payment processor located in a high-risk jurisdiction.



## Unusual and High-risk Mining Activity

Illicit actors also engage in cryptoasset mining to generate newly minted coins that do not have a tainted history.

Sanctioned actors use mining as a source of funds they can access outside the international financial system.

South Korean intelligence services reportedly speculate that North Korea may be involved in mining cryptoassets. Such activity may be lower scale and could also be difficult to detect.<sup>75</sup>

Iran and Venezuela have also shown interest in mining to undercut US sanctions. In July 2020, the Iranian government issued licenses to 14 Bitcoin mining farms and provided them with reduced energy rates.<sup>76</sup> In September 2020, Venezuela also created a licensing regime for cryptoasset mining that ensures it is involved at all stages of the mining process.<sup>77 78</sup> In April 2022, OFAC issued sanctions against the Russian mining company BitRiver. The sanctions appear to have been pursued in response to statements from the Russian government – including President Vladimir Putin directly – suggesting that Russia may seek to leverage its vast energy reserves to mine Bitcoin and circumvent sanctions, potentially attempting to emulate the Iranian approach.

We expect that in 2023, OFAC will ramp up its efforts to target mining activity in sanctioned jurisdictions by designating further mining-related entities in countries such as Russia and Iran.

Other criminal actors may engage in large-scale Bitcoin mining that could draw significant attention. For example, this could include criminals who steal electricity to mine Bitcoin or who steal mining equipment that they then use for their own purposes. Or it could be thieves who aim to conceal the proceeds of crime by using illicit funds to buy mining equipment that can be used to obtain newly minted cryptoassets.

Mining pools also present money laundering risks insofar as illicit or sanctioned actors may participate in a pool and benefit from – or contribute resources to – the pool's operations. Mining pools can also present sanctions risks where their operations are carried out in sanctioned countries. In August 2020, a Chinese Bitcoin mining pool called Lubian.com announced it had established a mining farm in Iran at the site of a Chinese-Iranian owned power plant.<sup>79</sup>

Red flags of potentially suspicious activity that a conversion service such as an exchange might consider if in receipt of funds from a miner include the following:

- the customer resides in a jurisdiction where there is little economic incentive to engage in mining – the jurisdiction lacks tax incentives and is generally not known for large-scale mining, for instance – and can not provide a convincing explanation for why they are mining Bitcoin;
- information in the public domain suggests the customer may be involved in mining activity in sanctioned jurisdictions;
- the activity involves a mining pool that accepts participants from sanctioned jurisdictions; and
- the customer attempts to deposit a large volume of cryptoassets close to the time of publicly-revealed crypto-jacking campaign.

## 12.4. Dark Web Laundering

The Financial Action Task Force (FATF) has highlighted the increasing professionalism of money launderers utilizing cryptoassets<sup>80</sup> It describes a Russian police investigation into money laundering techniques employed by organized criminals operating on the dark web.

The case involved a dark web drug dealer with a Tor-hosted storefront that accepted both Bitcoin and fiat-denominated payments from customers. The criminals running the site employed professional money launderers in order to move funds through a complex series of activities, including:

- money mules – generally students unaware that they were engaged in criminal activity – to open fiat-denominated bank accounts and prepaid cards where funds could be cashed out;
- swapping funds that had been received for drug payments from Bitcoin into fiat at many cryptoasset exchanges;
- moving funds through many cryptoasset wallets to avoid detection; and
- distributing Bitcoin among members of the criminal network to pay their salaries – including various low-level members of the organization.

The FATF report also suggests that there is increasing evidence of professionalized money laundering networks using Bitcoin mixers before transferring funds on to other members of criminal networks. They then fund prepaid cards with the laundered cryptoassets before spending it on various goods and services.

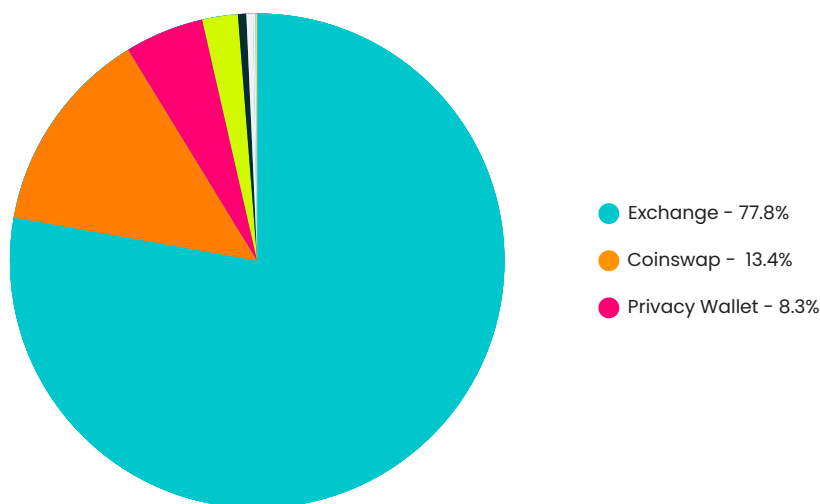
The report also warns that insiders at complicit digital asset exchanges can be exploited by criminal networks seeking to move large volumes of cryptoassets.<sup>81</sup>

## 12.5. Ransomware: the Colonial Pipeline Attack

Ransomware gangs have been especially effective at harnessing multiple techniques to launder the proceeds of their crimes. This was apparent during one of the most widely publicized ransomware attacks to date: the Colonial Pipeline attack of May 2021.

In that case, a major US oil and gas company called Colonial Pipeline was the target of a ransomware attack perpetrated by the Russia-based DarkSide ransomware gang. To recover access to its IT systems, Colonial Pipeline paid a ransom of 78.29 Bitcoin – approximately \$4.4 million at the time – to DarkSide and its affiliate that conducted the attack. Using techniques such as blockchain analytics, US law enforcement managed to recover approximately 85% of the ransom payment – robbing the attackers of their profits.

However, DarkSide still did manage to launder approximately 15% of the ransom payment it received. To do so, it used a variety of techniques as indicated in the chart below. Most of the funds – approximately 90% – were laundered through unregulated and non-compliant exchange services and coinswap platforms. A further 5% was laundered using privacy wallets. And several other techniques – including sending funds to Hydra market, potentially to use dark web cash out services – were used to enable the remainder of the laundering.



*Destination of funds laundered from the Colonial Pipeline ransomware attack.*

## 12.6. Other Examples

Elliptic's research has identified several other multi-technique and multi-service typologies of note that may appear in money laundering schemes as follows:

- criminals relying on chain-peeling to hide their Bitcoin transaction trail. They deposit funds at exchanges, potentially relying on fraudulent documents, or by making deposits at numerous unlicensed and non-compliant exchanges;
- customers using cryptoasset ATMs to purchase Bitcoin that is swiftly transferred to illegal offshore gambling sites. The payments made to the gambling sites is the only activity the customer engages in;
- customers using cryptoasset ATMs to buy Bitcoin they can use to purchase stolen card information from dark web carders;
- customers receiving large volumes of cryptoassets into a cryptoasset custodial wallet service. They immediately transfer the funds to cryptoasset prepaid cards and cryptoasset ATMs in volumes and values that have no obvious explanation;
- customers withdrawing illicit origin cryptoassets from cryptoasset ATMs using a cryptoasset prepaid card; and
- cybercriminals instruct victims of ransomware attacks to purchase cryptoassets on exchanges in Europe and the US. After receiving the tokens, the thieves use a complex chain of mixers and other techniques before cashing out at unregulated exchanges.

→ 02.

# Terrorist Financing



The number of reliable and publicly confirmed cases of terrorist financing (TF) involving cryptoassets remains relatively small in comparison to general money laundering activity, and compared to their broader use by sanctioned actors.

Analysis of TF campaigns between 2020 and 2022 suggests that they have become more sophisticated in their use of cryptoassets through the following:

- successfully raising greater amounts than before;
- identifying new methods for obtaining cryptoassets;
- raising funds in cryptoassets other than Bitcoin; and
- taking additional steps to obfuscate their use, such as using privacy coins and encrypted chat communications.

TF often involves only very small amounts of funds directed towards specific activities – therefore making it extremely difficult to detect. A cryptoasset business might struggle to identify that TF is occurring at all, with no knowledge of specific terrorist-associated cryptoasset addresses, or being supplied with direct information from law enforcement that a customer is a terrorist suspect.

Nonetheless, there are instances of TF using cryptoassets of which it is important to be aware.

# 13. TF Involving Crowdfunding Through Charities and Other Organizations

## Jihadist Activity

Jihadist actors have been identified engaging in cryptoasset-enabled fundraising activities through apparent charities, media or propaganda offices, and other organizations.

One prominent case is that of Al Sadaqah – an apparent charitable and fundraising organization supporting militants in Syria.

In December 2017, Al Sadaqah began posting on forums such as Telegram and Twitter calling for supporters to send Bitcoin to an address controlled by the group (see image below). In early 2018, Al Sadaqah then began posting on its Twitter account calls for supporters to send funds to the group through Bitcoin ATMs, and posted links to CoinATMRadar maps showing the locations of ATMs.<sup>82</sup>



As of September 2018, the Al Sadaqah Bitcoin address had received Bitcoin only totaling approximately \$575. However, at that time, the group also began soliciting donations in three privacy coins: Monero, Dash and Verge. It is unclear how much funding they generated in these altcoins, but the fact that the group looked to these coins as a source of funding suggests they had concerns about the transparency Bitcoin affords.

Ultimately, the Al Sadaqah fundraising campaign was dismantled by US law enforcement in August 2020.<sup>83</sup> US agencies seized funds belonging to Al Sadaqah and other supposed charities operating on behalf of Al-Qaeda. Many of the donations made to these organizations were laundered through BitcoinTransfer – a Syria-based crypto exchange business. BitcoinTransfer operates through Telegram channels and an office in the Syrian city of Idlib.

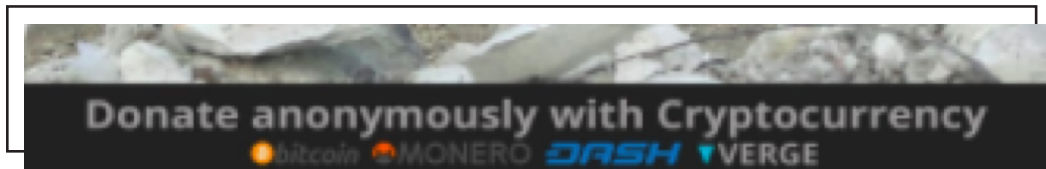


Image from the Al Sadaqah Twitter account soliciting donations in various cryptoassets.

The US law enforcement action in August 2020 also targeted the Al-Qassam Brigades campaign – a fundraising initiative first identified by Elliptic in January 2019. The Al-Qassam Brigades is the military wing of Hamas. In early 2019, it began soliciting Bitcoin donations to support its militant activities.

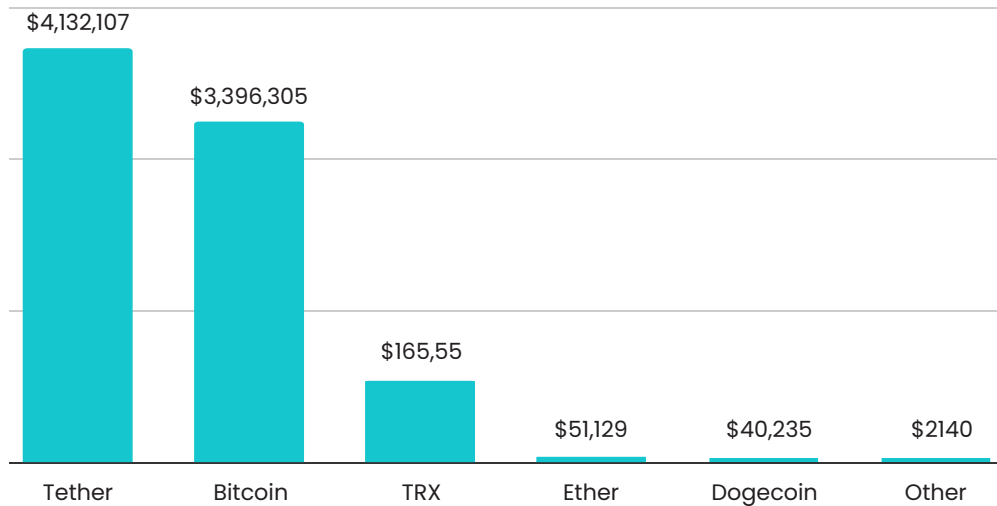


Initially, it began the campaign by requesting funds be sent to a static donation address listed on its website. Approximately \$4,000 worth of cryptoasset donations were received in the first few weeks. The organization subsequently launched a new fundraising website that generated unique donation addresses for each visitor. This technique is commonly seen with ransomware, and makes it more challenging for outside observers to monitor donations and trace where the funds are sent.

Elliptic identified a set of addresses used to receive donations during this campaign. This involved network analysis of transactions associated with previous campaigns by the same actor. The majority of donated Bitcoins came from a single, major cryptoasset exchange. These donations were then swept up by the Al-Qassam Brigades and sent to another exchange based in a country without strong AML controls – perhaps to be cashed out for fiat currency.

US law enforcement agencies seized the Al-Qassam website infrastructure and dismantled the fundraising campaign. They captured funds from 150 cryptoasset wallets involved in sending donations to and from Al-Qassam. Despite this law enforcement action, Elliptic’s analysis indicates that the Al-Qassam Brigades managed to raise approximately \$7.7 million through July 2021 across a range of cryptoassets, as indicated in the chart below.<sup>84</sup>

## Value of Cryptoassets Received By Hamas-linked Addresses Subject to Israeli Government Seizure Order



Another case of cryptoasset-enabled TF involving jihadist organizations is the Ibn Taymiyya Media Center (TMC). TMC acts as the media and propaganda office of the Mujahideen Shura Council in the Environs of Jerusalem (MSC), which is a US-designated terrorist organization operating in the Gaza Strip. In mid-2016, the TMC began soliciting Bitcoin donations to fund militant activities. As of September 2018, the Bitcoin address posted in its funding adverts on Twitter indicated that the group had raised Bitcoin worth approximately \$9,000 in two years. Analysis of Bitcoin payment flows linked to the TMC address reveal that some donations made to the organization ultimately trace back to BTC-e. This suggests that some jihadist supporters may attempt to exploit non-compliant exchanges when making donations. The US indictment of BTC-e and Alexander Vinik also indicates that aliases used by illicit actors to establish accounts at BTC-e included names such as "ISIS".<sup>85</sup> Bitcoin blockchain analysis also indicates that wallets associated with TMC donations have also sent funds to other unregulated exchanges, P2P exchanges and online gambling sites.<sup>86</sup>

A 2017 report by the FATF on emerging TF typologies also shows that at least one FATF member has observed instances of a jihadist propaganda organization buying web hosting services using donations received in Bitcoin.<sup>87</sup>

A recent case in the UK showed that while relatively small scale, terrorist financiers are seeking out additional innovative ways to utilize cryptoassets. Khuram Iqbal was a supporter of al-Qaeda based in Wales who was convicted of supporting violent extremism and distributing propaganda material on behalf of the organization. In December 2021, a UK court held that Iqbal had failed to disclose information about his cryptoasset activity, which included using Bitcoin to purchase stolen credit card details on the dark web. This activity came to light due to SAR filings by Coinbase, where Iqbal maintained an account.<sup>88</sup>

## Political Extremist Activity

Political extremist groups have also attempted to use cryptoassets to raise funds outside of the traditional financial sector. Neo-Nazi and other right-wing extremist organizations have expressed an ideological preference for digital assets over the traditional banking system. These organizations may seek to raise cryptoassets to further propaganda campaigns as well as buying and using web-based services. Elliptic's research indicates that extreme right-wing organizations have amassed a total of \$8.9 million in cryptoassets to date.<sup>89</sup>

Examples of neo-Nazi and other right-wing militant organizations using cryptoassets include the following:

- Elliptic's research in December 2021 indicated Bitcoin transactions sent to extreme right-wing wallets are frequently sent in amounts using the value "1488". This number represents common neo-Nazi symbolism. The number "88" is used by many far-right extremists to represent the phrase "Heil Hitler", because H is the eighth letter in the alphabet. The number "14" is numerical shorthand for the white supremacist slogan known as the "14 Words". These numbers are commonly combined, with "1488" acting as a key symbol of neo-Nazi and white supremacist ideology. In the case of one extremist wallet, 47% of all payments received were for amounts containing "1488". This is 30,000 times more than was seen for active cryptoasset wallets with no known links to the far-right.
- In August 2018, an Eastern European-based neo-Nazi militant group called the Order of Dawn was identified soliciting cryptoasset donations on its website.<sup>90</sup> The group asks supporters to send Monero to a Monero address listed on the site, and instructs them to purchase Bitcoin on US-based exchanges. The Bitcoin is then used to buy Monero at an EU-based exchange. The group's site also includes an embedded Monero mining tool – allowing visitors to the site to loan their computer power to provide Order of Dawn with newly-minted Monero. Order of Dawn claimed to have raised 62 Monero – worth approximately \$6,000 – and asserts that the cryptoassets will fund the development of a volunteer militant army.
- The Daily Stormer – a neo-Nazi website – has raised large values of funds in Bitcoin, receiving individual donations of as much as \$50,000.<sup>91</sup>
- The US-based neo-Nazi and white supremacist group Vanguard America has also attempted to raise funds using Bitcoin.<sup>92</sup>

Researchers of extreme right-wing activity also point out that these groups may be looking increasingly to Monero and privacy coins. This is because their Bitcoin activity has come under scrutiny, and they have been denied accounts at Bitcoin exchanges.<sup>93</sup>

Additionally, as extremist groups have been dropped from major social media platforms and from fundraising sites such as Patreon, they have switched to raising funds on extremist-run crowdfunding sites such as Hatreon, or on Tor-based donation sites.

## Red Flags

Red flags associated with TF activity involving jihadist and extremist groups and organizations may include the following:

- cryptoassets identified as deposited to, or originating from, a specific wallet address that has appeared on jihadist or extremist-sponsored social media and messaging sites, associated with Twitter and Telegram;
- cryptoassets identified as deposited to – or originating from – a specific wallet address that has appeared on jihadist or extremist-sponsored ads on fundraising sites such as Kickstarter, Patreon or on sites such as Hatreon;
- cryptoassets identified as deposited to – or originating from – a specific wallet address that has appeared on jihadist or extremist-sponsored sites on Tor;
- funds deposited to – and withdrawn from – relevant cryptoasset addresses may trace to unregulated and non-compliant exchanges; and
- funds are transmitted in figures using “1488” – a customer repeatedly sends or receives transactions of .00001488 Bitcoin, for instance.

## 14. TF Involving Individuals or Small Cells

Individual and small-cell terrorist supporters have been identified as attempting to fund activity using cryptoassets in some limited instances.

Small cell and lone actor TF activities can sometimes be nearly impossible to spot, or to distinguish from normal customer activity, or from patterns of generic money laundering. It is important to be aware of the threat in case a cryptoasset business is ever directly exposed to it. Some examples of TF involving individuals and small cells include:

- 2015: Virginia teenager Ali Shukri Amin was charged with providing support to ISIS. He had posted instructions on Twitter describing how other supporters of ISIS could fund the organization using Bitcoin.<sup>94</sup>
- 2016: the Indonesian government announced that members of a jihadist cell based in Java had used Bitcoin and FinTech services such as PayPal to transfer funds between them.<sup>95</sup>
- December 2017: Zoobia Shahnaz – a US citizen residing in New York – was arrested for attempting to fund ISIS. She first used stolen cards and compromised accounts to purchase cryptoassets. Shahnaz sold these for fiat and transferred onward to accounts held in the names of front companies in countries such as Pakistan.<sup>96</sup>
- November 2020: a white supremacist supporter started a betting pool on the social media platform 4Chan that solicited Bitcoin bets. It involved speculating on the assassination or resignation of then-presidential nominee Joe Biden.

### Red Flags

Red flags associated with TF activity involving lone actors and small cells may include the following:

- customer attempts to establish accounts with false identity documentation and purchasing cryptoassets with stolen card details;
- customer withdraws cryptoassets from an exchange. The cryptoassets trace immediately – or through multiple hops – to an address associated with terrorist and extremist content on social media, Tor-hosted sites or general crowdfunding platforms;
- customer attempts to swap cryptoassets at an exchange for fiat, and funds ultimately trace to an address associated with terrorist or extremist content;

- the customer's social media presence may indicate that they post on sites or share information about extremist content, such as jihadist or neo-Nazi material on platforms such as Twitter, Facebook and others;
- multiple individuals operating together may open accounts at a similar time and transfer funds among one another's wallets. Transfers may be made to or from wallets associated with individuals, exchanges or other services located in high-risk terrorist financing jurisdictions; and
- immediately after swapping cryptoassets for fiat, the fiat funds may be transferred onward to accounts in high-risk terrorist financing jurisdictions.



#### Terrorist Cell Using Bitcoin Coupons

In September 2020, French law enforcement announced the dismantling of a terrorist financing cell that used cryptoassets to support militants in Syria.

According to reports, France arrested 29 individuals associated with Al-Qaeda affiliate Hayat Tahrir Al-Sham. Those arrested were involved in purchasing Bitcoin coupons from licensed tobacco shops around France. The cell members used cash to purchase the coupons, which can be redeemed in Bitcoin in values ranging from 10 to 150 euros (\$11 to \$165). Once they were in possession of the Bitcoin, the members of the network transferred them to French jihadists residing in Syria.<sup>97</sup>



→ 03.

## Key Trends: Criminal and Threat Actors

The first two parts of this report provide an overview of key money laundering and TF typologies in the cryptoasset space. In this section, we summarize the trends our research has revealed about how certain types of criminals and threat actors use these techniques.

The table below offers a high-level summary of how certain actors are known to use various cryptoasset-laundering methods:

Methods	Crypto Exchanges	DEXs	ATMs	Cards	Mixers/Privacy Wallets	Tokens & Stable coins				Metaverse
						Wallet-Specific	Privacy Coins	NFTs		
<b>Criminal/Threat Actor</b>										
Hacker/Cybercriminal	X	X	X	X	X	X	X	X	X	X
Dark Web Vendors (including online drug dealers, carders, etc.)	X	X	X	X	X		X	X		
Fraudsters (including Ponzi scheme perpetrators)	X		X	X	X	X			X	X
Professional Money Launderers	X	X	X	X	X	X	X	X		
Street Drug Dealer	X		X	X						
Human Traffickers/Sex Trade	X		X	X						
Tax Evaders	X			X	X	X		X	X	
State Actors/Sanctions Evaders	X	X		X	X	X	X	X	X	
Terrorist/Political Extremist	X	X	X	X	X	X	X	X	X	

The sections below provide further detail regarding these trends.

## 15. Hackers and Cybercriminals

Hackers and other cybercriminals – such as perpetrators of exchange thefts and ransomware attacks – are the category of illicit actors most likely to operate comfortably in the cryptoasset domain. They rely most heavily on cryptoasset laundering at every stage of their operations. Hackers, ransomware attackers and other cybercriminals have been especially adept at leveraging cross-chain typologies of money laundering that we describe in section 3 of this report.

Cybercriminals exploit every money laundering method described in this report, and they employ relatively complex schemes with numerous layers of obfuscation along the way.

Bad actors employ these techniques to clean illicit-origin cryptoassets – such as digital assets obtained in the hack of an exchange, or from a ransomware attack – as well as to layer illicit fiat-denominated proceeds of crime, like laundering funds obtained from online banking compromises or other fiat-based hacks by converting the money into cryptoassets.

Recent trends our research points to in cybercrime-related cryptoasset laundering include the following:

- employing intricate money mule schemes in coordination with complex multi-service laundering techniques (see sections 1.3, 2, 6.1 and 12.1);
- a willingness to cash out at legitimate cryptoasset exchanges – rather than relying purely on complicit exchanges – while using stolen identity information from KYC kits (see section 1.3);
- use of cross-chain and cross-asset typologies, including laundering funds through DEXs, and DeFi bridges (see section 3);
- Using cryptoasset debit cards to spend large volumes of funds on luxury items (see section 8.1);
- ransomware perpetrators encouraging victims to purchase cryptoassets on exchanges that do not collect KYC information;<sup>98</sup>
- laundering illicit origin cryptoassets by purchasing tokens and stablecoins (see section 4.1);
- hacking centralized exchanges to obtain tokens and stablecoins, with laundering occurring via DEXs, DeFi mixers and cross-chain bridges (see section 3);
- simultaneous use of both mixing services and privacy wallets (see section 2);
- laundering funds through metaverse-related tokens and services (see section 11).

## 16. Dark Web Vendors

Criminal enterprises operating on the dark web have long relied on cryptoassets in order to sell goods and services to other criminal actors.

Goods and services marketed by dark web vendors include the following:

- narcotics, with a growing emphasis on the availability of highly-dangerous drugs such as fentanyl;
- stolen debit and credit card information, available on Tor-based storefronts that allow carders to buy and sell compromised data;
- guns, ammunition and other arms and weapons; and
- crime-as-a-service (CaaS) models, this includes the provision of malware kits, KYC kits and assistance with cashing out cryptoasset-based criminal proceeds.

Elliptic has detected a trend of migration to decentralized dark web marketplaces in recent years. Unlike the major established dark markets to date, these markets do not offer a custodial account service for settling payments among buyers and sellers. They sometimes rely on coinswap services to immediately swap Bitcoin that vendors receive into Monero.

Recent cryptoasset-laundering trends highlighted among dark web vendors include the following:

- Bitcoin remains the favored cryptoasset owing to its high liquidity, despite some dark web vendors and marketplaces having looked increasingly to Monero and other privacy coins, as well as Litecoin. Vendors may also look to privacy coins more as a layering tool in the money laundering process – sometimes relying on coinswap services to do so (see section 5.2);
- some vendors – including carders and drug vendors – may also make regular use of mixers and privacy wallets (see section 2);
- a noticeable reduction in the number of dark web vendors using static cryptoasset addresses and, or recycling old addresses when trading. A growing number appear to be generating new addresses for each trade and employing more complex wallet behaviors (see section 6); and
- like cybercriminals, dark web vendors may increasingly rely on money mules and KYC kits to exploit legitimate exchanges (see section 1.3);

## 17. Fraudsters

Fraudsters have long attempted to abuse the cryptoasset ecosystem – especially through Ponzi Schemes (as described in the text box in section 8). Fraudsters remain a major ongoing threat of which cryptoasset businesses must remain aware.

Laundering trends among fraudsters as revealed by our research include:

- an increasing number of scams instruct victims to make payment via cryptoasset ATMs (see section 7.3);
- using cryptoassets to carry out frauds and launder funds through services such as iTunes gift cards (see section 8.3);
- using cryptoassets to purchase fiat prepaid cards and gift cards, which can then be laundered through fraudulent accounts (see section 6.2);
- scams perpetrated via social media – such as the Twitter hack – with fraudulently-obtained cryptoassets laundered via mixers and privacy coins (see section 2);
- scams involving NFTs (see section 10);
- scams involving users of the metaverse (see section 11).

### Pig Butchering: Using Blockchain Analytics to Detect and Disrupt Fraudsters

Recently, a form of investment scam involving cryptocurrencies has become among the top fraud concerns of law enforcement agencies around the world: pig butchering.

Pig butchering scammers are raking in increasingly massive sums in Bitcoin and other cryptoassets, with a devastating impact on their victims.

However, one key weapon that law enforcement agencies and financial crime compliance teams have in their arsenal to stop pig butchering scammers is the transparency of the blockchain.

Below, we will describe how blockchain analytics can enable the detection and disruption of pig butchering scams.

### Pig Butchering: a Growing, Devastating Form of Fraud

“Pig butchering” is not a legal term, but rather refers to a variety of investment fraud that originated in China – where the scams are referred to as “*Sha Zhu Pan*” – and has spread to target victims across the globe.

In pig butchering schemes, victims are targeted through social media platforms, dating apps, or other approaches online by scammers who often pose as a potential romantic partner and who claim to be successful cryptocurrency investors. Criminals may establish elaborate, phoney, social media profiles designed to make it appear as though they live a lavish lifestyle funded by cryptocurrencies. After establishing a trusted relationship with the victim, the scammer will convince the victim to begin investing their own money in cryptocurrencies to get a slice of wealth themselves.

Gradually, over the course of weeks or months, the scammer will persuade the victim to depart with their money, supposedly to invest it in cryptocurrencies. This is where the term “pig butchering” comes from, since the process resembles fattening an animal before slaughtering it. To lure in their victims, scammers will sometimes create fake websites designed to mimic authentic crypto trading platforms.

Victims are instructed to purchase cryptocurrencies on crypto exchanges, and then transfer the funds to crypto addresses supposedly associated with these fake trading sites. In October 2022, the US Federal Bureau of Investigation (FBI) also warned that victims are also increasingly instructed to transfer payment by withdrawing cash from their bank accounts and depositing it into Bitcoin ATMs.

The crypto addresses where the victim transfers the funds are controlled by the scammers, who take in the funds from their unsuspecting victims. To persuade the victim to continue “investing” their funds, the scammer may even create fake account statements designed to make it look like the victim’s supposed crypto investments are generating large returns.

However, once the victim has invested large sums of money – sometimes thousands or even millions of dollars – the scammer will suddenly cut off all contact. The victim is left without their money, and in many cases suffers complete financial ruin. In one recent case, a man in the US lost \$1 million in a pig butchering scam after he was befriended by a potential romantic interest who turned out to be a fraudster.

According to the FBI, most victims of crypto investment scams are in the age range of 30 to 49 years old. However, scammers may target victims across a variety of demographics, seeking out those who are vulnerable, such as people with ill family members, those in financial distress, or people grieving from a recent divorce or other devastating life event.

The exact scale of pig butchering scams is difficult to pinpoint, particularly given the likelihood that many if not most cases go unreported. One US government estimate put the figure at nearly \$430 million in fraud losses suffered from pig butchering, though the true figure is likely greater, given that the FBI claims that reported crypto frauds in 2022 raked in at least \$2.5 billion in the US alone.

Another terrible side to pig butchering involves the experience of many of the individuals who carry out the scams. In many cases, the people actually acting as pig butchering scammers are individuals in countries in regions such as Southeast Asia who have been coerced by human traffickers to carry out these crimes. These individuals are forced to conduct pig butchering frauds from scam call centers that are run by organized criminal syndicates who ultimately profit from the underlying crimes.

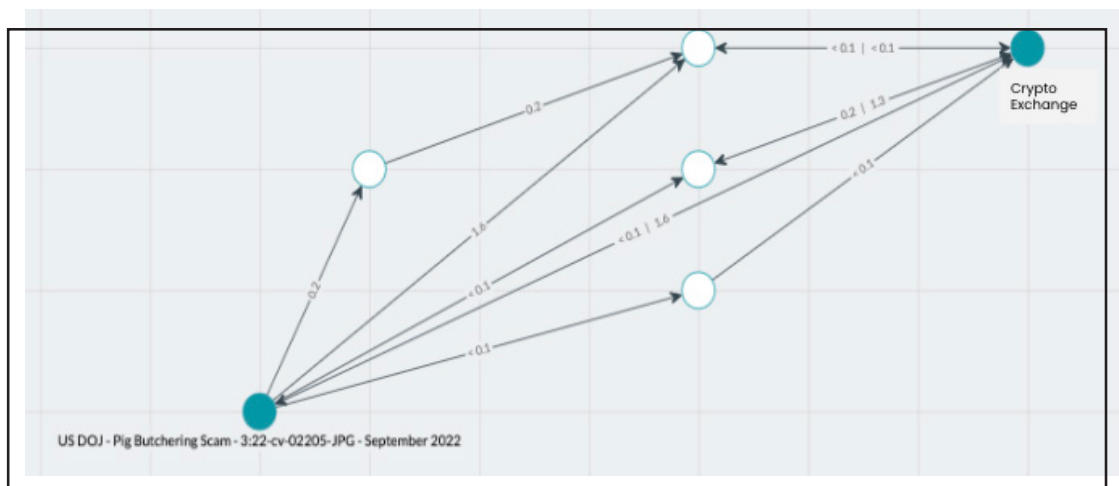
## Using Blockchain Analytics to Identify and Disrupt Fraudsters

Pig butchering scams reap a horrible toll on their victims, and consequently, combatting pig butchering has become a major law enforcement priority in the US and elsewhere.

One key tool in uncovering these scams and their perpetrators is the ability to follow related cryptoasset funds flows on the blockchain.

When defrauding their victims, pig butchering scammers can leave a trail of clues on the blockchain that can be revealed using analytics capabilities like those Elliptic has pioneered.

For example, after receiving cryptoassets from a victim, a scammer will generally attempt to swap the funds at a cryptoasset exchange service, as is detailed in the image below, which shows a Bitcoin address belonging to pig butchering scammers revealed as part of the US Department of Justice (DoJ's) efforts to disrupt websites used by scammers.



*The image above from Elliptic Investigator – our multi-asset investigative software – shows the flow of funds between a Bitcoin wallet belonging to a pig butchering scammer identified by the US Department of Justice (indicated by the green circle on the bottom left) and a wallet belonging to a cryptoasset exchange platform (indicated by the green circle on the top right).*

It is at this stage that the perpetrators behind these schemes become vulnerable to detection and disruption. Using a blockchain analytics forensics solution such as Elliptic Investigator, a law enforcement agency can see that funds from a scam have been sent to an exchange. This allows agents to request information from that exchange, such as know-your-customer (KYC) details that can reveal the identities of the individuals behind those accounts.

Similarly, using blockchain analytics transaction screening capabilities, the cryptoasset exchange that receives the funds from the fraudsters can see that they were in receipt of funds from a pig butchering scam, which can allow them to file suspicious activity reports (SARs) or otherwise alert law enforcement to the transactions in question.



## 18. Professional Money Launderers

A growing body of evidence suggests that professional money laundering networks have made more frequent use of cryptoassets. And criminal actors such as cybercriminals and dark web vendors now look to professional money launderers to move illicit origin crypto on their behalf.

Observed cryptoasset-laundering trends involving professional networks include:

- exploiting non-compliant and complicit exchanges (see section 1.1 and 1.2);
- carrying out complex multi-service technologies using mixers, wallet-specific behaviors and other techniques on behalf of organized criminals selling drugs on the dark web (see section 12.3);
- utilizing stablecoins to avoid price volatility during the money laundering process (see section 4);
- exploiting money mule networks in coordination with services such as cryptoasset ATMs and cryptoasset prepaid cards (see sections 7.2 and 8.1);
- utilizing cryptoasset ATMs located in jurisdictions with no cryptoasset regulation to launder funds internationally on behalf of drug cartels or other organized crime groups (see section 7.1); and
- owning and operating cryptoasset ATMs (see section 7.1).

## 19. Street Drug Dealers

In addition to dark web-based drug distribution, street drug dealers – sometimes separately, but in other instances possibly working with dark web vendors – can also exploit cryptoassets.

Certain services and typologies may prove particularly attractive for street dealers seeking to move swiftly between cash and digital assets – or vice versa. Even relatively unsophisticated, localized drug dealing networks may attempt to take advantage of cryptoassets' P2P nature as a method for bypassing the mainstream banking system.

Methods that street drug dealers may employ to exploit and launder digital assets include the following:

- engaging in cross-wallet activity among a network of customers at an exchange or wallet provider (see section 6.2);
- using cryptoasset ATMs to “smurf” large values of high value fiat notes for conversion into digital assets and eventual onward transfer to other members of the criminal network (see section 7.1);
- a group of individuals may regularly use the same cryptoasset ATMs at odd hours of the day, giving the impression they could be at a street corner, and making frequent deposits or cash outs to fund their business (see sections 7.1 and 7.2);
- some street drug dealers may be willing to accept cryptoassets directly from buyers, and then cashing out via services cryptoasset ATMs (see section 7.1);
- accounts of street drug dealers may also become highly active around major events or public holidays – such as New Year’s Eve – with dealers receiving small amounts of cryptoassets from other customers’ wallets and then cashing out immediately (see section 6.2).

## 20. Human Traffickers and Sex Trade Perpetrators

The US law enforcement takedown of Backpage.com illustrated that cryptoassets have come to play a meaningful role in at least some corners of the illicit sex trade – as well as related human trafficking activity.

Escorts – often victims forced into the trade – whose services were advertised on Backpage paid for ads using Bitcoin. The site’s administrators collected these cryptoasset payments and laundered them onwards – eventually cashing out through an elaborate network of bank accounts.<sup>99</sup>

Our research indicates that methods and typologies for using cryptoassets in human trafficking and the sex trade include the following:

- customer purchases cryptoassets at a cryptoasset ATM and makes an immediate onward transfer to addresses associated with an escort site, likely to pay for ads (see section 7.1);
- a customer’s email address, phone number or other details match to ads on escort sites;
- small value purchases of cryptoassets – worth \$3, \$12, \$20, for instance – may be made at cryptoasset ATMs, exchanges or other conversion services at late hours of the evening that would otherwise appear to have no clear legitimate business purpose;
- criminals purchase Bitcoin on P2P sites using prepaid cards and then use the Bitcoin to purchase ads<sup>100</sup> (see section 8);
- escort sites may use cryptoasset payment processors to facilitate purchases from customers, sometimes relying on front companies to create the appearance that the payments relate to legitimate business activities unconnected to the sex trade<sup>101</sup>;
- victims may also be coerced into accepting cryptoassets for payment or using digital assets to make onward funds transfers to members of the criminal network who have forced them into the trade;
- where cryptoasset ATMs are used, cameras embedded in the ATMs may have footage of groups of women accompanied by males and in some cases, being forced to use the machines.

## 21. Tax Evaders

Cryptoassets and related products and services – such as newly launched tokens – can offer an attractive vessel for tax evaders seeking to conceal their wealth. Digital assets offer the prospect of storing and transferring value cross-border, outside of the formal banking system and beyond the ready purview of regulators.

Furthermore, the tax status of cryptoassets in many jurisdictions is complex and often in flux – therefore creating space for individuals to avoid declaring digital assets for tax purposes.

The following are some of the methods employed by tax evaders when using cryptoassets, and indicators of their activity:

- utilizing exchanges with lax KYC standards and, or exploiting exchanges domiciled in, or owned by companies registered in, high-risk jurisdictions and regions associated with tax evasion, such as the Caribbean (see sections 1.1 and 1.2);
- ultra-high net worth individuals (UHNWIs) may establish accounts and attempt to swap a large volume of cryptoassets at an exchange. When asked about the source of funds, they may refuse to provide information or may provide inconsistent and unconvincing information;
- customers – including UHNWIs – who claim to have cryptoassets as a result of a life event such as a divorce settlement or inheritance, but who can not provide documentary evidence of the event in question. Some individuals also attempt to move fiat funds into crypto as a method for concealing their assets during divorce or similar proceedings;
- US citizens attempt to open accounts at overseas exchanges with the aim of avoiding US tax filing requirements. They tend to be unwilling to answer questions about their activity;
- corporate entities with accounts at exchanges have a level of cryptoasset trading that is inconsistent with their stated business activities. They attempt to declare their cryptoasset holdings as technology expenditures – rather than appropriately declaring any capital gains;<sup>102</sup>
- individuals or businesses that receive income or payment for goods and services in cryptoassets – or who earn significant income from activities such as mining – seek to avoid declaring cryptoasset-related income for tax purposes;
- one typology identified by the Internal Revenue Service (IRS) involved individuals repatriating funds from offshore foreign brokerage accounts, transferring funds to a US bank, and then purchasing cryptoassets at a cryptoasset exchange. The tax evaders then used the digital assets to purchase goods and services without declaring any gains or losses made on the cryptoasset trades;<sup>103</sup>

- sending funds via mixing services to hide their ultimate origin (section 2);
- purchasing NFTs with the proceeds of tax fraud, or failing to declare taxes related to NFT sales (section 10).



#### Tax Fraud

In November 2020, a former Microsoft contractor was sentenced to nine years in prison on counts of fraud.

According to the criminal complaint against him, Volodymyr Kvashuk was hired by Microsoft to test a new online store that allows payment in digital gift cards.<sup>104</sup> During the testing phase, Kvashuk made unauthorized payments through the system and stole and sold gift cards worth \$10 million.

Kvashuk sold the gift cards for Bitcoin – including on a popular P2P exchange – and then eventually swapped the Bitcoin back into dollars at a large exchange. He moved some of the Bitcoin via ChipMixer to hide their origin before depositing them at the exchange. Kvashuk used the proceeds to purchase luxury items, such as cars and a \$1.6 million home.

Kvashuk also attempted to falsify his tax records. When filing his tax return with the IRS, he declared that he had received the Bitcoin as a gift, with a view to have them exempt from his income taxes.



#### NFT Tax Fraud

In March 2023, reports indicated that Israeli tax authorities were investigating two individuals for failing to declare income related to their sale of NFTs.

The two individuals reportedly created more than 1,000 NFTs of the Western Wall – a holy site in Jerusalem – and generated 620 Ether worth approximately \$2 million by selling the NFTs on their website [holyroknft.com](https://www.holyrocknft.com).

However, the pair never reported the income they generated from these NFT sales, and the Israeli Tax Authority alleges they deliberately attempted to shield their income to avoid paying tax.<sup>105</sup>

## 23. State Actors and Sanctions Evaders

From late 2018 to date, there has been an enormous amount of activity related to sanctioned actors and their use of cryptoassets.

Elliptic's research and available open source reporting suggests that sanctioned nations and threat actors are using cryptoassets with growing frequency, and increasing complexity in their operations.

The most notorious offender is North Korea – with credible estimates from organizations such as the United Nations pegging the country's haul of cryptoassets from exchange hacks in the hundreds of millions dollars. Equipped with a cybercriminal infrastructure engaged in ransomware, hacking and cryptojacking, North Korea has integrated cryptoasset activity as a regular feature of its sanctions evasion techniques.

Venezuela's launch of the petro is another prime example of overt sanctions evasion efforts using cryptoassets. Since 2020, Venezuela has worked to bolster its domestic network of exchanges involved in petro trading, and also indicated its intention to integrate other cryptoassets such as Bitcoin and Litecoin into its domestic payment networks.

Venezuela and Iran also enable domestic mining operations under strict government oversight. These regimes have looked to cryptoasset mining as a strategy to evade sanctions. Mining also enables these countries to harness natural resources they struggle to sell due to international sanctions. Iran in particular has turned to cryptoasset mining on a significant scale. Elliptic's research indicates that nearly 4.5% of all Bitcoin mining activity takes place in Iran – potentially netting the country as much as \$1 billion in revenues.

In response to these and other trends, in the last three years OFAC has undertaken a series of aggressive actions targeting these threat actors. Cryptoasset addresses belonging to these threat actors have been placed on its list of Specially Designated Nationals and Blocked Persons (SDN List).

Threat actors using cryptoassets that OFAC has targeted to date include the following:

- Iranian money launderers associated with the SamSam ransomware campaign;
- Chinese fentanyl traffickers;
- money launderers supporting the North Korea-linked cybercriminal Lazarus Group;
- Russian cybercriminals hacking cryptoasset exchanges;
- Russian-linked individuals involved in US election interference; and
- Cryptoasset exchanges known to facilitate money laundering on behalf of ransomware gangs.

The following include cryptoasset-enabled methods that state actors and sanctions evaders have employed to date:

- cybercriminal tactics – such as ransomware – to raise funds in Bitcoin, using methods such as layering via privacy coins, and through unregulated or non-compliant exchanges, to realize their profits (see section 1.1);
- Venezuela declaring that only approved cryptoasset exchanges can process domestic trades involving the petro, and working with governments and financial institutions in other sanctioned jurisdictions – such as Russia – to provide funding for related projects (see section 1.3);
- mining cryptoassets, either through supposed legitimate mining operations or through crypto-jacking attacks (see section 12.2);
- using cryptoassets to purchase infrastructure for use in cybercrime attacks, as in the Russian hacking of the 2016 US election. Adopting multi-service typologies to conceal the origin of their cryptoassets (see section 13.2); and
- individuals from sanctioned countries – such as Venezuela – that have also imposed capital controls, may attempt to use cryptoassets to remit funds from their home countries by cashing it out at exchanges in the US or other regions.



#### Iranian Money Launderers

On November 28th 2018, the US Department of the Treasury's Office of Foreign Assets Control (OFAC) undertook a milestone action when, for the first time, it added two Bitcoin addresses to its list of Specially Designated Nationals (SDNs).

The two addresses were controlled by Ali Khorashadizadeh and Mohammad Ghorbaniyan – Iranian-based cryptoasset brokers who moved funds for the perpetrators of the SamSam ransomware campaign. They also engaged in other cryptoasset transactions totalling more than \$17 million using the two OFAC-listed addresses alone.

The November 2018 OFAC action is notable not only because it was the first time cryptoasset addresses were singled out for sanction purposes. By listing specific addresses belonging to known facilitators of illicit cryptoasset activity, the US Treasury provided our team at Elliptic with the clues required to allow us to understand in detail how these actors operate.

Elliptic's response to the OFAC action was swift: we immediately updated our systems to clearly label the two OFAC-listed addresses. Furthermore, we were able to detect two additional Bitcoin addresses in the same wallet as the OFAC-listed addresses, not explicitly mentioned by the organization in its action. This is significant considering all of these addresses can be associated with the individuals on the SDN list. If you are unaware of these additional addresses you run the risk of unknowingly transacting with these individuals.

Adding these addresses to our tool has enabled compliance officers using our AML software to identify potential links to the sanctioned persons and identify historical activity of concern.

We learned a tremendous amount about how Khorashadizadeh and Ghorbaniyan were operating.

By examining Bitcoin blockchain data, we can see that they were prolific Bitcoin users. They had engaged in thousands of transactions for many years to move funds – before being added to the OFAC SDN list.

These are the methods they used below:

- targeting the now-defunct BTC-e exchange – which was a favored exchange for global criminals – to swap cryptoassets;
- using peer-to-peer trading platforms to facilitate business;
- using dozens of compliant exchanges in the US, Europe and Asia;
- relying on cryptoasset payment processing services in the US and Europe to make direct purchases for items using Bitcoin;
- the use of cryptoasset debit card services;
- moving funds via gambling sites that accept cryptoassets; and
- using at least one decentralized exchange (DEX) platform.

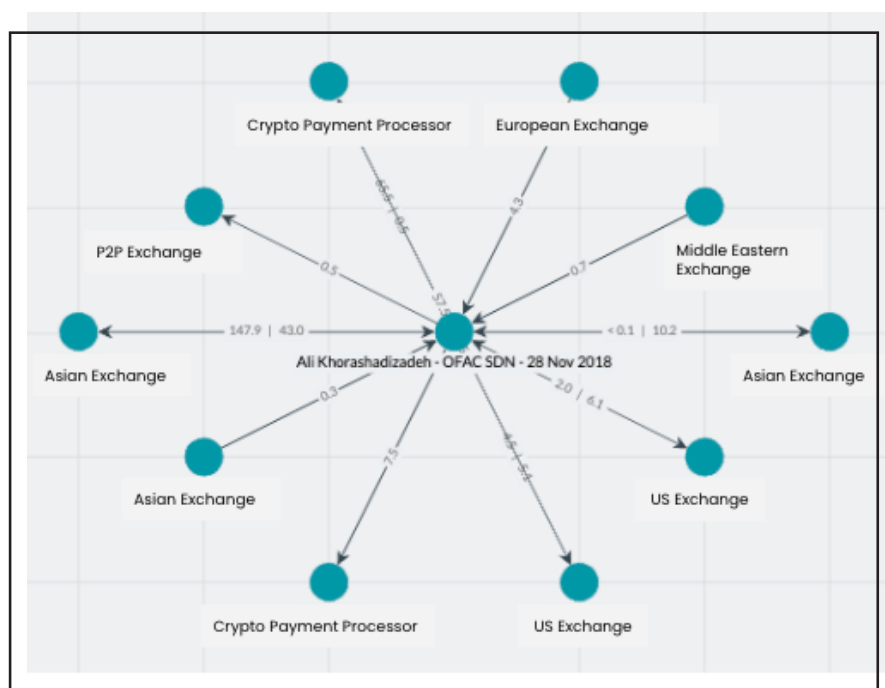
This activity demonstrates that OFAC hit the mark by targeting adept and prolific users of cryptoassets. It also illustrates that all types of cryptoasset platforms – even those that strive to be compliant – must be alert to the risk of exposure to sanctioned parties.



As the image below shows, prior to his listing by OFAC, Khorashadzadeh transacted with P2P exchange platforms, centralized exchanges and crypto payment processors – many of them outside Iran. Listing his Bitcoin address will ensure that many of those platforms do not interact with that address again.

This does not confirm that sanctions actions targeting these activities are fool-proof. Reporting suggests that Ghorbaniyan has used Perfect Money – a centralized online value transfer system – to skirt sanctions. He also claims to have created a new Bitcoin address that has not been listed publicly.<sup>106</sup>

Having the ability to monitor potential interactions with the two OFAC-listed entities is a critical step in any cryptoasset business’s sanctions compliance journey.



The image above from Elliptic Investigator shows that the OFAC SDN Ali Khorashadzadeh had numerous interactions with crypto exchanges and other service providers located globally.



The link between ransomware and financial and economic sanctions first became apparent in May 2017 with the launch of the WannaCry ransomware attack, which infected hundreds of thousands of computers around the world, and inflicted billions of dollars worth of damages to impacted businesses and organizations.

That breach was soon attributed to the Lazarus Group – a North Korean cybercrime gang – which has been using cybercrime as a way to generate funds for North Korea’s cash-starved regime. The US Department of the Treasury’s Office of Foreign Assets Control (OFAC) later sanctioned the Lazarus Group, prohibiting US persons from making or facilitating payments to the organization.

In November 2018, OFAC undertook a milestone action when it sanctioned two Iranian nationals the US accused of laundering Bitcoin on behalf of ransomware perpetrators. As part of that action, OFAC listed on its Specially Designated Nationals and Blocked Persons List (SDN List) two Bitcoin addresses belonging to the Iranian money launderers. It was the first time OFAC had ever included crypto addresses on the SDN List, and sent a clear message that the US would seek to disrupt crypto activity that facilitated crimes such as ransomware.

In October 2020, OFAC issued guidance entitled “Potential Sanctions Risks for Facilitating Ransomware Payments”, which it later updated in September 2021. The guidance aimed to clarify for the private sector and individuals the potential sanctions implications they could face when making or facilitating ransomware payments.

The guidance clarified that it is forbidden for US persons to make or facilitate ransomware payments to sanctioned entities or individuals, or to ransomware campaigns undertaken by individuals in sanctioned jurisdictions. OFAC also warned that ransomware payments can result in a sanctions violation if those payments ultimately benefit a sanctioned person or jurisdiction, even if that connection is not apparent at the time the payment was made.

As the scale of ransomware attacks grew across 2021 and into 2022, so too did OFAC’s response. Between September 2021 and April 2022, the agency sanctioned three cryptoasset exchanges registered in Eastern Europe – SUEX, Chatex, and Garantex – that it accused of laundering crypto on behalf of ransomware gangs. In April 2022, OFAC also sanctioned the Hydra darknet marketplace, which had played a critical role in facilitating activity on behalf of ransomware gangs and their affiliates before it was taken down by German law enforcement.

In February 2023, OFAC undertook a coordinated, joint action alongside the UK's Office of Financial Sanctions Implementation (OFSI) to target ransomware perpetrators. OFAC and the OFSI both sanctioned seven Russian nationals allegedly associated with the Trickbot malware, and who are also associated with the Conti and Ryuk ransomware campaigns. While neither OFAC nor OFSI included crypto addresses belonging to the individuals on their sanctions lists, at Elliptic we identified 53 addresses belonging to six of the seven sanctioned cybercriminals.

As sanctions authorities like OFAC and the OFSI increasingly target ransomware gangs and their support networks, it is critical that compliance teams can identify related transactional typologies and red flags. Some key red flags include:

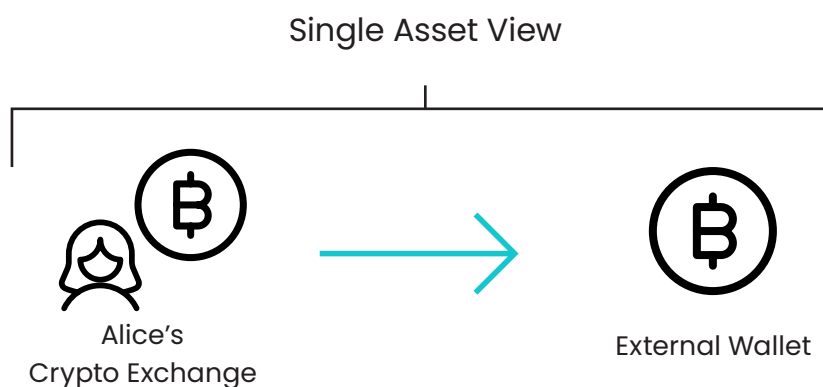
- direct transactions with the crypto wallets of sanctioned cybercriminals;
- transactions sent through intermediary unhosted wallets that have significant exposure to sanctioned cybercriminals' wallets;
- the use of "peeling chain" techniques to transfer funds through numerous intermediary wallets with the aim of breaking the connection back to the original source of funds;
- transactions involving cryptoasset exchanges that have been sanctioned by OFAC for supporting ransomware gangs;
- transactions involving cryptoasset exchanges in high-risk jurisdictions associated with ransomware, such as Russia and Iran;
- transactions involving cryptoasset exchanges with weak or no AML/CFT controls;
- the frequent use of anonymizing services – such as mixers and privacy wallets – known to facilitate transfers with ransomware attackers, such as the ChipMixer service, which was dismantled by law enforcement in March 2023;
- transfers made through coinswapping services that allow users to swap Bitcoin for privacy-enhanced cryptoassets such as Monero; and
- transfers made through one or several cross-chain or cross-asset services, which can be indicative of "chain-hopping" typologies of money laundering.

Detecting ransomware activity with a sanctions nexus requires having access to blockchain analytics solutions that can identify these and other indicators of risk. In particular, it is essential that compliance teams can spot instances where funds are swapped across assets and blockchains with the involvement of sanctioned actors.

Elliptic's unique Holistic Screening capabilities can enable the detection of these risks, ensuring that compliance teams can identify exposure to sanctioned entities among their customers' transactions. Ransomware attackers may use services such as decentralized exchanges (DEXs), which allow them to swap assets seamlessly, and cross-chain bridges, which facilitate the movement of funds across different blockchains, in order to obscure a sanctions nexus to their activity.

To understand the importance of Holistic Screening in detecting sanctions risks related to ransomware, consider the following scenario:

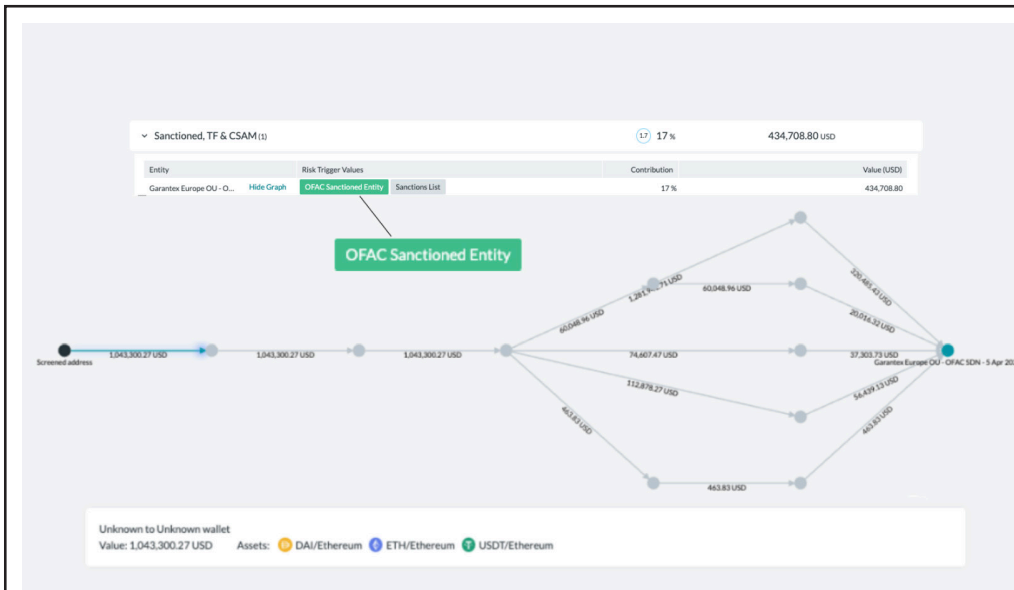
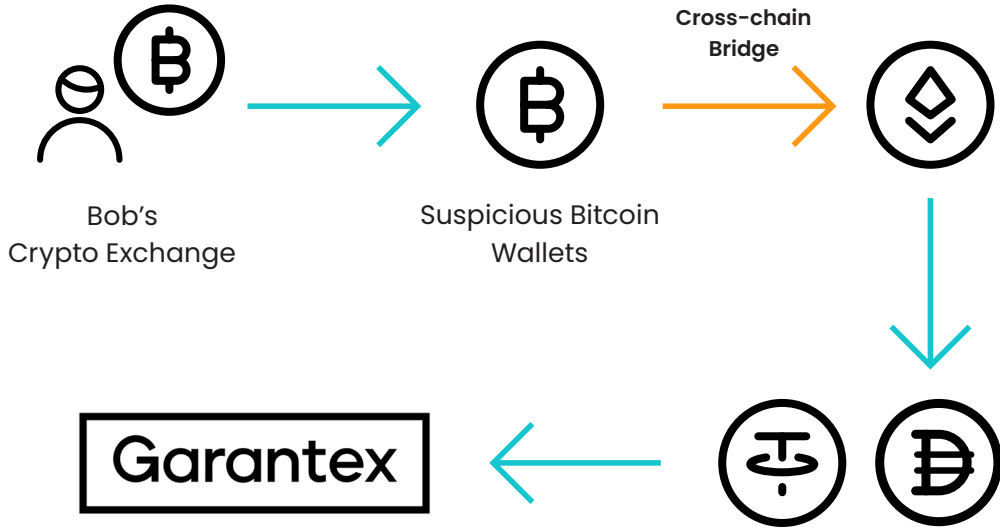
A cryptoasset exchange's customer has withdrawn Bitcoin to a private wallet. When screening the private Bitcoin wallet using blockchain analytics that only enable a single-asset view of sanctions risks, the exchange determines that there are no risks associated with the transaction. This is illustrated in the image below.



However, when using Elliptic's unique Holistic Screening capabilities, we can go deeper. In this case, it turns out that the funds did not stop at the Bitcoin wallet, but rather, were transferred onwards and swapped for Ether at a cross-chain bridge service. Following the conversion to Ether, the funds were swapped again for the stablecoins Dai and Tether at a DEX. From there, the funds were sent to the OFAC-sanctioned cryptoasset exchange Garantex. This sequence of transfers is illustrated in the image below.

This is an increasingly common typology of money laundering deployed by ransomware attackers. With Elliptic's Holistic Screening solutions, compliance teams can obtain insights into these activities seamlessly through a single screening, enabling them to respond to transactions efficiently and at scale, for example by closing or blocking accounts associated with sanctions-related activity.

## Sanctions Screening - the Impact of Holistic Screening



This image from Elliptic Navigator shows the flow of funds from a ransomware attacker's Ethereum address (the black circle on the left) and the subsequent trail after the funds were converted for DAI and Tether, before being deposited at Garantex, an OFAC-sanctioned exchange (represented by the green circle on the right).

## Preventing Exposure to Sanctions

Controls used for identifying exposure to sanctions risks include the following:

- comprehensively screening all customers against sanctions lists issued by the US, EU, UN and other relevant authorities;
- comprehensively screening all transactions and wallets against cryptoasset addresses listed by OFAC, using screening solutions such as Elliptic Lens and Elliptic Navigator;
- blacklisting Bitcoin addresses associated with exchanges known to operate from a sanctioned jurisdiction;
- prohibiting customer log-ins from sanctioned jurisdictions;
- prohibiting customers from logging in using VPNs;
- exercising extra scrutiny over transactions involving activities such as ransomware and mining where there are suspected interactions with sanctioned jurisdictions or persons; and
- blocking customer accounts where a customer adds an email address, phone number or other data point related to a sanctioned jurisdiction.

## 24. Terrorists and Political Extremists

Terrorists and political extremists are making use of cryptoassets for crowdfunding campaigns, and for making P2P transfers to other members of their networks.

Recent trends and behaviors observed among terrorist and extremist actors that warrant further monitoring include:

- Using privacy coins, particularly where a group's Bitcoin addresses have been the subject of public and press scrutiny (see section 5);
- the use – in at least one case – of embedded mining tools to enable donors to supply a neo-Nazi organization directly with newly minted Monero – allowing donors to bypass exchanges (see section 5);
- jihadist and extremist organizations providing supporters with instructions – generally via social media – on how to use cryptoasset-related services such as cryptoasset ATMs, and instructing supporters to purchase digital assets from specific exchanges (see section 7);
- Using fraudulently-obtained debit and credit cards to purchase cryptoassets (see section 8);
- Bitcoin coupons for the purchase of cryptoassets – similar to prepaid card typologies (see section 8);
- reliance on wallet-specific techniques to hide funds flows (see section 6); and
- use of exchanges in jurisdictions that present high terrorist financing risks (see section 1).

# Index

1. Financial Action Task Force, Virtual Asset Red Flag Indicators of Money Laundering and Terrorist Financing, September 2020, <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf>, p. 17.
2. This typology is gathered from numerous publicly available law enforcement reports from the US and EU, as well as knowledge drawn from Elliptic's network of compliance officers.
3. Testimony of Kathryn Huan Rodriguez before the US House of Representatives Committee on Financial Services Subcommittee on Terrorism and Illicit Finance, June 8th 2017, <https://financialservices.house.gov/uploadedfiles/hhrg-115-ba01-wstate-khaun-20170608.pdf>
4. United States Department of the Treasury, "Treasury Takes Robust Actions to Counter Ransomware," September 21st 2021, <https://home.treasury.gov/news/press-releases/jy0364>
5. David Carlisle, "OFAC Ransomware Crackdown Targets SUEX Crypto Exchange That Has Received More than \$900 Million," Elliptic blog, September 21st 2021, <https://www.elliptic.co/blog/ofac-ransomware-crackdown-targets-suex-crypto-exchange-that-has-received-more-than-900-million>
6. Anna Baydakova, "Chatex Users Ask US Treasury to Release Crypto Frozen by Sanctions," CoinDesk, December 13th 2021, <https://www.coindesk.com/policy/2021/12/13/chatex-users-ask-us-treasury-to-release-crypto-frozen-by-sanctions/>
7. United States Department of the Treasury, "Treasury Sanctions Russia-Based Hydra, World's Largest Darknet Market, and Ransomware-Enabling Virtual Currency Exchange Garantex," April 5th 2022, <https://home.treasury.gov/news/press-releases/jy0701>
8. Europol, 2017 Virtual Currencies Money Laundering Typologies: Targeting Exchanges and Other Gatekeepers, p. 10.
9. Aziz Abdel Qater, "16 Cryptocurrency Exchanges Get Approval to Launch in Venezuela, List Petro," Finance Magnates, April 30th 2018, <https://www.financemagnates.com/cryptocurrency/news/16-cryptocurrency-exchanges-get-approval-launch-venezuela-list-petro/>
10. United States of America vs. Anthony R Murgio, sentencing submission, June 20th 2017, p.7, <https://regmedia.co.uk/2017/06/27/murgiosentencingsubmission.pdf>.
11. Catalin Cimpanu, "95% of All Ransomware Payments Were Cashed out via BTC-e Platform," Bleeping Computer, July 27th 2017.



12. United States of America v. BTC-e, a/k/a Canton Business Corporation and Alexander Vinnik, superseding indictment, p.2, <https://www.justice.gov/usao-ndca/press-release/file/984661/download>.
13. United States Department of the Treasury Financial Crimes Enforcement Network, Assessment of Civil Monetary Penalty, July 26th 2017, p.5 [https://www.fincen.gov/sites/default/files/enforcement\\_action/2017-07-26/Assessment%20for%20BTCeVinnik%20FINAL%20SignDate%2007.26.17.pdf](https://www.fincen.gov/sites/default/files/enforcement_action/2017-07-26/Assessment%20for%20BTCeVinnik%20FINAL%20SignDate%2007.26.17.pdf).
14. Geoff White, "UK company linked to laundered Bitcoin billions," BBC News, March 7th 2018, <https://www.bbc.co.uk/news/technology-43291026>; see Companies House entry for Always Efficient LLP, <https://beta.companieshouse.gov.uk/company/OC394172/filing-history>
15. Ibid., p.3.
16. "Prepared Remarks of FinCEN Director Kenneth A. Blanco, delivered at the Chicago-Kent Block (Legal) Tech Conference," August 9th 2018, <https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-2018-chicago-kent-block>
17. United States Department of the Treasury Financial Crimes Enforcement Network, "FinCEN Identifies Virtual Currency Exchange Bitzlato as a 'Primary Money Laundering Concern' in Connection with Russian Illicit Finance," January 18th 2023, <https://www.fincen.gov/news/news-releases/fincen-identifies-virtual-currency-exchange-bitzlato-primary-money-laundering>
18. "How Chinese Crypto Money Laundering Networks Enable Money Laundering Cartels," The New Lens, January 14th 2019, <https://international.thenewslens.com/article/111965>
19. "Chinese Authorities in Guangdong Province Freeze 4,000 Banks Allegedly Linked to OTC Cryptocurrency Desks Engaging in Money Laundering," June 15th 2020, <https://www.crowdfundinsider.com/2020/06/162760-chinese-authorities-in-guangdong-province-freeze-4000-banks-allegedly-linked-to-otc-cryptocurrency-desks-engaging-in-money-laundering/>
20. Steve Goodrich, "From Russia with Crypto: Moscow-Based Exchanges Offering to Anonymously Convert Stablecoins for Cash in the UK," Transparency International, March 15th 2023, <https://www.transparency.org.uk/Russia-cryptocurrency-exchange-UK-money-laundering-investigation-USDT>
21. Anna Tims, "Money mules: how young people are lured into laundering cash," The Guardian, October 4th 2021, <https://www.theguardian.com/money/2021/oct/04/money-mules-laundering-cash-students-funds-bank-accounts>

22. "Eastern District of Texas Announces Multi-Year Investigation Into Transnational Cryptocurrency Money Laundering Networks," US Department of Justice, November 30th 2022, <https://www.justice.gov/usao-edtx/pr/eastern-district-texas-announces-multi-year-investigation-transnational-cryptocurrency>
23. Matthew Hughes, "Exclusive: Cyber-criminals are selling victim's selfies on the dark web," The Next Web, March 12th 2018, <https://thenextweb.com/security/2018/03/12/exclusive-cyber-criminals-selling-victims-selfies-dark-web/>
24. "Ohio Resident Charged with Operating Darknet-Based Bitcoin 'Mixer' Which Laundered Over \$300 Million," US Department of Justice, February 13th 2020, <https://www.justice.gov/opa/pr/ohio-resident-charged-operating-darknet-based-Bitcoin-mixer-which-laundered-over-300-million>
25. "Individual Arrested and Charged with Operating Notorious Darknet Cryptocurrency 'Mixer'," United States Department of Justice, April 28th 2021, <https://www.justice.gov/opa/pr/individual-arrested-and-charged-operating-notorious-darknet-cryptocurrency-mixer>
26. "First Bitcoin "Mixer" Penalized by FinCEN or Violating Anti-Money Laundering Laws," Financial Crimes Enforcement Network," October 19th 2020, <https://www.fincen.gov/news/news-releases/first-Bitcoin-mixer-penalized-fincen-violating-anti-money-laundering-laws>
27. "Assessment of Civil Money Penalty in the Matter of Larry Dean Harmon, d/b/a Helix," Financial Crimes Enforcement Network," Annex A, p. 1, [https://www.fincen.gov/sites/default/files/enforcement\\_action/2020-10-19/HarmonHelix%20Assessment%20and%20SoF\\_508\\_101920.pdf](https://www.fincen.gov/sites/default/files/enforcement_action/2020-10-19/HarmonHelix%20Assessment%20and%20SoF_508_101920.pdf)
28. United States of America vs. Larry Dean Harmon, p. 2 <https://www.justice.gov/opa/press-release/file/1249026/download>
29. Ibid, p.3.
30. "Assessment of Civil Money Penalty in the Matter of Larry Dean Harmon, d/b/a Helix," Financial Crimes Enforcement Network," Attachment A, p.1, [https://www.fincen.gov/sites/default/files/enforcement\\_action/2020-10-19/HarmonHelix%20Assessment%20and%20SoF\\_508\\_101920.pdf](https://www.fincen.gov/sites/default/files/enforcement_action/2020-10-19/HarmonHelix%20Assessment%20and%20SoF_508_101920.pdf)
31. Ibid.
32. Ibid, p. 2.
33. ERC-20 refers to a technical standard used to implement the launch of new tokens on the Ethereum blockchain.

34. FATF Report to the G20 Ministers and Central Bank Governors on So-Called Stablecoins, FATF, June 2020,
35. Zhang Yuze and Denise Jia, "How illegal online gambling launders \$150 million from China," Nikkei Asia, December 22nd 2020, <https://asia.nikkei.com/Spotlight/Caixin/How-illegal-online-gambling-launders-150bn-from-China>
36. Sam Reynolds, "US Drug Enforcement Agency Seized \$1.8M From Binance in 2022," CoinDesk, February 24th 2023, <https://www.coindesk.com/business/2023/02/24/us-drug-enforcement-agency-seized-18m-from-binance-in-2022/>
37. Ana Alexandre, "New Study Says 80 Percent of ICOs Conducted in 2017 Were Scams," CoinTelegraph, July 13th 2018, <https://cointelegraph.com/news/new-study-says-80-percent-of-icos-conducted-in-2017-were-scams>
38. Wassayos Ngamkham, "Fraudsters adopt Bitcoin to evade cops," Bangkok Post, August 13th 2018, <https://www.bangkokpost.com/news/general/1520574/>
39. Anthony Cuthbertson, "Bitcoin Millionaire Loses \$35 Million in Cryptocurrency Scam," August 15th 2018, <https://www.independent.co.uk/life-style/gadgets-and-tech/news/Bitcoin-millionaire-cryptocurrency-scam-thailand-a8492606.html>
40. "Japan cryptocurrency exchange to refund stolen \$400 million," The Guardian, January 28th 2018, <https://www.theguardian.com/technology/2018/jan/28/japan-cryptocurrency-exchange-coincheck-refund-stolen-nem>
41. Sebastian Sinclair, "Tether Froze \$300k of Stablecoin Hacked After Victims Left Wallet Keys in Evernote," Coindesk, October 26th 2020, <https://www.coindesk.com/tether-froze-300k-of-stablecoin-hacked-after-victims-left-wallet-keys-in-evernote>
42. David Z. Morris, "The Rise of Cryptocurrency Ponzi Schemes," The Atlantic, May 31st 2017, <https://www.theatlantic.com/technology/archive/2017/05/cryptocurrency-ponzi-schemes/528624/>
43. The term "privacy coins" refers to cryptoassets that integrate anonymizing techniques (such as the use of stealth addresses, ring signatures, or zk-SNARKs) as part of their design and that feature blockchains that do not reveal full details of counterparties and transactions. Privacy coins contrast to more transparent digital assets, such as Bitcoin or Litecoin, that require a third party mixing service to achieve similar anonymizing effects.
44. Ryan Browne, "Hackers have cashed out on \$143,000 of Bitcoin from the massive WannaCry ransomware attack," CNBC.com, August 3rd 2017, <https://www.cnbc.com/2017/08/03/hackers-have-cashed-out-on-143000-of-Bitcoin-from-the-massive-wannacry-ransomware-attack.html>

45. "Bithumb Has Recovered Nearly Half of Funds Stolen in Last Week's Hack," CCN, June 28th 2018, <https://www.ccn.com/bithumb-has-recovered-nearly-half-of-funds-stolen-in-last-weeks-hack/>
46. See CoinATM Radar data.
47. This basic typology has been derived from Europol reports, numerous press articles, and discussions with members of the Elliptic compliance officer network.
48. Koos Couvee, "European Traffickers Pay Colombian Cartels Through Bitcoin ATMs: Europol Official," ACAMS Moneylaundering.com, February 28th 2018, [http://files.acams.org/pdfs/2018/280218\\_European\\_Traffickers\\_Pay\\_Colombian\\_Cartels\\_Through\\_Bitcoin\\_ATMs.pdf](http://files.acams.org/pdfs/2018/280218_European_Traffickers_Pay_Colombian_Cartels_Through_Bitcoin_ATMs.pdf)
49. Europol, "Virtual Currencies Money Laundering Typologies: Targeting Exchanges and Other Gatekeepers," p. 9.
50. Couvee, "European Traffickers Pay Colombian Cartels Through Bitcoin ATMs: Europol Official."
51. "Cryptocurrency laundering as a service: members of a criminal organization arrested in Spain," Europol press release, May 8th 2019, <https://www.europol.europa.eu/newsroom/news/cryptocurrency-laundering-service-members-of-criminal-organisation-arrested-in-spain>
52. Jessi Schultz "3 men, 1 business charged in cryptocurrency scam; avoid Bitcoin of America ATMs, Cuyahoga Co. prosecutor says," News 5 Cleveland, March 2nd 2023, <https://www.news5cleveland.com/news/local-news/3-men-1-business-charged-in-cryptocurrency-scam-avoid-bitcoin-of-america-atms-cuyahoga-co-prosecutor-says>
53. This typology is adapted from descriptions of criminal activity in public reports issued by Europol.
54. JP Buntinx, "Criminals Direct Money Mules Bitcoin ATMs Launder Hacked Funds," NewsBTC, September 30th 2016, <https://www.newsbtc.com/2016/09/30/criminals-direct-money-mules-bitcoin-atms-launder-hacked-funds/>; "Teamviewer Money Mules" BitBargain blog, March 3rd 2016, <http://blog.bitbargain.com/post/140405376397/teamviewer-money-mules-facebook-bitcoin-fraud-victims-in>
55. Cameron Cooper, "Beware of Bitcoin fake tax debits scam," In the Black, May 21st 2018, <https://www.intheblack.com/articles/2018/05/21/Bitcoin-fake-tax-debits-scam>; Katie DeRosa, "Victoria man loses \$11,000 in Bitcoin-ATM tax scam," Times Colonist, 29 March 2018, <https://www.timescolonist.com/news/local/victoria-man-loses-11-000-in-bitcoin-atm-tax-scam-1.23245878>
56. Robert Johnson, "Hawaii's Latest Bitcoin Scam," CryptoDaily, August 20th 2018, <https://cryptodaily.co.uk/2018/08/hawaiis-latest-bitcoin-scam/>

57. "Cryptocurrency Investment Schemes," Federal Bureau of Investigation, October 3rd 2022, <https://www.ic3.gov/Media/Y2022/PSA221003>
58. Matt Burgess, "Inside the takedown of the alleged lbn cyber bank robber," April 4th 2018, Wired, <https://www.wired.co.uk/article/carbanak-gang-malware-arrest-cybercrime-bank-robbery-statistics>
59. "Mastermind Behind EUR 1 Billion Cyber Bank Robbery Arrested in Spain," Europol press release, March 26th 2018, <https://www.europol.europa.eu/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain>
60. TRACFIN, Rapport analyse TRACFIN 2016, <https://www.economie.gouv.fr/files/rapport-analyse-tracfin-2016.pdf>
61. Lorenzo Francheschi-Bicchieri, "Alleged 19-Year-Old SIM Swapper Used Stolen Bitcoin to Buy Luxury Cars," Motherboard, August 22nd 2018, [https://motherboard.vice.com/en\\_us/article/wjka95/sim-swapper-arrest-Bitcoin-luxury-cars](https://motherboard.vice.com/en_us/article/wjka95/sim-swapper-arrest-Bitcoin-luxury-cars).
62. Tom Robinson, "One of the World's Most Prolific Cybercriminals Has Retired - And May Well Be a Billionaire," Elliptic blog, February 12th 2021, <https://www.elliptic.co/blog/jokers-stash-retiring>
63. "Supplemental Advisory on Identifying and Reporting Human Trafficking and Related Activity," FinCEN Advisory, October 15th 2020, [https://www.fincen.gov/sites/default/files/advisory/2020-10-15/Advisory%20Human%20Trafficking%20508%20FINAL\\_0.pdf](https://www.fincen.gov/sites/default/files/advisory/2020-10-15/Advisory%20Human%20Trafficking%20508%20FINAL_0.pdf)
64. "Long Island Woman Sentenced to 13 Years' Imprisonment for Providing Material Support to ISIS," US Department of Justice, March 13th 2020, <https://www.justice.gov/opa/pr/long-island-woman-sentenced-13-years-imprisonment-providing-material-support-isis>
65. "Treasury Sanctions Individuals Laundering Cryptocurrency for Lazarus Group," US Department of the Treasury, March 2nd 2020, <https://home.treasury.gov/news/press-releases/sm924>
66. "NFT Sales Surge to \$10.7 billion in Q3 As Crypto Asset Frenzy Hits New Highs," Reuters, October 5th 2021, <https://gadgets.ndtv.com/cryptocurrency/news/cryptocurrency-nft-sales-surge-q3-2021-usd-10-7-billion-buying-frenzy-opensea-dappradar-2564362>
67. Taylor Locke, "NFT trading volume hit \$10.7 billion last quarter -here are 2 reasons why people are spending thousands on digital assets," CNBC, October 6th 2021, <https://www.cnbc.com/2021/10/06/nft-trading-volume-hit-10-billion-2-reasons-why-people-are-buying.html#:~:text=NFT%2C%20or%20nonfungible%20token%2C%20trading,in%20particular%2C%20fueled%20this%20growth>.

68. For further analysis of this case, see, Elliptic, "Was Bansky Hacked to Sell a Fake NFT for \$360,000?" August 31st 2021, <https://www.elliptic.co/blog/was-a-fake-banksy-nft-just-sold-for-336000>
69. This is adapted from Elliptic's report NFTs and Financial Crime.
70. This case study is derived from Elliptic's report NFT and Financial Crime.
71. "Crypto Addresses Holding NFTs Worth \$532k are Among the Latest Sanctioned by OFAC," Elliptic blog, November 9th 2021, <https://www.elliptic.co/blog/crypto-addresses-holding-nfts-worth-532k-are-among-latest-sanctioned-by-ofac>
72. Citi, Metaverse and Money, March 30th 2022, [https://icg.citi.com/icghome/what-we-think/citigps/insights/metaverse-and-money\\_20220330](https://icg.citi.com/icghome/what-we-think/citigps/insights/metaverse-and-money_20220330)
73. Europol, Virtual Currencies Money Laundering Typologies: Targeting Exchanges and Other Gatekeepers, pp. 8 – 9.
74. Tom Robinson, "How the DOJ Indictment of Russian Hackers is Supported by Blockchain Analysis," July 24th 2018, <https://www.elliptic.co/our-thinking/doj-indictment-russian-hackers-blockchain-analysis>
75. "N. Korea appears to have tried cryptoasset mining," Yonhap News Agency, August 27th 2017, <http://english.yonhapnews.co.kr/news/2018/08/27/0200000000AEN20180827007700320.html>
76. Kevin Helms, "Iran Licenses 14 Bitcoin Mining Farms, Cuts Electricity Tariff up to 47% for Miners," Bitcoin.com, July 14th 2020, <https://news.Bitcoin.com/iran-licenses-Bitcoin-mining-farms-cuts-electricity-tariff/>
77. Arnab Shone, "Venezuelan Government Takes Control of Crypto Mining Industry," Finance Magnates, September 24th 2020, <https://www.financemagnates.com/cryptocurrency/news/venezuelan-government-takes-control-of-crypto-mining-industry/>
78. "N. Korea appears to have tried cryptocurrency mining," Yonhap News Agency, August 27th 2017, <http://english.yonhapnews.co.kr/news/2018/08/27/0200000000AEN20180827007700320.html>
79. Vincent He, "China-based Lubian.com Boasts the Largest Compliant Bitcoin Mining Farm in Iran," 8BTC, August 12th 2020, <https://news.8btc.com/china-based-lubian-com-boasts-the-largest-compliant-Bitcoin-mining-farm-in-iran>
80. FATF, Professional Money Laundering Networks, July 2018, pp.25 – 26, <http://www.fatf-gafi.org/media/fatf/documents/Professional-Money-Laundering.pdf>

81. Ibid, p. 15.
82. Brett Forrest and Justin Scheck, "Jihadists See a Funding Boon in Bitcoin," Wall Street Journal, February 20th 2018, <https://www.wsj.com/articles/jihadists-see-a-funding-boon-in-Bitcoin-151913160>
83. "Global Disruption of Three Terror Finance Cyber-Enabled Campaigns," US Department of Justice, August 13th 2020, <https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns>.
84. " Hamas-Linked Wallets Have Received \$7.7 million in Cryptoassets, Including Dogecoin," Elliptic blog, July 7th 2021, <https://www.elliptic.co/blog/hamas-linked-wallets-have-received-7.3-million-in-cryptoassets>
85. See BTC-e superseding indictment, p. 11.
86. Yaya J. Fanusie, "The New Frontier in Terror Fundraising: Bitcoin," The Cipher Brief, August 24th 2016, <http://www.defenddemocracy.org/media-hit/yaya-j-fanusie-the-new-frontier-in-terror-fundraising-Bitcoin/>
87. FATF, Financing of Recruitment for Terrorist Purposes, January 2018, p.20, <https://www.fatf-gafi.org/media/fatf/documents/reports/Financing-Recruitment-for-Terrorism.pdf>
88. "Cryptocurrency: Cardiff terrorist Khuram Iqbal jailed over trading," BBC.com, December 21st 2021, <https://www.bbc.co.uk/news/uk-wales-59748896>
89. "Hate Symbols in the Blockchain Used to Flag Crypto Fundraising by Neo-Nazis," December 8th 2021, <https://www.elliptic.co/blog/blockchain-hate-symbols-flag-crypto-fundraising-by-neo-nazis>
90. "Far Right European Terrorist Group Crowdfunding Cryptocurrency," Counter Extremism Project, August 28th 2018, <https://www.counterextremism.com/blog/far-right-european-terrorist-group-crowdfunding-cryptocurrency>
91. Billy Bambrough, "Bitcoin Donations to Neo-Nazis Are Climbing Ahead of This Weekend's Unite the Right Rally," Forbes, August 6th 2018, <https://www.forbes.com/sites/billybambrough/2018/08/06/Bitcoin-donations-to-neo-nazis-are-climbing-ahead-of-this-weekends-unite-the-right-rally/#4851460469ac>
92. Louise Matsakis, "This Twitter Bot Tracks Neo-Nazi Bitcoin Transactions," Motherboard, August 29th 2017, [https://motherboard.vice.com/en\\_us/article/paax7z/this-twitter-bot-tracks-neo-nazi-Bitcoin-transactions](https://motherboard.vice.com/en_us/article/paax7z/this-twitter-bot-tracks-neo-nazi-Bitcoin-transactions)
93. Julia Ebner, "The currency of the far-right: why neo-Nazis love Bitcoin," Guardian, January 24th 2018, <https://www.theguardian.com/commentisfree/2018/jan/24/Bitcoin-currency-far-right-neo-nazis-cryptocurrencies>

94. FATF, Emerging Terrorist Financing Risks, October 2015, p. 36, <http://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf>
95. Resty Woro Uniar, "Bitcoin, PayPal Used to Finance Terrorism, Indonesian Agency Says," Wall Street Journal, January 10th 2017, <https://www.wsj.com/articles/Bitcoin-paypal-used-to-finance-terrorism-indonesian-agency-says-1483964198>
96. "Long Island Woman Indicted for Bank Fraud and Money Laundering to Support Terrorists," US Department of Justice, December 14th 2017, <https://www.justice.gov/usao-edny/pr/long-island-woman-indicted-bank-fraud-and-money-laundering-support-terrorists>
97. "France arrests 29 in anti-terror Syria financing sting," September 29th 2020, <https://www.france24.com/en/20200929-france-arrests-29-in-anti-terror-syria-financing-sting>.
98. Mark Stockley, "How Bitcoin and the Dark Web hide SamSam in plain sight," Naked Security, August 7th 2018, <https://nakedsecurity.sophos.com/2018/08/07/how-bitcoin-and-the-dark-web-hide-samsam-in-plain-sight/>
99. FATF, Financial Flows from Human Trafficking, July 2018, p. 56 <http://www.fatf-gafi.org/media/fatf/content/images/Human-Trafficking-2018.pdf>
100. Ibid, p. 56.
101. Ibid.
102. United States Districts Court for the Northern District of California, John Doe filing, p. 8, <https://www.justice.gov/opa/press-release/file/914256/download>.
103. Ibid.
104. United States of America vs. Volodymyr Kvashuk, July 16th 2019, <https://www.courtlistener.com/recap/gov.uscourts.wawd.275443/gov.uscourts.wawd.275443.1.0.pdf>
105. "Western Wall NFT Creators Suspected of Large-Scale Tax Evasion," Jersulaem Post, March 5th 2023, <https://www.jpost.com/business-and-innovation/all-news/article-733386>
106. See: <https://brief.kharon.com/updates/iranian-cryptotrader-implicated-in-ransomware-scheme-turning-to-mysterious-payment-system/>



# About Elliptic

Elliptic is the global leader in cryptoasset risk management for crypto businesses, governments and financial institutions worldwide. Recognized as a WEF Technology Pioneer and backed by investors including J.P. Morgan, Wells Fargo Strategic Capital, SBI Group and Santander Innoventures, Elliptic has assessed risk on transactions worth several trillion dollars, uncovering activities related to money laundering, terrorist fundraising, fraud and other financial crimes. Elliptic is headquartered in London with offices in New York, Singapore and Tokyo.

## ELLIPTIC

[London](#) • [Tokyo](#) • [New York](#) • [Singapore](#)



[Connect on LinkedIn](#)



[Follow us on Twitter](#)



[Contact us at hello@elliptic.co](mailto:hello@elliptic.co)