

ELLIPTIC TYPOLOGIES REPORT 2022 EDITION

# Preventing Financial Crime in Cryptoassets

The Definitive Practical Guide  
for Governance, Risk and  
Compliance Professionals

**ELLIPTIC**

# Executive summary to the 2022 Edition

Since Elliptic released the first version of this report in 2018, the cryptoasset space has grown by leaps and bounds, evolved at incredible speed, and taken on a new face.

New innovations are transforming the cryptoasset space. Decentralized finance (DeFi), non-fungible-tokens (NFTs), stablecoins and other new facets of the ecosystem are providing alternative mechanisms for consumers to engage with cryptoassets. They are also driving the development of the “metaverse” – a burgeoning self-contained virtual ecosystem where the sale and purchase of goods, services and other complex social interactions can be facilitated cryptoassets.

These innovations have been met in parallel with a corresponding development: increasingly, banks and other institutional firms are engaging the cryptoasset space like never before. A growing number of traditional financial services firms and investors are launching cryptoasset products and services in response to insatiable client demand.

These dual trends are having an undeniable transformative impact on the cryptoasset space. The proliferation of new products and services – and the entry of traditional financial services firms into the space – offer a foundation for true mainstream adoption of cryptoassets. At Elliptic, it’s always been our vision that this will produce a financial sector that is ultimately freer, fairer and more accessible for all.

However, these developments come with inevitable risks. For example:

- DeFi presents opportunities for criminal exploitation and offers a mechanism for laundering money without the application of know-your-customer (KYC) provisions.
- NFTs offer a new potential method of money laundering using cryptoassets, as well as presenting opportunities for fraud and manipulation.
- Sanctioned actors and nation-states are proving adept at exploiting new innovations in the cryptoasset space, and for taking advantage of gaps in the regulatory framework. This risk in particular has escalated globally following the Russian invasion of Ukraine in February 2022.
- As the cryptoasset and traditional financial sectors increasingly converge, there will be new opportunities for criminals to take advantage of this complex landscape – transferring funds from the fiat currency economy to the cryptoasset ecosystem and back again.

It is therefore more important than ever for governance, risk, and compliance professionals to understand the evolving nature of illicit behaviors and financial crime typologies in the cryptoasset space.

# Our Survey: Compliance and Risk Management Practices for Cryptoassets

To better understand how compliance and risk management professionals are responding to the challenges and risks presented by cryptoassets, we conducted a survey of around 100 risk and compliance professionals across the crypto and financial sectors. The survey was conducted online in February 2022 and the complete findings will be released as a supplement to this report.

Of the around 100 respondents, 56.25% said they face “significant” or “moderate” financial crime risk from cryptoassets. Meanwhile, confidence in their ability to detect crypto-related financial crime to a high degree of accuracy was split 50/50 between “extremely” to “mostly” confident and “somewhat” to “not confident”.

Tellingly, however, over half (51.04%) of respondents already use blockchain analytics solutions for detecting financial crime, and a further 28.13% plan to do so in the future. This is reflected in Elliptic’s own growth over the last few years, where we have experienced significant appetite from crypto natives – and increasingly, financial institutions – for blockchain analytics tools.

Unsurprisingly, money laundering and fraud & scams top the list of financial crime types involving crypto that present the biggest risks to respondents – followed closely by sanctions and terrorist financing. Had we deployed this survey just a few weeks later, there is a high probability that sanctions activity would have factored higher – [given the situation in Ukraine that is rapidly evolving at the time of writing](#).

When it comes to the biggest challenge for a respondent’s business in detecting financial crime in cryptoassets, the leading answer by a wide margin was “identifying transactions that show characteristics of structuring or other money laundering behaviors”. Throughout this report, we offer insight into numerous red flags of structuring activity involving cryptoassets – but we recommend that you read Chapter 10 on “Wallet-specific Behaviors” in particular for insights into detecting this type of activity.

When asked which new cryptoasset innovation presents the greatest financial crime risks, the most popular response – chosen by nearly 47% of respondents – was DeFi. In Chapter 3 of this report, we outline typologies commonly associated with the DeFi space and give recommendations for how to spot them. To learn more about risks associated with the DeFi space, as well as compliance strategies for addressing them, you should also read Elliptic’s November 2021 report: [DeFi: Risk, Regulation, and the Rise of DeCrime](#).

We will go into greater detail with respect to the risks and typologies surrounding money laundering in the accompanying supplement to this report, but what’s clear from the survey is that compliance teams understand the criticality and risk posed by cryptoassets and recognize the need for compliance solutions to protect their business.

David Carlisle  
Director of Policy and Regulatory Affairs



**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 around  
money laundering and terrorist financing  
using cryptoassets on  
[elliptic.co](https://elliptic.co)**

# Introduction

The public discussion around cryptoassets frequently mentions their use in money laundering, terrorist financing and other financial crime. It is often anecdotal, sensationalized, and of little practical use to compliance officers at cryptoasset businesses and financial institutions, or to regulators and other governance, risk and compliance professionals.

This detailed guide to money laundering and terrorist financing typologies details the true impact on the cryptoasset industry, its users and its counterparties. Elliptic's intention is for this study to provide a meaningful contribution to the cryptoasset industry as it works to root out illicit actors.

This report is designed to equip governance, risk and compliance professionals with the knowledge and insights needed to proactively and practically:

- Identify specific money laundering and terrorist financing risks.
- Develop anti-money laundering and counter-terrorist financing (AML/CTF) governance systems.
- Evolve the controls in place to manage risk to business, customers and society.

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

- Data insights drawn from Elliptic's continuous research and analysis of blockchain data.
- Consultations with compliance officers from cryptoasset businesses about the typologies they face and risks encountered 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.

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 team will use these inputs, together with Elliptic's bespoke monitoring and analysis techniques, to uncover new typologies and bad actors – ensuring the industry can rely on the most accurate and up-to-date blockchain analytics tools.

Our intention is for this comprehensive guide to help crypto businesses and financial institutions compliance teams benchmark compliance controls and inform policy development as we work towards common goals: building trust in crypto, managing risk and maintaining the highest standards of regulatory compliance.

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 digital assets.

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

A summary view of how specific sets of illicit actors make use of the particular 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

These summarize solutions that compliance officers in Elliptic's network have devised to manage exposure to certain risks to demonstrate mitigating actions that have been effective.

# How to Use This Report

This report is designed to be a desk guide to complement Elliptic's blockchain analytics tools for compliance teams. It can be studied top to bottom for compliance analysts to become familiar with red flags or used as a reference as and when suspicious activity emerges.

The Elliptic Suite of crypto AML risk management solutions enables compliance teams, regulators and FIUs to:

- 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 compliance teams with a comprehensive set of additional red flag indicators:

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

<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	16
1.3 Use of Money Mules or Fraudulent Documents at Legitimate Exchanges	21
<b>2. Peer to Peer (P2P) Platforms</b>	<b>28</b>
<b>3. Decentralized Finance (DeFi)</b>	<b>34</b>
3.1 Money Laundering through DEXs	34
3.2 Money Laundering through DeFi Mixers	38
3.3 Money Laundering through Cross-chain Bridges	40
<b>4. Cryptoasset ATMs</b>	<b>42</b>
4.1 Facilitation of Illicit Transfers	42
4.2 Money Mule Activity	46
4.3 Victims of Scams Send Funds via Cryptoasset ATMs	48
<b>5. Cryptoasset Gambling and Gaming Services</b>	<b>52</b>
5.1 Use of Online Casinos to Clean Coins	52
5.2 Cryptoassets Swapped for In-game Currencies	53
<b>6. Cards</b>	<b>56</b>
6.1 Use of Cryptoasset Prepaid Cards to Layer Criminal Proceeds	56
6.2 Dirty Cryptoassets Used to Purchase Fiat Cards for Laundering	61
6.3 Fiat Cards Used to Purchase Cryptoassets for Illicit Purposes	63
<b>7. Mixers and Privacy Wallets</b>	<b>66</b>
<b>8. Tokens and Stablecoins</b>	<b>72</b>
8.1 Tokens Used to Clean Dirty Cryptoassets	73
8.2 Laundering of Proceeds from ICO Scams	76
8.3 Laundering of Hacked Tokens and Stablecoins	78
<b>9. NFTs</b>	<b>82</b>
9.1. NFTs and Money Laundering	82
9.2. NFTs and Fraud	83
9.3. NFTs and Theft	86



<b>10. Wallet-Specific Behaviors</b>	<b>88</b>
10.1. Chain Peeling	88
10.2. Multi-Customer Cross-wallet Activity	91
<b>11. Banks and Indirect Exposure to Cryptoasset Risks</b>	<b>92</b>
11.1. Indirect Exposure through processing VASP transactions	92
11.2. Indirect Exposure through Correspondent Relationships	94
<b>12. Privacy Coins &amp; Chain Hopping</b>	<b>96</b>
12.1. Use of Privacy Coins to Layer Illicit Proceeds	96
12.2. Laundering Illicit-origin Privacy Coins	98
<b>13. Multi-technique and Multi-service Typologies</b>	<b>102</b>
13.1. Operation Argenti	102
13.2. Russia Hacking	102
13.3. Dark Web Laundering	105
13.4. Ransomware: The Colonial Pipeline Attack	105
13.5. Other examples	106
<b>Part II: Terrorist Financing</b>	<b>108</b>
14. TF Involving Crowdfunding Through Charities and Other Organizations	109
15. TF Involving Individuals or Small Cells	114
<b>Part III: Key Trends: Criminal and Threat Actors</b>	<b>116</b>
16. Hackers and Cybercriminals	118
17. Dark Web Vendors	118
18. Fraudsters	119
19. Professional Money Launderers	119
20. Street Drug Dealers	120
21. Human Traffickers and Sex Trade Perpetrators	120
22. Tax Evaders	121
23. State Actors and Sanctions Evaders	123
24. Terrorists and Political Extremists	129
<b>Citations</b>	<b>130</b>

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 September 2020 report on cryptoasset red flags by the Financial Task Force (FATF) highlights the specific risks coming from unregulated exchanges, or those that don't have AML/CTF controls. It notes 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.

This section highlights three major money laundering typologies related to the 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.

Given that unlicensed and non-compliant exchanges often do not require any know your customer (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 have 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 exchanges should be alerted to customers whose cryptoasset transaction histories include frequent interactions with unregulated or non-compliant exchanges. Similarly, legitimate exchanges and

cryptoasset 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 perpetrator of ransomware – 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, like listing residential addresses at 123 Main Street.<sup>3</sup>
3. The criminal swaps their dirty cryptoassets for fiat currencies, or for other digital assets.
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 digital assets.
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 such as Bitcoin and Litecoin for privacy coins like Monero.

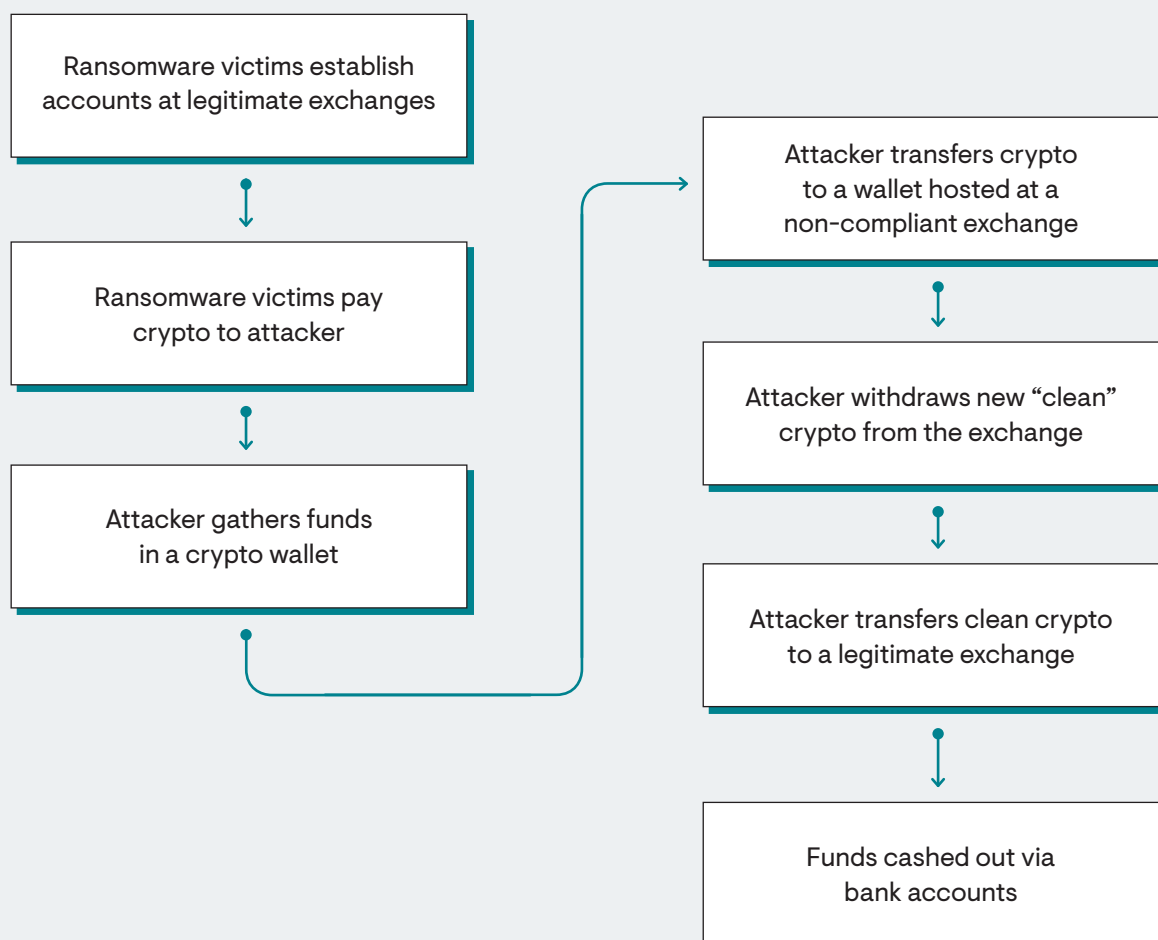
## Red Flags

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 engage in business with other non-compliant and, or opaque exchanges;
- the exchange’s website warns customers not to make mention of Bitcoin or cryptoassets when talking to external parties such as banks;

- 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 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.

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





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

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

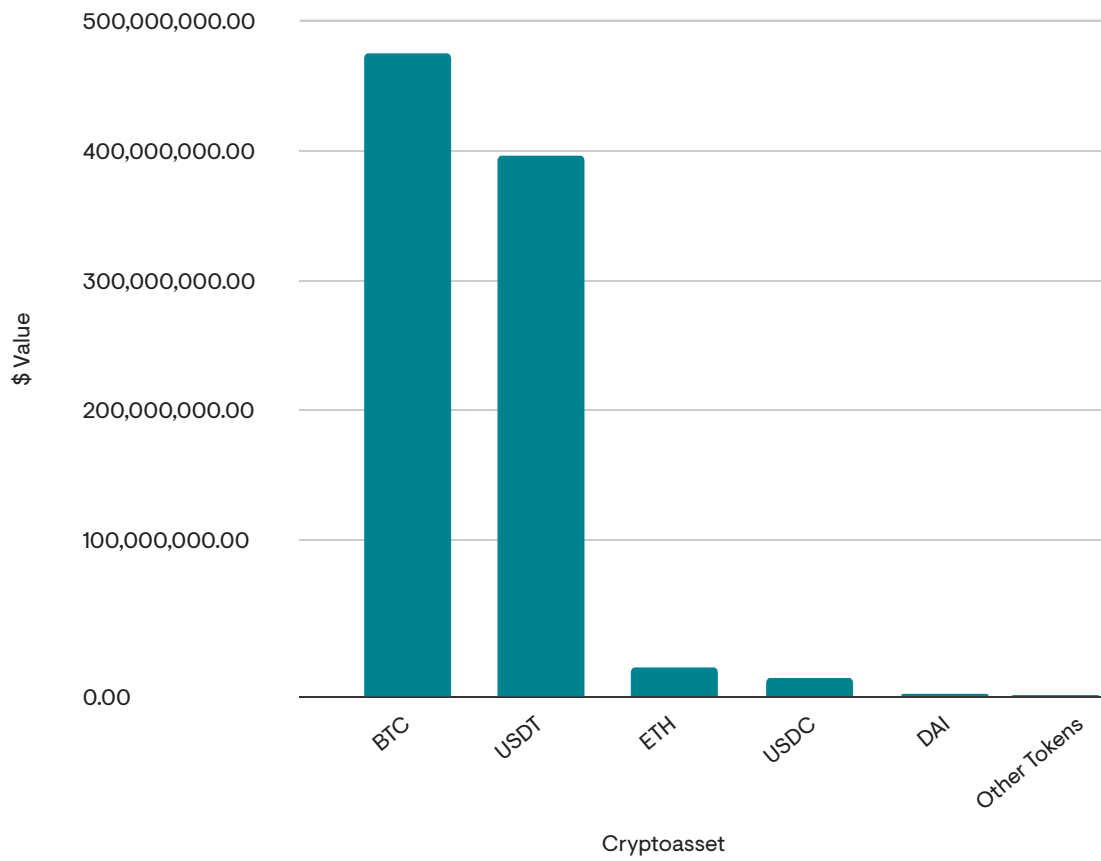
That month, OFAC placed sanctions on SUEX OTC, S.R.O. – a cryptoasset trading business registered in the Czech Republic and with operations in Russia. The company had a limited online presence, advertising boutique services for a largely Russian clientele, including enabling users to buy cryptoassets 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, which enabled ransomware perpetrators to launder their ill-gotten gains. According to OFAC, it 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. That suggests SUEX processed more than \$370 million in illicit transactions in the course of just three years, which is a substantial sum for a seemingly small exchange service.<sup>5</sup>

As part of its sanctions action targeting SUEX, OFAC included 25 Bitcoin (BTC), Ethereum (ETH), and Tether (USDT) addresses that it controlled to enable the private sector to block transactions with SUEX. Because the company 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, OFAC followed the SUEX action by placing sanctions on another exchange called 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> The sanctions targeting SUEX and Chatex 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.

### Value of cryptoassets received by SUEX addresses listed by OFAC



## 1.2 Use of Exchanges in High-risk Jurisdictions

### The Problem

Criminals will often look to exchanges that are in high-risk jurisdictions when seeking to exploit.

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 cryptoasset-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 – e.g. the Seychelles, Belize, Marshall Islands – associated with easy and non-transparent company formation;
- information on registration or legal status is unclear or contradictory with no available explanation, so it could be headquartered in Bulgaria but subject to the laws of Cyprus;
- 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 – in the Caribbean, for instance – even though nearly all its customers are located elsewhere – e.g. 75% or more are located in the EU;
- the exchange provides fiat currency trading pairs that are illogical or do not make business sense, so it could be an exchange in Finland offering high value trading in Colombian pesos<sup>7</sup>, or an exchange in Cyprus trading in Russian rubles;



- registration in a jurisdiction associated with international sanctions like 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 – the Venezuelan petro, for instance;
- the exchange has been explicitly licensed by a sanctioned jurisdiction to offer services in a state-owned cryptoasset, so the exchange could be a Venezuelan exchange authorized by the Venezuelan government to facilitate trading in the Venezuelan petro;<sup>8</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 – e.g. 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 - like the British Virgin Islands;
- reliance on payment processors in higher risk jurisdictions to process customers' fiat payments for no apparent reason – for instance, a US-based exchange uses an Azerbaijani payment processor;<sup>9</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.



## CASE STUDY

### **BTC-e**

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 a Russian national called Alexander Vinnik, 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>10</sup> According to US authorities, BTC-e engaged in a wide array of crimes "including computer hacking and ransomware, fraud, identity theft, tax refund fraud schemes, public corruption, and drug trafficking".<sup>11</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. FinCEN noted: "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."<sup>12</sup> BTC-e also allowed customers to transact after using mixers and provided customers with 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. The company 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>13</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>14</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 it to detect BTC-e's evasive behavior. He noted: "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>15</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.



#### KEY CONTROLS:

### Dealing with Unlicensed, Non-Compliant Exchanges (Including Exchanges in Higher Risk Jurisdictions)

Below are some of the controls compliance officers use to assist in the detection of unlicensed and non-compliant exchanges, including those in higher risk jurisdictions:

- Elliptic Lens and Elliptic Navigator: finds where a cryptoasset address or transaction is associated with an entity that is located in a high risk or sanctioned jurisdiction;
- Elliptic Discovery: identifies where an exchange is unlicensed, lacks KYC requirements or AML policies, or presents other high-risk factors;
- Elliptic’s Forensic software: determines if the exchange is associated with significant levels of transactions with illicit entities. This includes dark web marketplaces or Bitcoin addresses associated with ransomware or other cybercrime;
- 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).



## WARNING

### 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 on 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 on 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>16</sup> Authorities in China also undertook a major crackdown on OTC traders across 2020 – responding in part to their potential involvement in money laundering.<sup>17</sup>

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

### The Problem

Criminals will target non-compliant or unlicensed exchanges, legitimate exchanges that are subject to regulation and licensing, or those that are voluntarily compliant and have strong risk mitigation measures in place.

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. This is because the cryptoasset industry is online, and not face-to-face.

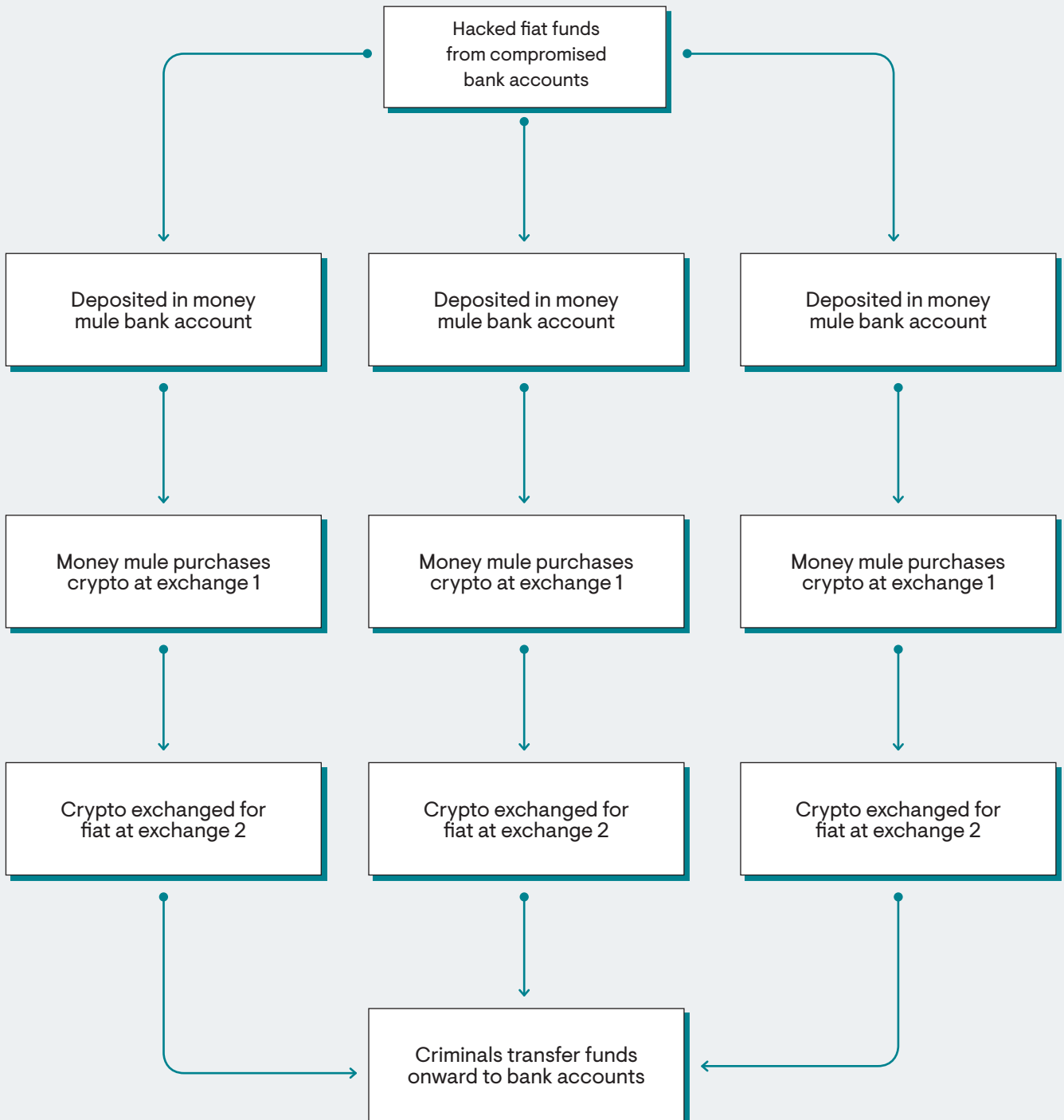
Criminals often rely on fraudulent documents to open accounts in their own names, or in the names of other individuals. One method involves employing money mules – individuals who are used to open accounts and move funds on behalf of the criminal network.

### 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 licenses. 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.



## 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, as can be seen in 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, this could include 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 may 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 the digital assets 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 example, the mule could be 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 has been 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.



## CASE STUDY

### **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>18</sup>

In this scheme, university students responded to job advertisements on social media offering £500-£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 group then instructed the students to open accounts on 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 were told to buy digital assets with the proceeds of crime.

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





## WARNING

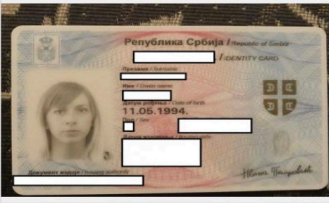
### KYC Kits

A recent trend enabling money muling is the availability of “KYC kits”. Sold on the dark web, these provide criminals with stolen identity details of victims that can be used to open accounts and bypass AML controls.<sup>19</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 licenses;
- selfies taken using a mobile device during online account opening; and
- logins and passwords for online bank accounts and other sites.

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.

**Terms and conditions of CardPass**

New USA SELFIES in stock:

SELFIE HOLDING DRIVER LICENSE WISCONSIN USA  
<http://5gc3hz66ulfzgwu.onion/viewProduct?offer=533530.604443>

Selfie holding driver license Missouri USA  
<http://5gc3hz66ulfzgwu.onion/viewProduct?offer=503638.6344>

Selfie holding driver license OKLAHOMA USA  
<http://5oc3hz66ulfzgwu.onion/viewProduct?offer=175866.535537>

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

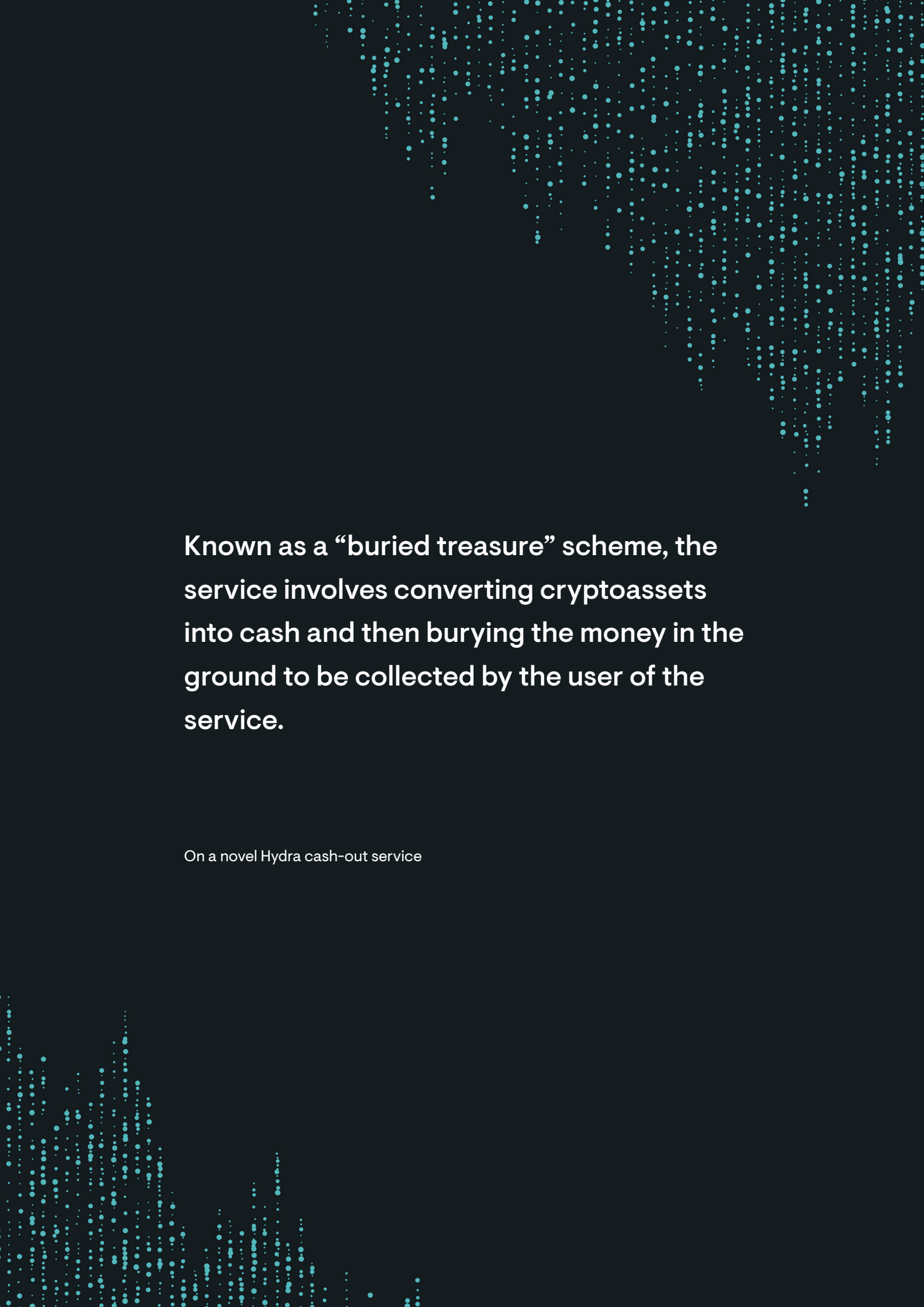


#### KEY CONTROLS:

### Dealing with Money Mules

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

- using cryptoasset transaction monitoring software – such as Elliptic Navigator – to identify transactions among customers that demonstrate patterns of money mule activity. Examples include repeated low-value transactions that ultimately derive from or flow to an illicit source of funds;
- 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; and
- imposing limits or prohibitions on customers to transfer funds to – or receive funds from – third-party accounts.



**Known as a “buried treasure” scheme, the service involves converting cryptoassets into cash and then burying the money in the ground to be collected by the user of the service.**

On a novel Hydra cash-out service

## 2. Peer to Peer (P2P) Platforms

P2P platforms are separate from large centralized exchanges that actively manage orders for large books of customers.

They act as focal points for cryptoasset users to interact directly when swapping fiat and digital assets – including through in-person exchanges involving direct cash transfers.

These platforms play an important role in the cryptoasset ecosystem by enabling cryptoasset users to interact without the involvement of large, centralized intermediaries.

### The Problem

P2P platforms may not be subject to regulation depending on their jurisdictions. Users are often not required to provide personal identifying information.

While major P2P platforms such as LocalBitcoins and Paxful have developed robust compliance operations, many others do not have them. KYC and CDD information is often gathered incompletely, inconsistently and unreliably among the non-compliant ones. This leaves the platforms vulnerable to exploitation by individuals seeking to operate with a large degree of anonymity and without the risk of regulatory or law enforcement oversight.

Distinguishing legitimate and illegitimate activity on P2P platforms can prove extremely challenging. Some P2P platforms include the use of a site-specific wallet service, identifiable on the Bitcoin blockchain, while others offer a platform purely for finding other traders. They do not provide a wallet service that can clearly link specific trades to that site. The likes of BitcoinCashout.com allow users to rapidly swap cryptoassets using services such as Western Union among others.

Some P2P exchanges have seen a rise of the unlicensed Bitcoin broker – individual users who charge a fee to process cryptoasset-to-fiat trades for other users of the site.

Criminals can use these unlicensed individual P2P traders to clean their illicit funds – fiat for drugs sold on the street that is exchanged into cryptoassets, or cryptoasset proceeds from dark web sales converted to cash.

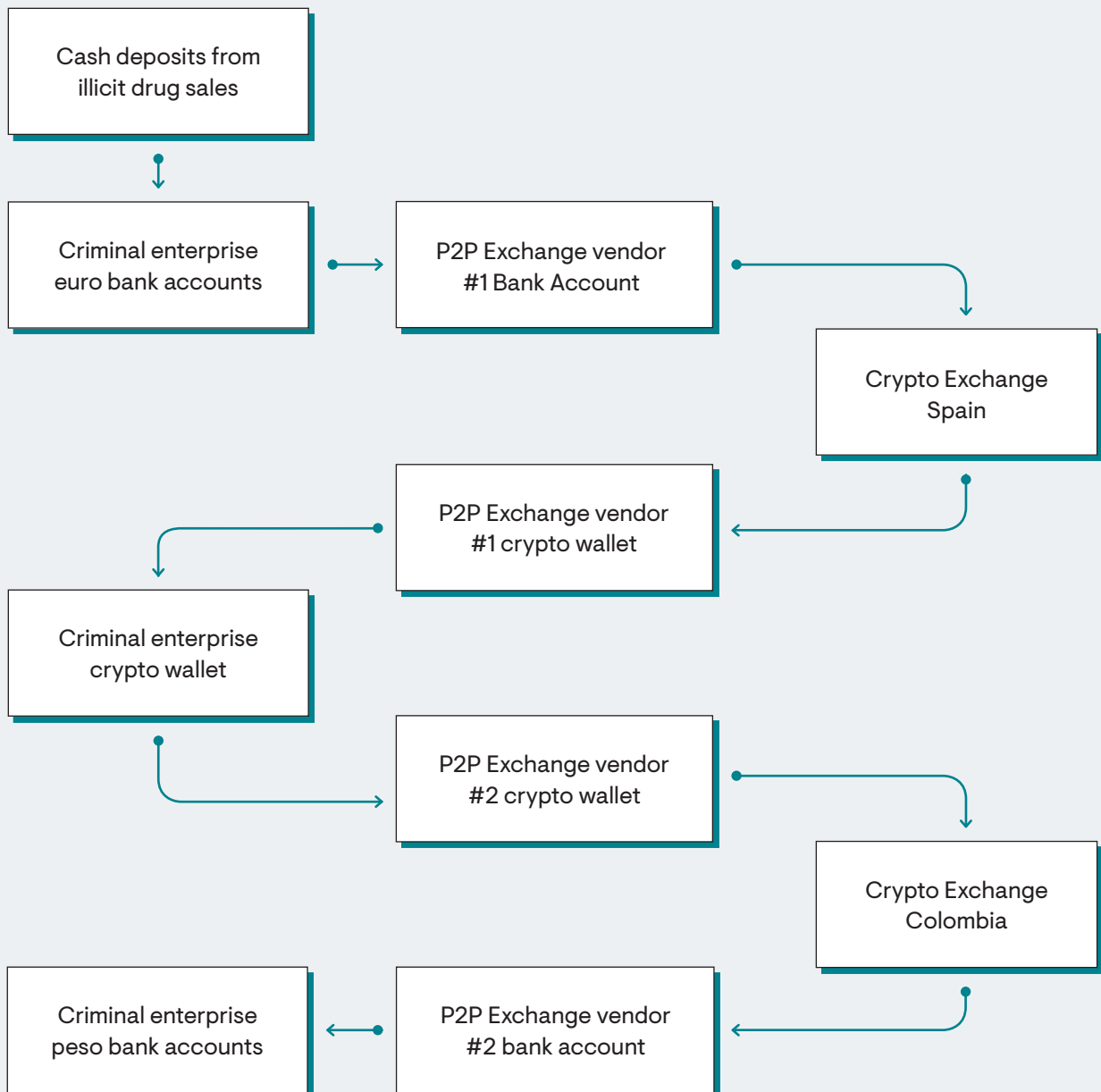
### The Typology

Europol has identified a typology that involves criminals exploiting cryptoasset brokers operating through P2P platforms to launder drug proceeds.<sup>20</sup>

It works as follows:

- A street drug dealer in Europe provides fiat cash to, or makes multiple fiat bank transfers to a P2P exchange vendor in a narcotics consumer country like Spain.

- The P2P exchange vendor then deposits a large volume of Bitcoin (BTC) or other cryptoasset into the P2P exchange wallet of the criminal enterprise.
- An equal amount of BTC is sent from the criminal's P2P exchange wallet to a second P2P exchange broker located in a source country for narcotics – Colombia, for instance – on the same day.
- The P2P exchange vendor may then send the illicit cryptoasset to an exchange, where they cash out and eventually transfer funds onward to their personal bank account.
- The P2P exchange vendor transfers the fiat currency to numerous bank accounts located in the narcotics source country. The domestic banks will only observe a fiat transfer being made from one individual to another, they may not realize that the underlying transaction relates to cryptoassets.





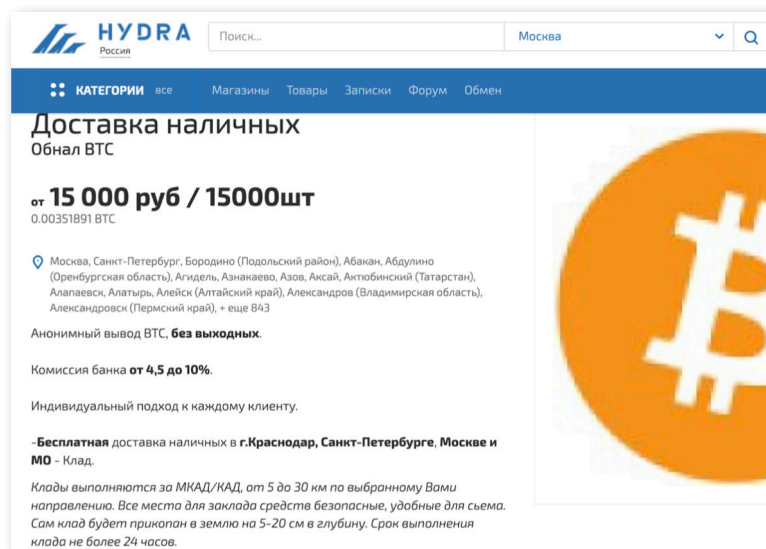
## WARNING

### Dark Web Cash-out Services

In addition to P2P exchanges on the surface web, unlicensed and unregulated P2P exchange services operate on the dark web and can provide criminals with another route for cryptoasset laundering. These dark web cash-out services are similar to surface web P2P exchanges – the difference being an additional cloak of anonymity provided by services such as Tor. Cash-out services are often advertised directly to users of illicit online marketplaces and storefronts, they sometimes include tutorials and user guides on how to launder funds with cryptoassets.<sup>21</sup>

In March 2021, Elliptic analysts uncovered a dark web-based cash-out service with a novel twist.<sup>22</sup> The scheme runs on Hydra, which is a dark web service that targets Russian users. Numerous types of cash-out schemes are advertised on Hydra – including schemes to launder cryptoassets by transferring them on prepaid cards into Russian ruble bank accounts.

The screenshot shows a storefront on Dream Market for a "BTC Cashout Service: \$1,000 Cash Mailed to You". The vendor is "allthemoney (20) (5.00★) (@ 5/0/0)". The price is \$0.1739 (\$1144). The service ships to the United States and includes escrow. A central image shows a Bitcoin icon with a dollar sign and circular arrows, symbolizing the conversion of crypto to cash. The product description states: "TURN YOUR BITCOIN INTO CASH AND REMAIN ANONYMOUS!!! You send us your Bitcoin using escrow protection and we send you cash in the mail." It includes instructions on how to use the service and terms and conditions. A "Javascript is enabled" notification is visible in the bottom right corner.



However, one cash-out service takes an altogether different approach. Known as a “buried treasure” scheme, the service involves converting cryptoassets into cash and then burying the money in the ground to be collected by the user of the service.

Hydra has an army of couriers, known as “treasure men” – although they’re often women – or “droppers”, who will deliver any item purchased on the site to a discrete location. This technique has long been used for the delivery of drugs, but the same techniques are now being used to facilitate the exchange of cryptoassets for physical cash.

The Hydra listing shown above advertises a service, where in return for a cryptoasset payment, the vendor will bury bales of vacuum-packed physical cash “5-20 cm under the ground”. The exact GPS coordinates are shared with the buyer, so they can dig it up at their convenience. The service is costly, with fees of around 7% of the amount being exchanged, as well as somewhat risky – thieves known as “seekers” sometimes trail the treasure men and steal the deliveries.

A major cryptoasset money laundering case highlights the value of these services. In 2016, the cryptoasset exchange Bitfinex was the target of a cybercriminal hack that resulted in 120,000 Bitcoins being stolen – worth more than \$7 billion at the time of writing. Among the techniques the hackers used to launder the funds was to send them to Hydra market. Between 2017 and early 2021, they sent more than \$72 million worth of Bitcoin to Hydra. It is likely these funds were sent there to take advantage of laundering services such as those noted above.



## CASE STUDY

### Singapore P2P Traders

In June 2020, authorities in Singapore charged a 23-year-old woman acting as an unlicensed P2P trader.


The woman allegedly received funds into her Singapore dollar bank account from fraudsters. The criminals paid her a commission to convert the funds into Bitcoin for onward laundering.<sup>22</sup> She was charged with failing to obtain a license to provide exchange services under Singapore's Payment Services Act (PSA).

### Red Flags

Red flag indicators associated with brokers operating on P2P exchanges include the following:


- abnormally large values, volumes, or turnover of cryptoassets cashed out at exchanges from P2P platform-associated wallets and for onward transfer to bank accounts - all of which appear to contain no logical business explanation;
- an individual who frequently sends cryptoassets to wallets at P2P exchanges may claim that they are trading for purely speculative purposes. However, their cryptoasset trading activity does not correlate logically with day-to-day movements in the price of digital assets;
- brokers may refuse to provide KYC information to legitimate exchanges and may then open accounts at other exchanges that are non-compliant or that have weak KYC measures;
- the broker's wallet is associated with a large number of transfers to or from separate customers at a level that is improbable for a normal cryptoasset user;
- the broker may have a social media profile on Twitter or Facebook offering their services, or may provide them through sites such as [Bitcointalk.org](https://www.bitcointalk.org) and [Bitcoin-otc.com](https://www.bitcoin-otc.com); or
- cryptoassets may originate from sources such as the dark web or from mixers, before being rapidly transferred out from the P2P trader's address, then to an exchange, and finally cashed out quickly from the exchange to bank accounts.





**In many jurisdictions, cryptoasset ATMs remain unregulated. This makes them an attractive target for criminals, who use ATMs to convert large amounts of cash into cryptoassets.**

There are more than 11,600 cryptoasset ATMs worldwide



## 3. Decentralized Finance (DeFi)

Decentralized finance (DeFi) was one of the most exciting areas of cryptoasset growth and investment across 2021. 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 across 2021 was truly explosive. The total value of capital locked in Dapps grew 1,700% in 2021 to reach \$247 billion, and monthly trading volumes on DEXs hit \$300 billion. 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. To date, DeFi investors have suffered losses totalling more than \$12 billion to date – including \$10.5 billion in 2021 alone. 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.

We’ve outlined these risks and challenges in detail in our separate Elliptic report “DeFi: Risk, Regulation, and the Rise of DeCrime”, which was originally published in November 2021. Below we summarize three of the primary DeFi money laundering typologies outlined in that report, and tips for how you can spot them.

### 3.1. Money Laundering through DEXs

Unlike simple P2P exchange platforms – which are basic websites enabling cryptoasset users to connect – DEXs built on Ethereum utilize smart contracts to enable users to undertake cryptoasset-to-cryptoasset exchanges in real time.

Some observers see DEXs as providing an advantage over centralized exchanges, in that they prove less vulnerable to theft and loss because they are non-custodial in nature.

DEX trading volumes have exploded across 2021, hitting highs of more than \$30 billion per month. Major DEXs such as Uniswap are now competing with large centralized exchanges in overall trading volumes. Though this increase in liquidity on DEXs has made them increasingly vulnerable to exploitation by money launderers, who can layer large volumes of funds through these increasingly active platforms.

## 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. September 2020's KuCoin hack case saw criminals launder millions of dollars worth of cryptoassets via DEXs. This illustrates the emergence of these platforms as a viable money-laundering avenue.

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.

## 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:

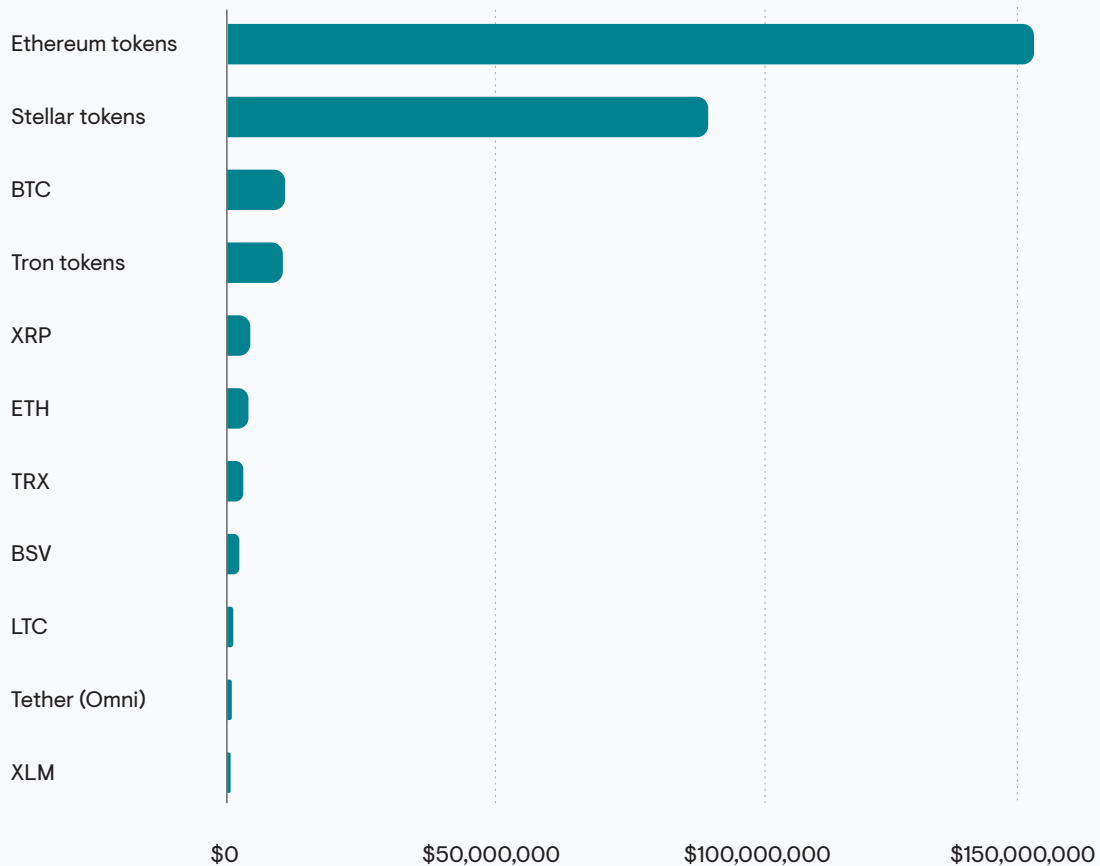
- a customer suddenly receives a large amount of cryptoassets directly from a DEX-associated account and attempts to cash out immediately;
- the customer can not provide any evidence or logical explanation for their source of funds and why they were engaged in dealings through a DEX; and
- the DEX in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



### CASE STUDY

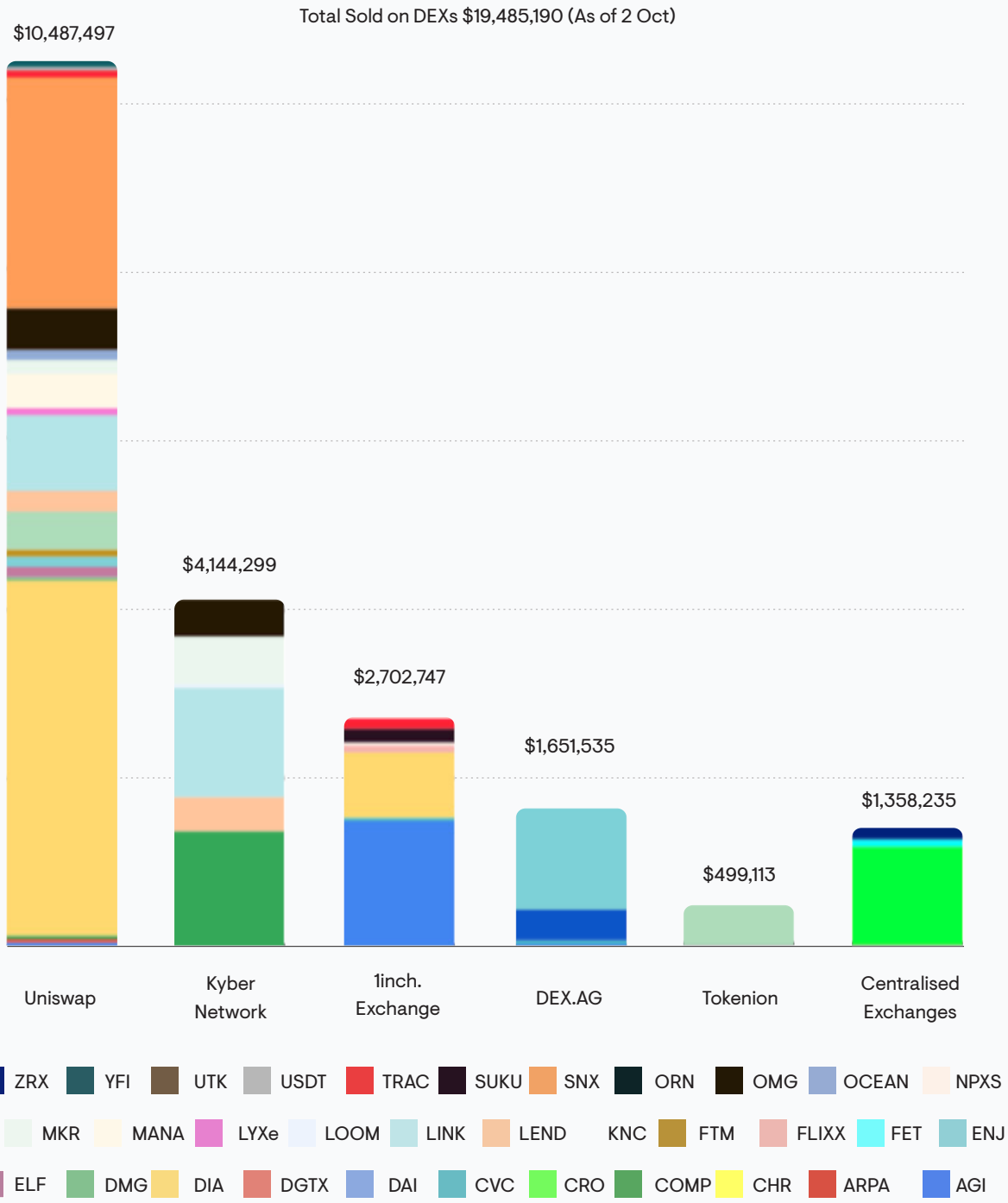
#### Singapore P2P Traders

In June 2020, authorities in Singapore charged a 23-year-old woman acting as an unlicensed P2P. On September 25th 2020, the Singapore-based KuCoin exchange was the target of a major hack. Cybercriminals stole \$281 million in cryptoassets from the exchange including Bitcoin, Litecoin, XRP, Tether and Ether. Approximately \$152 million of the total stolen funds included a range of Ethereum-based tokens.



Once in possession of these funds, the criminals undertook a complex series of laundering techniques. They moved funds through mixing services, and also attempted to exchange them via DEXs. The criminals had sold nearly \$20 million of the stolen tokens on DEXs within one week of the hack. Most of these funds were deposited at Uniswap and Kyber Network DEXs.

### Ethereum Tokens Stolen From Kucoin: Value Sold on DEXs



## 3.2 Money Laundering through DeFi Mixers

Criminals are well aware that the transparency of blockchains makes them vulnerable to tracing and detection.

To evade detection, criminals have routinely sought to make use of cryptoasset “mixers”. These are services which co-mingle funds from different users – making it more challenging to trace funds to their ultimate source. Mixers have long been a favored money laundering technique of online criminals, and we detail the use of these technologies in Chapter 7 of this report.

When it comes to the DeFi ecosystem, it’s critical to be aware of the emergence of specific mixing services that enable financial crime, and to be alert to one service in particular: Tornado Cash.

### The Problem

Compliance professionals and law enforcement agencies leverage the transparency of public blockchains to identify and act against money laundering and other financial crime activity. This transparency allows for insights into illicit activity across the DeFi ecosystem – acting as an important mitigant.

However, criminals operating in the DeFi space have been quick to leverage Tornado Cash, a Dapp that facilitates the mixing of transactions on the Ethereum and other DeFi blockchains. By sending illicit funds to Tornado Cash, criminals can obfuscate the funds trail – making it more difficult to decipher their activity. Tornado Cash is an increasingly popular service with criminals, so being alert to transactions involving the platform can provide indicators of potential suspicious activity.

### 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 provide 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.



### CASE STUDY

#### **The Liquid Exchange Hack and Laundering Through Tornado Cash**

On August 19th 2021, the Japanese cryptoasset exchange platform Liquid was the target of a major hack.<sup>24</sup> Cybercriminals managed to steal more than \$97 million in cryptoassets, including \$45 million of Ethereum tokens.

After stealing these Ethereum tokens, the hackers converted them to Ether at DEXs such as Uniswap and SushiSwap, which prevented the funds from being seized by the token issuers. Having converted the funds into Ether, the hackers then laundered approximately \$20 million worth of the funds through the Tornado Cash mixer.

## 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 include RenBridge VoltSwap and WanBridge. Rather than relying on a centralized exchange to swap Bitcoin for Ethereum, 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 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.

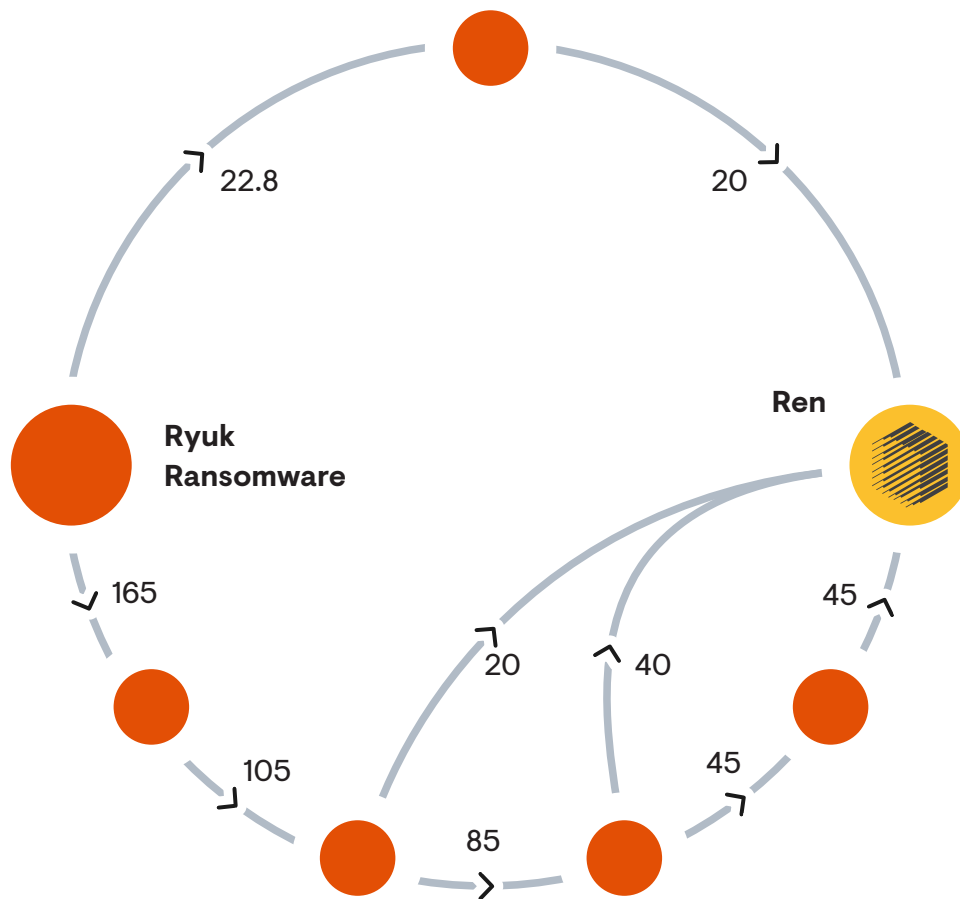




### Laundering Ryuk Ransoms Through Cross-chain Bridges

Emerging in 2018, the Ryuk ransomware strain has been used by multiple criminal groups to extract tens of millions of dollars in Bitcoin ransom payments from organizations around the world. Their proceeds have been laundered in multiple ways – including the use of mixers, non-compliant exchanges and privacy wallets.

In July 2021, Bitcoin from Ryuk began to be sent to RenBridge, which is a decentralized cross-asset bridge. At least 125 BTC – then worth around \$4 million – in funds from ransom payments was “wrapped” through Ren, allowing it to be used on another blockchain such as Ethereum.



## 4. Cryptoasset ATMs

Cryptoasset ATMs play an increasingly 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 11,600 cryptoasset ATMs located around the world<sup>25</sup>, and many provide access to a growing range of altcoins: Ether, Litecoin, Dash, Zcash, Monero and others.

In many jurisdictions, cryptoasset ATMs remain unregulated – or of unclear regulatory status. This makes them an attractive target for criminals, who use ATMs to convert large amounts of cash into cryptoassets.

The scenarios described below have featured most significantly in regions that to date have not issued clear regulatory guidance surrounding cryptoasset ATMs, such as in Europe and South America – though the general typologies apply more broadly.

### 4.1. Facilitation of Illicit Transfers<sup>26</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.



## CASE STUDY

### 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>27</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>28</sup>

The dealers deposit the funds in round value increments such as 1,000 euros – 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 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>29</sup>



## CASE STUDY

### 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>30</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.

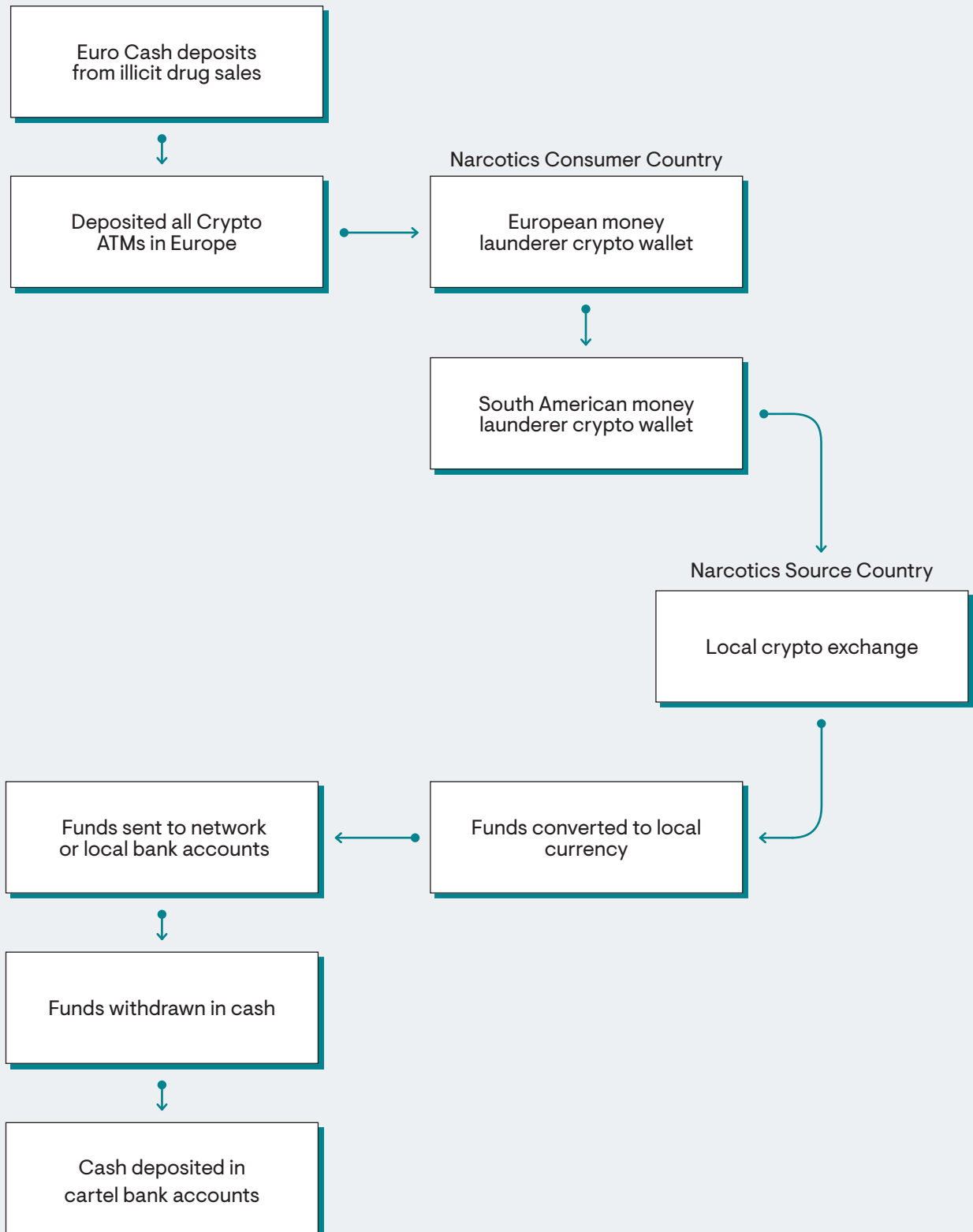


### Red Flags

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

- large denomination notes – e.g. 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; including for example
- a single ATM used to process as much as 200,000 euros per month in areas or regions that are not known to have exceptionally high cryptoasset adoption.

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



## 4.2 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.

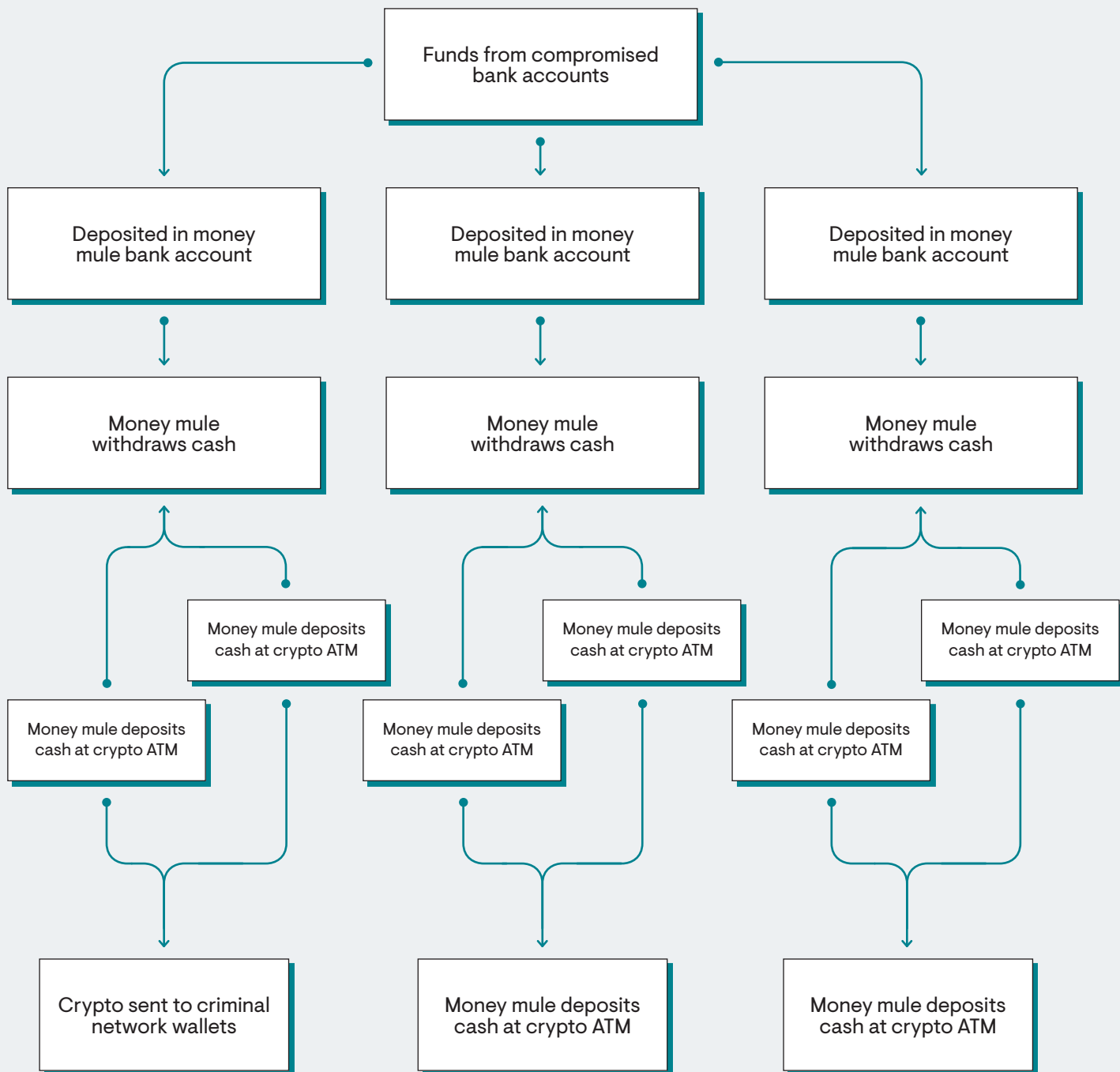
### The Typology<sup>31</sup>

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, Facebook 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>32</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 similar identity indicators sign up for accounts within 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 – e.g. to buy furniture or other ordinary items – for the large value transfers given the sums involved.



## 4.3 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.

### 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 also sound panicked and frightened if contacted by the cryptoasset ATM operator – especially if threatened by fraudsters. Financially vulnerable people 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.





## CASE STUDY

### 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>33</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>34</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.



#### KEY CONTROLS:

### 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.




## WARNING

### Bitcoin ATM Scammers Exploiting COVID-19

In November 2021, the US Federal Bureau of Investigation (FBI) warned of an increase in Bitcoin ATM scams.

The FBI highlighted in an alert that it had seen an increase in scams which involved fraudsters directing victims to make payments using Bitcoin ATMs and digital QR codes.<sup>35</sup> The FBI noted that it had seen a proliferation of fraud schemes involving payment through Bitcoin ATMs – including scams related to online impersonation fraud, romance scams and lottery schemes.

The FBI's alert details the highly coordinated nature of these scams: “Regardless of the scheme, the methods using crypto ATMs and QR codes appear similar. The scammer often requests payment from the victim and may direct the victim to withdraw money from the victim's financial accounts – such as investment or retirement accounts. The scammers provide a QR code associated with the scammer's crypto wallet for the victim to use during the transaction. The scammer then directs the victim to a physical crypto ATM to insert their money, purchase cryptoassets, and use the provided QR code to auto-populate the recipient address. Often the scammer is in constant online communication with the victim and provides step-by-step instructions until the payment is completed.”



**Fraudsters used stolen credit card information to purchase V-bucks – the in-game currency of the popular video game Fortnite. The fraudsters then sold the tokens at a discount on the dark web in exchange for Bitcoin.**

On cryptoasset laundering via gaming currency

## 5. Cryptoasset Gambling and Gaming Services

Cryptoasset gambling services such as Satoshi Dice were among the earliest, most successful and resilient cryptoasset apps. A wide range of digital asset-focused gambling sites now exist, and a growing number of online casinos have begun to accept cryptoassets from customers. Similarly, new online exchanges enable users to swap digital assets for in-game currencies – such as Linden Dollars and World of Warcraft Gold. This helps to build an increasingly intricate online gambling and gaming ecosystem.

While these services are supporting an impressive online infrastructure, they can also be exploited in money laundering schemes. Many online gambling services do not require KYC and CDD information. Elliptic’s research has shown that gambling sites processed approximately 20% of all Bitcoin laundered from the Alphabay dark web market during the years 2015 and 2016.<sup>36</sup>

In more recent years, gambling services have dropped substantially as a destination for illicit Bitcoin proceeds relative to their past use. Today, less than 2% of criminal proceeds in Bitcoin are sent to gambling services directly from illicit sources. Nonetheless, they can still offer a useful avenue for cryptoasset laundering.

Two key methods criminals employ for laundering cryptoassets via gambling and gaming services are outlined below.

### 5.1 Use of Online Casinos to Clean Coins

#### The Problem

Online casinos – including those that are cryptoasset-only and those that accept both fiat and digital assets – are effective for cleaning illicit funds. These schemes resemble tried and tested money laundering methods that criminals have employed for decades at casinos globally.

Chips or credits are purchased from the casino using dirty funds. When the criminal cashes out their winnings – or accepts a loss as part of the cost of laundering – they receive new funds and a receipt from the casino that disguises the gambling activity as the source of the original funds.

Criminals are particularly quick to exploit casinos that do not require KYC or other information of customers.

#### The Typology

1. A criminal has a Bitcoin wallet that has received illicit funds. This could be from a ransomware attack, or funds generated from dark web sales.
2. The criminal transfers the funds to a gambling service that accepts cryptoassets. In some cases, they will use a mixer prior to transferring funds to the gambling site.

3. The funds are used to play the game in question and are quickly cashed out.
4. The criminal receives new, “clean” cryptoassets.
5. They may then attempt to route the funds through another conversion service. Examples include an exchange, cryptoasset ATM or other service to cash out into fiat currency.

## Red Flags

Common red flag indicators associated with cryptoasset gambling typologies include:

- use of unlicensed, unregulated, or Tor-based gambling;
- regular use of online gambling sites such as Seals with Clubs that do not require any KYC, and make an open commitment to protecting anonymity of users;
- gambling sites that do not publish information about their ownership or their jurisdiction of registration;
- gambling sites that do not impose limits on volumes and values of cryptoassets used; and
- funds are sent to mixers immediately before or after funds are deposited, or withdrawn at gambling sites.<sup>37</sup>

## 5.2 Cryptoassets Swapped for In-game Currencies

### The Problem

In-game currencies such as Linden Dollars and World of Warcraft Gold are available on a growing number of online exchanges, such as VirWox. They can be swapped for cryptoassets – thus providing a useful method for layering criminal proceeds through multiple online environments. This in turn allows a criminal to break up their transaction trail through cyberspace. The method may be used to clean illicit cryptoassets, or to conceal dirty fiat.<sup>38</sup>

### The Typology

1. A criminal transfers illicit-origin cryptoassets – for example, from a ransomware attack – to an exchange that provides access to in-game currencies.
2. The criminal receives “clean” in-game currencies.
3. The criminal sells the clean in-game currency to players of the game in exchange for fiat currency.
4. The fiat currency is cashed out directly to the criminal’s account at PayPal, a bank or other similar service.

## Red Flags

Red flag indicators associated with cryptoasset or in-game currency laundering can include:

- large volumes or values of cryptoassets deposited into, or received at an exchange that facilitates swaps with in-game currencies over a short time period;
- the individual is unable to explain why they require cryptoasset to in-game currency swaps of such a significant value; and
- the criminal uses exchange sites that are unregulated, or that require no KYC information.

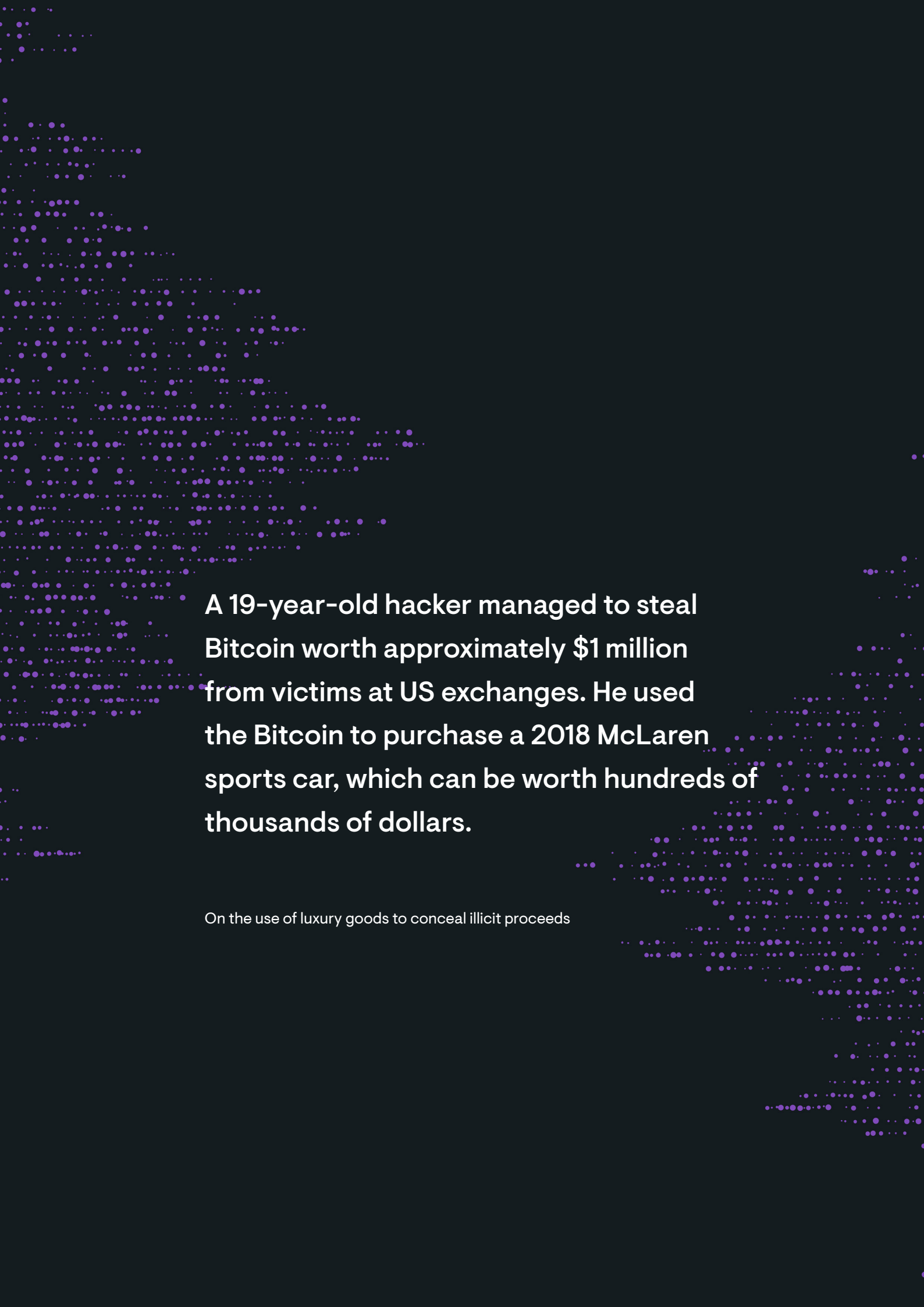


### CASE STUDY

#### **Credit Card Fraud Enabled By Gaming Currency and Cryptoasset Laundering**

In 2019, *The Independent* exposed an online money laundering scheme enabling credit card fraud.

Fraudsters used stolen credit card information to purchase V-bucks – the in-game currency of the popular video game Fortnite. The fraudsters sold the tokens at a discount on the dark web in exchange for Bitcoin or Bitcoin Cash, which they could then launder.<sup>39</sup>



**A 19-year-old hacker managed to steal Bitcoin worth approximately \$1 million from victims at US exchanges. He used the Bitcoin to purchase a 2018 McLaren sports car, which can be worth hundreds of thousands of dollars.**

On the use of luxury goods to conceal illicit proceeds

## 6. 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.

Recent cases suggest criminals have been trying to take advantage of the convenience of cryptoasset prepaid cards to quickly move dirty funds.

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.

### 6.1 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 group 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.

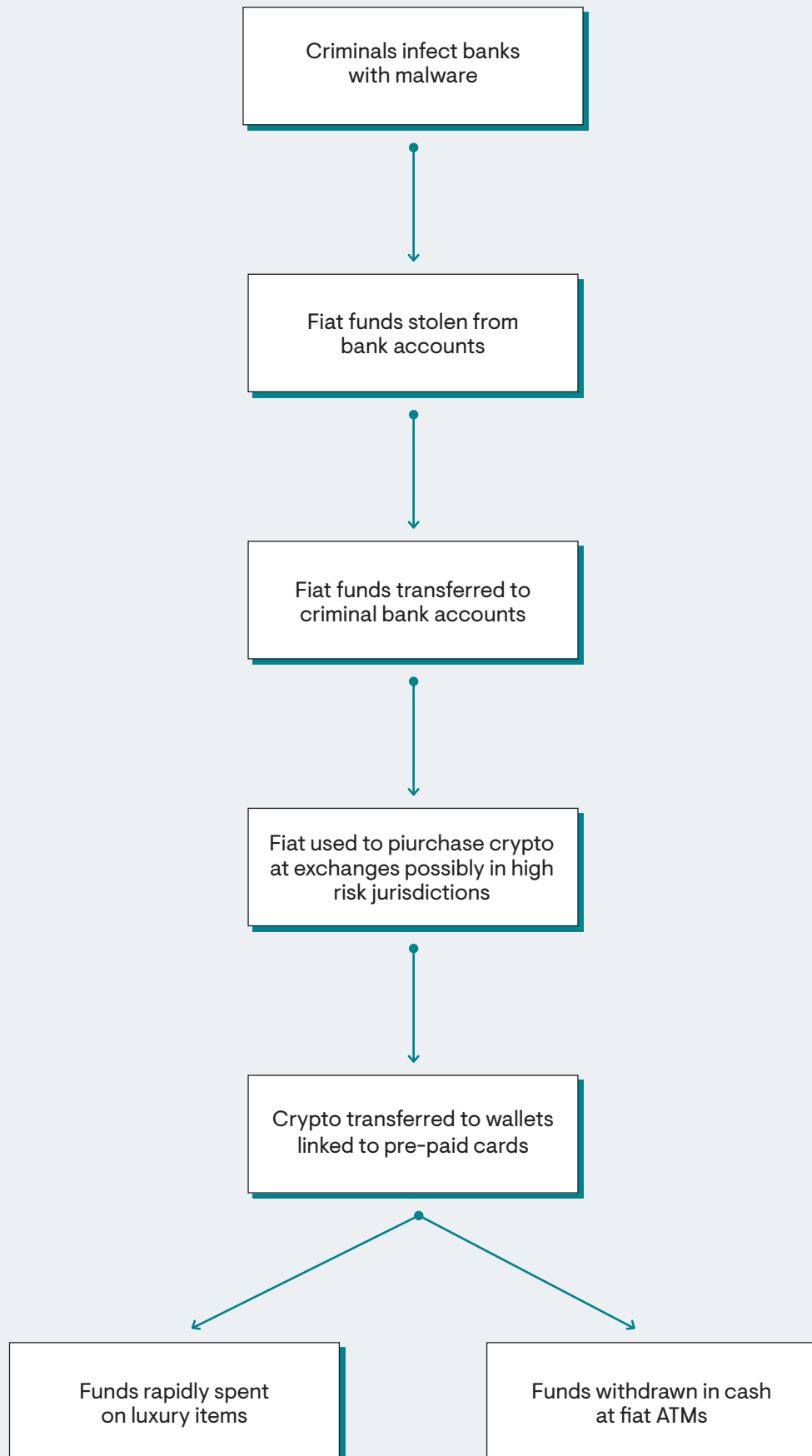
The criminal network moved these stolen funds through numerous fiat bank accounts using money mules in countries such as Taiwan, Spain and Belarus.<sup>40</sup> They eventually converted the funds into cryptoassets through exchanges and wallet service providers offering prepaid card services. According to Europol, the prepaid cards were used to buy luxury items such as houses and cars.<sup>41</sup>

## 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 spend 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>42</sup>; and, or
- criminals targeting providers of prepaid cards that are unlicensed or non-compliant.

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





## WARNING

### 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. These include houses and other property, vehicles, artwork, watches and jewelry.

Customers making high value cryptoasset transfers to dealers in high value 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 2018 McLaren sports car, which can be worth hundreds of thousands of dollars.<sup>43</sup>

## 6.2 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 – e.g. 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.

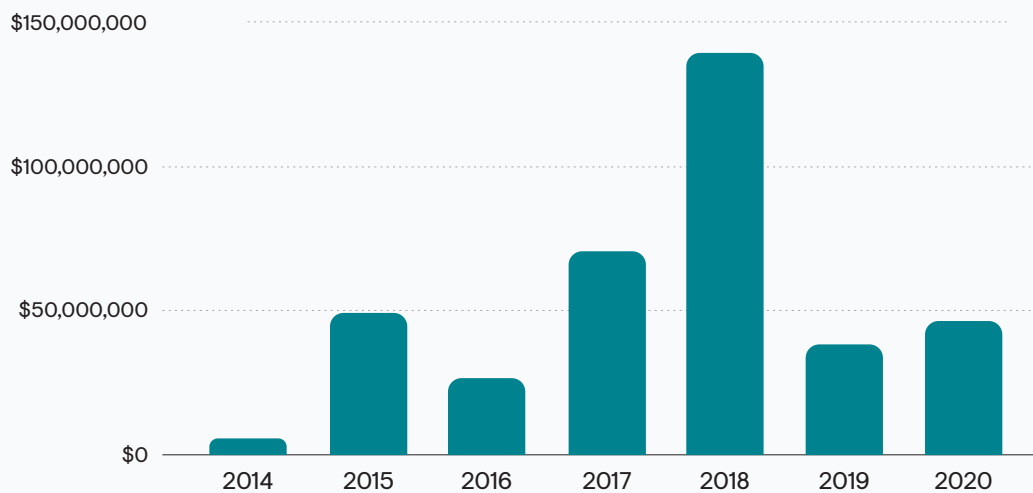


## CASE STUDY

### 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 below.

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>44</sup>

ID	BIN	Bank	Level	Credit	Country	State	City	ZIP	DOB?	SSN?	E-mail?	Phone	Address	F. Name	Ref.?	Price
3004	409961	Banco Cooperativo E...	Electron	Debit	ES		Gabarras	37000 [-]						Garron	Yes	\$25.00
3004	468893	Banque Bank Plc	Classic	Debit	GB	GB	Aveley Road							Max 02	Yes	\$25.00
3004	413383	Banco Nacional de...	Electron	Debit	ES		Las Palmas	35000 [-]						Clara	Yes	\$25.00
3004	376078	Banco Nacional de...	Class	Credit	ES		Madrid	28000 [-]						Clara	Yes	\$25.00
3004	525678	Banco Nacional de...	Standard	Debit	ES		Pinar del Rio, Talpan	30000 [-]						Clara	Yes	\$25.00
3004	492048	La Banque Postale	Classic	Debit	FR		Wick, Colombes	93200 [-]						Wick	Yes	\$25.00
3004	527523	Endic Bank A.S. Ind...	Standard	Debit	VE		Pedregosa	51000 [-]						Wick	Yes	\$25.00
3004	521729	Commonwealth Ban...	Standard	Debit	AU		Osney	50000 [-]						Wick	Yes	\$25.00
3004	462768	Endic And Stinson...	Electron	Debit	US		Seminole	33000 [-]						Wick	Yes	\$25.00
3004	466254	Hong Leong Bank B...	Classic	Debit	MY		Klang	41000 [-]						Wick	Yes	\$25.00
3004	428332	Malayan Banking In...	Classic	Debit	MY		Arang	70000 [-]						Wick	Yes	\$25.00
3004	482561		Classic	Debit	NC		Nelson	67000 [-]						Wick	Yes	\$25.00
3004	474313	Nationwide Building...	Classic	Debit	GB	GB	Sunderland	SR6 7HJ [-]						Wick	Yes	\$25.00
3004	325678	Banco Nacional de...	Standard	Debit	ES		Quited Juste	30000 [-]						Wick	Yes	\$25.00
3004	517041	Turkmenistan Bank...	Standard	Debit	TJ		Starbul	30000 [-]						Wick	Yes	\$25.00
3004	521729	Commonwealth Ban...	Standard	Debit	AU		Bagjata	12000 [-]						Wick	Yes	\$25.00
3004	494075	Banco Pinaros, S.A.	Classic	Credit	ES		General Pineda	37000 [-]						Wick	Yes	\$25.00
3004	492009	State Bank Of India	Global	Debit	IN		Nagpur	44000 [-]						Wick	Yes	\$25.00
3004	524182	Stc Cards & Paymen...	Tranum	Credit	SI		Kh-Niger Channel	50000 [-]						Wick	Yes	\$25.00
3004	461566	Banco Mercantil del	Electron	Debit	ES		Guadalupe	30000 [-]						Wick	Yes	\$25.00
3004	518813	Sveobank AB	Standard	Debit	SE		Maskolva	30000 [-]						Wick	Yes	\$25.00
3004	548901	Banco Santander, S.A.	Standard	Debit	ES		León	24000 [-]						Wick	Yes	\$25.00

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

## 6.3 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.



## CASE STUDY

### 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, during a case in 2018, 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>45</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>46</sup>



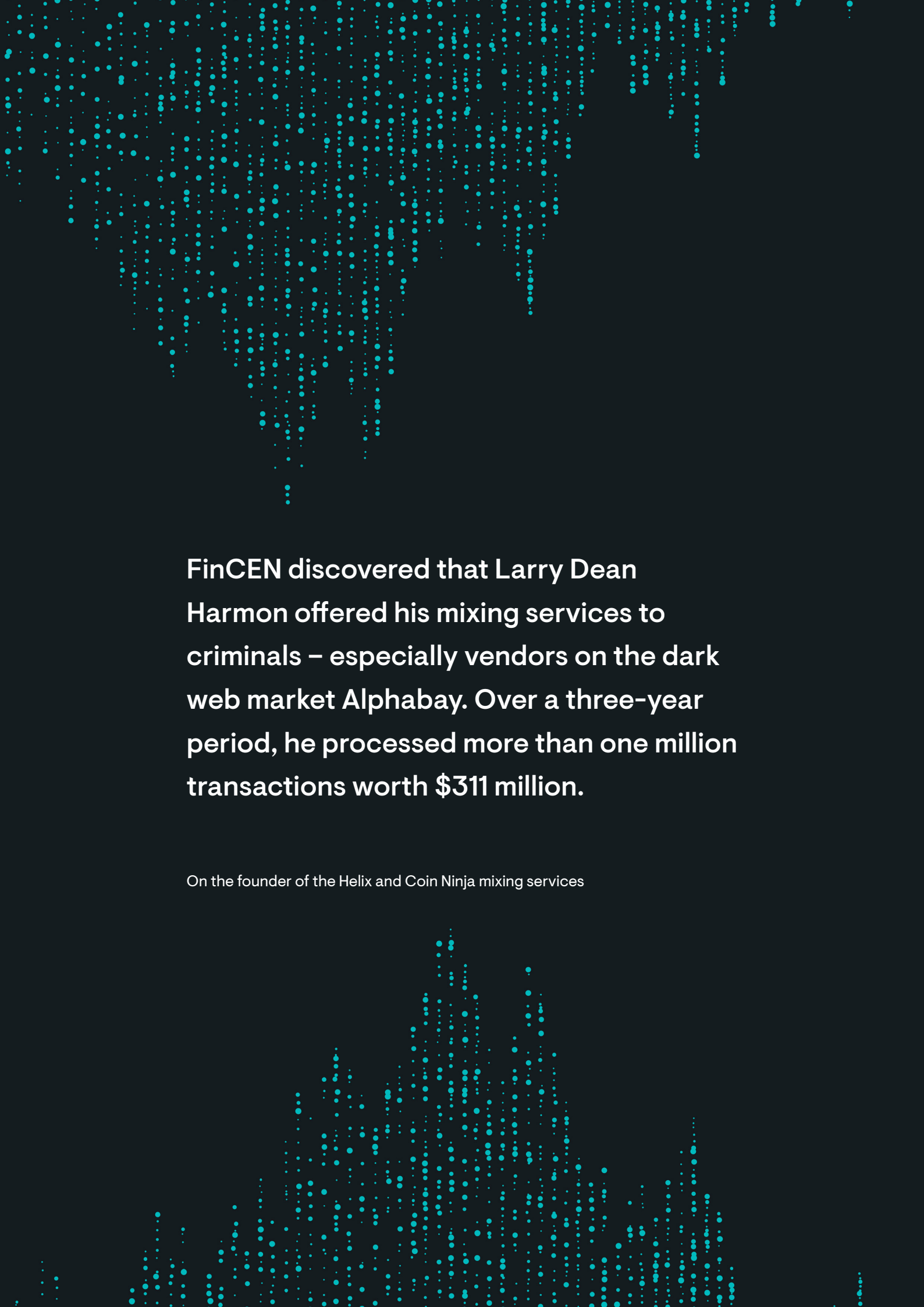
#### KEY CONTROLS:

#### 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.





**FinCEN discovered that Larry Dean Harmon offered his mixing services to criminals – especially vendors on the dark web market Alphabay. Over a three-year period, he processed more than one million transactions worth \$311 million.**

On the founder of the Helix and Coin Ninja mixing services

## 7. Mixers and Privacy Wallets

Cryptoasset mixing services add an element of privacy and opaqueness to the otherwise highly transparent Bitcoin ecosystem. By collating and redistributing BTC 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.

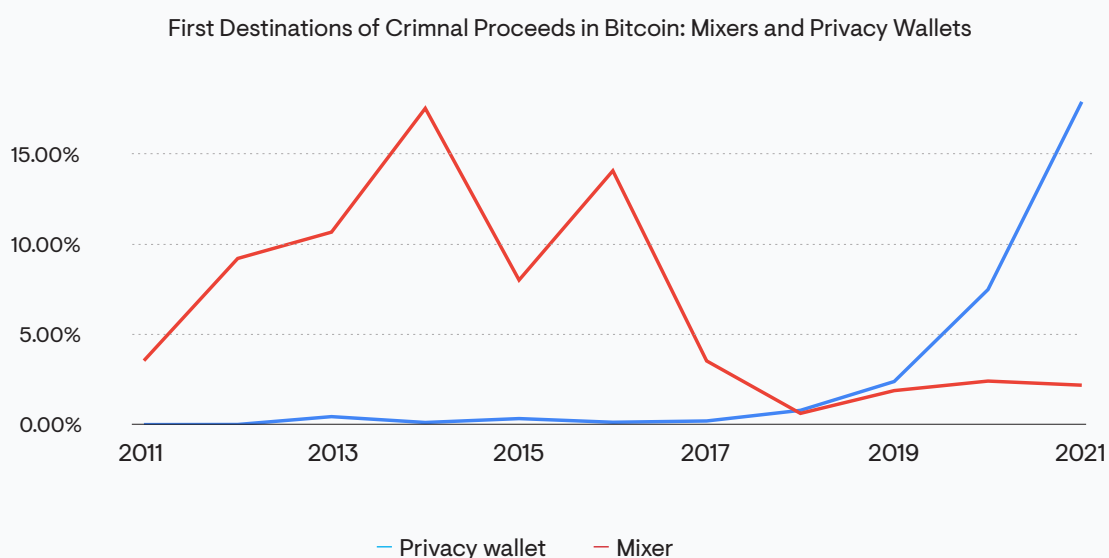
Among the most prolific mixers to date was the Helix mixer, which went offline in early 2018 but operated as a significant money laundering vehicle for criminal actors. In February 2020, Helix founder Larry Dean Harmon was arrested and charged with laundering over \$300 million via the Helix mixer on behalf of criminals.<sup>47</sup> In October, FinCEN announced a \$60 million penalty against Harmon for operating an unlicensed MSB.

### 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).

Recently, Elliptic has observed the rapidly accelerating use of privacy wallets emerge as a money laundering vehicle for criminals. Privacy wallets such as Wasabi Wallet 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, darknet market vendor or other criminal obtains cryptoassets.
2. The perpetrator transfers the funds through multiple wallets, potentially using chain-peeling techniques (see Chapter 10), 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.

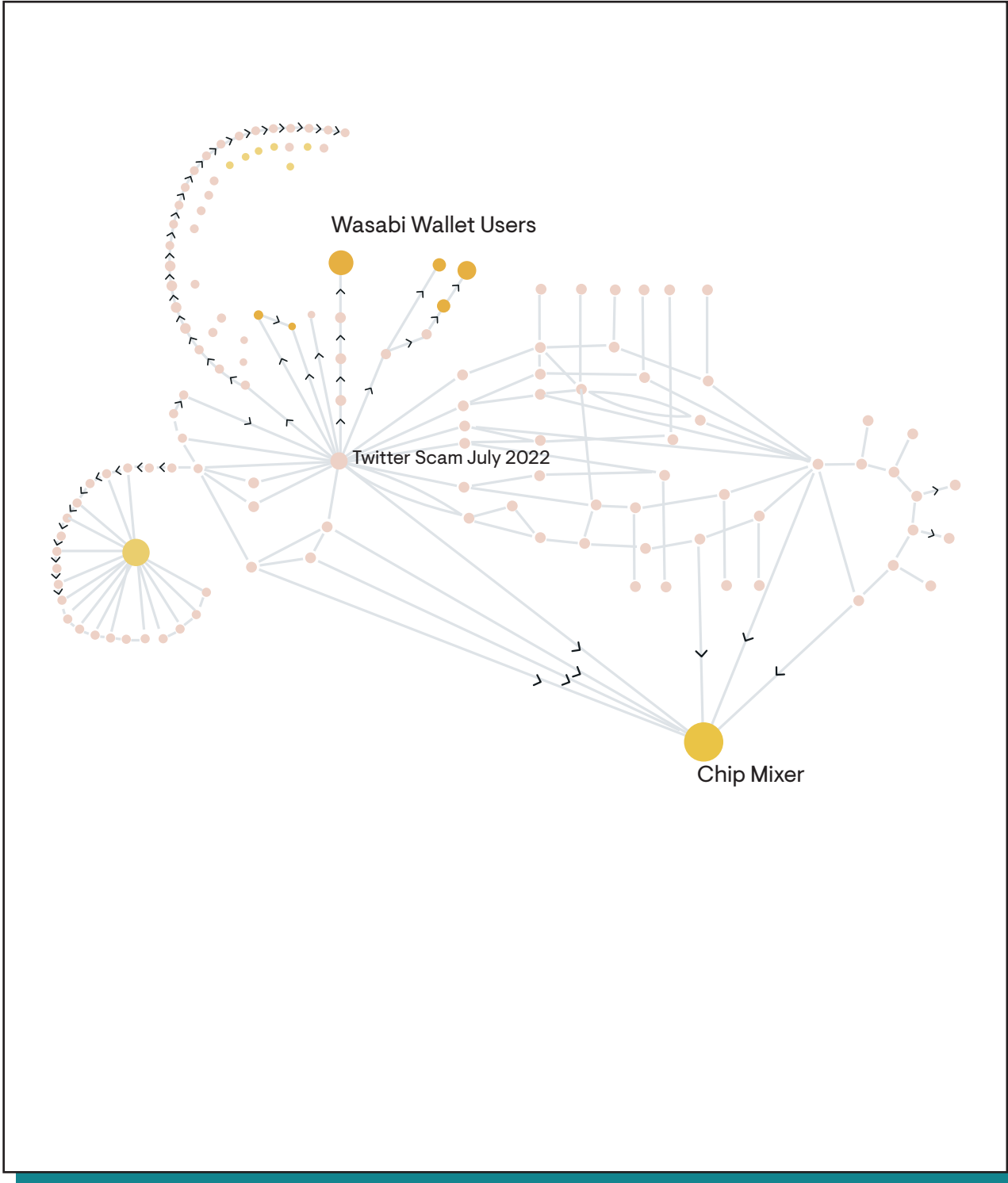
On July 15th 2020, Twitter suffered a major breach, which allowed hackers to post fraudulent tweets through 130 compromised accounts owned by a range of well-known individuals and corporations. The hack started with a phone scam known as spear-phishing – targeting Twitter employees.

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. 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, 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.





### Helix Mixer and Coin Ninja

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 Alphabay. Over a three-year period, he processed more than one million transactions worth \$311 million.<sup>48</sup>

Harmon ran Helix on the Grams darknet.onion site<sup>49</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>50</sup> From April 2014 to December 2017, Helix was the mixer of choice for dark web vendors on Alphabay, Agora Market, Nucleus, Dream Market and others.<sup>51</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>52</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>53</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>54</sup>



KEY CONTROLS:

## 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 – including seeking additional information from the customer about the purpose and ultimate source or destination of funds.

## 8. 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>55</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, tokens were associated with 2017's initial coin offering (ICO) bubble that featured widespread fraud. While that craze has simmered down, tokens continue to flourish and can offer certain 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, Binance USD, DAI and others are playing an increasingly 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. As a result, this provides financial institutions and investors with greater confidence to enter the space.

The rapid rise of stablecoins has led to inevitable concerns about their role in financial crime. Facebook's announcement of its Libra stablecoin project, primarily, has led regulators and global watchdogs to examine the risks of stablecoins. Indeed, in June 2020, the FATF published a report dedicated to the risks posed by them.<sup>56</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.

In practical terms, the current use of stablecoins in money laundering appears to be small. While certain cases in laundering operations have emerged – such as the KuCoin exchange hack – Elliptic's research advocates that use of stablecoins for money laundering is infrequent. Furthermore, 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.



## 8.1 Tokens Used to Clean Dirty Cryptoassets

Tokens are sometimes launched with no requirement for investors to provide KYC information or supply evidence around the source of funds they've used to purchase ICO tokens.

Consequently, tokens provide useful mechanisms for criminals seeking to clean dirty cryptoassets.

In some cases, token issuers with no ill intention are unaware that the cryptoassets they have received come from illicit sources. In other cases, the token issuers are likely to be complicit in the illicit activity. The token itself is of dubious legitimacy – acting as a veil for laundering criminal funds.

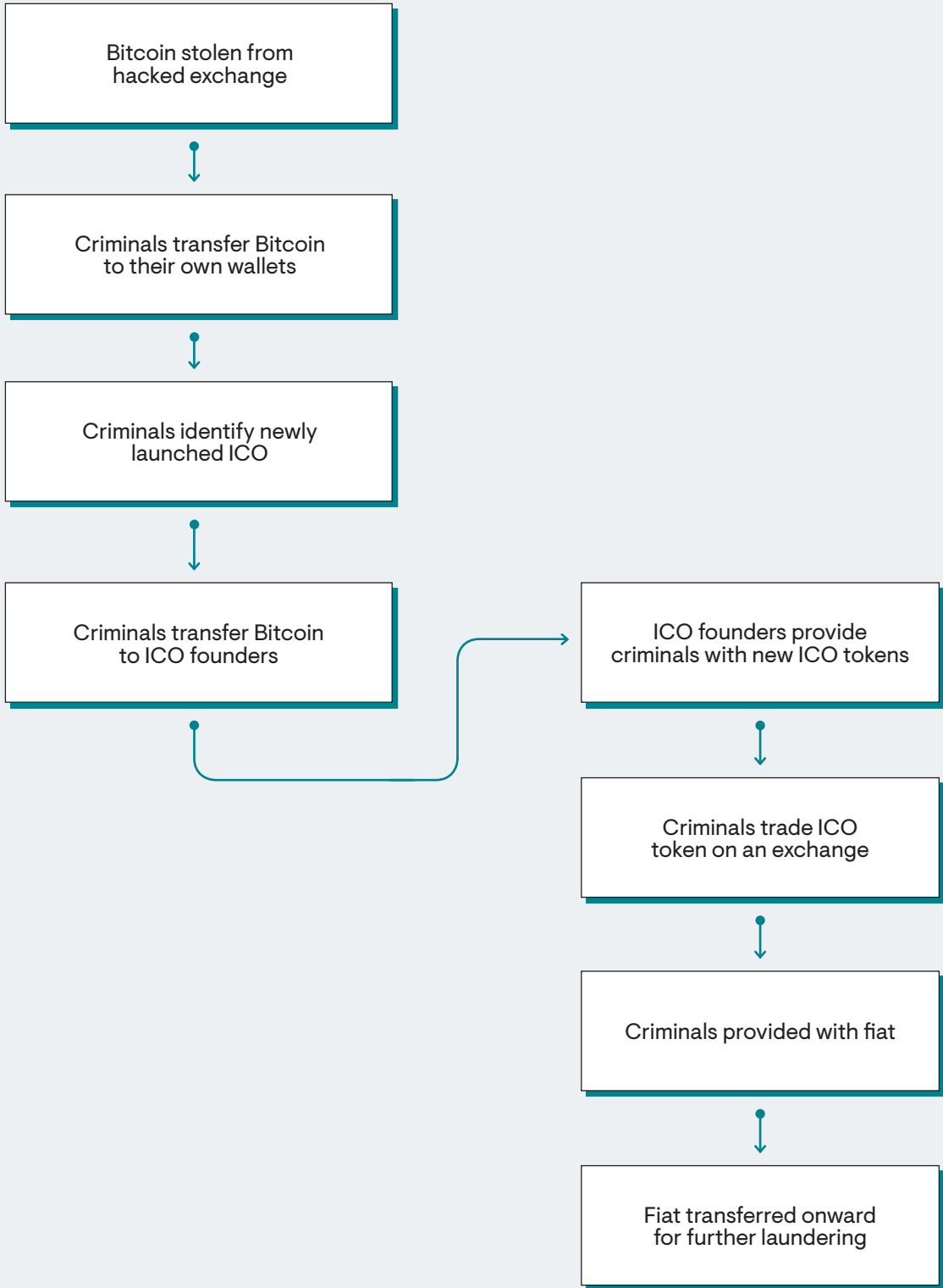
### The Typology<sup>57</sup>

1. A new token is launched, offering Token X up to investors to fund a new blockchain project.
2. A criminal with dirty cryptoassets – e.g. Bitcoin or Ether they acquired through an exchange hack, ransomware or even the hack of another token – purchases a large quantity of Token X coins using their dirty digital assets.
3. The Token X team receives the dirty cryptoassets and disburses new Token X coins to the criminal.
4. The criminal identifies an exchange that offers Token X trading.
5. The criminal swaps their Token X coins for fiat currency or other cryptoassets at the exchange, now in possession of completely “clean” funds.

### Red Flags

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

- a customer wishes to exchange a large volume of newly-issued tokens – very suddenly and without explanation. This may occur immediately after a token sale, and the customer may appear unconcerned about sustaining a loss on their trade;
- the website of the token in question suggests it does not conduct KYC or CDD of investors or have controls in place to protect against ICOs;
- there is little or no information about where the token's founders are based and what jurisdictions they operate in; and
- the token has not registered as an MSB or securities broker in jurisdictions where this is required.





### **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>58</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>59</sup>

## 8.2 Laundering of Proceeds from ICO 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.<sup>60</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.

### 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 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.



### Thailand Dragon Coin Scam

A case in Thailand involved a token scam that was used to launder Bitcoin worth nearly \$35 million.<sup>61</sup>

Fraudsters claiming to represent founders of the Dragon Coin ICO – an actual initial coin offering 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>62</sup>

## 8.3 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 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 token scams include:

- 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.



## CASE STUDY

### Stablecoins Used to Launder the Proceeds of Illegal Gambling

Law enforcement cases from China have highlighted the use of stablecoins in facilitating illegal online gambling.

According to news reports,<sup>63</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. The criminal syndicates 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.



#### KEY CONTROLS:

### 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.



## WARNING

### 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>64</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.





**In 2021, a page appeared on the website of the famous British artist Banksy showing an image linked to NFT marketplace OpenSea – where an NFT featuring the same image was listed for auction. The NFT sold for \$336,000 but was not created by Banksy.**

On fraudsters exploiting NFT marketplaces

## 9. 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 more and more people to engage with the cryptoasset ecosystem. Companies in the NFT space – such as Dapper Labs and OpenSea – are 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>65</sup> – a staggering increase of more than 704% on the previous quarter.<sup>66</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.

Below, we describe three financial crime typologies involving NFTs that are likely to grow in significance as the NFT space continues to boom.

### 9.1 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 piece “Everydays: The First 5000 Days,” by the graphic artist Beeple, which sold for more than \$69 million in March 2021.

Markets where large volumes of money can be moved swiftly are vulnerable to money laundering. 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 3.3; for more general information on mixing services, see Chapter 7.

## 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 Ether-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.

## 9.2 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 market place, 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.



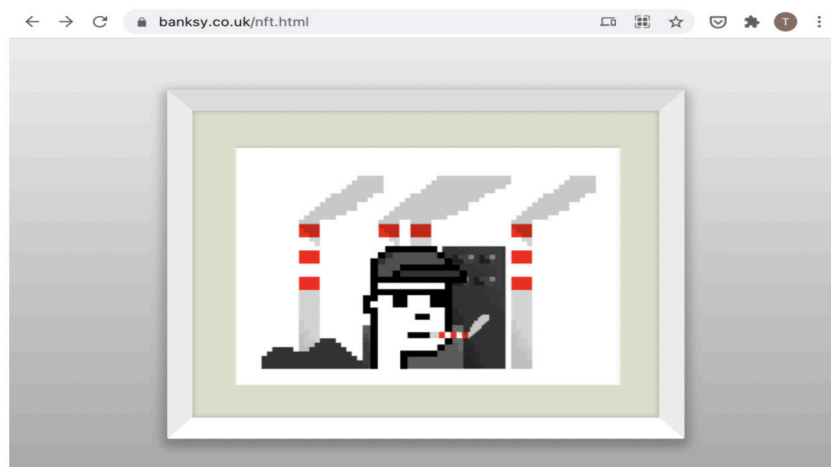
## Fraud and NFTs

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>67</sup>



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

## 9.3 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. Elliptic’s research indicates that criminals stole NFTs worth at least \$14 million in the second half of 2021 alone.

### 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.



KEY CONTROLS:

## 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.



### WARNING

#### 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>68</sup>

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

# 10. 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. These might include Litecoin and Bitcoin Cash, which rely on the Unspent Transaction Output (UTXO) model.

## 10.1 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

An address is in receipt of a very large volume of criminal proceeds – for example Bitcoin resulting from the hack of an exchange.

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.

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.

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.



### 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 – e.g. 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.

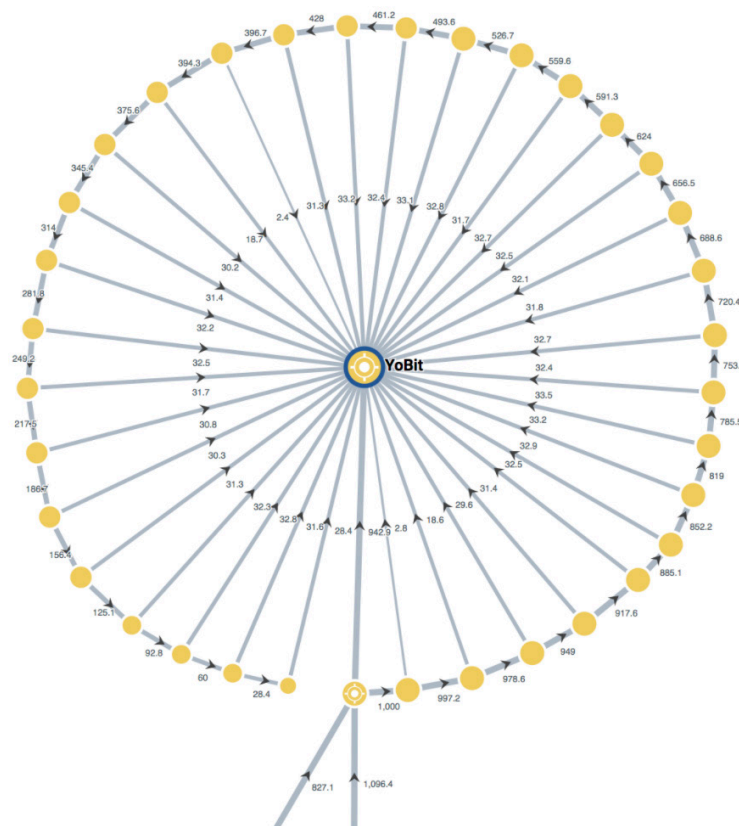


### The Bithumb Hack

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>69</sup>

Elliptic’s research reveals that after stealing the Bitcoin, the hackers – who some analysts suggest may be the North Korea-linked Lazarus hacking 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 hackers 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.



## 10.2 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 – e.g. 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 are discovered to create accounts at the same time. They begin sending funds on a continuous basis – e.g. daily – 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.

# 11. 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.

## 11.1 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”.



### CASE STUDY

#### 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 – a North Korean state-sponsored cybercrime organization.<sup>70</sup> In April 2018, the Lazarus Group succeeded in stealing 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.

## 11.2 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.

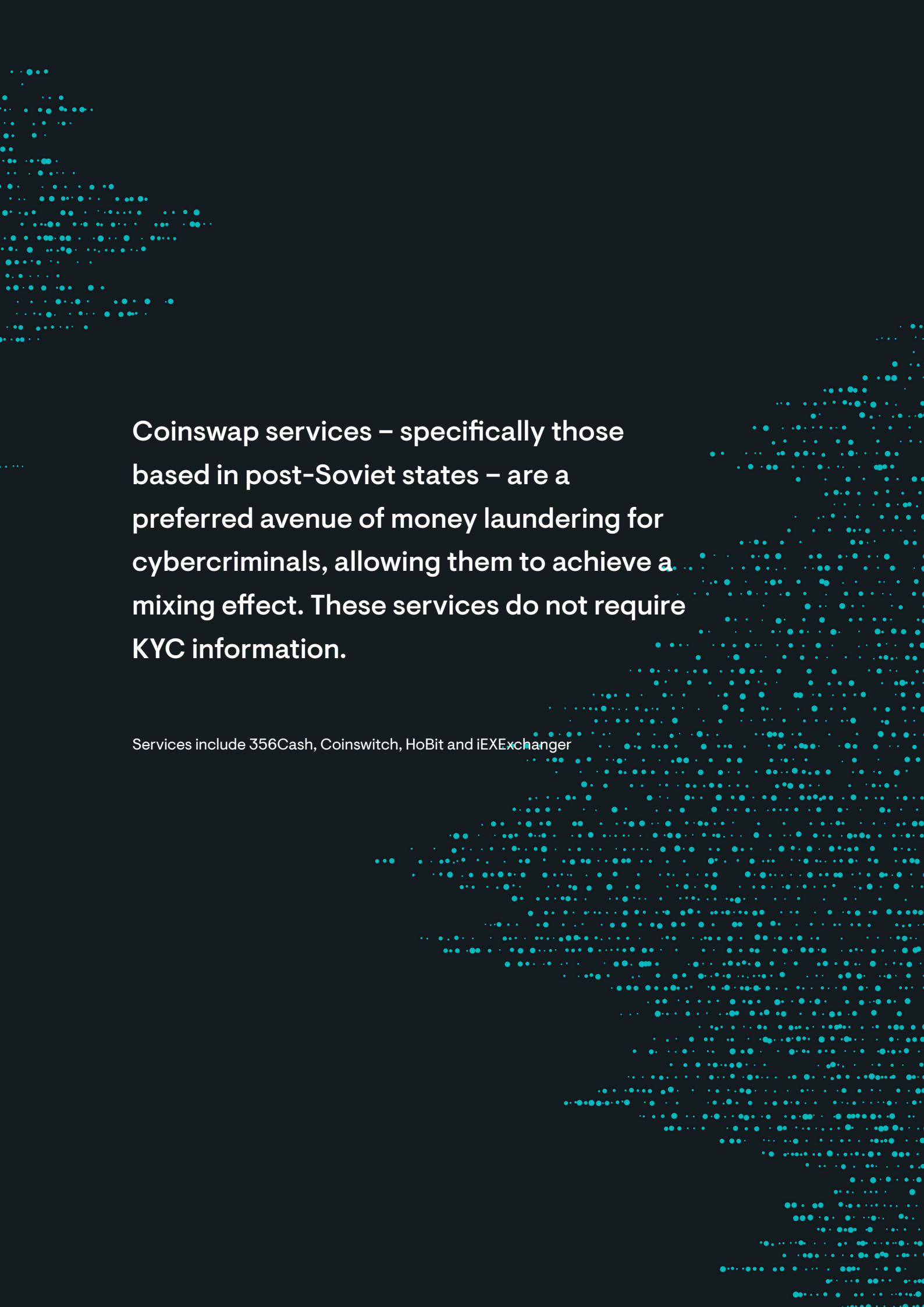


#### KEY CONTROLS:

### 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 risk 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.



**Coinswap services – specifically those based in post-Soviet states – are a preferred avenue of money laundering for cybercriminals, allowing them to achieve a mixing effect. These services do not require KYC information.**

Services include 356Cash, Coinswitch, HoBit and iEXExchanger

## 12. Privacy Coins and 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 and fungibility.

Privacy coins<sup>71</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. Privacy coins 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.

### 12.1 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 like 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, ransomware or other – 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).



#### CASE STUDY

### 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>72</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.

## 12.2 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 first 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

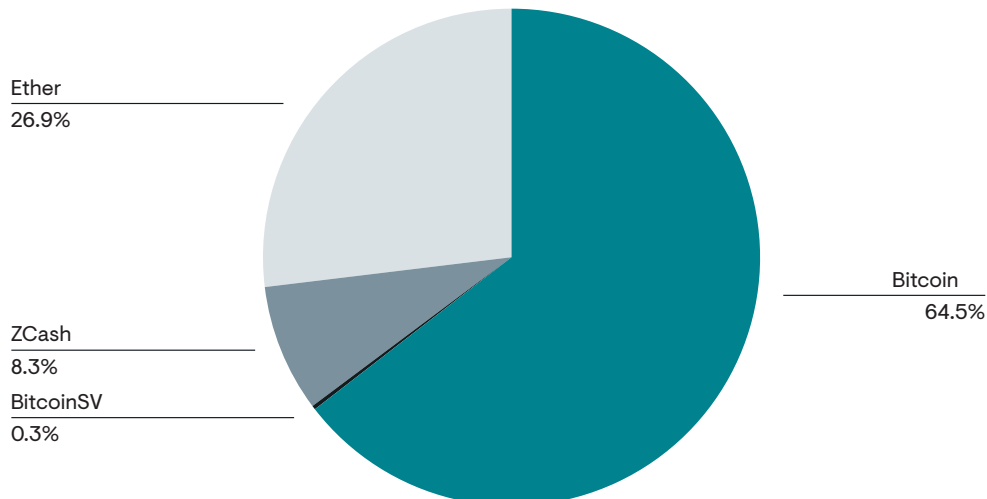
In two September 2020 sanctions actions, OFAC outed Russian cybercriminals and election hackers who rely on privacy coins.

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 1Q6saNmqqKyFB9mFR68Ck8F7Dp7dTopF2W; alt. Digital Currency Address - XBT 1DDA93oZPn7wte2eR1ABwcFoxUFxkKMwCf; Digital Currency Address - ETH 0xd882cfc20f52f2599d84b8e8d58c7fb62cfe344b; Digital Currency Address - XMR 5be5543ff73456ab9fd207887e2af87322c651ea1a873c5b25b7ffae456c320; Digital Currency Address - LTC LNwgtMxcKUQ51dw7bQL1yPQJBVZh6QEqs; Digital Currency Address - ZEC t1g7wowvQ8gn2v8jrU1biyJ26sieNqNsBJy; Digital Currency Address - DASH XnPFSRWTa5glVauosEwQ6dEtGYXgwzn2; 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.





KEY CONTROLS:

## 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.



### WARNING

#### Coinswap Services Used for Chain Hopping

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. Popular services include 356Cash, Coinswitch, HoBit and iEXExchanger. These services do not require KYC information, and they often advertise this as a compelling feature to attract users.

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.

365 CASH

ABOUT US NEWS BLOG FAQ REVIEWS AFFILIATE PROGRAM

Schedule: Round the clock

SELL	BUY
100 PerfectMoney USD	97.57 PAYEER USD
100 PAYEER USD	2388.07 PRIVAT24
100 PRIVAT24	6393.46 Qiwi
100 Qiwi	0.01384189 Bitcoin
100 Bitcoin	6434.78 Yandex Money
100 Yandex Money	100.02 ADVCASH USD
100 ADVCASH USD	6364.04 Сбербанк

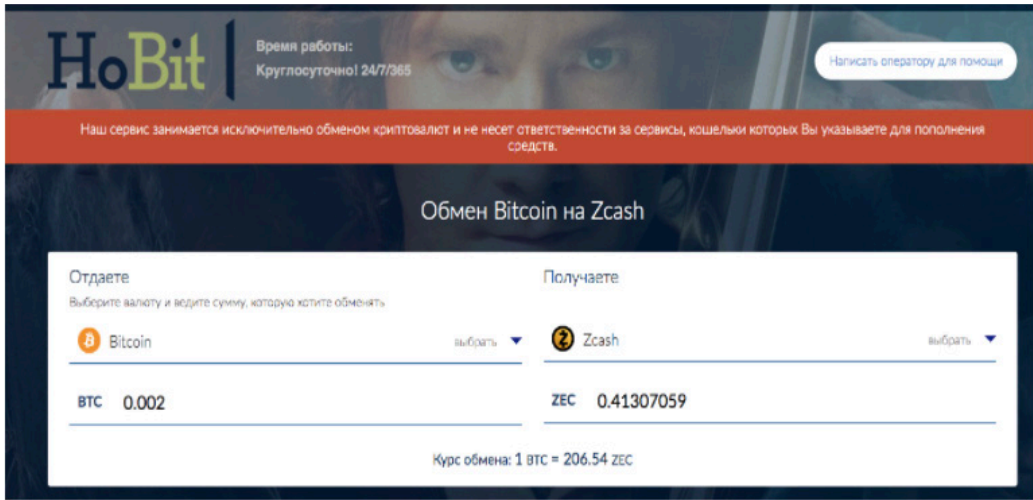
EXCHANGE PERFECTMONEY USD TO PRIVAT24

1 PMUSD = 23.88071 P24UAH

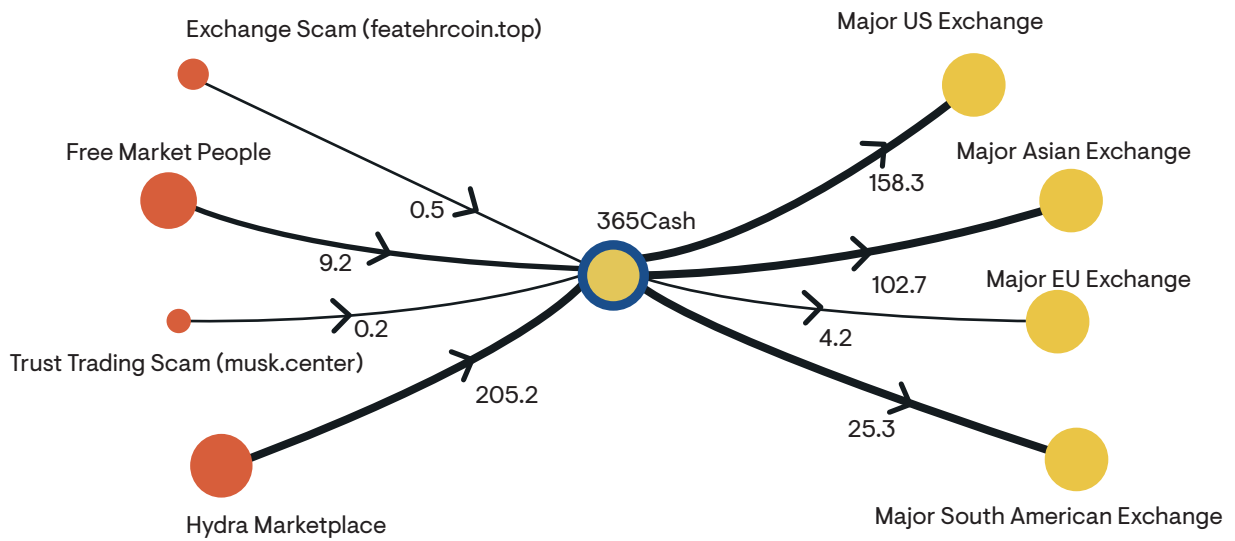
I give PerfectMoney USD

You give  
From 83.75 to 4515.83 USD  
83.75

You give with the commission  
85.43



The image below from Elliptic Forensics demonstrates the inflow of illicit funds to the 365Cash coinswap service, and outbound flows destined for major cryptoasset exchange businesses.



# 13. 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.

## 13.1. 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.

## 13.2. 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 as below:

- 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;
- third-party individual cryptoasset broker 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.



#### WARNING

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

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 11am 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.<sup>74</sup>

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>67</sup>



## WARNING

### 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. In the Russia hacking case, the volumes of Bitcoin mined were small enough that they did not generate significant attention when deposited at an exchange.

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>

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.



## 13.3 Dark Web Laundering

In a recent report,<sup>80</sup> the Financial Action Task Force (FATF) highlighted the increasing professionalism of money launderers utilizing cryptoassets. 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 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 onto 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>

## 13.4 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.

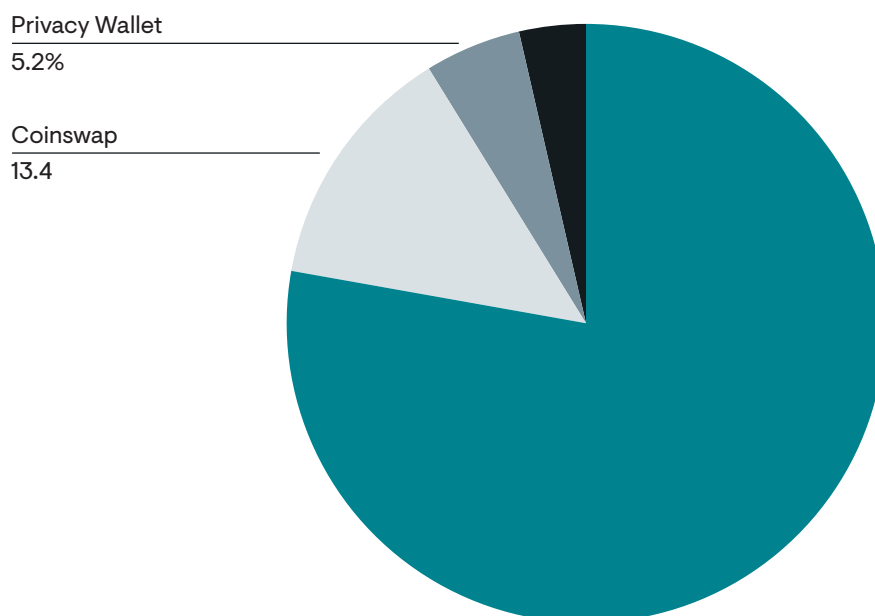
However, DarkSide still did manage to launder approximately 15% of the ransom payment they received. To do so, they used a variety of techniques as indicated in the chart below. Most of the funds – approximately 90% – were laundered through unregulated and non-compliant exchange services and coinswap 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.

## 13.5 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:

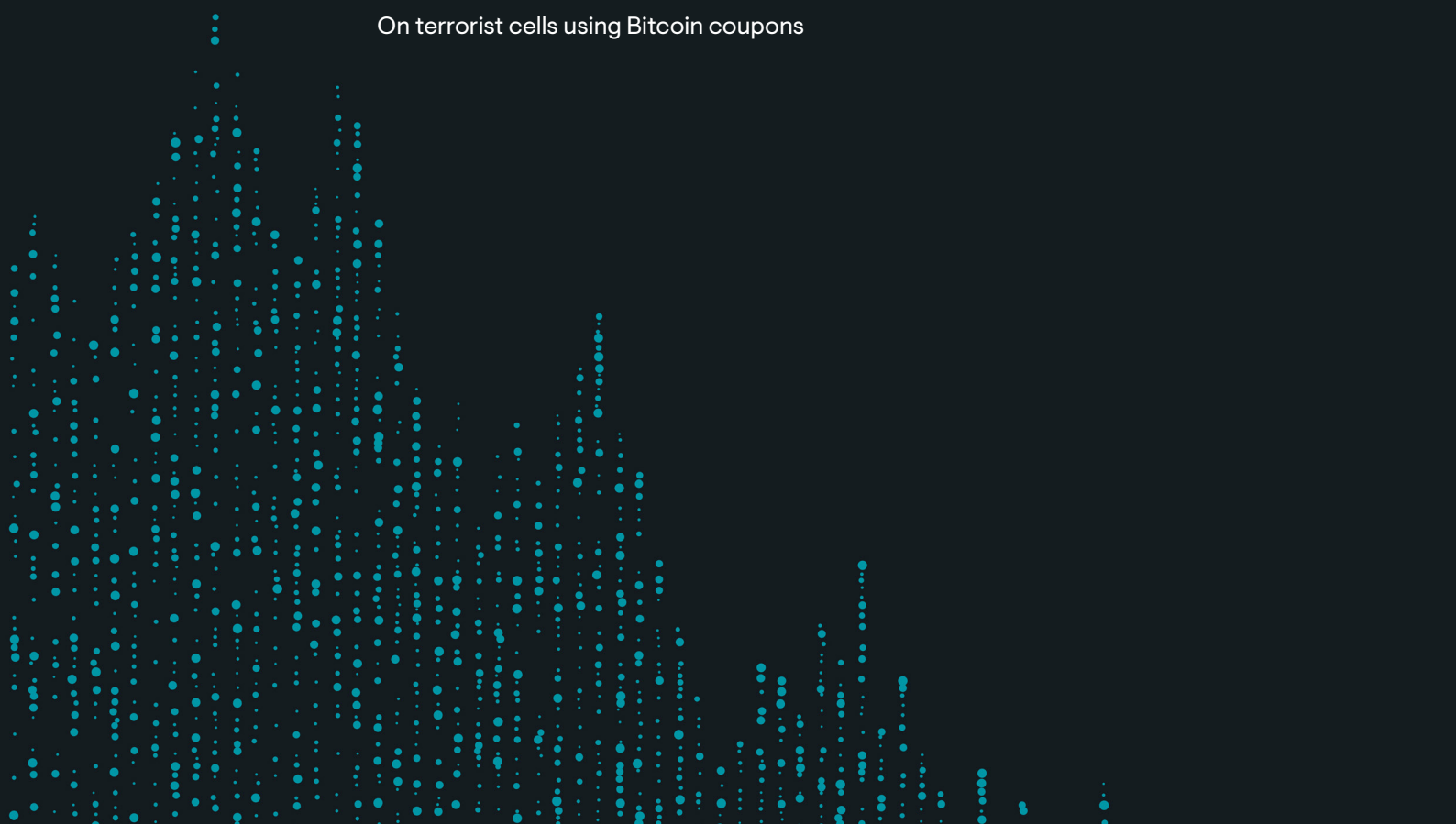
- criminals relying on chain-peeling to hide their Bitcoin transaction trail. They deposit funds at exchanges, potentially relying on fraudulent documents, or by making deposits at numerous unlicensed and non-compliant exchanges;
- customers using cryptoasset ATMs to purchase Bitcoin that is swiftly 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;
- cybercriminals' instruct victims of ransomware attacks to purchase cryptoassets on P2P exchanges. After receiving the tokens, the criminals use a complex chain of mixers and other techniques before attempting to cash out at exchanges.

Destination of funds laundered from Colonial Pipeline ransomware attack



**France arrested 29 individuals associated with Al-Qaeda affiliate Hayat Tahrir Al-Sham. Those arrested were purchasing Bitcoin coupons from licensed tobacco shops around France and transferring the Bitcoin to French jihadists residing in Syria.**

On terrorist cells using Bitcoin coupons





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 in 2020-2021 suggest 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.

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.

## 14. TF Involving Crowdfunding Through Charities and Other Organizations

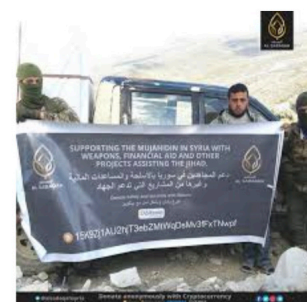
### Jihadist Activity

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.

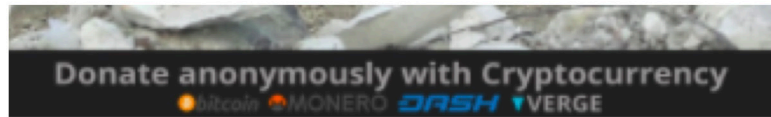


Image from Al Sadaqah Twitter Account Soliciting Donations in Various Cryptoassets

The US law enforcement action in August 2020 also targeted the Al-Qassam Brigades campaign – a fundraising campaign 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.

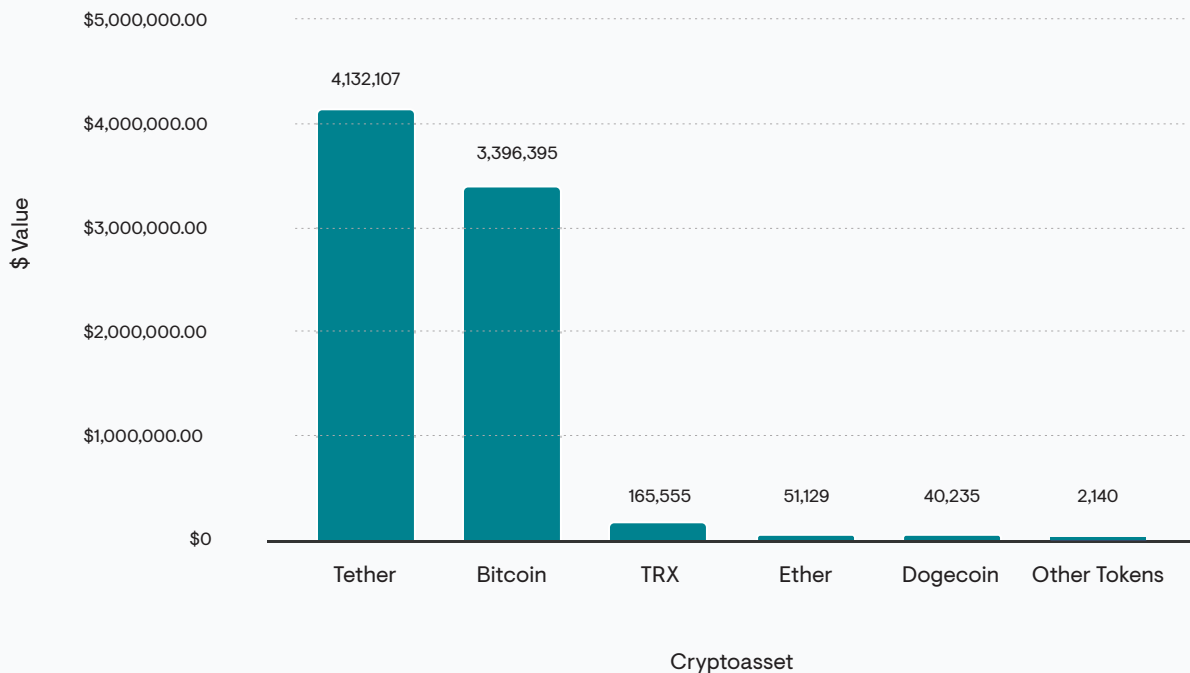


US law enforcement agencies seized the Al-Qassam website infrastructure and dismantled the fundraising campaign. They captured funds from 150 cryptoasset wallets involved in sending funds to and from Al-Qassam. Despite this law enforcement action, Elliptic’s analysis indicates that the Al-Qassam Brigades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

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>86</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.

### Value of cryptoassets received by Hamas linked addresses subject to Israeli government seizure order



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 Al Qaeda. 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 neo-Nazi website Daily Stormer 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.

## 15. 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 recent 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 app 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.



## CASE STUDY

### **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. Once they were in possession of the Bitcoin, the members of the network transferred them to French jihadists residing in Syria.<sup>97</sup>

The background of the slide is dark blue with a rain-like effect of small, light blue particles falling from the top right towards the bottom left. The particles are of varying sizes and are most concentrated in the upper right quadrant, becoming sparser as they move towards the bottom left.

# 03

Key Trends:  
Criminals 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:

Criminal/Threat Actor	Methods										
	Crypto Exchanges	P2P	DEXs	ATMs	Gambling/Gaming	Cards	Mixers/Privacy Wallets	Tokens & Stablecoins	Wallet-Specific	Privacy Coins	NFTs
Professional Money Launderers	x	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		x	x	x
Fraudsters (including Ponzi scheme perpetrators)	x			x		x	x	x			x
Professional Money Launderers	x	x	x	x	x	x	x	x	x	x	
Street Drug Dealer	x	x		x		x					
Human Traffickers/Sex Trade	x	x		x		x					
Tax Evaders	x	x				x	x	x		x	
State Actors/Sanctions Evaders	x	x	x			x	x	x	x	x	x
Terrorist/Political Extremist	x	x		x		x	x	x	x	x	

## 16. Hackers and Cybercriminals

Hackers and other cybercriminals – like 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.

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

Cybercriminals 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, 4.3, 6.1 and 13.1);
- an increasing willingness to cash out at legitimate cryptoasset exchanges – rather than relying purely on complicit exchanges such as BTC-e – while using stolen identity information from KYC kits (see section 1.3);
- Using cryptoasset debit cards to spend large volumes of funds on luxury items (see section 6.1);
- ransomware perpetrators encouraging victims to purchase cryptoassets on P2P exchanges that do not collect KYC information;<sup>98</sup>
- attempts to move between cryptoassets and in-game currency environments (see section 5.2);
- laundering illicit origin cryptoassets by purchasing newly-minted ICO tokens (see section 8.1);
- hacking centralized exchanges to obtain tokens and stablecoins, with laundering occurring via DEXs, DeFi mixers and cross-chain bridges (see section 3); and
- simultaneous use of both mixing services and privacy wallets (see section 7).

## 17. 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 such as Joker's Stash<sup>99</sup> that allow carders to buy and sell compromised data;
- guns, ammunition and other arms and weapons; and

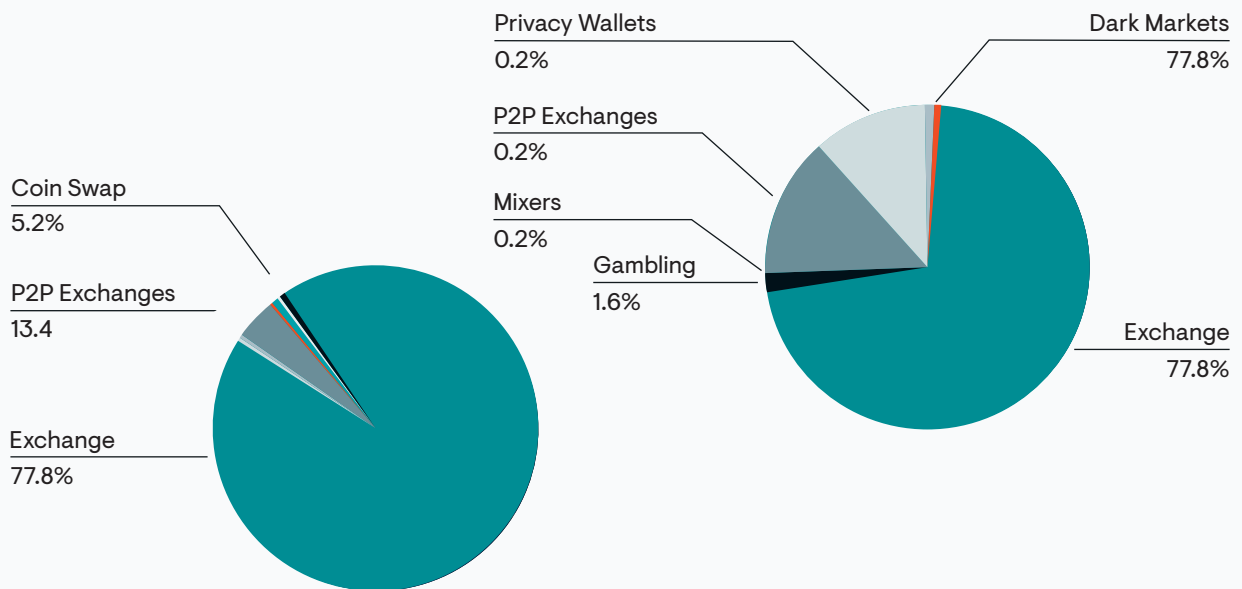
- crime-as-a-service (CaaS) models, this includes the provision of malware kits, KYC kits and assistance with cashing out cryptoasset-based criminal proceeds.

Large dark web marketplaces – such as Hydra – continue to operate and have provided a wide range of items and services. However, since the take down of Alphabay and Hansa Market in mid-2017, an increasing number of criminal vendors have established their own Tor-hosted storefronts – such as Joker’s Stash. These sell directly to buyers without relying on hosted, centralized marketplaces.

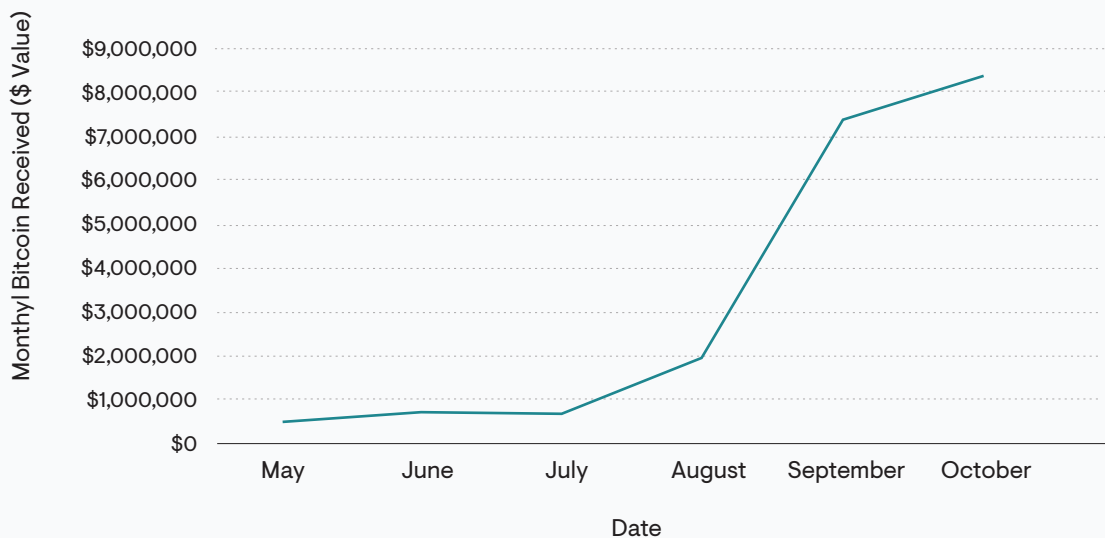
Elliptic has detected a trend of migration to decentralized dark web marketplaces across 2021. Unlike the major established dark markets to date, these markets do not offer a custodial account service for settling payments among buyers and sellers. They sometimes rely on coinswap services to immediately swap Bitcoin that vendors receive into Monero.

### User movement to “decentralized” dark markets:

Example decentralized market: sources/destination of funds



Example decentralized market: monthly Bitcoin inflows (\$Value)



## 18. 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:

- More and more scams instruct victims to make payment via cryptoasset ATMs (see section 4.3);
- using cryptoassets to carry out frauds and launder funds through services such as iTunes (see section 6.3);
- 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 7);
- scams involving NFTs (see section 9).

## 19. 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 digital assets 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 13.3);
- exploiting money mule networks in coordination with services such as cryptoasset ATMs and cryptoasset prepaid cards (see sections 4.2 and 6.1);
- 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 4.1); and
- owning and operating cryptoasset ATMs (see section 4.1).

## 20. 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 10.2);
- 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 4.1);
- 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 4.1 and 4.2);
- some street drug dealers may be willing to accept cryptoassets directly from buyers, and then cashing out via services such as P2P exchanges or cryptoassets ATMs (see sections 2 and 4.1);
- 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 10.2).

## 21. 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>100</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 4.1);
- 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>101</sup> (see section 2);

- 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>102</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.

## 22. 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>103</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>104</sup>
- sending funds via mixing services to hide their ultimate origin (section 7).



## CASE STUDY

### 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>105</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, Kvashuk declared that he had received the Bitcoin as a gift, with a view to have them exempt from his income taxes.

## 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.



**KEY CONTROLS:**

### Preventing Exposure to Sanctions

Controls used by compliance officers to 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.



## 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. We were also 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;

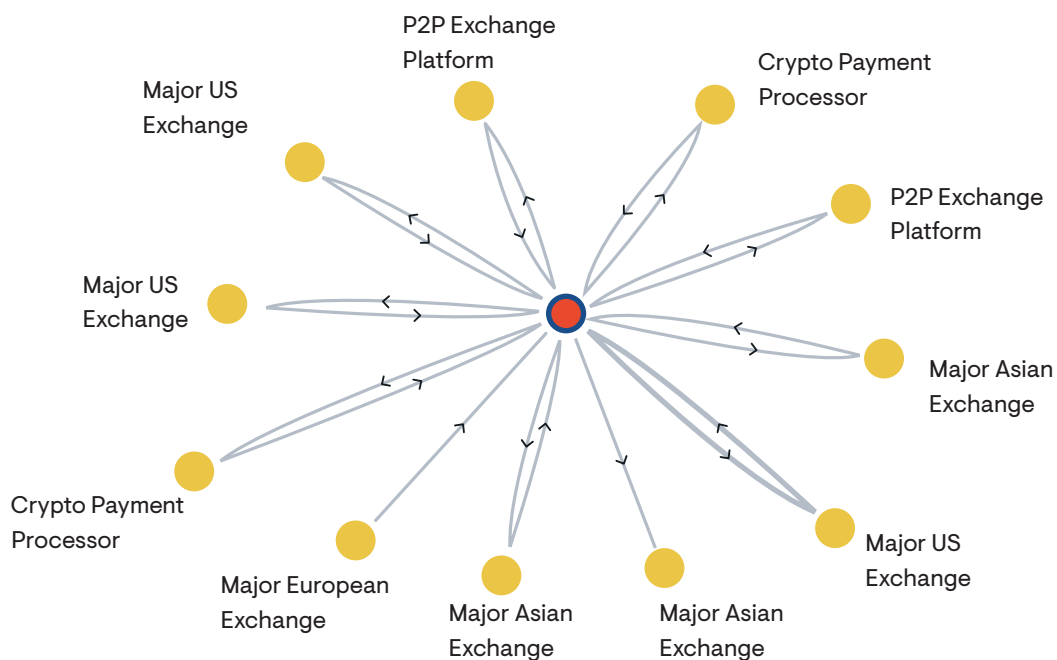
- using dozens of compliant exchanges in the US, Europe and Asia;
- relying on cryptoasset payment processing services in the US and Europe to make direct purchases for items using Bitcoin;
- the use of cryptoasset debit card services;
- moving funds via gambling sites that accept cryptoassets; and
- 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.





## WARNING

### Ransomware Payments and Sanctions Violations

On October 1st 2020, OFAC issued an advisory on the sanctions implications of ransomware payments.<sup>107</sup> In the notice, it clarified that US persons undertaking payments to ransomware campaigns that benefit sanctioned parties are violating OFAC's sanctions. This applies to any ransomware campaigns that could benefit individuals or entities listed on the OFAC Specially Designated Nationals List, or that could involve sanctioned countries such as North Korea, Iran or Venezuela.

OFAC's advisory notes three ransomware campaigns – Cryptolocker, SamSam, and Wannacry 2.0 – as associated with previously sanctioned individuals and jurisdictions. Separate open source reporting from November 2020 hints that Iranian cybercriminals were behind the Pay2Key ransomware attack targeting Israeli and Italian companies.<sup>108</sup> Elliptic's research indicates that funds from these attacks were cashed out via an Iranian cryptoasset exchange platform.

Cryptoasset exchanges need to ensure they can monitor for any potential payments from their customers to these and other ransomware campaigns. They should also exercise scrutiny to guarantee that they do not enable prohibited transactions. On the same day OFAC issued this advisory, the Treasury's Financial Crimes Enforcement Network (FinCEN) published red flag indicators related to potentially illicit ransomware payments.

Elliptic's Blockchain monitoring solutions can assist with detecting these types of risks in cryptoassets transactions. Digital asset businesses should ensure that their transaction monitoring systems are calibrated to implement the detection of ransomware campaigns associated with sanctioned persons.



## 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 14);
- 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 14);
- 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 14)
- Using fraudulently-obtained debit and credit cards to purchase cryptoassets (see section 6);
- Bitcoin coupons for the purchase of cryptoassets – similar to prepaid card typologies (see section 6);
- reliance on wallet-specific techniques to hide funds flows (see section 10); and
- use of exchanges in jurisdictions that present high terrorist financing risks (see section 1).

# Citations

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, 8 June 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 21, 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 21, 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 13, 2021, <https://www.coindesk.com/policy/2021/12/13/chatex-users-ask-us-treasury-to-release-crypto-frozen-by-sanctions/>
7. Europol, 2017 Virtual Currencies Money Laundering Typologies: Targeting Exchanges and Other Gatekeepers, p. 10.
8. Aziz Abdel Qater, "16 Cryptocurrency Exchanges Get Approval to Launch in Venezuela, List Petro," Finance Magnates, 30 April 2018, <https://www.financemagnates.com/cryptocurrency/news/16-cryptocurrency-exchanges-get-approval-launch-venezuela-list-petro/>
9. United States of America vs. Anthony R Murgio, sentencing submission, 20 June 2017, p.7, <https://regmedia.co.uk/2017/06/27/murgiosentencingsubmission.pdf>.
10. Catalin Cimpanu, "95% of All Ransomware Payments Were Cashed out via BTC-e Platform," Bleeping Computer, 27 July 2017.
11. 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>.
12. United States Department of the Treasury Financial Crimes Enforcement Network, Assessment of Civil Monetary Penalty, 26 July 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).
13. Geoff White, "UK company linked to laundered Bitcoin billions," BBC News, 7 March 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>
14. Ibid., p.3.
15. "Prepared Remarks of FinCEN Director Kenneth A. Blanco, delivered at the Chicago-Kent Block (Legal) Tech Conference," 9 August 2018, <https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-2018-chicago-kent-block>

16. “How Chinese Crypto Money Laundering Networks Enable Money Laundering Cartels,” The New Lens, 14 January 2019, <https://international.thenewslens.com/article/111965>
17. “Chinese Authorities in Guangdong Province Freeze 4,000 Banks Allegedly Linked to OTC Cryptocurrency Desks Engaging in Money Laundering,” 15 June 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/>
18. Anna Tims, “Money mules: how young people are lured into laundering cash,” The Guardian, October 4, 2021, <https://www.theguardian.com/money/2021/oct/04/money-mules-laundering-cash-students-funds-bank-accounts>
19. Matthew Hughes, “Exclusive: Cyber-criminals are selling victim’s selfies on the dark web,” The Next Web, 12 March 2018, <https://thenextweb.com/security/2018/03/12/exclusive-cyber-criminals-selling-victims-selfies-dark-web/>
20. Europol, Virtual Currencies Money Laundering Typologies: Targeting Exchanges and Other Gatekeepers, p. 10.
21. Nicolas Christin, “After the Breach: The Monetization and Illicit Use of Stolen Data” (Testimony before the Subcommittee on Terrorism & Illicit Finance, Committee on Financial Services, U.S. House of Representatives, 15 May 2018), p. 7.
22. Tom Robinson, “Buried Treasure - How Tightening Regulation is Forcing Criminals to go to Extreme Lengths to Cash-Out Their Cryptoassets,” Elliptic blog, March 22, 2021, <https://www.elliptic.co/blog/buried-treasure-criminals-to-go-to-extreme-lengths-to-cash-out-crypto>
23. “Twenty-three-year old to be charged with unlicensed Bitcoin dealing tied to online scams” The Banking Times, 23 June 2020, <https://www.businesstimes.com.sg/banking-finance/twenty-three-year-old-to-be-charged-with-unlicensed-bitcoin-dealing-tied-to-online>
24. “Liquid Exchange Hacked: \$97 Million Stolen,” Elliptic blog, 19 August 2021, <https://www.elliptic.co/blog/liquid-exchange-hacked-94-million-stolen>
25. See CoinATM Radar data.
26. This basic typology has been derived from Europol reports, numerous press articles, and discussions with members of the Elliptic compliance officer network.
27. Koos Couvee, “European Traffickers Pay Colombian Cartels Through Bitcoin ATMs: Europol Official,” ACAMS Moneylaundering.com, 28 February 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)
28. Europol, Virtual Currencies Money Laundering Typologies: Targeting Exchanges and Other Gatekeepers, p. 9.
29. Couvee, “European Traffickers Pay Colombian Cartels Through Bitcoin ATMs: Europol Official.”
30. “Cryptocurrency laundering as a service: members of a criminal organization arrested in Spain,” Europol press release, 08 May 2019, <https://www.europol.europa.eu/newsroom/news/cryptocurrency-laundering-service-members-of-criminal-organisation-arrested-in-spain>
31. This typology is adapted from descriptions of criminal activity in public reports issued by Europol.
32. JP Buntinx, “Criminals Direct Money Mules Bitcoin ATMs Launder Hacked Funds,” NewsBTC, 30 September 2016, <https://www.newsbtc.com/2016/09/30/criminals-direct-money-mules-bitcoin->

- [atms-launder-hacked-funds/](#); “Teamviewer Money Mules” BitBargain blog, 3 March 2016, <http://blog.bitbargain.com/post/140405376397/teamviewer-money-mules-facebook-Bitcoin-fraud-victims-in>
33. Cameron Cooper, “Beware of Bitcoin fake tax debits scam,” In the Black, 21 May 2018, <https://www.intheblack.com/articles/2018/05/21/Bitcoin-fake-tax-debts-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>
  34. Robert Johnson, “Hawaii’s Latest Bitcoin Scam,” CryptoDaily, 20 August 2018, <https://cryptodaily.co.uk/2018/08/hawaiis-latest-Bitcoin-scam/>
  35. Federal Bureau of Investigation, “The FBI Warns of Fraudulent Schemes Leveraging Cryptocurrency ATMs and QR Codes to Facilitate Payment,” November 4, 2021, <https://www.ic3.gov/Media/Y2021/PSA211104>
  36. Robinson and Fanusie, p. 7.
  37. Charles McFarland, et. al., Jackpot! Money Laundering Through Online Casinos, McAfee Labs White Paper, April 2014 p. 11.
  38. Steven Messner, “How microtransactions and in-game currencies can be used to launder money,” 13 April 2018, <https://www.pcgamer.com/how-microtransactions-and-in-game-currencies-can-be-used-to-launder-money/>
  39. Anthony Cuthbertson, “How children playing Fortnite are helping to fuel organized crime,” The Independent, 13 January 2019, <https://www.independent.co.uk/news/fortnite-v-bucks-discount-price-money-dark-web-money-laundering-crime-a8717941.html>
  40. Matt Burgess, “Inside the takedown of the alleged 1bn cyber bank robber,” 4 April 2018, Wired, <https://www.wired.co.uk/article/carbanak-gang-malware-arrest-cybercrime-bank-robbery-statistics>
  41. “Mastermind Behind EUR 1 Billion Cyber Bank Robbery Arrested in Spain,” Europol press release, 26 March 2018, <https://www.europol.europa.eu/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain>
  42. TRACFIN, Rapport analyse TRACFIN 2016, <https://www.economie.gouv.fr/files/rapport-analyse-tracfin-2016.pdf>
  43. Lorenzo Francheschi-Bicchieri, “Alleged 19-Year-Old SIM Swapper Used Stolen Bitcoin to Buy Luxury Cars,” Motherboard, 22 August 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).
  44. Tom Robinson, “One of the World’s Most Prolific Cybercriminals Has Retired - And May Well Be a Billionaire,” Elliptic blog, February 12, 2021, <https://www.elliptic.co/blog/jokers-stash-retiring>
  45. “Supplemental Advisory on Identifying and Reporting Human Trafficking and Related Activity,” FinCEN Advisory, 15 October 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)
  46. “Long Island Woman Sentenced to 13 Years’ Imprisonment for Providing Material Support to ISIS,” US Department of Justice, 13 March 2020, <https://www.justice.gov/opa/pr/long-island-woman-sentenced-13-years-imprisonment-providing-material-support-isis>

47. "Ohio Resident Charged with Operating Darknet-Based Bitcoin 'Mixer' Which Laundered Over \$300 Million," US Department of Justice, 13 February 2020, <https://www.justice.gov/opa/pr/ohio-resident-charged-operating-darknet-based-bitcoin-mixer-which-laundered-over-300-million>
48. "First Bitcoin "Mixer" Penalized by FinCEN or Violating Anti-Money Laundering Laws," Financial Crimes Enforcement Network," October 19, 2020, <https://www.fincen.gov/news/news-releases/first-bitcoin-mixer-penalized-fincen-violating-anti-money-laundering-laws>
49. "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)
50. United States of America vs. Larry Dean Harmon, p. 2 <https://www.justice.gov/opa/press-release/file/1249026/download>
51. Ibid, p.3.
52. "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)
53. Ibid.
54. Ibid, p. 2.
55. ERC-20 refers to a technical standard used to implement the launch of new tokens on the Ethereum blockchain.
56. FATF Report to the G20 Ministers and Central Bank Governors on So-Called Stablecoins, FATF, June 2020,
57. For further Elliptic analysis on this typology, see, Tom Robinson, "ICO Risk: Why AML Compliance Matters," <https://www.elliptic.co/our-thinking/ico-risk-why-aml-compliance-matters>
58. "Japan cryptocurrency exchange to refund stolen \$400 million," The Guardian, 28 January 2018, <https://www.theguardian.com/technology/2018/jan/28/japan-cryptocurrency-exchange-coincheck-refund-stolen-nem>
59. Sebastian Sinclair, "Tether Froze \$300k of Stablecoin Hacked After Victims Left Wallet Keys in Evernote," Coindesk, 26 October 2020, <https://www.coindesk.com/tether-froze-300k-of-stablecoin-hacked-after-victims-left-wallet-keys-in-evernote>
60. Ana Alexandre, "New Study Says 80 Percent of ICOs Conducted in 2017 Were Scams," CoinTelegraph, 13 July 2018, <https://cointelegraph.com/news/new-study-says-80-percent-of-icos-conducted-in-2017-were-scams>
61. Wassayos Ngamkham, "Fraudsters adopt Bitcoin to evade cops," Bangkok Post, 13 August 2018, <https://www.bangkokpost.com/news/general/1520574/>
62. Anthony Cuthbertson, "Bitcoin Millionaire Loses \$35 Million in Cryptocurrency Scam," 15 August 2018, <https://www.independent.co.uk/life-style/gadgets-and-tech/news/bitcoin-millionaire-cryptocurrency-scam-thailand-a8492606.html>
63. Zhang Yuze and Denise Jia, "How illegal online gambling launders \$150 million from China," Nikkei Asia, December 22, 2020, <https://asia.nikkei.com/Spotlight/Caixin/How-illegal-online-gambling-lauanders-150bn-from-China>

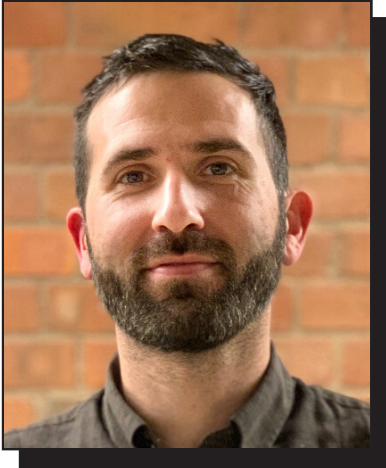
64. David Z. Morris, "The Rise of Cryptocurrency Ponzi Schemes," The Atlantic, 31 May 2017, <https://www.theatlantic.com/technology/archive/2017/05/cryptocurrency-ponzi-schemes/528624/>
65. "NFT Sales Surge to \$10.7 billion in Q3 As Crypto Asset Frenzy Hits New Highs," Reuters, October 5, 2021, <https://gadgets.ndtv.com/cryptocurrency/news/cryptocurrency-nft-sales-surge-q3-2021-usd-10-7-billion-buying-frenzy-opensea-dappradar-2564362>
66. 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 6, 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.>
67. For further analysis of this case, see, Elliptic, "Was Bansky Hacked to Sell a Fake NFT for \$360,000?" August 31, 2021, <https://www.elliptic.co/blog/was-a-fake-banksy-nft-just-sold-for-336000>
68. "Crypto Addresses Holding NFTs Worth \$532k are Among the Latest Sanctioned by OFAC," Elliptic blog, November 9, 2021, <https://www.elliptic.co/blog/crypto-addresses-holding-nfts-worth-532k-are-among-latest-sanctioned-by-ofac>
69. "Bithumb Has Recovered Nearly Half of Funds Stolen in Last Week's Hack," CCN, 28 June 2018, <https://www.ccn.com/bithumb-has-recovered-nearly-half-of-funds-stolen-in-last-weeks-hack/>
70. "Treasury Sanctions Individuals Laundering Cryptocurrency for Lazarus Group," US Department of the Treasury, 2 March 2020, <https://home.treasury.gov/news/press-releases/sm924>
71. 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 anonymising effects.
72. Ryan Browne, "Hackers have cashed out on \$143,000 of Bitcoin from the massive WannaCry ransomware attack," CNBC.com, 3 August 2017, <https://www.cnbc.com/2017/08/03/hackers-have-cashed-out-on-143000-of-Bitcoin-from-the-massive-wannacry-ransomware-attack.html>
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," 24 July 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, 27 August 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, 14 July 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, 24 September 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, 27 August 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, 12 August 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, 20 February 2018, <https://www.wsj.com/articles/jihadists-see-a-funding-boon-in-bitcoin-1519131601>
83. "Global Disruption of Three Terror Finance Cyber-Enabled Campaigns," US Department of Justice, 13 August 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 7 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, 24 August 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, 21 December 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 8, 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, 28 August 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, 6 August 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, 29 August 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, 24 January 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, 10 January 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, 14 December 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," 29 September 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, 7 August 2018, <https://nakedsecurity.sophos.com/2018/08/07/how-Bitcoin-and-the-dark-web-hide-samsam-in-plain-sight/>
99. "Carders park piles of cash at Joker's Stash," Krebs on Security, 16 March 2018, <https://krebsonsecurity.com/2016/03/carders-park-piles-of-cash-at-jokers-stash/>
100. FATF, Financial Flows from Human Trafficking, July 2018, p. 56 <http://www.fatf-gafi.org/media/fatf/content/images/Human-Trafficking-2018.pdf>
101. Ibid, p. 56.
102. Ibid.
103. 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>,
104. Ibid.
105. United States of America vs. Volodymyr Kvashuk, 16 July 2019, <https://www.courtlistener.com/recap/gov.uscourts.wawd.275443/gov.uscourts.wawd.275443.1.0.pdf>
106. See: <https://brief.kharon.com/updates/iranian-cryptotrader-implicated-in-ransomware-scheme-turning-to-mysterious-payment-system/>
107. "Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments," US Department of the Treasury, 1 October 2020, [https://home.treasury.gov/system/files/126/ofac\\_ransomware\\_advisory\\_10012020\\_1.pdf](https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf)
108. Hagay Hacohen, "Check Point unveils new Iranian cybercrime, ransoming companies' data," Jerusalem Post, 12 November 2020, <https://www.jpost.com/israel-news/check-point-unveils-new-iranian-cybercrime-ransoming-companies-data-648928>



## About the Author



David Carlisle

Director of Policy and Regulatory  
Affairs at Elliptic

David Carlisle is the Director of Policy and Regulatory Affairs at Elliptic, the global leader in cryptoasset risk management solutions for crypto businesses and financial institutions worldwide, where he leads engagement with regulators and other external stakeholders, such as the Financial Action Task Force (FATF). David has more than a decade of experience in AML/CTF compliance and regulatory matters, having previously worked as a Policy Advisor at the US Department of the Treasury's Office of Terrorism and Financial Intelligence. He is an associate fellow at the Royal United Services Institute, a UK think tank, where he has authored reports on the illicit use of cryptoassets, and appropriate policy responses.

# About Elliptic

Elliptic is the global leader in cryptoasset risk management for crypto businesses and financial institutions worldwide. Recognized as a WEF Technology Pioneer and backed by investors including Evolution Equity Partners, SoftBank Vision Fund 2 and Wells Fargo Strategic Capital, 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. To learn more, visit [www.elliptic.co](http://www.elliptic.co) and follow us on [LinkedIn](#) and [Twitter](#).

# ELLIPTIC

London • Tokyo • New York • Singapore



[Connect on LinkedIn](#)



[Follow us on Twitter](#)



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

