CONFRONTING THE ILLICIT-FINANCE HYDRA IN CRYPTO MARKETS: PROTECTING RETAIL INVESTORS AND DISRUPTING HOSTILE GOVERNMENT EXPLOITATION

By ALEXANDER BROWDER

HJS Henry Jackson Society

CENTRE FOR RESILIENT SOCIETY

DEMOCRACY | FREEDOM | HUMAN RIGHTS

March 2026

CONFRONTING THE ILLICIT-FINANCE HYDRA IN CRYPTO MARKETS: PROTECTING RETAIL INVESTORS AND DISRUPTING HOSTILE GOVERNMENT EXPLOITATION

By ALEXANDER BROWDER

Published in 2026 by The Henry Jackson Society

The Henry Jackson Society
Millbank Tower
21-24 Millbank
London SW1P 4QP

Registered charity no. 1140489
Tel: +44 (0)20 7340 4520

www.henryjacksonsociety.org

Title: “CONFRONTING THE ILLICIT-FINANCE HYDRA IN CRYPTO MARKETS:
PROTECTING RETAIL INVESTORS AND DISRUPTING HOSTILE GOVERNMENT EXPLOITATION”
By Alexander Browder

£9.95 where sold

Cover image: George Washington's image on US Dollar banknote with golden Bitcoin cryptocurrency coin by Robert Avgustin at Shutterstock (https://www.shutterstock.com/image-photo/closeup-george-washingtons-image-on-us-1224403570).

HJS
Henry
Jackson
Society

DEMOCRACY | FREEDOM | HUMAN RIGHTS

CENTRE FOR RESILIENT SOCIETY

March 2026

About the Author

Alexander Browder is the author of the report "Confronting the Illicit-Finance Hydra in Crypto Markets: Protecting Retail Investors and Disrupting Hostile Government Exploitation". Founder of the Global Cryptocurrency Laundering Database, the first open-source global database, which comprises 164 cases of crypto laundering in the last 20 years, Alexander is a young global leader, focused on issues of leadership, innovation, and the balance of responsibility of young adults and tech companies. He has spoken at international conferences, and his opinion column has been featured in *The Times*.

Acknowledgements

I am grateful to all those whose insights and guidance have informed the preparation of this report. In particular, I wish to thank Michael Mcmanus and external reviewers. Their reflections and advice were helpful. Finally, I would like to thank Kirill Korneev and Mykola Kuzmin for their valuable assistance in the production of this paper.

Contents

About Us

DEMOCRACY | FREEDOM | HUMAN RIGHTS

About The Henry Jackson Society

The Henry Jackson Society is a think-tank and policy-shaping force that fights for the principles and alliances that keep societies free, working across borders and party lines to combat extremism, advance democracy and real human rights, and make a stand in an increasingly uncertain world. The Henry Jackson Society is a company limited by guarantee registered in England and Wales under company number 07465741 and a charity registered in England and Wales under registered charity number 1140489.

For more information, please see **www.henryjacksonsociety.org**.

CENTRE FOR RESILIENT SOCIETY

About the Centre for Resilient Society

The **Centre for Resilient Society (CRS)** is a citizen-focused, international research centre within the Henry Jackson Society, which seeks to identify, diagnose and propose solutions to threats to the social resilience of liberal Western democracies.

The centre's work includes addressing the twin challenges posed by radicalisation and terrorism. The centre is unique in addressing violent and non-violent extremism. By coupling high-quality, in-depth research with targeted and impactful policy recommendations, it aims to combat the threat of radicalisation and terrorism in our society.

The centre's work also includes broader challenges of democratic resilience – including threats from both foreign interference and domestic issues. This includes the potential harm that various forms of social, cultural and political insecurity, conflict and disengagement can pose to the long-term sustainability of democracies, including the resilience of their institutions, public policy outcomes, citizens' health and wellbeing, and economic growth and prosperity. It also explores the balance between free speech and hate speech, and encourages respectful debate between those of different views, rather than cancellation. Moreover, it underscores how social and political instability can make nations vulnerable to internal and external actors seeking to deepen cleavages, undermine consensus and, ultimately, to weaken democratic functioning.

1. Executive Summary

This report is the first overview of cryptocurrency-enabled money laundering based on a newly created proprietary database spanning 164 cases across 20 years (2005 to 2025).

The total volume of illicit funds which have been laundered through cryptocurrency identified in these 164 cases amounts to $350 billion.

Over the full period examined, the compounded annual growth rate (CAGR) in the number of cases is 16.5%, reflecting a pronounced rise in the frequency of laundering cases. Across the cases examined, the recovery rate for funds stolen or obtained through illicit means has averaged 27%.

The cases span the globe from Asia and the Middle East to Europe and the United States. Many cases are not attributable to any single country. The geographies which are most affected or identified as points of origin are: 1) United States, 2) Russia and 3) United Kingdom.

The report is broken down into three different categories reflecting the three traditional stages of money laundering: on-ramps (placement), layering and off-ramps (integration). The report examines the trends and legal actions for each stage.

Within the on-ramps (identified as entry points into cryptocurrency), the report highlights six different mechanisms – Darknet Marketplaces, Hacks, Ransomware, Ponzi Schemes, ATMs and Criminal Enterprises – which in total amount to $127 billion at time of occurrence, or $307 billion in present value. $90.2 billion has been seized through successful legal actions by international law enforcement authorities, representing only 29% of the total illicit funds processed through on-ramp channels.

Within the layering stage, the report has examined four categories: on-chain, cross-chain, decentralised finance (DeFi) and digital coins. Each involves a range of different techniques and services. This report has highlighted five high-level techniques for on-chain, two techniques for cross-chain and four for DeFi. The most significant use has been in on-chain – through mixers, with $9.2 billion of illicit funds being moved through 10 mixers. They act as a key instrument for launderers to reduce the trace of their funds.

The choice of coin is an important mechanism for layering, and the report presents a detailed table summarizing the key characteristics of the coins most adopted for laundering. The report discusses 15 highly used instruments, including cryptocurrencies, privacy coins and stablecoins, and identifies particular features that make them susceptible for use in money laundering.

The report demonstrates that, historically, Bitcoin (BTC) was the primary currency used for illicit transactions, reflecting its early adoption and dominance in cryptocurrency markets. However, stablecoins are now increasingly preferred, largely due to their reduced price volatility and the availability of off-ramps that, in some cases, operate under weaker oversight and compliance regimes.

Within the off-ramps, the Global Cryptocurrency Laundering Database features 14 Centralised Exchanges (CEXs) and over-the-counter (OTC) products, and five payment platforms with a total of $22 billion of illicit outflows. CEXs have become the prominent method for criminals to turn their cryptocurrency into cash, and even regulated exchanges have had serious incidents of large amounts of laundering. From legal actions targeting off-ramp services, authorities have seized less than $500 million.

Across these different stages, the report draws out a set of trends and conclusions:

First, given the pseudonymous nature of cryptocurrency transactions, an alarming trend has emerged: a rise in physical violence against victims, intended to coerce transfers, steal assets and, in some cases, advance hostile state objectives.

A second recent development has been the increase of 'pig butchering' where innocent victims have been targeted in romance and fake investment scams. These schemes pose particular risks to those less familiar with emerging technologies, increasing the likelihood that ordinary individuals will be exploited.

Thirdly, different platforms highlighted in the database have either facilitated criminal financing or served as a proxy for hundreds of thousands of criminals and state actors. North Korea receives one-third of all government revenue from cryptocurrency schemes, which provide key funding for the state's weapons program. In addition, there have been thousands of services which have provided business to other hostile actors such as ChipMixer, which processed millions for the Russian GRU. Half of the CEX and OTC exchanges have conducted their operations from Russia. Four out of the five ransomware groups covered in the database were based in Russia and the fifth in Iran.

Across the cases examined, criminal enforcement action was pursued in 70 cases, and convictions were secured in 35 cases. Sanctions were imposed in 21 cases. In total, approximately $92 billion in assets was seized.

The US and Germany have been most active in enforcement and protecting victims. The report highlights that authorities in China and Russia have pursued prosecutions against certain actors, while simultaneously allowing many operators and platforms to proliferate. In contrast to efforts to disrupt these schemes, North Korea appears to have benefited from and, in some instances, supported their continuation.

Of the 164 cases in the database, 79% have resulted in no convictions. Most of these crimes go unpunished and more vigilant prosecution needs to be carried out.

There is a credible basis for optimism: several cases examined in this report demonstrate that cross-border litigation can facilitate the recovery of victims' funds and bring justice. Governments have taken decisive action through criminal investigations and prosecutions and, where perpetrators are beyond their reach, through sanctions measures. These tools are particularly relevant when offenders operate from jurisdictions that do not extradite their citizens.

In addition, there has been a growing set of enforcement and compliance actions by exchanges and other legitimate cryptocurrency service providers, including programs such as T3 and the expanded T3+.

While cryptocurrency is likely to remain a permanent feature of the financial landscape, protecting victims, who often face repeated hacking attempts, fraud and, in some cases, physical violence, requires targeted action.

This report concludes with 10 recommendations which are highlighted below:

1. Fully implement and harmonise crypto regulatory standards, including the Travel Rule.
2. Build specialist enforcement agencies and training units designed to protect victims and stop malicious activity.
3. The UK and the EU should establish a Cryptocurrency Asset Recovery Office to hold recovered funds and transfer them back to the rightful owners, similar to the US.

4. Release clearer guidance on high-risk services to stop sanctions evasion and protect victims.
5. Countries should create Crypto Risk Registries and have exchanges display them to protect retail investors.
6. Strengthen public–private partnerships to enable quick and swift detection and recovery of illicit flows.
7. Introduce a whistleblower reward scheme to reduce large schemes which target thousands of victims.
8. Authorities and exchanges should introduce fast-freeze mechanisms and 'kill switches' that allow rapid, time-limited freezing of assets where there is an immediate risk of dissipation.
9. Utilise AI tools to aid investigators and services to protect users.
10. Adopt responsible crypto advertising and coverage standards that both protect audiences and spotlight victims.

2. Key Highlights

- The total volume of illicit funds which have been laundered through cryptocurrency in the known 164 cases identified in the Global Cryptocurrency Laundering Database amounts to $350 billion.
- The compounded annual growth rate (CAGR) in the number of cases is 16.5%.
- Convictions have only been obtained in 21% of cases.
- Sanctions were imposed in 13% of cases.
- 54 cases have not faced any legal action.
- Stablecoins are now responsible for the majority of laundering, with new ones specifically designed to evade sanctions such as A7A5.
- Guarantee markets account for over $57 billion in illicit flows, dwarfing regular darknet marketplaces.
- $112 billion in additional premium value was added to the hackers due to the 'post-hack appreciation' of the value of coins.
- Half of the illicit CEX and OTC exchanges conducted their operations from Russia.
- Four out of the five major ransomware groups were based in Russia and the fifth was in Iran.
- One-third of North Korean Government revenue stems from illicit cryptocurrency schemes.
- Only 27% of assets – amounting to $92 billion – have been seized or recovered from all 164 cases.
- The highest asset recovery rate – 37% – has been achieved in relation to Ponzi schemes.
- A mere 2% of illicit assets were seized in relation to off-ramp channels.
- 31 cases of hacks have resulted in 0% recovery.

3. Introduction

In Greek mythology, the Lernaean Hydra was a multi-headed serpent whose most disturbing trait was not its size, but its resilience: whenever Heracles severed one head, two grew back in its place. Only by changing tactics and cauterising each neck as he struck, could he finally subdue the creature. Crypto money laundering exhibits the same regenerative behaviour. When one mixer is shut down, funds are rerouted through new protocols or exchanges. When a well-known laundering channel is exposed, substitute services and more complex layering patterns appear.

The Hydra offers a powerful frame for understanding why enforcement actions that merely 'cut off heads' are insufficient, and why durable progress against crypto laundering depends on measures that prevent new heads from emerging in place of the old ones.

Money laundering has been around for centuries. Three thousand years ago, Chinese merchants, facing official threats or confiscation risk, would hide their wealth, convert it into portable assets, such as jade or precious metals, and move them outside the local ruler's reach. This was just the beginning of an international market.

Initially, criminal money laundering occurred exclusively through cash, and later it evolved to make use of the banking system. As regulators wised up to the methods criminals had used, rules were put in place to curtail the criminal laundering. For cash, these included: cross-border cash declaration thresholds, registration of cash-intensive businesses and practical limits for withdrawing cash. With the expansion of banking, rules have been put in place which require banks to file Suspicious Activity Reports (SARs) for suspicious transfers, conduct know-your-customer (KYC) verification for clients, and undergo independent audits to help ensure the integrity of financial flows.

With the banking system becoming well regulated, criminals looked for additional ways to launder money. Following the emergence of cryptocurrency, new opportunities to launder funds developed. As the volume of cryptocurrency transactions soared, so did their use as a money laundering tool, representing a new, less understood and less regulated channel to move money.

The share of cryptocurrency laundering still remains small as a percentage of total laundering, estimated at less than 2% in 2024. The UN Office on Drugs and Crime estimates that 2–5% of global GDP is laundered each year via all channels. In 2024, this amounted to between $2.2 and $5.5 trillion. The share of laundering in cryptocurrency is gradually increasing.

This unique report builds on a newly created proprietary open-source database of money laundering cases, available at: **launderingdatabase.org**.

Based on the findings and analysis of 164 cases included in the Global Cryptocurrency Laundering Database, it is estimated that over the past 20 years, close to $350 billion in illicit funds has been moved through the crypto ecosystem. The number of cases has grown by 16.5% CAGR.

This report explores the cryptocurrency ecosystem and how criminals exploit it for money laundering. It examines the harm caused to victims and society, reviews legal responses and provides recommendations to strengthen enforcement and compliance.

4. Launderingdatabase.org – Global Cryptocurrency Laundering Database

The Global Cryptocurrency Laundering Database (**launderingdatabase.org**) presently comprises 164 cases of high-profile events of cryptocurrency laundering during the last 20 years (2005–2025). It builds on cases that have been identified publicly, allowing us to draw conclusions about the circumstances and responses to the instances of laundering.

The Global Cryptocurrency Laundering Database is broken down into three different parts. The first part is the on-ramps (entry points) which contains 130 different cases, involving cryptocurrency flows worth a total of $307 billion in present value.

The second part of the database includes mixers, bridges, currencies and CoinJoin services. It contains 14 cases that moved a total of $11.7 billion in illicit flows. In addition, it examines a range of laundering methods and currencies that launderers commonly use.

The third part includes the services and integration providers, and contains 19 cases with a total of $24.6 billion of illicit flows passing through them.

Figure 1: Breakdown by category of cases in the Global Cryptocurrency Laundering Database

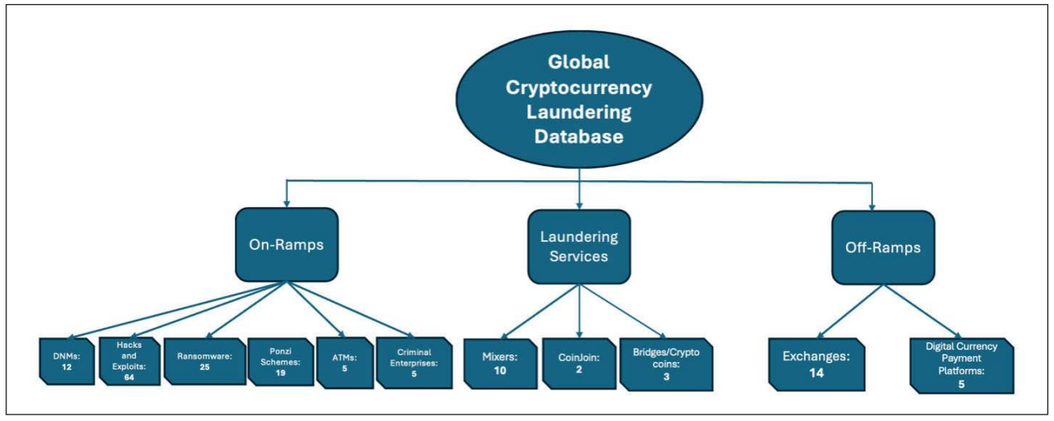


Table 1: Cases by category identified in the Global Cryptocurrency Laundering Database

Darknet Marketplaces	12
Hacks and Exploits	64
Ransomware	25
Ponzi Schemes	19
ATMs	5
Criminal Enterprises	5
Mixers/CoinJoin	12
Bridges/Cryptocurrency	3
Exchanges	14
Cryptocurrency Payment Platforms	5
TOTAL	**164**

The main method of obtaining information on cases for the database has involved gathering and examining publicly documented cases of laundering. The database incorporates well-known cases as well as records of on-ramps and illicit services that are less prominent. Research for cases has included scouring news archives, researching expert papers on cryptocurrency laundering and participating in the 9th Global Conference on Criminal Finances and Cryptoassets in October 2025.

For each case, the database identifies the following characteristics:

- Type of case
- Name of leader or group
- Location
- Origin date
- Disruption date
- Amount of illicit funds transferred
- Value of funds at present
- Amount of funds recovered
- Harm
- Current status
- Legal action
- Authorities involved in the case
- Links to mixers and laundering facilities
- Additional highlights.

A selection of five cases from the database is presented below for illustrative purposes:

Figure 2: Excerpt of five cases from the Global Cryptocurrency Laundering Database

Number	Name	Type	Leader(s)/ Group	Origin Date	End	Amount at Origin	Value at Seizure/Present	% Recovered/From	Region	Victims	Harm	Status	Legal Action	Prosecutor	Links to Mixers and Laundering facilities	Highlights
1	**Bitfinex Hack**	Security-infrastructure exploit	Ilya "Dutch" Lichtenstein	2/8/2016	14/11/2024	$72,000,000	##########	80%	Hong Kong	Retail and Institutional Investors	All users had a 36.067% reduction in their account balance, , being one of the largest exchanges, it could have potentially impacted thousands of its users.	Convicted; Lichtenstein plead guilty and was sentenced to 5 years in Prison.	Criminal: 1 Count of Conspiracy to commit money laundering; Court Seizure of 114,600 BTC and 7,113 ETH.	Head of Justice Department's Criminal Division, U.S. Attorney for the District of Columbia, Chief of IRS Criminal Investigation, Assistant Director of FBI's Cyber Divsion, Special Agent of the FBI Chicago Field Office, Special Agent of Homeland Security Investigations (HSI) New York Field Office	AlphaBay, Wasabi, Hydra	119,754 BTC Stolen, Value of the BTC rose to 3,600,000,000, Used Gift Cards for Off Ramp, Court Forfiture recovered ~80% of funds
2	**Silk Road Hack**	Exploitation	James Zhong	??/09/2012	14/04/2023	$625,000	##########	####	Georgia, U.S.A	N/A	Inside Job, Stealing money which was made from illicit goods.	Convicted: Zhong plead guilty and was sentenced to 1 year and 1 day in prison.	Criminal: 1 Count of Wire Fraud; Court Forfiture of 51,680 BTC and cash and gold.	United States Attorney for the Southern District of New York	Silk Road	51,680.32473733000 44 BTC, Total Value when seized was ~$3,600,000,000, Zhong used Casascius coins and faraday cages to increase the level of anonimity.
3	**MtGox Hack**	Exchange Compromise	Alexey Bilyuchenko , Aleksandr Vemer	########	Present	$83,000,000	##########	####	Tokyo, Japan	Consumer and Corporate Users	22,560 individual creditors	Charged	Criminal: Both: 1 Count of Conspiracy to Commit Money Laundering. Bilyuchenko: Additonal Counts of Conspiracy to Commit Money Laundering and Operating an Unlicensed Money Services Business. Civil: Civil Asset Forfeiture complaint against all assets seized from the exchange BTC-e back in 2017, which includes 300,000 BTC funded through the exchange from the Mt Gox Hack.	Criminal: United States Attorney for the Southern District of New York, Assistant Attorney General for the Department of Justice's Criminal Division, United States Attorney for the Northern District of California, Chief of the Internal Revenue Service-Criminal Investigation, Assistant Director in Charge of the New York Field Office of the Federal Bureau of Investigation, Special Agent in Charge of the U.S. Secret Service's Criminal Investigative Division, Acting Executive Associate Director of Homeland Security Investigations. Civil: Special Agent with the	BTC-e, Alexander Vinnik	647,000 Bitcoin stolen. Money was moved through two different other exchanges, >300,000 Bitcoin was laundered into cash through an Advertising contract cashing out $6.6 million. It recovered 200,000 BTC in an old wallet. There are seperate convictions for the laundering of the Mt Gox funds.
4	**ByBit Hack**	Social Engineering Attack	Lazarus Group	21/02/2025	Present	$1,460,000,000	##########	<6%	Dubai, UAE	Exchange and Retail Investors	It sparked volatility in the price of BTC and ETH; ByBit had to recover the funds themself and North Korea has allegedly been provided with significant capital for weapons. Many people lost their funds	Under Investigation	Greece: Hellenic Anti-Money Laundering Authority issued a freezing order for part of the funds which were stolen from ByBit. USA: FBI released a PSA warning of North Korea's involvement in the scheme and identifying addresses linked to it.	N/A	THORChain Bridge, Wasabi Wallet, Cryptomixer, Jambler, Coinomize, eXch, Railgun, Tornado Cash	In under 48 hours the bad actors had started laundering the money. Over $1 Billion has been laundered. It was the largest ever hack of an exchange.
5	**Coincheck Hack**	Malware Attack	Uknown	25/01/2018	Present	$534,000,000	N/A	0%	Tokyo, Japan	Retail Investors	260,000 customers had all of their funds stolen; however, later 90% were reimbursed.	Unresolved	Japan: Criminal: Two were charged on the count of Accepting Criminal Proceeds prohibited under the Act of Punishment of Organized Crimes, Control of Crime Proceeds and Other Matters (Allowing the XEM to be exchanged). One has pled not guilty. Civil: Financial Services Agency (FSA) issued an administrative "business improvement" order to Coincheck and launched nation-wide inspections of all domestic crypto exchanges. Tokyo District Court issued, on 30 March 2020, a protective order for confiscation against a company managed by one of those criminal suspects and	Tokyo District Public Prosecutors Office		Tokens stored on a hot-wallet. Used a self-run Darknet marketplace as an Off ramp, trading their stolen XEM tokens at a 15% discount, the buyers who exchanged the stolen XEM were charged.

The Global Cryptocurrency Laundering Database is by definition not fully complete. Due to the inherently pseudonymous and rapidly evolving nature of the sector, and the lack of documentation or definitive proof in many cases, there are understandable difficulties in tracking and analysing cryptocurrency activity. Cases may be missing or disputed because of the nature of this field, and thus it is an avenue for further enquiry. This means that the data gathered is not comprehensive, and is open to correction and expansion. The database captures only those laundering events that became visible through enforcement or reporting. It offers a streamlined way in which individual cases and trends can be tracked and analysed.

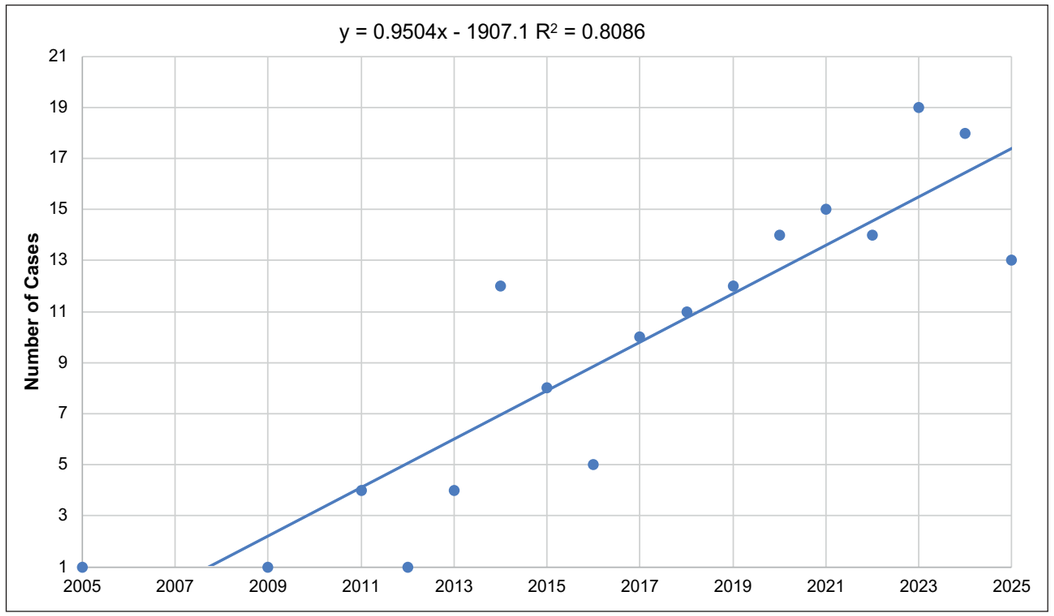
The cases have been included in the database based on several criteria: confirmation from multiple sources regarding the incident, the availability of supporting evidence from secondary studies and the high amounts of illicit funds.

The **launderingdatabase.org** also provides resources aimed at aiding those who are vulnerable to exploitation and laundering, and is a useful tool for law enforcement authorities, industry experts and victims of cryptocurrency crimes.

5. Trends in Incidents of Laundering

A review of 164 cases over the past 20 years indicates a clear increase in the number of cryptocurrency-related money-laundering incidents reported each year. Over the past decade, cryptocurrencies have become a prominent mechanism used by bad actors and hostile regimes to finance activities and launder proceeds of crime.

Figure 3: A scatter plot depicting the number of laundering cases at origin against time



As seen on the graph above, there is a direct correlation between time (measured since 2005 onward) and the annual number of reported laundering incidents, consistent with the positive fitted trend line (slope = 0.9504).

This can be explained by the increase in the volume of transactions and number of users in the crypto ecosystem. There are years in which the number of cases spike upwards: namely in 2014, which coincides with the first hack of a large Japanese exchange, Mt. Gox, which lost 640,000 BTC, with much of it being sent to different laundering avenues, with effects still felt today.[1]

The first case in 2005, Liberty Reserve, is particularly noteworthy because it was among the earliest systems to operate, predating major cryptocurrencies such as Bitcoin and Ethereum. Operating out of Costa Rica, Liberty Reserve allowed users to purchase credits via wire transfers to the reserve, which were then converted into 'Liberty Reserve Dollars' or 'Liberty Reserve Euros' for processing.[2] It accounted for a total illicit volume of $6 billion.[3] The founder was convicted and sentenced to 20 years in prison in 2016.

[1] Christian Decker and Roger Wattenhofer, "Bitcoin Transaction Malleability and MtGox", *Computer Security – ESORICS* (2014, vol. 8713), https://doi.org/10.1007/978-3-319-11212-1_18.

[2] "Founder of Liberty Reserve Pleads Guilty to Laundering More Than $250 Million through His Digital Currency Business", U.S. Department of Justice, 29 January 2016, https://www.justice.gov/archives/opa/pr/founder-liberty-reserve-pleads-guilty-laundering-more-250-million-through-his-digital.

[3] Jack Cloherty, "'Black Market Bank' Accused of Laundering $6B in Criminal Proceeds", *ABC News*, 29 May 2013, https://abcnews.go.com/US/black-market-bank-accused-laundering-6b-criminal-proceeds/story?id=19275887.

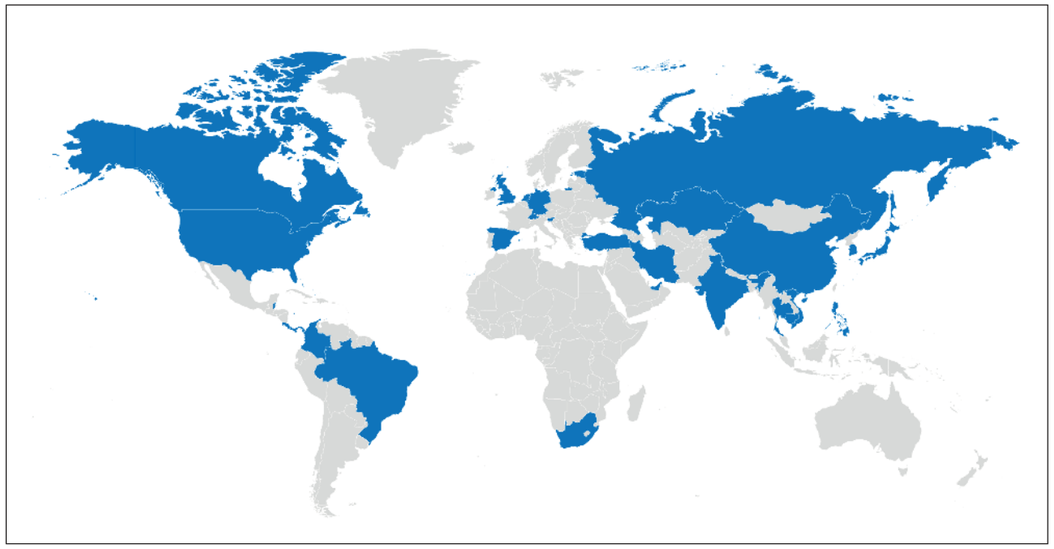
The rising number of cases indicates that cryptocurrency laundering has become a widely adopted method of laundering, and thus should be considered a high-priority issue for governments, exchanges and individuals who are transacting on different platforms.

6. Geography of Cases

Cryptocurrency is an inherently global industry. This report has identified 37 different countries where illicit cryptocurrency activity has been reported or has originated from. Geographical identification relied on either the on-ramp's target country or the origin of the illicit service provider.

This geographical map illustrates that illicit cryptocurrency laundering has become a transnational issue.

Figure 4: Geographical map of illicit crypto flows



Many cases included in the Global Cryptocurrency Laundering Database do not have a clearly defined geographic region. This is because the underlying services often operate entirely online, and counterparties are spread across multiple jurisdictions. As a result, transactions can pass through several countries in seconds, making it difficult to attribute the activity to a single location or to pin down where the criminal conduct is exclusively taking place. There are 31 events recorded in the database where this was the case.

Despite the cross-border characteristic of digital currency flows, a majority of recorded cases – 39 of 164 (23.8%) – have been concentrated in the United States. As a global financial centre, the US intrinsically presents more opportunities for money laundering activity and has a higher likelihood that victims will be targeted.

Russia accounts for the second-highest number of cases, with 19 recorded incidents or 11.6%. This could be attributed to the large size of the population, the sophistication and focus of the crypto criminals and the state support and funding for this activity. This concentration is also consistent with the widespread use of cryptocurrency as a tool to circumvent international sanctions imposed on the country and its individuals and entities.

The country with the third highest concentration of cases is the UK, with seven cases recorded in the database. For example, the prominent clothing retail company FatFace faced a ransomware attack in 2021. The criminals reportedly gained access to the company's data

via phishing, spent days moving through internal systems, then encrypted key business functions and stole roughly 200 GB of data. They initially demanded around $8 million, but after negotiation, the settlement was reported at about $2 million in exchange for a decryptor and a promise not to leak the stolen files. [4]

Five cases were identified in the Seychelles – $5.5 billion in illicit funds have either been stolen from or processed there.

Other notable countries include: China, Estonia, Germany, Hong Kong, Japan, Singapore and South Korea with four cases each.

Overall, each case spans multiple jurisdictions, complicating the legal and regulatory efforts required to mitigate and disrupt such activity.

[4] Alex Scroxton, "Retailer FatFace pays $2m ransom to Conti cyber criminals", *Computer Weekly*, 26 March 2021, https://www.computerweekly.com/news/252498463/Retailer-FatFace-pays-2m-ransom-to-Conti-cyber-criminals.

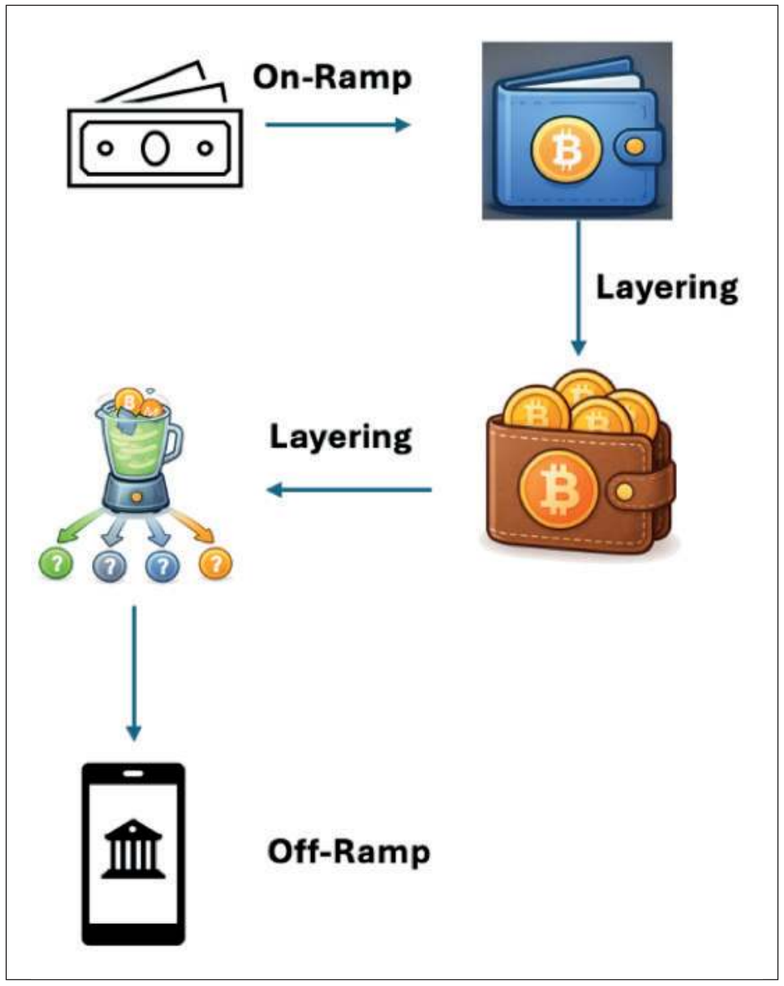
7. Different Stages of Laundering

In traditional analysis, classical money laundering follows three main stages: 1) placement, 2) layering and 3) integration. This report follows the cryptocurrency laundering along these three stages. However, in this new ecosystem, laundering becomes much more complicated and intricate.

First, money has to enter the virtual space through different channels known as on-ramps. Bad actors may also leverage existing cryptocurrency holdings that are already present in the ecosystem, rather than acquiring new funds through external on-ramps. Next, the funds are typically obfuscated to reduce traceability back to their source. This process takes place through a variety of distinct layering patterns. Once the funds have been 'cleaned', most bad actors attempt to move the funds off the chain into fiat (via off-ramps), in order to completely break the traceability of the source and the funds.

The model below illustrates the three stages of money laundering in the crypto sphere.

Figure 5: Cryptocurrency laundering model



Let's look at a hypothetical case of a malicious actor – a local drug dealer who sells his drugs on the darknet and wants to launder the proceeds from the drug sale (Person A).

Person A first completes a transaction on a darknet marketplace and funds would be immediately sent to his specific cryptocurrency address from the buyer. He would then send the drugs, for instance, fentanyl. The funds in this situation have been placed onto the cryptocurrency ecosystem through an on-ramp. He must now find a way to convert the funds into cash without having them seized.

The funds are then moved through multiple wallets using a range of methods, including mixers, which makes them more difficult to trace directly. Person A could then move their funds through different chains and could also utilise decentralised finance.

Once Person A feels like the funds are ready to be converted into cash or spent, the objective is to integrate the assets back into the regular world. Person A could contact an illicit over-the-counter broker to try and sell his cryptocurrency for cash. If that fails, there are different services which cater directly to criminals, such as high-risk exchanges, although there are more risks for Person A's funds.

This simplified account reflects the structure observed in the majority of cases, although in practice, these schemes often involve multiple strands and deploy hundreds of wallets.

This report analyses the structures and actors at each stage, following the sequence set out in the illustrative narrative.

8. Placement and On-Ramps

In classic money laundering, *placement* is when the proceeds of crime are, for the first time, introduced into the legal financial system. [5]

In the crypto space, placement is the first entry point where illicitly gained funds are introduced or made exchangeable in the crypto ecosystem. It relieves offenders of bulky cash and is often the riskiest moment for actors seeking to avoid detection. The processes through which offenders get onboarded are known as 'on-ramps'.

Because many crypto crimes begin with funds that are already held in virtual assets, the placement stage can be compressed or absent.

The bulk of the placement within the digital ecosystem occurs through specific 'on-ramps' which vary in the mechanisms and tools employed.

This report has identified the following six types of on-ramps:

1) Darknet Marketplaces;
2) Hacks and Exploits;
3) Ransomware;
4) Ponzi Schemes;
5) Automatic Teller Machines (ATMs);
6) Criminal Enterprises.

The Global Cryptocurrency Laundering Database comprises 130 on-ramp cases. The table below shows the breakdown by the type of on-ramp.

Table 2: Categories of on-ramps highlighted in the Global Cryptocurrency Laundering Database

	Darknet Marketplaces	Hacks and Exploits	Ransomware	Ponzi Schemes	ATMs	Criminal Enterprises	Total
Number	12	64	25	19	5	5	130
Illicit Assets (Millions, $)	65,600	12,810	1,540	21,300	53	25,940	127,243
Present Value (Millions, $)	N/A	124,850	16	88,500	N/A	N/A	306,753
Legal Action	9	21	21	19	5	5	75
Convictions	4	6	5	11	5	0	31
Asset Seized (Millions, $)	4,300	37,300	42	32,931	14	15,574	90,161

These six categories of on-ramps are discussed below.

[5] "Economic crimes", *Eurojust*, https://www.eurojust.europa.eu/crime-types-and-cases/crime-types/economic-crimes.

1) Darknet Marketplaces

Darknet marketplaces (DNM) are hidden, eBay-style bazaars tucked behind anonymity networks like Tor, where pseudonymous buyers and vendors trade mostly illicit goods and services, using cryptocurrencies. Most DNMs take buyer funds into a centralised escrow, then release payouts to vendors minus the market's commission.

Darknet commerce is organised around two models: (a) regular marketplaces that host listings and handle their own escrows, ratings and vendor management and (b) guarantee services that just escrow and arbitrate deals happening between customers. [6]

The two models are distinct in how they operate:

a) Regular DNMs

A platform with listings, a search engine, vendor pages, ratings and usually built-in escrow that the site controls. Buyers pay the market and vendors ship or deliver. These platforms range from multi-vendor marketplaces (with many sellers) to single-vendor shops that operate as a dedicated storefront for one seller. In both cases, the model remains platform-based commerce rather than an ad hoc escrow.

b) Guarantee DNMs

A service, not a catalogue. Deals are brokered peer-to-peer (often on forums/Telegram), while a neutral third party, called an escrow or a guarantor, holds the buyer's crypto and releases it once the goods/services are received. Fees are typically charged at a few percent, sometimes higher for risky or large deals. These services can be run by the forum itself (official guarantors) or by independent intermediaries. They provide arbitration when disputes arise.

Many DNMs provide laundering instruments as part of their service package, meaning the illicit funds are concealed even before they leave the on-ramp. Many of them deploy the same system of distribution and laundering and are primarily focused on selling narcotics and fraudulent goods.

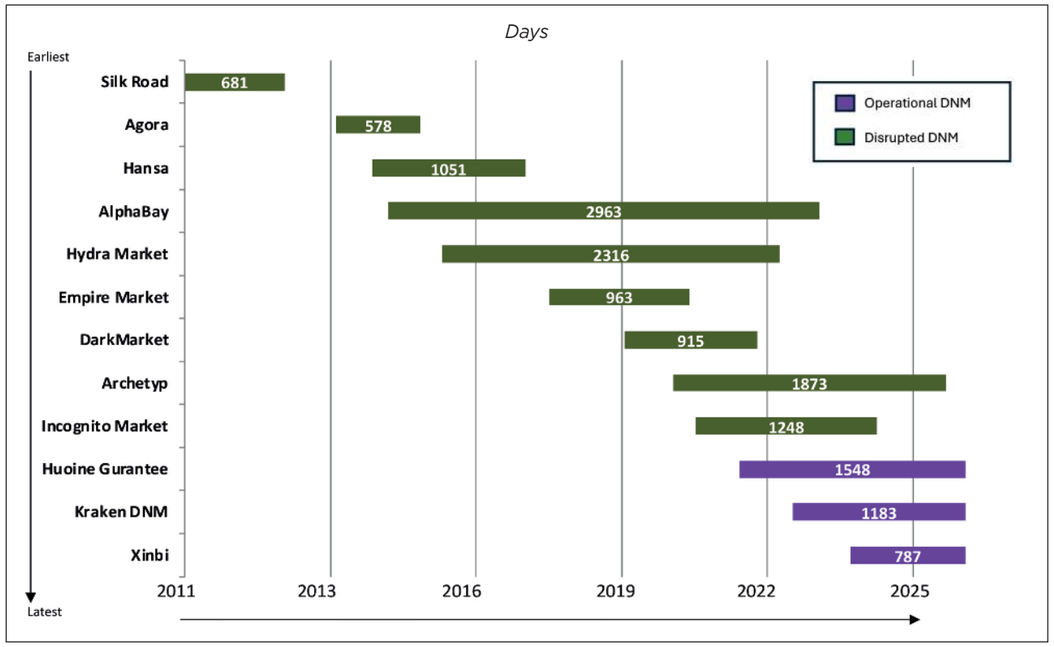
The early marketplaces, such as Silk Road and Hansa Market, predominantly used Bitcoin. In recent years, dark commerce operations have shifted to Monero and stablecoins as the dominant payment platforms. Some of the latest entrants, such as Archetyp, have exclusively used Monero.

There have been many small-scale DNMs that have popped up but they are often easily disrupted and are not able to maintain their operations long term. Many platforms are susceptible to operator-led fraud as an 'exit strategy', whereby operators defraud users and then disappear.

The Global Cryptocurrency Laundering Database includes the 12 largest DNMs, with total funds above $100 million each. A total of $65.6 billion in illicit cryptocurrency has been moved through these networks. Seven out of the 12 DNMs have provided internal laundering services and tools to their customers, directly aiding the obfuscation and layering of ill-gotten gains. The top DNMs had been operational for an average of three years and nine months or roughly 1343 days before their disruption. The first large DNM – Silk Road – appeared in February 2011 and lasted just under two years. The chart below shows the lifespan of the top 12 DNMs.

6 Dimitrios Georgoulias, Jens Pedersen, Morten Falch and Emmanouil Vasilomanolakis, "A qualitative mapping of Darkweb marketplaces", 2021 APWG Symposium on Electronic Crime Research (eCrime), Boston, MA, USA, 2021, pp.1-15, https://doi.org/10.1109/eCrime54498.2021.9738766.

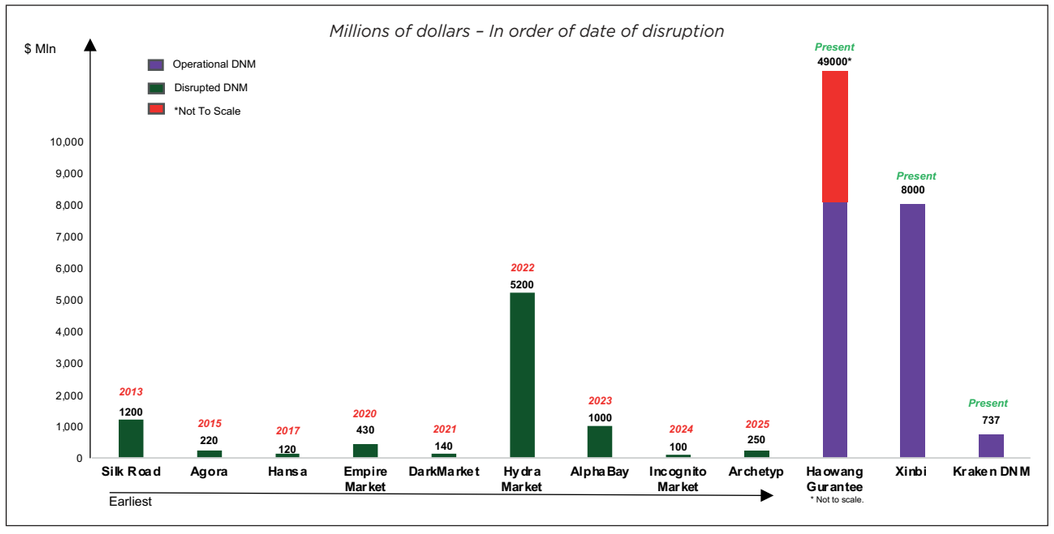
Figure 6: Lifespan of the top 12 DNMs



Six of the top 12 DNMs were created after 2019. During 2021, there were six DNMs operating at the same time. The longest running DNM was AlphaBay, which had been operational for just over eight years. It was disrupted in 2017, and then managed to rebuild and remain open until early 2023, when it voluntarily shut down.

The chart below maps the size of the assets accumulated by the top 12 DNMs and the date of their disruption by law enforcement authorities, starting from the first disruption and ending with the latest.

Figure 7: Scale and disruption of the top 12 DNMs



The two largest DNMs by size are Haowang and Xinbi, which are both guarantee markets. They now account for over $57 billion in illicit flows, or 87.1% of the total flows of the 12 DNMs. The other 10 of the top 12 are regular markets.

Nine of the top 12 DNMs have been disrupted by law enforcement and government actions and have ceased to exist. Two of the three which are still operational follow the guarantee model. Huonine Guarantee was recently banned on Telegram. Rather than stopping its services, it has allegedly merged with other guarantee markets and is onboarding its vendors elsewhere. [7]

Among the 10 regular markets, the largest was Hydra Market which peaked at $5.2 billion in 2022. Based on the size of illicit assets, Hydra was about 10 times smaller than the largest DNM of today, Huonine Guarantee. During the time of its operations, it was approximately five times the size of the nearest comparable large DNM. The rest of the top regular DNMs were under $1.2 billion of volume. The substantial rise of guarantee markets has displayed the dynamism of DNM operators. Xinbi is the newest market, created in 2023. It functions as a guarantee model. It offers illicit services such as sex trafficking, intimidation and stolen personal information databases. In addition, it advertises that it can specifically turn "tainted" cryptocurrency into "white capital" (i.e. clean capital). [8] During its two years of existence, it has reached $8 billion in volume, dwarfing the DNMs of the previous decade.

Xinbi's case illustrates that the guarantee market is growing rapidly. A reason for this growth is the reliance for operations on messaging platforms, such as Telegram. Operators are mobile and able to move decisively. [9] Rather than building their own interface, they can coordinate through bots and direct messaging. This rapid growth in guarantee-based DNMs presents a significant challenge for regulators and the financial system.

Legal Action against DNMs

Law enforcement authorities have been aware of the proliferation of DNMs. Legal action has been taken against nine of them, and eight have been shut down by law enforcement. Criminal charges have been filed in relation to seven DNMs, with money laundering charges issued in five of those cases; the other two faced charges of narcotics and fraudulent goods distribution. As of October 2025, four cases have resulted in convictions:

i) In 2015, the Silk Road founder, Ross Ulbricht, was convicted on seven counts and sentenced to life in prison. The prosecution was led by the United States Attorney for the Southern District of New York. [10] Ulbricht was pardoned in 2025.

ii) In 2022, the operator of DarkMarket, under the pseudonym 'JK', [11] was found guilty in Germany of 1,498 counts of aiding drug trafficking and was sentenced to nine years imprisonment. As a result of the investigation and conviction, German authorities managed to arrest 150 vendors and buyers. The prosecution was led by the Public Prosecutor General's Office of Koblenz. [12]

7 Andy Greenberg, "Chinese Crypto Scammers on Telegram Are Fueling the Biggest Darknet Markets Ever", *Wired*, 23 December 2025, https://www.wired.com/story/expired-tired-wired-chinese-scammer-crypto-markets/.

8 "Xinbi: The $8 Billion Colorado-Incorporated Marketplace for Pig-Butchering Scammers and North Korean Hackers", *Elliptic*, 13 May 2025, https://www.elliptic.co/blog/xinbi-guarantee.

9 "Telegram dark markets expand to fill the gap left by Huione Guarantee", *Elliptic*, 23 June 2025, https://www.elliptic.co/blog/telegram-dark-markets-expand-to-fill-the-gap-left-by-huione-guarantee.

10 "Ross Ulbricht, the Creator and Owner of the Silk Road Website, Found Guilty in Manhattan Federal Court on All Counts", U.S. Attorney's Office, 5 February 2015, https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/ross-ulbricht-the-creator-and-owner-of-the-silk-road-website-found-guilty-in-manhattan-federal-court-on-all-counts.

11 Name concealed due to German Privacy Laws.

12 "Urteil im Strafverfahren „DarkMarket" – 1 KLs 5 Js 503/20 (Judgment in criminal proceedings "DarkMarket" - 1 KLs 5 Js 503/20)", Rhineland-Palatinate, 5 December 2022, https://lgtr.justiz.rlp.de/presse-aktuelles/detail/urteil-im-strafverfahren-darkmarket-1-kls-5-js-503-20.

iii) In 2024, the Incognito Market operator, Rui-Siang Lin, pleaded guilty to three counts, including money laundering, and is scheduled to be sentenced in 2026. The prosecution was led by the United States Attorney for the Southern District of New York. [13] Lin cooperated with law enforcement authorities across multiple countries to help disrupt illicit cryptocurrency laundering, while simultaneously operating one of the world's largest darknet marketplaces.

iv) In 2024, the Hydra Market founder and 15 accomplices were found guilty in a Moscow regional court of several different counts. The sentences ranged from 8 to 23 years for the accomplices, with the founder being sentenced to life. [14] There were also separate charges filed in the United States for an operator of Hydra. [15]

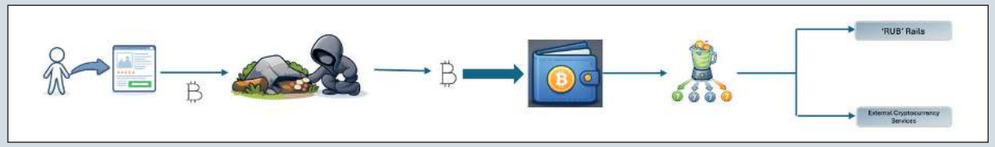
Case Study: Hydra Market

Hydra Market was an on-ramp laundering service and an off-ramp, set up in 2015 in Russia by Stanislav Moiseyev focusing on mainly Eastern European markets. In 2022, it captured over 90% of all darknet marketplaces in flow. [16]

Hydra was both a key service for narcotics sales and a vital on/off ramp. It was the only DNM which had direct operational capability to turn cryptocurrency into fiat currency (before the emergence of new guarantee markets). Mixing at the withdrawal stage introduced an immediate layering step, complicating on-chain attribution back to Hydra. It also reduced the need for users to interface with regulated exchanges, and concentrated demand in a semi-walled ecosystem.

It had an intricate laundering system which is described in the chart below:

Figure 8: Hydra DNM flow chart



Hydra had specific BTC wallets for each vendor on the site. The platform would then automatically send the proceeds through an in-house mixer. This immediately broke the trace between Hydra and the proceeds. The vendors would then either use external layering services or be provided with an in-house option, 'Crypto to Rubble rails'. This is significant as it is one of the only large DNMs which provided a specific internal fiat cash off-ramp. From internal vendors who specialise in over-the-counter services to cash 'dead drop' services, it provided the Russian criminal ecosystem with a way to fund illicit activities.

After Hydra's takedown, a flurry of smaller DNMs tried to fill the gap which Hydra had left. A series of 'wars' broke out between contesting Russian DNMs involving serious hacks, violence

13 "'Incognito Market' Owner Pleads Guilty For Operating One Of The Largest Illegal Narcotics Marketplaces On The Internet", U.S. Attorney's Office, 16 December 2024, https://www.justice.gov/usao-sdny/pr/incognito-market-owner-pleads-guilty-operating-one-largest-illegal-narcotics.

14 "Russia Sentences Alleged Founder of Hydra Darknet Market to Life in Prison", *The Moscow Times*, 2 December 2024, https://www.themoscowtimes.com/2024/12/02/russia-sentences-alleged-founder-of-hydra-darknet-site-to-life-in-prison-a87198.

15 "Justice Department Investigation Leads To Shutdown Of Largest Online Darknet Marketplace", U.S. Attorney's Office, 5 April 2022, https://www.justice.gov/usao-ndca/pr/justice-department-investigation-leads-shutdown-largest-online-darknet-marketplace.

16 "How Darknet Markets and Fraud Shops Fought for Users In the Wake of Hydra's Collapse", *Chainalysis*, 9 February 2023, www.chainalysis.com/blog/how-darknet-markets-fought-for-users-in-wake-of-hydra-collapse-2022/.

and propaganda campaigns.[17] It was conducted by launching distributed denial of service (DDoS) attacks and intrusion campaigns to knock rivals offline, disrupt withdrawals and publicise alleged compromises. Although many were not successful, some DNMs, like Kraken, managed to capture some of the illicit flows.

Legal action to combat the new guarantee markets has been less successful. Cambodia-based Haowang Guarantee has managed to continue its operations. In May 2025, the US Treasury's Financial Crimes Enforcement Network (FinCEN) identified Huione Group as a financial institution of primary money laundering concern, and in October 2025, issued a final rule that severed it from the US financial system, under the Patriot Act.[18]

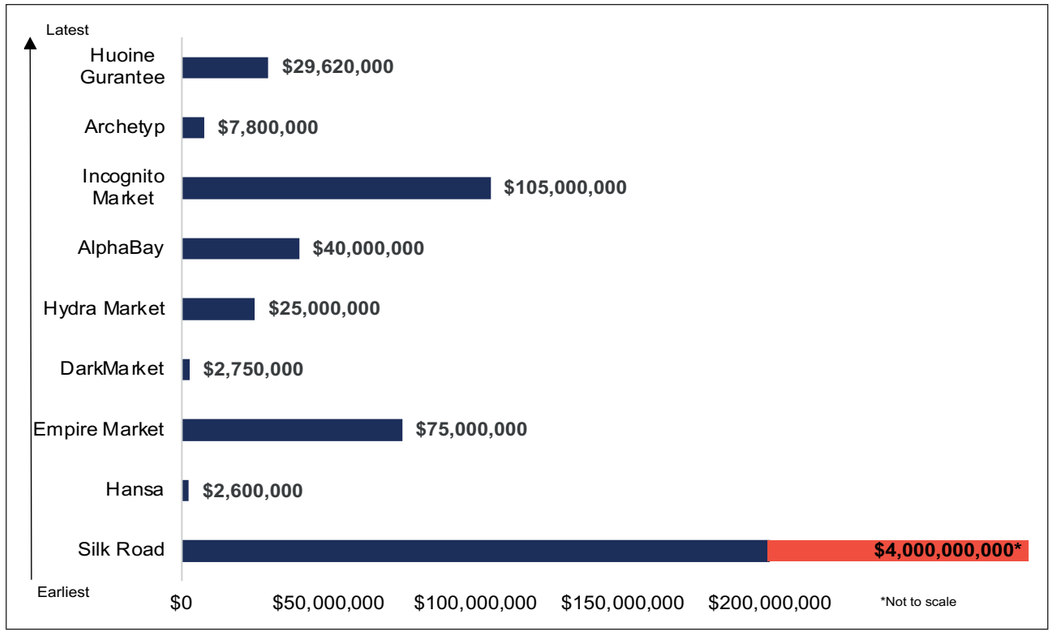
Asset Seizures in DNM Cases

As legal actions are undertaken, governments have the ability to seize cryptocurrency assets from the DNMs. However, the amount that has been seized is much lower than the amount the DNMs have processed.

Out of the top 12 DNMs, successful seizures have been undertaken in eight cases. Close to $4.3 billion in cryptocurrency has been seized by law enforcement authorities, but this represents only 7.1% of the total inflow into these DNMs. This low ratio reflects the difficulties of fighting illicit cryptocurrency inflows on DNM on-ramps, as most vendors on DNMs immediately move their profits along the chain.

The graph below shows the total value of assets seized for the eight DNMs.

Figure 9: Value of asset seizures – top eight DNMs



17 Max Daly, "Dead drops, PR stunts and punishment beatings: the rapid rise of Russia's powerful darknet drug industry", *The Guardian*, 14 November 2024, https://www.theguardian.com/world/2024/nov/14/russia-rise-of-powerful-darknet-drug-industry-dead-drops-punishment-beatings.

18 "Imposition of Special Measure Regarding Huione Group, as a Foreign Financial Institution of Primary Money Laundering Concern", Federal Register, 16 October 2025, https://www.federalregister.gov/d/2025-19571/p-3.

The biggest seizure came from Silk Road which had a total of $4 billion confiscated on three separate occasions. The last two seizures were executed five years after the conviction of the operator of Silk Road and totalled 120,046 BTC.[19] These actions suggest that enforcement efforts can bring successful outcomes even many years after a DNM's closure.

Below is a case study of the successful legal action in respect of AlphaBay DNM.

Case Study: AlphaBay[20, 21]

AlphaBay was set up in 2014 by Alexandre Cazes, a Canadian national. AlphaBay's number two administrator was a person using the alias 'DeSnake', who eventually took over the operations.

It was a Tor-hidden, multi-vendor darknet e-commerce site where customers could buy narcotics, including fentanyl, alongside fraud goods, malware and other contraband from registered vendors. It ran an internal bank of custodial marketplace wallets, initially in Bitcoin and from August 2016 in Monero, and processed transactions inside the site's controlled wallet system. It supported an escrow option that released funds to vendors only after specified actions to protect both parties. Core marketplace services included vendor rankings, based on buyer reviews and sales volume, and an administrator-handled dispute process. It also offered community features, like forums and private messaging.

AlphaBay hosted wallet addresses for buyers and vendors and ran its own mixing to obscure the on-chain trail of funds moving through the market. Beyond drugs and fraud, AlphaBay allowed listings for illegal services, such as money laundering, so launderers could advertise and sell their services directly on the site.

During its time of operation, AlphaBay processed over $1 billion in illicit flows and managed to evade law enforcement even after seizures. This example represents a significant on-ramp for cryptocurrency crime.

AlphaBay serviced 200,000+ users and ~40,000 vendors at its peak. The site posted 250,000+ drug/toxic-chemical goods and 100,000+ listings for fraud, hacking tools, counterfeit IDs, firearms and other illicit services[22, 23] as illustrated in the example overleaf.

US authorities linked multiple overdose deaths to drugs bought on AlphaBay. Despite later 'bans', research shows AlphaBay continued trading in fentanyl and fentanyl-laced drugs, including covert listings.[24]

Operation Bayonet

US authorities identified the founder of AlphaBay and cooperated with investigators in Holland who quietly seized a separate DNM, Hansa, on 20 June 2017, then altered the

19 "United States Files A Civil Action To Forfeit Cryptocurrency Valued At Over One Billion U.S. Dollars", U.S. Attorney's Office, 5 November 2020, https://www.justice.gov/usao-ndca/pr/united-states-files-civil-action-forfeit-cryptocurrency-valued-over-one-billion-us.

20 https://www.justice.gov/archives/opa/press-release/file/982826/dl?inline=.

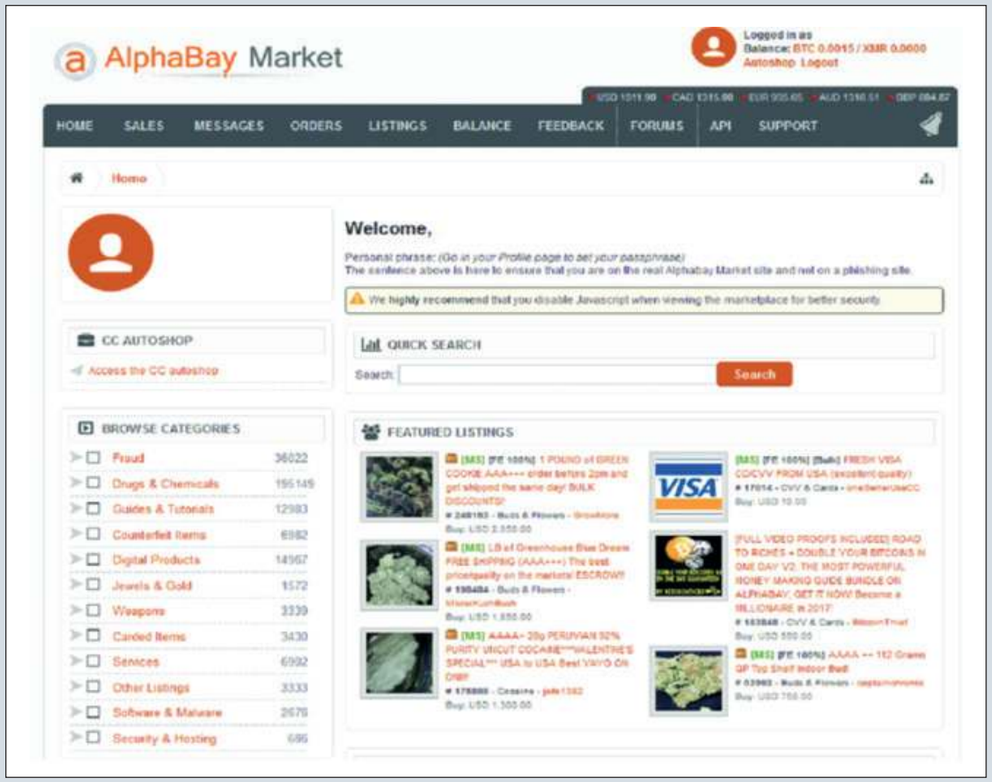
21 Andy Greenberg, "He Escaped the Dark Web's Biggest Bust. Now He's Back", *Wired*, 23 September 2021, https://www.wired.com/story/alphabay-desnake-dark-web-interview/.

22 Leah Koonthamattam, "The Impact of Dark Web Marketplace Takedowns [AlphaBay and Hansa]", *CybelAngel*, 24 September 2024, https://cybelangel.com/blog/alphabay-hansa-two-major-dark-web-marketplaces-shut/.

23 "Darknet Takedown", FBI, 20 July 2017, https://www.fbi.gov/news/stories/alphabay-takedown.

24 Marie-Helen Maras, et al., "Decoding hidden darknet networks: What we learned about the illicit fentanyl trade on AlphaBay", *Journal of Forensic Sciences*, 6 July 2023, https://ccybers.org/wp-content/uploads/2024/07/Journal-of-Forensic-Sciences-Maras-at-al.-2023-Decoding-hidden-darknet-networks-What-we-learned-about-the-illicit-fentanyl__.pdf.

Figure 10: AlphaBay Market listing page



code to log plaintext passwords, capture unencrypted order addresses and preserve photo metadata, building an intelligence trove in real time.

US-led teams then seized AlphaBay's servers worldwide and arrested the founder, Alexandre Cazes, in Thailand on 5 July 2017. He was charged on 16 different counts, including RICO conspiracy and Money Laundering conspiracy.

At the time of Cazes's arrest, his laptop was open, unlocked and actively logged in as 'Admin' to AlphaBay's server and forum, as he had just accessed the data to reboot a server after a law-enforcement-induced outage. This allowed the authorities to bypass encryption and use the live session to search the machine. They found passwords for the AlphaBay website and all AlphaBay servers, enabling them to seize the site's data and cryptocurrency. Agents moved AlphaBay proceeds to government-controlled wallets (about 1,605 BTC, 8,309 ETH, 3,691 ZEC, plus an unknown amount of XMR).

This meant that AlphaBay servers went offline. After it vanished, its users flooded into Hansa, unaware it was under police control, leading to an eight-fold surge in new members. Dutch authorities ran Hansa for 27 days, identifying ~420,000 users and 10,000+ postal addresses, which Europol shared with national law enforcement.

Following the takedown and forfeiture actions, no official AlphaBay services continued to operate. The brand name lingered in copycat claims and forum chatter, but the original site remained offline until 2021.

In August 2021, an entity using the old DeSnake acess key (AlphaBay's former #2) reappeared, proved control of the key to reporters and relaunched AlphaBay. In the first weeks, analysts observed frequent login problems, phishing attempts and slow vendor uptake. Within 10 months, the relaunched platform was reported to have roughly 30,000 listings and approximately 1,300 active vendors, illustrating that these services can persist even in the face of significant enforcement action.

In February 2023, AlphaBay entered a lockdown: users with two-factor authentication (including staff and vendors) couldn't log in. Community explanations pointed to a missed canary update (an operator-signed 'all clear' message) that DeSnake failed to sign on time. He did not reappear to fix it and the site ceased operations.

In conclusion, illicit marketplaces represent a major entry point for funds into the crypto-currency ecosystem, and some platforms further integrate laundering mechanisms as an additional service. The market is continually evolving, and guarantee services are capturing an increasing share of overall volume. With the large scale and sophisticated technology, DNMs act as a key proxy for illicit cryptocurrency to enter the money laundering system.

2) Hacks and Exploits

Hacks and exploits are thefts of digital assets, and include everything from exchange breaches and wallet drains to smart-contract bugs and phishing-led key compromises, where attackers seize funds they do not own. Because the funds arrive on-chain (BTC, ETH, stablecoins, DeFi tokens), they are instantly 'dirty', making these incidents the main on-ramp to money laundering.

Once a hack is completed, the clock starts ticking for the bad actors to move their cryptocurrency across the chain, so that it becomes unseizable by any authority or regulated exchange. Within minutes, most hackers start the obfuscation and layering processes.

There have been thousands of hacks and exploits since the creation of cryptocurrency. These can take the form of hacks of specific exchanges and infrastructure, hacks of private wallets belonging to corporations and individuals, and exit scams. Hacks have a direct impact on retail investors, individuals and companies, robbing them of gains and potentially bankrupting businesses.

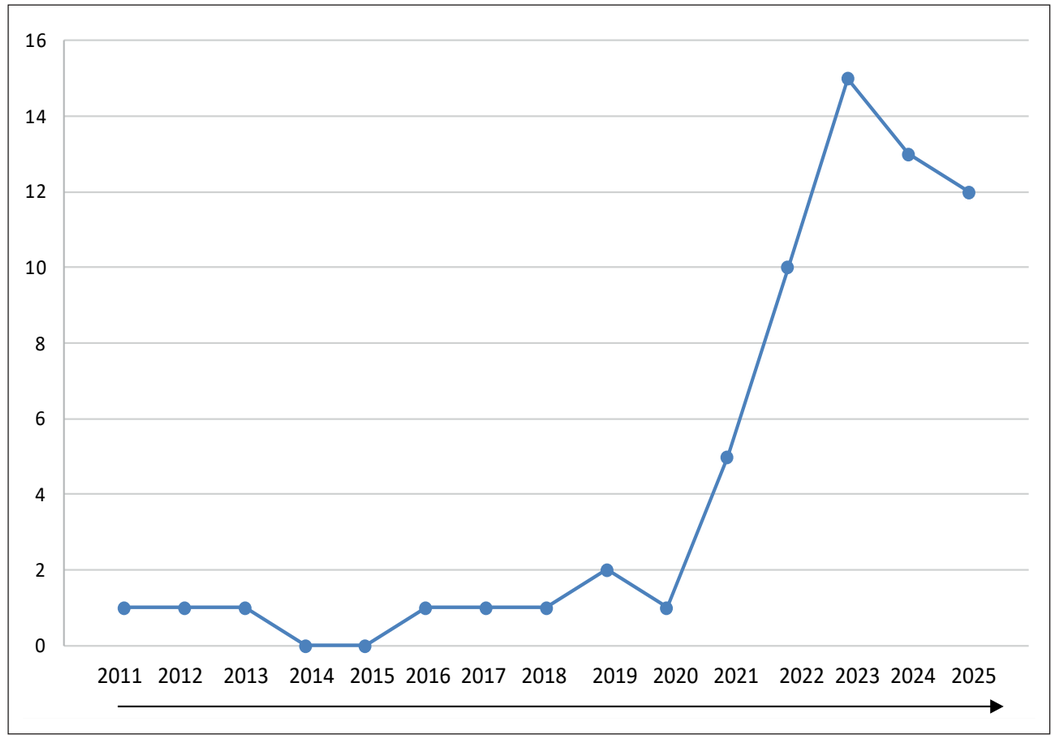
Many hacks are executed by specific bad actors, including hostile governments, such as North Korea, Iran and Russia. In addition to harming individuals and businesses, hostile governments use cyberattacks as a source of funding.

Every day, more hacks occur, and more money is stolen. It is hard to account for every single hack due to the frequency and also the fact that many hacks and exploits are unreported in order to shield exchanges from negative effects on their reputation and to protect institutions from the risk of panic withdrawals.

Hacks are one of the key sources of illicit fund placement into the crypto ecosystem. This report has identified 64 notable hacks and exploits which involved the theft of large volumes of assets or which had considerable victim impact. A total value of $12.8 billion has been stolen. Converted to today's value, the assets amount to $124.9 billion.

Recent years have seen a significant increase in the frequency of hacking incidents. The number of hacks peaked in 2023, with 15 large-scale incidents. In the first nine months of 2025, there were 12 large hacks.

Figure 11: Timeline of hacks per year



The first hack identified in this report, the Mt. Gox Hack, occurred in 2014. Mt. Gox was a large cryptocurrency exchange based in Japan. The hack was allegedly perpetrated by Alexey Bilyuchenko and Aleksandr Verner (both Russian nationals) [25] and involved them siphoning off funds for many years before they were stopped. Initially, the hackers stole cryptocurrency worth $83 million, which would have a present value of $73.3 billion due to cryptocurrency appreciation. According to the US Department of Justice, the hackers laundered the funds through different exchanges and even used advertising contracts with a New York Bitcoin broker to clean the cryptocurrency. In 2017, the two Russian nationals were charged with perpetrating the hack and accused of using the funds to set up an illicit currency exchange, BTC-e. [26]

Since then, hacks have become even more complex. For example, in the 2025 Cetus Protocol hack, more than $223 million was reportedly stolen within 15 minutes after attackers exploited a rounding bug in a third-party mathematics library used for liquidity and pricing calculations. [27]

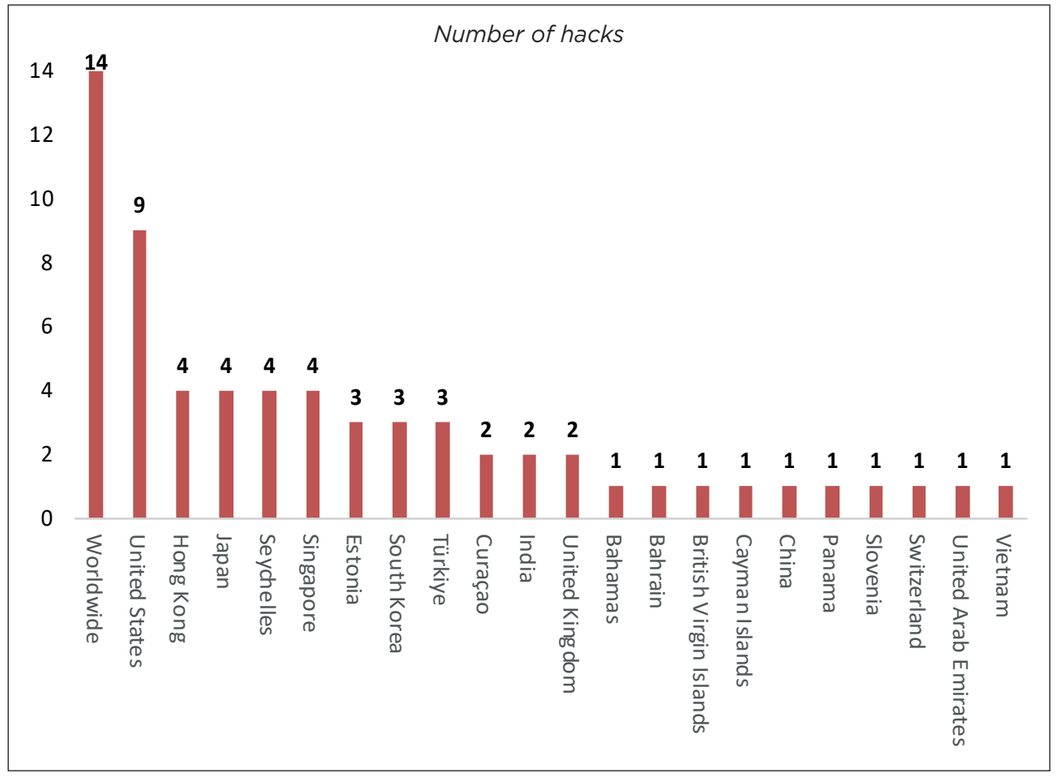
Due to the interconnected nature of the cryptocurrency system, hackers are able to target different locations with ease. The bar chart below presents the number of hacks by country; incidents that cannot be clearly attributed to a specific country are grouped under 'Worldwide'. For each case, geography is coded according to the country of the target, rather than the attacker's location.

[25] "Russian Nationals Charged With Hacking One Cryptocurrency Exchange and Illicitly Operating Another", U.S. Department of Justice, 9 June 2023, https://www.justice.gov/archives/opa/pr/russian-nationals-charged-hacking-one-cryptocurrency-exchange-and-illicitly-operating-another.

[26] Ibid.

[27] "Hack Track: How a Shared Library Bug Triggered the $223M Cetus Hack", *Merkle Science*, 26 May 2025, https://www.merklescience.com/blog/hack-track-how-a-shared-library-bug-triggered-the-223m-cetus-hack.

Figure 12: Geography of hacks



The United States has encountered the highest frequency of hacks and exploits. This is partly because it is a financial powerhouse and because bad actors specifically try to disrupt operations in the US. There are 20+ countries which have been affected by the hacks, which demonstrates the need for collective action by different national regulatory bodies and international partnerships.

Of the 64 cases identified, 19 were either directly perpetrated by North Korea or had direct ties to North Korean hacking groups. A total of $4.1 billion has been stolen by North Korea from these 19 hacks. At the beginning of 2017, North Korea faced a drastically dwindling economy and harsh economic sanctions. This caused North Korea to focus on cryptocurrency theft as a key source of revenue generation. By 2024, over one-third of foreign currency revenues generated by North Korea stemmed from cryptocurrency thefts and the rest came from the sale of military equipment and others economic activity with Russia. [28]

North Korea conducts hacks through specific groups organised under the Reconnaissance General Bureau. The main group within this system is known as Lazarus Group, with a specific subsection, TradeTraitor, focusing exclusively on cryptocurrency thefts. It has been linked to extremely large hacks, including the $1.5 billion Bybit hack in 2025. [29] After Lazarus Group brings illicit funds on-chain, it employs elaborate money laundering techniques and hires sophisticated groups to move its cash.

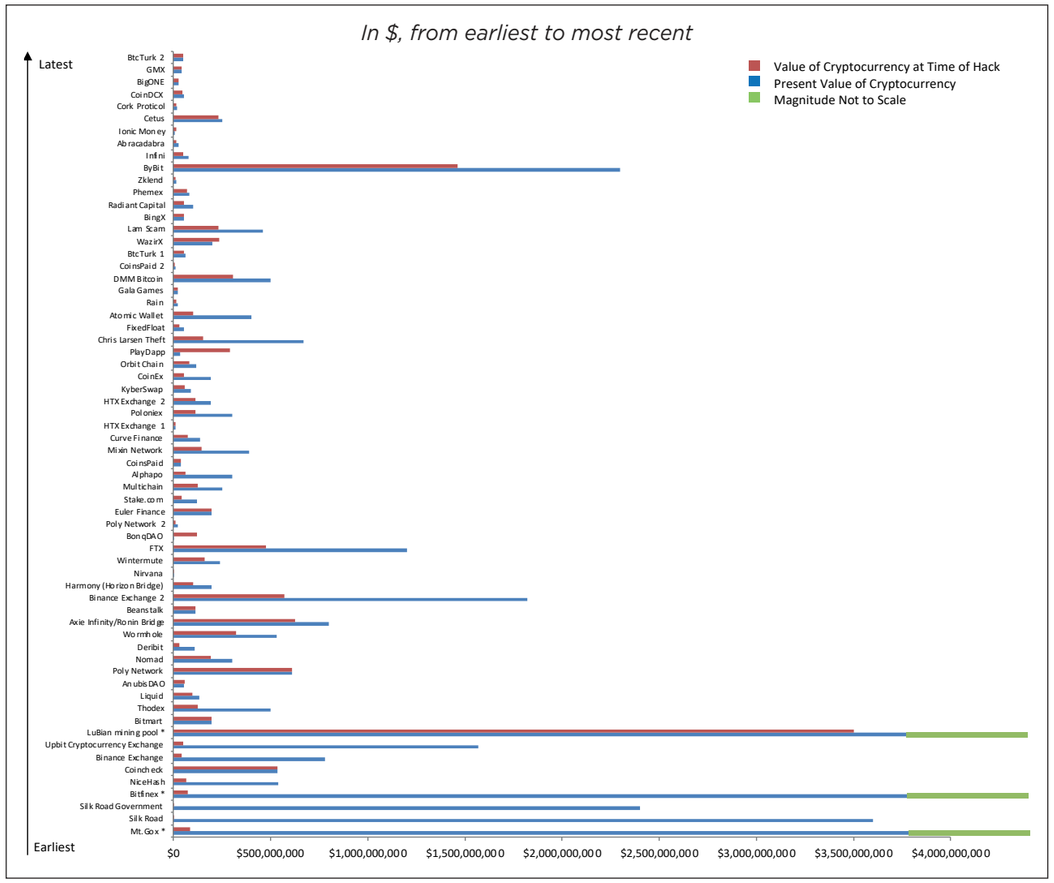
[28] "The DPRK's Violation and Evasion of UN Sanctions through Cyber and Information Technology Worker Activities", Multilateral Sanctions Monitoring Team, 22 October 2025, https://www.mofa.go.jp/files/100922718.pdf.

[29] "North Korea Responsible for $1.5 Billion Bybit Hack", FBI, 26 February 2025, https://www.ic3.gov/PSA/2025/PSA250226.

The chart below illustrates the magnitude of hacks over the past 14 years and compares the value of the stolen cryptocurrency at the time of each incident with its value at present.

The hacks have ranged in size from a $625,000 hack of Silk Road to a $3.5 billion hack of a Chinese mining pool, where an attacker purportedly stole 127,000 BTC in December 2020. [30] Across 64 cases, an average of $200 million has been stolen per incident, underscoring the substantial scale of these attacks.

Figure 13: Proceeds of top 64 cryptocurrency hacks



The graph clearly demonstrates that the value of funds stolen through hacks has significantly increased over time which has been the result of the increase in cryptocurrency value.

For example, the top five hacks amounted to $6.78 billion and accounted for 53% of the value of all hacks at the time of hack ($12.8 billion). Having risen in present value to $20 billion, these five hacks today constitute only 16% of the total present value of all hacks (at $124.9 billion), demonstrating how hackers are able to obtain long-term 'premium'.

Unusually, compared to other methods of revenue generation by criminal enterprises, this makes hacks and exploits a source of long-term investment. Due to the support around

[30] "Arkham uncovers $3.5b heist – the largest ever", *Arkham*, 2 August 2025, https://info.arkm.com/announcements/arkham-uncovers.

cryptocurrency by regular investors, the price of Bitcoin has risen by nearly 24,000 times since the first hack in 2011 and the price of Ethereum has risen by 5,576 times since its creation in 2015, indicating that any funds held in cryptocurrency may appreciate markedly over time. As a result, an estimated $112 billion in additional value was added to the hackers' proceeds due to 'post-hack appreciation'.

A striking example of this increased valuation of assets stolen through hacks was the 2019 Upbit hack, where hackers managed to steal 342,000 Ethereum, equivalent to $49 million. At present, the total value of this hack would be close to $1.58 billion. With less than 0.01% being recovered, this represents a substantial profit for the hackers. South Korean authorities identified the actors behind the hack as the Lazarus Group. [31] If these funds were not immediately sold, this would have given the North Korean government a tremendous boost in funding, including its war programs.

One of the largest hacks occurred in February 2025 when ByBit, a cryptocurrency exchange, was hacked for a total value of $1.5 billion by Lazarus Group. This hack affected hundreds of thousands of people, with many losing their life savings. Within hours, the hackers began laundering the cryptocurrency and after less than one month, 20% of the funds had gone dark, meaning they are unlikely to ever be recovered. [32]

Each hack has immense impact on both the company and the individuals who have their personal money invested. Often, even if the hack hasn't affected a victim who is on the platform, they will feel secondary consequences. Some services declare bankruptcy or close operations after a hack, leaving many struggling to recover their losses. For example, in the 2023 hack of the crypto company Multichain, $125 million was stolen and the company had to shut down, leaving many retail investors without compensation. [33]

This report has broken down the hacks and exploits into three categories: Hacks of Corporations and Individuals, Exit Scams and Hacks of Exchanges. Each of the three categories has a different mechanism for obtaining illicit funds:

Table 3: Different categories of hacks

Category	Corporations and Individuals	Exit Scams	Exchange Hacks	Total
Number	**4**	**2**	**58**	**64**

a) Hacks of Corporation and Individuals

Individuals and corporations are usually hit by hackers through social engineering and wallet-level tricks. Phishing pages or fake support reps talk people into revealing their seed phrase or private key or typing it into a 'verification' form. Once a seed phrase or private key is exposed, funds are swept instantly.

The private key is the only way for individuals to access their cryptocurrency. It is a specific 64-character-long string. If this key gets into the wrong hands, a hacker can drain the account within seconds into other cryptocurrency addresses.

[31] Lee Dong-hwan, "North Korea robbed 58 billion Ethereum from Upbit… Police 'First confirmation of North Korea's actions'", *Yonhap News*, 21 November 2024, https://www.yna.co.kr/view/AKR20241121075800004?input=1195m.

[32] "North Korean hackers cash out hundreds of millions from $1.5bn ByBit hack", *BBC News*, 10 March 2025, https://www.bbc.co.uk/news/articles/c2kgndwwd7lo.

[33] "Originating Claim No 621 of 2023 (Assessment of Damages No 2 of 2024) Between Fantom Foundation Ltd … Claimant And (1) Multichain Foundation Ltd (2) Multichain Pte Ltd", The High Court of the Republic of Singapore, 8 July 2024, https://www.elitigation.sg/gd/s/2024_SGHC_173.

Case Study: Chris Larsen's Private Wallet Hack [34, 35]

In January 2024, roughly 213 million XRP were drained from the personal wallets of Chris Larsen, founder of cryptocurrency company Ripple. At spot prices at the time, the value was ~ $112.5 million. On-chain analyst ZachXBT flagged the movements. Larsen posted that there was "unauthorized access to a few of my personal XRP accounts" and that law enforcement and exchanges had been alerted.

Investigators say the thieves accessed private keys that had been stored in a LastPass vault which was among the encrypted customer vaults stolen in the 2022 LastPass hack.

The XRP were rapidly split and sent to multiple exchanges (including Binance, Kraken, OKX, Gate, MEXC, HTX, HitBTC) to cash out or swap. Larsen also noted that nearly all the affected funds were converted out of XRP.

Binance froze about $4.2 million of XRP within days. Authorities sought and obtained seizure authority for ~$23–24 million linked to the theft. The hackers are still at large with the stolen cryptocurrency.

In recent years, due to improvements in cybersecurity, criminals have moved to staging kidnappings and assaults. They will hold victims until they reveal their private key and the criminals are then able to drain their account. This blurs the shielding between the online ecosystem and in-person safety.

For example, in January 2025, the co-founder of crypto hardware wallet company Ledger, David Balland, was kidnapped with his wife at his home in France by criminals trying to gain access to his cryptocurrency. While he was tortured, they demanded access to his private wallets and a ransom to be paid. *Le Monde* reported that the kidnappers used operational security measures (e.g., WhatsApp tied to a Southeast Asia number and a VPN) to make attribution harder. Balland was rescued in a police operation, involving the GIGN (elite tactical unit). The police discovered that his hand was mutilated. His wife was also rescued a day later. [36, 37]

b) Exit Scams and Rug Pulls

In an exit scam, also known as a rug pull, operators can create a token/DeFi/non-fungible token venue. They then drum up attention through advertisements and social media posts. This attracts deposits into the scheme and causes a large amount of liquidity to flow through the project. The operators then dump the assets in exchange for other cryptocurrencies, instantly devaluing the assets they set up, 'pulling the rug' underneath the retail investors and individuals who had their money exploited.

This exploit is very prevalent due to the fact that it is cheap and easy to launch, thus multiple operations can be going on at the same time. The operators act under pseudonymity, therefore making it hard to track the owners of the project. Finally, it is extremely quick and easy to gain liquidity.

[34] Brian Krebs, "Feds Link $150M Cyberheist to 2022 LastPass Hacks", *Krebs on Security*, 7 March 2025, https://krebsonsecurity.com/2025/03/feds-link-150m-cyberheist-to-2022-lastpass-hacks/.

[35] "Ripple's XRP falls amid reports it was likely hacked – CoinDesk", *Reuters*, 31 January 2024, https://www.reuters.com/technology/ripples-xrp-falls-amid-reports-it-was-likely-hacked-coindesk-2024-01-31/.

[36] Marine Strauss, "Kidnapped co-founder of French crypto firm Ledger had his hand mutilated", *Reuters*, 24 January 2025, https://www.reuters.com/world/europe/kidnapped-co-founder-french-crypto-firm-ledger-had-his-hand-mutilated-2025-01-24/.

[37] Aurélien Defer, Damien Leloup and Florian Reynaud, "Kidnappers of French crypto figure and his wife arrested after massive manhunt", *Le Monde*, 24 January 2025, https://www.lemonde.fr/en/pixels/article/2025/01/24/kidnappers-of-french-crypto-figure-and-his-wife-arrested-after-massive-manhunt_6737379_13.html.

Case Study: Thodex [38, 39]

Thodex was a Türkiye-based cryptocurrency exchange founded in 2017 by Faruk Fatih Özer. At its peak, it was among Türkiye's largest exchanges, with hundreds of thousands of users. In April 2021, Thodex ran an aggressive Dogecoin promotional campaign that drew a surge of new accounts and deposits.

In April 2021, the exchange halted trading and withdrawals, telling customers there was a "cyberattack/maintenance" issue. Users were soon locked out of their accounts and the site said that it was "temporarily closed". An estimated $43 million was stolen from users' accounts.

Large amounts of customer crypto were moved from three accounts under Özer's control to wallets at an offshore cryptocurrency platform. Using the customer funds, Özer bought physical gold bricks and converted some of the cryptocurrency into Turkish lira. Özer allegedly had access to "scores" of other people's accounts (relatives, employees, associates) to place trades and route funds, as a layering technique.

Ultimately, as Özer was being investigated, he fled Türkiye for Albania. Türkiye issued an Interpol Red Notice for his arrest. In 2022, he was arrested in Albania and returned to Türkiye to face trial.

An Istanbul court sentenced Özer to 11,196 years on fraud, money-laundering and criminal-organisation charges and imposed heavy fines. His siblings, who aided him, received the same term. This publicised trial led to strict regulations being implemented in Türkiye.

Immediately after the scam, the Central Bank of Türkiye barred the use of crypto assets in payments and prohibited e-money institutions from intermediating any transactions involving crypto assets. A Presidential Decision amended Türkiye's anti-money-laundering (AML) "Measures Regulation" to classify crypto-asset service providers as obliged entities. This classification triggers full KYC/identity checks, suspicious-transaction reporting, record-keeping and information-sharing duties to MASAK (the Financial Crimes Investigation Board).

c) Exchange Hacks

Exchange hacks are the type of hacks where attackers gain the ability to approve withdrawals. On centralised exchanges, hackers phish members of staff operating the exchange or breach servers, seeking to reach hot-wallet keys or admin panels, then drain funds with normal-looking withdrawals. In Decentralised Finance, they exploit smart-contract bugs or game price feeds, and sometimes compromise cross-chain bridges. It works because these systems are online and complex.

Retail investors, who have little control over how safe their cryptocurrency investments are, have to face the risk of their funds being stolen or exploited constantly. Most individuals are unable to obtain refunds or receive little compensation. In addition, many exchanges shut down or go bankrupt, leaving retail investors and individuals significantly harmed.

Since the funds are already on an exchange platform or service, hackers are often able to utilise exchanging, bridging and other capabilities.

[38] "Thodex cryptocurrency boss jailed for 11,196 years in Turkey for fraud", *BBC News*, 8 September 2023, https://www.bbc.com/news/world-europe-66752785.

[39] Taylan Bilgic and Firat Kozok, "Turkish Crypto Exchange Goes Bust as Founder Flees Country", *Bloomberg UK*, 22 April 2021, https://www.bloomberg.com/news/articles/2021-04-22/turks-suspect-massive-crypto-losses-as-exchange-ceo-goes-missing.

Case Study: Bitfinex Hack [40]

Bitfinex is a major cryptocurrency exchange launched in 2012 in Hong Kong. By 2016, it used BitGo-powered multi-signature wallets with segregated customer addresses. It attracted hundreds of thousands of clients.

On 2 August 2016, an attacker siphoned roughly 120,000 BTC, approximately $72 million at the time, by triggering ~2,000 approved withdrawals from users' segregated wallets into a single destination.

Bitfinex customers, many of whom had invested their life savings into it, had their accounts drained overnight. As a secondary effect, the price of Bitcoin dropped 20% within hours of the hack.

Bitfinex halted trades and withdrawals. The company 'socialised' the losses for all users: this meant every single user on the platform had a 36% reduction in their account balance.

The hacker was believed to be a US national called Ilya Lichtenstein. Agents followed the stolen BTC through peel-chains, accounts at multiple exchanges and even AlphaBay. Overlaps in IPs, reused email patterns and exchange records (including prepaid gift card buys from an IP tied to him) linked the laundering to Lichtenstein and his wife, Heather Morgan.

In 2021, agents obtained his US email/cloud account using a warrant. In 2022, they decrypted an encrypted file that listed 2,000 wallet addresses and their private keys – almost all tied to the hack. Using those keys, they seized ~94,636 BTC.

The pair was arrested in New York and they were both charged with conspiracy to commit money laundering. Morgan was also charged with conspiracy to defraud the United States. Lichtenstein pleaded guilty and was sentenced to five years imprisonment in a federal prison and three years' supervised release. Morgan pleaded guilty and was sentenced to 18 months in a federal prison.

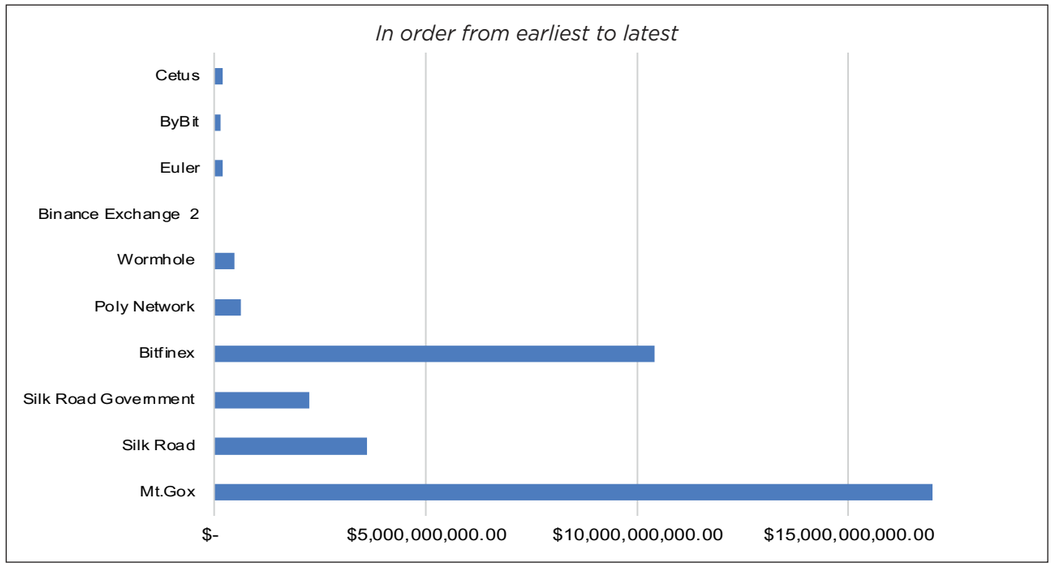
Legal Action

Of the 64 cases examined, only 21 hacking incidents resulted in formal legal action. Within this subset, criminal charges were brought in 15 cases, and six cases ultimately resulted in convictions. The gap between the number of reported hacks and the limited number of subsequent legal actions underscores the ease with which hackers remain anonymous and launder illicit proceeds. In addition, those who are charged with hacking and money laundering are often based in jurisdictions which don't extradite to prosecuting countries, making it much harder for justice to be served.

Although prosecutions are more difficult to pursue, some assets can still be recovered or seized to provide restitution to victims. The graph below shows the total amount of assets from the hacks that have been subsequently seized.

[40] Rachel Brodsky, "The Bizarre True Story Of "Bitcoin's Bonnie & Clyde" in Netflix's *Biggest Heist Ever*", *Time*, 28 January 2025, https://time.com/7200219/bitcoin-netflix-biggest-heist-ever/.

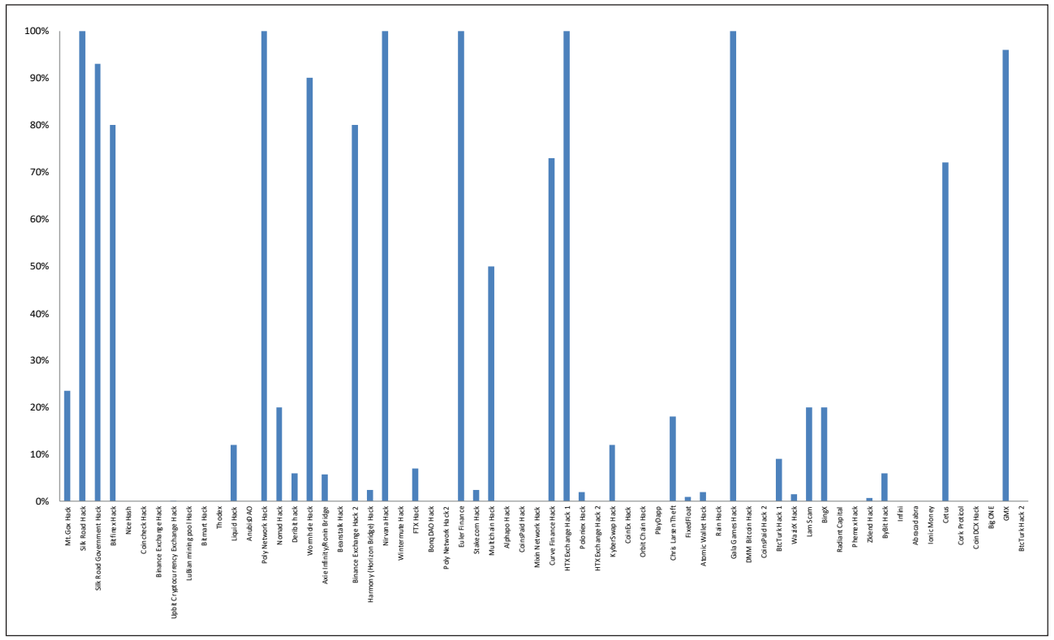
Figure 14: Value of top 10 seizures



A total of $37.3 billion has been seized through successful law enforcement action. The largest recovery was in the Mt. Gox case in 2014, where a court bankruptcy proceeding recovered over 200,000 BTC in an old wallet connected to Mt. Gox. In addition, further court-ordered forfeiture actions have been initiated to recover assets linked to BTC-e wallets.

The graph below shows the percentage of seized assets relative to the total value of assets stolen through hacks and exploits.

Figure 15: Value of seizures from hacks as a percentage of total



Across the 64 cases examined, authorities recovered an average of 21.6% of the stolen proceeds. In six cases, all stolen funds were fully recovered, achieving 100% recovery. These were the Silk Road Hack, Poly Network Hack, Nirvana Hack, Euler Finance Hack, the first HTX hack and the Gala Games Hack. Many were 'white-hat' actors who returned funds either for ethical reasons or in exchange for bug-bounty rewards. However, in 31 cases, none of the stolen funds has been recovered (0% recovery).

Each of the three categories discussed in the report has caused significant harm to retail investors and regular individuals. Most exchanges when they are hacked also lose victims' savings, exit scams lose retail investors' money and hacks of individuals directly affect users' funds. For example, in the 2022 FTX hack, millions of dollars were stolen and thousands of victims faced significant challenges in recovering their funds. [41]

In summary, hacks and exploits put dirty money on-chain by creating or seizing crypto assets right at the moment of the attack. When a service or account is compromised, funds are pushed straight into an attacker's fresh address. The theft itself is the on-ramp: the instant the bug or private key theft occurs, illicit balances appear on the blockchain.

3) Ransomware

Ransomware is malware that encrypts a victim's files or systems and requires payment in exchange for a decryption key. Attackers often also steal data and threaten to leak it (known as 'double extortion').

The victims – who include governments, corporations and individuals – have a choice: either pay the ransom exclusively through cryptocurrency and hope the ransomware operators stay true to their word or accept the loss and risk having sensitive data leaked.

If the operators are paid, then the cryptocurrency is often moved quickly and through intricate money laundering schemes. Many companies often pay ransoms and don't disclose it so it doesn't encourage more rampant blackmailing. This means that many fly under the radar without picking up media attention. According to estimates by Coveware, most ransomware payments average $377,000 per incident. [42]

Industry analytics firm Chainalysis concludes that the total revenue generated from all ransom operations since 2020 reached over $5 billion. [43] The firm also notes that there have been many more prolific attempts to obtain ransoms in each consecutive year. Although there have been more of these attempts, less have been successful and less have been paid out. In 2024, there was an estimated 35% decrease in the value of payments compared to 2023. [44]

Even if a company or government doesn't pay, the damage is already done. Social security numbers, addresses and payment information are often leaked and sold on darknet markets.

This report has identified 25 of the most notable ransomware operations and events which have resulted in payments. A total of $1.53 billion has been paid to operators in these cases.

41 "The $477 million FTX hack: a new blockchain trail", *Elliptic*, 12 October 2023 https://www.elliptic.co/blog/the-477-million-ftx-hack-following-the-blockchain-trail.

42 "Insider Threats Loom while Ransom Payment Rates Plummet", *Coveware*, 24 October 2025, https://www.coveware.com/blog/2025/10/24/insider-threats-loom-while-ransom-payment-rates-plummet.

43 "35% Year-over-Year Decrease in Ransomware Payments, Less than Half of Recorded Incidents Resulted in Victim Payments", *Chainalysis*, 5 February 2025, https://www.chainalysis.com/blog/crypto-crime-ransomware-victim-extortion-2025/.

44 Ibid.

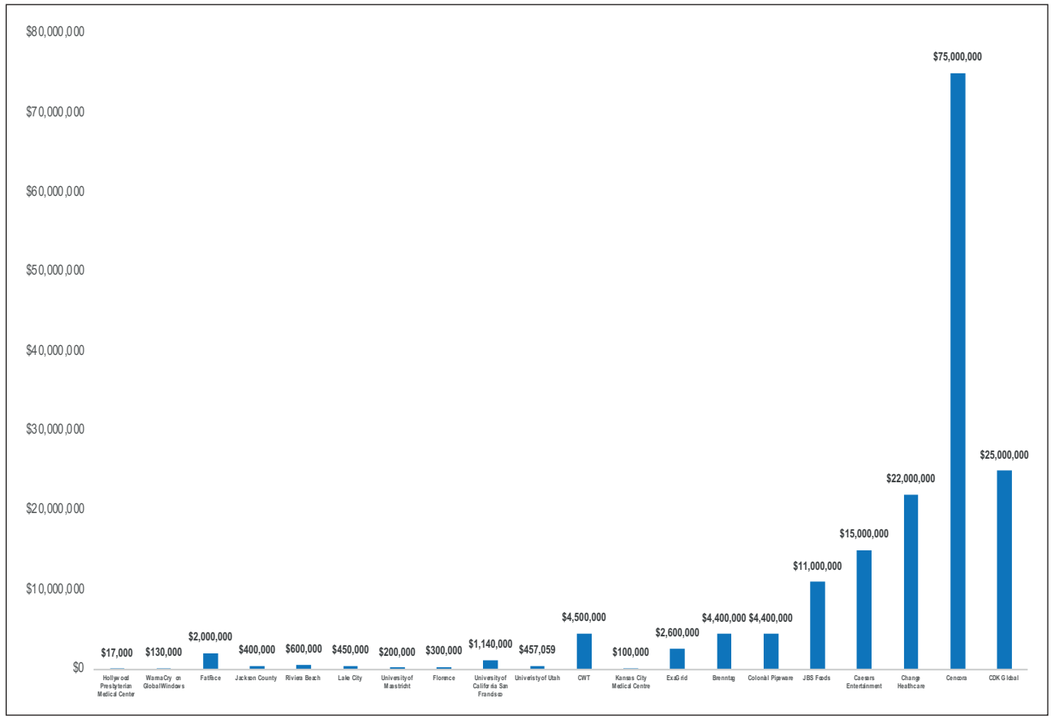
Table 4: Ransomware operations in the Global Cryptocurrency Laundering Database

Category	Ransomware Incident	Ransomware Group	Total
Number	20	5	25
Value (Millions $)	170	1,366	1,536
Legal Action	11	5	16
Convictions	4	1	5

a) Ransomware Incidents

The scale of 20 notable specific ransomware events is demonstrated in the graph below.

Figure 16: 20 Ransomware incidents by size – in chronological order from 2016



The graph clearly shows that ransom payments are getting larger as ransom operators develop more sophisticated strategies and target larger companies.

The largest ransomware event targeted the tenth biggest Fortune 500 company, Cencora, in 2024, in the United States. The data breach affected over 1.43 million people who had all their personal information stolen. The operators initially demanded $150 million from the company; after negotiations, the company paid $75 million in three instalments of Bitcoin. This is the largest ransomware paid in history. [45, 46]

45 Katrina Manson, "Hackers Got Record Ransom of $75 Million for Cencora Breach", *Bloomberg Law*, 18 September 2024, https://www.constangy.com/assets/htmldocuments/Hackers%20Got%20Record%20Ransom%20of%20%2475%20Million%20for%20Cencora%20Breach%202.pdf.

46 "Notice of Data Security Incident", *Cencora*, https://www.cencora.com/caredx-notice.

Each ransomware incident affects hundreds of thousands to millions of victims and causes millions of dollars in damages. Across the 20 incidents, the average direct payment by each affected company or government entity was $8.48 million. Not only does it cost the organisations millions in paying the ransom, but they also have to deal with repairing infrastructure, repaying users and dealing with lawsuits.

If the organisation doesn't pay the ransom, the information about customers and victims is often leaked and the organisation can't recover and protect the data. An example of a prominent case is the attack on Medibank in Australia in 2022. The health insurer stated that it would refuse to pay the ransom and the criminals dumped the healthcare data of 9.7 million people on the dark web. [47] According to CoveWare, in the third quarter of 2025, the rate of payments fell to a historical low of 23%. [48] This means that consumers and companies may be facing larger data leaks in the future.

For those who intend to pay, the situation is similar to a hospital billing negotiation. It starts off with the ransomware operators sending a message to the company or organisation stating how much they want to be paid. The company then tries to negotiate down as much as possible until they are forced to pay. Once the payment is received, the ransomware operators send a decryption key to the company so they can recover the data. However, sometimes the operators decide to take the money and run without sending the key. This doesn't happen often as it ruins their 'reputation' for future operations. There is also a chance that operators keep copies of stolen data and then leak it later.

As well as targeting corporations, ransomware operators tend to also attack medical institutions and government bodies. For example, a 2019 ransomware attack on Jackson County in Georgia took all county-wide system operations offline for two weeks, until they paid $400,000 for them to be restored. [49]

North Korean hackers tend to carry out ransomware attacks, specifically through the Andariel unit. They prioritise targeting US healthcare institutions to try and force them to pay and then they launder their proceeds through China-based services and ATMs. They would use this money to purchase internet infrastructure which is then used to launch attacks against the defence infrastructure of the country's enemies, such as targeting two US Air Force bases and NASA's Office of the Inspector General. [50]

[47] Josh Taylor, "Ransomware group starts publishing Medibank data as company warns customers to be vigilant for scammers", *The Guardian*, 8 November 2022, https://www.theguardian.com/australia-news/2022/nov/09/group-claiming-to-be-medibank-hackers-start-posting-client-data-on-dark-web.

[48] "Insider Threats Loom while Ransom Payment Rates Plummet".

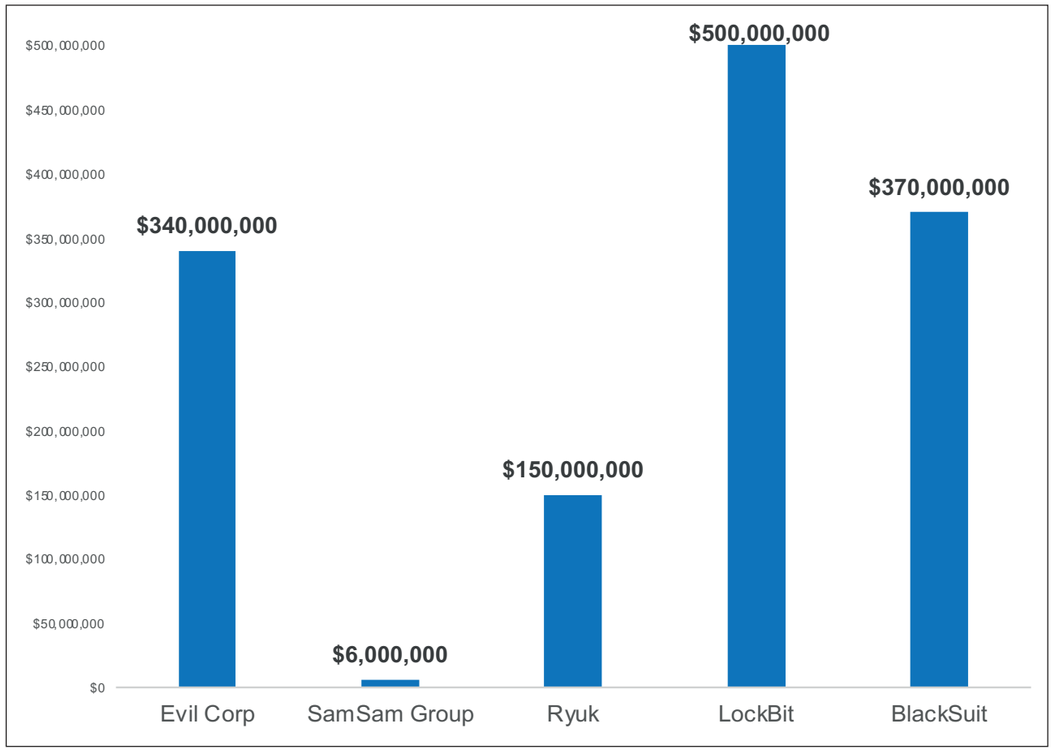
[49] Scott Ferguson, "Georgia County Pays $400,000 to Ransomware Attackers", *Bank Info Security*, 12 March 2019, https://www.bankinfosecurity.com/georgia-county-pays-400000-to-ransomware-attackers-a-12159.

[50] Doreen Horschig, "How Are Cyberattacks Fueling North Korea's Nuclear Ambitions?", *CSIS*, 31 July 2024, https://www.csis.org/analysis/how-are-cyberattacks-fueling-north-koreas-nuclear-ambitions.

b) Ransomware Groups

The graph below features five prominent ransomware groups.

Figure 17: Ransomware groups by size – in chronological order from 2009 onwards



Four out of the five ransomware groups were based in Russia and one was based in Iran. Their approaches differed, with distinct techniques being employed.

1) The largest featured ransomware group is LockBit, which was set up around 2020. It is estimated that around 2,500 organizations fell victim to its operations. It operated a 'ransomware-as-a-service' (RaaS) model, with many affiliates producing high volumes of ransoms, with different styles of intrusions. In 2022, it became the most deployed ransomware variant across the world. [51]

2) Evil Corp was the earliest group to enter the space in 2009. It had multiple different strains of ransomware and would constantly change tactics depending on law enforcement action. UK reporting has described Evil Corp as unusually close to Russian state structures, including allegations that it was "tasked" to conduct activity against NATO allies prior to 2019. [52]

Ryuk, SamSam and BlackSuit organised operator-led intrusions and deployed more consistent tradecraft during each campaign. They all targeted corporations, hospitals and governments.

[51] "Law enforcement disrupt world's biggest ransomware operation", Europol, 20 February 2024, https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation.

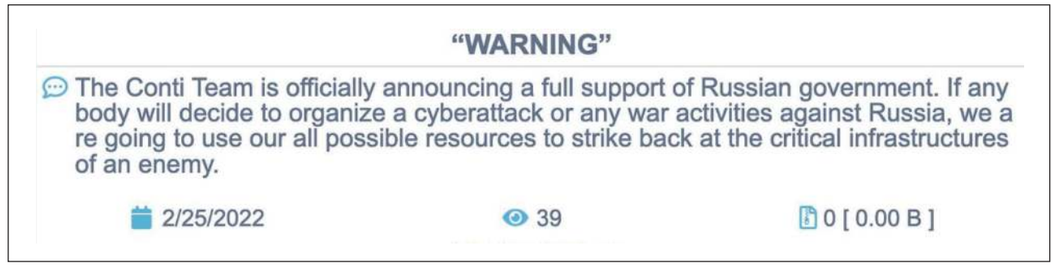
[52] Lily Hay Newman, "Notorious Evil Corp Hackers Targeted NATO Allies for Russian Intelligence", *Wired*, 1 October 2024, https://www.wired.com/story/evil-corp-lockbit-russian-intelligence/.

3) Ryuk is a targeted ransomware group, first seen in 2018, that attacks Windows environments, encrypts files across networks and demands payment, usually in Bitcoin. Ryuk targets large organisations with the ability to pay significant sums of money to regain access to their valuable data. It had committed over 2,400 cyberattacks worldwide. [53]

4) SamSam was set up in 2015 and operated until 2018. The operators were based in Iran and focused their attacks on US organisations. The campaign involved more than 200 victims, including the City of Atlanta, Port of San Diego and Colorado Department of Transportation. The activity collected over $6 million in ransom payments while also causing over $30 million in losses. [54]

5) The RaaS group Blacksuit, previously known as Conti, was first set up in 2019 and paid operators in wages rather than profits from ransomware operations. It declared its full support for Russia after Russia attacked Ukraine in 2022. It posted the following announcement on its forum:

Figure 18: Image showing Blacksuit announcement



This declaration caused infighting within the group and caused it to be hacked and have all its information released, including the primary Bitcoin addresses which allegedly held $2 billion in Bitcoin and had Russian FSB involvement. [55]

A decade ago, ransomware was a low-overhead industry. Access was cheap and abundant, and the same actors wrote the malware, broke in, encrypted data and negotiated payment. Profits were steady and reinvestment needs were minimal.

As organisations hardened their defences with backups and better cybersecurity, payment rates fell; bad actors added data theft to pressure victims, and the RaaS model scaled operations through affiliates. But growth brought costs plus infighting over revenue shares. By 2024, major RaaS brands had collapsed and the ecosystem frayed under thin margins and growing mistrust.

Today, the old, largely opportunistic playbook is giving way to targeted extortion economics. Rather than relying mostly on commodity access, actors increasingly use social-engineering helpdesks, and even insider bribes to penetrate better-defended enterprises. With profits

[53] "Ukraine extradites to U.S. hacker involved in over 2,400 cyberattacks worldwide", *Ukrinform*, 18 June 2025, https://www.ukrinform.net/rubric-crime/4005793-ukraine-extradites-to-us-hacker-involved-in-over-2400-cyberattacks-worldwide.html.

[54] "Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over $30 Million in Losses", U.S. Department of Justice, 28 November 2018, https://www.justice.gov/archives/opa/pr/two-iranian-men-indicted-deploying-ransomware-extort-hospitals-municipalities-and-public.

[55] "The Top 5 Russian Cyber Threat Actors to Watch", *Rapid7*, 3 March 2022, https://www.rapid7.com/blog/post/2022/03/03/the-top-5-russian-cyber-threat-actors-to-watch/.

shrinking and initial access costs rising, attackers are prioritising 'white-whale' organisations that can pay large sums.

As well as targeting corporations, ransomware operators tend to also attack medical institutions and government bodies. For example, a 2019 ransomware attack on Jackson County in Georgia took all county-wide system operations offline for two weeks, until they paid $400,000 for them to be restored. [56]

Legal Action

Of the 25 cases, 16 have been subject to legal action, and criminal charges have been brought in 10 cases. Five cases resulted in convictions. This low number of convictions is largely due to the fact that individuals charged in these ransomware incidents reside in countries that do not extradite their citizens, such as Russia and North Korea.

Many enforcement actions have cross-case relevance because ransomware incidents are often connected through shared jurisdictions, victim industries or perpetrator networks. This makes international cooperation and investigative analysis vital for obtaining convictions.

Over the last decade, ransoms have become an ever-growing and abundant phenomenon. By paying ransoms, governments, individual victims and corporations in effect contribute to the growth in illicit cryptocurrency laundering.

4) Ponzi Schemes

A traditional Ponzi scheme pays old investors with money from new investors instead of from real profit. In the crypto space, the scam involves digital tokens, 'staking', bots and mining contracts. The technique is the same. When inflows slow down (or withdrawals spike), the structure collapses and operators run with their proceeds.

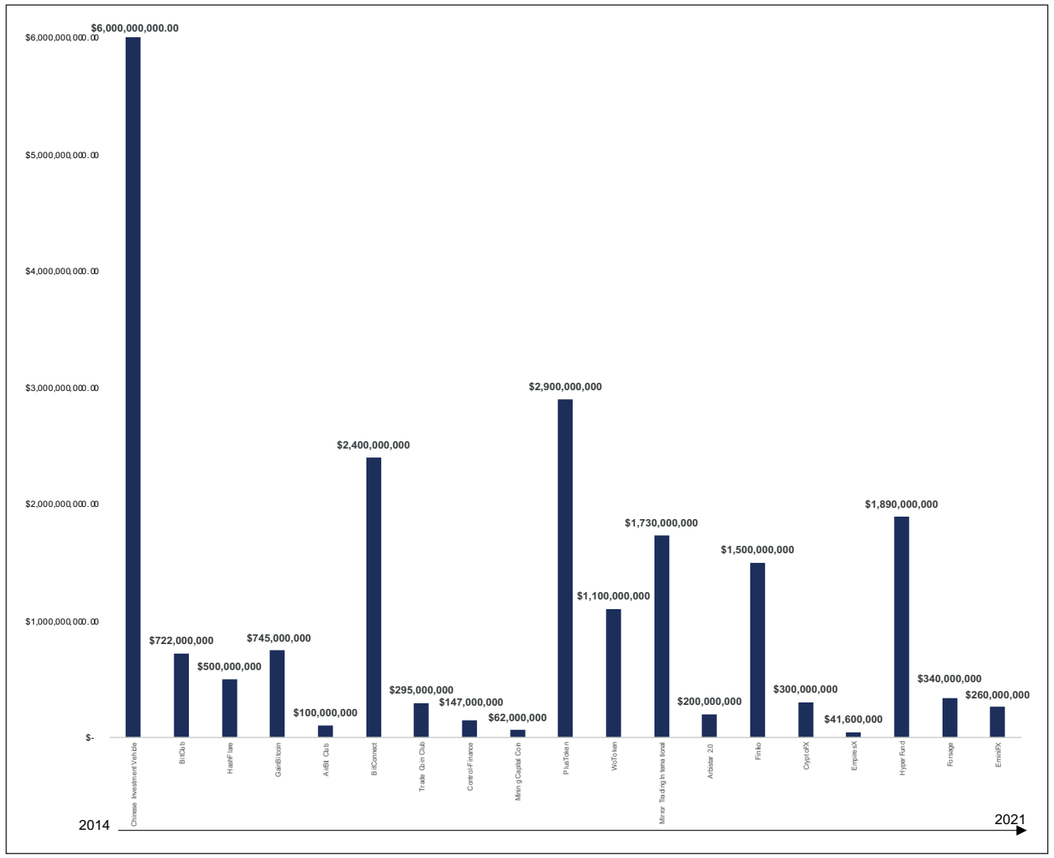
A pyramid scheme pays participants mainly for recruiting new participants, not for selling a real product or generating real revenue. New joiners buy a 'package' and their money flows up the pyramid as commissions to earlier members. When recruiting slows, payouts dry up and the scheme unravels. Many victims have their assets pooled into several wallet and exchange accounts, meaning when the scheme does collapse, it can instantly get laundered away.

This report has identified 19 different notable cases of large Ponzi/pyramid schemes that directly involve cryptocurrency. By the time of collapse, a total of $21.3 billion, equivalent to $88.5 billion in today's dollars, had moved through all the Ponzi schemes.

The graph below shows the scale of the Ponzi schemes included in the Global Crypto Laundering Database, in chronological order.

[56] Ferguson, "Georgia County Pays $400,000 to Ransomware Attackers".

Figure 19: Magnitude of 19 Ponzi schemes – in chronological order



Across the identified Ponzi schemes, average victim losses have totalled approximately $1.1 billion. The largest scheme was executed through a Chinese investment vehicle which defrauded victims of $6 billion. It sold 'high-yield investment products' and then converted the proceeds into cryptocurrency. It raised money from 128,000 people in China. The mastermind, Zhimin Qian, fled China and arrived in the UK with a device holding ~61,000 BTC. She then went on a spending spree, renting a house in Hampstead Heath and spending most of her time online shopping. In 2018, her house was raided by the UK Metropolitan Police. The police seized $6 billion on USB drives. After the raid, she was able to disappear and lived under a false identity until she was arrested in 2024 in York. She pleaded guilty in September 2025 to possessing and transferring criminal property (cryptocurrency) under the Proceeds of Crime Act 2002, and was sentenced to 11 years and eight months' imprisonment. [57] Legal steps toward victim compensation are currently underway.

Ponzi schemes primarily target less-technical victims who are often fooled by flashy advertisements and fake data. For example, CryptoFX has specifically targeted lower-income Latino communities. This enables operators to draw large amounts of capital quickly into the scheme. Once the capital reaches the bad actors, the funds are often immediately paid out to other people or sent into different wallets to be laundered.

[57] "REX -v- ZHIMIN QIAN (aka Yadi Zhang) & SENG HOK LING: Sentencing Remarks", Southwark Crown Court, 11 November 2025, https://www.judiciary.uk/wp-content/uploads/2025/11/Rex-v-Zhimin-Qian-and-Seng-Ling.pdf.

While the value of proceeds from Ponzi schemes at the time of theft totalled $21.3 billion, the current value of those assets is $88.5 billion, implying an increase of $67.2 billion attributable to post-theft appreciation.

Legal Action

As cryptocurrency Ponzi schemes draw large amounts of capital and receive media scrutiny, regulators and prosecutors are forced to act. All 19 cases detailed in this report involved some form of legal action. Criminal charges were filed in 17 cases and convictions were secured in 11 cases. These outcomes underscore that stronger enforcement measures can yield tangible results across the broader ecosystem.

However, most cryptocurrency is never returned to defrauded victims and instead passes through multiple stages of laundering. Across the 19 Ponzi schemes, an average of 22% of the total proceeds has been recovered, with a total for all schemes amounting to $32.9 billion. However, six cases resulted in no recovery of funds.

Case Study: Plus Token [58]

Plus Token was a crypto investment app launched in 2018, operating worldwide but mainly focused on China. It promised high, steady profits if you deposited BTC/ETH and bought its Plus Token. It marketed an 'AI-Dog' arbitrage bot and 'mining' as the source of returns, but it was really a classic Ponzi scheme.

Users were told they could earn 16% per month, usually paid in Plus Tokens, and they needed about $500 in crypto to 'activate' the bot. There was a multi-level referral structure that rewarded bringing in new members. An estimated $2.9 billion had been collected from two million victims.

In 2019, users in China, South Korea and Japan began reporting that they couldn't withdraw funds from the Plus Token wallet. This was the first public sign that the scheme was breaking down.

Plus Token-controlled wallets started pushing large batches of coins through long chains of new addresses and toward off-ramps. The operators used classic laundering techniques and also utilised Wasabi Wallet. Next, the operators off-ramped their funds through Huobi OTCs and OKX.

Six Chinese nationals linked to Plus Token were arrested in Vanuatu and repatriated to China following a Yancheng Police investigation. China's Ministry of Public Security announced it had arrested 27 primary suspects and 82 key members of Plus Token. A lower court in Yancheng issued initial convictions for organising and leading pyramid-selling activities and related offenses. The Yancheng Intermediate People's Court released its final judgment and disclosed the seizure of crypto worth over $2 billion.

Ponzi schemes can generate substantial inflows into the cryptocurrency ecosystem and are frequently accompanied by sophisticated laundering techniques designed to move proceeds off-chain and into the control of perpetrators. Most operate covertly and are typically identified as Ponzi schemes only after users have already incurred losses, totalling hundreds of thousands of dollars' worth of cryptocurrency.

[58] Shuyu Zhang, et al., "Plus Token and investor searching behaviour – A cryptocurrency Ponzi scheme", *Accounting & Finance* (63(4) 2023), 4713–4728, https://onlinelibrary.wiley.com/doi/abs/10.1111/acfi.13128.

5) Automatic Teller Machines (ATMs)

Cryptocurrency ATMs convert physical cash directly into cryptocurrency, often enabling the recipient to obtain immediate control of the funds. This makes them a convenient tool to place untraceable cash into the digital asset ecosystem. It is the only channel that allows an individual to convert cash directly into cryptocurrency without an intermediary, thereby facilitating its use by various low-level offenders. Where operators are non-compliant (or unlicensed), controls like customer identification and recordkeeping can be weak or absent, which increases the likelihood of abuse.

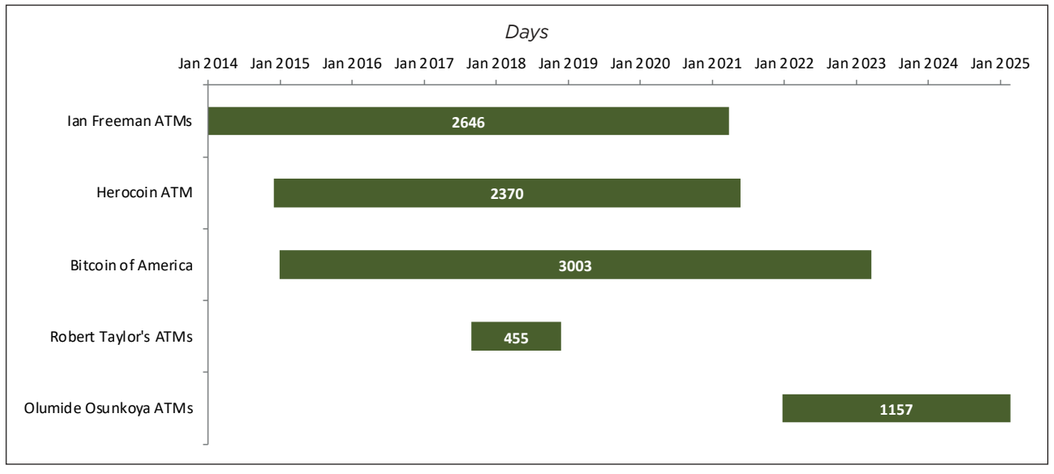
In a typical transaction, a user approaches a cryptocurrency ATM, selects 'Buy', scans a wallet QR code to provide the receiving address, deposits cash and the device transmits the corresponding cryptocurrency to that address. Such ATMs are frequently located in retail settings, such as convenience stores and petrol stations.

Criminals often coach or coerce others (including scam victims and seniors) to feed kiosks and scan wallet QR codes they control. Local networks of criminals can use them to move cash collected on-chain. Similar to regular ATMs, they often make small payments across multiple machines to stay off the radar.

This report has identified five of the most notable ATM operations which have a specific focus on money laundering and criminal enterprise. Collectively, these operators control networks comprising thousands of ATMs. An estimated total of $53 million has been moved through them, while the true amounts could be much higher.

These ATM services have been operational for an average of five years and three months. The graph below shows the duration of operations for the five ATMs identified in the Global Cryptocurrency Laundering Database.

Figure 20: Duration of operations of ATM services



The rapid growth of cryptocurrency ATMs has coincided with substantial levels of illicit activity and regulatory non-compliance among certain operators.

While the total number of cryptocurrency ATMs is estimated to be around 40,000 globally, many are fully compliant and implementing AML regulations. [59] The outliers provide a key avenue for criminals to launder ill-gotten gains. As shown in the chart above, they have managed to remain hidden and to last for many years by staying in the shadows and not drawing too much attention before being shut down.

However, even compliant cryptocurrency ATM operators may be misused for money laundering, whether by criminals acting directly or via transactions initiated by victims who have been defrauded. For example, in Australia, a crime syndicate managed to move $30 million from a series of different regulated ATMs. [60] In addition, there have been reports of many victims losing thousands of dollars through using regulated ATMs.

Legal Action

All five top ATM companies featured in the Global Cryptocurrency Laundering Database have been dismantled, and all five operators have been convicted on charges of money laundering and/or operating an unlicensed money-transmitting business. Relative to other on-ramps discussed in this report, this outcome shows the highest (100%) detection-to-conviction ratio. This is thanks to the presence of physical infrastructure that is maintained and operated in public view, facilitating identification through tips and enabling investigators to seize machines and shut down operations directly.

Additionally, the physical presence of these machines enables investigators to verify their functionality and compliance through direct, on-site testing. For example, in the Herocoin ATM case, investigators were able to deposit $14,500 in an ATM without having any KYC checks or filing a currency transaction report. [61]

From the five cases, $14 million in proceeds has been seized. However, this amount is far lower than the total value of transactions processed across these five ATM groups.

Given their distinct ability to convert cash into cryptocurrency, ATMs constitute one of the limited channels through which local criminal groups can introduce funds into the ecosystem with minimal logistical barriers. Therefore, legal action is vital to stop local criminals from exploiting this new channel.

6) Criminal Enterprises

Criminal enterprises are organised groups that engage in illicit activity to generate profit, typically operating through structured, business-like arrangements. Cryptocurrency has become one of the tools they use. Cryptocurrency is attractive to such actors because it enables rapid, cross-border transactions and can provide a degree of pseudonymity. Terrorist organisations have also leveraged these features by soliciting donations and transferring funds to operatives via cryptocurrency.

Criminal groups usually start by exploiting people, either as victims or as tools. A big and growing trend is the scam-centre model where people are trafficked to secluded compounds and forced under threats and violence to run romance scams, fake crypto-investment schemes and other online frauds that collect money from victims all over the world. Payments made by

59 "Bitcoin ATM Installations Growth", *Coin ATM Radar*, https://coinatmradar.com/charts/growth/.

60 "Australia's First Major Crypto Laundering Conviction: Inside Operation Taipan", *TRM*, https://www.trmlabs.com/resources/case-studies/australias-first-major-crypto-laundering-conviction-inside-operation-taipan.

61 "O.C. Man Admits Operating Unlicensed ATM Network that Laundered Millions of Dollars of Bitcoin and Cash for Criminals' Benefit", U.S. Attorney's Office, 22 July 2020, https://www.justice.gov/usao-cdca/pr/oc-man-admits-operating-unlicensed-atm-network-laundered-millions-dollars-bitcoin-and.

victims effectively constitute revenue for the criminal group, which is subsequently introduced onto the blockchain and routed through multiple transactions to enable rapid layering.

Criminals also exploit people as 'infrastructure' for getting money on-chain. This includes recruiting money mules who let criminals use their IDs or platform accounts in exchange for a fee, or who are tricked into thinking they're doing legitimate work. Criminal groups buy or steal identity data at scale and use it to open on-ramp accounts, run card fraud or set up merchant fronts. The fiat looks like it's coming from many different regular people, but in reality many are coerced or simply fronting for organised crime.

The most significant scam which has taken off across the criminal industry is 'pig butchering'. Pig butchering is a confidence-based investment scam where criminals slowly 'fatten up' a victim before financially 'slaughtering' them. Scammers typically contact people out of the blue on WhatsApp, social media or dating apps and pretend to be a friendly stranger or potential partner. Over weeks or months they build what feels like a real relationship, then introduce a 'can't-miss' investment opportunity. Early small deposits appear to grow, and victims may even be allowed to withdraw a little so they trust the system. Once the victim has poured in serious money, withdrawals are suddenly blocked and the scammer vanishes with everything. [62]

This activity is taking off because organised crime has turned it into an industrial business model, supercharged by tech. Scam compounds in parts of Southeast Asia use trafficked workers to run thousands of parallel chats at scale, often targeting people in North America, Europe and Asia. An estimate from Chainalysis indicates that in 2024, revenues from this activity grew nearly 40% year-on-year. [63]

The Global Cryptocurrency Laundering Database features five of the most prominent criminal groups: Prince Holding Group, Clan del Golfo, Lusocoin, TGR Group and Funnull Technology, which together are responsible for laundering an estimated $26 billion.

a) Prince Group

Prince Group was a Cambodia-based conglomerate founded in 2015 and headquartered in Phnom Penh. It presented itself as one of Cambodia's largest business groups, with interests in real estate development, financial services and airlines. The group was chaired by Chinese-born businessman Chen Zhi, who promoted a glossy image of rapid growth, philanthropy and adherence to international ESG standards. [64]

In 2025, major governments began publicly describing Prince Group not just as a conglomerate but as a transnational criminal organisation. On 14 October 2025, the US Treasury designated the Prince Group a "Transnational Criminal Organization" and sanctioned 146 associated individuals and entities, while the US Department of Justice unsealed charges accusing Chen Zhi and the group of running forced-labour scam compounds in Cambodia that carried out large-scale online investment and pig-butchering crypto scams. The UK and later South Korea followed with their own sanctions. [65]

62 "Avoid Scams: Investment Fraud and Pig Butchering", United States Secret Service, https://www.secretservice.gov/investigations/investmentfraud-pigbutcherings.

63 "Crypto Scam Revenue 2024: Pig Butchering Grows Nearly 40% YoY as Fraud Industry Leverages AI and Increases in Sophistication", *Chainalysis*, 13 February 2025, https://www.chainalysis.com/blog/2024-pig-butchering-scam-revenue-grows-yoy/#:~:text=In%202024%2C%20pig%20butchering%20revenue,butchering%20scams%20declined%2055%25%20YoY.

64 "Prince Group Transnational Criminal Organization (TCO)", U.S. Department of the Treasury, October 2025, https://ofac.treasury.gov/media/934686/download?inline.

65 https://th.usembassy.gov/prince-group-indicted-cambodian-scam-compounds/.

US authorities have also moved to forfeit roughly 127,000 BTC, valued at $14–15 billion, which makes it the largest seizure in history. Law-enforcement agencies in Singapore, Taiwan and elsewhere launched related asset seizures and investigations. [66] In January 2026, Zhi was extradited from Cambodia to China. [67]

b) Clan del Golfo

The second criminal enterprise highlighted in the Global Cryptocurrency Laundering Database is the crypto-based gambling money laundering network of the Colombian cartel Clan del Golfo, also known as the Autodefensas Gaitanistas de Colombia, the country's largest drug cartel. Clan del Golfo controls major cocaine routes from Colombia to Europe and has long relied on front companies and corrupt logistics to move money. Around 2020, one of its European finance structures evolved into a specialised laundering network. It handled proceeds from multi-ton cocaine shipments to Europe, then washed the profits using cryptocurrency and offshore companies, instead of bulk cash. This network operated across Colombia and Spain and was linked to other countries and various European hubs. It was closely integrated into the cartel's senior leadership.

According to Colombian and Spanish authorities, this crypto group was built by money-launderers who first used traditional hawala-style systems, then shifted heavily into crypto in late 2020 to move millions across borders, with fewer physical risks and less reliance on banks. [68] The group set up front companies and used virtual-asset service providers in different countries, including Spain, Lithuania, the United States and Colombia, coordinating via encrypted platforms.

Investigators who later broke into its communications and traced blockchain transactions were able to map more than $700 million in suspicious crypto flows tied to Clan del Golfo's cocaine trade, and in October 2025 an operation backed by Europol led to arrests of key operators and the seizure of at least 25 properties, nine companies and a fleet of luxury vehicles in Spain and Colombia. [69]

c) Lusocoin [70, 71]

Lusocoin is described by the Brazilian Federal Police (PF) as an international laundering scheme that allegedly converted criminal proceeds into crypto to obscure provenance and move value across borders. Investigators traced activity to a proprietary token called Lusocoin, allegedly used to attract investors while also functioning as a vehicle for laundering.

PF stated that the group operated largely remotely from Dubai (UAE) and that its laundering mechanism benefited criminal activity, including drug trafficking, smuggling, customs evasion and terrorism financing; $540 million was identified in illicit flows, although PF estimates that the true number could be more than $9 billion.

66 Martin Young, Jack Adamovic Davies, Yan Z.H. and Bernadette Carreon, "Multiple Identities Reveal Ties Between Chinese Businessman and Alleged Cambodian 'Criminal' Conglomerate", *OCCRP*, 19 December 2025, https://www.occrp.org/en/scoop/multiple-identities-reveal-ties-between-chinese-businessman-and-cambodian-criminal-conglomerate.

67 Sui-Lee Wee, "Why Cambodia Handed Over a Man Accused of Stealing Billions in Crypto Scam", *The New York Times*, 8 January 2026, https://www.nytimes.com/2026/01/08/world/asia/cambodia-scam-china-prince-group-chen.html.

68 "Five central suspects arrested in whole-sale cocaine trafficking case", Europol, 9 October 2025, https://www.europol.europa.eu/media-press/newsroom/news/five-central-suspects-arrested-in-whole-sale-cocaine-trafficking-case.

69 Ibid.

70 "PF triggers operation against money laundering through cryptoassets", Ministry of Justice and Public Security, Brazil, 24 September 2025, https://www.gov.br/pf/pt-br/assuntos/noticias/2025/09/pf-deflagra-operacao-contra-lavagem-de-dinheiro-por-meio-de-criptoativose.

71 "Brazil's Federal Police Dismantle $540 Million Crypto Laundering Network in 'Operation Lusocoin'", *TRM*, 10 October 2025, https://www.trmlabs.com/resources/blog/brazils-federal-police-dismantle-540-million-crypto-laundering-network-in-operation-lusocoin.

In September 2025, PF executed 13 search warrants and 11 temporary arrests. It reported precautionary asset measures that could exceed $563 million, including blocking bank accounts of 65 individuals and entities, seizing six vehicles and six properties and freezing approximately 30 crypto wallets plus additional exchange-held assets. With support from T3+ FCU, authorities made 4,336,883 USDT unavailable (approximately $4.34 million).

d) TGR Group

The TGR Group was an international illicit-finance operation that provided money-laundering and sanctions-evasion services, particularly for Russian elites and other high-end clients, including the Kinahan Cartel. According to the US Treasury, it used a mix of shell companies, "corporate concierge" services, traditional banking touchpoints and digital assets (notably stablecoins such as USDT/Tether) to help clients place, layer and integrate illicit funds. It is estimated that the group has laundered over $1 billion. [72]

The group's operations ranged from moving value between cash and crypto to obscuring sources of wealth for purchases, such as UK real estate. US authorities assessed that it was controlled by George Rossi, a Russia-born Ukrainian national, and that it also leveraged other illicit actors to support large-scale laundering activities.

On 4 December 2024, the US Treasury's Office of Foreign Assets Control (OFAC) announced sanctions against five individuals and four entities tied to or leveraging the TGR Group. In parallel, European and UK-led law-enforcement activity targeted the broader TGR laundering ecosystem, with 84 arrests and significant seizures, alongside convictions for some operational participants. [73]

e) Funnull Technology

Funnull Technology Inc. was a Philippines-based cloud and digital infrastructure provider. It enabled smaller illicit actors to carry out malicious activity by utilising its structure.

It bought IP address blocks and other hosting resources from major cloud providers and resold them to operators of fraudulent trading platforms, gambling sites and phishing pages, ultimately supporting hundreds of thousands of scam websites and causing more than $200 million in reported victim losses. By placing itself in the middle as a technical service provider rather than the visible face of the scam, Funnull acted as a kind of infrastructure laundromat, hiding criminal sites behind seemingly legitimate cloud networks and constantly rotating domains via domain-generation algorithms and ready-made web templates. [74]

It made it easy and cheap for scam syndicates to spin up and replace fake investment platforms at scale, ensuring a steady flow of new victims. Funnull itself accepted payment for its services via cryptocurrency, and the addresses OFAC listed for the company show multi-million-dollar flows from scam-linked wallets and direct ties to Huione Pay. [75]

On 29 May 2025, the US OFAC imposed sanctions on Funnull Technology Inc. and its administrator, Liu Lizhi, for providing computer infrastructure to hundreds of thousands of

72 "Operation Destabilise: NCA disrupts $multi-billion Russian money laundering networks with links to, drugs, ransomware and espionage, resulting in 84 arrests", National Crime Agency, 4 December 2024, https://www.nationalcrimeagency.gov.uk/news/operation-destabilise-nca-disrupts-multi-billion-russian-money-laundering-networks-with-links-to-drugs-ransomware-and-espionage-resulting-in-84-arrests.

73 Ibid; "Treasury Exposes Money Laundering Network Using Digital Assets to Evade Sanctions", U.S. Department of the Treasury, 4 December 2024, https://home.treasury.gov/news/press-releases/jy2735.

74 "Infrastructure Used to Manage Domains Related to Cryptocurrency Investment Fraud Scams between October 2023 and April 2025", FBI, 29 May 2025, https://www.ic3.gov/CSA/2025/250529.pdf.

75 "OFAC Sanctions Funnull Technology Inc. for Supporting Pig Butchering Scams", *Chainalysis*, 29 May 2025, https://www.chainalysis.com/blog/ofac-sanctions-funnull-technology-pig-butchering-scams-may-2025/.

websites involved in virtual-currency investment scams. The designation, taken in coordination with the FBI, added Funnull and Liu to the Specially Designated Nationals list and identified associated crypto addresses, effectively cutting them off from US persons and much of the international financial system. [76]

Cartels

Cartels and their facilitators have progressively integrated cryptocurrency into cross-border money laundering and value transfer. Notably, major Mexican drug cartels and their laundering networks now routinely use digital assets to move and obscure illicit proceeds.

In addition to regular types of layering techniques discussed above, this report has identified five of the main avenues in which cartels use cryptocurrency: 1) Digital Remittance Systems, 2) Paying Upstream Suppliers, 3) Professional Money Laundering Partners, 4) Trade-based money laundering schemes, 5) Extortion schemes.

1) Digital Remittance Systems

A remittance system is an organised arrangement that lets money be sent from one person or country to another, usually across borders, through a defined set of rules, providers and settlement processes. Cartels use cryptocurrency as a digital remittance system to move value across borders quickly and covertly.

Rather than smuggling bulk cash or using wire transfers that raise flags, cartels or their money brokers convert illicit proceeds into crypto and then transfer it internationally to counterparts who can reconvert it to local currency. For example, Jimenez Castro, a Sinaloa-linked launderer based in Mexico, directed couriers in the US to deposit drug cash into various crypto wallets, effectively beaming the funds to Mexico for the cartel. His Ethereum address was identified and sanctioned. [77]

2) Paying Upstream Suppliers

Cartels and drug trafficking networks use crypto to pay upstream suppliers for illicit commodities, notably precursor chemicals for fentanyl or methamphetamine from China, but also occasionally finished drugs on darknet markets. Rather than traditional bank payments, traffickers purchase Bitcoin or stablecoins and send them to the supplier's wallet as payment for goods. This typology has grown with the fentanyl trade.

97% of the Chinese precursor manufacturers for fentanyl offered payments in cryptocurrency. [78] Major cartels, such as the Sinaloa Cartel and the Cartel Jalisco Nueva Generación, purchase these precursors to manufacture synthetic opioids, including fentanyl, which they then traffic and distribute in the US. [79]

3) Professional Money Laundering Partners

Rather than cartels handling crypto themselves, they often rely on professional money launderers and underground brokers who specialise in moving funds through crypto. These

76 "Treasury Takes Action Against Major Cyber Scam Facilitator", U.S. Department of the Treasury, 29 May 2025, https://home.treasury.gov/news/press-releases/sb0149.

77 "Treasury Targets Sinaloa Cartel Fentanyl Trafficking Operations and a Colombian Cartel Leader", U.S. Department of the Treasury, 26 September 2023, https://home.treasury.gov/news/press-releases/jy1763.

78 "Beyond Fentanyl", *TRM*, 5 June 2024, https://www.trmlabs.com/reports-and-whitepapers/beyond-fentanyl-cryptocurrencys-role-in-the-international-drug-precursor-market.

79 "China-Based Chemical Manufacturing Companies and Employees Indicted for Alleged Fentanyl Manufacturing and Distribution", U.S. Department of Justice, 24 October 2024, https://www.justice.gov/archives/opa/pr/china-based-chemical-manufacturing-companies-and-employees-indicted-alleged-fentanyl.

intermediaries operate as black-market OTC crypto brokers or are part of broader money laundering organisations. Cartels deliver bulk cash to these brokers and the brokers handle the rest.

A prominent variant are the Chinese Money Laundering Networks (CMLNs), which pair cartel cash with China's underground finance: CMLNs collect drug dollars in cash, convert them into crypto and send value to China, while in parallel ensuring an equivalent amount in pesos is delivered to the Mexican cartel via a 'mirror' payout.

For instance, in 2024, Operation Fortune Runner identified an LA-based Chinese broker network which took Sinaloa Cartel cash, engaged in trade-based laundering and crypto purchases to hide the source, then made the proceeds available to cartel members in Mexico. The Justice Department investigation alleged the group used trade-based schemes and crypto purchases to conceal over $50 million in drug proceeds, making funds accessible in Mexico. [80]

4) Trade-Based Money Laundering Schemes (TBML)

In many cases, cartels use crypto as one link in a larger laundering chain that includes traditional trade and cash methods. Cartels often combine crypto with TBML. TBML is when illicit funds are used to buy commodities or goods, which are then sold and the proceeds moved, with crypto facilitating part of the loop.

5) Extortion Schemes

Cartels also utilise cryptocurrency for their revenue-generating schemes. Kidnapping or extortion schemes often demand that ransoms be paid in Bitcoin, while street-level drug sales use online platforms paid in crypto.

Investigative journalists reported in 2023 that MS-13 cells in Honduras and El Salvador were increasingly demanding payment in Bitcoin for helping move cocaine north, and in some extortion cases. [81]

Below are 10 examples of cryptocurrency usage within cartels which operate from Mexico, Venezuela, Brazil, Columbia, Central America, Ireland and Italy.

[80] "Federal Indictment Alleges Alliance Between Sinaloa Cartel and Money Launderers Linked to Chinese Underground Banking", U.S. Department of Justice, 18 June 2024, https://www.justice.gov/archives/opa/pr/federal-indictment-alleges-alliance-between-sinaloa-cartel-and-money-launderers-linked.

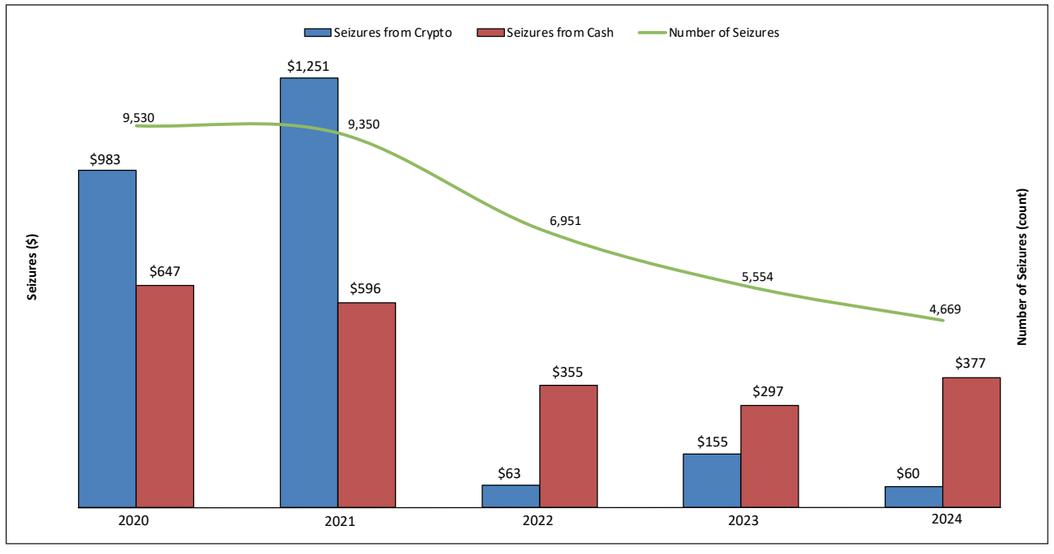
[81] Douglas Farah and Marianne Richardson, "The Growing Use of Cryptocurrencies by Transnational Organized Crime Groups in Latin America", *Georgetown Journal of International Affairs*, 20 March 2023, https://gjia.georgetown.edu/2023/03/20/the-growing-use-of-cryptocurrencies-by-transnational-organized-crime-groups-in-latin-america/.

Table 5: 10 Different cartels which have utilised cryptocurrency

Number	Cartel	Primary Operation Area	Crypto Involvement	Origin Date	Legal Action
1	Sinaloa Cartel	Mexico	Laundering drug proceeds via crypto; some factions accepting crypto for payments.	~2018	24 defendants were charged with 4 counts including conspiracy to launder monetary instruments, for running a cryptocurrency laundering ring between US and Mexico. US Authorities seized $5 million in narcotics proceeds, 302 pounds of cocaine, 92 pounds of methamphetamine.
2	Cártel de Jalisco Nueva Generación	Mexico	Laundering via crypto brokers; paying suppliers in crypto	~2016	Mexican national convicted for laundering $5.5 million through cryptocurrency. The DEA seized 3 kilograms of fentanyl, 52.77 kilograms of cocaine and $1.3 million.
3	Cartel del Noreste	Northeast Mexico	Accepting crypto as payment for fentanyl precursors (via China); possible use of stablecoins	~2020	N/A
4	Tren de Aragua	Venezuela	Value transfer and laundering via crypto: converted multi-crime proceeds to crypto.	~2021	In Spain, Rojas Guevara, one of Chile's most wanted and allegedly linked to the organized crime group Tren de Aragua, was detained in connection to a $150 million cryptocurrency fraud scheme used to launder proceeds from drug trafficking and extortion.
5	MS-13	Central America	Extortion and drug transport payments in Bitcoin; using crypto ATMs to convert cash	~2019	N/A
6	Primeiro Comando da Capital	Brazil	Adopting crypto for money moves and investments: internal money transfers, laundering via exchanges, possibly darknet use	~2019	N/A
7	Clan Del Golfo	Columbia	Crypto laundering of cocaine proceeds via brokers and online investments	~2020	Europol took down a cryptocurrency laundering ring within the cartel which processed $700 million. 25 properties, 9 companies and 17 vehicles were seized with an estimated value of EUR 12 million. There were 5 arrests.
8	Comando Vermelho	Brazil	Used cryptocurrencies to hinder tracking	~2023	In Brazil, 48 arrests took place and ~$42 million was seized in crypto assets and bank accounts.
9	Kinahan Cartel	Ireland	Laundering networks converting between cash and cryptocurrency as part of large-scale laundering networks.	~2021	N/A
10	Ndrangheta	Italy	Cryptocurrency in connection with illicit commerce and payments	~2018	N/A

As shown, cartels are beginning to heavily favour cryptocurrency as an avenue for laundering.

Figure 21: US seizures from transnational criminal organisations [82]



[82] "2025 National Drug Threat Assessment", U.S. Department of Justice, May 2025, https://www.dea.gov/sites/default/files/2025-05/2025%20National%20Drug%20Threat%20Assessment_Web%205-12-2025.pdf.

US authorities managed to seize a total of $2.5 billion in virtual assets from transnational crime organisations from 2020 to 2024, compared to only $2.2 billion in cash.

The total seizures from cryptocurrency per year has drastically decreased from $983 million in 2020 to only $60 million in 2024, highlighting how the cartels have been able to escape with billions of funds from fentanyl and other drug-related sales.

Although legal measures to secure takedowns have achieved partial success, sustained law enforcement action is still required. An example of a successful operation is discussed below.

Case Study: Treebu [83]

From 2020 to 2024, Alain Bibliowicz Mitrani, a dual French-Colombian citizen based in Miami, ran an elaborate money laundering enterprise that moved over $300 million in drug proceeds worldwide. His public-facing company Treebu masked the illicit operations. A significant portion of the proceeds he laundered came in the form of cryptocurrency from drug cartels in Colombia and Mexico (including the Sinaloa Cartel), which he and co-conspirators then converted into cash using a web of bank accounts and financial transactions. Essentially, his firm acted as a crypto cash-out service for cartels, taking their crypto and providing them with dirty cash in return (minus a fee). He established numerous shell companies and bank accounts to receive and transfer funds, lying to banks about the nature of the businesses. Mitrani integrated funds into the banking system and then withdrew and transported cash on behalf of traffickers. By the time of his arrest, he had funded a lavish lifestyle with his laundering commissions.

Cartel clients had already placed drug money into crypto and Mitrani's job was to monetise it. In 2025, Mitrani was convicted by a federal jury on five counts, including money laundering conspiracy and operating an unlicensed money transmitter, and is scheduled to be sentenced in 2026. This was a rare instance of a launderer going to trial; most plead out. The case was part of Operation Take Back America, a Department of Justice initiative against cartels.

To conclude, criminal groups use cryptocurrency as a convenient entry point into the financial system, exploiting loopholes in oversight and the speed of digital transfers. The cases highlighted here represent only a small fraction of the widespread adoption of this method by criminal and terrorist groups.

[83] "Florida Man Convicted of Leading $300 Million Money Laundering Operation for Transnational Criminal Organizations", U.S. Attorney's Office, 12 December 2025, https://www.justice.gov/usao-edny/pr/florida-man-convicted-leading-300-million-money-laundering-operation-transnational.

9. Layering and Obfuscation

Layering is the intermediate stage of the traditional money laundering process which follows placement. In conventional laundering, it creates distance between the criminal source and the funds by moving money through a maze of transactions across multiple banks and jurisdictions, obscuring the audit trail and complicating efforts to prove origin.

Obfuscation is the broader tactic that makes those layers hard to follow. In the world of banking it includes: structuring deposits to avoid reporting thresholds, using nominees and money mules, mixing dirty and clean revenues in cash-intensive businesses, falsifying documentation, and timing transfers to exploit gaps between institutions and regulators.

In cryptocurrency, layering and obfuscation pursue the same goal: to break the link between funds and their criminal source. The point isn't secrecy in the absolute sense; rather, it is to generate enough transactional noise and protocol changes so that attribution becomes costly and time consuming.

There are also important differences from traditional finance. Blockchains offer radical transparency: every transfer is permanently recorded, enabling analytics firms and law enforcement to cluster addresses, follow flows and flag patterns. On the other hand, crypto is borderless and always open, so movement can be faster, with fewer chokepoints, and pseudonymity may persist until transactions are traced or the underlying infrastructure is seized through law enforcement action.

For the purposes of layering and obfuscation, criminals have evolved to employ different methods, including:

1) On-chain;
2) Cross-chain/Asset;
3) Decentralised Finance (DeFi);
4) Cryptocurrency Assets.

Layering Methods

1) On-chain

On-chain is defined as anything "located, performed or run inside a blockchain system". [84] A blockchain is a shared digital ledger that many computers keep identical copies of; it records transactions in blocks that are linked together, and once the network agrees, a new block is added, and the record becomes very hard to change.

This report identifies five notable services and on-chain practices that malicious actors use to launder illicit funds: Peel Chains, Mixers, CoinJoins, Smurfing and Cryptocurrency Gambling. These are discussed below.

a) Peel Chains

A wallet first receives a large amount of cryptocurrency, e.g., from a hack or a Ponzi scheme. Small fractions of the funds are repeatedly sent to new wallets. This process continues in quick succession over several transactions, often across hundreds of wallets. They keep on moving

[84] "ISO/DIS 22739(en): Blockchain and distributed ledger technologies – Terminology", ISO, https://www.iso.org/obp/ui/es/#iso:std:iso:22739:dis:ed-1:v1:en:sec:3.6.

along a chain like a conveyor belt. At various points, the funds are transferred to different platforms to cash out into fiat currency. The rest of the funds continue to be transferred. Each step 'peels off' a small part of the original sum, breaking it down into smaller, less noticeable amounts, making it difficult to pinpoint the origin or final destination. [85]

This can be used for several different reasons: small 'peels' can be kept under exchange alert thresholds which stops automatic reviews; splitting funds lets the user test multiple exchanges in case one flags it; it doesn't require any specific tools meaning it's cheaper and easier to use; it can be executed rapidly and at scale with automation; and it can be effective to move funds across jurisdictions.

For example, in the Bitfinex hack, the stolen funds were sent through thousands of transactions and movements and then eventually reaggregated into a wallet controlled by the operator, Lichtenstein, on a regulated exchange. [86]

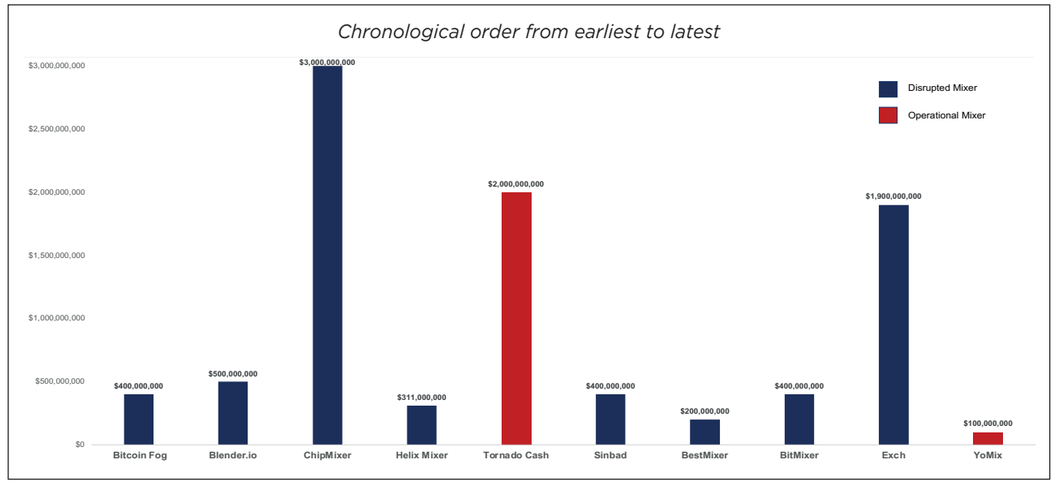
b) Mixers

Cryptocurrency mixers (also called tumblers) are services that take in coins from many users, shuffle them together and then send back equivalent amounts minus a fee to new addresses. By breaking the on-chain link between the coins put in and the coins which are sent out, mixers aim to make it harder to trace the flow of funds on public blockchains.

People sometimes cite privacy reasons for using them, such as separating their identity from their spending history or protecting salary payments from casual snooping. However, the same technique can also be abused to launder proceeds of hacks, scams, ransomware or sanctions-evading activity.

While not inherently illegal, mixers can be high-risk services. This report has identified 10 of the highest-risk mixers. An estimated total of at least $9.2 billion in illicit cryptocurrency has passed through these mixers.

Figure 22: Illicit flows into mixers



85 Robert Whitaker, "What Is a Peel Chain in Crypto Money Laundering?", *Merkle Science*, 17 December 2024, https://www.merklescience.com/blog/what-is-a-peel-chain-in-crypto-money-laundering.

86 "Bitfinex Hacker Sentenced in Money Laundering Conspiracy Involving Billions in Stolen Cryptocurrency", Office of Public Affairs, 14 November 2024, https://www.justice.gov/archives/opa/pr/bitfinex-hacker-sentenced-money-laundering-conspiracy-involving-billions-stolen.

Every single case identified has processed a minimum of $100 million and an average of $921 million, indicating the large size of this industry. The largest case was ChipMixer which accounted for over $3 billion in illicit flows. It had processed over $200 million from DNMs and at least $700 million from wallets which were designated from thefts. It was also used by Russia's GRU (APT28) to buy infrastructure and by North Korea's Lazarus group. [87]

Nine out of the top 10 mixers have predominantly accepted Bitcoin and six have exclusively taken Bitcoin. Six mixers have had their operators charged and three have had convictions: Bitcoin Fog, Helix Mixer and Tornado Cash. Eight mixers have been taken offline through seizures and law-enforcement shutdowns; however, two remain operational: Tornado Cash and YoMix. One platform, BitMixer, had voluntarily shut down, citing ethical reasons. Collectively, authorities have seized $579 million in cryptocurrency and other assets from these services.

Mixers are a key avenue for launderers to attempt to route illicit cryptocurrency from heists and scams. Used by many, they can directly break the on-chain link between the source and the new wallets.

c) CoinJoins

CoinJoin is a Bitcoin privacy technique where many users combine their coins into one transaction with multiple equal-value outputs. Because all the outputs look the same, it's hard for outsiders to tell which input paid which output. No third party ever holds anyone's coins due to it being non-custodial. Criminals use CoinJoin for the same reason regular users seek privacy: to break on-chain links and frustrate tracing. The Global Cryptocurrency Laundering Database includes the most prolific service that criminals have used to launder millions: Samourai Wallet.

Samourai Wallet was taken offline in April 2024 by US authorities in coordination with Icelandic officials. Samourai Wallet had a main CoinJoin protocol called Whirlpool. In addition, it had a second service called Ricochet. Both enabled users to create additional and unnecessary transactions between sending and receiving addresses. It facilitated $200 million in illegal transactions. The founders pleaded guilty and were sentenced to five years and ordered to forfeit $237 million. [88]

d) Smurfing

Smurfing, also called structuring, is a money-laundering tactic where a large amount of value is split into many small, ordinary-looking transfers to avoid triggering anti-money-laundering (AML) thresholds and reviews.

In crypto, this typically means funding many fresh wallets ('smurfs'), moving modest amounts over time and routing them through multiple venues before reconsolidating or cashing out. The intent isn't sophisticated movements but camouflage by volume and routine. The operators intend to keep each hop small and unremarkable so automated controls treat it as normal customer activity.

e) Cryptocurrency Gambling

Crypto gambling platforms let users deposit cryptocurrencies to place bets on casino games or sports and then withdraw their balance, often to a different wallet than the one they used

87 "Justice Department Investigation Leads to Takedown of Darknet Cryptocurrency Mixer that Processed Over $3 Billion of Unlawful Transactions", U.S. Department of Justice, 15 March 2023, https://www.justice.gov/archives/opa/pr/justice-department-investigation-leads-takedown-darknet-cryptocurrency-mixer-processed-over-3.

88 "Founders Of Samourai Wallet Cryptocurrency Mixing Service Plead Guilty", U.S. Attorney's Office, 6 August 2025, https://www.justice.gov/usao-sdny/pr/founders-samourai-wallet-cryptocurrency-mixing-service-plead-guilty.

to make the deposit. Once funds enter the platform, movements will happen on the casino's internal ledger and not on the public blockchain, so outside observers only see 'money went in' and 'money came out'. Many sites operate across borders. They may have weaker identity checks, and process large volumes of small, fast transactions which makes it difficult for regulators or investigators to follow a clear trail of where funds went.

Because of these features, crypto gambling can be misused as a tool for money laundering. Illicit crypto can be deposited, 'churned' through bets and transfers and then withdrawn to fresh addresses, breaking the direct link to the original crime. For example, 3,755 BTC were allegedly sent to MTI, the largest Ponzi scheme in South Africa, by victims in the hopes they would see an increased value of their portfolio, but instead their money was reportedly stolen and sent to an online sports betting site. [89]

2) Cross Chain/Asset

Cross chain is moving or exchanging a virtual asset from one blockchain to another. Cross assets is exchanging one virtual asset for a different virtual asset. Both of these are utilised to layer funds in high volumes.

Cross-chain laundering stands out as the main way criminals move illicit crypto value, overtaking older single-chain cash-out and mixer models. Research by Elliptic noted that by mid-2025, more than $21.8 billion in criminal and other high-risk crypto activity had been routed through cross-chain infrastructure. [90]

The predominance of cross-chain volumes over mixers, combined with the rapid growth in those volumes, shows that cross-chain laundering has shifted from a marginal technique into the primary mechanism for hiding crypto proceeds in today's multi-chain ecosystem.

This report has identified two of the most notable cross-chain/asset laundering techniques that bad actors have utilised: Bridging and DEX Swapping.

a) Bridging

Bridging in crypto is the process of moving tokens or data from one blockchain to another. A variety of methods are employed to accomplish this, each designed to increase transactional complexity and reduce traceability.

The most commonly used bridging mechanism involves locking tokens on the source chain and minting a corresponding 'wrapped' representation on the destination chain. When you go back, the wrapped tokens are burned and the originals are released. Another common version is a liquidity bridge where you move an asset from one blockchain to another by drawing from shared pools of that asset on each side, rather than minting a 'wrapped' version.

Launderers exploit this technique to blur the provenance of the funds. Once funds jump chains, single-chain analytics lose context and the money appears to restart with fresh tokens. Launderers often combine bridges with DEX trades and fresh addresses, so each hop changes both the asset and the network, fracturing the visible trail.

This behaviour has two big consequences for investigations. First, it multiplies the search space. Instead of tracing a single pathway, analysts must review movements across multiple chains. Second, it creates chokepoints. Because bridges can freeze or blacklist assets, one

89 Ciaran Ryan, "Data dump spills the beans on Mirror Trading International", *Tech Central*, 21 September 2020, https://techcentral.co.za/data-dump-spills-the-beans-on-mirror-trading-international/177117/.

90 "The state of cross-chain crime 2025", *Elliptic*, https://www.elliptic.co/resources/the-state-of-cross-chain-crime-2025.

can still interdict flows if they are promptly identified. Bridges are also attractive targets for attackers, as compromising them can both generate illicit proceeds and provide additional cover for laundering.

While bridges are not illegal, they can be abused by criminals to launder large sums of money. For example, an FTX-Affiliated company, RenBridge was used by many criminals to launder their funds. An estimated $540 million of illicit funds from hacks, fraud and ransomware was moved through RenBridge. [91] Reporting at the time also highlighted its use by Russia-linked ransomware groups and flows connected to North Korea-attributed thefts. The service was wound down after the FTX collapse. [92]

b) DEX Swapping

Decentralised exchange (DEX) swapping is trading one crypto token for another directly on the same blockchain, without a centralised intermediary. You connect a self-custody wallet, then pick the token you're selling and the token you want, and a smart contract handles the trade.

DEX swaps allow launderers to convert tokens to easier-to-launder virtual assets. It also means that the crypto is harder to trace.

As with bridges, DEX swaps aren't illegal but they can be abused. There have been many instances of different services processing illicit funds. For example, in the Horizon hack, the thieves obtained $100 million of different stolen tokens and swapped them for 85,837 ETH, using Uniswap. [93]

3) Decentralised Finance (DeFi)

DeFi is a way to offer financial services without traditional intermediaries such as banks or brokers. Instead, DeFi runs on public blockchains, where 'smart contracts' are small programs that automatically execute agreements, once conditions are met. Because the code is open and the ledger is transparent, anyone with an internet connection and a crypto wallet can access these services and interact directly, without permission from a central authority.

This report has identified four of the most prominent techniques launderers use on DeFi platforms: Liquidity pools, Flash loan obfuscation, NFT wash trading and Cross-chain aggregators.

a) Liquidity Pools

Liquidity pool cycling is the practice of moving the same capital between different DeFi liquidity pools to keep it parked where rewards are best. Criminals can 'cycle' funds through many automated market maker pools so the assets mingle with large, legitimate volumes and the trail gets harder to follow. Although on-chain forensics can reconstruct transaction flows, the process remains substantially more complex.

b) Flash Loan Obfuscation

A flash loan is a special kind of crypto loan that exists only for the duration of one blockchain transaction, meaning you borrow the funds and pay them back almost immediately in the same action.

91 "Cross-chain crime: over half a billion dollars laundered through a cross-chain bridge", *Elliptic*, 10 August 2022, https://www.elliptic.co/blog/analysis/cross-chain-crime-more-than-half-a-billion-dollars-has-been-laundered-through-a-cross-chain-bridge.

92 Ren (@renprotocol), *X* post, 7 December 2022, 6.34pm, https://x.com/renprotocol/status/1600559366440390657.

93 "The Harmony Horizon Bridge Hack", *Elliptic*, 2023, https://www.elliptic.co/hubfs/Harmony%20Horizon%20Bridge%20Hack%20P1%20briefing%20note%20final.pdf.

Flash loan obfuscation can be used to manufacture a very complex on-chain trail right before value is moved onward, making provenance harder to assess. The actor borrows a large amount for a single transaction and rapidly routes it through many swaps, tokens and protocols, often splitting the flow across multiple paths and then recombining it, so the trace looks like ordinary arbitrage or aggregator activity rather than a directed movement of funds.

Because the loan principal must be repaid, the only lasting piece is the net profit or extracted proceeds, which can then be sent to new addresses, bridged to another chain or deposited to an exchange. It increases the effort required to link the final beneficiary back to the original source.

c) NFT Wash Trading

An NFT (non-fungible token) is a unique digital token on a blockchain that represents ownership of something, usually a digital item or sometimes a right or claim tied to a real-world thing.

A key avenue for launderers through this environment is wash trading. This is when the same person or a small colluding group buys and sells an NFT among their own wallets to fake market activity. It creates the illusion of demand and higher prices, even though no real third-party buyer is involved. This leads to unsuspecting victims paying far more than the NFT is worth and providing the launderers with cleaner funds which they can then transfer.

d) Cross-Chain Aggregators

Cross-chain aggregators are tools that find you the best way to move value or execute a trade across multiple blockchains in one go. Instead of manually picking a bridge, a DEX and a route, the aggregator compares many options and builds a single transaction that aims for the best price, speed and reliability.

Aggregators can execute a swap → bridge → swap with a single signature and even complete the destination-side swap without the user signing there. This collapses multiple touchpoints and KYC points it may have passed through into one flow, which criminals can exploit. It can hop chains and assets in minutes, sometimes splitting flows. This shrinks the window available to law enforcement authorities and investigators to identify funds and coordinate freezes.

4) Coins and Tokens

Cryptocurrency is a form of digital money that lives on networks, such as blockchains, and that enables peer-to-peer transfers without reliance on a central intermediary.

Tokens are digital assets issued on top of an existing blockchain (usually via smart contracts). Unlike a blockchain's native coin (e.g., ETH on Ethereum), tokens ride on that chain and can represent access, rights or other assets.

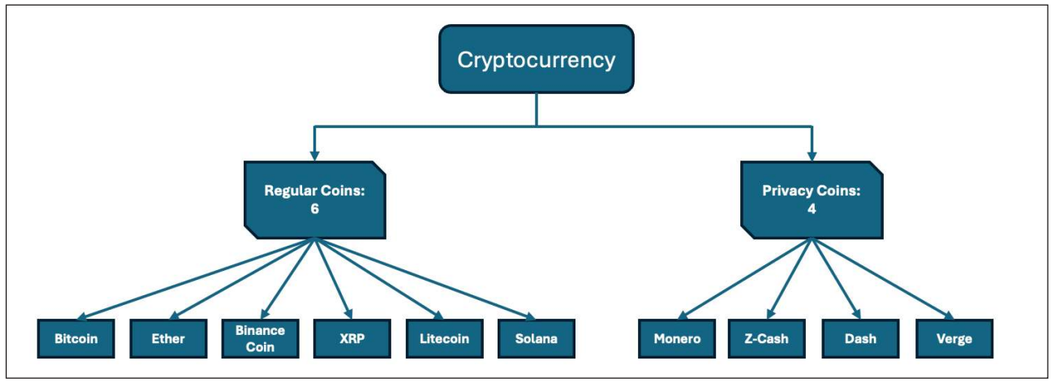
Stablecoins are a subset of crypto tokens that are designed to keep a stable price by linking to something like a currency and offering redeemability at par. They're issued by private entities and circulate on blockchains.

This report has examined coins, tokens and stablecoins which have had prevalent use with money launderers.

Cryptocurrency

Ten currencies have been identified as the most prominently used for money laundering. These comprise six regular crypto coins (Bitcoin, Ether, Binance Coin, XRP, Litecoin and Solana) and four privacy-tailored coins (Monero, Z-Cash, Dash and Verge).

Figure 23: Different types of cryptocurrency



Bitcoin (BTC), launched in 2009, was the first viable decentralised cryptocurrency. Since then, it has remained the dominant cryptocurrency among both mainstream users and money launderers. Most regulated exchanges and services, as well as illegal operations, accept Bitcoin. It is highly liquid as the world's largest token, can be split into smaller transactions similar to regular banking and it operates 24/7. From the time of its creation in 2009 to 2017, it was estimated that $76 billion in illicit flows had moved through Bitcoin.[94] However, after the addition of other major cryptocurrencies and specific privacy-tailored coins and stablecoins, the volume of illicit flows has dropped significantly.

The key reason for this decline is the traceability of Bitcoin. Every Bitcoin transaction exposes the input and output addresses, exact amounts and timings, and transaction graph structures. This allows chain analytics vendors to cluster transactions, which de-anonymises the wallets and makes transactions easier to track. This in turn pushes launderers, whose main mission is to stay anonymous, off this token. In addition, most exchanges that deal with Bitcoin have implemented strong KYC.

However, notwithstanding these concerns, Bitcoin retains its position as the largest cryptocurrency market and continues to record the highest daily transaction volume. This means that most illicit funds are received on-chain from hacks, scams and other criminal enterprises in Bitcoin. Thus, the laundering stage often involves Bitcoin.

Ether (ETH) is the native cryptocurrency of the Ethereum network. It went live in 2015 and has since had a large increase in volume. It is the second largest cryptocurrency by volume and market cap. It is also used to facilitate DeFi platforms, DEXs and bridges. ETH shares some characteristics with BTC, including traceability, pseudonymity and high liquidity. However, it has some differences. Ethereum uses an account-based model: each address has a running balance and transactions simply change balances. ETH's smart-contract features open up many more types of behaviour for laundering, as discussed in the previous section.

There are hundreds of other regular cryptocurrency tokens and most don't have the liquidity or growth to support laundering.

Privacy Coins

Within the thousands of tokens available, a distinct sub-section caters specifically to privacy which makes chain analytics harder. They are designed to obscure transaction details and

[94] Sean Foley, Jonathan R Karlsen and Tālis J Putniņš, "Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies?", *The Review of Financial Studies* (32, 5, May 2019), 1798–1853.

user identities through advanced cryptographic techniques. Privacy coins employ several sophisticated cryptographic mechanisms to achieve anonymity. The most widely adopted approaches include: 1) Ring signatures and stealth addresses and 2) Zero-knowledge proofs.

1) Ring signatures and stealth addresses work by mixing a user's transaction with others on the blockchain, making it impossible to determine the true sender. Stealth addresses generate a unique, one-time address for each transaction, hiding the legitimate recipient. When combined with RingCT (Ring Confidential Transactions), which conceals transaction amounts, the result is that sender, receiver and amount are all obscured from public view.

2) Zero-knowledge proofs is an alternative approach used by some privacy coins, like Z-Cash. They allow users to cryptographically prove a transaction is valid without revealing the amounts or parties involved. Notably, Z-Cash offers optional privacy – users can choose between transparent and shielded transactions, depending on their preferences.

The most prominent privacy coin is Monero. It has been linked to use by major terrorist organisations, ransomware operations and DNMs. According to TRM research, the proportion of newly launched Monero-only darknet marketplaces increased from a third in 2023 to nearly half in 2024. [95] It has a series of features, including stealth addresses and RingCT, which makes tracking it close to impossible.

Stablecoins

Stablecoins have emerged as the dominant cryptocurrency for illicit finance, fundamentally reshaping the money laundering landscape. Once overshadowed by Bitcoin in illicit use, dollar-pegged digital tokens now represent 63% of all illicit cryptocurrency transactions, reflecting a substantial shift in how criminals move and conceal their proceeds. [96]

The appeal of stablecoins to criminal enterprises is largely driven by a single defining feature. Their dollar peg eliminates the volatility risk associated with Bitcoin and Ethereum, ensuring that illicit proceeds maintain stable value during complex laundering operations.

This report has identified five different stablecoins which have seen use by launderers: USDT, USDC, BUSD, DAI and A7A5.

USDT (Tether) is the undisputed market leader, accounting for approximately 60% of all stablecoin supply with a market capitalisation exceeding $176 billion as of October 2025. [97] Issued by Tether, USDT was launched in 2014 as the first major stablecoin. It benefits from early-mover advantages that remain unmatched.

Being the market leader has also meant that it has emerged as the main choice for criminals, with $19.3 billion in illicit transactions being through Tether in 2023, representing 1.63% of its total transaction volume, according to TRM research. [98]

In addition to regular stablecoins, there has been a growth in stablecoins primarily used for laundering. For example, A7A5 is a ruble-pegged stablecoin launched in Kyrgyzstan in

[95] "2025 Crypto Crime Report", *TRM*, 10 February 2025, https://www.trmlabs.com/reports-and-whitepapers/2025-crypto-crime-report.

[96] "2025 Crypto Crime Trends: Illicit Volumes Portend Record Year as On-Chain Crime Becomes Increasingly Diverse and Professionalized", *Chainalysis*, 15 January 2025, https://www.chainalysis.com/blog/2025-crypto-crime-report-introduction/.

[97] "How stablecoins reached a $300 billion market cap in 2025", *ARKM*, 8 October 2025, https://info.arkm.com/research/how-stablecoins-reached-a-300-billion-market-cap-in-2025.

[98] "The Illicit Crypto Economy 2023", *TRM*, 27 March 2024, www.trmlabs.com/reports-and-whitepapers/the-illicit-crypto-economy-2023.

January 2025. It has become a critical tool for Russian sanctions evasion, money laundering and illicit cross-border payments.

Officially issued by Old Vector LLC, a Kyrgyzstan-registered company, and backed by deposits at Russia's sanctioned state-owned Promsvyazbank (PSB), A7A5 has been reported to have processed tens of billions of dollars in transactions and facilitated financial flows for ransomware operations, darknet markets and Russian businesses circumventing Western sanctions. [99]

The token was created by A7 LLC, a cross-border payment service that is 51%-owned by a convicted Moldovan fraudster Ilan Shor and 49%-owned by PSB. Shor, who fled Moldova for Russia after being convicted in 2017 of orchestrating a $1 billion bank fraud, has claimed that the broader A7 network facilitated over $86 billion in transactions in less than a year of operation. Elliptic estimates that A7A5 transfers exceeded $1 billion per day by July 2025. [100] A7 and Old Vector have been sanctioned by the US, UK and EU.

The table below shows the most prominent cryptocurrencies used for money laundering. It summarises the key characteristics of 15 cryptocurrencies and stablecoins, including the illicit use prevalence, native privacy features, delisting and traceability.

Table 6: Features of major cryptocurrencies and stablecoins

Asset	Traceable High/Medium/Low	Native Privacy Features None/Optional/Default	On Tier-1 KYC Exchanges Widely/Limited/No	Delisting due to AML Yes/No	How Concentrated Control is? High/Medium	Illicit use Prevalence High/Medium/Low	**Legal Designation** **Clear/Contested**	Market cap Top-10 / Mid-cap / Small-cap	Smart contract support? Yes/No
BTC	High	None	Widely	No	Medium	Medium	Clear	Top-10	No
ETH	High	None	Widely	No	Medium	Medium	Contested	Top-10	Yes
BNB	High	Optional	Widely	No	High	Low	Clear	Top-10	Yes
XRP	High	Optional	Widely	No	High	Medium	Contested	Top-10	Yes
LTC	High	Optional	Widely	Yes	Medium	Medium	Clear	Mid-Cap	No
SOL	High	Optional	Widely	No	Medium	Medium	Contested	Top-10	Yes
SOL	High	None	Widely	No	High	Medium	Clear	Top-10	No
XMR	Low	Default	Limited	Yes	Medium	High	Clear	Mid-Cap	No
ZEC	Medium	Optional	Widely	Yes	Medium	Medium	Clear	Mid-Cap	No
DASH	High	Optional	Widely	Yes	Medium	Medium	Contested	Mid-Cap	No
XVG	Medium	Optional	Limited	Yes	Medium	Medium	Contested	Small-Cap	No
USDT	High	None	Widely	Yes	High	High	Clear	Top-10	Yes
USDC	High	None	Widely	No	High	Low	Contested	Top-10	Yes
DAI	High	None	Widely	Yes	High	Medium	Contested	Mid-Cap	Yes
A7A5	High	None	No	No	High	High	Clear	Mid-Cap	Yes

The three most widely used instruments are: Monero (XMR), USDT (Tether) and A7A5. Monero, Z-Cash (ZEC) and Verge (XVG) exhibit the lowest levels of traceability. This means that laundered assets which pass through these coins have the highest chance of being untracked. Therefore, launderers rely heavily on them.

USDT, USDC and BNB have specific characteristics that enable the issuer to seize, freeze or blacklist addresses. The USDT contracts include blacklist and confiscation functions. When Tether blacklists an address, the USDT can no longer move. Tether can also reset balances and effectively destroy or reclaim them. USDC contracts have functions such as blacklist(address) and wipeFrozenAddress(address). Circle, operator of USDC, can freeze addresses and even wipe and reassign funds. The BNB chain itself has code that can block specific wallets at the protocol level, so those wallets can't move their BNB, or other assets on that chain, if they're blacklisted.

Several currencies in the table have faced delisting: LTC, XMR, ZEC, DASH, XVG, USDT and DAI. Often this is due to money laundering violations or regulatory concerns.

[99] "The rise of A7A5: the Ruble stablecoin now transfers $1 billion per day", *Elliptic*, 28 July 2025, www.elliptic.co/blog/the-rise-of-a7a5-the-ruble-stablecoin-now-transfers-1-billion-per-day.

[100] Ibid.; Elise Thomas, "To Evade Sanctions, the Kremlin Turns to a Convicted Money Launderer", *Lawfare*, 18 November 2025, www.lawfaremedia.org/article/to-evade-sanctions--the-kremlin-turns-to-a-convicted-money-launderer.

Each cryptocurrency instrument can present a different challenge for authorities. Many criminals do not deliberately choose from the available options; instead, they use whatever means are easiest to convert stolen or otherwise illicitly obtained funds.

To conclude, the laundering of illicit funds by criminals is growing substantially. From the point at which funds are misappropriated by illicit actors, they are routed through a series of complex transactions intended to stay ahead of investigators and prosecutors, creating a persistent cat-and-mouse dynamic between criminals and law enforcement.

10. Integration and Off-Ramps

Integration is the final stage of a money-laundering cycle where illicit funds, having already passed through placement and layering, are reintroduced into the legitimate economy in a way that appears clean. In crypto, integration occurs after funds have moved through obfuscation tools such as mixers, cross-chain bridges, privacy coins or complex transaction patterns. At this stage, the on-chain history has been sufficiently obscured (in the criminals' view) that the assets can be used for seemingly legitimate purposes and won't get flagged. Most criminals want to eventually turn the illicit cryptocurrency into cash which is where off-ramps come into play.

Off-ramps in crypto refer to the mechanisms and services that allow users to convert crypto assets into fiat currency or other real-world value, thereby exiting the purely digital environment. Off-ramps are critical control points because they often represent the first or last interface between the pseudonymous blockchain world and the fully identified, regulated financial system.

If an off-ramp's controls are weak, criminals can transform seemingly 'clean' crypto into usable fiat with minimal friction. For compliant institutions, however, off-ramps are where robust KYC, transaction monitoring and blockchain analytics and screening must be concentrated. Understanding how integration operates in crypto, and how off-ramps are used and potentially exploited, is central to investigating effective AML frameworks, conducting risk assessments and formulating regulatory responses in the digital asset ecosystem.

This report has identified two types of off-ramps:

1) Centralised Exchanges and OTC Brokers;
2) Digital Currency Payment Platforms.

Table 7: Categories of off-ramps from the Global Cryptocurrency Laundering Database

	Centralised Exchanges & OTCs	Digital Currency Payment Platforms	Total
Number	14	5	19
Illicit Assets	14,745	9,865	24,610
Legal Action	14	5	19
Convictions	6	1	7
Assets Seized	415	69	484

1) Centralised Exchanges and OTC Brokers

Centralised exchanges (CEXs) are platforms, such as Binance or Coinbase, where a company sits in the middle and runs the trading system, holds user deposits and matches buy and sell orders. A user typically deposits fiat or crypto, trades through their interface and withdraws funds when they are done.

OTC (over-the-counter) brokers handle large trades directly between buyers and sellers, instead of pushing those orders through a public order book. OTC is mainly used by funds and high-net-worth individuals who want to move sizable amounts of assets without causing big price swings or revealing their intentions to the market.

CEXs are a common integration point because they sit between crypto and the banking system. After dirty funds have been shuffled around on-chain, they're often sent to CEX

accounts, then run through a bit of trading, to look like normal activity. Then they are transferred to bank accounts as alleged 'investment gains'. If the exchange has weak AML controls or operates in a lightly regulated jurisdiction, it becomes an easy channel for turning laundered crypto into clean fiat.

OTC brokers play a similar role but are tailored for large, discreet deals. Instead of using a public order book, a launderer can go to an OTC desk, sell a big block of crypto in one shot and receive fiat (or cleaner crypto like stablecoins) without drawing much attention or moving the market. The broker might then use its own exchange and banking relationships to settle the trade.

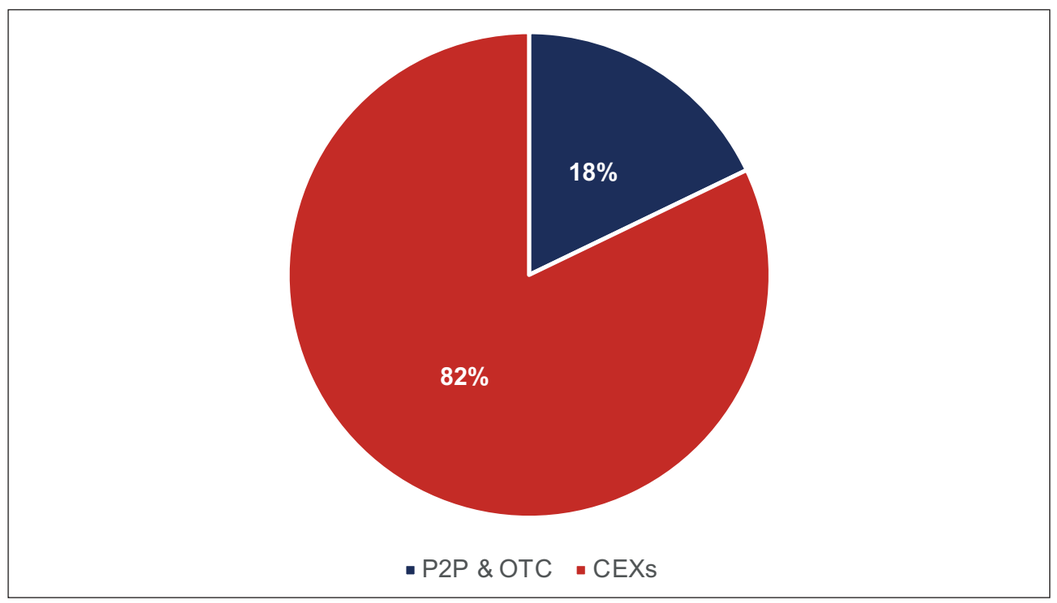
From the outside, those flows can look like ordinary institutional activity, which is exactly what makes both CEXs and OTC desks attractive for the integration stage, when controls are weak. According to estimates by Chainalysis, over 50% of illicit cryptocurrency ends up at centralised exchanges. [101]

A peer-to-peer exchange is similar to this. It lets people transact directly with each other instead of having to agree prices with a broker. Most often, this means a peer-to-peer (P2P) trading marketplace where a buyer and seller agree on a price and payment method, while the platform may provide escrow to hold the crypto until payment is confirmed.

This report has identified the 14 largest and most prolific exchanges and OTCs that are either high-risk or illegal. They have processed an estimated total of at least $14.7 billion in just illicit volume, although the true number could be much higher. This sector has fuelled extreme sanctions evasion, cross-border drug trade and fraud.

The graph below shows the percentage of illicit cryptocurrency, split between the full-service CEXs compared to the P2P and OTC services.

Figure 24: Composition of illicit inflows (% of total illicit inflows)

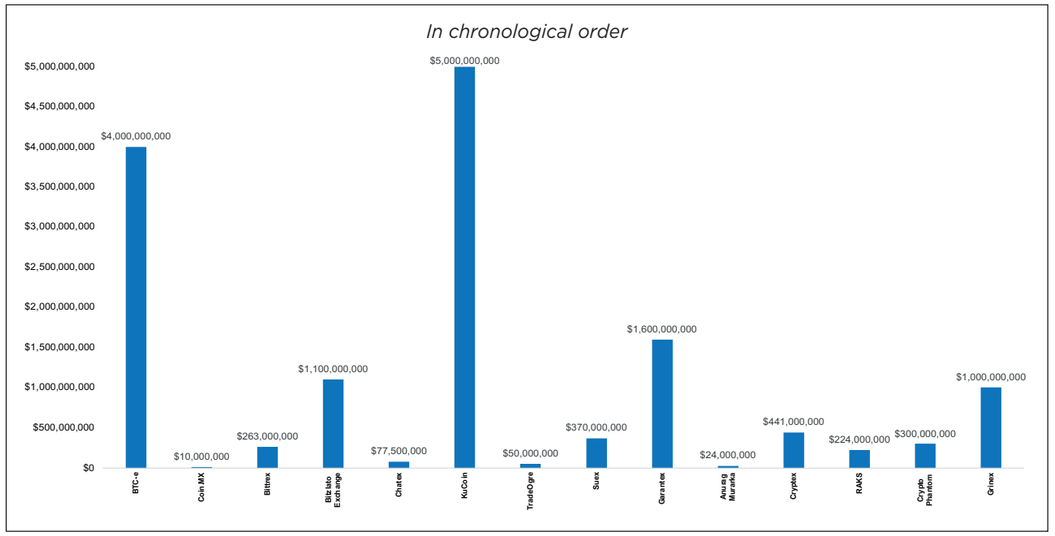


[101] "Money Laundering Activity Spread Across More Service Deposit Addresses in 2023, Plus New Tactics from Lazarus Group", *Chainalysis*, 15 February 2024, https://www.chainalysis.com/blog/2024-crypto-money-laundering/.

Centralised exchanges account for over four-fifths of illicit inflows. This is because large CEXs handle huge daily volumes in their order books. If a launderer is holding sizable proceeds, they would want to swap into clean assets quickly and without moving the market. In addition, many CEXs allow weak KYC information and can onboard users online in minutes, with hundreds of thousands to millions of accounts globally. In contrast, OTCs often require direct human interaction, either online or in person. This can limit the scale and creates higher risks for launderers.

The graph below shows a service-by-service breakdown of illicit inflows into the different exchanges.

Figure 25: Illicit inflows by service (USD)



There has been an average volume of $1 billion of illicit flows into these services over the last 14 years. These inflows could originate from sanctioned individuals, terrorism or criminal activity.

The largest CEX was KuCoin, a large crypto exchange based in the Seychelles which allowed users to trade a large variety of cryptocurrency. From the start of its operation in 2017 until 2023, it operated with no identity checks meaning anyone could register and transfer money. Two of its founders pleaded guilty in the US to processing over $5 billion in illicit and criminal flows. [102]

The largest OTC service was Suex. It was legally registered in the Czech Republic but was described by multiple sources as Russia-based, operating through branch offices in Moscow and St Petersburg. According to the US Treasury Department, Suex handled illicit proceeds from at least eight ransomware variants, and over 40% of its known transaction history was associated with illicit actors. [103]

Half of the illicit exchanges and OTC brokers conducted the majority of their operations from Russia. This concentration highlights the prominent role that high-risk, Russia-based

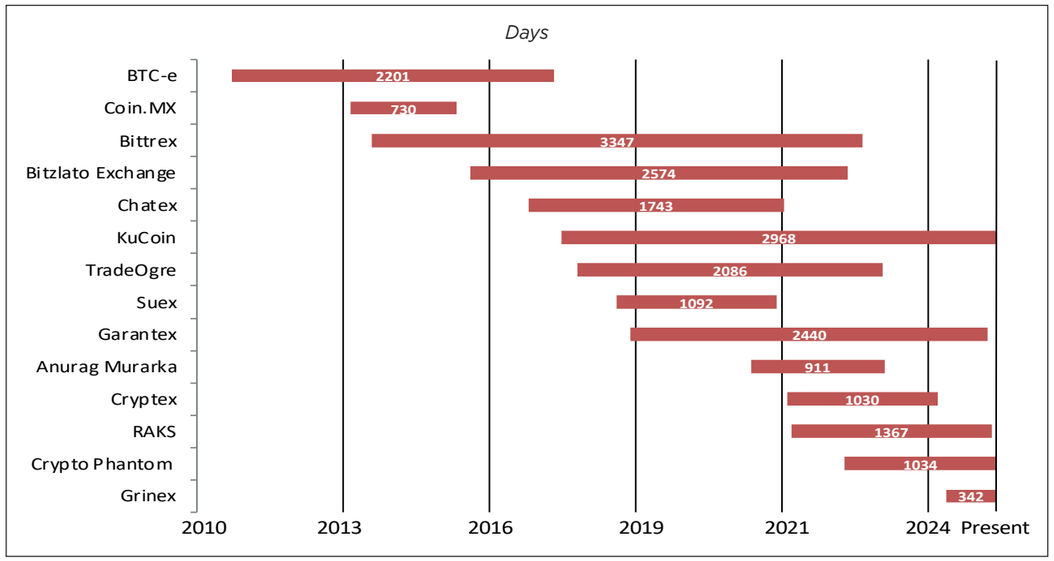
[102] "Prominent Global Cryptocurrency Exchange KuCoin And Two Of Its Founders Criminally Charged With Bank Secrecy Act And Unlicensed Money Transmission Offenses", U.S. Attorney's Office, 26 March 2024, https://www.justice.gov/usao-sdny/pr/prominent-global-cryptocurrency-exchange-kucoin-and-two-its-founders-criminally.

[103] "Treasury Takes Robust Actions to Counter Ransomware", U.S. Department of the Treasury, 21 September 2021, https://home.treasury.gov/news/press-releases/jy0364.

exchanges and OTC brokers play in facilitating sanctions evasion, underscoring both the jurisdictional exposure and the heightened compliance risk associated with counterparties operating from or through this region. In addition, non-Russia-based services have also played a large part in sanctions evasion. For example, Bittrex, based in the USA, conducted over 116,000 transactions with sanctioned jurisdictions, including Iran, Cuba, Sudan and Syria, without filing SARs or having an adequate AML program. [104]

The graph below shows the length of time that each service has been operational, including both exchanges and OTC brokers.

Figure 26: Timeline of exchange and OTC operations



The average lifespan of a high-risk service is four years and nine months. As operations ramp up and word of mouth spreads about the exchange, the exchanges and OTCs begin receiving a larger amount of inflows which draws regulatory and investigative scrutiny. At the peak, in 2022, there were eight high-risk services operating at the same time. This gives bad actors many different options for cash outs.

All 14 services have been subject to some form of legal action. Due to jurisdictional constraints, many cases have resulted primarily in sanctions and asset seizures rather than criminal charges or convictions. Formal charges were brought against seven services, and six cases resulted in convictions. While three services continue to operate, only KuCoin has remedied the identified money-laundering concerns and subsequently attained regulatory compliance. In total, $415 million has been recovered from these 14 companies through fines and seizures.

Many regulated exchanges have been responsible for allowing large amounts of illicit funds to move through the ecosystem. For example, Binance settled with OFAC for $968 million in relation to 1,667,153 apparent sanctions violations. [105] It had operated with limited KYC protocols

[104] "FinCEN Announces $29 Million Enforcement Action Against Virtual Asset Service Provider Bittrex for Willful Violations of the Bank Secrecy Act", Financial Crimes Enforcement Network, 11 October 2022, https://www.fincen.gov/news/news-releases/fincen-announces-29-million-enforcement-action-against-virtual-asset-service.

[105] "OFAC Settles with Binance Holdings, Ltd. for $968,618,825 Related to Apparent Violations of Multiple Sanctions Programs", Department of the Treasury, 21 November 2023, https://ofac.treasury.gov/system/files/2023-11/20231121_binance.pdf.

and didn't file SARs. As one of the compliance officers at Binance wrote: "we need a banner 'is washing drug money too hard these days - come to binance we got cake for you.'" *[sic]* [106]

As CEXs have strengthened KYC requirements and AML regulations, underground OTC and P2P operations have been growing rapidly. In addition, in-person operations have begun to pop up in different locations across the globe to cater to sanctioned individuals. [107]

2) Digital Currency Payment Platforms

Digital currency payment platforms are the services that turn crypto into something that looks and behaves like normal money. These platforms let criminals park the funds in accounts that resemble legitimate e-money or business balances. Because payments from these platforms look like ordinary commercial activity, they help dirty funds blend into the real economy.

Those same platforms often act as off-ramps from the crypto world into fiat and real-world value. They cash out or repurpose crypto by sending bank wires, issuing prepaid cards or vouchers or routing funds to merchants. Every time they convert crypto into everyday financial flows, they are effectively providing the bridge from anonymised crypto balances to apparently clean, usable money.

This report has identified five major payment platforms which are a concern for money laundering, with a conservative total of $9.9 billion of illicit flows having passed through these services. The five platforms are discussed below.

a) Liberty Reserve

The first was Liberty Reserve, a Costa Rica-based centralised digital currency service. Launched in the mid-2000s, it let users send and receive 'Liberty Reserve Dollars/ Euros' with just a name, email address and birth date. It used independent 'exchangers' for deposits and withdrawals and kept transfers instant. At its peak, it had over 5 million users before being shut down by US authorities in 2013 under the Patriot Act. [108]

The services of Liberty Reserve made it hugely attractive to criminals. US prosecutors said it functioned as a "black market bank" and "financial hub of the cyber-crime world", [109] processing around 55 million transactions and processed an estimated $6 billion tied to credit-card fraud, identity theft, hacking, child sexual-abuse material, narcotics trafficking and other crimes. Its founder, Arthur Budovsky, pleaded guilty to money-laundering in 2016 and was sentenced to 20 years in prison in the United States for running the scheme. [110]

b) Cryptonator

The second was Cryptonator, a web-based multi-currency crypto wallet and exchange launched around 2014. It was marketed as an 'all-in-one' online wallet that let users store various cryptocurrencies, send and receive funds, and instantly swap between

[106] "Binance and CEO Plead Guilty to Federal Charges in $4B Resolution", U.S. Department of Justice, 21 November 2023, https://www.justice.gov/archives/opa/pr/binance-and-ceo-plead-guilty-federal-charges-4b-resolution.

[107] "From Dubai to Toronto, inside the crypto-to-cash storefronts fueling money laundering's new frontier", *ICIJ*, 17 November 2025, https://www.icij.org/investigations/coin-laundry/crypto-cash-desk-currency-exchange-money-laundering/.

[108] Ibid.

[109] "Prepared Remarks of U.S. Attorney Preet Bharara", U.S. Attorney, May 28, 2013 https://www.justice.gov/sites/default/files/usao-sdny/legacy/2013/05/30/remarks.pdf.

[110] "Founder of Liberty Reserve Pleads Guilty to Laundering More Than $250 Million through His Digital Currency Business", Office of Public Affairs, 29 January 2016, https://www.justice.gov/archives/opa/pr/founder-liberty-reserve-pleads-guilty-laundering-more-250-million-through-his-digital; "Numerous BSA Records Aid in Liberty Reserve", May 2015 Investigation, https://www.fincen.gov/system/files/shared/May2015_Case4.pdf.

coins inside a single personal account, effectively acting as a small personal exchange for each user. It was operated by Russian national Roman Pikulev, also known as Roman Boss, and ran until about March 2023, when authorities say it had already processed hundreds of millions of dollars' worth of cryptocurrency.

According to US and German law-enforcement agencies, Cryptonator failed to implement basic AML and KYC controls and became a hub for illicit activity. Investigators alleged it was heavily used by ransomware gangs, darknet marketplaces and other cybercriminals to move and cash out stolen or extorted crypto, with the platform ultimately processing more than $235 million in illicit funds between 2014 and 2023. In 2024, US and German authorities seized the Cryptonator domain and indicted Pikulev for money laundering and running an unlicensed money-services business. [111]

c) Huione Pay

The third, Huione Pay, is the digital payments arm of Cambodia's Huione Group. It was set up as a payment services institution that let users hold and move money via a mobile wallet, do currency exchange and send funds in both fiat and crypto. It operated branches across Cambodia and, until 2025, held a license from the National Bank of Cambodia, positioning itself as a kind of all-purpose e-wallet and cross-border payments platform within the group's broader ecosystem of services. [112]

It effectively ended operations as a licensed payment institution in March 2025, when the National Bank of Cambodia revoked its payment-services/banking licence for regulatory non-compliance. The situation escalated internationally on 1 May 2025 when the US Treasury's Financial Crimes Enforcement Network (FinCEN) formally identified Huione Group (including Huione Pay) as a "financial institution of primary money laundering concern" under Section 311 of the Patriot Act and proposed cutting it off from the US financial system. [113] That proposal was finalised in October 2025.

d) Evita Pay

The fourth service was Evita Pay, a US-based cryptocurrency payments and money-transmission company, incorporated in Florida. Its founder, Russian national Iurii Gugnin, marketed Evita as a cross-border payments service. Foreign clients (often with funds at Russian banks) would send cryptocurrency, mainly Tether, and Evita would convert it to US dollars or other fiat via US bank accounts and crypto exchanges, then make payments on their behalf. Gugnin registered Evita Pay as a money transmitter with FinCEN and the State of Florida, telling banks and regulators that the firm had robust KYC/AML controls, even though prosecutors say those controls were largely ignored in practice. [114]

According to a June 2025 US Justice Department indictment, between June 2023 and January 2025, Evita was used to move about $530 million through the US financial system, much of it on behalf of sanctioned Russian banks and companies, and to pay for export-controlled US technology and goods tied to Russia's state nuclear firm Rosatom. Gugnin

111 "United States of America v. Roman Boss", United States District Court, 9 March 2023, https://www.documentcloud.org/documents/25029923-cryptonator-complaint/.

112 Jack Adamović Davies, "Exclusive: World's 'largest online black market' loses banking license", *Radio Free Asia*, 6 March 2025, https://www.rfa.org/english/cambodia/2025/03/06/huione-cambodia-cyberscam-cryptocurrency/.

113 "FinCEN Finds Cambodia-Based Huione Group to be of Primary Money Laundering Concern, Proposes a Rule to Combat Cyber Scams and Heists", FinCEN, 1 May 2025, https://www.fincen.gov/news/news-releases/fincen-finds-cambodia-based-huione-group-be-primary-money-laundering-concern.

114 Alena Koroleva, "Feds: Russian Laundered Half a Billion Through Manhattan Crypto Firms", OCCRP, 11 June 2025, https://www.occrp.org/en/news/feds-russian-laundered-half-a-billion-through-manhattan-crypto-firms.

faced 22 federal counts, including wire and bank fraud, sanctions and export-control violations, operating an unlicensed money-transmitting business, failing to implement an effective AML program, failing to file suspicious-activity reports and money laundering. He was arrested in New York when the indictment was unsealed and faces trial. [115]

e) Exved

Finally, Exved is a Russian cross-border payments platform launched on 7 December 2023. It was founded by Russian crypto entrepreneur Sergey Mendeleev, who also co-founded the OFAC-sanctioned exchange Garantex. According to analysis firm Elliptic, Exved is marketed to Russian importers and exporters "under sanctions pressure", letting them settle trade using USDT, rubles and US dollars, often via links with Mendeleev's InDeFi (InDeFi Bank) project. [116]

The service presents itself as a compliant payments solution and claims to process cross-border flows, totalling tens of billions of rubles per month. Officials and investigators say Exved is not just a neutral payment rail but part of a sanctions-evasion and laundering ecosystem built around Garantex. On 14 August 2025, OFAC sanctioned Exved alongside Garantex's other successors, describing it as a payment platform working with InDeFi Bank to facilitate crypto-mediated trade between Russia and other countries, in ways that help skirt Western financial sanctions. [117]

These five cases provide insight into a different area of laundering tactics which focuses more on using services which are similar to banks to move cryptocurrency. As more sanctioned individuals try to move their cryptocurrency, the level of demand for these services only increases. To conclude, in the final stage of laundering, illicit actors typically pursue the path of least resistance to make sure their illicit funds remain secure.

115 "Founder of Cryptocurrency Payment Company Charged with Evading Sanctions and Export Controls, Defrauding Financial Institutions, and Violating the Bank Secrecy Act", Office of Public Affairs, 9 June 2025, https://www.justice.gov/opa/pr/founder-cryptocurrency-payment-company-charged-evading-sanctions-and-export-controls.

116 "OFAC targets use of stablecoins for Russian sanctions evasion", *Elliptic*, 14 August 2025, https://www.elliptic.co/blog/ofac-targets-use-of-stablecoins-for-russian-sanctions-evasion.

117 "Treasury Sanctions Cryptocurrency Exchange and Network Enabling Sanctions Evasion and Cyber Criminals", U.S. Department of the Treasury, 14 August 2025, https://home.treasury.gov/news/press-releases/sb0225.

11. Regulation and Legislation

This report has analysed 164 different cases which have involved cryptocurrency money laundering and illicit proceeds. Among the 110 cases in which legal action was pursued, enforcement efforts have yielded both successful and unsuccessful outcomes. Government actions have included sanctions, court forfeitures, fines and criminal charges. Fifty-four cases have not faced any form of legal action. This underscores persistent gaps in enforcement and highlights opportunities to expand prosecution.

This report discusses the legal action in four parts:

1) Direct Legal Action
2) International Frameworks
3) Public–Private Partnerships
4) Confronting Sanctions Evasion in Crypto

1) Direct Legal Action

Direct legal actions undertaken by governments around the world have included a combination of criminal prosecution, civil action, imposition of sanctions and asset seizures. The table below provides an overview of the type of legal actions executed in relation to the 164 cases included in the Global Cryptocurrency Laundering Database.

Table 8: Legal action overview

	No. of Cases	Total	%
Criminal Charges	70	164	43%
Convictions	35	164	21%
Civil Action	65	164	40%
Sanctions	21	164	13%
Assets Seized ($ Billion)	92	342	27%

Criminal charges have been brought in 43% of the cases, with convictions obtained in 21% of the cases. Civil actions, including civil forfeiture, have been undertaken in 40% of the cases. In 13% of cases, governments imposed sanctions on operators or services.

This report identifies $92 billion in funds recovered through legal action, either seized from illicit services or recovered following illicit thefts. This represents 27% of the total illicit funds processed in these cases. Many seized assets lack a clear link to direct victims (e.g., funds seized from exchanges). This means that the recovered funds may be retained by the government and deployed to support socially beneficial programs. For instance, the United States recently established a Strategic Bitcoin Reserve that holds forfeited Bitcoin, which may be used to support public objectives.

Across different categories of on-ramp cases, legal actions, which include both civil and criminal proceedings, have been pursued only in 58% of cases (75 out of 130 cases), and convictions have been achieved in 22% of those cases (29 out of 130 cases).

Within these cases, significantly, legal actions have been undertaken in 100% of cases in relation to Ponzi schemes (19 out of 19), ATMs (5 out of 5) and criminal enterprises (5 out of 5). For Ponzi schemes, 58% of cases have resulted in convictions. For ATMs, 100% of cases have resulted in convictions. For criminal enterprises, zero cases have resulted in convictions.

In relation to DNMs, legal actions have been brought in 75% of cases, with convictions obtained in 33% of those cases. For ransomware, legal actions have been brought in 64% of cases, and convictions have been issued in 20% of those cases.

For hacks, the percentage of legal action has been the lowest, at 32%, and the percentage of convictions of the total number of hacking cases has been only 9%. This is the lowest ratio after criminal enterprises.

The most significant area of law enforcement success has been in relation to Ponzi schemes. Given that these schemes can affect hundreds of thousands to millions of victims, governments are often compelled to intervene and seek redress for the harm inflicted upon them.

The least successful area of law enforcement action has been hacking. There has been the fewest number of legal actions brought in response to them among all identified cases. Often, it is very hard to detect who perpetrated the hacks, and bad actors are able to launder the funds quickly, meaning enforcement action is obstructed.

The assets seized in all on-ramp cases totalled over $90 billion, or 30.3% of total assets moved through those channels in present value ($307 billion).

In relation to off-ramps, legal action was brought in 100% of these cases (19 out of 19) and convictions have been obtained in 63% of those cases. However, the amount of assets seized ($484 million) is dramatically low compared to the assets processed through these services ($24.6 billion), and amounts to a mere 2%.

Case Study: Wormhole Hack

An example of the successful legal recovery of funds was achieved in connection with the Wormhole hack. The legal action took impressive steps which involved cross-border international cooperation.

On 2 February 2022, an unknown attacker exploited a bug in the Wormhole bridge and fraudulently minted 120,000 ETH, worth about $325 million. The hacker later used a large chunk of the stolen ETH for Oasis.app, a DeFi front-end for Maker, depositing them into Oasis ‘vaults’ and using them as collateral to borrow other assets.

White-hat researchers discovered that Oasis’s smart-contract architecture still allowed the Oasis team to upgrade contracts and seize certain assets interacting with the app, which basically acted as a backdoor. [118]

TMSL, the company overseeing Wormhole, went to the High Court of England and Wales. It sued “persons unknown” (the hacker) and Oazo Apps Ltd (the UK company behind Oasis) and applied for an urgent proprietary injunction and related relief against Oazo as a “non-cause-of-action defendant”, meaning they control the infrastructure than can reach their property so the court can order them to help. [119]

[118] “$325 Million Stolen from Wormhole DeFi Service”, *Elliptic*, 3 February 2022, https://www.elliptic.co/blog/325-million-stolen-from-wormhole-defi-service.

[119] “US$400m+ proceeds of a highly-publicised crypto hack successfully recovered through the English courts”, *Fountain Court*, 28 November 2024, https://fountaincourt.uk/2024/11/us400m-proceeds-of-a-highly-publicised-crypto-hack-successfully-recovered-through-the-english-courts/.

On 21 February 2023, the High Court granted an order requiring Oasis to "take all necessary steps" to recover assets linked to the Wormhole hacker's wallet, including modifying its app and exploiting its own admin powers to seize the crypto. In response to the High Court order, Oasis upgraded its contracts to take control of the hacker's Oasis vault positions and seized the assets from the hacker's wallet. The seized crypto was sent to a wallet controlled by a court-authorised third party.

TMSL then filed a lawsuit in the US, Tai Mo Shan Limited v. John Doe Nos. 1–100, claiming that the unknown defendants hacked Wormhole and stole $320 million of tokens, and that TMSL had replenished the protocol and should now be treated as owner of the stolen assets. [120] Because the hackers were anonymous, the court allowed service via NFTs. TMSL sent NFTs, embedding links to court documents to the hacker's known wallet addresses. On 26 March 2024, when the hackers didn't appear in court, the New York court entered a default judgment in TMSL's favour, declaring that TMSL had proprietary rights to the seized assets. [121]

TMSL then asked the High Court to recognise and enforce the New York judgment in rem so the seized assets in England-controlled wallets could be legally transferred to TMSL. In mid-2024, the English court recognised and enforced the New York judgment and ordered that all recovered tokens be transferred to TMSL. The final transfers were completed on 19 July 2024. By then, the tokens were worth over $400 million. [122]

This case displays the ability for direct recovery and seizure of stolen or criminal assets. In addition, it provides evidence that legal action can directly force secondary platforms to assist in action.

Case Study: LockBit [123]

LockBit's takedown was the culmination of multi-year criminal proceedings that began well before the headline operation. In France, the Paris Public Prosecutor's cybercrime section opened an investigation in 2020, and framed the case around organised extortion and organised offences, involving unauthorised access to, interference with and obstruction of automated data processing systems.

International judicial cooperation was vital, including repeated coordination meetings at Eurojust and the creation of a dedicated task force inside Europol that was initiated to align cross-border legal steps and evidence handling. This enabled the coordinated enforcement week starting in February 2024, referred to as Operation Cronos. Authorities from 10 countries acted in parallel, with Eurojust and Europol supporting the coordination. There was a takedown of 34 servers across multiple jurisdictions, alongside arrests in Poland and Ukraine.

French authorities also seized additional servers in Germany and the Netherlands and took control of LockBit's 'wall of shame' leak site on the darknet, while the wider operation included the freezing of more than 200 cryptocurrency accounts linked to the group.

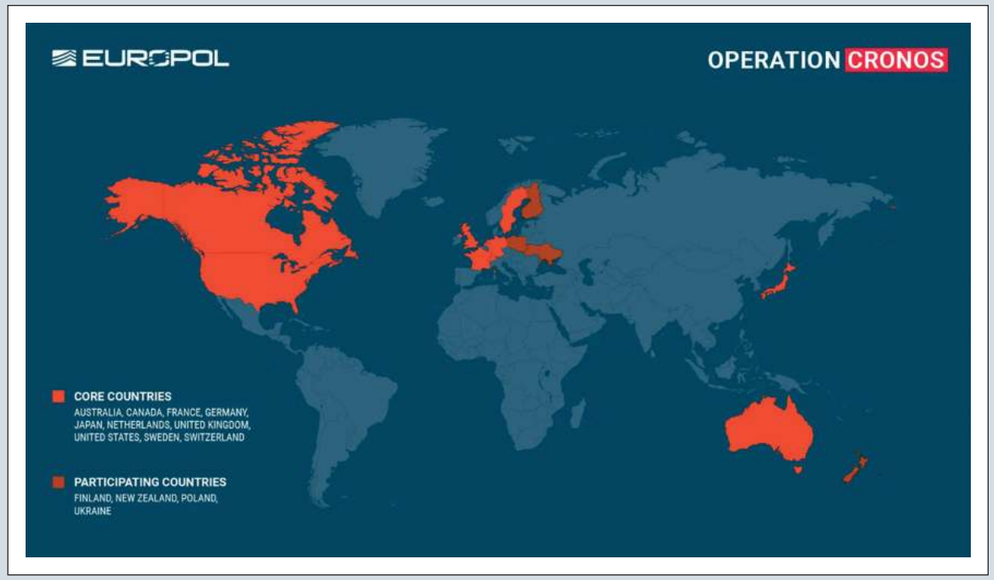
120 "Syedur Rahman, 'Crypto-related crime – taking a cross-border, multi-court approach", *Rahman Ravelli*, 18 November 2024, https://www.rahmanravelli.co.uk/expertise/cryptocurrency/articles/crypto-related-crime-taking-a-cross-border-multi-court-approach/.

121 Ibid.

122 Ibid.

123 "Law enforcement disrupt world's biggest ransomware operation", Europol, 20 February 2024, https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation/.

Figure 27: Map showing countries participating in the takedown [124]



On 20 February 2024, the UK National Crime Agency, working with the Department of Justice (DOJ) and FBI in the US, seized public-facing websites used to connect victims and affiliates to LockBit's infrastructure and took control of administrator servers to prevent further extortion activity.

The DOJ also unsealed two search warrants issued in the District of New Jersey that authorised the FBI to disrupt multiple US-based servers used by LockBit members, including servers hosting the 'StealBit' platform used to organise and transfer stolen victim data. The DOJ also unsealed an indictment against two alleged affiliates.

After the February 2024 action, authorities emphasised that the legal seizures created downstream leverage for victim support. The DOJ stated that decryption capabilities and keys recovered from seized infrastructure could help hundreds of victims.

In May 2024, the United States publicly identified and sanctioned Dmitry Khoroshev as a senior LockBit leader, while DOJ unsealed charges alleging he acted as developer and administrator, and the United Kingdom and Australia announced parallel sanctions measures.

Case Study: Anurag Murarka Network [125, 126]

Anurag Pramod Murarka ran an international crypto-to-cash money-laundering operation (often advertised on DNMs) in which customers contacted him via encrypted messages, agreed an exchange rate and sent cryptocurrency to addresses he controlled. Murarka then used a pre-arranged hawala pipeline out of India to move value into cash, relying

124 Ibid.

125 "International Crypto Vendor Sentenced for Money Laundering Conspiracy", U.S. Attorney's Office, 17 January 2025, https://www.justice.gov/usao-edky/pr/international-crypto-vendor-sentenced-money-laundering-conspiracy.

126 Luis Prada, "The FBI Ran an 'Elon Musk' Crypto Money Laundering Operation for Almost a Year", *Vice*, 9 April 2025, https://www.vice.com/en/article/the-fbi-ran-an-elon-musk-crypto-money-laundering-operation-for-almost-a-year/.

on a distributed network of associates (in the US and overseas) to pick up the cash, conceal it in mail parcels (including inside books and layered envelopes) and ship it to customers. Authorities said that Murarka understood that many clients were engaged in crimes, such as hacking and drug trafficking, and that the scheme laundered more than $20 million in criminal proceeds.

US authorities took down Anurag Pramod Murarka by building a case over time that combined undercover work, postal interdiction and court-authorised data collection. Investigators say they first identified the laundering service in 2021 when the operator, using handles such as 'elonmuskwhm', advertised on darknet venues and related forums that he could swap cryptocurrency for mailed US cash.

From there, the FBI and US Postal Inspection Service (USPIS) ran controlled exchanges and tracked how the cash moved through the mail, including parcels that concealed currency inside books and multiple layers of envelopes. The investigation also focused on US-based logistics.

In early 2023, agents tied shipments to Davis Paolucci, who was indicted and arrested, and a search of his home recovered about $600,000 in cash. To strengthen attribution and map communications and financial flows, prosecutors sought warrants for stored account data under the Stored Communications Act, including an Apple account request in June 2023 that laid out suspected money laundering and unlicensed money transmitting violations.

Murarka was ultimately arrested on 29 September 2023 in a joint FBI and USPIS action. He was drawn to the United States after officials approved a travel visa, allowing agents to take him into custody once he arrived. After the arrest, the FBI assumed control of his online identity and continued operating the service as an undercover measure to identify customers and generate follow-on seizures and prosecutions, including stopping attempted account takeovers that exceeded $1.4 million and supporting drug-related seizures. The case concluded with a federal judge, in 2025, sentencing Murarka to 121 months in prison for conspiracy to commit money laundering.

2) International Frameworks

As shown in this report, offenders aggressively exploit multiple jurisdictions, underscoring the critical need for harmonised legislation. Given the cross-border proliferation of money laundering, the Financial Action Task Force (FATF) was established in 1998, to be responsible for setting global standards on anti-money laundering legislation. Today, it includes 40 members. In 2019, FATF extended its recommendations to cryptocurrency. FATF guidance is structured at both the national level and in provisions directed specifically at virtual asset service providers (VASPs):

FATF recommendations at the country level include:

- Apply a risk-based approach: stronger rules and supervision where the crypto risks are higher;
- VASPs must be licensed or registered in the jurisdiction where they are created/operating, and subject to ongoing AML supervision or monitoring;
- Operating a VASP without registration should be a violation with effective, proportionate and dissuasive sanctions that can hit the business, its directors and senior management;

- Ensure VASPs apply targeted sanctions;
- Make VAs and VASPs part of the suspicious-transaction reporting system and implement the Travel Rule (see below) for virtual assets;
- Support cross-border cooperation on crypto cases.

FATF recommendations include that VASPs must:

- Identify and assess their own money laundering risks and adjust controls accordingly;
- Conduct adequate KYC controls and apply enhanced due diligence for transactions above $1,000;
- Keep customer and transaction records for at least five years so authorities can trace VA flows;
- Apply extra measures for politically exposed persons and high-risk situations;
- Apply the Travel Rule for VA transfers above the threshold: VASPs must obtain, hold and transmit the originator's name and VA wallet information and the beneficiary's name and VA wallet information;
- Screen customers and transactions against terrorism/proliferation lists and freeze VA holdings without delay where required.

As of April 2025, among 138 jurisdictions that have been formally assessed by FATF: one jurisdiction is fully compliant, 40 jurisdictions are largely compliant, 68 jurisdictions are partially compliant and 29 jurisdictions are not compliant. For comparison, a year earlier, 75% of assessed jurisdictions were only partially compliant or non-compliant.

FATF's Travel Rule is one of the most concrete pieces of the standard. It requires financial institutions and VASPs to share information about the sender (originator) and receiver (beneficiary) with each transfer of funds or virtual assets, creating transparency to combat money laundering and terrorist financing, essentially making a customer's information 'travel' with the transaction. [127] Among 117 jurisdictions that allow VASPs (i.e. that don't ban them): 85 jurisdictions (73%) have passed the Travel Rule legislation, 14 jurisdictions (12%) are in the process of passing it, the rest (about 15%) have no Travel Rule framework yet.

Of those 85 jurisdictions with Travel Rule laws, 59% (50 of 85) have not yet taken any enforcement or supervisory action focused on compliance with the rule. The gap between formal legislation and real-world enforcement remains significant; addressing implementation should therefore be the primary focus.

3) Public–Private Partnerships

As well as international intergovernmental cooperation, cooperation among different cryptocurrency services is vital for protecting both individuals and the broader space. The most significant partnership is the T3 Financial Crime Unit (FCU), launched in September 2024. This comprises three of the largest firms in the cryptocurrency space: TRM (a crypto-currency analytics firm), TRON (a decentralised blockchain) and Tether (the issuer of the largest stablecoin, USDT).

Its main role is to aid law enforcement and to help crypto platforms detect, track and freeze illicit funds on the blockchain, especially USDT on the TRON network. They monitor on-chain transactions to spot patterns linked to scams, hacks, money laundering, terrorism financing and other financial crimes. As of 31 October 2025, the FCU has managed to freeze $300 million.

[127] "FinCEN Advisory", FinCEN, January 1997, https://www.fincen.gov/system/files/advisory/advissu7.pdf.

After Tron joined this initiative, it saw the biggest decline in illicit volume of any major chain, with illicit volume dropping by about $6 billion and its own share of Tron's on-chain activity that was illicit decreasing by a half. [128]

To conclude, most jurisdictions are gradually adopting anti-money laundering legislation, but substantial gaps remain. Moreover, in many countries, the implementation of these new frameworks has yet to be meaningfully tested. Public–private partnerships are therefore essential to protect society and to support the cryptocurrency industry's continued growth and legitimacy.

4) Confronting Sanctions Evasion in Crypto

Many cases identified in the Global Cryptocurrency Laundering Database have had direct implications by allowing sanctioned individuals or countries to process billions of dollars, either voluntarily or involuntarily. It has now become an area of importance for regulators and law enforcement authorities.

Three countries which have been sanctioned in the EU, US and UK have been prolific in using cryptocurrency for sanctions evasion: Russia, North Korea and Iran. As such, they have come into focus by authorities responsible for the detection of sanctions evasion.

a) Russia

Garantex was a crypto exchange that functioned as a sanctions-evasion tool because it provided services that helped users move value. Prosecutors later alleged its operators actively adapted their operations to evade US restrictions, including continuing transactions that touched the United States and rotating wallet infrastructure to make screening and blocking harder. [129]

Garantex processed over $100 billion in transactions, with 82% of its total volume linked to sanctioned entities worldwide. [130] This displays how cryptocurrency services can act as a severe tool for sanctions evasion. It's likely that UK, EU and US firms come into contact with such exchanges, meaning it is vital to improve screening and regulation.

In March 2025, US and partner agencies seized Garantex domains and servers and froze funds, and the platform suspended services after Tether blocked wallets linked to the exchange.

Even after its takedown, it transformed into a successor exchange, Grinex, which was created by Garantex insiders to move customers and deposits and keep the activity going, despite sanctions and law enforcement action.

b) North Korea

North Korea has been carrying out mass exploitations of companies and private individuals within the cryptocurrency space. This report has identified $4.1 billion that has been stolen through just 19 hacks by North Korean actors, including the largest cryptocurrency hack in history, the hack of ByBit, where North Korean hackers stole $1.5 billion.

128 "Category deep-dive: Overall 2024 figures and declining illicit crypto volume on TRON", *TRM*, 17 February 2025, https://www.trmlabs.com/resources/blog/category-deep-dive-overall-2024-figures-and-declining-illicit-crypto-volume-on-tron.

129 "Garantex Cryptocurrency Exchange Disrupted in International Operation", Office of Public Affairs, 7 March 2025, https://www.justice.gov/opa/pr/garantex-cryptocurrency-exchange-disrupted-international-operation.

130 "Grinex Emerges as Likely Garantex Rebrand", *TRM*, 28 April 2025, https://www.trmlabs.com/resources/blog/grinex-emerges-as-likely-garantex-rebrand.

All revenue received by North Korea directly contravenes EU, UK and US sanctions regimes, thereby sustaining its war-related programs and contributing further harm to civilian populations. Available estimates suggest that approximately one-third of annual government revenue is derived from cryptocurrency-based schemes, a rapidly evolving ecosystem that continues to adapt in response to enforcement efforts.

c) Iran

Iran relies on specific persons and partners to help evade sanctions. For example, two Iranian individuals, Alireza Derakhshan and Arash Estaki Alivand, helped facilitate over $100 million in profit through cryptocurrency for Iran through the sale of oil. They were sanctioned by OFAC in 2025. [131] As OFAC says:

> Iranian "shadow banking" networks like these – run by trusted illicit financial facilitators – abuse the international financial system, and evade sanctions by laundering money through overseas front companies and cryptocurrency. The IRGC-QF and MODAFL use these proceeds to support regional terrorist proxy groups and develop advanced weapons systems, including ballistic missiles and unmanned aerial vehicles (UAVs), which threaten the security of U.S. forces and those of our allies. [132]

Iran also relies on partner exchanges. For example, two Iran-linked exchanges have been registered in the UK. In January 2026, the US sanctioned both exchanges and Iranian national Babak Zanjani. The UK sanctioned the individual Babak Zanjani in early February 2026. The exchanges have been estimated to process $94 billion, while filing dormant accounts with the UK Companies House. [133]

In addition, terrorist groups have also managed to use cryptocurrency to evade sanctions and receive donations. For example, BuyCash was a Gaza-based money transfer business that also operated as a virtual currency exchange, offering services that included handling Bitcoin alongside more traditional remittance-style transfers. Over time, authorities tied the business to wallets and accounts that appeared in multiple terrorism-finance investigations. It has allegedly been implicated in Hamas fundraising operations, and also in financial activity involving affiliates of al-Qa'ida and ISIS. [134] In October 2023, OFAC sanctioned BuyCash and its founder, characterising the exchange as having materially supported Hamas and describing additional alleged links to other terrorist groups' financial activity. In July 2025, the US Department of Justice announced a civil forfeiture action targeting roughly $2 million in digital currency connected with BuyCash. [135]

131 "Treasury Targets Financial Network Supporting Iran's Military", U.S. Department of the Treasury, 16 September 2025, https://home.treasury.gov/news/press-releases/sb0248.

132 Ibid.

133 https://home.treasury.gov/news/press-releases/sb0375.

134 "DOJ Targets Hamas-Linked BuyCash Exchange in $2 Million Civil Forfeiture for Terrorist Financing", *TRM*, 24 July 2025, https://www.trmlabs.com/resources/blog/doj-targets-hamas-linked-buycash-exchange-in-2-million-civil-forfeiture-for-terrorist-financing.

135 "United States Unseals Civil Action Filed Against Approximately $2M in Digital Currency Involved in Hamas Fundraising", Office of Public Affairs, 22 July 2025, https://www.justice.gov/opa/pr/united-states-unseals-civil-action-filed-against-approximately-2m-digital-currency-involved.

12: AI Implementation

AI can help stop money laundering in crypto by handling monitoring work that is too big and too detailed for people to do well by hand. Older systems that rely on fixed rules often miss things because there are so many transactions, they happen quickly and wallet owners are not always easy to identify. Machine learning can look at past cases of fraud or crime and learn what suspicious activity tends to look like. It can then flag risky behaviour as it happens. This helps exchanges and other VASPs to adjust their controls over time as criminals change how they operate.

One of the main uses of AI is watching transactions and spotting unusual patterns. Instead of only checking simple limits, these models learn what normal activity looks like for different customers and wallets. They then point out behaviour that does not fit the usual pattern. For example, a wallet that suddenly starts sending many transactions in a short time, or money that is moved through many steps across different chains or tokens, can be marked as suspicious.

Another area where AI helps is looking at the network of blockchain transactions. Every transfer creates a link between wallets, so over time you get a map of how money moves. AI can work through that map at scale and pick up connections that are easy to miss. It can spot groups of wallets that seem to be run by the same person or service, follow funds coming from known criminal sources and catch patterns where money is split up and moved around to hide where it came from. That can help an exchange decide when to hold a transfer or stop it.

AI can also help by using text analysis on information outside the blockchain. A lot of risk signals show up off-chain, such as public reporting and official records. Natural Language Processing Models can scan this kind of material and surface names, services or contracts that are linked to scams, ransomware or sanctions. That information can then be added to risk scores and to customer checks, so investigators have better context when an alert comes in.

Although one cannot exclusively rely on AI for combatting money laundering entirely, it can provide a holistic overview to investigators to assist in spotting trends and patterns which would otherwise take much longer to implement. Thus, AI can be a useful tool that enables more direct intervention and leads to faster asset recovery.

13: Findings

1) **State-sanctioned sponsors are responsible for large attacks and laundering, used to fund state-linked military and cyber programs**

   State-sanctioned sponsors have emerged as key drivers of some of the largest cyberattacks, thefts and laundering schemes in the cryptocurrency ecosystem, using illicit proceeds to directly support weapons development and military programs. The laundered funds are not merely a source of general revenue: in many documented cases, they are explicitly linked to strategic objectives, such as financing missile programs. For example, the North Korea-backed Andariel unit identified in this report hacked several US healthcare institutions to fund cyberattacks against US military bases. This reliance on cryptocurrencies creates a feedback loop in which successful cyber operations generate capital that is reinvested into offensive capabilities, further increasing both the scale and sophistication of future attacks. A total of $4.1 billion has been identified in this report as stemming from North Korea-backed agents. The estimates show that cryptocurrency schemes account for one-third of North Korea's government revenue. As a result, state-sponsored laundering via cryptocurrency is no longer solely a financial integrity challenge. It constitutes a national and international security concern, insofar as it directly facilitates the financing of state-linked weapons development and military programs.

2) **Rising prevalence of illicit stablecoin usage despite enforcement efforts**

   Stablecoins have become increasingly central to illicit finance in the cryptocurrency ecosystem (estimated to account for 63% of illicit transactions today), even as regulators and industry actors have stepped up controls. They appeal to bad actors as they combine the speed and pseudonymity of crypto transactions, but do not swing in price like most tokens. Issuers have stepped up to try and stop this, with efforts like T3 and more cooperation from firms such as Tether and Circle. That has helped in some cases, but it has not stopped misuse. Because the volumes are so large, stablecoins are still an easy tool for laundering even with stronger rules and enforcement.

3) **Most 'clean exits' still interact with a regulated touchpoint**

   Most clean exits from illicit crypto funds still pass through at least one regulated touchpoint, such as a centralised exchange, before reaching the traditional financial system. Even when criminals use mixers or complex layering to obscure on-chain provenance, they usually need a regulated service to convert those assets into spendable cash or to enter the ecosystem. This reliance on regulated infrastructure creates critical chokepoints where AML controls, sanctions screening and blockchain analytics can intersect. However, when large, regulated exchanges don't follow the intended measures, they can be easily exploited.

4) **Recovery and seizures are possible, if acted on quickly and succinctly**

   Most people think once cryptocurrency is stolen or gained illicitly, it's no longer possible for the assets to be recovered, but that is not true. Rapid detection and response are critical to maximising recovery and seizures in cryptocurrency cases because the transparency and settlement speed that benefit criminals can also be used against them. When investigators or victims identify an exploit or suspicious outflow quickly, they can trace funds in real time across addresses and flag them with major services before the assets are fully laundered or cashed out. Overall, the report has identified the seizure of $92 billion across 164 cases involving illicit activity.

5) **Cryptocurrency's potential to appreciate post-offense can increase the value of illicit proceeds, while simultaneously strengthening governments' incentives to target and dismantle laundering networks**

Because many cryptocurrencies can rise in price over time, money stolen in hacks and other crypto crimes can appreciate even after the damage is done. If criminals keep control of the assets in wallets they own, the value can climb during a bull market. That gives them more money to keep operating. The same effect can work in the other direction too. If investigators trace the funds and seize them later, they may recover more than was illicitly gained at the start. That can make major seizures more meaningful in real terms. It can help cover restitution for victims and it can also support future enforcement work when the recovered value goes back into public resources. This report has identified $215 billion of accrued capital gains from hacks, fraud, Ponzi schemes and other illicit activities. This either ends up in the pockets of the criminals, which can fund future illicit activity, or is returned to the rightful owners.

6) **Fraud, including 'pig-butchering' scams, is increasingly used as an initial entry point for acquiring and laundering illicit cryptocurrency**

These scams are often organised by large groups, including Prince Group identified in this report, and have taken off in recent months. In these schemes, victims are groomed over weeks or months and then pressured to move growing amounts of fiat through compliant exchange accounts into wallets under the fraudsters' control. Because the person providing the KYC information is a genuine customer rather than a mule or a hacked account, these flows can initially resemble ordinary retail investing or savings behaviour which weakens traditional screening focused on obviously suspicious profiles.

7) **Cross-chain laundering has exploded**

Cross-chain laundering has surged as criminals lean on bridges and chain hopping to move funds between incompatible networks and slip past controls that are still organised chain by chain, rather than ecosystem-wide. About $22 billion in illicit crypto is attributed to cross-chain laundering. Many pass-through mixers, such as Tornado Cash, move over bridges into Bitcoin and on to high-risk mixers, a pattern documented in many such cases. Ransomware operators have begun to mirror these tactics as well, which spreads investigative trails across several networks and jurisdictions at once.

8) **Platform freezes and takedowns materially shift behaviour for bad actors**

When a major service suddenly blocks addresses or goes offline, criminals can lose access to operational wallets and long-standing laundering pipelines in a single move. That shock pushes them to diversify services. It often introduces mistakes and fresh visibility for investigators which they can capitalise on, e.g. in the AlphaBay takedown. After a takedown, launderers often fragment their services to try and fill the void.

9) **Large-scale hacks are very underrepresented within the docket**

Ponzi schemes in the crypto space tend to attract the most legal and regulatory action, while protocol hacks and technical exploits often see far fewer formal cases, even when the absolute losses are comparable. Consumer-facing investment scams generate large numbers of victims and strong political pressure, which makes them a natural focus for prosecutors. By contrast, many hacks involve pseudonymous attackers and complex technical attack paths, so attribution is harder and the evidentiary burden is higher. The result is an enforcement landscape that appears skewed: Ponzi and high-yield schemes

dominate the visible docket of crypto-related legal actions, while large-scale hacks remain underrepresented despite their material role in generating illicit funds. The identified hacks have had a 9% conviction rate while Ponzi schemes have had a 65% conviction rate.

10) **International cooperation and public–private partnerships are essential**

International cooperation and public–private partnerships are essential because crypto crime crosses borders far faster than any single regulator or agency can respond. Laundering chains often touch multiple jurisdictions, with on-ramps, mixers and off-ramps each sitting under different legal regimes, so meaningful disruption depends on fast mutual legal assistance. When law enforcement agencies work directly with exchanges and analytics providers, they can move from reactive case work to proactive disruption. Joint investigations also give private actors clearer legal and operational frameworks for freezing assets and providing data, which reduces hesitation at critical moments. The T3 Financial Crime Unit and its expanded T3+ Global Collaborator Program show how effective this model can be in practice. T3 has worked with law enforcement agencies in 23 jurisdictions to freeze around $300 million in criminal crypto assets in one year alone since its creation.

14: Recommendations

1. Fully implement and harmonise crypto regulatory standards

Policymakers should prioritise full and timely transposition of the FATF standards on virtual assets and VASPs into national law, and ensure they are applied consistently across all relevant entities. This includes comprehensive implementation of the Travel Rule. Many jurisdictions already have strong AML laws covering virtual assets on paper, but suffer from weak or uneven implementation. Authorities should prioritise using the powers they have. Regular public reporting on supervisory activity and outcomes in the crypto sector can reinforce accountability and deterrence.

Within the EU, uneven rollout of the Travel Rule and different national approaches to freezing and confiscating crypto can create gaps that criminals can use. EU institutions should align technical standards and data-sharing requirements across Member States, and clarify how the Travel Rule applies to self-hosted wallets and DeFi activity.

The EU should also publish a common crypto-freezing and confiscation playbook that sets out how to freeze assets, secure and manage private keys and run cross-border actions. A single EU approach would reduce confusion for VASPs that operate across borders and make it easier for law enforcement to act quickly and consistently.

2. Build specialist enforcement agencies and training units

Governments should create a dedicated cryptocurrency enforcement body with clear powers to investigate and prosecute crypto-related crime, instead of spreading these cases across multiple general agencies. A single body can build and retain specialist capability in digital forensics and blockchain investigations, which supports faster identification of criminal activity and more effective disruption of networks that use virtual assets.

Where a new body is not practical, governments should strengthen existing law enforcement, supervisory and prosecutorial organisations by setting up specialist crypto AML units and funding formal training. These units should be staffed with investigators, analysts and prosecutors who work primarily on crypto-enabled threats, including ransomware, darknet market activity, fraud, sanctions breaches and terrorist financing linked to virtual assets.

3. Freezing and asset-recovery capabilities

While the US has it, the UK and EU should establish a dedicated Crypto Asset Recovery Office to lead on identifying, preserving, managing and ultimately realising seized digital assets. This office would support law-enforcement investigations, coordinate with courts and insolvency practitioners and manage relationships with custodial service providers. It could secure storage of seized crypto, as well as implement policies for returning assets to victims or channelling proceeds into public funds.

Authorities should introduce fast-freeze mechanisms that allow rapid, time-limited freezing of suspicious crypto assets where there is an immediate risk of dissipation, coupled with legal safe-harbours for intermediaries who act in good faith.

Because virtual assets can be moved or obfuscated in minutes, traditional freezing orders are often too slow to be effective. A fast-freeze regime would enable exchanges, custodians and other VASPs to act swiftly on law enforcement or FIU alerts, while protecting them from civil liability if the freeze is later found to be unwarranted, provided they followed prescribed procedures.

4. Regulate and harden high-risk crypto services to stop sanctions evasion and protect victims.

The Ruble-backed stablecoin A7A5 is one of the most prevalent issues facing the West. It is sanctioned in the UK, US and EU but it still operates. A7A5 holds value through its ability to be converted into cash by criminals. Western governments need to put pressure on the specific exchanges which allow the conversions to happen and the countries which facilitate these exchanges.

In the United States, sanctions policy should incorporate a dynamic escalation framework tailored to smart contracts and crypto protocols. Rather than treating all on-chain activity as identical, OFAC could start with targeted measures and escalate to broader designations or restrictions if a protocol repeatedly facilitates sanctioned or high-risk activity and governance actors fail to mitigate it.

5. Upgrade data and transparency for on-chain risk

Authorities should establish a national On-Chain Risk Registry that aggregates and classifies high-risk crypto addresses. Regulators and industry should also work together to develop compliance oracles that feed real-time risk and sanctions information into DeFi protocols. These oracles would reference trusted datasets, such as the On-Chain Risk Registry, and provide a standardised signal that smart contracts can use to block or flag high-risk transactions.

Local exchanges and brokerages should be required to display clear, intuitive risk indicators to retail customers at the point of transaction. These indicators might flag if a token is associated with frequent scams or recent hacks. They could use simple labels or colour-coded scores rather than complex technical metrics. Regulators should set minimum standards for how such indicators are calculated and presented and ensure comparability across platforms.

6. Strengthen public–private partnerships and innovation-friendly compliance

Authorities should formalise and expand structured public–private partnerships focused specifically on crypto-related financial crime, building on existing models. These PPPs should bring together law enforcement, major exchanges, blockchain analytics firms and banks in a regular operationally focused setting. The partnerships should support rapid sharing of typologies, emerging threats, high-risk indicators and anonymised case studies, as well as coordinated responses to major incidents, such as exchange hacks or large-scale frauds. Specifically, more exchanges and services should join T3+ in order to have a broader impact.

Additionally, these partnerships can offer training and simulations through a dedicated AML sandbox for small banks and financial institutions. The sandbox would let participating institutions test limited products and services under close supervisory engagement. By reducing uncertainty and lowering the upfront compliance burden, the sandbox would help smaller banks build practical capability and bring more crypto activity into the regulated space, mitigating risks of laundering.

7. Create whistleblowing rewards for stopping cryptocurrency schemes

While the US and South Korea have a system to provide compensation and incentives to whistleblowers, it is not common practice in the UK and the EU. There should be a rewards system established by government agencies to help with the identification of illicit crypto services and fraud schemes. The whistleblower can receive a payout from funds collected by the government. This can establish an incentive and lead to the exposure of laundering operations that otherwise would remain undetected, before billions are stolen from individuals and businesses. This shifts the balance of power from criminals to law enforcement.

8. Implement kill switches and red-team testing

For products and features with elevated money-laundering or sanctions risk, exchanges and crypto services should design and maintain technical 'kill switches' that allow rapid, controlled shutdown when serious concerns emerge. These kill switches can stop laundering in its tracks if a big transaction is about to occur.

Exchanges should institutionalise red-teaming and adversarial testing to probe how well their AML controls hold up against realistic crypto-native laundering scenarios. Internal or external red teams should design test campaigns that mimic sophisticated bad actors.

9. Build advanced data and investigative capabilities employing AI

In the age of AI, exchanges should deploy AI-driven tools to aid human investigators. AI can be used to automatically cluster related addresses and wallets, suggest likely beneficial ownership links, identify recurring typologies and rank alerts by probable severity.

Exchanges should build data architectures that natively join blockchain activity with off-chain KYC, behavioural and device information at the customer level. Every deposit, withdrawal and internal transfer should be linked back to a verified customer profile or cluster, enabling investigators and monitoring systems to see who ultimately controls the funds.

10. Adopt responsible crypto advertising and coverage standards that both protect audiences and spotlight victims

Media organisations should tighten their advertising policies for crypto products so that promotional content does not outpace consumer protection. This includes performing due diligence on advertisers, especially around volatility and the prevalence of scams. Crypto ads should be clearly distinguished from editorial content, with strict rules against advertising that could mislead audiences into confusing paid promotions with independent journalism.

At the same time, media outlets should recognise that maximised, timely coverage is crucial when assets are stolen or launderers are trying to disappear. Examples of this can be seen throughout this report. By giving victims a voice to report rapidly on major thefts or large-scale laundering schemes and highlighting investigative leads can increase public awareness. This can help mobilise community efforts and pressure bad actors who are attempting to lie low. Media reporting has put pressure on bad actors and enabled recovery of funds.

15: Further Important Resources

Guide on Relevant Aspects and Appropriate Steps for the Investigation, Identification, Seizure, and Confiscation of Virtual Assets:

biblioteca.gafilat.org/wp-content/uploads/2024/04/Guide-on-relevant-aspects-and-appropriate-steps-for-the-investigation-identification-seizure-and-confiscation-of-virtual-assets.pdf

FBI Guidance for Cryptocurrency Scam Victims:

https://www.ic3.gov/PSA/2023/psa230824

NCSC: Recovering a hacked account:

https://www.ncsc.gov.uk/guidance/recovering-a-hacked-account

House of Commons Library: What digital assets are, how they work, their history, the benefits and risks, and how regulators and policy makers are approaching them:

https://commonslibrary.parliament.uk/research-briefings/cbp-10329/

Report Fraud: The place to report/prevent/understand cyber crime and fraud

https://www.reportfraud.police.uk/

Title: “CONFRONTING THE ILLICIT-FINANCE HYDRA IN CRYPTO MARKETS: PROTECTING RETAIL INVESTORS AND DISRUPTING HOSTILE GOVERNMENT EXPLOITATION”
By Alexander Browder

The Henry Jackson Society
Millbank Tower, 21-24 Millbank
London SW1P 4QP, UK

www.henryjacksonsociety.org

HJS
Henry
Jackson
Society

CENTRE FOR RESILIENT SOCIETY

DEMOCRACY | FREEDOM | HUMAN RIGHTS

March 2026