GLOBAL INITIATIVE
AGAINST TRANSNATIONAL ORGANIZED CRIME

THE CURRENCY OF GLOBAL CRIME

HOW CRYPTO IS RESHAPING ILLICIT ECONOMIES

John Collins

JUNE 2026

ACKNOWLEDGEMENTS

The author wishes to thank the various colleagues at the Global Initiative Against Transnational Organized Crime (GI-TOC) who contributed to this report, either through their existing work or their inputs into its development. In particular, Mark Shaw and Tuesday Reitano, who provided invaluable guidance and direction. Further, Minna Fisher, who provided research assistance.

Sections of this report were drafted with generative AI assistance (Chat GPT 5). All editing, analysis, fact-checking and conclusions remain the author's own.

ABOUT THE AUTHOR

John Collins is the director of academic engagement at the GI-TOC. He is also a fellow at the Centre for Criminology, University of Hong Kong, and editor-in-chief of the *Journal of Illicit Economies and Development*, LSE Press. John's interests focus on the political economy of international drug control and the dynamics of national and international policy reforms.

© 2026 Global Initiative Against Transnational Organized Crime.
All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means without permission in writing from the Global Initiative.

Cover: © *GI-TOC*

Please direct inquiries to:
The Global Initiative Against Transnational Organized Crime
Avenue de France 23
Geneva, CH-1202
Switzerland
www.globalinitiative.net

CONTENTS

ACRONYMS AND ABBREVIATIONS

AML/CTF	Anti-money laundering/counter-terrorism financing
CAR	Central African Republic
DeFi	Decentralized finance
FATF	Financial Action Task Force
FBI	US Federal Bureau of Investigation
IWF	Internet Watch Foundation
MiCA	Markets in Crypto-Assets
OTC	Over-the-counter
PCC	Primeiro Comando da Capital
VASP	Virtual asset service provider

EXECUTIVE SUMMARY

Cryptocurrency has shifted from a supplementary payment method into a core enabler of organized crime and cyber-enabled illicit activity. Its key features, including speed, borderless transferability, pseudonymity and growing liquidity, provide criminal networks with a flexible financial infrastructure that is difficult to disrupt using traditional enforcement tools.

Across a range of illicit activities, crypto facilitates the movement and laundering of funds, supporting increasingly sophisticated financial architectures that combine decentralized and regulated systems. As adoption expands, particularly through stablecoins and accessible platforms, barriers to entry are lowered, enabling greater scale, resilience and geographic dispersion, and positioning cryptocurrency as a strategic asset that is reshaping global illicit economies.

Cryptocurrencies have streamlined the movement of illicit funds and strengthened the financial resilience of organized crime by integrating laundering, transfer and conversion functions. The result is the emergence of a layered and adaptive laundering ecosystem in which exchanges, stablecoins, brokers and informal financial networks collectively provide the infrastructure through which illicit capital can circulate globally with unprecedented speed and flexibility.

In addition, the evidence shows that cryptocurrencies are not merely augmenting existing criminal practices but transforming them across several sectors, including cyber-enabled fraud, drug trafficking, human exploitation and sanctions evasion.

The perceived transparency of blockchain systems does not readily translate into effective enforcement. Criminal actors exploit fragmentation, jurisdictional divergence and a wide range of obfuscation tools to reduce the practical risks of detection and disruption.

Without more coordinated and adaptive responses, current regulatory and enforcement frameworks are unlikely to keep pace with the scale, sophistication and transnational nature of crypto-enabled crime.

This report examines how cryptocurrencies are reshaping the operational and financial dynamics of organized crime, with particular attention to the emergence of increasingly complex laundering ecosystems, the expansion of crypto-enabled criminal markets and the growing convergence between licit and illicit financial infrastructures. It explores how criminal actors exploit technological innovation, regulatory fragmentation and global financial asymmetries to operate across borders with greater speed, resilience and adaptability. Drawing on a range of international case studies, the report also analyzes the uneven global regulatory environment surrounding cryptocurrencies, including weak governance zones, sanctions evasion systems and emerging financial peripheries, while assessing the broader implications for law enforcement, governance and international financial security.

Methodology

This report is based on a qualitative analysis of open-source material examining the relationship between cryptocurrencies and organized crime in a number of jurisdictions and criminal markets. The research draws on academic literature, investigative journalism, regulatory documents, law enforcement reporting, blockchain analytics publications, policy papers and court records to analyze how cryptocurrencies are being integrated into contemporary illicit economies. Particular attention is given to laundering infrastructures, the role of exchanges and stablecoins, the expansion of crypto-enabled criminal markets and the emergence of regulatory and enforcement gaps.

The report adopts a comparative and case study-based approach, examining developments across a range of geopolitical and regulatory contexts, including major financial centres, weak governance environments and sanctions-affected jurisdictions. It combines analysis of global trends with illustrative criminal cases to explore how criminal actors adapt to changing financial technologies and fragmented regulatory systems. The report also draws on existing blockchain analysis and enforcement data to assess the opportunities and limitations of tracing illicit crypto activity, while situating these developments within broader debates on financial governance, transnational organized crime and illicit markets.

Key points

- Cryptocurrencies are no longer a supplementary payment mechanism, but a core component of contemporary organized infrastructures, facilitating laundering, value transfer and operational coordination across borders.
- Crypto-enabled criminality is increasingly industrialized and globalized, supported by sophisticated financial ecosystems linking exchanges, stablecoins, brokers, decentralized finance (DeFi) systems and informal financial networks.
- Stablecoins, particularly Tether (USDT), have become central to illicit financial flows, combining the speed and borderless transferability of cryptocurrencies with the relative stability of fiat currencies.
- Organized crime groups today use cryptocurrencies not only for laundering, but also as operational infrastructure supporting fraud, ransomware, drug trafficking, migrant smuggling, human trafficking and sanctions evasion.
- Complex shadow laundering ecosystems have emerged involving over-the-counter (OTC) brokers, cash desks, cross-chain bridges, mixers, unhosted wallets and decentralized exchanges that enable criminals to fragment and obscure illicit financial flows.
- Cryptocurrency-enabled fraud has expanded significantly through AI-enhanced impersonation scams, romance scams and large-scale scam compounds, particularly in South East Asia, where groups operate highly structured cyber-fraud ecosystems.
- There is a growing convergence between organized crime, state-linked actors and sanctions evasion systems, particularly around Russian financial networks, Chinese money laundering systems and North Korean cyber activity.
- Weak governance environments, regulatory fragmentation and uneven enforcement create financial peripheries that allow crypto-enabled criminal ecosystems to scale and integrate into broader global financial systems.
- While blockchain systems are theoretically traceable, the practical realities of enforcement remain highly constrained by resource limitations, jurisdictional fragmentation and increasingly sophisticated obfuscation techniques used by criminal actors.
- The rapid mainstreaming of cryptocurrencies, combined with inconsistent global regulation and growing institutional integration of digital assets, risks further expanding opportunities for organized crime and illicit financial activity unless more coordinated international responses emerge.

CRYPTO CURRENTS

Cryptocurrency has moved from the margins of the financial system to a position of deep integration within modern criminal economies. What was once a major constraint for organized crime groups – laundering proceeds without detection – has been fundamentally altered. Digital assets offer a flexible and relatively opaque means of moving and disguising value without relying on more tightly regulated parts of the global financial system. This shift has lowered barriers to entry and accelerated the speed and scale at which illicit funds can circulate. Senior law enforcement authorities have warned that the ability to track financial flows is being eroded, highlighting how the traditional 'follow the money' investigative approach is becoming less effective in the face of increasingly sophisticated crypto-enabled networks.

At the same time, crypto is no longer confined to facilitating existing crimes but is shaping new ones. Offences such as targeted kidnappings and extortion aimed at accessing digital wallets demonstrate how traditional organized crime methods are adapting. More broadly, the spectrum of crypto engagement in illicit activity is widening, from fraud and ransomware to migrant smuggling, where payments and coordination increasingly rely on digital assets. This reflects a wider transformation: crypto has shifted from a niche payment mechanism into a widely accepted medium of exchange with several spillover uses, including in illicit markets.

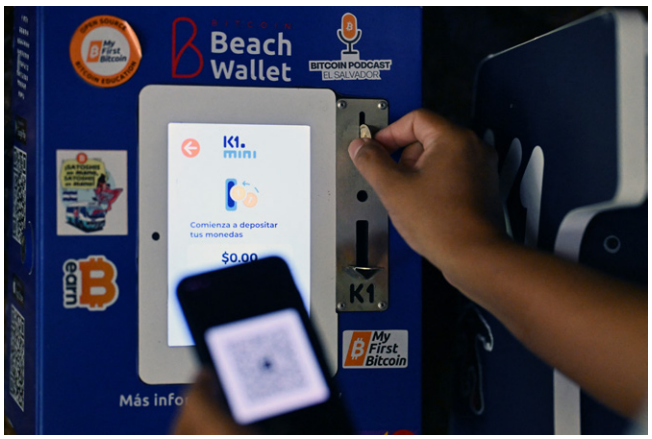
The diversification and mainstream adoption of these technologies are now outpacing the capacity of law enforcement and regulatory systems. This raises concerns that the original aspirations of decentralized finance have, in practice, created an ecosystem that is criminally exploitable at scale. Moreover, the crypto regulatory environment is varied, oscillating and fragmenting globally, opening large enforcement and regulatory gaps that criminals can readily exploit.

CRIME AT SCALE

The Chainalysis 2026 Crypto Crime Report highlights a rapidly changing and increasingly industrialized illicit crypto ecosystem, with illicit addresses receiving an estimated US$154 billion in 2025, a record driven largely by sanctions evasion and state-linked activity. The report points to the growing role of stablecoins, which account for most illicit transaction volume, as well as the expansion of sophisticated laundering networks using decentralized finance (DeFi), cross-chain transfers, mixers and unhosted wallets.

Scam activity was exceptionally high, with an estimated US$17 billion stolen through fraud schemes increasingly enabled by AI-generated impersonation and scam operations linked to organized crime networks in South East Asia. At the same time, ransomware, darknet markets and crypto-enabled human trafficking continued to expand, while North Korean and other state-affiliated actors played an increasingly prominent role in large-scale thefts and sanctions evasion. Despite this growth, Chainalysis emphasises that illicit activity still represents less than 1 per cent of total cryptocurrency transaction volume and argues that blockchain transparency continues to provide significant investigative opportunities for law enforcement and regulators.[1]

In 2025, the US Federal Bureau of Investigation (FBI) reported that cryptocurrency fraud reached US$9.3 billion in 2024, 66 per cent more than a year earlier.[2] This was despite large-scale enforcement operations such as the FBI's Operation Level Up, which is estimated to have prevented US$285 million in fraud by using blockchain analysis and intelligence to proactively contact people being defrauded to prevent further financial losses.[3] In 2025, US authorities seized approximately US$15 billion in Bitcoin in connection with a single cryptocurrency fraud case, the largest forfeiture in Department of Justice history.[4] The FBI estimated that Bitcoin ATM fraud reached US$333 million, twice the 2022 total, with a notable impact on older adults.[5] Most cases involve scammers impersonating companies or banks and flagging alleged suspicious activities before convincing victims to deposit funds into an ATM to remedy the issue. The money ends up in the scammers' accounts.[6]



The expansion of Bitcoin ATMs has been accompanied by a marked increase in fraud. In 2025, reported losses reached US$333 million, roughly double the level recorded in 2022. *© Marvin Recinos/AFP via Getty Images*

THE FINANCIAL ARCHITECTURE OF CRYPTO-ENABLED CRIME

Crypto's criminal significance and appeal can be understood across several interrelated dimensions. First, crypto increasingly operates as a form of infrastructure for organized crime, supporting coordination, transactions and cross-border activity. Second, it enables specific crime types, such as drug trafficking, fraud and human exploitation. Third, it has contributed to the emergence and scaling of new criminal markets, particularly in the digital sphere, where decentralized and irreversible payments support novel forms of online offending. Finally, cryptocurrencies function as a tool for concealment and laundering, enabling criminal actors to obscure financial flows, bypass regulated systems and integrate illicit proceeds into the global economy.

Crypto as core criminal infrastructure

Cryptocurrencies have become deeply embedded in the day-to-day operations of organized crime groups. Drug trafficking organizations, online black markets, human smugglers, extortion networks and mafia-style groups increasingly rely on crypto assets to move funds, conceal transactions and facilitate coordination across borders. Rather than serving as a peripheral payment mechanism, crypto now supports core operational functions and geographic reach.

The exposure of encrypted communication platforms such as Sky ECC illustrates this integration. Investigations by the European Union Agency for Law Enforcement Cooperation (Europol) and the EU Agency for Criminal Justice Cooperation revealed that tens of thousands of devices linked to organized crime groups were used to coordinate activities including drug trafficking, arms dealing and violent offences. Subsequent law enforcement actions, including large-scale cocaine seizures, demonstrated the operational scale of these networks.[7] Evidence further indicated that cryptocurrency, particularly Bitcoin, was used within this ecosystem to facilitate illicit financial flows.[8]

Financial functions: laundering and value transfer

Cryptocurrency laundering no longer relies on isolated actors or simple wallet transfers. It increasingly operates through a sophisticated and interconnected financial ecosystem that links licit and illicit infrastructures.[9] Centralized exchanges play a pivotal intermediary role while investigations repeatedly demonstrate that criminal proceeds flow through platforms with weak compliance controls

or inconsistent enforcement.[10] Illicit actors exploit regulatory arbitrage by shifting activity across jurisdictions and platforms, while exchanges face strong competitive incentives not to impose restrictions. Alongside regulated exchanges, decentralized exchanges, cross-chain bridges, mixers and unhosted wallets enable criminals to fragment transactions, obscure audit trails, and move funds rapidly across several blockchains before cashing out through fiat off-ramps or informal intermediaries.[11]

A broader laundering infrastructure has emerged around over-the-counter (OTC) brokers, informal cash desks and shadow financial facilitators.[12] These have become particularly important within transnational scam economies, sanctions evasion networks and drug trafficking systems. In South East Asia, scam compounds rely on OTC brokers and regionally connected financial intermediaries to move and cash out proceeds from large-scale fraud operations. Similar structures have emerged in Russian-linked sanctions evasion systems and Chinese money laundering networks connected to fentanyl trafficking.

Stablecoins have become especially important, combining the speed and borderless transferability of cryptocurrencies with the relative price stability of fiat currencies. The Financial Action Task Force (FATF) estimates that stablecoins accounted for most illicit crypto transaction volume in 2025, reflecting their growing attractiveness for organized crime groups, sanctions evasion networks and state-linked actors.[13] Tether (USDT), in particular, has become deeply integrated into illicit financial ecosystems. For example, it is used by sanctioned actors and Russian oligarchs for cross-border transactions and sanctions evasion. This includes large-scale money laundering operations such as those conducted by the Smart and TGR networks – uncovered in 2024 as part of an international investigation led by the UK National Crime Agency.[14]

Another major development is the emergence of Chinese money laundering systems that connect criminal proceeds with demand for foreign currency.[15] Blockchain analytics firms have identified links between cryptocurrency flows, trafficking operations, online fraud networks and these systems.[16] For example, crypto plays a central role in laundering fentanyl proceeds,[17] while Mexican cartels, including Sinaloa, increasingly use cryptocurrencies to pay Chinese suppliers for precursor chemicals, embedding crypto within transnational fentanyl supply chains.[18] Chainalysis reports that Chinese precursor suppliers received more than US$250 million in cryptocurrency between July 2015 and April 2023.[19]

Expansion into specific crime markets

Cryptocurrencies have driven the expansion of criminal activity across several sectors. In the field of cyber-enabled fraud, cryptocurrencies have become central to a range of scams. The speculative appeal of crypto markets enhances these schemes, allowing perpetrators to exploit expectations of high returns while benefiting from systems in which payments are difficult to reverse. As a result, fraud has become more personalized, scalable and profitable, with organized networks able to target many victims simultaneously while reducing risk of detection.[20]

Impersonation scams involve criminals posing as trusted individuals or institutions to gain victims' confidence before persuading them to transfer funds in cryptocurrency. According to Chainalysis, impersonation scams increased by 1 400 per cent between 2024 and 2025, with the use of artificial intelligence significantly amplifying their effectiveness, including through deepfakes and voice imitation, making scams up to 4.5 times more profitable.[21]

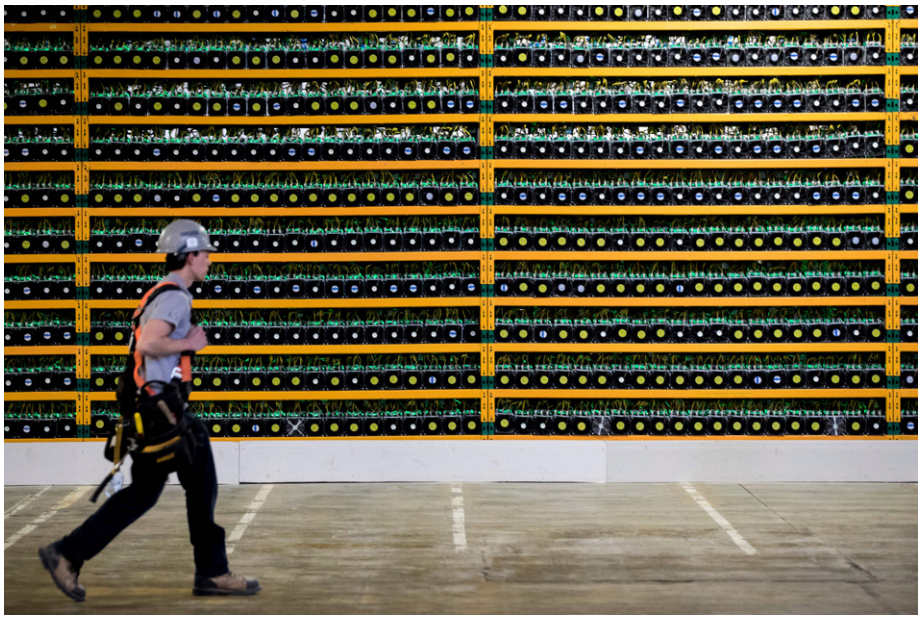
Romance scams, often referred to as 'pig butchering', are another major category of crypto-enabled fraud. In these schemes, perpetrators build long-term relationships with victims through social media or messaging platforms, gradually gaining trust before introducing fraudulent investment opportunities. Victims are encouraged to invest through fake or compromised cryptocurrency platforms, ultimately losing their funds.[22]

Beyond fraud, cryptocurrencies have also reshaped the economics of human trafficking, sexual exploitation and child abuse networks. In these contexts, crypto is not merely a payment method but a structural enabler, supporting the coordination, monetization and persistence of exploitative systems.[23] Chainalysis reported an 85 per cent increase in crypto payments linked to suspected human trafficking services in 2025, including prostitution networks, scam compounds and child sexual abuse material distribution, particularly in South East Asia. These networks increasingly relied on stablecoins and platforms such as Telegram for cross-border payments and coordination.[24] Investigative reporting further indicates that crypto payments linked to sexual extortion operations frequently involve transactions of about US$10 000.[25]

According to the Internet Watch Foundation, cryptocurrency has become the mainstream payment method for child sexual abuse material, with more than 1 000 identified URLs in 2025 accepting crypto payments for exploitative content. The Kidflix platform illustrates the scale of these operations:[26] Europol found that between 2022 and 2025 the platform hosted more than 90 000 child sexual abuse videos and maintained about 1.8 million users worldwide. Cryptocurrency was the exclusive payment method.[27]

Obfuscation, anonymity and enforcement challenges

Cryptocurrencies also support criminal anonymity and operational security, especially when combined with encrypted communication systems.[28] Although Chainalysis notes that many criminal actors still use relatively unsophisticated and traceable cryptocurrency payment methods, tracking these transactions nevertheless requires extensive technical expertise and significant law enforcement resources.[29] As a result, cryptocurrencies have altered the operational environment of organized crime even where they do not guarantee complete anonymity.



Cryptocurrency mining supports the ecosystem's legitimacy, but blockchain traceability does not ensure recovery or prosecution. Criminals often spread funds across multiple wallets and transactions to obscure illicit flows. *© Lars Hagberg/AFP via Getty Images*

Criminal actors increasingly exploit a broad range of blockchain-based obfuscation tools to conceal the source and movement of illicit funds before they reach regulated exchanges or fiat off-ramps. These include automated swap services and decentralized exchanges, which allow users to convert assets rapidly and often without formal identity verification; mixers and tumblers, which pool and redistribute funds to disrupt transaction tracing; cross-chain bridges and chain-hopping techniques, which move assets across several blockchains and cryptocurrencies to fragment audit trails; and privacy-focused assets and technologies designed to conceal wallet addresses, balances and transaction histories.[30] The FATF highlights the role of unhosted wallets and peer-to-peer transactions, allowing users to transfer funds directly without intermediaries such as regulated exchanges or financial institutions.[31]

The limits of blockchain traceability

Commentators point to a critical gap between the theoretical traceability of cryptocurrency transactions and the practical realities of law enforcement. While blockchain technology allows transactions to be followed, this does not automatically lead to asset recovery or successful prosecution. In practice, criminals exploit the system by dispersing funds across many wallets and transactions, a process (often referred to as 'smurfing') that fragments illicit proceeds through thousands of small movements.

This significantly increases the technical and resource burden on investigators, as tracing each transaction becomes computationally intensive and operationally unmanageable at scale. Even when flows can be partially mapped, converting that insight into enforcement outcomes is highly challenging. At the same time, the continued and growing use of cryptocurrency by criminal actors indicates that these barriers to enforcement are well understood and factored into their risk calculations, reinforcing the perception that the likelihood of detection, disruption or asset recovery remains relatively low.[32]

Implications

Taken together, these dynamics point to a broader set of systemic risks within the cryptocurrency ecosystem, particularly where governance remains weak, fragmented or contested. More broadly, cryptocurrency exchanges and related service providers occupy a critical intermediary position between illicit and licit financial systems. Where regulatory frameworks are underdeveloped or inconsistently applied, these platforms can facilitate the conversion, movement and integration of illicit funds with limited scrutiny. This not only enables individual criminal activities but strengthens the resilience and adaptability of wider illicit networks. As such, the risks are not confined to discrete cases but reflect structural weaknesses in governance that allow criminal infiltration and exploitation of the broader ecosystem.

THE CHANGING GLOBAL REGULATORY ENVIRONMENT

The global crypto regulatory environment continues to oscillate, but the direction of travel is towards deregulation in some major markets, such as the US, broad regulatory ambiguity in large parts of the world and expanding dark zones in others, enabling broad ranges of illicit and problematic activities. Where such gaps exist and such divergences between jurisdictions become apparent, tighter and standardized global regulations and enforcement are increasingly unlikely.

The EU and the UK

Europe is experiencing regulatory tightening, and new consumer protection and transparency requirements took effect in the EU at the end of 2024. They stem from the implementation of the Markets in Crypto-Assets (MiCA) regulation, which establishes a comprehensive legal framework for crypto assets across the bloc. The rules introduce stricter obligations for virtual asset service providers (VASPs),[33] including requirements on licensing, governance, consumer disclosures and the safeguarding of client funds. They also mandate greater transparency on token issuance, risks and business practices, while imposing measures to prevent market abuse and ensure operational resilience.[34]

A similar approach is emerging in the UK under the Financial Services and Markets Act, led by the Financial Conduct Authority. The proposed regime would introduce MiCA-like requirements for crypto firms, including authorization, consumer protection, disclosures, market abuse controls and prudential standards. However, the framework remains under consultation. In the meantime, the UK already applies stricter anti-money laundering (AML) and financial promotion rules and may ultimately go further than MiCA by regulating crypto lending, staking and aspects of DeFi.[35]

The US

In the US, the Trump administration has declared an end to the 'war on crypto', pardoning convicted fraudster Changpeng 'CZ' Zhao in October 2025.[36] Zhao pleaded guilty in 2023 to violating AML laws after Binance – the world's largest cryptocurrency exchange by daily trading volume – failed to implement effective controls against illicit activity, including transactions linked to organized crime and sanctions evasion. As part of the settlement, Zhao stepped down as CEO, paid substantial fines,

and Binance agreed to US$4.32 billion in penalties, marking one of the largest enforcement actions in the crypto industry.[37]

In February 2026, the *Wall Street Journal* reported that Binance had dismissed or suspended staff who had identified more than US$1 billion in transactions linked to sanctioned Iranian entities, shortly after these concerns had been raised internally.[38] The company denied the allegations and is suing the publication for defamation.[39]

Weaker regulation and enforcement in parts of the crypto sector have created opportunities for both organized and decentralized criminal networks. Competitive pressures may also discourage exchanges from aggressively policing illicit activity for fear of losing users and transaction fees. Investigations found that accounts linked to the Sinaloa cartel, Chinese fentanyl traffickers and Russian laundering networks connected to North Korea's weapons programme moved funds through major exchanges including Binance, Coinbase, OKX and HTX.[40]

Regulators under the Trump administration have also withdrawn civil lawsuits against Coinbase, Kraken and Binance, while the Department of Justice has continued to pursue criminal cases against OKX and Tornado Cash, a service designed to obscure the origin of funds by mixing cryptocurrencies from several sources.[41] The result is a rapidly shifting regulatory and enforcement environment, coinciding with greater mainstream adoption of cryptocurrencies as an asset by more traditional financial institutions.

As a bellwether of mainstream financial opinion in the US, JP Morgan Chase CEO Jamie Dimon is an example of the world's largest banks' shift in thinking on virtual assets. In 2022, Dimon declared himself 'a major sceptic on crypto tokens which you call currency, like Bitcoin. They are decentralized Ponzi schemes.'[42] As recently as January 2025, while signalling the potential inevitability of his bank engaging with 'some kind of digital currency at some point', he reiterated his view that 'Bitcoin itself has no intrinsic value. It's used heavily by sex traffickers, money launderers, ransomware.'[43]

Despite Dimon's cautious scepticism, JPMorgan Chase has made significant investments in blockchain infrastructure.[44] Major financial institutions are increasingly engaging with the crypto sector, a shift accelerated by the changing federal policy aimed at integrating digital assets into the mainstream financial system.[45] The risks of abuse, fraud and utilization by organized crime become even more pervasive under a more relaxed regulatory environment.

REGULATORY AND ENFORCEMENT GAPS IN THE FINANCIAL PERIPHERIES

Crypto-related illicit activity is increasingly concentrated in what can be understood as regulatory and enforcement peripheries, where oversight is limited, uneven or strategic. These financial peripheries are not confined to weak states but encompass a spectrum of environments characterized by weak enforcement capacity, regulatory arbitrage, political capture or deliberate state tolerance of certain forms of activity.

In such contexts, gaps between formal regulation and actual practice create opportunities for criminal actors to operate, scale and integrate into broader financial systems. Different types of enabling environments, ranging from zones of impunity and fragile governance to more ambiguous or strategically managed regulatory systems, facilitate the persistence and development of crypto-enabled crime.

Weak governance or impunity zones: Myanmar, Cambodia and Laos

Countries with weak governance are characterized by limited state oversight, corruption and the presence of entrenched criminal ecosystems. Cambodia, Myanmar and Laos are major hubs where scam compounds operate with relative impunity. Exploiting weak governance, special economic zones and limited financial oversight, these networks use cryptocurrency to support fraud, money laundering, human trafficking and other illicit financial flows.[46]

Myanmar and Cambodia remain weakly regulated crypto jurisdictions despite growing scrutiny over links to fraud, money laundering and transnational scam networks. Myanmar lacks a comprehensive legal framework for crypto or VASPs, with oversight further weakened by the post-2021 political instability, although its 2025 Cybersecurity Law expanded state surveillance of digital activity.

Cambodia has adopted a more structured but restrictive approach, prohibiting licensed financial institutions from handling crypto while introducing licensing and AML/counter-terrorism financing (CTF) requirements for digital asset businesses through recent Securities and Exchange Regulator regulations.[47]

Cyber scam centres in South East Asia illustrate how cryptocurrency has developed from a supplementary payment method into a core enabler of organized cyber fraud. Large-scale scam compounds in Cambodia, Myanmar's border regions and Laos's Golden Triangle Special Economic Zone are hubs where organized crime groups operate highly structured fraud schemes, most prominently investment scams. Victims can be recruited through social media or dating platforms, and are gradually convinced to invest through fraudulent applications that mimic legitimate crypto trading environments.

Targets from countries including China, the US and European nations were induced to transfer funds – primarily in Bitcoin, Ethereum and Tether – to wallets controlled by scam operators, often resulting in losses ranging from tens of thousands to several million US dollars.[48] Cryptocurrency also plays a critical role in laundering proceeds of these scam operations, with funds routed through a combination of centralized exchanges, DeFi protocols and cross-chain bridges to obscure their origin.[49]

Fragile or experimental states: Central African Republic and El Salvador

Fragile states adopt crypto initiatives in the absence of robust institutional capacity, creating environments where innovation outpaces regulation. The Central African Republic (CAR) illustrates how cryptocurrency adoption in brittle governance environments can generate significant risks when institutional capacity and regulatory oversight are limited.

The CAR's decision to adopt Bitcoin as legal tender in 2022, followed by the launch of the Sango Coin project and later the $CAR meme coin, was presented by President Faustin-Archange Touadéra as a strategy to modernize the economy, attract foreign investment and reduce dependence on traditional financial systems.

The Sango initiative offered foreign investors access to tokenized land, e-residency and potential investment opportunities tied to mining and forestry, while promoting ambitious infrastructure concepts such as a 'crypto city'. However, these ideas unfolded in a context of extreme fragility, where only a small proportion of the population had reliable access to electricity, mobile connectivity or the internet, making meaningful public participation in crypto markets unrealistic.[50]

The initiatives were introduced amid broader patterns of political consolidation, foreign influence and organized criminal penetration. The country's crypto agenda developed alongside the growing influence of foreign actors such as the Wagner Group, which has become deeply embedded in the CAR's political and extractive sectors. A 2023 law enabling the tokenization of natural resources, including land, oil, gold and timber, lacked robust governance safeguards and raised concerns about sovereignty, transparency and the exposure of state assets to transnational criminal exploitation. Individuals linked to fraud allegations and opaque business networks played roles in shaping and promoting the country's crypto projects, while Sango Coin and $CAR suffered from poor transparency, weak investor protections, technical irregularities and questions about market manipulation.[51]

A comparison with El Salvador illustrates that the same risks can emerge in more institutionally developed contexts when crypto adoption is driven by political strategy instead of regulatory readiness. El Salvador's 2021 decision to adopt Bitcoin as legal tender was framed as a tool for financial inclusion, remittances and economic modernization, supported by state infrastructure such as the Chivo wallet. As in the CAR, however, the rollout raised concerns about transparency, governance and the concentration of decision making within the executive. While El Salvador has stronger institutions than the CAR, critics (including the International Monetary Fund) have pointed to limited oversight of

public crypto investments, volatility risks and questions about the use of state funds, as well as the potential for crypto to facilitate illicit financial flows in a dollarized economy.[52]

The comparison underscores a broader pattern: where crypto adoption is rapid and politically driven, and where regulatory, technical and oversight mechanisms do not keep pace, digital assets can become embedded within existing governance dynamics, creating opportunities for opacity, elite control and potential misuse, even if the scale and nature of risks differ across contexts.[53]

Ambiguous or transitional regulatory systems: the former Soviet space

Transitional states are marked by shifting, inconsistent or incomplete frameworks, often seen in parts of the Caucasus and eastern Europe, where uncertainty creates opportunities for regulatory arbitrage. The former Soviet space, particularly where enforcement of AML/CTF measures is inconsistent, is a key enabling environment for crypto-related organized crime. The picture is nuanced, however, due to the strong adoption of blockchain technology in the region and complex intersections with regulations and state interests.

Eastern Europe and parts of the former Soviet space, especially Russia, are not simply sources of crypto crime but key nodes in global crypto ecosystems where illicit activity can be enabled, concentrated or scaled.[54] Crypto exchanges and financial intermediaries operating in or linked to these regions have, in some cases, processed large volumes of transactions tied to ransomware groups, darknet markets and sanctioned entities.[55] Weak compliance mechanisms, regulatory arbitrage and political constraints have been foundational enabling factors.

Recent research examining crypto and crime in Russia, Ukraine, Belarus, Moldova, Georgia, Armenia and Azerbaijan shows an ever-increasing blurring of the lines between organized criminal and state-led activity, diverging perspectives on the utility of crypto for sanctions evasion, and ongoing tactical shifts by law enforcement and illicit actors. Regulatory uncertainty and ambiguity is pervasive in Azerbaijan and Armenia, while Georgia has increasingly sought to regulate the sector while benefiting from low energy costs that attract crypto miners.[56] Ukraine has taken significant steps to establish a regulated cryptocurrency market, seeking to integrate digital assets into its financial system while mitigating their use for illicit activities. At the same time, cryptocurrency has played a notable role in supporting Ukraine's war effort, facilitating donations amounting to hundreds of millions of dollars.[57]

Strategic state integration or tolerance: Russia

Russia exemplifies contexts in which states with relatively strong capacity selectively incorporate or permit crypto activity to serve economic or geopolitical objectives. The state's approach to crypto-currencies has changed considerably over the past decade. Initially restrictive, the Central Bank of Russia classified cryptocurrencies as monetary surrogates in 2014 and prohibited their issuance, reinforcing this position in 2017 with warnings about their speculative risks.[58]

In the early 2020s, this stance began to shift. By 2021, President Vladimir Putin acknowledged the potential role of cryptocurrencies, though the Central Bank remained opposed to their use for every-day payments.[59] In January 2022, the Central Bank proposed a comprehensive ban on cryptocurrency activities, but it reversed its position in favour of partial legalization after Russia's invasion of Ukraine and resulting sanctions pressures.[60]

A Bitcoin mining farm in Norilsk, Russia. Russia is increasingly using cryptocurrency to bypass Western sanctions, as well as for intelligence operations.
© Andrey Rudakov/Bloomberg via Getty Images

From July 2024, Russia expanded cryptocurrency use and mining for international trade while maintaining a ban on domestic crypto payments.[61] In March 2025, the Central Bank proposed a three-year experimental regime allowing high net worth individuals and selected entities to invest in crypto assets, with plans to extend access to retail investors under strict controls, including annual purchase limits and authorized cryptocurrencies.[62] Proposed regulations include exchange licensing, restrictions on privacy coins and continued prohibition of domestic payments, while permitting regulated cross-border transactions.[63]

At the same time, Russian banks such as Sberbank are expanding crypto services, including crypto-backed loans and custody, as regulators consider allowing banks to operate crypto exchanges under existing licences, signalling deeper integration of crypto into the financial system.[64] While not a full liberalization, there is a continued trend towards crypto acceptance and integration, driven and fuelled by the war against Ukraine.

The Garantex-Grinex case

Moves against Garantex and the emergence of Grinex show the potential for coordinated action and the crypto ecosystem balloon effect – driving activity into other spheres or spawning new exchanges.

Garantex, a Russia-based cryptocurrency exchange founded in 2019, grew rapidly by facilitating high-volume transactions, including those linked to illicit finance. In April 2022, it was sanctioned by the US Department of the Treasury Office of Foreign Assets Control for its role in enabling transactions associated with darknet markets and ransomware actors.[65]

Despite the sanctions, Garantex processed transactions worth more than US$100 billion, with an estimated 70–80 per cent linked to sanctioned entities, while continuing as a major hub for ransomware, darknet markets and other illicit activities.[66] Garantex was ultimately shut down through coordinated US and European action, with authorities seizing its main domain on 6 March 2025 after Tether blocked approximately US$28 million in USDT transactions.[67]

Days later, affiliated social media began promoting Grinex, which had a nearly identical interface and was registered in Kyrgyzstan in December 2024.[68] In August 2025, US authorities expanded sanctions to Grinex based on similar allegations.[69] The case shows how illicit crypto exchanges often mirror cybercrime tactics by rebranding and restarting when one variant is shut down.[70] ■

Crypto, state-linked crime and sanctions evasion

Sanctions regimes have accelerated crypto adoption and scale. Russia is increasingly using crypto-currency as a practical tool to sustain international trade and bypass Western sanctions and the SWIFT system. Simultaneously, Russian institutions and actors are experimenting with crypto in several domains, including commodity trade settlements and intelligence operations, where digital wallets have reportedly been used to fund activities abroad.[71]

This shift reflects a broader reliance on informal and shadow economic practices under sanctions pressure. However, unlike traditional illicit trade, crypto transactions leave traceable digital footprints, prompting efforts by Russian actors to obscure flows and conceal activity. This creates a strategic challenge for Western governments to anticipate how these crypto-based systems may develop.[72]

Sanctioned entities received a record surge of crypto inflows in 2025. A 694 per cent increase drove illicit transaction volume to US$154 billion, reflecting how nation state actors are embedding cryptocurrency into financial infrastructure and strategic policy.[73] In Iran, activity has become increasingly state dominated, with the Islamic Revolutionary Guard Corps and affiliated networks responsible for over half of all value received in the final quarter and more than US$3 billion during the year.[74] Russia has developed parallel mechanisms such as the rouble-backed A7A5 stablecoin, which processed US$93.3 billion in less than a year and enabled businesses to access global markets despite sanctions.[75]

Russia is reportedly attempting to develop an alternative cross-border payments network in Africa using a rouble-backed cryptocurrency linked to the A7 network as part of efforts to bypass Western financial systems and sanctions. The initiative reflects a broader strategy to expand economic ties in Africa and reduce reliance on Western infrastructure, with reported expansion into countries such as Nigeria, Togo and Zimbabwe, though there is limited evidence of significant traction.[76]

North Korea recorded its most successful year of crypto theft, exceeding US$2 billion, with proceeds reportedly funding weapons of mass destruction programmes, while in Venezuela crypto continued to serve as a financial lifeline amid hyperinflation, with citizens and regime-linked actors relying on global exchanges and peer-to-peer channels rather than domestic systems.[77]

North Korea has increasingly turned to cryptocurrency as a central pillar of its sanctions-evasion strategy, using state-backed cyber units to conduct large-scale hacks targeting exchanges, DeFi platforms and private wallets, and stealing billions of dollars in digital assets. These stolen funds are laundered through complex chains of wallets, mixing services and cross-chain transactions, often routed through loosely regulated financial systems, for example in South East Asia, before being converted into usable currency. This crypto-based model is reinforced by networks of overseas information technology workers, allowing Pyongyang to bypass traditional financial controls and sustain revenue flows despite international restrictions.[78]

The Bybit theft

The Bybit theft is a key example of North Korea's strategy. It involved hacking a major cryptocurrency exchange, resulting in the loss of about US$1.5 billion in digital assets, making it one of the largest financial thefts on record. It is widely attributed to North Korean state-linked actors who used sophisticated methods to steal and rapidly launder the funds through the crypto ecosystem.[79]

Rather than an isolated cybercrime, crypto and cybercrime investigative journalist Geoff White argues that the attack reflects a broader pattern in which state-linked actors conduct highly sophisticated hacking operations to steal large volumes of cryptocurrency.[80] These operations are carefully planned, often involving infiltration of third-party systems and prolonged surveillance before execution. They resemble intelligence operations as much as criminal acts, blurring the line between organized crime and state activity.[81] ■

CRYPTO AND ORGANIZED CRIME IN LATIN AMERICA: A COMPARATIVE OVERVIEW

Cryptocurrencies are becoming increasingly embedded within legitimate financial activity and organized crime ecosystems in Latin America.[82] Adoption has been driven by a combination of economic instability, dollarization, demand for cross-border transfers, growing retail investment and expanding digital financial markets. At the same time, organized crime groups have increasingly integrated crypto assets into money laundering schemes, fraud operations, cross-border value transfers and illicit financial concealment strategies. Despite significant variation in legal frameworks and institutional capacity, the research shows that Brazil, Colombia, Ecuador and Panama face major challenges in regulating and disrupting crypto-enabled criminality.

Brazil

Brazil is arguably the most institutionally mature crypto environment in Latin America, but also one of the clearest examples of how sophisticated organized crime adapts rapidly to formal regulation.

Crypto is not legal tender in Brazil but it is regulated as a 'virtual asset' by financial authorities such as the Central Bank, the Special Department of Federal Revenue, the Financial Intelligence Unit and the Securities Commission. In December 2022, Law 14.478/2022 (also known as the Brazilian Virtual Assets Law) created a formal VASP framework, later strengthened through implementing regulations in 2025–2026. The system requires registration, AML/CTF controls, suspicious transaction reporting and enhanced supervision of exchanges. Yet broad regulation has not displaced criminal usage; instead, criminal actors increasingly rely on intermediaries, shell companies, OTC brokers and informal 'crypto-dollar' networks to limit visibility.

The Brazilian case confirms that crypto does not replace traditional organized crime finance but becomes embedded within sophisticated laundering architectures. Major criminal groups, particularly the Primeiro Comando da Capital (PCC), use crypto as a complementary infrastructure that accelerates cross-border transfers, reduces reliance on physical cash logistics and enables rapid layering between legal and illegal economies through hybrid systems involving banks, fintechs, OTC brokers, shell firms, mule accounts and crypto exchanges. Stablecoins are increasingly preferred because they preserve

dollar value while enabling rapid international movement, showing that organized crime adopts crypto primarily as a financial optimization tool rather than as a purely pseudonymous technology.

Meanwhile, Brazil's large retail crypto market provides camouflage for criminal transactions within substantial legitimate transaction volumes. Although Brazilian authorities have comparatively advanced investigative capabilities, important gaps remain in crypto custody, asset management and inter-agency coordination, meaning that while transactions can often be traced effectively, the seizure and management of crypto assets remains difficult.

Several extensive and high-profile cases have pointed to a professionalized and complex crypto and crime nexus in the country. The Lusocoin investigation allegedly involved more than BRL 50 billion (about US$9 billion) in suspicious transactions and resulted in the freezing of about BRL 3 billion (about US$540 million) in assets. Authorities alleged that the scheme used crypto brokers, shell companies and international transfers to disguise laundering activity linked to drug trafficking, smuggling, tax evasion and other illicit finance.[83]

The Crypto Pharaoh/GAS Consultoria case became one of Brazil's largest crypto Ponzi scandals, with authorities alleging that the scheme moved about BRL 38 billion (about US$6.8 billion) and affected hundreds of thousands of investors. GAS Consultoria promised fixed high-yield crypto returns while allegedly recycling investor funds and laundering proceeds through exchanges and shell structures. Authorities seized crypto wallets, luxury vehicles and property connected to the network.[84]

Another major case involved the PCC-linked 4TBANK structure, which Brazilian authorities alleged was used to launder hundreds of millions of dollars through fintech platforms and crypto operations, with approximately US$1.5 billion in assets frozen during the investigation. The case is conceptually important because it demonstrates the convergence of fintech infrastructure and organized crime. Rather than operating outside the financial system, criminal actors increasingly inserted themselves into emerging financial technologies.

Similar investigations involving shell companies, fintech entities and crypto-enabled financial layering reflect the same broader pattern: crypto is rarely the crime, but it is a mechanism for scaling, obscuring and internationalizing organized crime finance.[85]

Cryptocurrency is increasingly embedded in everyday transactions, reflecting its shift from a niche payment tool to a more widely used medium of exchange, including in illicit contexts. *© Marvin Recinos/AFP via Getty Images*

Colombia

In Colombia, crypto is primarily an extension of longstanding organized crime financial systems linked to narcotics trafficking, armed groups and cross-border laundering. The country has comparatively high retail adoption and significant informal crypto use. Crypto is not legal tender or currency, but it is treated legally as an intangible asset subject to taxation and seizure. The legal framework is strong: prosecutors can use ordinary criminal law, non-conviction-based confiscation and financial crime statutes to pursue crypto-enabled crime. The challenge is applying legal authority to increasingly decentralized and transnational financial ecosystems.

Colombia is an important example of post-cash criminal finance. Historically, organized crime depended heavily on bulk cash smuggling and dollar repatriation. Crypto reduces those logistical burdens. Stablecoins and Bitcoin allow drug revenues generated abroad to be transferred and reintegrated without physically transporting large quantities of cash. Criminal groups facilitate laundering through brokers, OTC traders, peer-to-peer exchanges and *ciberburreros* – digital couriers who move crypto across wallets and jurisdictions. The implication is significant: crypto decreases transaction costs and risks for transnational organized crime. It enables smaller, more fragmented criminal cells to move value globally without maintaining traditional banking relationships.

Colombian enforcement capacity is relatively advanced. The Attorney General's Office, the Directorate of Criminal Investigation, INTERPOL, the Technical Investigative Corps and specialized cyber units use blockchain tracing, financial intelligence, interception powers and digital forensics. Colombia also benefits from substantial international cooperation, especially with the US.

However, regulatory fragmentation persists. Many VASPs operate without consistent oversight, individual brokers are difficult to supervise, and crypto flows often move through informal or offshore channels outside effective visibility. The country therefore faces a paradox common throughout the region: authorities possess increasingly sophisticated investigative tools but criminal innovation moves faster than institutional adaptation.

Operation Gulupa

Operation Gulupa, led by Colombian and Spanish authorities, with the support of Europol, in 2025, revealed a sophisticated narcotics-trafficking and crypto-laundering network linked to the Clan del Golfo, Colombia's largest drug cartel. Investigators uncovered the use of shell companies, crypto exchanges and international virtual-asset intermediaries operating across several jurisdictions to move illicit proceeds derived from cocaine trafficking. Authorities reported seizures exceeding 5 tonnes of cocaine and identified about US$46 million in crypto-linked laundering flows. The case demonstrated how crypto was integrated into broader logistics, export and transnational trafficking systems rather than functioning independently.[86] ■

Ecuador

Ecuador is one of Latin America's most vulnerable crypto environments because of the interaction between dollarization, institutional weakness, regulatory contradictions and rapidly expanding organized crime, representing a 'perfect storm' of risk.

The country officially prohibits crypto as a payment method, yet simultaneously recognizes VASPs within AML/CTF reforms. This contradiction has created a large grey market in which crypto is heavily used but minimally supervised. Because Ecuador operates in US dollars, criminal groups avoid many exchange-stage laundering problems common elsewhere in Latin America since there is no need to convert local currency into dollars before entering global crypto markets. Criminal groups can move proceeds from extortion, cocaine trafficking, illegal mining or kidnapping directly into USDT-based systems.[87]

Overall, the national enforcement picture is weak. Ecuadorian authorities possess broad legal authority but operational capacity is limited. Prosecutors and police lack blockchain analytics software, 'cold-storage' facilities (secure offline systems used to store seized cryptocurrency assets), specialist hardware and advanced training. There are also suggestions of corruption and criminal infiltration of financial intelligence structures, undermining trust and enforcement effectiveness.

Panama

Panama is less a domestic organized crime producer and more a strategic financial transit jurisdiction. It permits crypto ownership and transactions but has no comprehensive crypto law or VASP supervisory framework. There is no dedicated supervisory authority, no consistent AML/CTF reporting obligation, and limited financial intelligence on crypto flows. Crypto is treated as a private digital asset rather than currency. This ambiguity creates a permissive environment in which legitimate finance, offshore corporate structures and illicit crypto flows coexist.

Panama illustrates how crypto-enabled organized crime benefits from financial opacity rather than technological anonymity. The country's importance comes from its corporate secrecy, territorial tax system, dollarized economy and historical role as a regional financial hub. Criminal actors exploit these structural conditions using crypto as an additional layer of concealment and mobility. Rather than replacing offshore finance, crypto enhances Panama's role as an intermediary node connecting Latin American organized crime with global financial systems.

Investigative agencies can prosecute fraud and money laundering under ordinary criminal law, but operational capacity is limited in highly technical cases involving mixers, cross-chain transfers or offshore exchanges. Panamanian authorities depend heavily on international cooperation, foreign regulators and private blockchain-analysis firms.

The Billions Trade Club case involved a large Ponzi scheme launched in 2022 by Marco Galbiati.[88] It promised monthly returns of 6–9 per cent through crypto trading and coaching services paid in USDT. About 40 000 victims were affected and more than US$300 million was generated. Panama served as a financial hub because of its looser regulatory environment. In 2025, authorities seized 32 properties, luxury vehicles, cash and electronic equipment linked to the fraud, and Galbiati was detained in Italy pursuant to a Panamanian arrest warrant.[89]

Another Panama-linked case, Crypto Capital, is conceptually important because it illustrates the convergence of mainstream crypto infrastructure and opaque transnational financial networks. Founded in Panama in 2013, Crypto Capital allegedly operated as a shadow payment processor and intermediary connecting crypto exchanges with fiat banking systems through shell companies, pooled accounts and informal cross-border financial arrangements. According to an independent digital news website, the company reportedly serviced major exchanges, while investigators alleged that associated networks laundered proceeds linked to Colombian narcotics trafficking.[90] Founder Iván Manuel Molina Lee was arrested in Greece and extradited to Poland in 2019 in connection with money-laundering investigations.[91]

Regional implications

Cryptocurrency is becoming deeply integrated into Latin America's organized crime economies, primarily as a tool to optimize and internationalize existing illicit financial systems rather than replace them. Crypto enables faster, cheaper and more flexible cross-border value transfers, reduces reliance on bulk cash movement, and facilitates the blending of licit and illicit financial activity. Crypto-related criminality is shaped less by technology than by underlying structural conditions such as dollarization, offshore financial systems, weak oversight, corruption vulnerabilities and large informal economies.

Criminal actors increasingly combine crypto with shell companies, fintech platforms, brokers and traditional laundering networks, creating hybrid financial ecosystems that are harder to detect and disrupt. Stablecoins seem particularly important because they provide dollar-denominated value storage and rapid international mobility.

A key regional challenge is the growing gap between criminal adaptation and state capacity. Even where legal frameworks and investigative tools are relatively advanced, enforcement agencies struggle with regulatory fragmentation, technical expertise, asset seizure and cross-border coordination, while organized crime networks adapt rapidly across jurisdictions and exploit inconsistencies in supervision and enforcement.

SMART CONTRACTS AS TRANSNATIONAL ORGANIZED CRIME ENABLERS

As decentralized finance ecosystems expand, organized crime and cybercriminal actors are increasingly exploiting the vulnerabilities of smart contracts, digital asset platforms and key management systems. The Forsage case and the Resolv hack illustrate how crypto-enabled crime is developing beyond laundering and illicit payments towards more technically sophisticated forms of financial exploitation operating at transnational scale. They also demonstrate how decentralized systems can facilitate rapid movement of illicit proceeds while complicating oversight, attribution and enforcement.

The Forsage case

Forsage was a DeFi scheme launched in early 2020, operating initially on the Ethereum blockchain before expanding to Binance Smart Chain and Tron. At its peak it was one of the biggest actors within the Ethereum chain.[92] Marketing itself as a 'smart contract' platform that enabled users to earn passive income through peer-to-peer transactions without intermediaries, it instead functioned as a classic pyramid scheme: participants paid fees to join and were incentivized to recruit new members, with returns almost entirely dependent on continuous inflows of new users. It spanned numerous countries, including the US, Russia, Georgia and Indonesia.[93]

In February 2023, a US grand jury in the District of Oregon charged four founders of Forsage for their involvement in a global Ponzi scheme that raised about US$340 million from investors.[94] This was the first case in which law enforcement pursued criminal charges in connection with a DeFi-based Ponzi scheme.[95] Forsage attracted millions of participants globally, focusing on South East Asia, Africa and eastern Europe, by promoting the perception of legitimacy through blockchain technology and claims of decentralization.

The transparency of Forsage's code and the visibility of its transactions on the blockchain provided an unprecedented level of detail for researchers and prosecutors to dissect the workings of the pyramid scheme, with early research estimating that 88 per cent of users suffered losses.[96] Moreover, the overt use of promotional videos and social media provided clear examples of how the Ponzi scheme's marketing strategy operated.

Despite its purported decentralized structure, investigators found that a small group of developers controlled key aspects of Forsage and profited significantly from user deposits. Most participants incurred losses, while a small percentage of early entrants captured most of the gains.[97]

The outcome of Forsage was a combination of regulatory enforcement, criminal prosecution and the effective collapse of the scheme. The 2023 indictments of key founders on charges including conspiracy to commit wire fraud reflect a shift towards treating large-scale crypto fraud as serious organized financial crime. The case shows how crypto-based platforms can facilitate traditional Ponzi schemes at global scale, leveraging smart contracts and online networks to evade oversight and prolong operation. It also demonstrates that global law enforcement is increasingly looking to crypto activity as a key enabler of serious and organized crime.[98]

The Resolv hack

The Resolv hack involved an attacker using a compromised private key to fraudulently mint about 80 million USR tokens without proper collateral, effectively creating value out of nothing.[99] The attacker then rapidly converted these illegitimate tokens into real assets, moving them through liquidity pools and swapping them into more stable cryptocurrencies before consolidating the proceeds into Ether. About US$23 million was extracted in a short period, before intervention was possible.[100]

The theft did not occur by breaking the blockchain. Instead, the attackers gained control over a privileged key that authorized transactions the system treated as valid, allowing them to drain real value using artificially created tokens and debasing the underlying value of the USR tokens. The weakness was in how the system was managed behind the scenes.[101]

The Resolv hack illustrates how criminal actors can exploit vulnerabilities within increasingly complex digital financial systems. It reflects a broader shift towards highly technical, coordinated operations targeting the intersection of blockchain infrastructure, cloud services and key management systems. Such attacks require specialized expertise, planning and rapid execution, characteristics commonly associated with professionalized cybercriminal networks.

The case also highlights the attractiveness of decentralized finance environments for illicit activity. These systems enable rapid cross-border transfers with limited friction, facilitating the concealment and movement of illicit proceeds. More broadly, the Resolv hack demonstrates how cyber-enabled financial exploitation is becoming an increasingly important dimension of organized crime, where a single compromised credential or security failure can generate substantial gains. This creates growing challenges for enforcement, requiring advanced technical defences and stronger international coordination.

At the same time, it remains unconfirmed whether the Resolv hack was carried out by organized crime. In cyber and crypto-related incidents, attacks of this scale can sometimes be conducted by a single highly skilled actor. However, operations involving sophisticated planning, rapid execution and subsequent laundering efforts are also consistent with methods commonly used by organized cybercriminal groups. The case should therefore be understood as indicative of shifting organized crime methodologies, rather than definitive proof of organized crime involvement.[102]

THE PROMISES AND PITFALLS OF ENFORCEMENT

In principle, blockchain transactions are publicly recorded; in practice, identifying the individuals behind transactions requires advanced analytical tools, specialized expertise and significant time investment. Even relatively unsophisticated actors using traceable assets such as Bitcoin can exploit basic obfuscation techniques, such as the use of several wallets, exchanges or intermediary services, to complicate attribution. As a result, the investigative burden is shifted onto authorities, which must piece together fragmented digital trails across jurisdictions and platforms. This makes crypto-enabled crime not inherently untraceable but operationally demanding to investigate at scale.

These challenges are compounded by constraints in manpower and resources that affect not only less developed jurisdictions but also law enforcement agencies across Europe and the UK. Effective cryptocurrency investigations require highly trained personnel capable of blockchain analysis, digital forensics and financial intelligence work, skills that are in limited supply. Moreover, such investigations are often resource intensive and time consuming, reducing the capacity of agencies to respond to a growing volume of cases.

Even where legal frameworks and regulatory tools are in place, the ability to operationalize them is uneven, with agencies facing backlogs, limited technical infrastructure and competing priorities. Consequently, the gap between the theoretical traceability of cryptocurrencies and the practical realities of enforcement remains a significant vulnerability in the response to crypto-enabled crime.

Another emerging dimension of crypto-enabled crime is the rise of informal 'mercenary' blockchain investigations and vigilante-style financial tracking. After several major cryptocurrency thefts linked to North Korean hacking groups, including the 2025 Bybit hack, crypto firms increasingly turned to independent blockchain analysts, amateur investigators and bounty hunters to trace stolen funds across wallets and decentralized exchanges.

Bybit publicly launched a bounty programme offering rewards to people who could identify and help freeze stolen assets, effectively outsourcing elements of financial investigation and asset recovery to a decentralized network of private actors.[103] This reflects a broader shift in which blockchain surveillance and financial enforcement are no longer conducted solely by states or regulated institutions, but increasingly by private companies, freelance investigators and online vigilantes motivated by financial incentives. While these efforts can support asset recovery, they also blur the line between law enforcement, private security and opportunistic cyber-mercenary activity, contributing to the emergence of a largely unregulated ecosystem of bounty hunting and quasi-vigilante justice in the cryptocurrency space.

CONCLUSION

Cryptocurrencies are transforming organized crime groups and state-linked actors by embedding digital assets within their operational and financial infrastructures. As a result, the longstanding 'follow the money' investigative paradigm is increasingly strained, while law enforcement agencies face growing demands for specialized expertise, technological capacity and sustained international cooperation.

Addressing these challenges will require a fundamental recalibration of law enforcement and regulatory responses. Incremental reforms are unlikely to keep pace with the speed and adaptability of crypto-enabled criminal ecosystems. Instead, more coordinated and resource-intensive approaches are needed, combining enhanced regulatory harmonization, targeted enforcement against key facilitators, and deeper collaboration between public authorities and private sector actors.

Without such efforts, existing gaps in oversight, capability and cooperation risk being further exploited, allowing crypto-enabled illicit markets to expand and mature. The trajectory is clear: unless matched by equally adaptive and coordinated responses, the continued development of cryptocurrency will further entrench its role at the centre of transnational organized crime.

Recommendations

- Establish specialized crypto investigation units within national law enforcement agencies, equipped with blockchain analytics capabilities, digital asset seizure expertise and dedicated cyber-financial intelligence functions. The increasing technical sophistication of crypto-enabled crime means governments should treat these units as long-term institutional priorities rather than ad hoc cybercrime initiatives.
- Strengthen cross-border judicial cooperation mechanisms, including joint investigation teams and streamlined mutual legal assistance procedures tailored to cryptocurrency investigations. As crypto-enabled criminality operates transnationally by design, fragmented national enforcement approaches are increasingly ineffective.
- Mandate real-time information sharing between regulators, financial intelligence units and law enforcement agencies on suspicious crypto transactions, particularly those involving exchanges, stablecoins, mixers, OTC brokers and cross-chain transfers. The speed at which illicit crypto assets can be moved and layered means faster intelligence exchange is essential.

- Enhance regulatory oversight and licensing enforcement of VASPs, ensuring consistent AML/CTF compliance standards across jurisdictions. Regulatory arbitrage and uneven enforcement continue to allow exchanges and intermediaries to function as gateways between illicit and licit finance.
- Develop coordinated international enforcement strategies targeting high-risk exchanges and laundering facilitators, including synchronized sanctions, asset freezes, domain seizures and coordinated compliance actions. Enforcement should focus not only on criminal users but on the systemic infrastructures enabling large-scale illicit financial flows.
- Expand legal and regulatory frameworks to address unhosted wallets, peer-to-peer transactions and decentralized financial environments that fall outside many traditional monitoring systems. These should include clearer obligations on beneficial ownership, suspicious activity reporting and cross-chain transaction tracing.
- Invest in sustained training and capacity building for investigators, prosecutors and judges on cryptocurrency-related evidence, blockchain analytics and digital asset seizure procedures. Many jurisdictions face a significant gap between the theoretical traceability of blockchain transactions and practical enforcement capacity.
- Create permanent public-private partnerships with blockchain analytics firms, cybersecurity companies and financial institutions to improve detection of laundering networks, fraud schemes and sanctions evasion systems. The pace of technological change means governments increasingly depend on private sector expertise and intelligence.
- Standardize evidentiary, seizure and asset management procedures for digital assets across jurisdictions to improve asset recovery and reduce delays caused by differing legal interpretations. Effective crypto enforcement requires not only tracing illicit assets but securing and managing them operationally.
- Prioritize disruption of crypto-enabled laundering ecosystems rather than isolated transactions or low-level actors. Enforcement strategies should focus on systemic facilitators such as OTC brokers, Chinese-language laundering systems, shadow banking structures and cross-border conversion networks that underpin large-scale organized criminal finance.
- Address the persistent lack of political will on crypto regulation and enforcement. In many jurisdictions, economic competition, lobbying pressures and political narratives on innovation have contributed to weak oversight and regulatory hesitation. Governments should recognize crypto-enabled illicit finance as a systemic organized crime and national security issue rather than solely a technology or investment matter.
- Expand public awareness and prevention campaigns addressing the risks and harms associated with cryptocurrencies, particularly fraud, scams and organized criminal exploitation. Public discourse on crypto is often dominated by narratives of rapid wealth generation and financial disruption, which can obscure the scale of associated criminality and victimization. Governments, regulators and civil society should support initiatives that improve digital financial literacy, deglamourize speculative crypto culture, and increase awareness of fraud risks and broader social harms.

NOTES

1 Chainalysis, The Chainalysis 2026 Crypto Crime Report, https://www.chainalysis.com/reports/crypto-crime-2026.

2 Digital Watch, FBI reports $9.3 billion lost to cryptocurrency fraud in 2024, Geneva Internet Platform, 25 April 2025, https://dig.watch/updates/fbi-reports-9-3-billion-lost-to-cryptocurrency-fraud-in-2024.

3 Ibid.

4 US Attorney's Office, Chairman of Prince Group indicted for operating Cambodian forced-labor scam compounds engaged in cryptocurrency fraud schemes, 14 October 2025, https://www.justice.gov/usao-edny/pr/chairman-prince-group-indicted-operating-cambodian-forced-labor-scam-compounds-engaged.

5 Jordan Pandy, Bitcoin ATM fraud hits record $333 million: FBI, Business Insider, 3 January 2026, https://www.businessinsider.com/Bitcoin-crypto-atm-fraud-rises-fbi-333-million-stolen-2026-1.

6 Ibid.

7 Europol, New major interventions to block encrypted communications of criminal networks, 12 March 2021, https://www.europol.europa.eu/media-press/newsroom/news/new-major-interventions-to-block-encrypted-communications-of-criminal-networks.

8 US Attorney's Office, Sky global executive and associate indicted for providing encrypted communication devices to help international drug traffickers avoid law enforcement, 12 March 2021, https://www.justice.gov/usao-sdca/pr/sky-global-executive-and-associate-indicted-providing-encrypted-communication-devices; Frédéric Zalac and Paul Émile d'Entremont, The crime messenger, CBC, 26 November 2024, https://www.cbc.ca/newsinteractives/features/the-crime-messenger.

9 TRM Labs, Shadow Bankers, 22 May 2025, https://www.trmlabs.com/reports-and-whitepapers/shadow-bankers; Gonzalo Saiz Erausquin, The shadow crypto economy feeding Russia's war machine, Royal United Services Institute, 11 May 2026, https://www.rusi.org/explore-our-research/publications/commentary/shadow-crypto-economy-feeding-russias-war-machine.

10 Spencer Woodman et al, Crypto giants moved billions linked to money launderers, drug traffickers and North Korean hackers, International Consortium of Investigative Journalists, 17 November 2025, https://www.icij.org/investigations/coin-laundry/cryptocurrency-exchanges-binance-okx-money-laundering-crime.

11 FATF, Targeted report on stablecoins and unhosted wallets, March 2026, https://www.fatf-gafi.org/content/dam/fatf-gafi/publications/targeted-report-on-stablecoins-and-unhosted-wallets.pdf.coredownload.inline.pdf.

12 TRM Labs, 2026 crypto crime report, 28 January 2026, https://www.trmlabs.com/reports-and-whitepapers/2026-crypto-crime-report.

13 FATF, Targeted report on stablecoins and unhosted wallets, March 2026, https://www.fatf-gafi.org/content/dam/fatf-gafi/publications/targeted-report-on-stablecoins-and-unhosted-wallets.pdf.coredownload.inline.pdf.

14 These networks acted as hybrid laundering infrastructures, linking physical cash from illicit activities with digital assets such as Tether. Criminal clients could swap cash for crypto and vice versa, bridging the gap between the conventional financial system and blockchain-based transactions. See Jamie MacColl and Kathryn Westmore, Operation Destabilise: Russia, organised crime and illicit finance, Royal United Services Institute, 6 November 2024, https://www.rusi.org/explore-our-research/publications/commentary/operation-destabilise-russia-organised-crime-and-illicit-finance.

15 US Treasury Financial Crimes Enforcement Network, FinCEN advisory on the use of Chinese money laundering networks by Mexico-based transnational criminal organizations to launder illicit proceeds, 28 August 2025, https://www.fincen.gov/system/files/2025-08/FinCEN-Advisory-CMLN-508.pdf.

16 TRM Labs, 2026 crypto crime report, 28 January 2026, https://www.trmlabs.com/reports-and-whitepapers/2026-crypto-crime-report.

17 *Financial Times*, Chinese brokers launder hundreds of millions for global crime groups, 27 June 2024, https://www.ft.com/video/cfb4c5c0-be2d-45f3-aba6-c9fa6da69a3d.
18 TRM Labs, Understanding the use of cryptocurrencies by cartels, 21 January 2025, https://www.trmlabs.com/resources/blog/understanding-the-use-of-cryptocurrencies-by-cartels.
19 Chainalysis, Crypto and the opioid crisis: What blockchain analysis reveals about global fentanyl sales, 7 March 2024, https://www.chainalysis.com/blog/cryptocurrency-fentanyl-analysis-2023.
20 John Collins, Crypto, crime and control: Cryptocurrencies as an enabler of organized crime, GI-TOC, 16 June 2022, https://globalinitiative.net/analysis/cryptocurrencies-crime.
21 TRM Labs, 2026 crypto crime report, 28 January 2026, https://www.trmlabs.com/reports-and-whitepapers/2026-crypto-crime-report.
22 Ibid.
23 IWF, 'On-demand premium access' to children's suffering as gangs reap profits from online sexual exploitation, 23 April 2026, https://www.iwf.org.uk/news-media/news/on-demand-premium-access-to-children-s-suffering-as-gangs-reap-profits-from-online-sexual-exploitation.
24 Taylor Herzlich, Cryptocurrency use explodes in human trafficking networks, online scams: report, *New York Post*, 16 February 2026, https://nypost.com/2026/02/16/business/use-of-cryptocurrency-explodes-in-human-trafficking-networks-online-scams-report.
25 Chainalysis, Human trafficking rings raking in crypto gains: report, *Asia Times*, 17 February 2026, https://asiatimes.com/2026/02/human-trafficking-rings-raking-in-crypto-gains-report.
26 IWF, 2025 annual data & insights report: Executive summary, 2025, https://www.iwf.org.uk/annual-data-insights-report-2025/executive-summary.
27 Europol, Global crackdown on Kidflix, a major child sexual exploitation platform with almost two million users, April 2025, https://www.europol.europa.eu/media-press/newsroom/news/global-crackdown-kidflix-major-child-sexual-exploitation-platform-almost-two-million-users.
28 Europol, Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe, July 2020, https://www.europol.europa.eu/media-press/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe.
29 Chainalysis, Organized crime shows high level of professionalization, low level of crypto sophistication, 2 May 2025, https://www.chainalysis.com/blog/organized-crime-crypto.
30 FATF, FATF report to the G20 finance ministers and central bank governors on so-called stablecoins, June 2020, https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-FATF-Report-G20-So-Called-Stablecoins.pdf.
31 FATF, Targeted report on stablecoins and unhosted wallets, March 2026, https://www.fatf-gafi.org/content/dam/fatf-gafi/publications/targeted-report-on-stablecoins-and-unhosted-wallets.pdf.coredownload.inline.pdf.
32 Organized Crime Dispatch (by GI-TOC), How the tech industry washes money for the world's deadliest crooks | Underworlds with Mark Shaw, YouTube, 2025, https://www.youtube.com/watch?v=WDwvBBkUMos.
33 A VASP is a business or entity that facilitates activities involving cryptocurrencies or other digital assets on behalf of others. According to the FATF, this includes services such as exchanges, wallet providers, and platforms that transfer or manage virtual assets. FATF, Updated guidance for a risk-based approach: Virtual assets and virtual asset service providers, October 2021, https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf.
34 European Commission, Crypto-assets, 20 May 2026, https://finance.ec.europa.eu/digital-finance/crypto-assets_en.
35 Sebastian J Barling et al, UK legal framework for crypto takes shape with draft legislation and three new FCA consultations, Skadden, 18 December 2025, https://www.skadden.com/insights/publications/2025/12/uk-legal-framework-for-crypto.
36 See Liv McMahon, Trump pardons Binance founder Changpen Zhao, BBC, 23 October 2025, https://www.bbc.com/news/articles/cly1qrl9l1qo; Spencer Woodman et al, Crypto giants moved billions linked to money launderers, drug traffickers and North Korean hackers, International Consortium of Investigative Journalists, 17 November 2025, https://www.icij.org/investigations/coin-laundry/cryptocurrency-exchanges-binance-okx-money-laundering-crime.
37 Ibid.
38 Patricia Kowsmann, Angus Berwick and Ben Foldy, Binance fired staff who flagged $1 billion moving to sanctioned Iran entities, *Wall Street Journal*, 23 February 2026, https://www.wsj.com/finance/currencies/binance-iran-sanctions-financing-staff-b1648133.
39 Ashley Belanger, Binance sues WSJ, panicked by gov't probes into sanctioned crypto transfers, Ars Technica, 11 March 2026, https://arstechnica.com/tech-policy/2026/03/binance-sues-wsj-over-report-sparking-government-probes-into-exchange.
40 Spencer Woodman et al, Crypto giants moved billions linked to money launderers, drug traffickers and North Korean hackers, International Consortium of Investigative Journalists, 17 November 2025, https://www.icij.org/investigations/coin-laundry/cryptocurrency-exchanges-binance-okx-money-laundering-crime.
41 Ibid.
42 C-SPAN, Jamie Dimon calls crypto tokens 'decentralized Ponzi schemes', 21 September 2022, https://www.c-span.org/video/?c5032117%2Fjamie-dimon-calls-crypto-tokens-decentralized-ponzi-schemes.

43 Katie Balevic, Jamie Dimon says Bitcoin is the crypto of choice for 'sex traffickers, money launderers, ransomware', Business Insider, 13 January 2025, https://www.businessinsider.com/jamie-dimon-Bitcoin-criticism-crypto-criminals-choice-2025-1.

44 George Hristov, Jamie Dimon crypto quotes & opinions 2026, Milk Road, accessed 25 March 2026, https://milkroad.com/influencers/jamie-dimon.

45 Federal Deposit Insurance Corporation, Update from the prudential regulators: rightsizing regulation to promote American opportunity, 26 February 2026, https://www.fdic.gov/news/speeches/2026/update-prudential-regulators-rightsizing-regulation-promote-american-opportunity.

46 GI-TOC, Compound crime: Cyber scam operations in Southeast Asia, 29 May 2025, https://globalinitiative.net/analysis/compound-crime-cyber-scam-operations-in-southeast-asia.

47 Proelium Law, Cryptocurrency regulation tracker, accessed 7 May 2026, https://proeliumlaw.com/cryptocurrency-regulation-tracker.

48 GI-TOC, Compound crime: Cyber scam operations in Southeast Asia, 29 May 2025, https://globalinitiative.net/analysis/compound-crime-cyber-scam-operations-in-southeast-asia.

49 Ibid.

50 GI-TOC, Cryptocurrency and criminal capture in the Central African Republic, 17 December 2025, https://globalinitiative.net/analysis/behind-the-blockchain-cryptocurrency-and-criminal-capture-in-the-central-african-republic.

51 Ibid.

52 John Collins, Crypto, crime and control: Cryptocurrencies as an enabler of organized crime, GI-TOC, 16 June 2022, https://globalinitiative.net/analysis/cryptocurrencies-crime.

53 Ibid.

54 See Chainalysis, crypto crime reports, 2023–2026.

55 Andy Greenberg, Most criminal cryptocurrency funnels through just 5 exchanges, *Wired*, 26 January 2023, https://www.wired.com/story/cryptocurrency-money-laundering-chainalysis-report.

56 GI-TOC, unpublished Eurasia Observatory research, 2025.

57 David Kirichenko, Crypto boosts Ukraine – and Russia, Center for European Policy Analysis, 5 January 2024, https://cepa.org/article/crypto-boosts-ukraine-and-russia.

58 John Collins, Crypto, crime and control: Cryptocurrencies as an enabler of organized crime, GI-TOC, 16 June 2022, https://globalinitiative.net/analysis/cryptocurrencies-crime.

59 Jake Rudnitsky, Putin says he accepts crypto's role in making payments, Bloomberg, 14 October 2021, https://www.bloomberg.com/news/articles/2021-10-14/putin-defends-cryptocurrencies-amid-global-regulation-push.

60 Max Seddon and Eva Szalay, Russia's central bank proposes ban on crypto trading and mining, *Financial Times*, 20 January 2022, https://www.ft.com/content/54433e18-7442-4804-9fec-f0f934bf8b4e.

61 Bloomberg, Russia races to legalize crypto as sanctions weigh on firms (1), 30 July 2024, https://news.bloomberglaw.com/crypto/russia-races-to-legalize-crypto-as-sanctions-weigh-on-companies.

62 Reuters, Russian central bank proposes wealthy individuals be allowed to invest in crypto, Reuters, 12 March 2025, https://www.reuters.com/technology/russian-central-bank-proposes-wealthy-individuals-be-allowed-invest-crypto-2025-03-12.

63 Victor, Russia plans crypto rules with retail investor limits, Altcoin Buzz, 29 January 2026, https://www.altcoinbuzz.io/cryptocurrency-news/russia-plans-crypto-rules-with-retail-investor-limits.

64 MEXC, Russia considers simplified licensing path for bank-run crypto exchanges, Bitcoin Magazine, 6 March 2026, https://www.mexc.com/news/868709; Reuters, Russia's Sberbank plans crypto-backed loans to corporate clients, 5 February 2026, https://www.reuters.com/sustainability/boards-policy-regulation/russias-sberbank-plans-crypto-backed-loans-corporate-clients-2026-02-05.

65 US Department of the Treasury, Treasury sanctions Russia-based Hydra, world's largest darknet market, and ransomware-enabling virtual currency exchange Garantex, 5 April 2022, https://home.treasury.gov/news/press-releases/jy0701.

66 TRM Labs, Grinex emerges as likely Garantex rebrand, 28 April 2025, https://www.trmlabs.com/resources/blog/grinex-emerges-as-likely-garantex-rebrand.

67 TRM Labs, The takedown of Garantex: A notorious crypto exchange's role in illicit finance, 5 March 2025, https://www.trmlabs.com/resources/blog/the-takedown-of-garantex-a-notorious-crypto-exchanges-role-in-illicit-finance.

68 TRM Labs, Grinex emerges as likely Garantex rebrand, 28 April 2025, https://www.trmlabs.com/resources/blog/grinex-emerges-as-likely-garantex-rebrand.

69 Ibid.

70 Discussions with GI-TOC experts.

71 John Kennedy et al, Russia's use of crypto schemes, RAND, 7 August 2025, https://www.rand.org/pubs/commentary/2025/08/russias-use-of-crypto-schemes.html.

72 Ibid.

73 Chainalysis Team, 2026 Crypto Crime Report introduction, *Chainalysis*, 8 January 2026, https://www.chainalysis.com/blog/2026-crypto-crime-report-introduction/.

74 Chainalysis Team, Inside Iran's growing $7.8 billion crypto ecosystem, Chainalysis, 15 January 2026, https://www.chainalysis.com/blog/iranian-crypto-activity-geopolitical-tensions-2026/.

75 John Kennedy et al, Russia's use of crypto schemes, RAND, 7 August 2025, https://www.rand.org/pubs/commentary/2025/08/russias-use-of-crypto-schemes.html.

76 Polina Ivanova and Jacob Judah, Russian crypto payment system expands into Africa, *Financial Times*, 6 April 2026,

https://www.ft.com/content/a9de2bb5-7bbf-4d04-9424-25d4b9cda2b6.

77 John Kennedy et al, Russia's use of crypto schemes, RAND, 7 August 2025, https://www.rand.org/pubs/commentary/2025/08/russias-use-of-crypto-schemes.html.

78 Lindsey Kennedy and Nathan Paul Southern, Where does North Korea get its cash?, GI-TOC, 31 March 2025, https://globalinitiative.net/analysis/where-does-north-korea-get-its-cash.

79 FBI, North Korea responsible for $1.5 billion Bybit hack, 26 February 2025, https://www.fbi.gov/investigate/cyber/alerts/2025/north-korea-responsible-for-1-5-billion-bybit-hack.

80 ACAMS, Understanding North Korea's $1.5B Bybit theft, with Geoff White, 20 March 2025, https://www.acams.org/en/opinion/understanding-north-koreas-1-5-b-bybit-theft-with-geoff-white.

81 Ibid.

82 This section draws extensively from GI-TOC, Cryptocurrencies in Latin America research note, forthcoming.

83 TRM Labs, Brazil's Federal Police dismantle $540 million crypto laundering network in 'Operation Lusocoin', 10 October 2025, https://www.trmlabs.com/resources/blog/brazils-federal-police-dismantle-540-million-crypto-laundering-network-in-operation-lusocoin.

84 Binance Square, Police officer and three police officers involved in the Bitcoin Pharaoh case are arrested, 21 December 2024, https://www.binance.com/en/square/post/17863437560898.

85 Demian Bio, Brazil's largest cartel is laundering drug money through a fintech company and public transport contracts, Latin Times, 3 December 2024, https://www.latintimes.com/brazils-largest-cartel-laundering-drug-money-through-fintech-company-public-transport-contracts-567687.

86 Chainalysis, How Colombia's National Police dismantled the Clan del Golfo's 'Black Jack' crypto laundering network, 17 October 2025, https://www.chainalysis.com/blog/columbia-national-police-dismantled-crypto-laundering-network.

87 GI-TOC, Global Organized Crime Index 2025, https://ocindex.net/report/2025.

88 Newsroom Panama, Cryptocurrency scam that crossed borders into Panama, 2 March 2025, https://newsroompanama.com/2025/03/02/cryptocurrency-scam-that-crossed-borders-into-panama.

89 Ibid. See also Juan Manuel Díaz, *Detienen a italiano implicado en estafa a través de criptomonedas; fiscalía solicita extradición*, *La Prensa*, 19 February 2025, https://www.prensa.com/judiciales/detienen-a-italiano-implicado-en-estafa-a-traves-de-criptomonedas-fiscalia-solicita-extradicion/.

90 Cali Haan, Crypto Capital president, banker to Bitfinex, Kraken, Binance and BitMEX, held in Poland for alleged money laundering, Crowdfund Insider, 27 October 2019, https://www.crowdfundinsider.com/2019/10/153346-crypto-capital-president-banker-to-bitfinex-kraken-binance-and-bitmex-held-in-poland-for-alleged-money-laundering/.

91 Landon Manning, Crypto Capital president arrested, Bitfinex releases statement, Bitcoin Magazine, 25 October 2019, https://bitcoinmagazine.com/culture/crypto-capital-president-arrested-bitfinex-releases-statement.

92 Tyler Kell et al, Forsage: Anatomy of a smart-contract pyramid scheme, arXiv, 24 August 2021, https://doi.org/10.48550/arXiv.2105.04380.

93 US Securities and Exchange Commission, SEC charges eleven individuals in $300 million crypto pyramid scheme, 1 August 2022, https://www.sec.gov/newsroom/press-releases/2022-134.

94 US Department of Justice, Forsage founders indicted in $340m DeFi crypto scheme, 22 February 2023, https://www.justice.gov/archives/opa/pr/forsage-founders-indicted-340m-defi-crypto-scheme.

95 Ari Redbord, US DOJ charges four Russian-nationals for role in DeFi Ponzi scheme Forsage, TRM Labs, 13 June 2023, https://www.trmlabs.com/resources/blog/law-enforcement-spotlight-forsage.

96 Tyler Kell et al, Forsage: Anatomy of a smart-contract pyramid scheme, arXiv, 24 August 2021, https://doi.org/10.48550/arXiv.2105.04380.

97 Ibid.

98 US Department of Justice, US Dep. Justice, 'Forsage Founders Indicted in $340M DeFi Crypto Scheme'.

99 USR tokens are specific to the Resolv protocol. They are not a widely used or independent cryptocurrency but a native stablecoin within Resolv's DeFi system. Their value and function depend on the Resolv platform's design, particularly its collateral and stabilization mechanisms. USR has no standalone significance outside that ecosystem and its stability relies on the protocol operating correctly. When the exploit occurred, the integrity of the system was undermined, which is why USR rapidly lost its value.

100 Liam Kelly, 'Resolv Labs Stablecoin Plummets 80% as Exploiter Mints Millions in Unbacked USR Tokens', DL News, accessed 23 March 2026, https://www.dlnews.com/articles/defi/resolve-labs-stablecoin-falls-80-per-cent-as-millions-tokens-minted/.

101 Ibid.

102 For an overview of cybercrime and organized crime terminological debates see: Mark Shaw et al, Organized crime and illicit markets: Understanding criminal connections between actors and economic forces, GI-TOC, forthcoming.

103 Lorenzo Franceschi-Bicchierai, Hacked crypto exchange Bybit offers $140m bounty to trace stolen funds, TechCrunch, 26 February 2025, https://techcrunch.com/2025/02/26/hacked-crypto-exchange-bybit-offers-140-million-bounty-to-trace-stolen-funds.

GLOBAL INITIATIVE
AGAINST TRANSNATIONAL ORGANIZED CRIME

ABOUT THE GLOBAL INITIATIVE

The Global Initiative Against Transnational Organized Crime is a global network with 800 Network Experts around the world. The Global Initiative provides a platform to promote greater debate and innovative approaches as the building blocks to an inclusive global strategy against organized crime.

www.globalinitiative.net