

Behind the Headlines:

Debunking Misconceptions of Cryptocurrency and Crime

Kristofer Doucette, Jennifer Jensen, Tonja Denny, Sydney Robertson, Isaac Rits, Adam Hill, Sean Swentkowski, Kellee Wicker

Science and Technology Innovation Program | Digital Assets Forum

February 2025



Overview

This paper examines the relationship between cryptocurrency and illicit finance, challenging prevalent misconceptions about their role in criminal behavior through four key findings:

- Misinformation about blockchain technology spreads rapidly and persistently, often outpacing factual understanding of its capabilities and limitations.
- There is no fundamental difference between traditional financial crime and cryptocurrency-enabled crime—criminals have simply added digital assets to their existing toolkits.
- Contrary to popular perception, blockchains are not opaque but rather provide unprecedented transparency, enabling groundbreaking successes in tracking and preventing illicit finance.
- While autocratic regimes do exploit cryptocurrency, their methods reveal more about their behavioral patterns than any inherent vulnerability in the technology.

Since the mining of the first Bitcoin in 2009, blockchain technologies have evolved from a niche experiment into a significant component of the global financial system, fundamentally transforming our ability to track and analyze financial flows. At the heart of misconceptions about cryptocurrency's involvement in financial crimes lies a crucial irony: the very transparency that allows us to measure cryptocurrency's use in illicit activity has contributed to negative perceptions about its role in criminal behavior. While blockchain analytics companies can definitively show that less than 1% of cryptocurrency transaction volume is connected to illicit activity, no comparable measurement exists for traditional financial systems. This data asymmetry has led to distorted public discourse about cryptocurrency's role in global financial crime. Through data-driven analysis, this paper demonstrates that while cryptocurrencies can be exploited for illegal purposes, they represent only a small fraction of global financial crime, while providing unprecedented insight into illicit financial activity that traditional finance, in its opacity, cannot match.

At the heart of misconceptions about cryptocurrency's involvement in financial crimes lies a crucial irony: the very transparency that allows us to measure cryptocurrency's use in illicit activity has contributed to negative perceptions about its role in criminal behavior.

Introduction to The Evolution and Misconceptions of Cryptocurrency

Blockchain technologies and cryptocurrencies, which emerged in 2009, have been frequently featured in mainstream media. This coverage is often accompanied by misconceptions, especially regarding their supposed connection to illicit activities. These misunderstandings influence public perceptions and regulatory approaches, hindering the industry’s development. According to data analysis of cryptocurrency transactions, less than 1% of all cryptocurrency transactions are illicit.¹

It is important to clarify that any money tainted by criminal activity, no matter how small, is not something any government or reputable institution wants in their financial system. Unfortunately, many concerns about cryptocurrency arise from exaggerated fears about its use by criminals, rogue nations, or money launderers. However, it is essential to understand that money, in any form, lacks an inherent agency; it cannot make decisions or produce outcomes on its own. Instead, individuals, entities, and the networks they form determine how money is utilized—whether legitimately for productive purposes, or for criminal activities. Just like physical cash, Venmo payments, gold bars, or municipal bonds, cryptocurrency holds value within our financial system. Like these other forms of value, cryptocurrency can be exploited by criminals.

Cryptocurrency has broad and consistently growing mainstream uses, and legitimate adoption continues to grow around the world. There is cryptocurrency activity in almost every country globally and the rate of adoption grows every year. The daily number of transactions continues to grow as well, as more users adopt the technology, with Bitcoin’s network alone averaging over 700,000 transactions per day. Cryptocurrency is now a permanent piece of global finance.

US dollars. (Avery Evans/Unsplash)



Credit cards. (JP Valery/Unsplash)



Bitcoin token. (Kanchanara/Unsplash)



Although the pace of general acceptance of new financial technology is slow, overall public judgements are swift and often rooted in biases. For example, a well-known news clip from 1993 covers a Burger King announcement stating it would begin accepting credit cards as a form of payment. The coverage includes several responses that range from disbelief and annoyance to excitement.² Thirty years later these reactions look outdated. The clip serves as a reminder of how perceptions of technological advances evolve over time. Similarly, when the first bitcoin block was mined on January 3, 2009, few could have anticipated the impact it would have on the global financial system.

However, as with any major technological innovation, cryptocurrency has attracted bad actors seeking to exploit its capabilities. This paper examines how misconceptions about cryptocurrency's role in illicit finance have evolved and reinforced other misconceptions. Several fundamental misconceptions have emerged in the course of this study, including: the false equivalence between measurable illicit activity when compared to traditional finance; media narratives built on incomplete blockchain analysis leading to misguided policy decisions; the misattribution of autocratic exploitation to technological flaws rather than regime behavior; the overlooked advantages blockchain transparency provides to law enforcement; and the tendency to blame cryptocurrency for systemic issues in cybersecurity and governance that predate its existence.

Understanding these misconceptions is crucial as cryptocurrency continues to evolve from a niche technology into an integral part of the global financial system. This report will explore how, through blockchain's unprecedented transparency, we have gained new capabilities for measuring and combating illicit activity, providing law enforcement with powerful tools while supporting legitimate innovation. This report also shares how this transparency, combined with proper understanding of the technology, offers a path forward that balances security with innovation in the global financial system.

Section 1: Data Transparency vs. Lack of Comparable Metrics in Traditional Finance

Many people incorrectly assume that the scale of financial crime involving cryptocurrency is larger than it actually is. The ability to measure illicit activity in financial systems is crucial for effective regulations and law enforcement, yet traditional financial systems remain largely opaque.

Blockchain technology's inherent transparency has created an unexpected paradox: the ability to precisely measure cryptocurrency's role in illicit finance has contributed to public misconceptions about its use in criminal activity. When illicit transactions are detected on the blockchain, they become highly visible, creating an impression of widespread criminal use that data does not support. This visibility bias has led to several persistent myths that shape public perception and policy decisions, which will be explored throughout this report.

The Anonymity Myth

The myth that “cryptocurrency is anonymous and untraceable” represents a fundamental misunderstanding of blockchain technology. In reality, blockchain creates an immutable, publicly viewable record of every transaction that surpasses traditional financial transparency. Unlike banking records siloed within institutions, blockchain transactions create permanent public records allowing investigators to track fund histories, identify connected wallets, and monitor money flows in real-time. While blockchain addresses are pseudonymous, offering users a layer of privacy and protection, this pseudonymity does not equate to full anonymity, and law enforcement can leverage this transparency for groundbreaking insights into financial networks. This core capability of blockchain will feature prominently throughout this report, as it is a central component of how law enforcement can respond to illicit activity in cryptocurrency and is essential to understanding the realities of how criminals can and cannot use crypto for scams, skirting sanctions, theft, and more. More detail on the level of user information accessible through analysis and investigation follows in the sections below.

The Criminal Usage Myth

The widespread belief that “most cryptocurrency is used for criminal activity” stands in stark contrast to empirical evidence. Blockchain analytics consistently show that less than 1% of all cryptocurrency transactions are connected to illegal activities, with identified illicit transactions totaling \$24.2 billion out of \$2.4 trillion in total volume in 2023. This percentage is significantly lower than estimates of funds laundered annually through traditional financial systems. Cash remains the preferred method of transaction in criminal operations due to it being untraceable and universally accepted. In the EU, cash accounts for 34% of all suspicious activity reports within their financial system.³

Understanding Blockchain’s Capabilities

Blockchain technology represents a fundamental shift in financial transparency, establishing an ability to track and analyze monetary flows that has no analog in the legacy systems of banks. Unlike traditional financial systems, where transaction data remains isolated within individual institutions, blockchain creates a permanent, immutable, and publicly accessible record of all its transactions. This architectural difference provides a revolutionary foundation for detecting and analyzing illicit financial activity.

It is crucial to understand how blockchain’s fundamental architecture enables this revolutionary transparency and tracking capability. At its core, blockchain technology operates on a digital, decentralized ledger system that records transactions in a secure and transparent manner. Unlike traditional financial records, which are often controlled by a single authority, the blockchain operates through a network of nodes, each maintaining a complete copy of the ledger. This decentralized nature eliminates the need for intermediaries, as transactions are verified by the network itself. Every transaction is stored as a “block,” which is linked to the previous one, forming a continuous “chain” of information that dates back to the very first transaction. This structure ensures that all records are accurate, synchronized, and viewable across the network, fostering a high level of trust in the recorded data.

One of the most distinctive features of blockchain is its immutability—once a transaction is recorded, it cannot be altered or deleted. This permanence is achieved through cryptographic techniques and consensus mechanisms, which secure each block against tampering. Any attempt to change a past transaction would require altering every subsequent block across all network nodes, making such modifications practically impossible. As a result, blockchain technology provides an unchangeable history of all transactions, with every transfer beginning with its inception publicly accessible and open to scrutiny. Users can track the entire lifecycle of an asset at any time.

...Blockchain technology provides an unchangeable history of all transactions, with every transfer beginning with its inception publicly accessible and open to scrutiny.

Tracking and Analysis in Practice

This public availability of all transactions provides extraordinary insight into financial flows and transforms how illicit finance can be investigated. Blockchain analysis companies can identify wallet owners through intelligence operations, tag those wallets, and enable anyone with access to the technology to see the history of transactions sent to those wallets. For instance, when a scammer convinces someone to send cryptocurrency, law enforcement can

analyze the receiving address and all associated transactions. They can trace both the source and destination of funds by “following the money” to lead to more wallets. Through subsequent subpoenas to relevant services, law enforcement can obtain personal identifiable information to establish the scammer’s identity. Unlike traditional financial investigations, this complete transaction history remains available indefinitely, allowing investigators to reconstruct money flows even years after transactions.

In contrast, tracking illicit activity in traditional finance has historically proven far more challenging, largely due to the siloed nature of financial institutions. Unlike blockchain’s transparency, conventional financial systems maintain transaction records within individual banks or institutions, significantly limiting visibility across the broader network of financial activity. When a bank suspects fraudulent activity, it must rely on internal records and coordinate with other institutions to gain insight into the larger financial flow. This process requires time-consuming legal requests and cooperation from multiple parties, each with its own data-sharing policies and jurisdictional boundaries. The complexity of building a complete picture of financial flows multiplies exponentially with cross-border transactions and multiple intermediaries, making it exceptionally difficult to identify broader patterns of suspicious activity.

The Measurement Advantage

The scale of illicit activity in traditional finance remains largely unknown due to it operating in essentially a statistical dark zone. The most widely cited figure comes from the United Nations Office of Drugs and Crime (UNODC), which estimates that between 2%-5% of global GDP is associated with money laundering. However, a recent study by University of Maryland Distinguished University Professor Peter Reuter and Dutch economist Joras Ferwerda from Utrecht University found fundamental flaws in this estimate. Their analysis found that the UNODC study relied heavily on questionable assumptions and insufficient data, leading to unreliable conclusions.⁴

This flawed UNODC estimate persists because accurately quantifying global money laundering and financial crime is nearly impossible within traditional systems. National risk assessments suffer from poor data quality, inconsistent methodologies across countries, and vague definitions of terms like “threats” and

Neon dollar sign at night in Moscow. (Aleksandr Popov/Unsplash)



“vulnerabilities.” Many assessments are treated primarily as compliance exercises, with limited participation from risk assessment professionals and little integration of broader research. The fragmentation of law enforcement agencies, often withholding high-level crime statistics, creates blind spots that obscure the true scale of financial crime.

This uncertainty in traditional finance stands in stark contrast to blockchain’s ability to provide precise measurements of illicit activity. One percent of cryptocurrency transactions are attributed to illicit activity, a measurement that can be independently verified through blockchain analysis. This innovative technology offers increasingly sophisticated tools for detecting criminal activity through pattern analysis. Though this 1% figure represents a “lower bound” of illicit activity, blockchain’s baseline immutability and openness also allows newly identified illicit transactions to be quickly analyzed and incorporated into updated statistics—a dynamic capability impossible in traditional finance.

This transparency paradox—where better visibility into cryptocurrency crime has sometimes led to negative perceptions—demonstrates the need for a more comprehensive understanding of how these technologies can actually enhance our ability to combat financial crime. The ability to track and analyze blockchain transactions represents a significant advancement in financial oversight, even as we acknowledge the technology’s current limitations.

Section 2: The Challenge of Media Misrepresentation

Media coverage of cryptocurrency’s role in illicit finance often relies on incomplete analysis and rushed conclusions, creating narratives that can mislead both the public and policymakers. While blockchain technology offers innovative transparency, partial or premature analysis of this data can lead to sensational headlines that distort reality. These distortions, once published, often persist in public discourse even after being thoroughly debunked.

The Anatomy of Misrepresentation

Public blockchains’ pseudonymous nature presents unique analytical challenges. While every transaction is recorded and accessible, interpreting blockchain data can be complex, and drawing conclusions from it can sometimes lead to misleading outcomes. While often well-intentioned, inaccurate analyses leave a lasting mark. Even when subsequent analysis reveals the errors of a previous analysis, the initial misrepresentations often continue to influence policy discussions and public perception.

Even when subsequent analysis reveals the errors of a previous analysis, the initial misrepresentations often continue to influence policy discussions and public perception.

One of the key challenges is attribution—determining which wallet belongs to which actor. This process is often complex. Large exchanges or payment providers may handle transactions for millions of users through common wallets, making it easy to misinterpret normal trading activity as suspicious. Additionally, preliminary analysis might identify concerning transactions without understanding their full context, leading to exaggerated estimates of illicit activity.

For instance, large exchanges or payment providers may not be publicly identifiable, creating confusion. If someone sends cryptocurrency to a large exchange and that exchange later sends cryptocurrency to an individual in Singapore from the same wallet, it does not necessarily mean the two transactions are connected. Additionally, illicit groups often deliberately obscure their activities by employing techniques to mask the wallets and services they operate. Without complete data, even the most well-intentioned researchers can misinterpret what they are observing, leading to speculative or exaggerated claims that may not reflect reality.

Case Study: October 7 Hamas Attack Reporting

Following the October 7, 2023 attacks in Israel, the Wall Street Journal published an article titled “Hamas Militants Behind Israel Attack Raised Millions in Crypto.”⁵ The article, based

on data from two blockchain analytics firms, claimed that Hamas and Palestinian Islamic Jihad (PIJ) had raised a staggering \$130 million in cryptocurrency. By October 17, the article had become the focal point of a significant political controversy with over 100 members of Congress signing a letter to the White House and Treasury Department expressing “grave concern” over the alleged millions in crypto funding terrorist operations.⁶ The letter posed questions about how terrorist groups use cryptocurrency, exchange it for weapons, and what legislative changes might be required to address this national security threat.

Subsequent analysis, however, revealed that the figures were grossly exaggerated. A separate blockchain analytics firm clarified that the \$82 million figure included unrelated transactions processed by service providers, and the actual amount sent to terrorist groups was closer to \$450,000.⁷ One of the analytics firms cited in the WSJ article later corrected its initial statement, emphasizing that post October 7, Hamas had raised only \$21,000, much of which had already been seized.⁸ See the chart below for actual figures for Hamas crypto donations in this time period.

The Wall Street Journal’s claim in October 2023 that Hamas and Palestinian Islamic Jihad received tens of millions in cryptocurrency donations—figures that were later debunked—illustrates the risk of extrapolating incomplete data and emphasizes the need for rigorous validation before disseminating conclusions.

Enabling Swift Verification and Consequently, Sound Policy

The Hamas funding reporting is just one of many instances where stories, no matter how inaccurate, can get recycled endlessly, cementing existing prejudices. While these cases demonstrate the challenges of media misrepresentation, they also highlight the critical role of blockchain analytics in preventing and correcting such mischaracterizations. These analytical capabilities are particularly crucial given how inaccurate narratives, when amplified through social and academic platforms, can distort public discourse and influence policy decisions on critical issues. The impact of such misrepresentation is twofold: it unfairly stigmatizes an emerging financial technology based on flawed analysis, while more critically diverting resources and attention away from effectively fighting illicit finance. By fixating on cryptocurrency as a “technological boogeyman,” we risk missing real opportunities to effectively disrupt these groups’ financial networks.

In reality, the inherent traceability of blockchain technology has enabled both governments and the private sector to track, isolate, and seize terrorist illicit assets. For instance, in April 2023, six months before the October attacks, Hamas’ armed wing, the Izz al-Din al-Qassam Brigades, announced it would stop accepting Bitcoin donations, warning that such transactions exposed donors to detection and targeting.⁹ This example demonstrates how focused, informed countermeasures can effectively combat the misuse of cryptocurrency by terrorist groups.

A critical but less headline-grabbing contribution to this discussion is the 2024 National

Terrorist Financing Risk Assessment released by the US Department of the Treasury.¹⁰ This comprehensive report details how various terrorist organizations utilize different financial methods to send, receive, and transfer funds. Regarding cryptocurrency, referred to as “virtual assets” in the report, it states:

“Since the 2022 NTFRA [National Terrorist Financing Risk Assessment], certain terrorist groups, such as ISIS-K and Hamas, have increased their understanding of and are experimenting with different types of virtual assets. However, the U.S. government assesses that terrorists still prefer traditional financial products and services. This preference is likely in part due to the price volatility of many virtual assets, the limited ability to purchase goods and services with virtual assets, and a lack of infrastructure necessary to exchange virtual assets for fiat currency in some jurisdictions where terrorist groups operate.”¹¹

This measured analysis highlights an important reality: while some terrorist groups experiment with cryptocurrency, they continue to rely primarily on traditional financial systems. Rather than relying on sensational headlines, this clear-headed understanding provides a foundation for sound policy development. While policymakers must remain vigilant about how these groups transfer value, blockchain analytics offers the tools to maintain perspective and respond appropriately to emerging threats. By combining technological capabilities with grounded, evidence-based assessments, we can craft effective, long-term strategies that address genuine risks while supporting financial innovation.

Section 3: Autocracies Exploiting Cryptocurrency: Tools, Not Causes

The relationship between autocratic regimes and cryptocurrency illustrates one of the most powerful arguments for blockchain's inherent transparency. While media narratives often portray cryptocurrency as a tool that enables sanction evasion and other illicit activities by rogue states, the reality is more complex: blockchain's permanent, public ledger provides unprecedented visibility into how these regimes attempt to move and hide wealth. This transparency has transformed our ability to track, understand, and counter autocratic financial maneuvers in ways impossible with traditional banking systems.

When autocratic regimes attempt to exploit cryptocurrency, they leave permanent, traceable records of their every move. Unlike traditional banking channels where cross-border money movements can disappear behind a web of shell companies and correspondent banking relationships, blockchain transactions create immutable evidence that allows investigators to follow money flows in real-time. This capability has proven particularly valuable in tracking state-sponsored cyber operations, monitoring sanction evasion attempts, and mapping the financial networks of regime-connected entities.

The examples of North Korea, Iran, and Russia demonstrate how blockchain analysis has revolutionized our understanding of autocratic financial behavior. Each of these nations has approached cryptocurrency differently, but in every case, blockchain transparency has provided investigators with powerful new tools to detect and counter their activities. North Korea represents one extreme, using state-sponsored cyberattacks to steal cryptocurrency. By contrast, Iran and Russia view cryptocurrency as a potential tool for sanction evasion, but their economies remain heavily reliant on traditional banking systems for their primary revenues. These regimes manipulate cryptocurrency. The problem lies not with the technology, but with the regimes' actions.

Blockchain's Revolutionary Intelligence Value

The contrast in tracking capabilities between traditional and blockchain-based systems is particularly striking. When autocracies move money through conventional banking routes, investigators frequently encounter insurmountable obstacles where funds vanish into opaque banking systems or uncooperative jurisdictions. However, cryptocurrency transactions provide investigators with unprecedented ability to track cross-border money flows in real-time, identify behavioral patterns, and construct comprehensive maps of financial networks. This enhanced visibility has enabled groundbreaking enforcement actions and offered unprecedented insight into how autocratic regimes attempt to circumvent international controls.

This transformation in financial intelligence gathering has revolutionized investigative capabilities in three key areas that were previously impossible to achieve in traditional systems.

First, investigators can now track state-sponsored cyber operations in real-time. Second, they can detect sanction evasion attempts as they occur. Third, they can comprehensively map regime-connected financial networks, revealing previously hidden relationships and patterns. These capabilities have particular value when investigating groups like the Lazarus Group, where investigators could trace stolen funds through multiple wallets and jurisdictions as transactions occurred.

When autocratic regimes use cryptocurrency, they inadvertently create permanent forensic evidence that reveals their broader patterns of behavior. Blockchain analytics has successfully identified specific transaction patterns associated with state-sponsored hacking groups, creating distinctive signatures that help investigators attribute attacks to known actors and often expose connections between seemingly unrelated incidents. The permanence of blockchain records ensures that even years after an incident, new analytical techniques can uncover previously hidden connections and patterns of behavior.

When autocratic regimes use cryptocurrency, they inadvertently create permanent forensic evidence that reveals their broader patterns of behavior.

The shift has fundamentally transformed investigation strategies from reactive to proactive approaches. Rather than waiting months for suspicious activity reports or depending on voluntary cooperation from foreign institutions, investigators can now actively monitor known threat actors and take immediate action when suspicious patterns emerge. This capability has proven instrumental in disrupting ongoing cyber campaigns and preventing stolen funds from being converted into fiat currency. The immutable nature of the blockchain records also means that evidence gathered today becomes part of a permanent database that grows more valuable over time as analytical techniques advance and new connections are discovered.

The North Korean Model: State-Sponsored Cyber Crime

North Korea has constructed an economy rooted in crime, using illicit activities to sustain itself amid international sanctions and economic isolation. Cryptocurrency, for North Korea, is not a tool to promote financial efficiency but a resource to be stolen and monetized. Over decades, the regime has experimented with a wide array of illegal enterprises, including methamphetamine trafficking, counterfeiting currency, arms sales, human trafficking, and, most recently, cybercrime. These activities are not incidental but central to the survival of a state cut off from legitimate global financial systems.

Extensive US and UN sanctions in place since 2006 have aimed to curtail the regime's funding sources. In response, North Korea has adapted, leveraging sophisticated state-sponsored cyberattacks to replenish lost revenue. The Lazarus Group, one of the regime's more notorious

Online crime scene with North Korean flag. (DD Images/Shutterstock)



hacking units, exemplifies this strategy. Since 2015, the group has reportedly stolen over \$1 billion through ransomware attacks, cryptocurrency exchange breaches, and cryptojacking schemes.¹² Their operations demonstrate a systematic approach to financial crime. For example, the 2016 Bangladesh Bank heist saw Lazarus hackers attempt to steal \$951 million by infiltrating

banking systems. While most of the theft was thwarted, the group successfully laundered \$81 million through Philippine casinos and Macau, exploiting global traditional financial loopholes.¹³

In 2022, North Korea's cryptocurrency theft operations peaked, with stolen assets estimated at \$1.7 billion—critical funding for its missile and nuclear weapons programs.¹⁴ The Lazarus Group used advanced techniques to breach exchanges and obscure stolen funds using tools like Tornado Cash and other mixers to launder assets.¹⁵ This reliance on cybercrime demonstrates North Korea's broader strategy to evade sanctions and finance its ambitions through criminal ingenuity.

North Korea's cryptocurrency operations reveal an ironic truth: while the regime has stolen billions in digital assets—an estimated \$1.7 billion in 2022 alone through groups like Lazarus¹⁶—every theft leaves permanent forensic evidence on the blockchain. Unlike the Bangladesh Bank heist where money vanished into opaque banking systems, these digital transactions create an ever-growing map of the regime's criminal networks. This transparency has led to concrete results: law enforcement seized \$30 million from the \$625 million Axie Infinity theft¹⁷, Norway recovered an additional \$5.8 million from the same hack¹⁸, and in December 2024, authorities disrupted a major North Korean laundering network in the UAE.¹⁹ When North Korean hackers extorted \$100,000 in Bitcoin from a Kansas medical center, FBI agents traced the funds through the blockchain to China-based money launderers and recovered the stolen funds.²⁰

By combining blockchain analytics with traditional cybersecurity measures, the international community can leverage this transparency to detect and disrupt state-sponsored financial crime more effectively than ever before. Efforts should focus on strengthening cybersecurity measures, enhancing regulatory frameworks to combat cryptocurrency laundering, and closing the global financial loopholes that North Korea continues to exploit. By addressing these vulnerabilities, the international community can disrupt the regime's ability to sustain itself through cybercrime.

Iran and Russia: Oil Exports and Cryptocurrency

Between 2010 and 2020, Iran and Russia emerged as the two most heavily sanctioned countries by the United States.²¹ As these sanctions accumulated, US policy circles increasingly debated the role of cryptocurrency in undermining their effectiveness. High-profile policy discussions in the United States have even touched on claims of Russian oligarchs using cryptocurrency to obscure billions in assets. Unfortunately, much of this discourse has been steeped in hyperbole, overshadowing the nuanced realities of the issue.

This is not to say cryptocurrency does not facilitate sanction evasion—it does, but on a much smaller scale than often portrayed. Both Russian and Iranian officials have recognized cryptocurrency’s potential. For instance, a Russian oligarch reportedly established a cryptocurrency mining facility at a shuttered industrial site²², and an Iranian general publicly praised cryptocurrency as a tool to bypass sanctions.²³ However, both governments have displayed inconsistent stances on cryptocurrency, oscillating between outright bans on ownership and mining to periods of active encouragement.

Adding to the complexity is the widespread use among these countries’ populations. This high domestic adoption may be driven more by economic instability and financial necessity than with any deliberate government strategy to use cryptocurrency as a sanction evasion tool. Cryptocurrency provides citizens with a way to store value amid currency devaluation and inflation rather than serving as a deliberate tool of state policy.

Regardless of their stance on cryptocurrency, both nations overwhelmingly rely on oil and natural gas exports to sustain their economies. In the 12 months ending in March 2024, Iran’s oil exports reached \$35.8 billion, accounting for 82% of its export revenues, while Russia projected \$239.7 billion in oil and gas sales for 2024.²⁴ These revenues flow through established traditional

Oil refinery plant at sunset. (Green Oak/Shutterstock)



banking systems, often outside US regulators’ reach or obscured by complex networks of trusts and shell companies.²⁵ By comparison, cryptocurrency plays a minimal role. Iran’s first official cryptocurrency-based import transaction in August 2023 totaled just \$10 million—a mere 0.028% of its annual export earnings—underscoring its limited significance.²⁶

The notion that Iran and Russia depend on cryptocurrency to evade sanctions oversimplifies

their economic realities. Both nations continue to navigate sanctions primarily through traditional trade and financial systems. While cryptocurrency offers niche opportunities for evasion, its role is secondary to the substantial revenues generated through natural resource exports, which remain the cornerstone of their economic strategies.

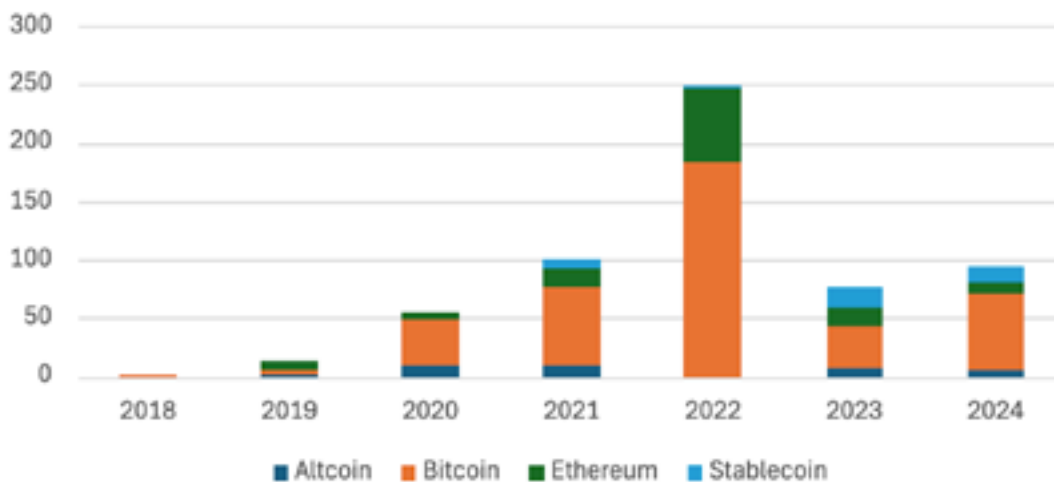
Sanctions and Cryptocurrency: Unlikely Allies in Enforcement

Cryptocurrency is often misunderstood as being uniquely suited for evading US sanctions, but this oversimplifies both how sanctions work and how evasion occurs. Sanction enforcement is a perpetual cat-and-mouse game: as new evasion methods emerge, they are countered. No single financial instrument, including cryptocurrency, offers an inherent advantage for sanction evasion, as workarounds will always exist. Sanctioned actors leverage a mix of tools, including traditional banking systems, trade networks, hawalas, and, occasionally, cryptocurrencies.

Effective sanctions hinge on precise targeting—restricting specific individuals, entities, and assets. Since 2018, the US Treasury’s Office of Foreign Assets Control has included cryptocurrency wallet addresses linked to sanctioned actors, enabling exchanges and financial institutions to block transactions involving these wallets. Blockchain transparency has not only enhanced vigilance within the cryptocurrency sector but also benefited the broader financial community. The clearer the picture of which wallets and services are linked to sanctioned actors, the easier it is to isolate them. This duality highlights crypto’s potential to serve as a valuable tool for enforcement rather than solely a means of evasion.

Cryptocurrency Addresses Added to OFAC’s Specially Designated Nationals List

Since 2018, OFAC has included cryptocurrency addresses on its sanctions list, enabling financial institutions to identify and monitor these addresses and their associated actors.



Source data from the Office of Foreign Assets Control

The Critical Role of Foreign Intermediaries

The most effective pressure point in combating foreign adversaries lies not in restricting legitimate US cryptocurrency activity, but in targeting the foreign exchanges and services these actors rely on to convert stolen cryptocurrency into usable currency. These foreign centralized exchanges serve as critical chokepoints where several key activities converge. Stolen funds must eventually be converted to fiat currency at these exchanges, and during this process, illicit actors are forced to reveal identifying information. These points also represent the locations where law enforcement can intervene most effectively and where international pressure can be applied to maximum effect.

Section 4: Fraud, Drugs and Cybercrime: Systemic Issues, Not Cryptocurrency-Caused

The last few years have seen an explosion of cryptocurrency-related fraud and cybercrime that has attracted significant media attention. At the same time, it offers no solace to the victims of financial crime whether an old or new financial technology was used—the pain and damage are the same. As discussed in previous sections, cryptocurrency often receives an outsized share of blame for its role in illicit finance. However, long-established methods such as high-end real estate transactions, black market peso exchanges, and trade-based money laundering remain more effective at concealing illicit funds. These traditional techniques, honed over decades, exploit cross-border vulnerabilities and weak international cooperation, challenges that also complicate efforts to combat financial crimes involving cryptocurrency. The key difference is that while traditional financial crimes often disappear into opaque banking systems, cryptocurrency leaves an immutable trail of evidence that investigators can follow indefinitely.

The misuse of cryptocurrency is not a new kind of crime but an evolution of existing schemes that integrate new tools. Its exploitation reflects broader issues in tackling transnational organized crime and drug trafficking organizations, including corruption and inconsistent enforcement across jurisdictions. What sets cryptocurrency apart is that every transaction creates permanent forensic evidence available to be analyzed to identify patterns, track funds, and map criminal networks. This transparency has enabled groundbreaking enforcement, with the IRS Criminal Investigation Unit seizing over \$7 billion in illicit cryptocurrency assets in 2022.²⁷

The misuse of cryptocurrency is not a new kind of crime but an evolution of existing schemes that integrate new tools.

Financial crime changes. As law enforcement raises the costs of one activity, criminals innovate to reap the financial rewards of a new approach and to stay one step ahead of governments. Drug trafficking organizations, for example, began with cash, used bank accounts, progressed to integrating trade-based schemes, and now incorporate cryptocurrency into their operations. This adaptability underscores the need for a holistic view of financial crime that goes beyond individual tools or technologies. The key is understanding how blockchain’s transparency can be leveraged to combat criminal activity across all domains. For example, blockchain analysis played a crucial role in the Welcome to Video child exploitation site, with investigators using transaction records to identify both operators and users of the platform. This led to 337 arrests across 38 countries and the rescue of 23 victims—an outcome that would have been nearly impossible to achieve through traditional financial investigation methods.

This section explores how blockchain’s inherent transparency transforms our ability to combat

financial crimes, providing investigators with unprecedented capabilities to trace funds, identify perpetrators, and disrupt criminal networks. While criminals may attempt to exploit cryptocurrency like any financial tool, blockchain analytics has enabled law enforcement to achieve remarkable success rates in asset recovery and prosecutions that would be nearly impossible in traditional finance. Recent cases and enforcement actions demonstrate how cryptocurrency's public ledger creates powerful new opportunities to curtail financial crime, even as criminal tactics evolve.

However, the evidence also reveals that additional domestic cryptocurrency regulations alone would fail to address the underlying problems: weak security practices within organizations and insufficient international cooperation in pursuing organized crime networks. These root causes, rather than the financial technologies used, are what enable criminal enterprises to thrive. Effective solutions require strengthening fundamental security practices and expanding cross-border enforcement capabilities, not simply adding regulatory burden to emerging financial technologies.

Fraudulent Foundations: How Blockchain Transparency is Disrupting Traditional Scams

In the 20th century, Ponzi schemes became emblematic of financial fraud, with Charles Ponzi enticing investors with promises of extraordinary returns paid not through legitimate profits but from the contributions of new participants. This foundational scam set the stage for modern iterations, such as Bernie Madoff's infamous \$65 billion operation, and Allen Stanford's \$7 billion scheme. These massive frauds succeeded by preying on investors' desire for high returns and fostering the illusion that their money was being responsibly and legitimately managed.

While scammers have attempted to repackage these traditional tactics for the cryptocurrency era, the transparent nature of blockchain creates unprecedented opportunities for detection and recovery. One notorious example is BitConnect, a cryptocurrency investment platform that capitalized on the 2017-2018 Bitcoin price surge. Promising high returns through a proprietary lending program, BitConnect lured users to exchange Bitcoin for its native token, BitConnect Coin (BCC), which soared from \$0.40 in 2016 to an all-time high of \$463 in December 2017.²⁸

When BitConnect collapsed, revealing itself as a \$2.4 billion Ponzi scheme²⁹, investigators had access to something unavailable in traditional financial fraud cases—a complete, immutable record of every transaction. This transparency enabled authorities to trace funds across multiple jurisdictions, leading to rapid asset recovery and criminal charges against key operators. Unlike the Madoff case, where investigators spent years attempting to reconstruct money flows from fragmentary banking records, blockchain analytics allowed investigators to map the entire scheme's operation within months.

While high-profile cases like BitConnect and Madoff's are widely known, these types of fraud are far from isolated. Such schemes continue to emerge, often targeting specific communities

through a practice known as affinity fraud. This form of financial crime exploits trust within tight-knit groups, such as religious congregations, immigrant communities, or professional associations. Fraudsters either emerge from within the community or infiltrate it, promoting fake investments in real estate, bonds, or other assets to devastating effect. Victims not only suffer financial losses but also endure a betrayal of trust that can ripple through entire communities. Blockchain analytics has proven particularly powerful in disrupting smaller-scale fraud operations before they can grow. Law enforcement can now track suspicious patterns in real-time, often freezing fraudulent operations before significant losses occur. When scammers know their transactions can be traced indefinitely, many may be deterred from using cryptocurrency altogether.

Interestingly, recent trends suggest that cryptocurrency-related Ponzi schemes, while still significant, have decreased as a proportion of total scams. In 2022, over 25% of uncovered Ponzi schemes were linked to cryptocurrencies, but in 2023, that figure fell to approximately 15%.³⁰ While cryptocurrency is used for these scams, traditional systems, such as fiat-based schemes and affinity fraud, continue to dominate.

Ultimately, while cryptocurrency can be exploited for fraud like any financial tool, blockchain’s inherent transparency has created a fundamentally more hostile environment for large-scale scam operations. The ability to track and trace funds indefinitely, combined with improving coordination between law enforcement and cryptocurrency exchanges, has enabled unprecedented success in fraud disruption and asset recovery. These capabilities stand in stark contrast to traditional financial fraud, where investigators often lose money trails as soon as funds enter the banking system.

Financial Losses from Ponzi Schemes

Money lost to crypto-based Ponzi schemes is significantly lower than that of traditional finance schemes.

Crypto Ponzi Schemes	Fiat Ponzi Schemes
OneCoin (2014-2017), \$4 billion	Bernie Madoff (2008), \$65 billion
PlusToken (2018-2019), \$2 billion	MMM (1990s), \$10 billion
BitConnect (2016-2018), \$2 billion	Allen Stanford (2009), \$7 billion
Mirror Trading International (2019-2020), \$1 billion	Tom Petters (2008), \$3.7 billion
WoToken (2018-2019), \$1 billion	Scott Rothstein (2009), \$1.2 billion

Industrial Scale Financial Fraud

A troubling evolution in financial crime is the convergence of fraud, human trafficking, organized crime, and inadequate governmental responses. This marks the industrialization of fraud, with large-scale scam centers that originated in Southeast Asia now spreading across the globe. Over 200,000 people in Southeast Asia have been trafficked and forced into online “pig butchering” scams. These operations, which involve building trust with individuals to steal money through fake investment platforms—often using cryptocurrency—are run primarily by Chinese criminal syndicates. Exploiting weak governance in countries like Myanmar, Cambodia, and Laos, these scams have generated billions of dollars in stolen funds. The operations have expanded globally to regions including the Middle East, Eastern Europe, Latin America, and West Africa, with people trafficked from over 60 countries to work in abusive environments.⁵¹

The scale and sophistication of these operations underscore why domestic cryptocurrency regulations would fail to address the underlying problems. These criminal enterprises thrive not because of any particular financial technology, but because of systemic vulnerabilities: weak cybersecurity practices within organizations, limited technological capabilities among law enforcement agencies, and insufficient cross-border cooperation in investigating and prosecuting organized crime. Blockchain technology, rather than being merely something to regulate, provides powerful tools for combating these operations through its inherent transparency and traceability.

Scam centers rely on trafficked labor, coercing people into brutal conditions. Workers are often confined, beaten, and forced to meet quotas under threats of further violence. Dubai, within the UAE, has emerged as a major hub for these scams, alongside nations like Nigeria, which already have established scamming cultures. Alarming, some individuals, initially trafficked, return voluntarily due to the financial incentives of the work, perpetuating the cycle of exploitation.

The human cost is immense. Financial victims suffer emotional trauma, financial ruin, and in some tragic cases, suicide. Meanwhile, trafficked workers endure unimaginable suffering, forced to perpetrate crimes as they too are stuck in the cycle. The convergence of fraud and trafficking has created self-sustaining systems of exploitation, enabled by gaps in regulation, enforcement, and international collaboration.

Despite crackdowns by Chinese authorities, the profitability of pig butchering schemes continues to fuel their proliferation. In 2023 alone, nearly \$4 billion in losses were reported in the United States, with global losses exceeding \$75 billion. Romance scams, a subset of pig butchering, have also grown exponentially. The FTC reported \$1.3 billion in losses from such scams in 2022, which skyrocketed to \$5.6 billion in 2023.⁵² Experts warn that these scams, which blend financial fraud and human trafficking, inflict damages rivaling those of drug trafficking and terrorism. Without stronger global action, these operations will continue to expand.

Cryptocurrency often serves as a facilitator in these scams, leveraging its rapid, borderless

Fraudsters' process. (ATS Technologies)



nature to obscure the movement of stolen funds. However, it is merely a tool—not the cause. Cryptocurrency lacks agency; it is people who execute the transactions, and the technology does not move on its own. The true culprits are the criminal networks that exploit systemic vulnerabilities and scale their operations through activities like human trafficking. These organizations flourish in regions with weak regulatory frameworks, inadequate enforcement, and limited international cooperation, enabling them to operate with relative impunity.

However, when scammers using cryptocurrency attempt to cash out through exchanges, law enforcement can identify and freeze these funds—a powerful deterrent that makes cryptocurrency increasingly risky for fraudsters. Furthermore, blockchain's immutable public ledger provides valuable insight to law enforcement, who can trace the movement of funds from sender to receiver in real time, potentially identifying illicit activity and facilitating the recovery of stolen funds.

The rapid evolution of these scams highlights the critical importance of public education and digital literacy, as well. Just as traditional financial institutions invest in teaching consumers about conventional banking safety, consumers also need comprehensive programs to understand both the capabilities and limitations of digital assets. This education must go beyond simple warnings about cryptocurrency risks to include practical training on secure digital transactions, understanding blockchain traceability, and recognizing sophisticated social engineering tactics used by scammers. When people understand how blockchain's transparency can help track and recover stolen funds, they're better equipped to both protect themselves and assist law enforcement.

These industrial-scale operations demonstrate why effective solutions must combine enhanced technological capabilities, improved international cooperation, and broad-based public education. Rather than creating new domestic regulations that may simply push criminal activities into less transparent channels, the United States should strengthen fundamental investigative capabilities and cross-border enforcement mechanisms while simultaneously building public resilience through education. The transparency of blockchain technology offers unprecedented opportunities to track and disrupt these criminal networks, but only when paired with the international cooperation frameworks and public understanding needed to fully utilize these capabilities.

The Evolution of Drug Sales: From Street Deals to Encrypted Marketplaces, Leveraging Traceability for Enforcement

The global drug trade encompasses various substances – from heroin sourced in Central Asia and cocaine from South America, to domestically produced methamphetamine and fentanyl manufactured using imported chemical precursors. The trading has evolved from street-level cash transactions into a complex system of online marketplaces and transnational supply chains. This evolution in both distribution methods and financial techniques has posed significant challenges for law enforcement. These operations leverage sophisticated financial networks and exploit regulatory weaknesses, using cryptocurrency alongside other tools to move money across borders.

While cryptocurrency initially seemed to offer drug traffickers new tools for anonymity, the transparent nature of blockchain technology has actually created unprecedented opportunities for law enforcement to track and disrupt these operations. What traffickers hailed as their cloak of invisibility became the very lens through which they were exposed.

The story of cryptocurrency and drug sales is closely tied to the emergence of anonymous web browsing, which enabled the creation of online drug markets. The advent of these markets revolutionized the trade, offering sellers and buyers newfound anonymity and global reach. Darknet markets (DNMs), accessed via encrypted networks like Tor, represented a significant technological leap. Originally developed by the US Naval Research Laboratory in the 1990s for secure communications, Tor became a double-edged sword—protecting legitimate privacy while fostering a black market for illegal goods. This shift required an innovative payment system, and Bitcoin quickly became the preferred method for “anonymous” transactions. Together, Tor and Bitcoin ushered in a new era of illicit commerce.

The Silk Road, launched in 2011, became the first platform to integrate Tor and Bitcoin in drug commerce. With nearly 70% of its transactions involving drugs, the marketplace became synonymous with the darknet economy, generating over \$500,000 in daily revenue before its 2013 shutdown. The novelty of the Silk Road presented unprecedented challenges for law enforcement, including the corruption of two federal agents later convicted of stealing Bitcoin tied to the investigation. Despite its closure, imitators such as Silk Road 2.0 and AlphaBay emerged, refining the marketplace model and generating millions in sales until their own

These criminal enterprises thrive not because of any particular financial technology, but because of systemic vulnerabilities: weak cybersecurity practices within organizations, limited technological capabilities among law enforcement agencies, and insufficient cross-border cooperation in investigating and prosecuting organized crime.

closures, highlighting the resilience and adaptability of online drug networks. Initially, the combination of Tor’s anonymity and Bitcoin’s perceived untraceability seemed to offer perfect cover for illicit trade. However, this perception proved fatally flawed, as blockchain’s inherent transparency provided investigators with a permanent evidence trail. When the Silk Road was shut down in 2013, blockchain analysis played a crucial role not only in identifying the site’s operator but in mapping entire networks of vendors and buyers.

AlphaBay darknet market screenshot. (Department of Justice/Public domain)



This pattern has repeated with subsequent darknet markets. When AlphaBay was dismantled in 2017, blockchain analytics enabled investigators to trace over \$1 billion in transactions, leading to hundreds of arrests worldwide.³³ In 2022, the Hydra market takedown showcased the evolution of these capabilities - investigators used advanced blockchain analysis to track

money flows dating back to 2015, identifying key operators and seizing \$25 million in Bitcoin. The permanent nature of blockchain records means that even years after a marketplace closes, investigators can continue identifying and prosecuting participants.³⁴

Even as authorities dismantled major darknet markets and arrested key operators, drug marketplaces continued to adapt. The shift to mainstream platforms like Telegram marked a new phase in the evolution of drug sales. Easier to access than the darknet, Telegram’s user-friendly interface and automation tools have made it an increasingly popular venue for illicit transactions. Automated bots on Telegram enable seamless, 24/7 transactions without human involvement, providing a more accessible and efficient alternative to the technical barriers of darknet platforms. Telegram’s meteoric rise as a hub for illegal activity underscores the drug trade’s ability to harness new technologies and stay ahead of enforcement.

The drug trade’s evolution reflects an eternal cat-and-mouse game between criminals and law enforcement, but blockchain technology has fundamentally tilted the playing field. While weak regulatory environments and complicit jurisdictions still provide cover for drug production and trafficking, the transparent nature of cryptocurrency transactions gives investigators powerful new tools for following money flows and mapping criminal networks. The success of recent enforcement operations demonstrates that when properly leveraged, blockchain analytics can transform our ability to combat drug trafficking, creating an environment where the technology’s transparency becomes a powerful deterrent rather than an enabling tool.

Crossing Jurisdictions

Mexican cartels and Chinese organized crime dominate fentanyl production, while overseas laboratories supply the essential chemical precursors. These networks strategically leverage favorable jurisdictions to evade enforcement, creating a complex, transnational web that continues to challenge policymakers and law enforcement agencies worldwide.

Within this intricate ecosystem, value flows seamlessly from consumers to the criminal organizations that orchestrate these operations. Bulk cash, front businesses, real estate, and bank transfers serve as the financial lifeblood that sustains the drug trade. Cryptocurrency also plays a role, offering a transfer mechanism with global reach and instantaneous settlement, making it particularly attractive to traffickers. However, permanent records created by cryptocurrency transactions allow investigators to follow money across jurisdictions and map previously invisible parts of trafficking networks, even in regions where traditional financial investigation methods face obstacles.

However, the drug economy's hallmark is its adaptability. While cryptocurrency is a favored tool today, persistent law enforcement efforts, arrests, and asset seizures will undoubtedly force another evolution in criminal behavior, ensuring the cycle continues. For now, though, transactions leave a trail of evidence on the blockchain, allowing investigators to study and predict how these networks adapt and evolve. This growing body of forensic intelligence represents a fundamental shift in our ability to understand and combat drug trafficking operations, even as they attempt to stay one step ahead of enforcement.

Section 5: Ransomware, Fraud and DNMs: Law Enforcement Takedowns - Highlighting Cryptocurrency's Strengths

Cryptocurrency is often portrayed in popular media as a favored tool for criminals, with headlines frequently highlighting law enforcement “takedowns” involving digital assets. While this narrative is compelling, it ignores the fact that these takedowns are only possible due to cryptocurrency’s defining strength: its immutable public ledger. This ledger often gives law enforcement a distinct advantage, allowing them to trace the lifecycle of assets, detect patterns of illicit activity, and track the source and destination of illicit funds. Ironically, the same qualities that fuel misconceptions about cryptocurrency as a haven for illicit activities also make it an exceptional tool for combating financial crime.

This ledger often gives law enforcement a distinct advantage, allowing them to trace the lifecycle of assets, detect patterns of illicit activity, and track the source and destination of illicit funds.

This stands in stark contrast to traditional financial systems, where tracking illicit activity is often hampered by fragmented data and institutional silos. Transaction records are typically confined to individual banks or financial institutions, limiting visibility across the broader financial ecosystem. Investigations require complex legal requests and multi-jurisdictional cooperation, making it difficult to build a complete picture of financial flows. This lack of transparency slows investigations and often makes tracking cross-border transactions or layered financial structures prohibitively challenging.

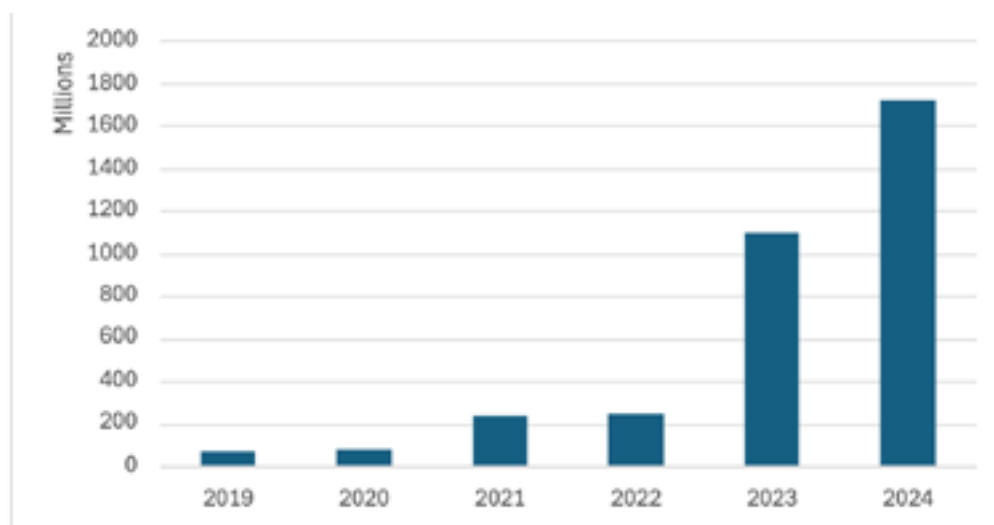
The misconception that cryptocurrency is dominated by crime stems largely from the public’s inability to contextualize its transparency. While it is easy to interpret transactions linked to ransomware or darknet wallets, understanding the intent behind transactions involving mainstream exchanges can be more complex. As discussed previously, headlines about “cryptocrime” amplify these perceptions, yet they are better viewed as evidence of blockchain’s transparency. The visibility that enables these investigations underscores cryptocurrency’s unique value in law enforcement efforts, rather than proving it to be a criminal tool.

The transparency provided by blockchain has become one of cryptocurrency’s greatest strengths, particularly for supporting law enforcement investigations. High-profile operations often succeed not despite cryptocurrency but because of it, as the immutable ledger provides a roadmap to uncover illicit activities. Law enforcement agencies may come to prefer criminals to use cryptocurrency because its traceability offers a distinct advantage over cash. This reality is evident in cases involving ransomware, darknet marketplaces, and other criminal networks,

where blockchain analysis has led to significant law enforcement successes.

This traceability facilitates arrests, as demonstrated in the case studies below, as well as seizure of illicit funds. Blockchain transparency allows law enforcement to pinpoint the location of these funds, monitor their movements, and employ legal measures to freeze and confiscate them. The US Department of Justice alone recovered over \$1 billion in 2023 through cryptocurrency seizures exceeding \$1 million each. Additional seizures by IRS-Criminal Investigations (IRS-CI) and other US governmental organizations amount to much more, while the scale of seizures on a global level is even higher.

U.S. Department of Justice Cryptocurrency Seizures over \$1 Million



Source: U.S. Department of Justice. Asset Forfeiture Program Reports. U.S. Department of Justice, <https://www.justice.gov/afp/reports>

The next case studies will review major law enforcement wins, including seizures of illicit crypto assets, dismantling of darknet marketplaces, and actions against ransomware operators. These cases demonstrate how blockchain tracing has exposed child exploitation networks, profiled criminal actors, and tracked vendors and consumers in illegal marketplaces. As cryptocurrency adoption grows, understanding its potential to enhance financial transparency and support law enforcement becomes increasingly vital for policymakers, investigators, and the public alike.³⁵³⁶

Welcome to Video and CSAM

Blockchain technology has proven to be a powerful weapon in the fight against child sexual abuse material (CSAM), rescuing children, unmasking predators, and dismantling global networks of exploitation. By analyzing the transparent properties of blockchains, investigators can identify international CSAM networks, profile recurring offenders, and expose vendors

attempting to evade detection by blending into the digital landscape. One of the most harrowing yet impactful victories made possible by blockchain intelligence was the takedown of Welcome to Video (WTV), a South Korean-based CSAM platform.

WTV operated by assigning each user a unique Bitcoin address to purchase exploitative content. Using blockchain tracing and Know Your Customer (KYC) compliance processes, law enforcement tracked these addresses back to key offenders. In 2018, investigators arrested the site's owner, dismantled the operation, and seized over 8 terabytes of CSAM—alongside 1.3 million Bitcoin addresses tied to the platform. This breakthrough not only shut down one of the largest CSAM distribution networks in history but also laid the groundwork for further arrests worldwide.³⁷

Other cases highlight blockchain's unmatched ability to dismantle CSAM networks. One operation began with the arrest of New York City resident Jason Seto, who was caught in an undercover sting. A Tor address for a CSAM site discovered in Seto's home led investigators to use blockchain analysis to identify the site administrator. While monitoring transactions, they uncovered another Bitcoin address used to purchase CSAM videos. Pursuing this lead, law enforcement rescued a child and secured a 55-year prison sentence for the buyer.³⁸

The Silk Road Marketplace Seizure

The largest cryptocurrency seizure to ever take place occurred in 2011 when IRS-CI seized 50,676 BTC, worth \$3.4 billion at the time, from James Zhong, an individual who stole the Bitcoin from the Silk Road marketplace. (See Section 4 for more detailed discussion of Bitcoin and Silk Road.)

Since blockchain analytics software allows for fund tracing regardless of the age of the transaction, it was possible to see not only the original theft from the Silk Road marketplace, but also the attempt almost a decade later to launder the funds through a mixing service. In spite of the use of these mixing services, investigators were able to connect the identity of Zhong to the original stolen funds when Zhong attempted to cash out at a centralized exchange. These exchanges require users to submit Know Your Customer ("KYC") information in order to open accounts and crucially connect those accounts to banks where fiat conversions can be made. Investigators identified the user of the account on the centralized exchange that received the funds, prosecuted that individual, and finally recovered the stolen funds.

Bitfinex Exchange Hack Seizure

The Bitfinex exchange hack in August 2016 showcased the risks inherent in cryptocurrency exchanges but also highlighted the unique benefits of blockchain technology for law enforcement. Hackers stole approximately 120,000 Bitcoin, worth \$72 million at the time, and attempted to hide their tracks by spreading the funds across numerous wallets. The hack raised significant concerns about security in the cryptocurrency industry, but it also set the

stage for one of the most remarkable asset recoveries to date.

In February 2022, the U.S. Department of Justice announced the recovery of 94,000 Bitcoin, valued at \$3.6 billion at the time, making it the largest cryptocurrency seizure to date. Law enforcement used advanced blockchain analytics to follow the trail of funds across wallets, even as the perpetrators attempted to obscure their movements through mixers, darknet markets, and fraudulent accounts.

Opportunities with Centralized Cryptocurrencies

The opportunity for seizing or freezing funds gets even more straightforward with centralized currencies such as Tether (USDT). Tether (USDT) operates as a centralized stablecoin, meaning that its issuance and management are controlled by a single entity, Tether Limited. Tether Limited is able to intervene in special circumstances and “freeze” addresses that are associated with illicit activity.

In November 2023, Tether executed its largest-ever freeze of USDT tokens, amounting to approximately \$225 million. This action was taken in collaboration with the US Department of Justice and the cryptocurrency exchange OKX. The frozen funds were linked to an international human trafficking syndicate operating in Southeast Asia, responsible for orchestrating a global “pig butchering” romance scam.³⁹ According to the Tether website as of 2023,

“Tether has aided 31 agencies worldwide with investigations across 19 jurisdictions, freezing a total of \$835 million in assets mostly associated with theft (blockchain and exchange hacks) with a minor portion to other crimes. Some of the countries Tether has joined hands with include Brazil, Singapore, Philippines, Germany, South Korea, Norway, Poland, Switzerland, Greece, Canada, Croatia, Italy, Argentina, Australia, Belgium, Cayman Islands, China, Netherlands, El Salvador, Germany, Hong Kong, India, Ireland, Israel, Kyrgyzstan, New Zealand, Spain, Taiwan, UK, Ukraine, Estonia, and the United States.”⁴⁰

Tether Limited enforces freezes on USDT tokens by utilizing administrative control over the token’s smart contracts. These contracts include a function called **addBlackList(address)**, which allows Tether to designate specific wallet addresses as blacklisted. Once an address is blacklisted, the USDT tokens in that wallet become immovable and unusable, effectively freezing the funds. The freeze remains in place until Tether either removes the blacklist using the **removeBlackList(address)** function or redirects the frozen funds to an authorized party, such as a law enforcement agency. This capability enables Tether to respond swiftly to regulatory or legal requests to block illicit transactions or recover stolen assets.

These cases and scenarios underscore the tremendous opportunity for law enforcement to recoup illicit funds in a substantially more straightforward manner than available in traditional finance. While asset seizures in traditional finance would use the same legal methods to engage

with centralized services, the technological components of blockchain give broader access to transaction history of bad actors that would be otherwise more complicated to acquire. The opportunity with centralized services such as Tether means that authorities can instantly freeze any funds proven to be associated with illicit actors and redirect those funds to the proper authorities.

International Action Taken and Arrests Made Against Ransomware Threat Actors

Perhaps the most promising signal about the effectiveness of international coordination, rising ransomware arrests facilitated by blockchain forensics, comes from looking at greater ransomware trends. Each year from 2019 to 2022, the amount of value stolen by ransomware actors continued to rise. In 2022, however, there was a massive decrease in the amount of revenue received by ransomware actors, from total tracked ransomware payments of \$983 million in 2021 to \$567 million in 2022.⁴¹

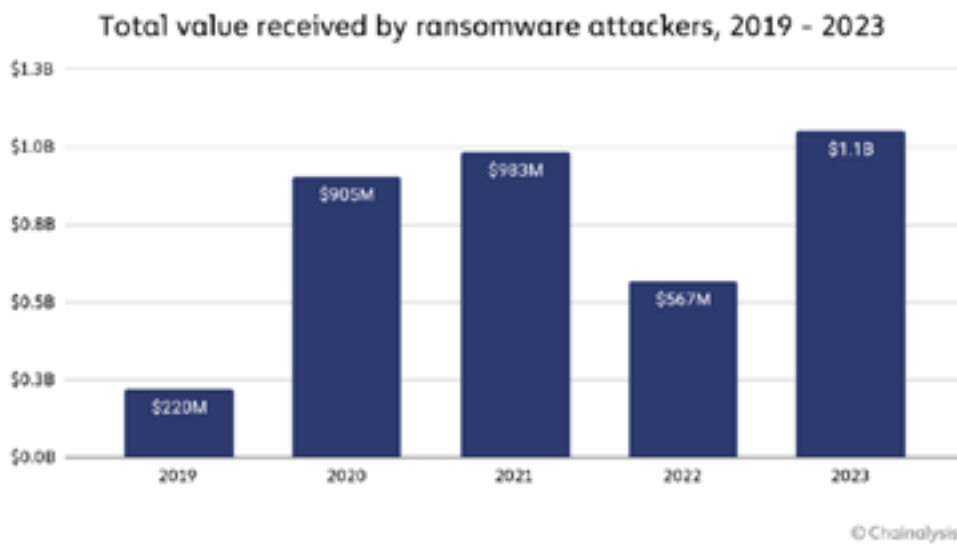


Chart republished with permission from Chainalysis

This decline can be directly attributed to actions taken by the international community to disrupt ransomware activity. Specifically, the FBI's infiltration of Hive provided decryption keys to over 1,300 people robbed, preventing approximately \$130 million in ransom payments.⁴² This intervention significantly impacted the ransomware landscape, with total tracked ransomware payments dropping from \$983 million in 2021 to \$567 million in 2022, partly due to the disruption of Hive's operations. On the next page, Hive revenue is mapped out against the FBI infiltration period. As can be seen, revenue by Hive actors greatly decreased during this time.⁴³



Chart republished with permission from Chainalysis

The arrests and action taken by the international community can have tremendous impact. Blockchain forensics facilitates greater international collaboration, which in turn leads to more asset recovery, more arrests, and more impact. Gurvais Grigg, a former FBI Special Agent and current Global Public Sector CTO at Chainalysis, highlighted the transformative impact of blockchain intelligence on law enforcement:

“Bad actors are often the first to adopt new technologies in attempt to obscure their activities. But with blockchain, you have this incredibly transparent and permanent ledger, which can be a huge advantage for law enforcement if we know how to use it.”⁴⁴

The transparent nature of the blockchain allows real-time data sharing between law enforcement in different countries, bypassing traditional barriers like differing financial regulations or jurisdictional challenges. The level of coordination used to tackle ransomware could be applied to any crime type and crucially, the impact of this coordination can be measured in real-time with blockchain forensic tools. This further allows for the experimentation with different strategies of intervention based on the impact on global crime numbers.

Privacy Coins: Misunderstood and Overemphasized

It is important to note the existence of privacy coins like Monero, ZCash, and Dash, which are designed to provide enhanced anonymity through advanced cryptocurrency techniques. While these coins make tracing transactions more challenging, their impact on illicit finance is often overstated. Despite the attention given to privacy coins and their potential use for illicit activity, their low volume and lack of liquidity have significantly limited their impact. This section will explain what privacy coins are, debunk exaggerated claims of their use by criminals, and emphasize that, while privacy coins do exist, their practical role in illicit finance is overstated.

Privacy coins like Monero and ZCash mask the user's identity using a variety of cryptographic techniques. One technique is using stealth addresses, in which a user's private cryptocurrency address is simply replaced with a new public one for every transaction. Ring signatures allow users to combine addresses on the blockchain to obscure individual identities. ZSNARKS (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) verifies transactions using cryptocurrency functions without revealing transactors' information.⁴⁵

This diversity in cryptocurrencies demonstrates that far from being interchangeable, different cryptocurrencies serve distinct purposes and cater to various needs in the evolving digital economy.

Monero's trading volume is currently under \$3 billion per day across all major exchanges.⁴⁶ This is roughly between 1% to 10% of bitcoin's average daily trading volume. The low volume and lack of liquidity of privacy coins have limited their practical use in large-scale illegal activities. If a criminal were to receive tens of millions of dollars of Monero in a scam or ransomware attack, selling this off on an exchange while retaining the price would be harder than a higher liquidity asset with greater order book depth.

There is evidence of criminals using privacy coins for illicit activities, but practical limitations prevent this from becoming widespread. For instance, many cryptocurrency scammers target less tech-savvy individuals who lack the expertise needed to acquire Monero. Hackers, on the other hand, often target exchange reserves and tend to be coin-agnostic. While some ransomware actors do use Monero, onboarding targeted people to this coin can be challenging, and with limited exchange support, converting Monero into fiat currency is difficult.

Section 6: The Threat of Misunderstanding an Industry

Cryptocurrency has undeniably entered the public zeitgeist, making it an easy scapegoat for societal concerns. Half-truths and sensationalized narratives have skewed the discourse, overlooking that the qualities attracting criminals—anonymity, speed, and accessibility—are features of any transformative technology, such as encrypted messaging. This scapegoating not only obscures the real challenges but also risks stifling innovation if adoption of policies and regulation of cryptocurrency is reactionary or based on incomplete narratives. One-sided views of complex issues, particularly in combating illicit finance, often lack the nuance required for effective policy making. These misconceptions have significantly influenced how policymakers choose to engage with cryptocurrency.

Misinformation about new technologies like blockchain is pervasive, leading to widespread myths and false narratives. Cryptocurrency is not a separate category of crime but rather an addition to the existing toolkit of criminals. Furthermore, while autocratic regimes exploit cryptocurrency, their misuse reflects the behaviors of the regimes themselves rather than any intrinsic flaw in cryptocurrency. The transparency inherent in blockchains has enabled groundbreaking enforcement actions against illicit activities, countering the misconception that these systems are entirely opaque. Additionally, cryptocurrency service providers and intermediaries take proactive steps to prevent illicit activity on their platforms. Know Your Customer (KYC) and identity verification, Anti-Money Laundering (AML) monitoring and reporting, and sanctions screening initiatives are only a few examples of the measures taken to ensure regulatory compliance.

Without addressing these misconceptions, regulators risk misjudging the true scope of risks in the industry and the prevalence of threats. Mischaracterizations of cryptocurrency as primarily a tool for illicit finance or as inherently opaque hinder the establishment of collaborations and effective regulations that simultaneously fight financial crime and allow a new industry to flourish in the United States. Regulators must develop an understanding grounded in facts to ensure policies accurately address the risks and opportunities presented by this evolving technology.

Mischaracterizations of cryptocurrency as primarily a tool for illicit finance or as inherently opaque hinder the establishment of collaborations and effective regulations that simultaneously fight financial crime and allow a new industry to flourish in the United States.

The United States currently maintains robust sanctions and AML programs. Multiple federal and state agencies are involved in these efforts, and law enforcement agencies are actively

apprehending individuals and seizing cryptocurrency linked to illicit activities. However, as the use of cryptocurrency expands, there is a growing impetus to address the global nature of criminal misuse. Domestic policy updates alone are insufficient in combating this challenge, so it is crucial that new regulations be grounded in reliable data and coordinated internationally to close gaps. Done right, it can secure the economic and technological benefits of this growing industry, including job creation, advances in financial technology, and more efficient payment systems. Done wrong, it could push the industry overseas, with far-reaching consequences. Lax regulation in some jurisdictions already enables regulatory arbitrage, allowing bad actors to exploit gaps in oversight. The ease of shifting operations to crypto-friendly jurisdictions undermines international efforts to combat financial crime and facilitates the growth of illicit activity.

Financial Policy—and Crime—Are International

One possible negative outcome if the United States fails to establish thoughtful and effective cryptocurrency regulation, the industry is likely to migrate to jurisdictions that are less stringent and more permissive, a concept known as regulatory arbitrage. The lack of consistent, global standards for cryptocurrency regulation allows bad actors to exploit gaps in oversight, creating a fragmented environment where illicit activities thrive in jurisdictions with weak KYC and AML requirements. This inconsistency undermines global efforts to combat financial crime and highlights the urgent need for coordinated international policymaking.

By addressing the issue of regulatory arbitrage, policymakers can resolve many systemic problems linked to cryptocurrency misuse. Establishing and enforcing robust KYC and AML standards across global jurisdictions will help close loopholes that enable criminal activity while safeguarding the legitimate benefits of blockchain technology. Rather than banning or over-restricting cryptocurrency, the focus should be on fostering global collaboration to create a coherent regulatory framework that supports innovation while mitigating risks.

Globe resting on US dollars. (Vladyslav Travel photo/Shutterstock)



The conversation around cryptocurrency is part of a broader, more significant global debate about the dominance of the US dollar as the world's reserve currency. Since the end of World War II, the dollar has served as the default currency for international trade, granting US financial institutions immense influence and enabling American sanctions to exert significant pressure on foreign adversaries. However, this dominance is

increasingly being challenged.

The BRICS nations—Brazil, Russia, India, China, and South Africa—are at the forefront of efforts to reduce reliance on the dollar in international trade. They have advocated for the use of local currencies and alternative financial systems, including discussions of a common BRICS currency. These de-dollarization initiatives reflect a broader desire to create a multipolar financial system that diminishes the outsized role of the dollar and insulates their economies from US sanctions and monetary policy decisions.

In response to sanctions, countries have intensified their search for alternatives to the dollar, Russia foremost among them following the increase of sanctions after its invasion of Ukraine. Russia has accelerated efforts to develop a digital ruble and has allowed certain entities to use cryptocurrencies for international trade. These strategies aim to bypass the traditional financial system, reducing reliance on the US dollar while creating payment channels less vulnerable to Western sanctions. Russian President Vladimir Putin highlighted this shift, stating, “The dollar was used as a weapon. It is true... If they don’t let us work with it, what else should we do? We should seek other alternatives.”⁴⁷ Similarly, Venezuela’s launch of the Petro in 2018 was explicitly marketed as a tool to evade US sanctions, though its success has been limited.

These examples underscore a growing trend: nations under economic pressure are exploring ways to circumvent the dollar-centric financial system. This movement reflects a broader sentiment that the global concentration of financial power in the United States creates vulnerabilities for other nations, fueling efforts to decentralize the international monetary system. If successful, such moves could significantly reshape the global financial order, challenging the dollar’s supremacy and diminishing the United States’s ability to wield sanctions as a foreign policy tool.

Recommendations

Ultimately, cryptocurrency’s transparency is a strength, not a flaw. Properly understood, it offers a unique opportunity to enhance the fight against illicit finance. To ensure this potential is fully realized, it is imperative to dispel misconceptions and establish cohesive policies that prevent criminal use while encouraging innovation. Cryptocurrency itself is not the root of the problem. Rather, the issue lies in the absence of a comprehensive, multi-governmental strategy that is adequately funded and equipped to understand and target the criminals who exploit this technology.

The challenges and opportunities presented by cryptocurrency represent a pivotal moment for policymakers. Through thoughtful, well-informed regulation, the United States can leverage the transparency and efficiency of blockchain technology to bolster the fight against illicit finance and solidify its position as a global leader in innovation. As discussed throughout this report, several key policy moves could both enable financial innovation while mitigating illicit

use and empowering law enforcement to act:

- **Regulatory clarity on oversight agencies:** Clarity on which government agencies have jurisdiction over cryptocurrency regulation, as well as a well-defined regulatory framework from those agencies would provide legal certainty that enables businesses to grow while understanding how to mitigate fraud, consumer risk, and illicit activity. Clear regulation also limits industry flight to other friendlier jurisdictions.
- **Training for relevant investigative agencies:** Personnel should be well-versed with the capabilities of blockchain analysis and forensics when working at agencies charged with overseeing sanctions, counter-cybercrime operations, or other defense and security matters where actors may use cryptocurrency as a tool. Offering training that allows them to understand what investigative power exists and how to work with forensic labs to leverage this capability would increase government ability to track and clamp down on illicit activity.
- **International collaboration to close loopholes:** Bad actors often exploit weak security practices internationally, as well as law enforcement's variable capacity to work internationally. The United States should work with international partners to close these gaps, by sending technical assistance to facilitate stronger cybersecurity and by expanding cross-border enforcement capabilities. Improved coordination between law enforcement and cryptocurrency exchanges is also essential.
- **Public education and digital literacy efforts:** As cryptocurrency adoption increases in popularity, users need access to education on capabilities and limitations of digital assets, including practical training on secure digital transactions, understanding blockchain traceability, and recognizing sophisticated social engineering tactics used by scammers. This effort should be part of general digital literacy offerings that help consumers take advantage of modern technology while protecting themselves from new threats.

Caution is essential. The success of this endeavor depends on rejecting sensationalized narratives and fostering global cooperation to close regulatory gaps. By promoting consistent, balanced oversight, policymakers can curb misuse, preserve legitimate applications, and secure the long-term benefits of cryptocurrency for the global economy. The future of this technology—and its ability to coexist with traditional financial systems—rests on the ability to strike the right balance between regulation and innovation.

Endnotes

- 1 TRM Labs. (2023). *The Illicit Crypto Economy Report*. TRM Labs. <https://www.trmlabs.com/the-illicit-crypto-economy-report>
- 2 Hernandez, N. (2023, October 3) “I can’t imagine it working”: Old Burger King video from 1993 emerges of people freaking out over credit cards. *The Daily Dot*. www.dailydot.com/news/1993-burger-king-credit-cards/
- 3 U.S. Department of Justice, Drug Enforcement Administration. (2024, May). *National Drug Threat Assessment 2024 (Report No. DEA-DCT-DIR-010-24)*. U.S. Department of Justice. https://www.dea.gov/sites/default/files/2024-05/NDTA_2024.pdf
- 4 Ferwerda J., & Reuter, P. (2024). *National assessments of money laundering risks: Stumbling at the start*. Risk Analysis. Wiley-Blackwell. <https://doi.org/10.1111/risa.14302>
- 5 Talley, A., & Berwick, I. (2023, October 10). “ Hamas militants behind Israel attack raised millions in crypto.” *The Wall Street Journal*. <https://www.wsj.com/world/middle-east/militants-behind-israel-attack-raised-millions-in-crypto-b9134b7a>
- 6 Warren, E., et al. (2023). *Letter to Treasury and White House re: Hamas crypto security*. <https://www.warren.senate.gov/imo/media/doc/2023.10.17%20Letter%20to%20Treasury%20and%20White%20House%20re%20Hamas%20crypto%20security.pdf>
- 7 Chainalysis Blog. (2023, October 18). *Cryptocurrency and terrorism financing: correcting the record*. Retrieved from <https://www.chainalysis.com/blog/cryptocurrency-terrorism-financing-accuracy-check/>
- 8 Elliptic Blog. (2023, October 25). *Setting the record straight on crypto crowdfunding by Hamas*. Retrieved from <https://www.elliptic.co/blog/setting-the-record-straight-on-crypto-crowdfunding-by-hamas>
- 9 Al-Mughrabi, N. (2023, April 28). “ Hamas armed wing announces suspension of Bitcoin Fundraising.” *Reuters*. Retrieved from, <https://www.reuters.com/world/middle-east/hamas-armed-wing-announces-suspension-bitcoin-fundraising-2023-04-28/>.
- 10 U.S Department of Treasury. (2024, February). *2024 national terrorist financing risk assessment*. <https://home.treasury.gov/system/files/136/2024-National-Terrorist-Financing-Risk-Assessment.pdf>
- 11 U.S Department of Treasury. (2024, February). *2024 national terrorist financing risk assessment* (p. 20). <https://home.treasury.gov/system/files/136/2024-National-Terrorist-Financing-Risk-Assessment.pdf>
- 12 Nichols, J., et al. (2022, May 12). *Cryptocurrencies and U.S. sanctions evasion: Implications for Russia*. Center for Strategic and International Studies (CSIS), <https://www.csis.org/analysis/cryptocurrencies-and-us-sanctions-evasion-implications-russia>
- 13 Whittell, G. (2018, May 3). “How a billion-dollar cyberheist foiled its victims.” *The New York Times*. <https://www.nytimes.com/interactive/2018/05/03/magazine/money-issue-bangladesh-billion-dollar-bank-heist.html>
- 14 Chainalysis Team. (2023, February 1). *2022 biggest year ever for crypto hacking with \$3.8 Billion Stolen, primarily from DeFi protocols and by North Korea-linked attackers*. Chainalysis. <https://www.chainalysis.com/blog/2022-biggest-year-ever-for-crypto-hacking/>
- 15 Nichols, J., et al. (2022, May 12). *Cryptocurrencies and U.S. sanctions evasion: Implications for Russia*. Center for Strategic and International Studies (CSIS), <https://www.csis.org/analysis/cryptocurrencies-and-us-sanctions-evasion-implications-russia>
- 16 Smith, J. (2023, February 6). “Crypto hacks stole record \$3.8 billion in 2022, led by North Korea Groups - report.” *Reuters*. <https://www.reuters.com/technology/crypto-hacks-stole-record-38-billion-2022-led-by-north-korea-groups-report-2023-02-01/>
- 17 Lyngaas, S. (2022, September 9). “US seizes \$30 million in stolen cryptocurrency from North Korean hackers.” *CNN Politics*. <https://www.cnn.com/2022/09/08/politics/fbi-north-korea-hackers-30-million-axie-infinity/index.html>
- 18 Howcroft, E., & Pearson, J. (2023, February 16). “Norway seizes record \$5.8 million of crypto stolen by North Korea.” *Reuters*. <https://www.reuters.com/technology/norway-seizes-record-58-million-crypto-stolen-by-north-korea-2023-02-16/>
- 19 U.S. Department of the Treasury. (2024, December 17). *Treasury Disrupts North Korean Digital Assets Money*

- Laundering Network*. U.S. Department of the Treasury. Retrieved February 26, 2025, from <https://home.treasury.gov/news/press-releases/jy2752>
- 20 Sayki, I. (2022, July 22). *U.S. Seizes Crypto Funds from North Korean Ransomware Attack*. Organized Crime and Corruption Reporting Report. Retrieved Feb 26, 2025, from <https://www.occrp.org/en/news/us-seizes-crypto-funds-from-north-korean-ransomware-attack>
 - 21 Center for a New American Security. (2019, June 4). *Sanctions by the numbers: The geographic distribution of U.S sanctions*. <https://www.cnas.org/publications/reports/sanctions-by-the-numbers-1>.
 - 22 Zmudzinski, A. (2019, November 24). *Former Soviet metal construction plant is now mining Bitcoin*. Cointelegraph. <https://cointelegraph.com/news/russian-oligarch-turns-soviet-plant-into-a-major-bitcoin-mining-hub>
 - 23 Wright, T. *Iranian general calls for use of crypto to evade sanctions*. Cointelegraph. <https://cointelegraph.com/news/iranian-general-calls-for-use-of-crypto-to-evade-sanctions>.
 - 24 Reuters Staff. (2024, April 2). *Iran's oil exports reached \$35 Billion in last 12 months - ILNA*. Reuters. <https://www.reuters.com/markets/commodities/irans-oil-exports-reached-35-billion-last-12-months-ilna-2024-04-02/>.
 - 25 The Economist. (2024, October 17). *Inside the secret oil trade that funds Iran's wars*. The Economist. <https://www.economist.com/finance-and-economics/2024/10/17/inside-the-secret-oil-trade-that-funds-irans-wars>.
 - 26 Lindrea, B. (2022, August 10). *Iran makes \$10M import with cryptocurrency, plans 'widespread' use by end of Sept*. Cointelegraph. <https://www.cointelegraph.com/news/iran-makes-10m-import-with-cryptocurrency-plans-widespread-use-by-end-of-sept>
 - 27 Chainalysis. (2023, January 25). *Crypto money laundering: Insights from 2022*. Chainalysis Blog. <https://www.chainalysis.com/blog/crypto-money-laundering-2022/>
 - 28 BDO Canada. (2022, October 27). *Case study: BitConnect cryptocurrency fraud*. BDO Canada. <https://www.bdo.ca/insights/cryptocurrency-execs-charged-for-2-4-billion-ponzi-scheme>
 - 29 U.S Department of Justice. (2022, February 25). *BitConnect founder indicted in global \$2.4 billion cryptocurrency scheme*. U.S. Department of Justice. www.justice.gov/archives/opa/pr/bitconnect-founder-indicted-global-24-billion-cryptocurrency-scheme.
 - 30 PonziTracker. (2024, December 13). *PonziTracker*. Retrieved January 3, 2025, from <https://www.ponzitracker.com/>
 - 31 Chainalysis Team. (2024, February 24). *The on-chain footprint of Southeast Asia's 'pig butchering' compounds: Human trafficking, ransoms, and hundreds of millions scammed*. Chainalysis. <https://www.chainalysis.com/blog/pig-butchering-human-trafficking/>
 - 32 Federal Trade Commission (2023, February 9th). *Romance scammers' favorite lies exposed*. Federal Trade Commission. <https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/02/romance-scammers-favorite-lies-exposed>
 - 33 U.S. Federal Bureau of Investigation. (2017, July 20). *Darknet Takedown: Authorities Shutter Online Criminal Market AlphaBay*. FBI.gov. Retrieved February 26, 2025, from <https://www.fbi.gov/news/stories/alphabay-takedown>
 - 34 Office of Public Affairs. (2022, April 5). *Justice Department Investigation Leads to Shutdown of Largest Online Darknet Marketplace*. U.S. Department of Justice. Retrieved February 26, 2025, from <https://www.justice.gov/archives/opa/pr/justice-department-investigation-leads-shutdown-largest-online-darknet-marketplace>
 - 35 TRM Labs. (2024, August 1). *Illicit cryptocurrency*. TRM Labs. <https://www.trmlabs.com/report#Illicit-Cryptocurrency>
 - 36 Chainalysis. (2024). *The 2024 cryptocurrency crime report*. Chainalysis. <https://go.chainalysis.com/crypto-to-crime-2024.html>
 - 37 Chainalysis Team. (2019, October 16). *Chainalysis in Action: DOJ Announces Shutdown of Largest Child Pornography Website*. Chainalysis. <https://www.chainalysis.com/blog/chainalysis-doj-welcome-to-video-shutdown/>
 - 38 Chainalysis. (2024). *The 2024 cryptocurrency crime report*. Chainalysis. <https://go.chainalysis.com/crypto-to-crime-2024.html>
 - 39 Decrypt. (2024). *Tether freezes \$225M USDT, feds say is linked to human trafficking*. Decrypt. <https://decrypt.co/206694/tether-freezes-225m-usdt-feds-say-is-linked-to-human-trafficking>

-
- 40 Tether. (2023, October 31). *Tether freezes 32 addresses linked to terrorism and warfare in Israel and Ukraine*. Tether. <https://tether.io/news/tether-freezes-32-addresses-linked-to-terrorism-and-warfare-in-israel-and-ukraine/>
- 41 Chainalysis Team. (2024, February 7). *Ransomware Hit \$1 Billion in 2023*. Chainalysis. Retrieved February 25, 2025, from <https://www.chainalysis.com/blog/ransomware-2024/>
- 42 U.S. Department of Justice. (2023, January 26). *U.S. Department of Justice disrupts Hive ransomware variant*. U.S. Department of Justice. <https://www.justice.gov/archives/opa/pr/us-department-justice-disrupts-hive-ransomware-variant>
- 43 Chainalysis Team, *Ransomware Hit \$1 Billion in 2023*. Chainalysis. <https://www.chainalysis.com/blog/ransomware-2024/>
- 44 Chainalysis Team. (2024, November 13). *All Crime is Crypto Crime: Gurvais Grigg on How Blockchain Intelligence is Changing Law Enforcement*. Chainalysis. Retrieved February 25, 2025, from <https://www.chainalysis.com/blog/blockchain-intelligence-is-changing-law-enforcement/>
- 45 Chainalysis. (2023). *Privacy coins: Anonymity-enhanced cryptocurrencies*. Chainalysis. <https://www.chainalysis.com/blog/privacy-coins-anonymity-enhanced-cryptocurrencies>
- 46 Forbes. (2024, September 23). "Crypto prices." *Forbes*. <https://www.forbes.com/digital-assets/crypto-prices/?sh=5057f0122478>
- 47 Gomez, E. (2024, October 23). *BRICS Bitcoin strategy summit*. Crypto Briefing. <https://cryptobriefing.com/brics-bitcoin-strategy-summit/#:~:text=BRICS%20lawmakers%20advocate%20for%20Russian,of%20digital%20assets%20at%20VanEck>

About the Authors

Kristofer Doucette is the CEO of Applied Technology Solutions (ATS), a company specializing in comprehensive intelligence services tailored to customers with complex needs. ATS provides a broad spectrum of open-source competencies, including social media monitoring, corporate due diligence, and financial intelligence. Mr. Doucette brings over two decades of experience in financial intelligence, sanctions, and national security.

Before ATS, he spent six and a half years at Chainalysis, where he was instrumental in establishing and expanding the company's efforts with U.S. government agencies to combat illicit cryptocurrency activities. Prior to joining Chainalysis in January 2018, Mr. Doucette spent over 14 years at the U.S. Department of the Treasury, specializing in terrorist financing, sanctions evasion, and money laundering. In December 2014, he co-led a multi-agency cell focused on combating Islamic State finances, working closely with various branches of the U.S. government.

Jen Jensen is the Chief Operating Officer of Applied Technology Solutions (ATS). With over 15 years of experience in open-source intelligence supporting federal government clients, Mrs. Jensen directs the company's operational strategy and execution. Her career includes successful roles as Public Sector Capture Manager at Zignal Labs and Federal Account Executive at Zayo Group, where she developed expertise in government contracting and strategic account management. Ms. Jensen holds both an MBA and a BBA in Business Administration and Management, applying her academic foundation to drive ATS's delivery of comprehensive intelligence services.

Tonja Denny is a Senior Intelligence Analyst and Financial Intelligence Specialist at Applied Technology Solutions (ATS). Mrs. Denny combines her academic background in Sociology of Law, Criminology, and Deviant Behavior with professional experience in investigations and homicide research. She brings a unique skill set to intelligence work with her training as a Forensic Artist and experience in Graphic Design and Visual Information.

Sydney Robertson is a Senior Intelligence Analyst and Financial Intelligence Specialist at Applied Technology Solutions (ATS). Mrs. Robertson uses her education in strategic intelligence to deliver high-quality intelligence services. She is currently expanding her expertise by pursuing additional education in Cybersecurity and Information, reinforcing ATS's commitment to providing cutting-edge intelligence solutions in an evolving security landscape.

Adam Hill is a Senior Intelligence Analyst at Applied Technology Solutions (ATS) with over 10 years of experience in the technology, defense, and intelligence sectors. He currently serves as Mission Delivery Manager and Senior Solutions Consultant, developing strategic partnerships and leading pre-sales efforts for government clients. His background includes six years at Joint Special Operations Command, where he directed portfolio managers across five major divisions

and coordinated collaboration between the Department of Defense and National intelligence agencies. Mr. Hill previously worked as a Business Development Consultant at Front Line Advisory Group, connecting technology providers with military technical requirements managers. He holds a degree in Criminal Justice with an emphasis in Counter-Terrorism and Homeland Security and has studied Project Management.

Isaac Rits is an Intelligence Intern at Applied Technology Solutions (ATS), currently completing his B.A. in Strategic Intelligence in National Security at Patrick Henry College. Mr. Rits previously served as a Border Security and Immigration Intern at The Heritage Foundation, where he gained valuable experience in policy analysis and national security matters. His academic focus and practical experience align with ATS's mission to provide comprehensive intelligence services.






Sean Swentkowski is currently pursuing a B.S. in Accounting at the University of Tampa. He serves as a University Ambassador and is an active member of the personal finance club, developing analytical skills and financial knowledge through his academic studies and extracurricular activities.

Kellee Wicker directs the Science and Technology Innovation Program at the Wilson Center, a Congressionally-chartered think tank that provides nonpartisan counsel and insights on global affairs to policymakers through deep research, impartial analysis, and independent scholarship. The STIP team provides research and insight to Congress, global policymakers, and the general public on a number of emerging technologies and scientific advances, with special emphasis on artificial intelligence, cybersecurity, space in the commercial age, and more. Through games, experiential learning, and educational opportunities, STIP also works beyond traditional research to directly provide policymakers and their staff with the foundational knowledge they need to devise smart legislation and regulation that protects individuals and workers while continuing to bolster flourishing technological innovation.






Woodrow Wilson International Center for Scholars
One Woodrow Wilson Plaza
1300 Pennsylvania Avenue NW
Washington, DC 20004–3027

The Wilson Center

-  wilsoncenter.org
-  [woodrowwilsoncenter](https://www.facebook.com/woodrowwilsoncenter)
-  [@TheWilsonCenter](https://twitter.com/TheWilsonCenter)
-  [@thewilsoncenter](https://www.instagram.com/thewilsoncenter)
-  [The Wilson Center](https://www.linkedin.com/company/the-wilson-center)

Science and Technology Innovation Program

-  wilsoncenter.org/science-and-technology-innovation-program
-  [@WilsonSTIP](https://twitter.com/WilsonSTIP)
-  [linkedin.com/showcase/science-and-technology-innovation-program](https://www.linkedin.com/showcase/science-and-technology-innovation-program)