Traceable Money

Blockchain Analytics and the Conditions for Crypto Institutionalization

About

Metanomia is a think tank focused on analyzing transformations in the cryptocurrency market and related technologies.

Researchers

Sanghyeon Park

Corresponding Author

Taemin Oh

Contents

Introduction

Have you ever seen a scene in a film or television where kidnappers demand a ransom? The criminals on screen no longer ask for bags of cash. They ask for Bitcoin. Embedded within that brief scene is a familiar assumption: no names, no identities, and no easy way to trace the money. Most audiences rarely question that assumption. The belief that crypto is untraceable money has already become part of popular common sense.

That perception was not simply a popular misunderstanding. For the libertarians and cypherpunks who shaped the early crypto ecosystem, anonymity was central to the design itself. Crypto emerged as a technological expression of the belief that individuals should be able to protect their economic freedom from the control of states and central banks. The drug vendors of Silk Road chose Bitcoin for that reason. Ransomware groups demanded payment in crypto for the same reason. North Korea turned stolen crypto assets into a source of state revenue based on that same belief. For a time, the belief even appeared to hold true in reality.

Yet that gap quietly — and rapidly — began to narrow. As blockchain analytics technologies emerged, it became possible to trace the flow of funds hidden behind anonymous wallet addresses, analyze transaction patterns, and connect specific addresses to real organizations or individuals.

In 2018, Jeongwoo Son, the operator of the world's largest child sexual exploitation website, Welcome to Video, was arrested. Operating through Bitcoin payments, the site was ultimately dismantled through an international investigation spanning 38 countries, leading to the arrest of 337 individuals. The U.S. Internal Revenue Service Criminal Investigation division (IRS-CI) played a key role by tracing Bitcoin transaction flows and identifying critical leads that helped pinpoint the operator. Following international cooperation, Son was arrested by South Korean police.[1] The crime had operated on the belief that Bitcoin was anonymous money. In the end, it collapsed because of the very records that money left behind.

States still remain uncomfortable with crypto. And complete control remains impossible. But states now know that, when necessary, crypto can be traced and blocked. Governments around the world began casting regulatory nets over the crypto ecosystem. Crypto, once seen as existing beyond the reach of the state, is now being reframed in terms acceptable to institutional finance. Where did that confidence come from?

This report follows that question. It examines how the maturation of blockchain analytics technologies became one of the central conditions for the institutionalization of crypto. It also explores how the logic that "what can be analyzed can be managed, and what can be managed can be institutionalized" fundamentally transformed the landscape surrounding crypto.

1) U.S. Department of Justice, “South Korean National and Hundreds of Others Charged Worldwide in the Takedown of the Largest Darknet Child Pornography Website, Which Was Funded by Bitcoin,” Office of Public Affairs, October 16, 2019, accessed April 16, 2026, https://www.justice.gov/archives/opa/pr/south-korean-national-and-hundreds-others-charged-worldwide-takedown-largest-darknet-child.

01

Blockchain Analytics Technology

The Paradox of the Public Ledger: All Can See It, But Not All Can Read It

Blockchain appears anonymous and yet entirely public at the same time. Every transaction is permanently recorded on a public ledger that anyone can inspect. All transactions occurring on the Bitcoin network can be queried in real time through a blockchain explorer. Every record of when a particular wallet address sent funds, how much, and to which address is disclosed with full transparency. This transparency is a core design principle of blockchain. All participants share the same ledger in order to prevent double-spending and guarantee the integrity of transactions.

Yet this transparency is deliberately only half-open. Transaction records are visible, but the parties behind those transactions are not. On the blockchain, users exist not as names or account numbers but solely as strings of characters called wallet addresses. Addresses in the form of 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa stand in for the sender and recipient of a transaction. Nowhere in the ledger is there any record of who owns that address or what purpose it serves. The data exists, but without context.

This is precisely where the paradox arises. Blockchain is a transparent ledger that makes every transaction public, yet it tells you nothing about whose transactions those are. Transparency and pseudonymity coexist within a single structure. The transaction records are fully disclosed, but the ability to convert those records into meaningful information — the ability to read them — is not given to everyone. In an environment where millions of wallet addresses and billions of transaction data points pour forth, determining who owns a particular address, or which flows of funds are connected to criminal activity, is in practice extremely difficult without sophisticated technology and vast data. All can see it, but not all can read it.

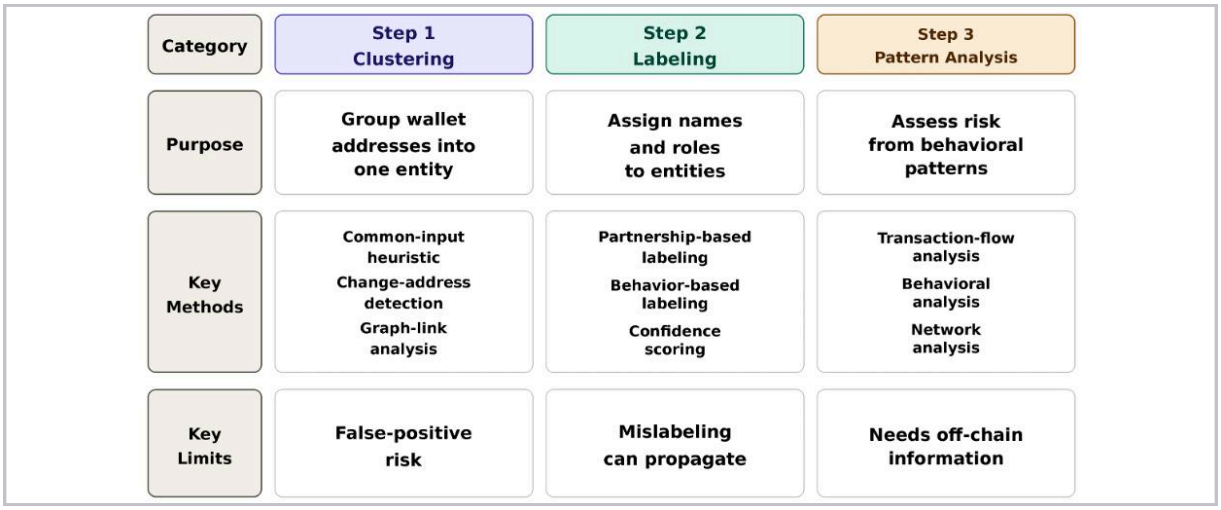
The political scientist James C. Scott, in his book Seeing Like a State, observed that for a state to govern society it must first convert it into a "legible form." To manage a forest, trees must be classified and surveyed; to manage a population, surnames and addresses must be standardized. Abstracting a complex reality into a simplified form that the state can perceive and intervene in — that, he argued, is the starting point of governance.[2] The key point in Scott's logic is that visibility is not simply a matter of collecting information. Making something readable is an act of converting it into a manageable object, and it is at that moment that the governing power of the state begins to operate. What cannot be seen cannot be managed, and what cannot be managed cannot be institutionalized.

2) James C. Scott, Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed (New Haven: Yale University Press, 1998).

Blockchain is a space where Scott's insight finds new expression in the digital age. As we have seen, the blockchain ledger is transparent but not legible. Blockchain analytics technology is a translation apparatus — one that converts this visible ledger into a readable one; that is, it transforms context-free transaction records into information in which actors, actions, and risks are linked together.

Clustering, Labeling, and Pattern Analysis: The Common Methodology of the Blockchain Analytics Industry

The blockchain analytics industry broadly shares three methodological stages for linking anonymous wallet addresses to real-world actors and detecting criminal signals within flows of funds: clustering, labeling, and pattern analysis. These three stages operate in close combination, forming the core structure that transforms raw transaction records into actionable investigative intelligence. Major blockchain analytics firms — including Chainalysis, Elliptic, and TRM Labs — all operate on the basis of this methodology.

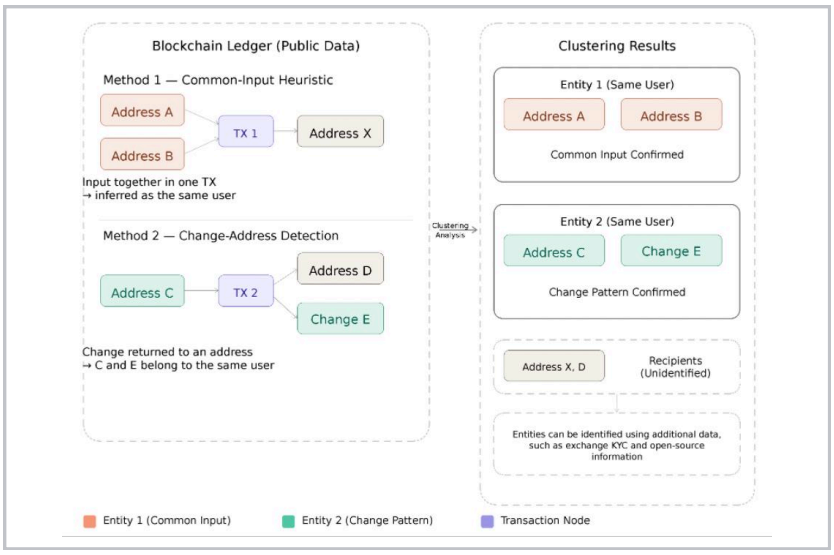


[Figure 1] **Core Methodology of Blockchain Analytics: Clustering, Labeling, and Pattern Analysis**

The first stage, clustering, is the technique of grouping multiple wallet addresses on the blockchain into a single entity. Because a single user can generate hundreds or even thousands of wallet addresses, examining data at the level of individual addresses alone makes it difficult to identify the actual actor behind them. Clustering employs several techniques to solve this problem. The Common-Input Heuristic, for example, infers that when multiple addresses are used as inputs in a single transaction, those addresses are controlled by the same user. The Change Address Heuristic analyzes the pattern of change addresses — the addresses to which remaining funds are returned after a payment — in UTXO[3]-based blockchains, and groups them into the same entity.[3] Graph-based connection analysis is layered on top of this, tracking a single user group within a network in which addresses and transactions are represented as nodes and edges, combining time, amounts, and behavioral

3) UTXO (Unspent Transaction Output) is the asset-recording model adopted by Bitcoin. Whereas a conventional bank account maintains a single balance that increases and decreases over time, the UTXO model represents ownership as a collection of individual unspent outputs. Like physical banknotes in a wallet, a UTXO is consumed in its entirety when spent. Any remaining value is typically returned as a newly created output to a change address generated by the wallet software.

patterns. Clustering is the foundational stage that determines the accuracy of all subsequent analysis.

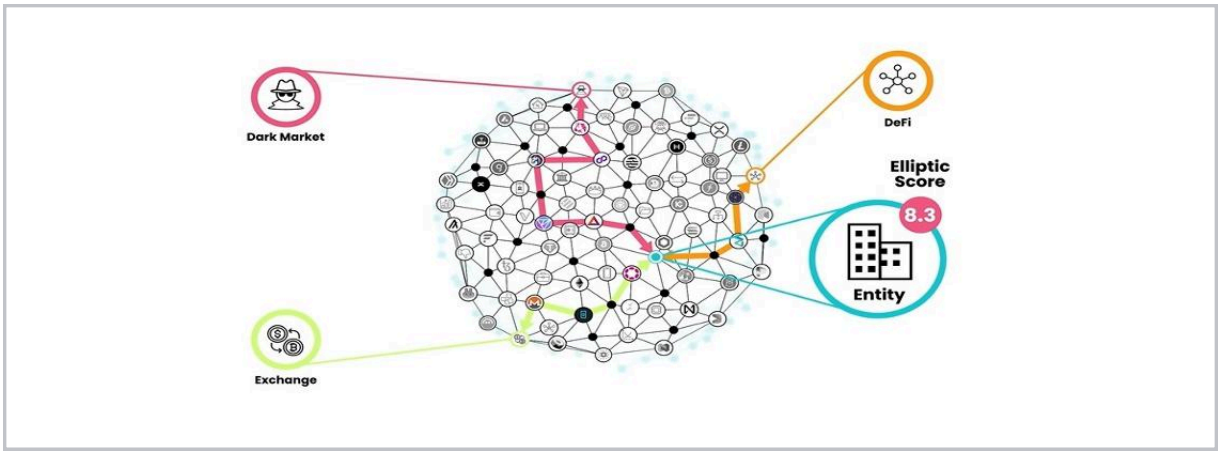


[Figure 2]
Clustering Process Using Common-Input and Change-Address Heuristics

False positives arising in this process — errors in which addresses belonging to distinct entities are incorrectly grouped into the same entity — can undermine the reliability of the analysis as a whole. Cybersecurity researchers Kelvin Lubbertsen, Michel van Eeten, and Rolf van Wegberg verified the effectiveness of blockchain analytics techniques using server data obtained from actual illicit services. Their study found that Chainalysis's clustering accuracy varies considerably depending on the type of service being analyzed. True positive rates ranged widely by service, from 24.54% for Bestmixer to 94.85% for Wall Street Market, while false positive rates remained below 0.15% in all cases.[4] This means that labels assigned by analytics firms can function as a reliable lower bound, but it cannot be assumed that unlabeled addresses are necessarily unrelated to illicit services. This limitation remains a challenge across the industry, and ongoing efforts to improve accuracy continue through machine learning, integration with external datasets, and real-time address verification in cooperation with exchange partners.

The second stage, labeling, is the process of assigning identity to addresses or entities grouped through clustering. If clustering creates a shape, labeling is the stage that assigns a name and role to it. The outputs of labeling include classifying a particular cluster as the hot wallet of a global exchange, an OTC desk, or a ransomware-linked address. Labeling is carried out primarily through three methods. Partnership-based labeling — directly labeling wallet address data received through cooperation with exchanges or financial institutions — carries the highest reliability. Behavioral labeling is used when official data is unavailable: on-chain behavioral characteristics such as transaction frequency, deposit and withdrawal patterns, and mixer usage are analyzed to infer patterns. A confidence score is then assigned to quantify the reliability of each label and indicate the degree to which it can be trusted.

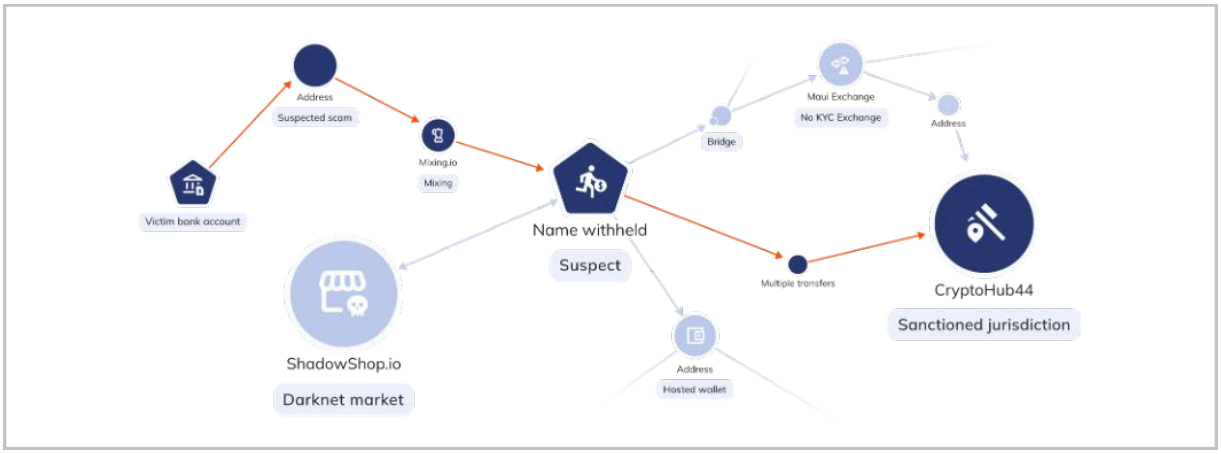
4) Kelvin Lubbertsen, Michel van Eeten, and Rolf van Wegberg, "Ghost Clusters: Evaluating Attribution of Illicit Services through Cryptocurrency Tracing," in Proceedings of the 34th USENIX Security Symposium, August 13–15, 2025, 1363, https://www.usenix.org/system/files/usenixsecurity25-lubbertsen.pdf.
The true positive rate refers to the proportion of actual illicit service addresses correctly identified, while the false positive rate refers to the proportion of legitimate addresses incorrectly classified as illicit. A lower true positive rate indicates more failures to detect illicit services, whereas a lower false positive rate indicates fewer innocent addresses being misclassified.



[Figure 3] **Entity Identification (Labeling)**
Source: Elliptic

The greatest risk to guard against in labeling is false label propagation. If a single incorrect label spreads like a domino to other connected clusters, it can lead to the serious error of classifying a legitimate user's wallet as a suspicious address. The fact that labeling criteria and risk assessment logic are protected as trade secrets, making external verification impossible, amplifies this risk further — and it remains an important challenge for the industry.

The third stage, pattern analysis, evaluates the level of risk and the likelihood of criminal activity by analyzing the behavioral patterns of labeled entities. The core task goes beyond identifying an entity to reading how that entity behaves. A cluster with frequent outflows and dispersed inflows is likely an exchange; small repeated transfers are classified as resembling phishing or scam patterns; sending large amounts to mixing services is interpreted as an attempted money laundering. Pattern analysis reveals abnormal behavior and hidden criminal signals through three methods: transaction flow analysis, behavioral analysis, and network analysis. This stage plays the most decisive role in anti-money laundering (AML) activity and criminal investigations.



[Figure 4] **Illicit Fund Movement Routes via Mixers and Bridges**
Source: Chainalysis

The Symbiosis of Analytics Firms and the State: How Private Technology Became Public Infrastructure

The existence of blockchain analytics technology and the establishment of that technology as public infrastructure trusted and relied upon by the state are two entirely different matters. The

mere existence of a technology does not produce institutionalization. The key question is how that technology becomes incorporated into the machinery of governance. To understand this structure, however, it is useful to begin somewhere other than blockchain itself.

Palantir: A Precedent for Private Technology Becoming the Eyes of the State

Founded in 2003 under the leadership of PayPal co-founder Peter Thiel, Palantir Technologies was never an ordinary startup. In 2005, the company received an initial investment of $1.25 million from In-Q-Tel, the venture capital arm of the CIA. More importantly, the CIA directly participated in improving Gotham, Palantir's first software product, and became one of its earliest major customers.[5)]

Palantir was not merely a company that received government funding. It was a company whose software was co-developed with a state intelligence agency from the design stage onward. This starting point defined the company's nature. Although formally a private enterprise, Palantir was born out of the needs of the state.

Palantir's flagship platform, Gotham, is designed to integrate and analyze vast quantities of heterogeneous data within a single environment. Arrest records, license-plate recognition data, immigration records, social media activity, and numerous other fragmented datasets that were previously held separately by different agencies are brought together and transformed into searchable information. Law-enforcement agencies and government analysts use the platform to map social networks, track movements, identify individuals through physical characteristics, and review criminal histories. Tasks that once required weeks of cross-checking across separate systems can now be completed within hours.[6)]

By 2025, Palantir generated approximately $1.855 billion in revenue from the U.S. government, accounting for roughly 41 percent of its total revenue of $4.475 billion.[7)]

The structure demonstrated by Palantir is both simple and powerful. Rather than merely selling software to government agencies, the company embeds engineers within those agencies and jointly develops customized tools for tracking terrorist networks, criminal activity, and financial fraud. Technology and state power were not separate; they were designed from the outset as parts of the same ecosystem. Palantir provided a clear illustration of how that ecosystem operates.

Chainalysis: Becoming the State's New Eyes on the Blockchain

If Palantir became the eyes of the state by integrating diverse datasets, Chainalysis became the state's new eyes by tracing the flow of funds on public blockchains. The object of analysis changed, but the underlying structure remained the same: private technology became incorporated into state infrastructure.

5) Tom Knowles, "'Our Product Is Used, on Occasion, to Kill People': Inside Palantir, the World's Scariest AI Company," BBC Science Focus, March 23, 2026, accessed May 12, 2026, https://www.sciencefocus.com/future-technology/inside-palantir-the-worlds-scariest-ai-company.

6) The Conversation, "When the Government Can See Everything: How One Company—Palantir—Is Mapping the Nation's Data," The Conversation, January 20, 2026, accessed May 12, 2026, https://theconversation.com/when-the-government-can-see-everything-how-one-company-palantir-is-mapping-the-nations-data-263178.

7) Palantir Technologies, FY 2025 Earnings Release, SEC Form 8-K, February 2026, accessed May 12, 2026, https://www.sec.gov/Archives/edgar/data/0001321655/000132165526000004/a2025q4ex991earningsrelease.htm. Author's calculation.

Chainalysis was founded in 2014 in the aftermath of the Mt. Gox hack.[8] When approximately 850,000 BTC vanished from what was then the world's largest Bitcoin exchange, the incident threw into sharp relief the need for specialized tools capable of visualizing and tracing blockchain transactions. Chainalysis was among the first companies to meet that need in a systematic and scalable way.

From its earliest years, the company built cooperative relationships with major U.S. law-enforcement and regulatory agencies, including the FBI and the IRS,[9] establishing a powerful first-mover advantage that soon expanded into a network effect. Because Chainalysis had accumulated and labeled vast volumes of on-chain data ahead of its competitors, a virtuous cycle took hold: the more institutions used Chainalysis, the more refined its data became; the more refined its data became, the more institutions chose Chainalysis. In practice, Chainalysis's exchange customers share tens of thousands of wallet addresses with the company every day, enabling real-time verification of clustering accuracy. This self-reinforcing data loop creates a competitive advantage that rival latecomers cannot easily close. Today, Chainalysis is widely regarded as the dominant firm in the global blockchain analytics market, with more than 1,500 organizations using its platform worldwide.[10]

Geopolitics also plays a decisive role in this position. For U.S. agencies such as the FBI and the Financial Crimes Enforcement Network (FinCEN), relying on infrastructure provided by an American company is a natural choice from the perspectives of data sovereignty and legal jurisdiction. In a world where the United States occupies the center of the global financial system, analytical frameworks adopted as standards by U.S. institutions often become de facto global standards. The fact that investigative agencies and exchanges in South Korea, Europe, and Japan routinely cooperate using Chainalysis data is a direct consequence of this structure.

As a result, private blockchain analytics firms such as Chainalysis have evolved beyond the role of technology vendors. They now function as public infrastructure upon which states depend in order to govern and manage crypto. As with Palantir, private technology has become an instrument of public power. The same pattern is now unfolding in the blockchain sector. Only when this structure is in place do the conditions for the institutionalization of crypto fully emerge.

That said, blockchain analytics technology alone has its limits. For ordinary transactions conducted through exchanges, combining KYC (Know Your Customer) information with on-chain data is sufficient to identify the individuals involved. The problem arises with sophisticated criminals who conceal their identities thoroughly and bypass exchanges altogether. In such cases, off-chain information — law enforcement HUMINT, devices obtained through search and seizure, testimony from victims who have escaped — becomes the first link connecting a specific wallet address to a real person. The moment that link is secured, blockchain analytics operates as an amplifier capable of tracing flows of funds worth tens of billions of dollars. How this combination of off-chain and on-chain intelligence actually works in practice can be seen in the following chapter's case study of Prince Group chairman Chen Zhi.

8) Decrypt, “How Chainalysis Helps Catch Cryptocurrency Criminals,” September 7, 2020, accessed May 12, 2026, https://decrypt.co/41127/how-chainalysis-helps-catch-cryptocurrency-criminals.

9) Danny Nelson, “Inside Chainalysis’ Multimillion-Dollar Relationship With the US Government,” CoinDesk, February 10, 2020, accessed May 8, 2026, https://www.coindesk.com/business/2020/02/10/inside-chainalysis-multimillion-dollar-relationship-with-the-us-government

10) Chainalysis, “Why Chainalysis,” Chainalysis Official Website, accessed April 16, 2026, https://www.chainalysis.com/why-chainalysis.

02

Case Studies in Blockchain Analysis

The clustering, labeling, and pattern analysis described in Chapter 1 are not mere theory. These technologies have operated on actual crime scenes, redirecting the course of investigations and serving as evidentiary intelligence underpinning international sanctions. The cases below most clearly illustrate how blockchain analytics technology has evolved and how it functions as an instrument of state governance.

Lazarus and the Ronin Bridge: Tracing a Nation-State Hack

In March 2022, the Lazarus Group — believed to be affiliated with North Korea — attacked the Ronin Bridge, the underlying network of the blockchain game Axie Infinity. The method of attack was sophisticated. Lazarus seized the private keys of five of the nine validators on the Ronin network, thereby obtaining transaction approval authority, and then used that authority to approve two fraudulent transactions, stealing approximately 173,600 ETH and 25.5 million USDC.[11]

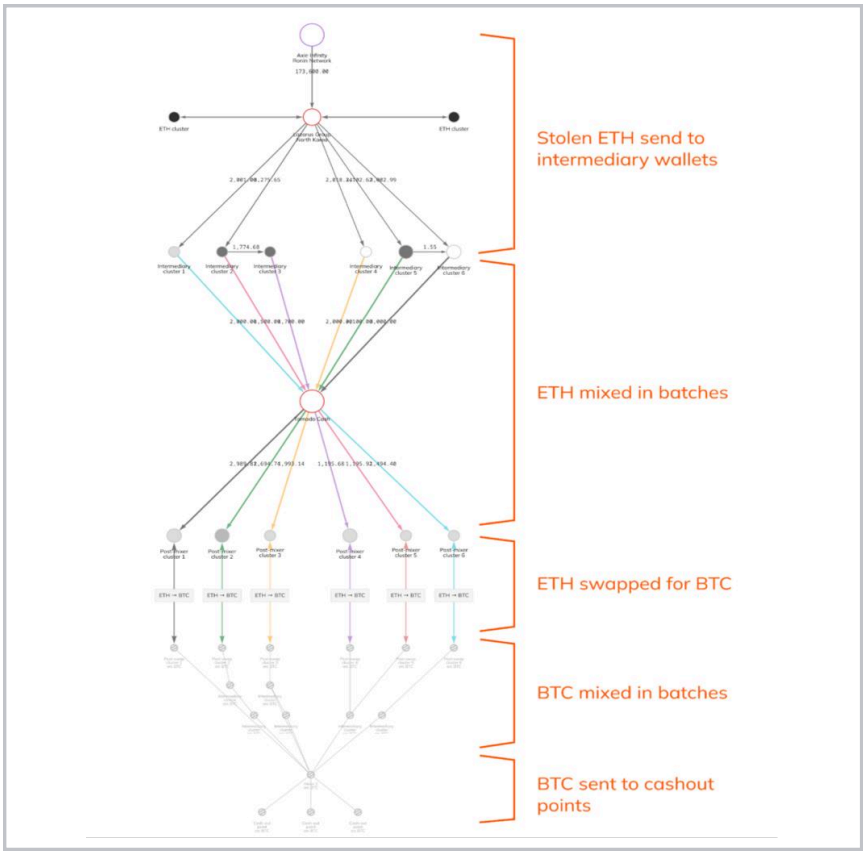
Immediately after the theft, Lazarus launched a rapid dispersal operation to make the funds difficult to trace. The stolen funds were dispersed across multiple intermediary wallets. Chainalysis succeeded in visualizing this complex flow of funds through its Reactor tool. By organizing on-chain data into graph structures, it traced step by step the routes through which the funds had moved, and reconstructed how billions of dollars' worth of stolen assets had been dispersed and mixed into a single flowchart.[12] This went beyond simple address tracking — it rendered the entirety of Lazarus's money laundering strategy visible.

Elliptic also independently traced and published the money laundering routes and movement patterns through its own public analysis. Elliptic separately analyzed the proportion of stolen funds that had completed laundering and the routes through which they had entered exchanges, sharing these findings with law enforcement and exchanges, thereby enabling them to identify and respond to the relevant funds.[13] The analyses produced by the two firms complemented one another, enhancing the accuracy of the investigation.

11) Ronin Network, "Back to Building: Ronin Security Breach Postmortem," Ronin Network Blog, April 27, 2022, archived version, accessed May 16, 2026, https://web.archive.org/web/2022/https://roninchain.com/blog/posts/back-to-building-ronin-security-breach-6513cc78a5edc1001b03c364.

12) Chainalysis, "Crypto Community Makes Profiting Hard for North Korean Hackers," Chainalysis Blog, accessed April 16, 2026, https://www.chainalysis.com/blog/axie-infinity-ronin-bridge-dprk-hack-seizure.

Lazarus's money laundering process was traced across five stages. In the first stage, the stolen ETH was dispersed across multiple intermediary wallets, severing any direct connection to the initial point of theft. In the second stage, large volumes of ETH were mixed through the mixer service[14] Tornado Cash, concealing the origin of the funds. In the third stage, ETH withdrawn from Tornado Cash was exchanged for BTC, raising the difficulty of tracing. In the fourth stage, the exchanged BTC was sent through another round of mixing services, performing a second layer of laundering. In the fifth and final stage, the laundered BTC was converted into fiat currency and cashed out.



[Figure 5]
Lazarus Group Money Laundering Routes
Source: Chainalysis

The findings of Chainalysis and Elliptic translated directly into policy action. The U.S. Treasury Department's Office of Foreign Assets Control (OFAC) drew on blockchain analytics data to impose OFAC sanctions on Tornado Cash in August 2022.[15] The designation of a decentralized, smart-contract-based mixer service was an unprecedented move.[16] This case clearly demonstrated that blockchain analytics can function not merely as an investigative support tool but as intelligence that directly underpins the state's sanctions policy.

Following the Tornado Cash sanctions, Lazarus changed its strategy. No longer relying on the well-known Ethereum-based mixer, it began making active use of various decentralized

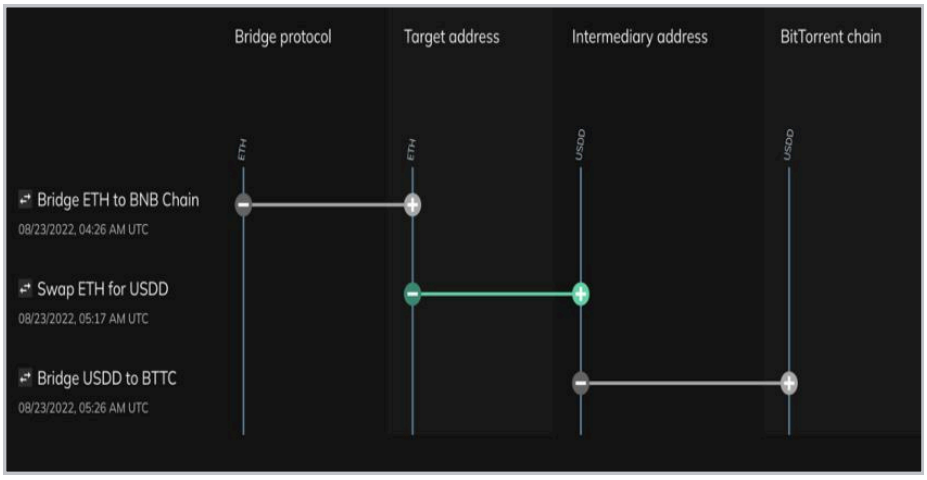
13) Elliptic, "North Korea's Lazarus Group Identified as Exploiters Behind $540 Million Ronin Bridge Heist," Elliptic Blog, April 14, 2022, accessed April 16, 2026, https://www.elliptic.co/blog/540-million-stolen-from-the-ronin-defi-bridge.

14) A mixer service combines cryptocurrency from multiple users and redistributes equivalent amounts to designated recipients, making it substantially more difficult to trace the origin and destination of funds. Such services are commonly used as privacy-enhancing or anonymization tools.

15) U.S. Department of the Treasury, "U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash," Press Release, August 8, 2022, accessed April 16, 2026, https://home.treasury.gov/news/press-releases/jy0916.

finance (DeFi)[17] services and cross-chain bridges[18] to convert assets across multiple chains — a technique known as chain hopping. Because the same assets are continuously converted across multiple blockchains and multiple token forms, tracing the flow of funds within a single coherent narrative becomes extremely difficult.

In response, Chainalysis developed a tool called Storyline. Storyline visualizes complex flows of funds moving across multiple blockchains and asset forms in a timeline format and has played a central role in identifying Lazarus's chain-hopping routes.



[Figure 6]
Storyline
Source: Chainalysis

FTX: Making Internal Corruption Visible

Blockchain analysis works not only to expose external hacks but equally to lay bare corruption from within. The FTX case is a prime example. In November 2022, FTX — one of the world's largest crypto exchanges — collapsed under a liquidity crisis. The substance of the matter was not a simple bankruptcy. At the core was the fact that founder Sam Bankman-Fried (SBF) had illegally diverted customer deposits to affiliated firm Alameda Research and used them to cover underwater positions.[19] In the immediate aftermath of the bankruptcy announcement,

16) In November 2024, the U.S. Court of Appeals for the Fifth Circuit ruled that OFAC's sanctions against Tornado Cash's immutable smart contracts were unlawful. The court held that immutable smart contracts, which cannot be owned or controlled by any person, do not constitute "property" subject to OFAC sanctions authority. In March 2025, the U.S. Treasury removed Tornado Cash from the sanctions list. Criminal proceedings against individual developers, however, continue separately. This case illustrates that legal disputes concerning the scope of state sanctions authority over decentralized protocols remain unresolved. See Digital Asset, "Why the U.S. Court Ruled That Tornado Cash Could Not Be Sanctioned," November 27, 2024, accessed May 8, 2026, https://www.digitalasset.works/news/articleView.html?idxno=23622.

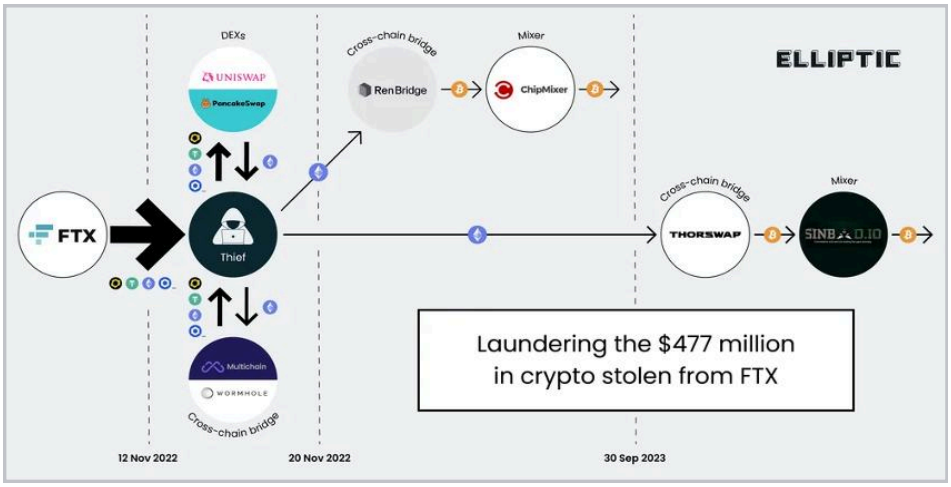
17) Decentralized finance (DeFi) refers to a blockchain-based financial system that provides services such as lending, trading, and deposits without relying on centralized intermediaries such as banks.

18) A cross-chain bridge is a protocol that enables assets to move between different blockchain networks. For example, it may allow assets originating on Ethereum to be transferred for use on another blockchain. Cross-chain bridges have also been exploited to obscure transaction trails by dispersing funds across multiple chains.

19) U.S. Department of Justice, "United States Attorney Announces Charges Against FTX Founder Samuel Bankman-Fried," U.S. Attorney's Office for the Southern District of New York, December 13, 2022, accessed April 17, 2026, https://www.justice.gov/usao-sdny/pr/united-states-attorney-announces-charges-against-ftx-founder-samuel-bankman-fried.

funds of unknown origin began flowing out of the system in abnormal patterns. It was impossible to determine immediately who was moving the funds or for what purpose, and market distrust reached an extreme.

In the midst of this chaos, blockchain analysis operated as a central tool. Elliptic traced and published the laundering routes of the stolen funds through its own independent public analysis. It was found that the stolen funds had moved through decentralized exchanges such as Uniswap and PancakeSwap, then on to cross-chain bridges such as RenBridge, before being laundered through mixer services including ChipMixer and Sinbad.[16] The identified wallets were immediately labeled and shared with major exchanges worldwide, enabling the rapid construction of a defensive system to block the inflow of suspicious funds. Blockchain analytics data ultimately served as decisive evidence in court, used to substantiate the fraud and embezzlement charges against Sam Bankman-Fried.[20]



[Figure 7]
FTX Hack Money Laundering Routes
Source: Elliptic

Bybit: Real-Time Tracing and International Cooperation

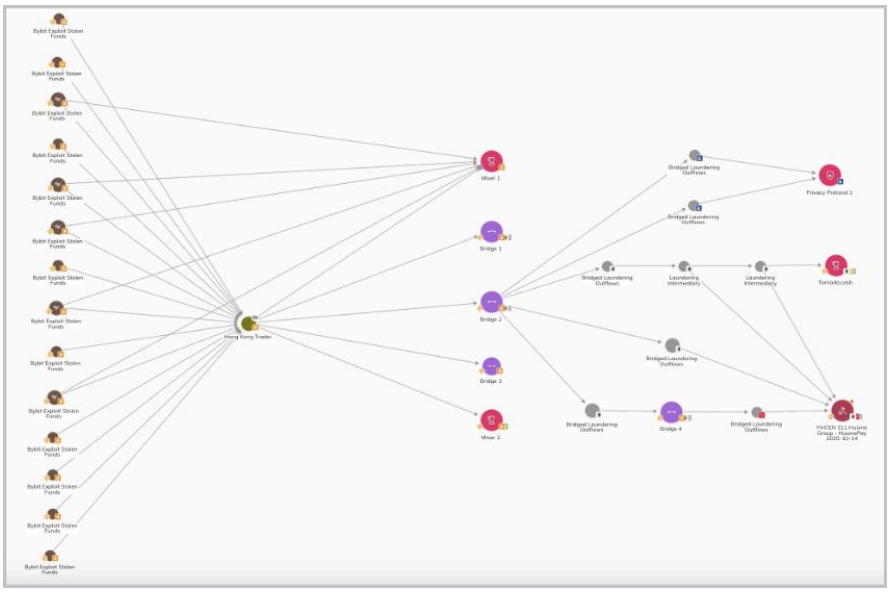
In February 2025, the TraderTraitor organization — operating under North Korea's Reconnaissance General Bureau — carried out a hack of approximately $1.5 billion against major global crypto exchange Bybit. It was the largest single theft of its kind in history. The hackers compromised the software of a third-party vendor that Bybit used for transaction signing, injecting malicious JavaScript that made it appear as though the exchange was signing ordinary transactions, and in doing so stole approximately 401,000 ETH. The attack was disguised as a routine transfer of funds from a cold wallet to a hot wallet — a regular operational procedure within the exchange — making it exceptionally difficult to detect.

The stolen funds were subsequently dispersed through various intermediary wallets and multiple networks. The hackers exchanged ETH for BTC and DAI (a decentralized stablecoin collateralized by crypto assets) and alternated between decentralized exchanges (DEXs), cross-chain bridges, and KYC-free instant swap services[21] to complicate tracing efforts. Notably, a characteristic strategy of North Korean hacker groups was also observed: certain assets were left dormant for extended periods to avoid the heightened scrutiny of the

20) Elliptic, "The $477 Million FTX Hack: A New Blockchain Trail," Elliptic Blog, November 20, 2022, accessed April 17, 2026, https://www.elliptic.co/blog/the-477-million-ftx-hack-following-the-blockchain-trail.

21) A swap service allows users to exchange one type of cryptocurrency for another through smart contracts without relying on a centralized exchange.

immediate aftermath, then reactivated after enough time had passed for the trail to grow cold.22)



[Figure 8]
Bybit Hack Money Laundering Routes
Source: Chainalysis

In this case, blockchain analytics data was shared rapidly with investigative and regulatory agencies across multiple countries, enabling key hub jurisdictions — including Hong Kong and Singapore — to cooperate in real time on the basis of the same blockchain analytics data without any lag. As a result, the movement route of the stolen funds was mapped in concrete detail. The funds were found to have passed through a Hong Kong-based trader, through various bridges and mixers, before being ultimately cashed out through Huione Pay, a subsidiary of Cambodia's Huione Group.23) This analysis subsequently became one of the decisive grounds on which the U.S. FinCEN designated Huione Pay as a subject of special measures.24)

The Case of Chen Zhi, Chairman of Prince Group: The Combination of Off-Chain and On-Chain Intelligence

The Lazarus, FTX, and Bybit cases examined above all involved blockchain analytics technology capturing criminal activity by tracing on-chain data. The Chen Zhi case, however, poses a more fundamental question: how were investigators able to detect the movement of funds worth tens of billions of dollars in near real time and take immediate freezing action? There is something in the background of this case that cannot be explained by blockchain analytics technology alone.

22) Chainalysis, "Bybit Hack: Leveraging Transparency for Collaboration in the Wake of Record-Breaking Theft," Chainalysis Blog, February 26, 2025, accessed April 16, 2026, https://www.chainalysis.com/blog/bybit-exchanc ıack-february-2025-crypto-security-dprk.

23) Chainalysis, "Five Key Takeaways from MSMT's Report on North Korean Cyber Operations," Chainalysis Blog, October 27, 2025, accessed May 17, 2026, https://www.chainalysis.com/blog/msmt-report-north-korea-dprk-cyber-threats.

24) Financial Crimes Enforcement Network (FinCEN), "FinCEN Issues Final Rule Severing Huione Group from the U.S. Financial System," News Releases, October 15, 2025, accessed April 16, 2026, https://www.fincen.gov/news/news-releases/fincen-issues-final-rule-severing-huione-group-us-financial-system.

In October 2025, the U.S. Department of Justice and OFAC indicted Chen Zhi — chairman of Cambodia-based Prince Group — on charges of wire fraud and money laundering, and seized 127,271 BTC connected to him. It was the largest single-case crypto seizure in the history of the U.S. Department of Justice. Prince Group presented itself outwardly as a real estate, financial, and entertainment conglomerate, but was in reality a transnational criminal organization operating throughout Southeast Asia that combined human trafficking, forced labor, and online investment fraud. The organization lured victims through fraudulent job advertisements, confiscated their passports, and forced them to send scam messages, siphoning astronomical sums from victims around the world.[25]

Where the first thread of the investigation came from cannot be confirmed from publicly available records alone. Yet examining the structure of the investigation allows for one reasonable inference. The reason investigators were able to detect fund movements in near real time and take immediate freezing action was that they had already identified in advance the wallet addresses Chen Zhi was using. The fact that China had been investigating Prince Group since at least 2020, that U.S. investigators had been accumulating evidence over the course of several years, and that testimony from escaped victims and international cooperative investigations had been ongoing for years — all of this strongly suggests that off-chain intelligence preceded and enabled the on-chain tracing.[26] The most reasonable inference as to what made real-time tracking possible in this case is the following structure: investigators shared with blockchain analytics firms the complex body of information obtained off-chain — wallet addresses, exchange accounts, money laundering routes, associated individuals — and the analytics firms used that as the basis to reverse-trace all connected fund flows and stitch the dispersed threads into a single coherent picture.

A further question remains, however. How was it possible to seize 127,271 BTC held in a private wallet — that is, a wallet whose private key is held directly by the individual, not by an exchange or third party? Without the private key, access to the wallet is impossible by definition. The U.S. Department of Justice has not disclosed how the private key was obtained. However, according to TRM Labs' analysis of the indictment, the charging documents state that Chen Zhi personally held the seed phrases for multiple wallets and that investigators recovered them in the course of the investigation.[27] The conclusion that can reasonably be drawn from publicly available materials is that years of accumulated off-chain intelligence — informants, victim testimony, and leads obtained through search and seizure — made it possible to secure the private keys.

Whatever the precise method of obtaining the private keys, what is clear is that this seizure would not have been possible without the combination of off-chain intelligence and on-chain tracing. Once that combination had yielded a complete picture of the fund flows, investigators waited for the decisive moment. The United States and the United Kingdom jointly imposed sanctions on 146 targets connected to Prince Group and froze assets belonging to Chen Zhi,

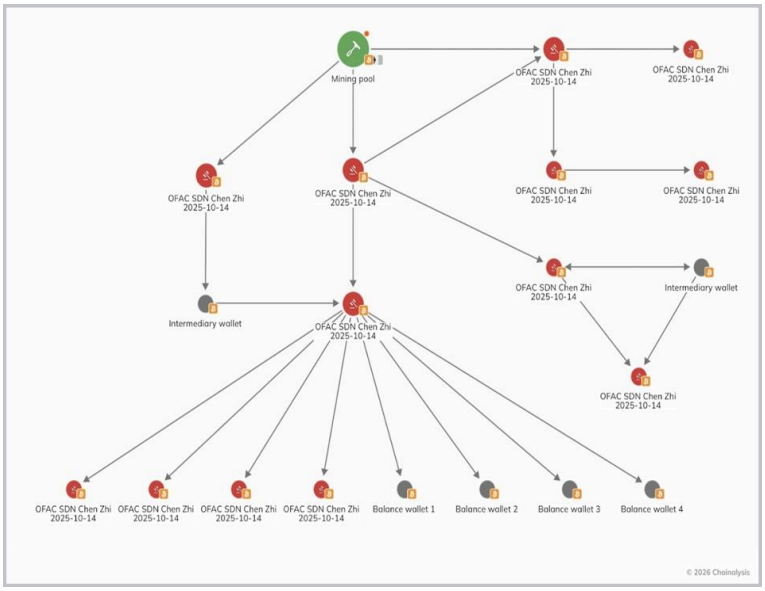
25) U.S. Department of Justice, “Chairman of Prince Group Indicted for Operating Cambodian Forced Labor Scam Compounds Engaged in Cryptocurrency Fraud Schemes,” Office of Public Affairs, October 15, 2025, accessed April 17, 2026, https://www.justice.gov/opa/pr/chairman-prince-group-indicted-operating-cambodian-forced-labor-scam-compounds-engaged.

26) East Asia Forum, “Unravelling Prince Group’s Criminal Networks,” November 29, 2025, accessed April 17, 2026, https://eastasiaforum.org/2025/11/29/unravelling-prince-groups-criminal-networks-2

27) TRM Labs, “Operation Prince: Inside the Global Effort That Led to the Largest Forfeiture in U.S. History,” TRM Labs Blog, October 20, 2025, accessed April 17, 2026, https://www.trmlabs.com/resources/blog/operation-prince-inside-the-global-effort-that-led-to-the-largest-forfeiture-in-us-history.

his associates, and affiliated entities.28) Not only the United States but also the United Kingdom froze real estate owned by Chen Zhi in London, and in November 2025 South Korea joined the international effort by sanctioning 15 individuals and 132 organizations including Prince Group and Chen Zhi. Chen Zhi was arrested in Cambodia on January 6, 2026 and extradited to China.29)

Notably, according to Chainalysis, even after sanctions were imposed on Chen Zhi, the addresses under his control continued laundering remaining assets on-chain until his arrest.30) The fact that on-chain fund movements did not stop even after sanctions were issued demonstrates that while blockchain analytics enables tracing, it still has limits when it comes to real-time interdiction. What this case reveals is both the limitation and the potential of blockchain analytics technology. On-chain data alone cannot identify a criminal from the outset. But the moment it is combined with investigators' off-chain intelligence, blockchain analytics becomes a decisive weapon for tracing and containing criminal funds worth tens of billions of dollars. This case most clearly illustrates that the cooperation between state investigative agencies and private analytics firms is evolving beyond the mere provision of tools into a three-dimensional investigative architecture.



[Figure 9]

On-Chain Fund Movement Routes Following Chen Zhi Sanctions

Source: Chainalysis

From Terrorist Financing to Cross-Chain Crime: The Expanding Scope of Tracing

While Chainalysis has established itself as the de facto standard in the blockchain analytics industry, Elliptic and TRM Labs have also produced meaningful results in their own distinct

28) U.S. Department of the Treasury, "U.S. and U.K. Take Largest Action Ever Targeting Cybercriminal Networks in Southeast Asia," Press Release, October 15, 2025, accessed April 17, 2026, https://home.treasury.gov/news/press-releases/sb0278.

29) Kyunghyang Shinmun, "Prince Group's Chen Zhi, Alleged Mastermind Behind Cambodian Scam Operations, Repatriated to China Following Arrest" (in Korean), January 8, 2026, accessed April 17, 2026, https://www.khan.co.kr/article/202601080645001.

30) Chainalysis, The 2025 Crypto Crime Report (Chainalysis, 2025), accessed April 16, 2026, https://go.chainalysis.com/2025-Crypto-Crime-Report.html.

areas. The cases of these two firms demonstrate that blockchain analytics is not the exclusive capability of any single company, but a structural trend of sophistication advancing across the industry as a whole.

In August 2024, TRM Labs joined forces with the TRON blockchain and Tether to form the T3 Financial Crime Unit, beginning direct intervention in the freezing of illicit funds. Within just four months of its launch, T3 achieved the freezing of over $100 million in illicit USDT, with cumulative freezes subsequently surpassing $300 million.[31] This structure — in which a private blockchain analytics firm, a blockchain network, and a stablecoin issuer formed a tripartite cooperative framework to directly counter illicit funds — is regarded as a case that advances the existing state-private symbiosis model by one further step.

TRM Labs has also produced notable results in terrorist financing investigations. In terrorist financing cases resolved in Indonesia in 2024 and 2025, TRM Labs' on-chain analysis was adopted as key evidence. Indonesia's Financial Intelligence Unit (PPATK) and its counter-terrorism police unit Detachment 88 used TRM Labs' analytical tools to trace and secure a conviction in court against a specific suspect who had transferred a total of $49,000 worth of USDT to an ISIS-affiliated fundraising campaign in Syria across 15 transactions through an exchange.[32] This case — in which an Indonesian court recognized on-chain blockchain data as core evidence in a terrorist financing prosecution — marked an important turning point in the establishment of crypto forensics as legally admissible evidence in Southeast Asia.

Elliptic has distinguished itself in research on cross-chain crime. According to Elliptic's 2025 research, the scale of cross-chain crime reached $21.8 billion — more than triple the figures of $4 billion in 2022 and $7 billion in 2023 within just two to three years, illustrating how rapidly money laundering through cross-chain asset movement is becoming more sophisticated.[33] In response, Elliptic has built an analytical framework covering more than 50 blockchains and more than 250 bridges, and major global exchanges including Coinbase and Revolut have adopted this solution as a core compliance tool.[34]

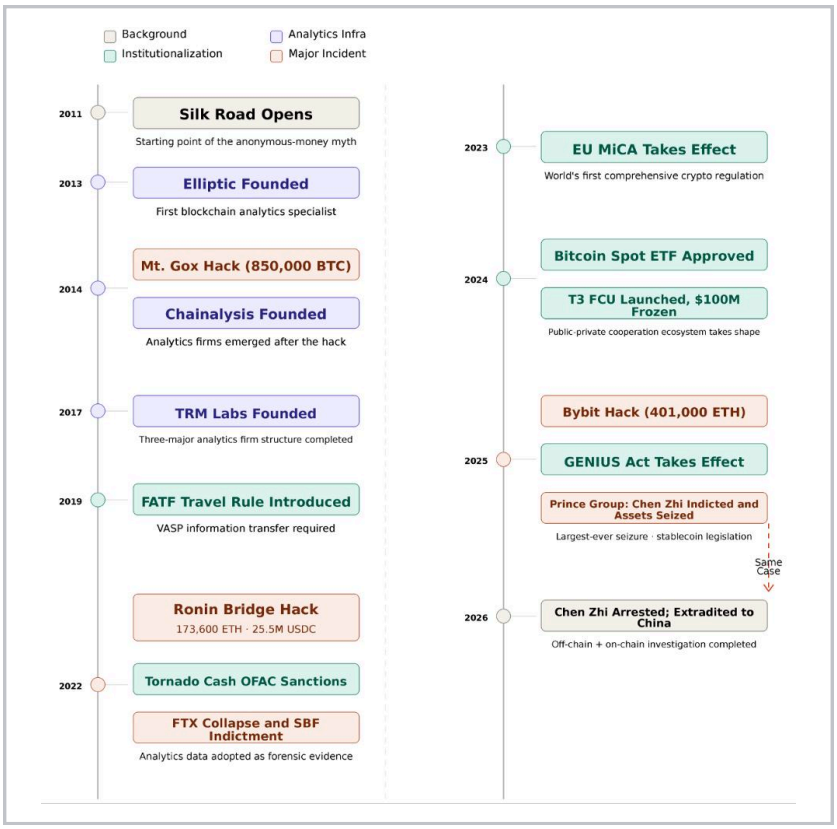
Chainalysis visualizing Lazarus's money laundering routes, TRM Labs providing on-chain analysis for terrorist financing investigations, Elliptic tracing the full picture of cross-chain crime — the cases of these three firms demonstrate that blockchain analytics has matured from the capability of a single company into a structural capability of the industry as a whole. The scope of tracing is widening, the precision of analysis is deepening, and the speed of response is accelerating. And as this capability matures, so too does the confidence of states that crypto can be institutionalized.

31) TRM Labs, “T3 Financial Crime Unit Marks Enforcement Victory: $100 Million in Criminal Assets Frozen Across Five Continents,” TRM Labs Blog, September 10, 2024, accessed April 17, 2026, https://www.trmlabs.com/resources/blog/t3-financial-crime-unit-marks-enforcement-victory-100-million-in-criminal-assets-frozen-across-five-continents.

32) TRM Labs, “How Indonesian Law Enforcement Used On-Chain Intelligence to Secure Convictions for Terrorism Financing,” TRM Labs Blog, February 15, 2024, accessed April 17, 2026, https://www.trmlabs.com/resources/blog/how-indonesian-law-enforcement-used-on-chain-intelligence-to-secure-convictions-for-terrorism-financing.

33) Elliptic, The State of Cross-Chain Crime 2025 (Elliptic Resources, January 2025), accessed April 17, 2026, https://www.elliptic.co/resources/the-state-of-cross-chain-crime-2025.

34) Elliptic, “Crypto Compliance,” Elliptic Solutions, accessed April 17, 2026, https://www.elliptic.co/solutions/crypto-compliance.



[Figure 10]

Blockchain Analytics Technology and Crypto Institutionalization Timeline

03

Institutionalization Made by Analytics Technology

The cases examined above showed how blockchain analytics technology works. The question now shifts. How has that technology contributed to the institutionalization of crypto? Institutionalization begins only when something can be traced, when intervention becomes possible, and when it can be connected to the real legal order.

The Conditions for Institutionalization Proven by the Cases

The cases covered in Chapter 2 differ in character from one another. Nation-state hacking, collapse driven by internal corruption, the largest theft in history, the dismantling of a transnational criminal organization, terrorist financing investigations, cross-chain crime research — the types of crime, their scale, and their backgrounds are all different. Yet running across all of these cases, one thing has been repeatedly confirmed: for blockchain analytics to actually function, and for it to serve as the basis for institutionalization, three conditions must be met.

The first condition is traceability. The anonymity of blockchain is growing thinner in the face of analytics technology. Whether funds dispersed across thousands of wallets, internal embezzlement of billions of dollars, the largest theft in history, criminal proceeds running into the tens of billions of dollars, or terrorist financing crossing borders — as long as it is recorded on-chain, a thread for tracing necessarily exists. Through the process by which clustering groups scattered wallets into a single entity, labeling attaches a name to that entity, and pattern analysis evaluates the risk level of its behavior, anonymous addresses are gradually converted into identifiable actors. There is no such thing as complete anonymity. There is only data that has not yet been read.

The second condition is the capacity for intervention. As tracing became possible, the state gained the ability to intervene. Behind all of these outcomes — the OFAC sanctions on Tornado Cash, the designation of Huione Pay as subject to special measures, the conviction of Sam Bankman-Fried, the indictment of Chen Zhi and the largest crypto seizure in history — lay blockchain analytics data. The subjects of intervention have also expanded. As a public-private cooperative ecosystem has formed that encompasses not only state agencies but also blockchain networks, stablecoin issuers, and exchanges, the response to illicit funds has become faster and more wide-ranging.

The third condition is real-world connectivity. As on-chain data has been admitted as evidence in courts, and as countries with different laws and institutions have come to share the same analytics platforms, the speed and scope of international cooperation have been transformed. The reality that an Indonesian court recognized blockchain data as core evidence in a terrorist

financing prosecution, and that 38 countries jointly investigated a single case, would have been difficult to imagine just a decade ago. Crypto is no longer a domain outside the real legal order. As analytics data has become the starting point of investigations, the basis for sanctions, and evidence in courts, blockchain has entered the real legal order.

Visibility Is Governability: If It Can Be Seen, It Can Be Managed

For the state to institutionalize something, it must first be able to see it. Historically, states have been unable to manage what they cannot see. Underground economies, informal transactions, black markets — the reason these economic activities remain outside the institutional framework is not simply that they are illegal, but that the state has been unable to grasp their flows. Institutionalization begins with visibility. In its early days, crypto was a domain invisible to the state. Transactions were taking place, but it was impossible to know who was sending what to whom. The reason the state was uncomfortable with crypto was not simply because of the ideology of decentralization. It was because crypto could not be seen. What cannot be seen cannot be managed, and what cannot be managed cannot be institutionalized.

The emergence of blockchain analytics technology began to transform crypto into something the state could read. The figure who most symbolically embodies this transformation in the field of investigation is Kathryn Haun.[35] In 2012, Haun — then a federal prosecutor at the U.S. Department of Justice — took on a Bitcoin investigation and made a decisive discovery. The blockchain was a public ledger that permanently recorded every transaction, and these records left traces that were in fact easier to trace than cash or international wire transfers. Haun called this "digital breadcrumbs."[36]

[Figure 11]
Kathryn Haun
Source: Haun Ventures

Haun used this characteristic to successfully prosecute a Drug Enforcement Administration (DEA) agent who had embezzled Bitcoin during the Silk Road investigation, creating one of the

35) Kathryn Haun's formal professional name is Kathryn Haun, although she is frequently referred to in industry and media circles as "Katie Haun." Because this report focuses primarily on her role as a federal prosecutor, it uses "Kathryn Haun" throughout.

36) Quartz, "The Woman Who Led Crypto Policing in the U.S. Guesses What's Next for Regulation," March 24, 2018, accessed April 17, 2026, https://qz.com/1236501/the-woman-who-once-policed-the-crypto-world-for-the-us-government-says-a-crackdown-is-coming.

earliest cases in which blockchain data was used as decisive evidence in court.[37] In the course of the investigation, Haun made another discovery: within the crypto industry — widely regarded as a hotbed of illegality — companies like Coinbase were knocking on regulators' doors of their own accord. An industry that had been outside the institutional framework was trying to come in.[38]

Haun subsequently founded the first crypto investigation task force in U.S. Department of Justice history and led inter-agency cooperation on crypto investigations. After leaving the prosecutor's office, she joined the Coinbase board of directors, became a partner at Andreessen Horowitz running a crypto fund, and later struck out independently to establish Haun Ventures, a $1.5 billion fund.[39] This trajectory represents more than a simple career transition. In the field of investigation, Haun learned firsthand that while Bitcoin as a technology cannot itself be prosecuted, the traces it leaves can be traced — and that within the industry there exist companies willing to embrace regulation. Bitcoin cannot be eliminated, but it can be managed. And if it can be managed, the state will take it in. The person who grasped that logic before anyone else stepped down from the prosecutor's office and walked straight into the heart of that new industry.

Institutionalization Built on Analytics Infrastructure: The Travel Rule, MiCA, the Spot Bitcoin ETF, and the GENIUS Act

The Travel Rule, MiCA, the spot Bitcoin ETF, and the GENIUS Act each have different purposes and backgrounds, but they share a common premise: none of them can function effectively in practice without blockchain analytics infrastructure.

The Travel Rule is a regulation that the Financial Action Task Force (FATF) applied to virtual asset service providers (VASPs) in 2019, requiring that sender and recipient information be transmitted alongside crypto transfers between service providers such as exchanges — a transplantation of principles already applied in the traditional financial system into the crypto domain.[40] For this regulation to be implemented in substance, real-time identification of counterparties and detection of suspicious transactions must be possible. The labeling frameworks and KYT (Know Your Transaction) solutions[41] built by blockchain analytics firms function as the core infrastructure underpinning that implementation.

The European Union's MiCA (Markets in Crypto-Assets) regulation, which entered into force in

37) U.S. Department of Justice, "Former Silk Road Task Force Agent Pleads Guilty to Extortion, Money Laundering and Obstruction," Office of Public Affairs, July 1, 2015, accessed April 17, 2026, https://www.justice.gov/archives/opa/pr/former-silk-road-task-force-agent-pleads-guilty-extortion-money-laundering-and-obstruction.

38) Brian Armstrong, quoted in "Brian Armstrong on the Crypto Economy," Conversations with Tyler, February 10, 2021, accessed May 12, 2026, https://conversationswithtyler.com/episodes/brian-armstrong.

39) Haun Ventures, "Team — Katie Haun," Haun Ventures Official Website, accessed April 17, 2026, https://www.haun.co/team/katie-haun.

40) Financial Action Task Force (FATF), "Virtual Assets," FATF Official Website, accessed April 17, 2026, https://www.fatf-gafi.org/en/topics/virtual-assets.html.

2023, is the world's first comprehensive crypto regulatory framework. MiCA requires all crypto-asset service providers (CASPs) operating in Europe to establish KYC obligations, internal controls, and risk management frameworks. The Transfer of Funds Regulation (TFR) mandates that sender and recipient information be transmitted with every virtual asset transfer.[42] The real-time transaction monitoring, risk assessment, and suspicious transaction reporting that MiCA demands are functions already provided by blockchain analytics solutions such as Chainalysis's KYT and Elliptic's holistic screening. Regulation has legislated into law what analytics technology had already put into practice.

If technology opened the door to regulation, regulation in turn created demand for technology. During the legislative processes for the Travel Rule and MiCA, blockchain analytics firms actively shaped public discourse on the meaning and direction of regulation, exercising considerable influence. Elliptic's Vice President of Policy and Regulatory Affairs David Carlisle analyzed the fact that the EU Travel Rule applies to all crypto transactions beyond FATF standards, presenting a framework for the industry's response; TRM Labs' Head of Legal and Government Affairs Ari Redbord characterized MiCA as "the most comprehensive legal framework for crypto in the world," lending support to the legitimacy of the regulation. Before joining TRM Labs, Redbord had served as Senior Advisor to the U.S. Deputy Secretary of the Treasury and the Under Secretary for Terrorism and Financial Intelligence.[43] This flow of personnel — in which key figures from regulatory authorities move into private blockchain analytics firms — is a telling illustration of a structure of co-evolution in which technology and institutions reinforce each other through policy and discourse as well.

The spot Bitcoin ETF was approved by the U.S. Securities and Exchange Commission (SEC) in January 2024. The core reason the SEC had refused to approve a spot ETF for years was concern over market manipulation. The situation changed when Grayscale filed suit in the U.S. Court of Appeals for the D.C. Circuit. The court ruled that the SEC's logic in permitting Bitcoin futures ETFs while rejecting spot ETFs was inconsistent, and the SEC was effectively compelled to grant approval by the court's decision.[44] Yet underlying that approval was the fact that the surveillability of the crypto market had materially improved. As blockchain analytics solutions from Chainalysis, TRM Labs, and others were adopted across exchanges, the premise that had long underpinned the SEC's objections — that the market was unsurveillable — was being eroded. If the court opened the door, blockchain analytics technology had been creating the conditions under which that door could be opened.

In July 2025, the GENIUS Act — the United States' first federal stablecoin regulatory law —

41) KYT (Know Your Transaction) refers to a transaction-monitoring system that analyzes the flow of funds associated with individual transactions in real time in order to detect suspicious activity, including money laundering, sanctions evasion, and other illicit financial behavior. Unlike KYC (Know Your Customer), which focuses on customer identity, KYT focuses on transaction behavior.

42) Valérie Métais et al., “MiCA & TFR: The Two New Pillars of the EU Crypto-Assets Regulatory Framework,” DLA Piper, June 2023, accessed May 8, 2026, https://www.dlapiper.com/en-us/insights/publications/2023/06/mica-tfr-the-two-new-pillars-of-the-eu-cryptoassets-regulatory-framework.

43) Brian Monroe, “EU Passes Landmark Crypto Regulation, MiCA, in Lock Step after Cementing Decried, Dreaded Virtual Value AML ‘Travel Rule,’” ACFCS, April 20, 2023, accessed May 8, 2026, https://www.acfcs.org/eu-passes-landmark-crypto-regulation.

44) U.S. Securities and Exchange Commission, “Statement on the Approval of Spot Bitcoin Exchange-Traded Products,” SEC Official Website, January 10, 2024, accessed April 17, 2026, https://www.sec.gov/newsroom/speeches-statements/gensler-statement-spot-bitcoin-011023.

was signed into law by President Trump. The GENIUS Act requires stablecoin issuers to maintain one-to-one reserves, comply with monthly disclosure obligations, and build AML and sanctions compliance programs. Notably, all issuers must possess the technical capability to freeze, seize, and burn stablecoins pursuant to legal orders.[45] The real-time monitoring and sanctions compliance infrastructure that blockchain analytics firms have already built underpins the practical enforceability of this law.

The arc from the founding of blockchain analytics firms, through the introduction of the Travel Rule, the implementation of MiCA, the approval of the spot Bitcoin ETF, and the enactment of the GENIUS Act is a process of co-evolution in which technology and institutions have matured together, each reinforcing the other. These frameworks each have different purposes and backgrounds, but share the common premise that none can function effectively without blockchain analytics infrastructure. Within a structure in which technology opens the door to regulatory enforceability and regulation in turn expands demand for technology, analytics infrastructure and institutionalization have made each other increasingly indispensable.

45) The White House, "Fact Sheet: President Donald J. Trump Signs GENIUS Act into Law," July 15, 2025, accessed April 17, 2026, https://www.whitehouse.gov/fact-sheets/2025/07/fact-sheet-president-donald-j-trump-signs-genius-act-into-law.

04

How Institutionalization Has Changed the Meaning of Crypto

The United States embraced crypto because it gained the confidence that crypto could be managed, and because it arrived at the strategic judgment that doing so could reinforce dollar hegemony. The technical foundation of that confidence and that strategic judgment is blockchain analytics infrastructure. Only when the traces left by blockchain can be read does institutionalization become possible. And institutionalization does not end simply with the imposition of a regulatory framework. It changes the vocabulary, the structure, and the meaning. Crypto still exists, but what it means has changed fundamentally.

From the Vocabulary of Resistance to the Vocabulary of Institution

Satoshi Nakamoto's 2008 white paper was written in a particular vocabulary. Terms like decentralization, censorship resistance, trustless transactions, and peer-to-peer payments were not mere technical terminology. They were a political declaration that compressed within itself a distrust of states and financial institutions, a conviction that individuals should have full sovereignty over their own assets, and a resistance to existing power structures. The early crypto community cohered around this shared vocabulary. To buy Bitcoin was not simply an investment — it was an ideological choice.

That vocabulary has not entirely disappeared. But the vocabulary of mainstream discourse around crypto has changed completely. KYC, AML, the Travel Rule, sanctions compliance — these are the terms the crypto industry now uses constantly. To operate an institutional exchange, KYC must be in place; for institutions to handle crypto, AML frameworks must be built; cross-border transfers are subject to the Travel Rule. The vocabulary of crypto has shifted from the vocabulary of resistance to the vocabulary of regulatory compliance.

This shift is not coincidental. As blockchain analytics technology made crypto visible, the state was able to impose the framework of institutionalization — and as that framework was imposed, the industry, seeking to survive within it, adopted a new vocabulary. Vocabulary follows power. The fact that the vocabulary of crypto has changed means that the power structure surrounding crypto has changed.

The Rhetoric of Decentralization Remains; the Structure Has Changed

Decentralization remains one of the most frequently invoked terms in the crypto community. Decentralized Finance (DeFi), Decentralized Autonomous Organizations (DAOs), Decentralized Exchanges (DEXs) — the rhetoric of decentralization has in fact proliferated into an ever wider range of forms. Yet when one looks at the actual structure, a different picture emerges.

The overwhelming majority of crypto transactions still take place through centralized exchanges (CEXs). Binance, Coinbase, Upbit and their peers require KYC, operate under government regulation, and have adopted blockchain analytics solutions to monitor transactions. The Bitcoin network itself is decentralized, but the gateway through which most people access Bitcoin is thoroughly centralized. It is a structure in which centralized infrastructure has been layered on top of decentralized technology.

The stablecoin ecosystem tells the same story. USDT and USDC — which underpin the liquidity of DeFi — are issued by Tether and Circle respectively, both centralized private companies. These companies hold the authority to freeze assets at specific addresses in accordance with U.S. financial regulations including OFAC sanctions. The core liquidity of what is called decentralized finance sits under the control of centralized issuers.

The data concentration of blockchain analytics firms is another form of structural centralization. The labeling data built by a small number of private firms — Chainalysis, Elliptic, TRM Labs — has become the de facto standard shared by investigative agencies, financial institutions, and exchanges worldwide. The authority to determine which addresses are dangerous and which transactions are suspicious on-chain has become concentrated in the hands of these few companies. Blockchain is distributed, but the power to interpret blockchain is concentrated. The rhetoric of decentralization remains, but the structure has already been moving in a different direction.

The Geopolitics of Analytical Power: Who Controls the On-Chain Narrative Controls the Story

That blockchain analytics firms are more than mere technology service providers was already established in Chapter 2. But the nature of the power these firms hold goes beyond simple market dominance. They effectively exercise the authority to define what is good and what is evil in the crypto ecosystem.

Consider Chainalysis's labeling framework. When a particular wallet address is labeled as ransomware-linked, darknet market-associated, or sanctions-designated, every transaction connected to that address is classified as high-risk. Exchanges refuse deposits of the relevant funds, investigators begin tracing, and through integration with OFAC sanctions the address is blocked from the global financial network. Conversely, addresses labeled as exchange hot wallets or legitimate services are incorporated as part of the normal financial system. A single label determines the fate of funds.

Yet the criteria and algorithms behind this labeling are protected as trade secrets and are not disclosed to the outside world. There is no way for anyone outside to verify who classified a particular address as dangerous, on what basis, or whether that judgment was right or wrong. When false positives occur, the assets of innocent individuals can be frozen — but accountability is unclear. It is a paradox in which a technology designed for transparency produces an opaque structure of judgment.

This structure also carries geopolitical implications. Chainalysis is an American company, and its data and labeling framework sit within U.S. legal jurisdiction. OFAC's sanctions list is

reflected in Chainalysis's labeling, and that labeling becomes the standard shared by more than 1,500 investigative agencies, financial institutions, and exchanges worldwide. When the United States decides on a sanction, that sanction is immediately propagated throughout the global crypto ecosystem through Chainalysis. This structure is extending into the Bitcoin network itself. Following the approval of the spot Bitcoin ETF, more than one million Bitcoin have become concentrated in U.S. financial institutions such as BlackRock and Fidelity.[46] Bitcoin moves from address to address, leaving traces. The more major addresses are held by U.S. financial institutions, the more of Bitcoin's fund flows come within range of American surveillance. The technical possibility of applying to the Bitcoin network the same method used to weaponize the dollar — freezing sanctioned addresses — is becoming structurally achievable. The fact that the authority to interpret on-chain data is concentrated in U.S.-centered analytics infrastructure means that the geopolitics of crypto continues to run along the same lines as the geopolitics of dollar hegemony. Who controls the on-chain narrative controls the story.

What Does Tamed Crypto Mean Now?

What, then, is institutionalized crypto? It is not the stateless money Satoshi dreamed of. Nor is it identical to the existing financial system. Institutionalized crypto sits somewhere in between.

Crypto now serves two functions simultaneously. The first is as infrastructure that extends dollar hegemony into the digital realm. As dollar stablecoins become the medium of global crypto transactions, and as the GENIUS Act obliges stablecoin issuers to hold U.S. Treasuries, the crypto ecosystem has become a structural instrument for extending the dollar's digital domain. From the American perspective, crypto is not a threat to dollar hegemony but a new layer that reinforces it.

The second is as infrastructure for financial innovation. Blockchain technology continues to work through problems that traditional finance has failed to solve — payments, clearing, asset tokenization, decentralized finance. Institutionalization has not entirely extinguished crypto's potential for innovation. In some respects, institutionalization has actually accelerated the pace of innovation by bringing in institutional capital and regulatory clarity.

What matters, however, is that neither of these two registers places at its core what Satoshi originally intended: the economic autonomy of individuals, free from states and financial institutions. That vision remains as the founding narrative of crypto's origin story, but it is no longer the animating principle that governs how crypto actually operates. Crypto was born as an instrument of freedom, but has grown into institutionalized financial infrastructure. And it was blockchain analytics technology that created the conditions for that growth. The question now is who, within the institutionalized crypto order, will analyze, interpret, and design the rules. It is precisely at this point that South Korea's position and challenges come into view.

46) The Armchair Trader, "BlackRock Dominates Bitcoin ETFs as Total Holdings Surge," 2024, accessed April 17, 2026, https://www.thearmchairtrader.com/exchange-traded-funds/blackrock-dominates-bitcoin-etfs.

05

South Korea's Position and Challenges

The Reality of Dependence on Analytics Infrastructure

South Korea is a powerhouse in virtual assets. In 2025, the daily average trading volume of domestic virtual assets exceeded five trillion won (approximately $3.6 billion).[47] Yet the infrastructure for monitoring and tracing that enormous volume of transactions comes not from South Korea but from the United States.

Domestic exchanges have also attempted to build independent infrastructure for Travel Rule compliance. CODE — established jointly by Bithumb, Coinone, and Korbit — is a representative example, but CODE operates by outsourcing its core AML analysis to TRM Labs through a strategic partnership.[48] The outward form of independent infrastructure has been achieved, but the core capability of actually analyzing fund flows and assessing risk remains delegated to an American firm. This structure reveals that South Korean exchanges have adopted the form of compliance, but the substantive judgment that fills that form depends on external parties.

The Financial Intelligence Unit (FIU) also announced in its 2026 work plan that it would introduce an AI-based analytics system and utilize Chainalysis as a virtual asset analytics tool.[49] The effort to strengthen analytical capability is positive in itself, but the structure of dependence on a U.S. private firm for the core analytics tool is no different from the situation of the exchanges.

The situation of investigative agencies is more serious. Over the five years from 2021 to 2025, losses from domestic virtual asset crime reached approximately seven trillion won, yet the assets actually seized by investigative agencies amounted to just 0.7 percent of that figure.[50] This number plainly reflects the structural limitation that without independent on-chain

47) Financial Services Commission (FSC) and Financial Intelligence Unit (FIU), "Results of the Second Half 2025 Survey of Virtual Asset Service Providers" (in Korean), March 25, 2026, accessed May 8, 2026, https://www.korea.kr/briefing/pressReleaseView.do?newsId=156750839.

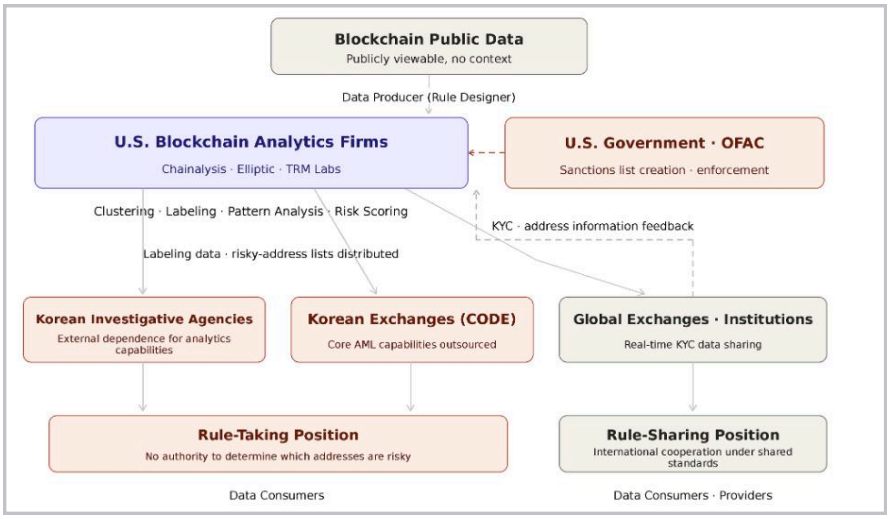
48) TRM Labs, "TRM Labs and CODE Enter Strategic Partnership to Enable AML and Travel Rule Compliance in Korea," TRM Labs Blog, accessed May 8, 2026, https://www.trmlabs.com/ko/resources/blog/trm-labs-and-code-enter-strategic-partnership-to-enable-aml-and-travel-rule-compliance-in-korea.

49) Financial Intelligence Unit (FIU), "2026 Anti-Money Laundering Work Plan," Financial Services Commission Press Release, February 5, 2026, accessed May 15, 2026, https://www.fsc.go.kr/no010101/86209.

50) Seoul Shinmun, "Crypto Crime Losses Reach ₩7 Trillion; Seizure and Recovery Rate Only 0.7%" (in Korean), February 27, 2026, accessed May 8, 2026, https://www.seoul.co.kr/news/society/accident/2026/02/27/20260227010007.

analytical capability, the initial freezing of criminal funds before they are transferred overseas is simply not possible.

In this structure, South Korea is a consumer of on-chain data, not a producer. When the United States designates a particular address as a sanctions target, that information is immediately reflected in South Korean exchanges through the analytics infrastructure of American firms. The fact that the authority to determine which addresses are dangerous and which transactions are suspicious does not rest with South Korea means that in the on-chain world, South Korea occupies the position of a rule-taker, not a rule-maker.



[Figure 12]
South Korea's Dependence on On-Chain Analytics Infrastructure

The Limits of Defensive Regulation

South Korea's crypto regulatory framework is built around two pieces of legislation. The amendment to the Special Financial Information Act in March 2021 introduced a registration system for virtual asset service providers and anti-money laundering obligations. The Virtual Asset User Protection Act, which came into force in July 2024, added user asset protection and regulations against market manipulation.[51] The direction this regulatory framework points in is singular: protecting investors and blocking illegal transactions — in other words, defense.

The limits of defensive regulation become sharper when viewed against the backdrop of the global crypto order. As examined above, the United States is accumulating Bitcoin as a national strategic asset and has legislated the dollar stablecoin ecosystem through the GENIUS Act. Movement in Asia is equally clear. In April 2026, the Japanese government passed an amendment to the Financial Instruments and Exchange Act, formally designating virtual assets as financial instruments and committing to the introduction of spot virtual asset ETFs by 2028. It also plans to lower the tax rate on virtual asset investment income from the current maximum of 55 percent to a flat rate of 20 percent, expanding individual investor participation in the market.[52]

Hong Kong approved spot Bitcoin and Ethereum ETFs in April 2024 — the first in Asia. The

51) Financial Intelligence Unit (FIU), "2026 Anti-Money Laundering Work Plan," Financial Services Commission Press Release, February 5, 2026, accessed May 15, 2026, https://www.fsc.go.kr/no010101/86209.

52) Edaily. "Japan Formally Defines Virtual Assets as Financial Instruments, Introducing Securities-Level Regulation." (in Korean), April 10, 2026. Accessed May 8, 2026. https://www.edaily.co.kr/News/Read?newsId=05080726645414808&mediaCodeNo=257

Ethereum spot ETF approval was also a world first, placing Hong Kong ahead of the United States. With China maintaining its ban on virtual asset trading, Hong Kong announced in 2022 its ambition to become the center of the virtual asset market, and has been refining its regulatory framework since June 2023 — when it launched a licensing regime for virtual asset trading operators and permitted individual investor participation.[53]

Dubai established the Virtual Assets Regulatory Authority (VARA) in 2022 — the world's first dedicated virtual asset regulator — and has been actively attracting global virtual asset firms using regulatory clarity and tax incentives as its competitive weapons. From 2022 to 2025, the number of registered virtual asset businesses in Dubai quadrupled from 10 to 39. Their approach to regulation is not mere defense but a strategic act of designing order. South Korea, by contrast, has remained in a defensive posture that keeps virtual assets and finance separate. As the migration of global blockchain firms to the Middle East has become a clear trend, South Korea's institutional environment has been unable to stem the outflow of domestic operators.[54] Indeed, while the number of registered crypto businesses in Dubai grew from 10 to 39, the number in South Korea fell from 42 to 27 — a decline of roughly 36 percent.

Discussion of introducing spot virtual asset ETFs in South Korea has yet to gain any serious momentum, and derivatives trading remains restricted. As a result, the flow of domestic investment capital to overseas exchanges with more flexible regulatory environments is accelerating. In 2025, funds transferred by domestic investors to overseas exchanges were estimated at approximately 160 trillion won (approximately $115 billion) annually.[55] Transactions are happening in South Korea, but the money is flowing out.

While South Korea's regulation has been focused on investor protection, the standards of the global crypto order are hardening — led by the United States, with Dubai emerging as a new hub. Despite its enormous trading volume, South Korea is structurally excluded from participating in the design of that order. There is regulation, but no strategy. This is the core limitation of South Korea's crypto regulatory framework.

Directions for Building South Korea's Own On-Chain Analytical Capability

To overcome the twin challenges of dependence on analytics infrastructure and the limits of defensive regulation, the direction South Korea must take is the development of independent on-chain analytical capability. Three directions are proposed toward this end.

The first is the construction of a Korean on-chain database and labeling framework that

53) Korea Capital Market Institute, "Current State of the Virtual Asset Market and Recent Approval of Spot Virtual Asset ETFs in the United States and Hong Kong," Capital Market Focus (in Korean), May 2024, accessed May 8, 2026, https://www.kcmi.re.kr/publications/pub_detail_view?syear=2024&zcd=002001016&zno=1785&cno=6337.

54) Maeil Business Newspaper, "'Move Aside, Singapore': Dubai Emerges as the New Blockchain Hub as the Number of Operators Quadruples" (in Korean), December 8, 2025, accessed May 8, 2026, https://v.daum.net/v/20251208002400226.

55) Newsis, "₩160 Trillion in Domestic Virtual Asset Funds Flow Overseas; Exchange Rankings Reveal the Trend" (in Korean), March 12, 2026, accessed May 8, 2026, https://www.newsis.com/view/NISX20260312_0003545463.

domestic exchanges and investigative agencies can jointly utilize. As examined above, domestic exchanges are outsourcing the core capabilities of blockchain analytics to American firms. In this structure, the more data accumulates, the more it is the analytical capability of American firms that is strengthened. If domestic exchanges were to jointly accumulate on-chain transaction data and cooperate with investigative agencies to build a labeling framework suited to the domestic context, the foundation for reducing long-term dependence on American firms would be laid. The fact that cooperative structures such as CODE already exist can serve as a starting point. In this process, the Financial Intelligence Unit (FIU) needs to make a role transition — moving beyond simple regulatory oversight to function as a domestic on-chain data hub.

The U.S. FinCEN functions as a central data hub that integrates and analyzes data collected from investigative agencies, financial institutions, and overseas FIUs, providing actionable intelligence to law enforcement.[56] Australia's financial intelligence agency AUSTRAC, through its public-private partnership program Fintel Alliance, operates a system in which major banks, remittance providers, and investigative agencies share and analyze financial intelligence on an integrated platform, jointly producing financial crime intelligence including on virtual assets.[57] If South Korea's FIU were equipped with a similarly integrated on-chain data analysis function, the core judgment authority currently delegated to American firms could be progressively internalized.

The second direction is to build a regulatory framework that meets global standards, but designed in the vocabulary of strategy rather than defense. Travel Rule compliance and the construction of an anti-money laundering framework are necessary conditions — but they are not sufficient. Just as the United States has designed the dollar stablecoin ecosystem through the GENIUS Act, and Dubai has attracted global firms using regulatory clarity and tax incentives as competitive weapons, South Korea also needs strategic regulatory design oriented toward fostering the crypto industry. It is worth beginning with a review of spot virtual asset ETF introduction, derivatives regulation reform, and tax clarification. On spot ETFs alone: following the U.S. approval in January 2024, more than one million BTC in institutional capital including BlackRock has flowed into domestically regulated financial infrastructure.[58] This created the structural conditions for expanding asset management revenues and the tax base. Singapore established a comprehensive licensing framework for stablecoin issuers in 2023 and moved to full implementation in 2025 — an approach assessed as strategic regulatory design aimed at attracting global crypto firms and capital, going beyond the defensive objective of investor protection.[59] The phenomenon of Korean investors moving funds to overseas exchanges can be seen as the accumulated result of this institutional gap.

The third direction is the cultivation of specialist talent in blockchain analytics technology and the fostering of a related corporate ecosystem domestically. Chainalysis, in its early days

56) Financial Crimes Enforcement Network (FinCEN), “What We Do,” FinCEN Official Website, accessed May 12, 2026, https://www.fincen.gov/about-fincen/what-we-do.

57) Australian Transaction Reports and Analysis Centre (AUSTRAC), “Fintel Alliance,” AUSTRAC Official Website, accessed May 12, 2026, https://www.austrac.gov.au/partners/fintel-alliance.

58) The Armchair Trader, “BlackRock Dominates Bitcoin ETFs as Total Holdings Surge,” 2024, accessed April 17, 2026, https://www.thearmchairtrader.com/exchange-traded-funds/blackrock-dominates-bitcoin-etfs.

59) Monetary Authority of Singapore, “MAS Finalises Stablecoin Regulatory Framework,” August 15, 2023, accessed May 12, 2026, https://www.mas.gov.sg/news/media-releases/2023/mas-finalises-stablecoin-regulatory-framework.

following its founding in 2014, secured its first customers by supporting dark web investigations, and grew in earnest by directly demonstrating to U.S. law enforcement agencies that its tracing tools could identify the perpetrators of the Mt. Gox hack.[60] TRM Labs, from its earliest days, recruited former government investigators as core personnel and — despite being a latecomer — rapidly built credibility in the law enforcement market.[61] Given that cooperation with investigative agencies was the core growth driver for both firms, this structure is a replicable model for South Korea. South Korea's National Police Agency, prosecution services, and financial authorities need to institutionally design a virtuous cycle in which they actively support startups in the blockchain analytics space, bring early-stage startups in as partners on joint investigation projects, and ensure that the outputs of those projects accumulate as a labeling database. When investigative agencies function as both early customers and collaborators, private analytical capability can grow on the foundation of public trust and data.

A phased approach is needed to implement these three directions. In the short term, a joint on-chain analytics task force involving the FIU, the Prosecution Service, the National Police Agency, and major exchanges should be established to integrate on-chain data currently fragmented across institutions, and substantive legislative discussion should begin on strategic regulatory measures including spot virtual asset ETF introduction, derivatives regulation reform, and tax clarification. In the medium term, a Korean on-chain analytics database equipped with clustering and labeling frameworks should be built as formal infrastructure, on the basis of data accumulated through pilot projects. In the long term, investigative agencies and financial authorities should conclude government contracts with domestic blockchain analytics startups on a project-by-project basis and prioritize their use in the compliance market, institutionally underpinning the growth of a private analytics ecosystem.

There is a reason the development of independent analytical capability is especially urgent for South Korea. The Lazarus Group has repeatedly targeted South Korean virtual asset infrastructure, including Upbit, the country's largest exchange.[62] Building South Korea's own on-chain analytical capability is not simply a matter of competition in financial infrastructure — it is a task directly linked to national security. Internalizing Korean on-chain analytical capability, designing the regulatory framework in the vocabulary of strategy rather than defense, and cultivating specialist talent and a corporate ecosystem in the analytics technology space — this is how South Korea can survive in an era of crypto institutionalization governed by traceable money.

60) Jonathan Levin, quoted in “How Chainalysis Turned Tracking Crypto Criminals into Big Business,” Fortune, July 31, 2025, accessed May 12, 2026, https://fortune.com/crypto/2025/07/31/chainalysis-cryptocurrency-crime-government.

61) “Crypto Crime-Fighting Startup TRM Labs Notches $1 Billion Valuation with New $70 Million Funding Round,” Yahoo Finance, February 4, 2026, accessed May 12, 2026, https://finance.yahoo.com/news/crypto-crime-fighting-startup-trm-100000946.html.

62) Seoul Economic Daily, “Lazarus Group Suspected as the Culprit Behind Upbit’s ₩44.5 Billion Hack” (in Korean), November 28, 2025, accessed May 12, 2026, https://www.sedaily.co.kr/NewsView/2H0MO4NIEW.

Conclusion

How to Read the Age of Traceable Money

The kidnapper on screen may still demand Bitcoin. But the premise that crypto is untraceable has already collapsed. This report has traced how that premise collapsed, and how its collapse led to a structural transformation. As blockchain analytics technology matured, the state gained the ability to see crypto. And institutionalization proceeded in tandem with that process of making crypto visible. The maturing of analytics technology and institutionalization cannot be said to be linked by a simple linear causality, but they have advanced together, each presupposing and reinforcing the other. A structure has formed in which manageability enables institutionalization, and institutionalization in turn enables more sophisticated management.

In the course of this process, the discourse of crypto changed as well. Instead of the defiant idiom of decentralization, censorship resistance, and stateless payments, the regulatory idiom of KYC, AML, the Travel Rule, and sanctions compliance has become the daily currency of the crypto industry. The rhetoric of decentralization remains, but the structure has changed. The Bitcoin network itself is decentralized, but the gateway through which most people access Bitcoin is the centralized exchange that requires KYC. The stablecoins that underpin DeFi's liquidity are issued by centralized companies — Tether and Circle — which can freeze specific addresses at the request of the U.S. government. And the authority to determine which addresses are dangerous and which transactions are suspicious is concentrated in the hands of a small number of private firms: Chainalysis, Elliptic, and TRM Labs. Blockchain technology is decentralized, but the power to interpret and define that technology is concentrated. This is an age in which those who analyze the on-chain world control the narrative.

To read crypto clearly, one must confront this paradox head-on. Blockchain technology continues to work through problems that traditional finance has failed to solve — payments, clearing, asset tokenization, decentralized finance. Yet the environment in which that technology operates has changed fundamentally. The technology still points toward decentralization, but the institutional environment that contains it is converging thoroughly in the direction of centralization. To hold onto the ideal of decentralization alone is to see only half of what crypto is in this age. Understanding and engaging with crypto while acknowledging the institutionalized reality it inhabits — that is the minimum perspective required of anyone participating in the crypto world today.

In the new order, the greatest risk factor is not the adversary. It is oneself — sitting at the table without knowing the rules.

Reference

Armstrong, Brian. "Brian Armstrong on the Crypto Economy." Conversations with Tyler, February 10, 2021. Access: 2026년 5월 12일. https://conversationswithtyler.com/episodes/brian-armstrong

Australian Transaction Reports and Analysis Centre. "Fintel Alliance." AUSTRAC Official Website. Access: 2026년 5월 12일. https://www.austrac.gov.au/partners/fintel-alliance

Chainalysis. "Bybit Hack: Leveraging Transparency for Collaboration in the Wake of Record-Breaking Theft." Chainalysis Blog, February 26, 2025. Access: 2026년 4월 16일. https://www.chainalysis.com/blog/bybit-exchange-hack-february-2025-crypto-security-dprk

Chainalysis. "Crypto Community Makes Profiting Hard for North Korean Hackers." Chainalysis Blog. Access: 2026년 4월 16일. https://www.chainalysis.com/blog/axie-infinity-ronin-bridge-dprk-hack-seizure

Chainalysis. "Five Key Takeaways from MSMT's Report on North Korean Cyber Operations." Chainalysis Blog, October 27, 2025. Access: 2026년 5월 17일. https://www.chainalysis.com/blog/msmt-report-north-korea-dprk-cyber-threats

Chainalysis. The 2025 Crypto Crime Report. Chainalysis, 2025. Access: 2026년 4월 16일. https://go.chainalysis.com/2025-Crypto-Crime-Report.html

Chainalysis. "Why Chainalysis." Chainalysis Official Website. Access: 2026년 4월 16일. https://www.chainalysis.com/why-chainalysis

Decrypt. "How Chainalysis Helps Catch Cryptocurrency Criminals." September 7, 2020. Access: 2026년 5월 12일. https://decrypt.co/41127/how-chainalysis-helps-catch-cryptocurrency-criminals

East Asia Forum. "Unravelling Prince Group's Criminal Networks." November 29, 2025. Access: 2026년 4월 17일. https://eastasiaforum.org/2025/11/29/unravelling-prince-groups-criminal-networks-2

Elliptic. "Crypto Compliance." Elliptic Solutions. Access: 2026년 4월 17일. https://www.elliptic.co/solutions/crypto-compliance

Elliptic. "North Korea's Lazarus Group Identified as Exploiters Behind $540 Million Ronin Bridge Heist." Elliptic Blog, April 14, 2022. Access: 2026년 4월 16일. https://www.elliptic.co/blog/540-million-stolen-from-the-ronin-defi-bridge

Elliptic. "The $477 Million FTX Hack: A New Blockchain Trail." Elliptic Blog, November 20, 2022. Access: 2026년 4월 17일. https://www.elliptic.co/blog/the-477-million-ftx-hack-following-the-blockchain-trail

Elliptic. The State of Cross-Chain Crime 2025. Elliptic Resources, January 2025. Access: 2026년 4월 17일. https://www.elliptic.co/resources/the-state-of-cross-chain-crime-2025

Europol Financial Intelligence Public Private Partnership. EFIPPP Homepage. Access: 2026년 5월 12일. https://efippp.eu

Federal Bureau of Investigation. "North Korea Responsible for $1.5 Billion Bybit Hack." Internet Crime Complaint Center, February 26, 2025. Access: 2026년 4월 16일. https://www.ic3.gov/psa/2025/psa250226

Financial Action Task Force. "Virtual Assets." FATF Official Website. Access: 2026년 4월 17일. https://www.fatf-gafi.org/en/topics/virtual-assets.html

Financial Crimes Enforcement Network. "FinCEN Issues Final Rule Severing Huione Group from the U.S. Financial System." News Releases, October 15, 2025. Access: 2026년 4월 16일. https://www.fincen.gov/news/news-releases/fincen-issues-final-rule-severing-huione-group-us-financial-system

Financial Crimes Enforcement Network. "What We Do." FinCEN Official Website. Access: 2026년 5월 12일. https://www.fincen.gov/about-fincen/what-we-do

Haun Ventures. "Team — Katie Haun." Haun Ventures Official Website. Access: 2026년 4월 17일. https://www.haun.co/team/katie-haun

Knowles, Tom. "'Our Product Is Used, on Occasion, to Kill People': Inside Palantir, the World's Scariest AI Company." BBC Science Focus, March 23, 2026. Access: 2026년 5월 12일. https://www.sciencefocus.com/future-technology/inside-palantir-the-worlds-scariest-ai-company

Levin, Jonathan. "How Chainalysis Turned Tracking Crypto Criminals into Big Business." Fortune, July 31, 2025. Access: 2026년 5월 12일. https://fortune.com/crypto/2025/07/31/chainalysis-cryptocurrency-crime-government

Lubbertsen, Kelvin, Michel van Eeten, and Rolf van Wegberg. "Ghost Clusters: Evaluating Attribution of Illicit Services through Cryptocurrency Tracing." In Proceedings of the 34th USENIX Security Symposium, August 13–15, 2025, 1363. https://www.usenix.org/system/files/usenixsecurity25-lubbertsen.pdf

Military.com. "Army Lets 3rd ID Use IED Intel System." September 21, 2012. Access: 2026년 5월 12일. https://www.military.com/daily-news/2012/09/21/army-lets-3rd-id-use-ied-intel-system.html

Military.com. "Special Forces, Marines Embrace Palantir Software." July 1, 2013. Access: 2026년 4월 16일. https://www.military.com/defensetech/2013/07/01/special-forces-marines-embrace-palantir-software

Monetary Authority of Singapore. "MAS Finalises Stablecoin Regulatory Framework." August 15, 2023. Access: 2026년 5월 12일. https://www.mas.gov.sg/news/media-releases/2023/mas-finalises-stablecoin-regulatory-framework

Monroe, Brian. "EU Passes Landmark Crypto Regulation, MiCA, in Lock Step after Cementing Decried, Dreaded Virtual Value AML 'Travel Rule'." ACFCS, April 20, 2023. Access: 2026년 5월 8일. https://www.acfcs.org/eu-passes-landmark-crypto-regulation

Nakamoto, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Access: 2026년 4월 16일. https://bitcoin.org/bitcoin.pdf

Nelson, Danny. "Inside Chainalysis' Multimillion-Dollar Relationship With the US Government." CoinDesk, February 10, 2020. Access: 2026년 5월 8일. https://www.coindesk.com/business/2020/02/10/inside-chainalysis-multimillion-dollar-relationship-with-the-us-government

Palantir Technologies. FY 2025 Earnings Release. SEC Form 8-K, February 2026. Access: 2026년 5월 12일. https://www.sec.gov/Archives/edgar/data/0001321655/000132165526000004/a2025q4ex991earningsrelease.htm

Quartz. "The Woman Who Led Crypto Policing in the US Guesses What's Next for Regulation." March 24, 2018. Access: 2026년 4월 17일. https://qz.com/1236501/the-woman-who-once-policed-the-crypto-world-for-the-us-government-says-a-crackdown-is-coming

Ronin Network. "Back to Building: Ronin Security Breach Postmortem." Ronin Network Blog, April 27, 2022. Archived. Access: 2026년 5월 16일. https://web.archive.org/web/2022/https://roninchain.com/blog/posts/back-to-building-ronin-security-breach-6513cc78a5edc1001b03c364

Scott, James C. Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed. New Haven: Yale University Press, 1998.

Statista. "Who Does Palantir Work For?" Access: 2026년 4월 16일. https://www.statista.com/chart/34846

TechCrunch. "Leaked Palantir Doc Reveals Uses, Specific Functions and Key Clients." January 11, 2015. Access: 2026년 4월 16일. https://techcrunch.com/2015/01/11/leaked-palantir-doc-reveals-uses-specific-functions-and-key-clients

The Armchair Trader. "BlackRock Dominates Bitcoin ETFs as Total Holdings Surge." 2024. Access: 2026년 4월 17일. https://www.thearmchairtrader.com/exchange-traded-funds/blackrock-dominates-bitcoin-etfs

The Block. "FTX's Latest Bankruptcy Report Outlines Dysfunction of SBF's Empire." Access: 2026년 4월 16일. https://www.theblock.co/post/225601/ftx-bankruptcy-report-latest

The Conversation. "When the Government Can See Everything: How One Company – Palantir – Is Mapping the Nation's Data." January 20, 2026. Access: 2026년 5월 12일. https://theconversation.com/when-the-government-can-see-everything-how-one-company-palantir-is-mapping-the-nations-data-263178

The White House. "Establishment of the Strategic Bitcoin Reserve and United States Digital Asset Stockpile." Presidential Actions, March 6, 2025. Access: 2026년 4월 17일. https://www.whitehouse.gov/presidential-actions/2025/03/establishment-of-the-strategic-bitcoin-reserve-and-united-states-digital-asset-stockpile

The White House. "Fact Sheet: President Donald J. Trump Signs GENIUS Act into Law." July 15, 2025. Access: 2026년 4월 17일. https://www.whitehouse.gov/fact-sheets/2025/07/fact-sheet-president-donald-j-trump-signs-genius-act-into-law

TRM Labs. 2025 Crypto Adoption and Stablecoin Usage Report. TRM Labs, 2025. Access: 2026년 4월 17일. https://www.trmlabs.com/reports-and-whitepapers/2025-crypto-adoption-and-stablecoin-usage-report

TRM Labs. Compliance in the Second Age of Digital Assets: How Crypto Compliance Programs Are Evolving in 2023. TRM Labs, 2023. Access: 2026년 4월 17일. https://www.trmlabs.com/ko/reports-and-whitepapers/crypto-compliance-in-the-second-age-of-digital-assets

TRM Labs. "How Indonesian Law Enforcement Used On-Chain Intelligence to Secure Convictions for Terrorism Financing." TRM Labs Blog, February 15, 2024. Access: 2026년 4월 17일. https://www.trmlabs.com/resources/blog/how-indonesian-law-enforcement-used-on-chain-intelligence-to-secure-convictions-for-terrorism-financing

TRM Labs. "Operation Prince: Inside the Global Effort That Led to the Largest Forfeiture in US History." TRM Labs Blog, October 20, 2025. Access: 2026년 4월 17일. https://www.trmlabs.com/resources/blog/operation-prince-inside-the-global-effort-that-led-to-the-largest-forfeiture-in-us-history

TRM Labs. "T3 Financial Crime Unit Marks Enforcement Victory: $100 Million in Criminal Assets Frozen Across Five Continents." TRM Labs Blog, September 10, 2024. Access: 2026년 4월 17일. https://www.trmlabs.com/resources/blog/t3-financial-crime-unit-marks-enforcement-victory-100-million-in-criminal-assets-frozen-across-five-continents

TRM Labs. "TRM Labs와 CODE, 한국에서 AML 및 트래블룰 컴플라이언스 활성화를 위한 전략적 파트너십 체결." TRM Labs Blog. Access: 2026년 5월 8일. https://www.trmlabs.com/ko/resources/blog/trm-labs-and-code-enter-strategic-partnership-to-enable-aml-and-travel-rule-compliance-in-korea

U.S. Department of Justice. "Chairman of Prince Group Indicted for Operating Cambodian Forced Labor Scam Compounds Engaged in Cryptocurrency Fraud Schemes." Office of Public Affairs, October 15, 2025. Access: 2026년 4월 17일. https://www.justice.gov/opa/pr/chairman-prince-group-indicted-operating-cambodian-forced-labor-scam-compounds-engaged

U.S. Department of Justice. "Former Silk Road Task Force Agent Pleads Guilty to Extortion, Money Laundering and Obstruction." Office of Public Affairs, July 1, 2015. Access: 2026년 4월 17일. https://www.justice.gov/archives/opa/pr/former-silk-road-task-force-agent-pleads-guilty-extortion-money-laundering-and-obstruction

U.S. Department of Justice. "South Korean National and Hundreds of Others Charged Worldwide in the Takedown of the Largest Darknet Child Pornography Website, Which Was Funded by Bitcoin." Office of Public Affairs, October 16, 2019. Access: 2026년 4월 16일. https://www.justice.gov/archives/opa/pr/south-korean-national-and-hundreds-others-charged-worldwide-takedown-largest-darknet-child

U.S. Department of Justice. "United States Attorney Announces Charges Against FTX Founder Samuel Bankman-Fried." Southern District of New York, December 13, 2022. Access: 2026년 4월 17일. https://www.justice.gov/usao-sdny/pr/united-states-attorney-announces-charges-against-ftx-founder-samuel-bankman-fried

U.S. Department of the Treasury. "U.S. and U.K. Take Largest Action Ever Targeting Cybercriminal Networks in Southeast Asia." Press Release, October 15, 2025. Access: 2026년 4월 17일. https://home.treasury.gov/news/press-releases/sb0278

U.S. Department of the Treasury. "U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash." Press Release, August 8, 2022. Access: 2026년 4월 16일. https://home.treasury.gov/news/press-releases/jy0916

U.S. Securities and Exchange Commission. "Statement on the Approval of Spot Bitcoin Exchange-Traded Products." SEC Official Website, January 10, 2024. Access: 2026년 4월 17일. https://www.sec.gov/newsroom/speeches-statements/gensler-statement-spot-bitcoin-011023

Métais, Valérie, et al. "MiCA & TFR: The Two New Pillars of the EU Crypto-Assets Regulatory Framework." DLA Piper, June 2023. Access: 2026년 5월 8일. https://www.dlapiper.com/en-us/insights/publications/2023/06/mica-tfr-the-two-new-pillars-of-the-eu-cryptoassets-regulatory-framework

Yahoo Finance. "Crypto Crime-Fighting Startup TRM Labs Notches $1 Billion Valuation with New $70 Million Funding Round." Yahoo Finance, February 4, 2026. Access: 2026년 5월 12일. https://finance.yahoo.com/news/crypto-crime-fighting-startup-trm-100000946.html

경향신문. "캄보디아 스캠범죄 배후 프린스그룹 천즈, 체포 후 중국 송환." 2026년 1월 8일. Access: 2026년 4월 17일. https://www.khan.co.kr/article/202601080645001

금융위원회. "내일(7.19일)부터 「가상자산이용자보호법」이 시행됩니다." 금융위원회 보도자료, 2024년 7월 17일. Access: 2026년 5월 8일. https://www.fsc.go.kr/no010101/82682

금융위원회·금융정보분석원. "'25년 하반기 가상자산사업자 실태조사 결과." 2026년 3월 25일. Access: 2026년 5월 8일. https://www.korea.kr/briefing/pressReleaseView.do?newsId=156750839

금융정보분석원. "'26년 자금세탁방지 주요 업무 수행계획." 금융위원회 보도자료, 2026년 2월 5일. Access: 2026년 5월 12일. https://www.fsc.go.kr/no010101/86209

뉴시스. "국내 가상자산 자금 160조 해외로…작년 거래소 순위 봤더니." 2026년 3월 12일. Access: 2026년 4월 30일. https://www.newsis.com/view/NISX20260312_0003545463

디지털애셋. "美 법원이 토네이도캐시를 제재할 수 없다고 판단한 이유." 2024년 11월 27일. Access: 2026년 5월 8일. https://www.digitalasset.works/news/articleView.html?idxno=23622

매일경제. "'싱가포르 비켜' 블록체인 새 메카 된 두바이…사업자수 4배로." 2025년 12월 8일. Access: 2026년 5월 8일. https://v.daum.net/v/20251208002400226

서울경제. "업비트 445억 원 해킹사고 배후로 北 라자루스 가닝성." 2025년 11월 28일. Access: 2026년 5월 12일. https://www.sedaily.com/NewsView/2H0MO4NIEW

서울신문. "코인 범죄 피해 7조원… 압수·회수 고작 0.7%." 2026년 2월 27일. Access: 2026년 5월 8일. https://www.seoul.co.kr/news/society/accident/2026/02/27/20260227010007

이데일리. "일본, 가상자산 '금융상품' 첫 규정…증권 수준 규제 도입." 2026년 4월 10일. Access: 2026년 5월 8일. https://www.edaily.co.kr/News/Read?newsId=05080726645414808&mediaCodeNo=257

자본시장연구원. "가상자산시장 현황 및 최근 미국과 홍콩의 가상자산 현물 ETF 승인." 『자본시장포커스』, 2024년 5월. Access: 2026년 5월 8일. https://www.kcmi.re.kr/publications/pub_detail_view?syear=2024&zcd=002001016&zno=1785&cno=6337

Traceable Money

Blockchain Analytics and the Conditions for Crypto Institutionalization

Researchers

Sanghyeon Park

Corresponding Author

Taemin Oh

Editorial Designer

Seongah Youn

Translator

Samuel J. Hahn

Contact

Sanghyeon Park kaistbab11@gmail.com