Written Testimony of:
Ari Redbord
Global Head of Policy
TRM Labs

Before the:
U.S. House Committee on Financial Services
Subcommittee on Digital Assets, Financial Technology and Inclusion

Hearing on:
Crypto Crime in Context Part II: Examining Approaches to Combat Illicit Activity

February 15, 2024

Introduction

Thank you Chairman McHenry, Ranking Member Waters, Subcommittee Chair Hill, Ranking Member Lynch and Members of the Committee for holding this hearing and inviting me to participate. It is a true honor to be here today. I am humbled by the critical role this institution plays in protecting our democracy.

My name is Ari Redbord. I am the Global Head of Policy at TRM Labs, a blockchain intelligence company.

At TRM, we deliver a dynamic picture of blockchain-based activity in order to mitigate financial crime and national security risks within the emerging digital asset economy. We do that by combining public data from 29 blockchains and over 70 million different digital assets with advanced analytics and proprietary threat intelligence.

Cryptocurrency businesses, financial institutions, law enforcement, national security, and regulatory agencies worldwide leverage our data and software solutions to measure, monitor, and investigate financial crime that involves digital assets and cryptocurrencies – from money laundering and ransomware attacks to hacks and terrorist financing.

I have spent my career working to protect the U.S. financial system from illicit actors – first for over a decade as a federal prosecutor in the U.S. Attorney's Office for the District of Columbia, and then at the Treasury Department as a Senior Advisor to the Under Secretary for Terrorism and Financial Intelligence. There, I worked with teams from Office of Foreign Assets Control (OFAC), Financial Crimes Enforcement Network (FinCEN), and across the interagency to safeguard the financial system from illicit use by terrorist financiers, weapons of mass destruction proliferators, drug kingpins, and other rogue actors.

During my time at the U.S. Attorney's Office I appeared almost daily in courtrooms just down the street from here. Each morning I would walk in and address the court, "Ari Redbord, for the United States." Those moments were the proudest of my professional life. I know that I can speak for my fellow witnesses, who have all dedicated their lives to the service of this country, when I say that we are all here "for the United States." We are here to work with you to protect the financial system from illicit actors, while, at the same time, ensuring that the U.S. remains the center of technological innovation in the world.

In this testimony, I hope to assist this Subcommittee in its consideration of several important issues that lie at the heart of both protecting the U.S. financial system and, at the same time, ensuring that the U.S. remains a hub for technological innovation. These issues include (1) the ability of U.S. regulators, law enforcement, and national security officials to leverage blockchain technology to track financial crime and other illicit activity; (2) ensuring that Treasury and other regulators have the tools and authorities necessary to effectively go after illicit actors who seek to take advantage of new technologies; and, (3) the importance of balancing national security interests with the need for privacy in a more open financial system by encouraging public-private partnerships, information sharing, capacity building and U.S. innovation.

Effective Detection and Investigation of Financial Crime is Enabled by the Blockchain

As we examine approaches to combating illicit finance in crypto it is paramount that we discuss and understand how we can leverage the native properties of public blockchains to disrupt it.

The native properties of public blockchains – data that is transparent, traceable, public, permanent, private, and programmable – can enable financial integrity professionals, law enforcement, regulators, supervisors, and other government agency officials to more readily identify risks and more effectively and efficiently detect and investigate financial crime. In this next section, I will go through the characteristics of blockchains and discuss how each native property allows for better financial crime compliance and investigation.

Transparent

Information about illicit funds moving through the financial sector currently resides on thousands of private corporate servers located in the U.S. and overseas. To combat financial crime, governments rely on financial institutions having adequate internal systems and data to report instances of fraud, money laundering, terrorist financing, and financial crime to regulators and law enforcement via Suspicious Activity Reports (SARs) or ad hoc notifications.

When I was a prosecutor I worked with agents from across U.S. law enforcement agencies to investigate cases involving bulk cash smuggling, networks of shell companies, hawalas, foreign banks, wire transfers, high value art, real estate, and around the dark corners of an opaque financial system.

The nature of public blockchains as open and distributed ledgers means that each transaction is verified and logged in a shared, immutable record with the timestamp of the transaction and the blockchain addresses involved. This data from the public blockchain is transparent, enabling the financial industry and government agencies to monitor trends in financial crime, market abuse, and financial stability in real-time and conduct more effective sectoral risk assessments.

The transparency of blockchain-based transactions provides visibility into illicit transaction volume that would otherwise be unattainable safely. For instance, the U.S. Department of Justice's (DOJ) press release[1] on the disruption of the Russian-language darknet market Hydra asserts that the market received approximately $5.2 billion in cryptocurrency for the purchase of illicit goods and services, such as illegal drugs, stolen financial information, fraudulent identification documents, and money laundering services.

Similarly, in two recent reports, TRM Labs' analysis showed that hack proceeds fell by around 50%[2] in 2023 to about $1.8 billion, down from $3.7 billion in 2022. Additionally, the growth rate of sales by online crypto-denominated vendors specializing in fentanyl and its precursor materials dropped by 150% in 2023.[3] We are only able to access this kind of data because of the transparent nature of public blockchains.

Traceable

For anti-money laundering (AML) compliance specialists and auditors working in traditional finance, cumbersome manual investigation is required to verify "source of wealth" and "source of funds" for a single customer, often requiring collecting information from independent sources such as company registries, banks, accountants, and lawyers. For government investigators, it may take months or even years to follow the trail of a sophisticated criminal, oftentimes requiring subpoenas across multiple service providers in various jurisdictions, necessitating law enforcement to go through the cumbersome Mutual Legal Assistance Treaty (MLAT) process to seek foreign law enforcement assistance to obtain evidence.

Because blockchains provide an immutable audit trail of every transaction, understanding the ultimate source and destination of funds, particularly across

[1]https://www.justice.gov/usao-ndca/pr/justice-department-investigation-leads-shutdown-largest-online-darknet-marketplace)
[2] https://www.trmlabs.com/post/hack-hauls-halve-from-2022
[3]https://www.trmlabs.com/post/crypto-denominated-fentanyl-sales-growth-falls-to-four-year-low-following-us-sanctions-and-enforcement-actions

jurisdictions, is substantially easier, faster, and more reliable compared to tracing funds through traditional financing mechanisms. Blockchain intelligence software can transform the alphanumeric characters on the blockchain to a visual representation of the flow of funds, allowing compliance specialists and law enforcement to "follow the money" around the world in real-time, accelerating investigation time.

The traceability of blockchain transactions also enables more advanced capabilities to detect suspicious activity. In traditional finance, compliance departments typically only view transactions which they are a direct counterparty in order to measure risk. The consequence is that transaction monitoring rules are limited to behavioral patterns such as transaction type, amount, or velocity. With blockchain transactions, transaction monitoring tools can be trained on a dataset that aren't just based on what one financial institution sees, they are based (in the case of TRM) on what we see on 29 blockchains – this gives virtual asset service providers (VASPs) an expansive view of risks.

Case Study: U.S. Secret Service Investigation Leads to $5M+ Seizure of Victim Funds

In the late summer of 2022, a soon-to-be victim was contacted by a scammer via the messaging feature of a real estate application. The scammer suggested moving the conversation onto a standard messaging app as the exchange between them became romantic in nature – a common feature of "pig butchering" scams. Over the course of a few months the victim sent about $1.1 million to the scammer before realizing that she had become the victim of a scam and reported to the U.S. Secret Service (USSS).

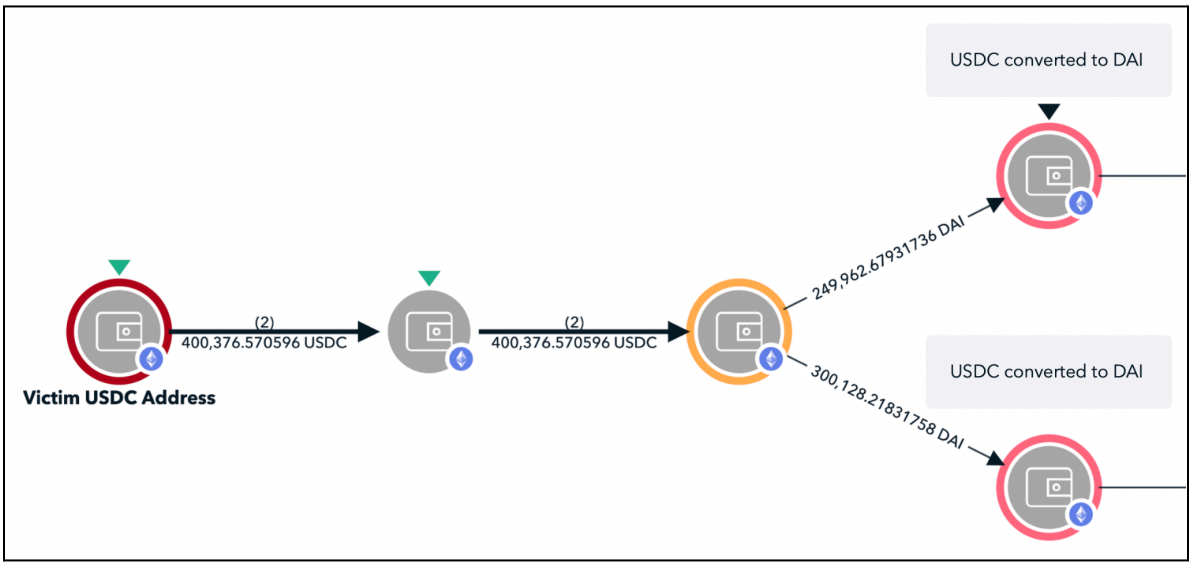
The victim's report resulted in the USSS opening an investigation. Using information provided by the victim, the investigators were able to plot the flow of funds from the original investment platform address through dozens of addresses and multiple types of cryptocurrency. The cryptocurrency tracing showed the non-economic laundering of funds through several addresses on the Ethereum blockchain, then coming to rest in an unhosted wallet.

Investigators used an alert function in TRM that would notify investigators each time funds moved from monitored wallet addresses, including the unhosted wallet where the victims' funds sat.

Getting these alerts – which are often triggered even before the transaction is registered on-chain – is critical, as scammers often park stolen funds in unhosted addresses for days, weeks, or even months at a time. The moment when they transfer the funds out of the unhosted addresses to cash-out at an exchange can be a prime opportunity for law enforcement intervention, but it must be done quickly before the funds are allowed to pass through the exchange successfully.

In this case, when the funds moved from the scammer's unhosted address to an exchange, the USSS received an alert and was able to act in real time to prepare a seizure warrant. Using data from the blockchain, combined with other evidence, the team secured a seizure warrant within hours and were ultimately able to seize about $5 million in stolen funds.

USSS investigators were only able to track, trace, and eventually seize back the stolen funds because they moved on public traceable blockchains.



Initial contribution by victim in USDC; scammer converted funds from USDC to DAI after two quick transactions.

[4] https://www.trmlabs.com/case-study/usss

Public

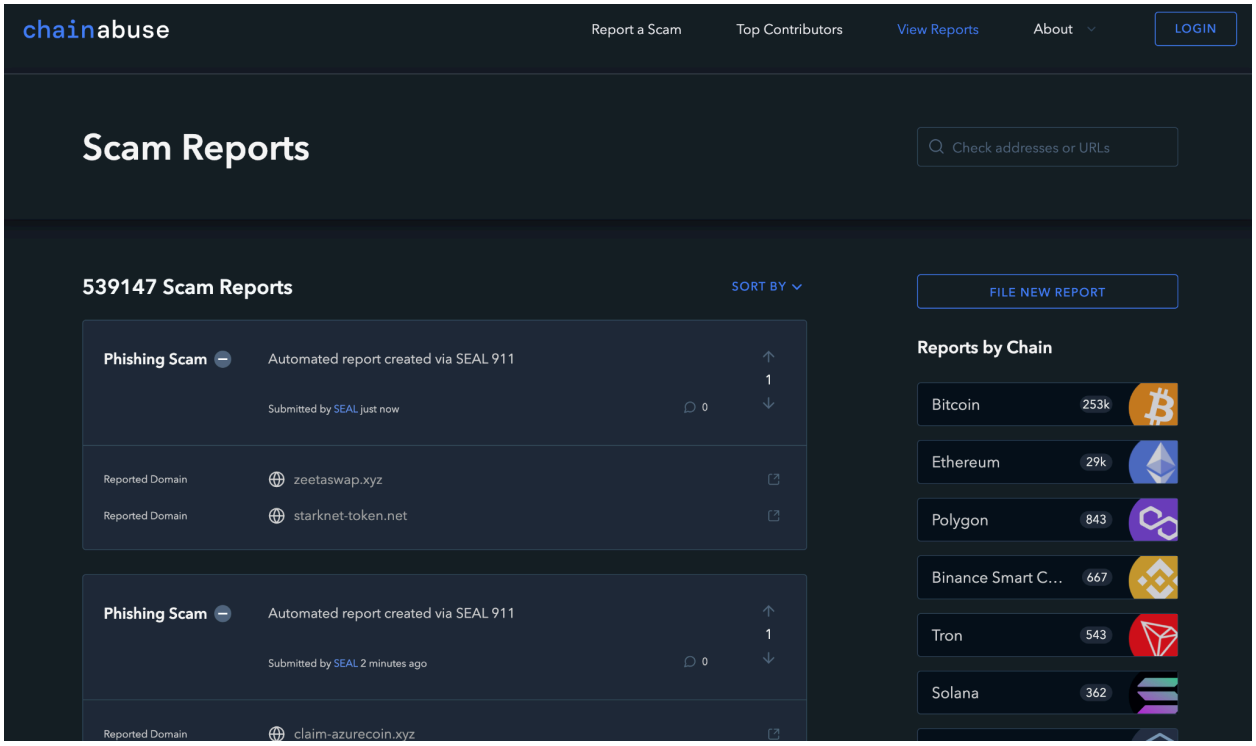
Unlike transaction and customer data held by companies or financial institutions, public blockchains are distributed and not managed by a central authority. Thus, anyone – including law enforcement officials and regulators – can access, identify, and trace blockchain transactions without a SAR, subpoena, search warrant, MLAT, or on-site examination because that information is free and publicly accessible, independent of a third-party. In court, prosecutors are then able to present the blockchain as an objective "eyewitness" on a single transaction rather than rely on a witness, such as a law enforcement investigator.

Using sophisticated tools, public blockchains enable law enforcement to link multiple victims together through on-chain transactional information, leading to more impactful investigations and disruptions.

For instance, inJuly 2022 a former product manager at Coinbase and his brother were arrested for insider trading. The conduct occurred as late as April 2022 and involved the Coinbase employee using insider information regarding the timing of coin listings on the platform. Because of the public nature of blockchains the case began, according to the DOJ release,[5] shortly after the trades occurred, when a Twitter account, that is well known in the crypto community, tweeted about an Ethereum blockchain wallet "that bought hundreds of thousands of dollars of tokens exclusively featured in the Coinbase Asset Listing post about 24 hours before it was published." Investigators were then able to review blockchain transactions to see when, precisely, the defendants traded. The brother pleaded guilty about two months after his arrest and the Coinbase employee pleaded guilty shortly thereafter. The case moved so quickly because law enforcement was so easily able to prove the conduct through transactions on the blockchain.

In addition, the public nature of blockchains enables greater information-sharing between consumers, enabling them to protect themselves from scams, hacks, and fraud. Through crypto fraud-reporting tools like Chainabuse.com,[6] members of the public can increase visibility of notable schemes and limit further victims. Since its launch in the summer of 2022, Chainabuse has received over 539,000 reports of fraud, with less than1% identified as false reporting.

[5]https://www.justice.gov/usao-sdny/pr/former-coinbase-insider-sentenced-first-ever-cryptocurrency-insider-trading-case
[6]https://www.chainabuse.com/

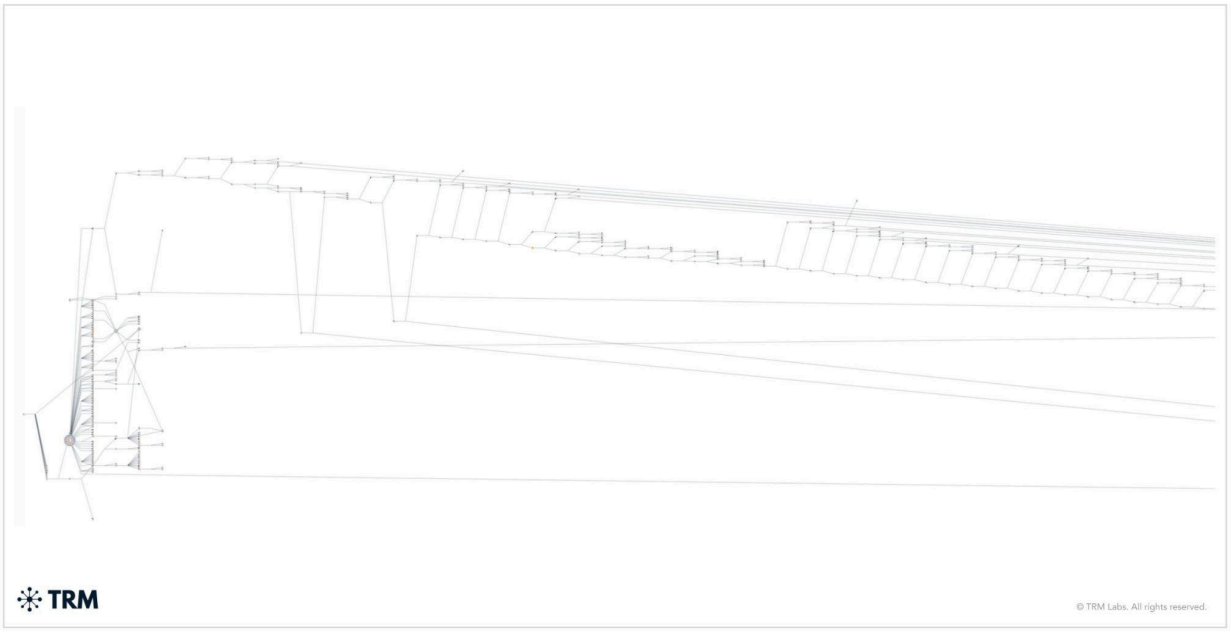


Permanent

Storing transaction records for long periods of time is costly, cumbersome, and may be prohibited under local law. Consequently, records are often missing, creating hurdles for financial crime investigations. In contrast, transactions are permanently recorded on the blockchain, which allows institutions, auditors, and government investigators greater ability to "follow the money," even if the transaction is several years old.

In 2016, the virtual currency exchange Bitfinex was hacked and 120,000 bitcoin (BTC) was stolen. In early 2022, two individuals were arrested,[7] and eventually pled guilty,[8] for the hack and their laundering of the stolen proceeds then valued at over $4.5 billion. According to the public statement of facts,[9] blockchain transactions from 2017 appear to have played a large role in ultimately identifying the alleged launderers despite a years-long money laundering campaign. Other cases such as the Silk Road and Alphabay takedowns were successfully prosecuted because of breadcrumbs on the blockchain that happened months or years before the investigation.

[7]https://www.trmlabs.com/post/suspects-accused-of-laundering-funds-stolen-from-bitfinex-in-2016-arrested-today-in-new-york
[8]https://www.trmlabs.com/post/bitfinex-money-launderers-plead-guilty-in-the-razzlekhan-case
[9]https://www.justice.gov/opa/press-release/file/1470186/download



TRM Graph: Excerpt of thousands of deposits to the Wasabi mixing services conducted by the Bitfinex hackers in April 2021

Private

As more and more consumers, businesses, and governments transact on blockchains, it is even more important to enable financial privacy on blockchains, in order to protect consumer privacy, prevent corporate and nation-state espionage, reduce the risk of data breaches, and protect national security.

It bears emphasizing that privacy and blockchains are not incompatible. In many ways, blockchain-based technologies – by minimizing the need to store personal data in one centralized repository, by empowering individuals to assert control over who accesses their data, and by allowing individuals to determine for what purposes their data will be used – are more privacy-protective than the status quo.

Meanwhile, within the industry, Privacy-Enhancing Technologies (PETs) like zero-knowledge proofs are being deployed at the protocol, middleware, and application layers to advance data protection and privacy goals. PETs can be used to make information on blockchains private, such as transaction details or data on blockchain-based computer programs. Notably, PETs can be configured to make information selectively visible depending on certain conditions and policies, such as whether the requester is authorized to view the data. For example,[10] layer 1 blockchain Solana recently announced the use of zero-knowledge proofs that allow for users to make blockchain transactions without revealing key details of the transaction, such as the transaction amount.

[10]https://www.helius.dev/blog/all-you-need-to-know-about-solanas-v1-16-update

Over the last few years there has been a growing focus by regulators on the use of privacy enhancing technologies such as mixers. Financial privacy is a standard expectation in traditional financial systems, and most consumers naturally expect their transactions to remain private. In a financial system in which more and more transactions occur on open, transparent blockchains, where every transaction is logged and immutable, crypto mixers extend this norm of financial privacy into the realm of cryptocurrencies by obfuscating transaction histories on the blockchain. This is especially useful in regions where exposing wealth could trigger kidnapping or extortion.

However, over the last few years, as discussed in more detail below, we have seen illicit actors, such as North Korea, use mixers[11] to launder billions of dollars in hacked and stolen funds. This is where the balancing comes in – how do we ensure that lawful users are able to transact in a private manner while mitigating the risks posed by illicit actors?

There are technology solutions, such as blockchain intelligence tools, that are being widely used by law enforcement and national security agencies today to build and investigate cases despite the use of mixers. The first line of defense from illicit actors who use mixing technologies is the ability to trace the flow of funds through mixers. TRM works with our law enforcement clients today to enable the ability to trace through many mixers with a high degree of confidence.

There are other solutions, such as digital identity and zero-knowledge proofs, that are in more nascent stages of development. Adoption of new technologies, along with ongoing dialogue with industry, will help regulators thread the needle between privacy and security.

Programmable

The blockchain provides a new opportunity to increase access to the financial system by reducing the cost of providing financial services. One example is compliance, the blockchain allows for the integration of automated know your customer (KYC)/AML controls at the protocol, smart contract, and application layer.

Blockchain-based "digital passports" could allow individuals and entities to store proof of KYC verification directly on the blockchain, a "win-win" for all parties – customers, institutions, and government – involved in transactions. Customers would seamlessly access financial services and minimize the distribution of sensitive personal information to new financial intermediaries. Developers could program automated approvals or denials directly into smart contracts and protocols to prevent sanctioned or other high-risk addresses from interacting with their services.

[11]https://www.trmlabs.com/post/inside-north-koreas-crypto-heists

The Use of Blockchain Intelligence for Sanctions and Enforcement Actions Has Been Effective

Over the last few years Treasury has created a playbook[12] that has effectively used sanctions to target illicit actors and those that facilitate illicit activity, while, at the same time, using enforcement actions to send a message about the importance of compliance. These actions utilize the native properties of public blockchains making both sanctions and AML enforcement more effective and easier to measure than in the traditional world.

Since September 2021, when OFAC first used sanctions against a cryptocurrency exchange – non-compliant Russian VASP SUEX[13] – Treasury has focused on using sanctions to target illicit actors and those that facilitate illicit activity without targeting the broader, overwhelmingly lawful, crypto ecosystem. Targets have included non-compliant exchanges Chatex,[14] Garantex,[15] Bitzlato,[16] and most recently Gaza-based BuyCash.[17]

In addition to non-compliant exchanges Treasury has used sanctions and other authorities to target darknet markets like Hydra,[18] facilitators of sanctions evasion,[19] drug trafficking,[20] and other illicit activity.

According to analysis by TRM, sanctions against crypto-related businesses and individuals by OFAC rose three-fold, from 11 designation events in 2022 to 33 in 2023. Among the targets were 12 ransomware groups, six high risk exchanges and a cryptocurrency mixing service.[21]

Treasury has been particularly focused on the use of sanctions to punish North Korea's malign activity. Hackers tied to North Korea stole at least $700 million in cryptocurrency in 2023, according to research by TRMs. Nearly $3 billion worth of crypto has been lost to Pyongyang-linked threat actors since 2017. However, OFAC has effectively used sanctions to target this activity adding significant friction to the laundering process.[22]

---

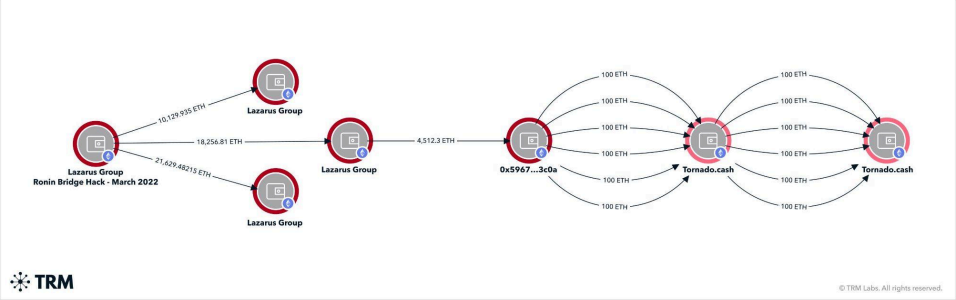
[12]https://www.trmlabs.com/post/us-treasury-continues-whirlwind-of-activity-in-the-crypto-space
[13]https://www.trmlabs.com/post/behind-suex-io-the-first-sanctioned-cryptocurrency-exchange
[14]https://www.trmlabs.com/post/treasury-designates-cryptocurrency-exchange-chatex
[15]https://www.trmlabs.com/post/darknet-markets-explained
[16]htttps://www.trmlabs.com/post/doj-and-treasury-announce-actions-against-bitzlato-exchange-for-facilitating-russian-illicit-finance
[17]https://www.trmlabs.com/post/treasury-sanctions-gaza-based-virtual-currency-exchange-buycash-in-wake-of-hamas-attacks
[18]https://www.trmlabs.com/post/hydra-market-takedown
[19]https://www.trmlabs.com/post/u-s-treasury-imposes-sanctions-on-money-launderer-responsible-for-moving-funds-on-behalf-of-russian-elites-and-ransomware-actors
[20]https://www.trmlabs.com/post/u-s-treasury-and-doj-take-action-against-chinese-fentanyl-trafficking-network
[21]TRM Labs analysis
[22]https://www.trmlabs.com/search?query=north+korea

While the North Korea issue is primarily a cyber security issue – the key is to stop attacks from happening in the first place – law enforcement and regulators have effectively used blockchain technology to add friction to the laundering process.

Case Study: Tornado Cash

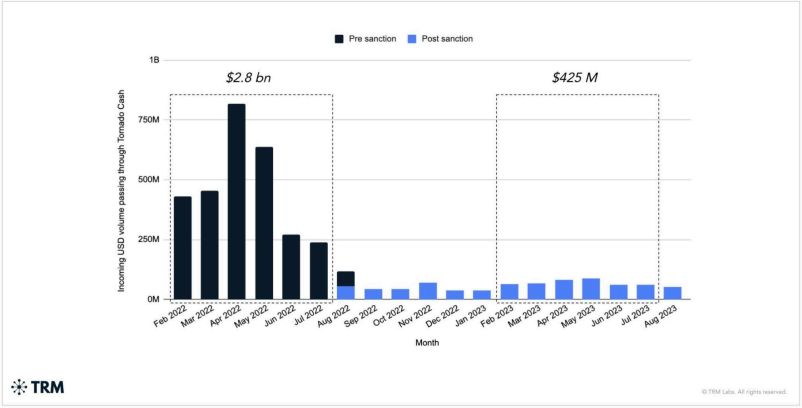
In March 2022, Lazarus Group struck the Ronin bridge,[23] a service that allows users to move funds from one blockchain to another, stealing over $600 million in cryptocurrency that could potentially be used by North Korea for weapons proliferation and other destabilizing activity.

What followed was OFAC, using blockchain intelligence to trace the stolen funds, sanctioning both the blockchain addresses to which the funds moved, and the mixing services that North Korea utilized to launder the proceeds – including centralized bitcoin mixer blender.io and decentralized Ethereum mixer Tornado Cash.[24] These rapid sanctions designations were only possible because of the transparent nature of public blockchains and allowed Treasury to target the bad actors rather than the activity itself.



TRM graph showing funds stolen from Ronin hack laundered through Tornado Cash

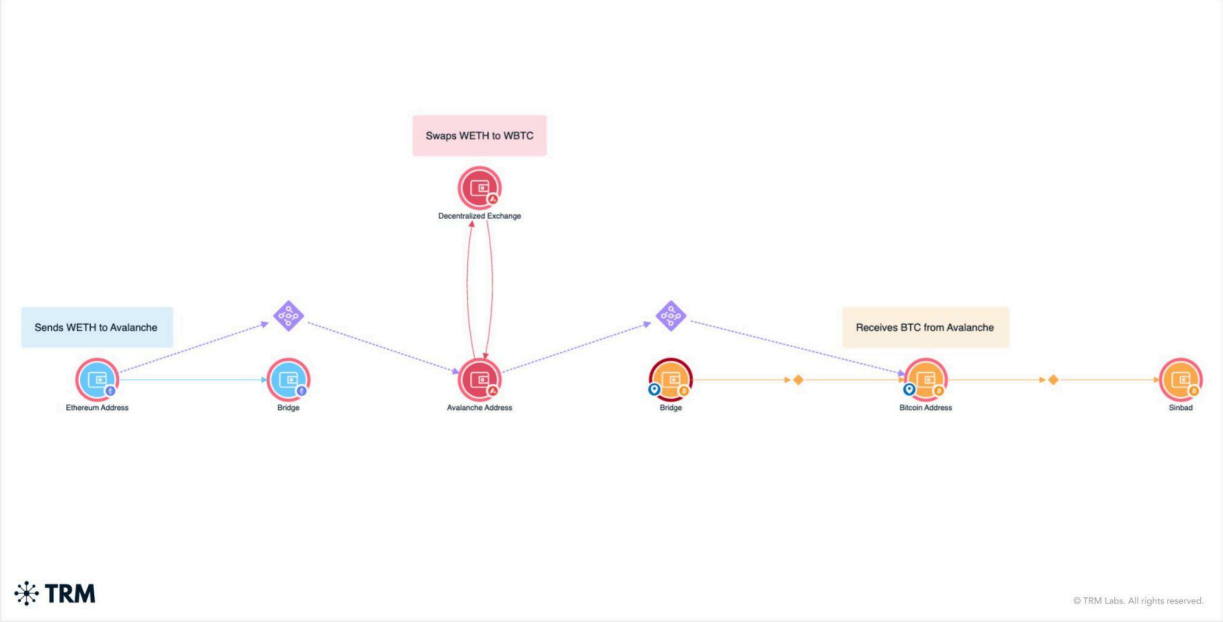
OFAC's sanctioning of Tornado Cash succeeded in radically reducing usage of the service. According to TRM,[25] the overall volume passing through Tornado Cash decreased by close to 85% post OFAC sanctions. Perhaps most importantly, North Korean hackers appear to have largely abandoned the service in favor of more traditional bitcoin mixers.[26]



TRM chart showing overall volume passing through Tornado Cash has decreased by close to 85% post-sanctions.

[23]https://www.trmlabs.com/post/north-koreas-lazarus-group-moves-funds-through-tornado-cash
[24]https://www.trmlabs.com/post/u-s-treasury-sanctions-widely-used-crypto-mixer-tornado-cash
[25]https://www.trmlabs.com/post/tornado-cash-volume-dramatically-reduced-post-sanctions-but-illicit-actors-are-still-using-the-mixer
[26]https://www.trmlabs.com/post/us-treasury-sanctions-north-koreas-preferred-mixer-sinbad

Similarly, in November 2023, OFAC sanctioned bitcoin mixer Sinbad,[27] calling the service "a key money-laundering tool of North Korea's OFAC-designated Lazarus Group." After Tornado Cash was the target of OFAC sanctions in August 2022 and ChipMixer was taken down by law enforcement in 2023, TRM analysis[28] shows North Korea used Sinbad to launder the proceeds of its more recent hacks, including the Harmony, Atomic Wallet, Alphapo, Coinspaid, Stake, and Ronin Bridge hacks. TRM's on-chain analysis[29] showed, at the time of designation, that Sinbad was the second largest mixer by volume in 2023, receiving close to a fifth of all funds sent to mixers in 2023. Following Treasury's designation of Sinbad, the mixing service essentially shutdown operations.



Funds moving through Sinbad after Atomic Wallet hack

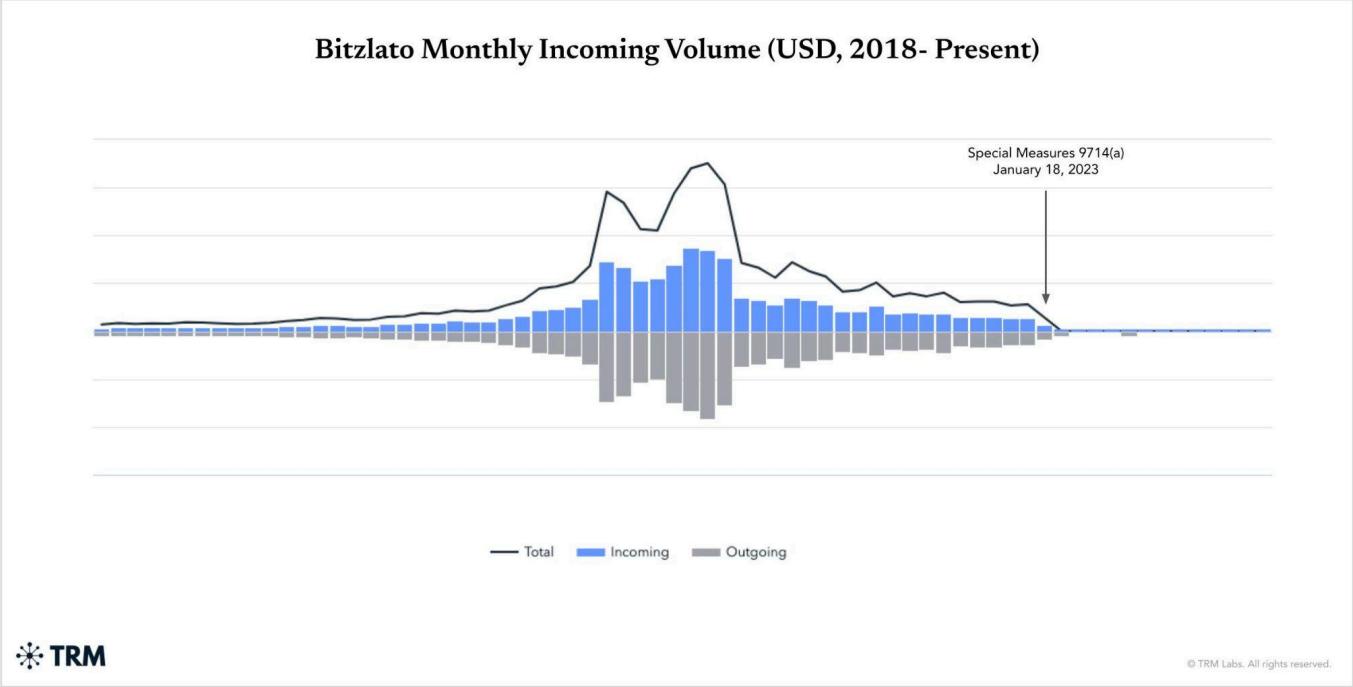
[27]https://www.trmlabs.com/post/us-treasury-sanctions-north-koreas-preferred-mixer-sinbad
[28]Id.
[29]Id.

Case Study: Bitzlato[30]

In January 2023, the DOJ and Treasury announced a coordinated action against non-compliant, Hong Kong-registered cryptocurrency exchange Bitzlato, and the arrest of its owner for "conducting a money transmitting business that transported and transmitted illicit funds and that failed to meet U.S. regulatory safeguards, including anti-money laundering requirements."

The actions directly linked Bitzlato to Russian illicit finance – particularly, ransomware and darknet markets – allowing FinCEN to issue, for the first time, an order pursuant to section 9714(a) of the Combating Russian Money Laundering Act. This order designated Bitzlato as a "primary money laundering concern" in connection with Russian illicit finance, and prohibits certain transmittals of funds involving Bitzlato by any covered financial institution.

According to TRM, over the course of its existence Bitzlato laundered nearly $2.5 billion in cryptocurrency. Treasury's 9714(a) designation, along with the concurrent law enforcement action, caused a 99% reduction in incoming volume, essentially putting an end to the exchange.[31]



[30]https://www.trmlabs.com/post/doj-and-treasury-announce-actions-against-bitzlato-exchange-for-facilitating-russian-illicit-finance
[31]TRM Labs analysis

There has been some discussion as to whether or not Treasury needs additional authorities to target illicit actors and mitigate financial crime risk in the crypto ecosystem will certainly continue to study the need to expand the regulatory perimeter. However, we have seen over the last few years, Treasury use its existing authorities, including sanctions, to effectively target illicit actors and those that facilitate money laundering while simultaneously using enforcement actions to send a message about the importance of compliance.

While sanctions and enforcement actions are effective, it is also important to maintain that effectiveness over time. Unlike sanctions in traditional finance, in blockchain we have a much greater ability to measure the short and long term impact of sanctions and other actions. After a few months does volume return to a service? If so, what part of the playbook should be used next to maintain pressure on the actor? On blockchains we can view all of this as it happens, allowing law enforcement and national security professionals to pivot their response based on real time insights.

Building a Safer Financial System Through Public, Private and Global Partnerships, Information Sharing and Education

The challenge for policymakers is to enable lawful users of blockchains to transact in a secure and private manner, while, at the same time, ensuring that illicit actors are not able to take advantage of new technologies.

As discussed in detail above, there are technology solutions to support this balancing. Blockchain intelligence allows law enforcement, regulatory and national security agencies to track and trace the flow of funds to build investigations, disrupt bad actors, and mitigate risks. The only barrier to effectiveness is the availability of tools and the training necessary to ensure that law enforcement professionals have the capacity required to meet the threat.

Because of the global nature of blockchains, on which value is moved cross-border at the speed of the internet, international cooperation, information sharing and resourcing regulators, law enforcement, and national security agencies around the world to more effectively combat crimes conducted with cryptocurrencies is essential. While TRM, through TRM Academy,[32] and in partnership with law enforcement entities worldwide, has trained[33] thousands of agents and investigators across the globe on cryptocurrency investigations, without access to blockchain intelligence tools law enforcement, regulators and national security agencies cannot effectively combat the increasingly sophisticated use of cryptocurrencies for illicit activity. In other words, in order to leverage the technology described above, law enforcement needs access to it.

[32] https://www.trmlabs.com/training-and-certifications

[33]https://www.trmlabs.com/post/trm-joins-us-secret-service-and-security-service-of-ukraine-for-training-on-crypto-investigations

In addition we must continue to foster and support innovation in the United States. This means building solutions – public and private sectors together – that give citizens the comfort to transact on-chain and commercial entities the incentive to build a thriving digital asset economy in the United States.

The recent FinCEN notice of proposed rulemaking (NPRM)[34] that would identify mixing transactions as a "primary money laundering concern," and recent assertions by Treasury that node validators, wallet providers, and DeFi protocols should potentially be treated as financial institutions for purposes of the Bank Secrecy Act (BSA),[35] highlight the need for greater collaboration and understanding about what is technically possible today to meet the objectives of compliance, privacy and security today and in the future. For example, Michael Mosier, also a witness before this Subcommittee today, and Rebecca Rettig recently wrote a paper outlining a potential path forward that would "achieve the policy goals of combating illicit financial activities while allowing for continued innovation in DeFi, a nascent technological sector."[36]

As recommended by the CFTC's Technology Advisory Committee's January 2024 report,[37] we should encourage public-private partnerships and information sharing initiatives in order to increase capacity among regulators and policy makers to better understand the growing digital asset and decentralized ecosystem, including the use of mapping data, expertise, and understanding what resources are needed.

These partnerships and information sharing initiatives should go beyond the digital world as blockchain intelligence solutions are only able to follow funds on-chain. Law enforcement and national security agencies must still understand and navigate the opaque corners of our financial system where illicit actors seek to move funds off the blockchain.

As we move into a more decentralized space, where more transactions occur peer-to-peer and cross border at the speed of the internet, public-private and global partnerships and information sharing efforts are more important than ever. We look forward to continuing to work with regulators and policy makers globally to provide the tools and training necessary to mitigate risk in the crypto ecosystem.

[34]https://www.federalregister.gov/documents/2023/10/23/2023-23449/proposal-of-special-measure-regarding-convertible-virtual-currency-mixing-as-a-class-of-transactions
[35]https://home.treasury.gov/news/press-releases/jy1934
[36]https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4607332
[37]https://www.cftc.gov/media/10106/TAC_DeFiReport010824/download

Recommendations

1. Ensure that law enforcement, regulatory and national security agencies have the tools to utilize blockchain technology to mitigate illicit finance and national security risks.
2. Deepen U.S law enforcement training and operational capacity for blockchain-related investigations and expand access to tools and capacity-building efforts with foreign law enforcement partners.
3. Encourage regulatory efforts with proven effectiveness based on a data-driven understanding of impact.
4. Encourage regulators and industry to work more closely together in order to better understand how to leverage new technologies including through public-private partnerships and information sharing initiatives related to illicit finance.
5. Focus on off ramps in non-compliant jurisdictions that facilitate the laundering of cryptocurrency by allowing illicit actors to move funds off-chain.

Conclusion

As we move further into the digital world, there will continue to be criminal activity in cryptocurrencies that pose a risk to national security. However, by harnessing the native properties of public blockchains we can enable compliance professionals, law enforcement, regulatory and national security agencies to investigate, mitigate, and measure illicit finance risk in new and more effective ways. This is something we cannot enable in the more traditional world where money laundering often occurs in cash and through networks of shell companies.

We are all working together – industry and government – to build a safer financial system. We look forward to working with this Committee and "for the United States."