

A LAW ENFORCEMENT SUPPLEMENT

Following the Money in a Cross-chain World

A law enforcement supplement to Elliptic's Cross-chain Crime report on the future of crypto crime and money laundering.

elliptic.co/law-enforcement

A network diagram consisting of numerous nodes connected by lines, forming a complex web. A thick, glowing arc in shades of green and yellow curves across the lower half of the image, connecting two specific nodes. The nodes are represented by small circles, some of which are highlighted with concentric circles, suggesting a focal point or a specific transaction.

ELLIPTIC

The **\$10.5 Billion** Cross-chain Crime Problem Facing Law Enforcement

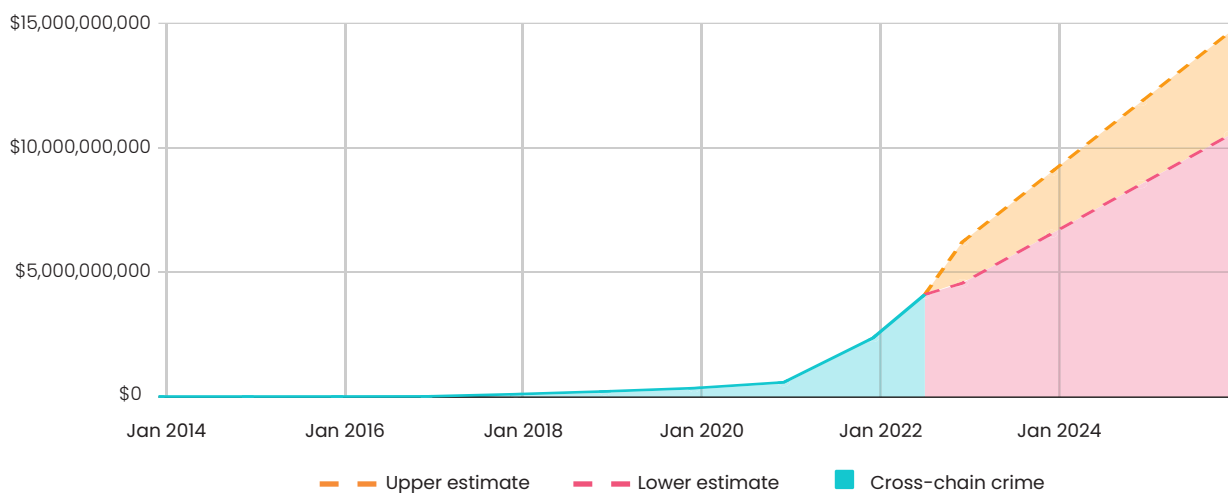
Though Bitcoin was the dominant (and only) blockchain in the early 2010s, the number of new blockchains and cryptoassets have skyrocketed in recent years. This emerging multi-chain ecosystem — while overwhelmingly facilitating legitimate activity — has nevertheless caught the attention of illicit actors seeking new ways to launder their criminal proceeds.

Ranging from low-level cybercrime such as scams and pig butchering cases, to large-scale drug and ransomware operations, savvy criminals are leveraging the ability to move proceeds between cryptoassets (asset hopping) or across blockchains (chain hopping) to conceal their funds. Yet legacy blockchain analytics tools do not have the capability to follow the money across and between different assets and chains — frustrating criminal investigators and handing crypto criminals the advantage.

By 2022, Elliptic has identified over **\$4.1 billion of illicit or high-risk¹ crypto that has been laundered through either asset-hopping or chain-hopping**. This has been made possible by decentralized exchanges (DEXs), cross-chain bridges and coin swap services — technologies that allow criminals to obfuscate the movement of illicit funds and achieve some degree of anonymity. As the multi-chain ecosystem continues to develop and existing popular crypto laundering methods (such as mixers) continue to be blocked by legal interventions, cross-chain crime will likewise grow as it becomes the laundromat of choice for crypto criminals.

Elliptic forecasts the value of crypto laundered through chain or asset hopping will increase by almost 60% year-on-year to reach \$6.5 billion by 2023, and reach at least \$10.5 billion by 2025.

The Rapid Rise of Cross-chain Crime



¹Crypto originating from sources often utilized by money launderers, such as mixers before they are sanctioned or gambling (services that may also be illegal in some jurisdictions).

About This Report

This briefing note is a supplement to Elliptic's *State of Cross-chain Crime 2022* report, written for criminal investigators at law enforcement and other government agencies. It contains a brief description of the cross-chain crime problem and its facilitators. We then provide practical recommendations to help law enforcement agencies stay ahead of the new ways bad actors are laundering the proceeds of crime and evading detection.

To Catch a Thief, Think Like a Thief. The Tools of the Cross-chain Criminal You Need to Know About

At Elliptic, we believe that cryptoassets will form the foundation of a financial system that is fairer, freer and safer for all to use. Cryptocurrencies, NFTs and other virtual assets are fast becoming part of the mainstream financial ecosystem, with around 20% of US adults estimated to be holding Bitcoin alone.

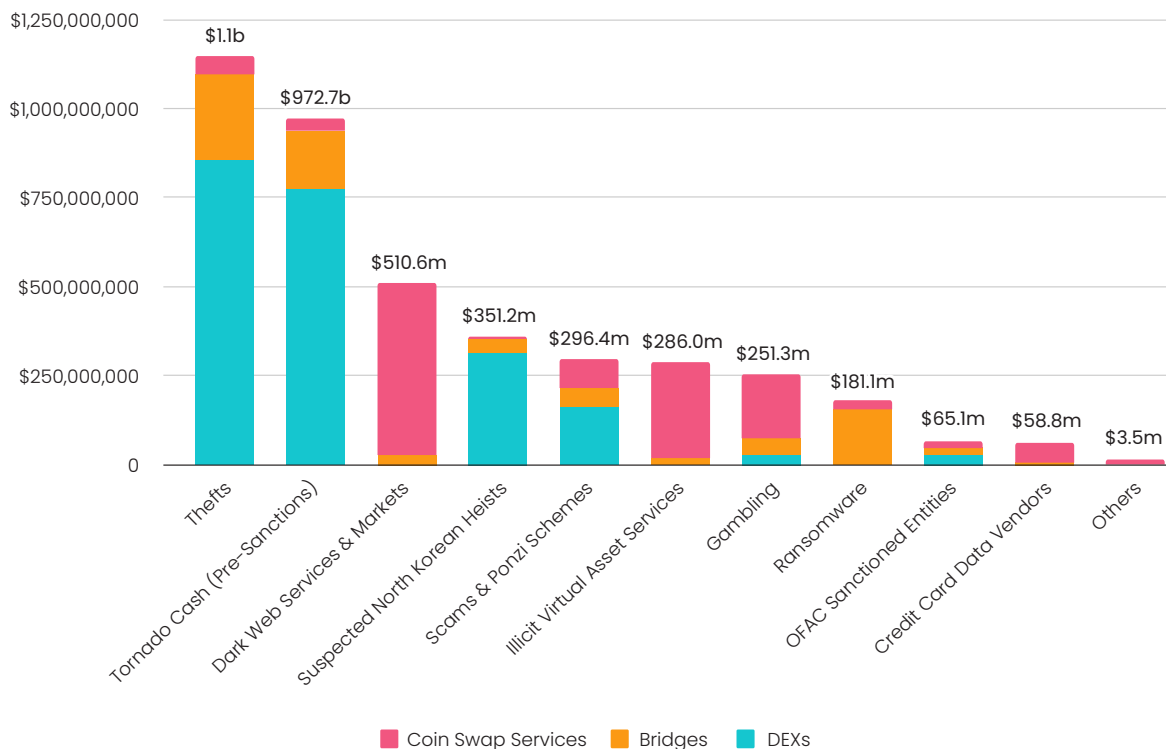
There are now more than 20,000 cryptocurrencies operating on hundreds of different blockchains around the world, with the total market capitalization worth in excess of \$1 trillion. Following Bitcoin's creation in 2009, thousands of different cryptocurrencies — such as Ether, BNB, Dogecoin, Monero, Solana and TRON — have launched, with more being released daily. Many of these cryptoassets support a range of different utilities, such as stablecoins and NFTs.

For bad actors, this expansion of blockchain technology and the growing adoption of cryptoassets by everyday citizens poses many opportunities for criminality. It's now typical for dark web markets to take payments in multiple cryptocurrencies, while terrorist organizations routinely advertise on social media for donations. Frontline police are increasingly being asked to investigate crypto thefts or find their investigations quickly cross into the digital realm as they track the proceeds of crime.

Understanding and pre-empting crime trends is critically important for law enforcement, so they can direct their resources to where they will be most effective against criminality.

The chart below demonstrates that perpetrators of all sorts of cybercrime utilize chain and asset hopping to launder their crypto.

Illicit and High Risk Crypto Laundered Through DEXs, Cross-chain Bridges and Coin Swap Services by Origin (2022)



The Big Three Cross-chain Crime Threats

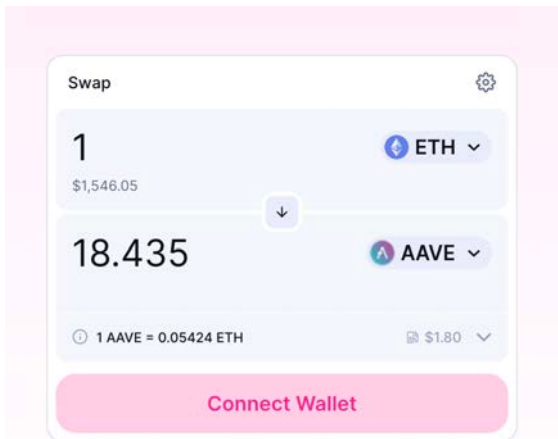
Three services are being leveraged by criminals that threaten the integrity of the crypto ecosystem: decentralized exchanges (DEXs), cross-chain bridges and coin swap services. These tools facilitate cross-chain money laundering and terrorist financing due to their lack of identity checks and anti-money laundering (AML) controls. The use of these services is overwhelmingly legitimate, but they nevertheless open the door for enterprising criminals to escape justice, often inadvertently.

See below for a summary of these services, and refer to Elliptic's [State of Cross-chain Crime report](#) (chapters 1 - 3) for more information.

Centralized exchanges – which also facilitate cross-chain or cross-asset swaps – are not considered here, as most mainstream services utilize AML and identity screening solutions.

Decentralized Exchanges (DEXs)

- Function: Swap between cryptoassets on the same blockchain (asset-hopping)
- Examples: Uniswap, Sushiswap, 1inch, Curve.fi, PancakeSwap
- High risk funds processed: Over \$1.2 billion since late 2020

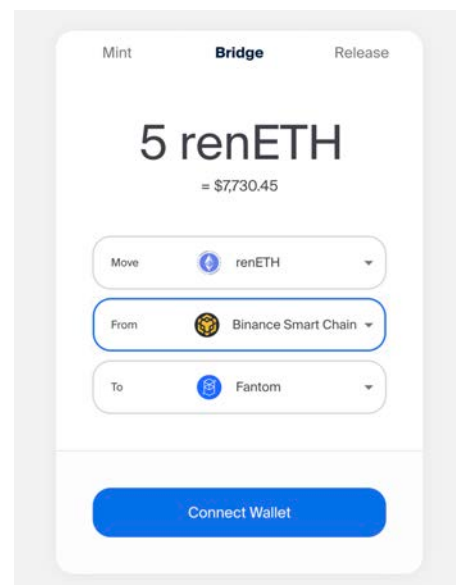


A DEX is a decentralized smart contract based crypto exchange that allows users to swap any tokens, as long as a liquidity pool exists for that token. Due to their legitimate use case, largely related to DeFi investing, criminals use them predominantly to launder proceeds of DeFi or exchange thefts. Anonymous by design, the services allow criminals to bypass the compliance checks required by most centralized exchanges.

Cross-chain Bridges

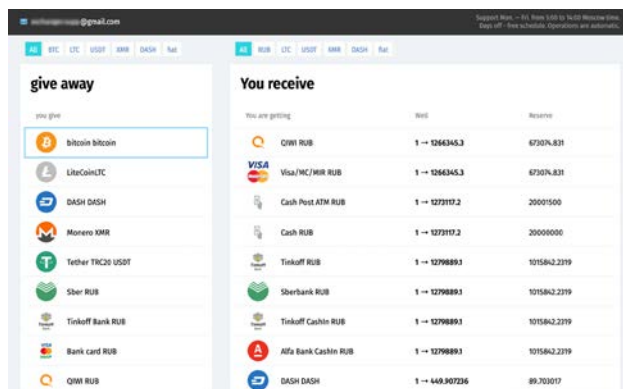
- Function: Swap between cryptoassets on different blockchains (chain-hopping)
- Examples: renBridge
- High risk funds processed: Over \$750 million since 2020

Bridges are also often decentralized and smart contract based, locking funds on one blockchain and issuing users the converted equivalent on another. They are mainly used to launder the proceeds of hacks (including those initiated by North Korea), ransomware, scams and Ponzi schemes.



Coin Swap Services

- Function: Swap assets either within or across blockchains without an account
- Examples: AudiA6
- High risk funds processed: Over \$1.2 billion since 2013



Coin swap services are centralized services that swap users' funds anonymously, almost instantly. Some are legitimate-facing services and may have AML controls. However, others cater only to cybercriminals and may process privacy coins such as Monero. Most of the illicit funds originate from dark web markets, scams, Ponzi schemes or data vendors.

Hitting Pay Dirt: Why Cross-chain Crime is Increasing

Cross-chain crime is on the rise, accelerating much faster than anyone anticipated.

By 2020, just over \$500 million had been laundered through DEXs, bridges and coin swap services. By July 2022, that figure had surged to \$4.1 billion, with just under half (\$1.8 billion) attributed to sanctioned or eventually-sanctioned entities (such as Tornado Cash).

Now, Elliptic projects cross-chain crime will rise even further, laundering over \$6.5 billion of high-risk crypto by 2023 and \$10.5 billion by 2025 (with an upper estimate of almost \$15 billion).

There are a number of reasons why cross-chain crime is projected to continue its rapid rate of growth:

- **Legacy blockchain analytics solutions cannot trace cross-chain crime** — Criminals are wise to this, so layer the proceeds of crime through a series of fast, complex transactions to evade detection. This turns investigations into resource intensive, cumbersome and time consuming ordeals.
- **It can be used to launder funds from small-scale scams to large-scale cybercrime** — Chain and asset hopping can be used to launder cryptoassets in the low thousands to many millions of dollars. The threat of abuse is therefore relevant to all levels of law enforcement.
- **Alternative laundering methods are being targeted** — Traditional crypto laundering tools, such as mixers, have been the target of enforcement actions and sanctions recently, leaving criminals to increasingly look at chain/asset hopping as alternatives. The theory of “crime displacement” means when one type of crime is prevented, bad actors will go where no one is looking or enforcing the law.
- **It provides a gateway to many crypto services** — Criminals raking in illicit crypto on one blockchain can use chain/asset hopping capabilities to invest those illicit funds into DeFi, NFTs and other similar opportunities on different chains
- **It’s anonymous** — Most (if not all) DEXs, cross-chain bridges and coin swap services allow users to transact anonymously, without any KYC checks or AML controls.

Mission Possible: Ensure Crypto Crime Doesn't Pay

Legacy blockchain analytics tools were built for a single cryptoasset world, when it wasn't possible to move funds between different assets and blockchains. Therefore, this legacy approach can no longer give a true representation of criminality and the bad actors moving funds chain agnostically.

The most important action that law enforcement can take to combat cross-chain crime is to adopt blockchain analytics solutions that screen the ecosystem holistically.

We're referring to the next generation of blockchain analytics tools that can track the proceeds of crime, even as funds are moved across and between multiple cryptoassets and blockchains. This way, you are not just viewing multiple currencies individually or seeing separate elements layered together in aggregate – you are in fact exposing the flow of funds across all assets and blockchains concurrently. This is because you are tracing across the ecosystem as a whole to give a complete picture of criminality.

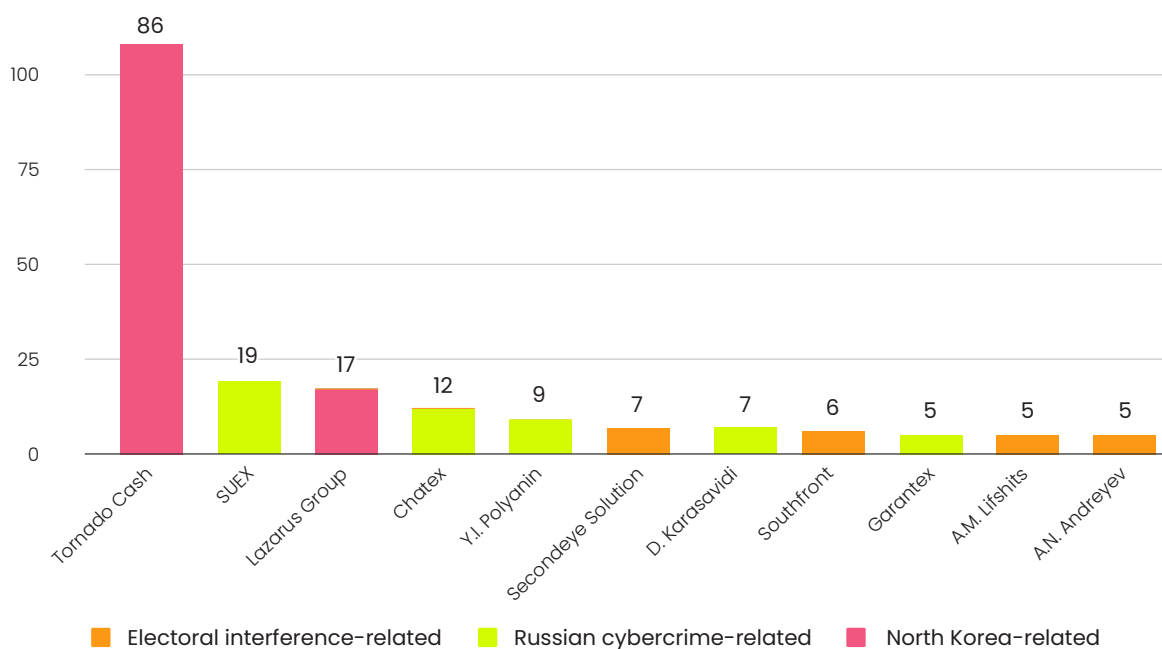
A demonstration of how these new blockchain analytics tools work, and the difference they make in helping solve more crypto-related crimes, can be found in Elliptic's *State of Cross-chain Crime report* (chapter 4).

Besides and in addition to holistic screening solutions, law enforcement agencies should:

- **Demystify and democratize** access to blockchain intelligence by upskilling your investigative teams. Make sure enough agents have access to the tools they need to effectively investigate their crypto-related crime cases with confidence, whatever their specialism – thus sharing the workload as the volume of crypto-related crime cases increases.
- Best practice is to get a second view by **corroborating your evidence** with an alternate blockchain analytics provider. When gathering intelligence in the early stages of an investigation, a quick re-screen of a suspect wallet with a second provider can help reduce false positives or uncover more leads. Further into your investigation, corroborating could identify additional evidential opportunities to strengthen your case and achieve a conviction.
- **Whodunit?** Once you've got the suspect, it can be difficult to prove they committed the crime. To build a strong case you need to defeat all defenses. Think like a defense attorney by looking outside the world of crypto to prove beyond all reasonable doubt exactly who was behind the computer. Make sure you can access the information you need quickly to issue subpoenas, seize stolen funds, and ultimately, get to trial.
- **Hit a dead end?** Criminals will make mistakes more often than not. Even the savviest will need to expose their position and cash-out eventually. Be patient and have the tools in place that will help you catch criminality as it happens, not tell you what has already happened.
- Understanding and pre-empting **crime trends** is critically important, so that agencies can direct their often limited resources to where there is the most criminality. Stay up to date on the latest crime typologies and learn how to think like a crypto thief.

- You're not investigating technology, **you're investigating people**. Technology is just a tool to help you tell a story of what happened. Don't feel daunted by the tools of the trade – the best ones are simple to use and are there to help you test your investigative theories.
- **Collaborate** with other law enforcement agencies nationally and around the world. Share information and build relationships with private sector participants. Cryptocurrencies are unconstrained by national borders and legal jurisdictions – no one organization holds all the knowledge.
- Keep up with the **growth in services** being developed both for illicit purposes, such as mixers, as well as those being developed for licit purposes. For example, as the crypto ecosystem develops, more services will become available for criminals to co opt and launder the proceeds of criminality – spanning terrorism financing through to CSAM and ransomware. Being ahead of those developments by leveraging solutions that identify those threats will help build a complete picture of exposure and increase your understanding.
- Keep up with the massive **growth in the number of assets** used by criminals to launder funds and subsequently, available to target for seizure and victim restitution. A Freedom of Information request submitted to all 45 UK Police Forces by *The Observer* newspaper in 2022 showed that out of the 27 that responded, seizures leapt from only two types of cryptoassets in 2019 to 22 in 2021. This pattern can also be observed when looking at the number of assets held in individual OFAC-listed wallets:

Number of Cryptoassets Possessed by OFAC-listed Wallets



Get in Touch With Us

We would love to learn more about you – and learn how we might be able to support your criminal investigations and intelligence gathering. Get in touch with our dedicated Government Solutions Team at government@elliptic.co to see a live demo of our tools or to start a trial.

See for yourself why many of the world's leading law enforcement agencies, tax authorities, regulators, financial intelligence units and central banks trust us to help them bring crypto criminals to justice at elliptic.co/law-enforcement.



Aruna Costa
VP Government Solutions



Arda Akartuna
Senior Crypto Threat Analyst



Thibaud Madelin
Research & Investigations Lead

About Elliptic

Solve more crime with powerful, practical blockchain intelligence.

Detect more illicit activity than you could before, with blockchain intelligence that makes it quicker and easier to investigate complex crypto crime. Founded in 2013, Elliptic pioneered the use of blockchain analytics to help public and private sector organizations fight crypto-related crime.

Go to elliptic.co/law-enforcement to find out more or contact us at government@elliptic.co.

Recognized as a WEF Technology Pioneer and backed by investors including J.P. Morgan, Wells Fargo Strategic Capital, SBI Group, and Santander Innoventures, Elliptic has assessed transactions worth several trillion dollars, uncovering activities related to money laundering, terrorist fundraising, fraud, and other financial crimes. Elliptic is headquartered in London with offices in New York, Singapore, and Tokyo.

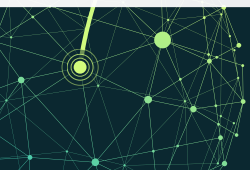
Between editions of this report, you will find the latest insights and trends around money laundering using cryptoassets on Elliptic Connect elliptic.co/connect

Research and Insights by Elliptic

ELLIPTIC CROSS-CHAIN REPORT 2022

The state of cross-chain crime


Countering the new age of crypto crime and money laundering in a cross-chain world



ELLIPTIC

Webinar

How to catch a crypto thief



Gary Alford
Special Agent
IRS Criminal Investigation

Liz Shetret
Director of Bank Policy & Regulation
FDIC

James Smith
Founder
Elliptic

Ardis Akotuna
Crypto Threat Analyst
Elliptic

What you don't know can give crypto criminals an advantage. Join our webinar with Special Agent Gary Alford – IRS Criminal Investigation – to find out the new ways bad actors are evading detection on the blockchain.


Watch on-demand →

ELLIPTIC

ELLIPTIC NFT REPORT 2022 EDITION

NFTs and Financial Crime

Money Laundering, Market Manipulation, Scams & Sanctions Risks in Non-Fungible Tokens




ELLIPTIC

ELLIPTIC BRIEFING NOTES | 2022

Tornado Cash Alternatives

The protocols competing for the Tornado Cash user base



ELLIPTIC