The Dark Side of Crypto and Web3: Money Laundering*

Lin William Cong† Kim Grauer‡ Daniel Rabetti§ Henry Updegrave¶

First Draft: August 2022; This Draft: February 2023

Abstract

Money laundering is a critical component of criminal activity, allowing criminals to access and protect the proceeds of their illegal activities. In the cryptocurrency world, money laundering is primarily focused on converting cryptocurrency to cash through centralized cryptocurrency exchanges, P2P exchanges, or over-the-counter trading desks. However, not all cryptocurrency-to-fiat (C2F) services implement effective anti-money laundering measures, and criminals use various techniques such as cryptocurrency mixers to hide the origin of their funds. Law enforcement has increased its efforts to crack down on C2F services that facilitate money laundering and trace the flow of funds from criminal addresses to C2F services through blockchain forensics. Despite these efforts, money laundering remains a significant challenge for law enforcement in the cryptocurrency ecosystem.

JEL classification: G15, G18, G29, K29, K42, M41, O16..

Keywords: Cryptocurrencies, Cyber Crime, Terrorist Financing, Money Laundering, Tax Evasion, Wash Trades.

*We are especially grateful to conference and seminar participants at the Interdisciplinary Challenges in Financial Data Science Conference, Pan-Asian Digital-Economy Meeting, Federal Reserve Cyber Monitoring Community of Interest Conference, The Economic Club of Memphis, European Securities and Markets Authority, Israel Money Laundering Authority Conference, University of Zurich (UZH) Blockchain Center, USAO-N.D. Cal. / U.S. DOJ Fraud Section / National Cryptocurrency Enforcement Team Cryptocurrency Fraud Seminar, and the US Treasury's Symposium on the Implications of Financial Technology for Banking for the insightful comments. Valerie Charlotte Hanke, Sanya Kohli and Mahitha Penmetsa provided excellent research assistance. The authors acknowledge FinTech@Cornell, DEFT Lab, and Ripple's University Blockchain Research Initiative for research support.

†Cornell University and NBER. Email: will.cong@cornell.edu.

‡Chainalysis. Email: grauer@chainalysis.com.

§Tel Aviv University and FinTech at Cornell Initiative. Email: rabetti@mail.tau.ac.il.

¶Chainalysis. Email: henry.updegrave@chainalysis.com.

1 Overview

Most criminals want to ensure that they can move, protect, and access the money made from their illegal activities — otherwise, what is the point of committing crimes in the first place? That is why money laundering is a crucial part of any criminal ecosystem. It enables all other forms of cryptocurrency-based crime that we discuss in this book, as well as offline criminal activity that incorporates cryptocurrency, such as the use of crypto for conventional drug trafficking transactions. Money laundering ties everything together.

In the world of cryptocurrency, money laundering is all about moving cryptocurrency services offering crypto-to-fiat (C2F) off-ramps so that the crypto can be converted to cash. Most off-ramping services are centralized cryptocurrency exchanges, but they can also include P2P exchanges or over-the-counter (OTC) trading desks. Other researchers have also pointed to more complex forms of crypto-based money laundering, such as using criminal funds to set up blockchain-based web3 services, which can generate "clean" money — a new twist on the classic "front business" form of money laundering.[1] However, we'll primarily focus our research here on the funneling of funds from addresses associated with crime to C2F off-ramp services.

Similar to banks, cryptocurrency exchanges and other C2F services in most jurisdictions are required to implement anti-money laundering compliance measures, such as KYC and origin of funds procedures. However, not all C2F services implement these procedures effectively, and some even appear to purposely flout them, effectively acting as specialized money laundering services. Additionally, there are a variety of techniques and specialized services criminals can use to hide the origins of their funds to fool legitimate C2F services. Cryptocurrency mixers are a common example. Mixers are services that take crypto deposits from several users, blend them together, and return to each user an equivalent amount to what they put in, making it difficult to detect the funds' original source on the blockchain.

Extant literature examines crypto laundering in several aspects, including detection techniques (Yining, Suranga, Kanchana, Kensuke, and Aruna (2019) and Oad, Abdul, Askar, Munif, Bandar, and Chenglin (2021)), behavioral analysis (Kramer, Blokland, Kleemans, and Soudjin (2023)), exploratory analysis (Dupuis and Gleason (2020) and

[1] See https://www.crowdfundinsider.com/2023/01/201556-venture-based-money-laundering-in-web3-becoming-a-serious-threat-report/.

van Wegberg, Oerlemans, and van Deventer (2018)), and regulatory challenges (Bryans (2014), Campbell-Verduyn (2018), Comolli (2021), and Wronka (2022)). Money laundering activity in cryptocurrency is heavily concentrated in the handful of services that have proven either incapable of stopping illicit deposits or willing to provide money laundering services. In recent years, law enforcement has ramped up the fight against these services, utilizing sanctions and seizures to stop them from operating. In this chapter, we explore what money laundering looks like on the blockchain and some of the efforts law enforcement has taken in recent years to crack down.

2 Where do criminals move their cryptocurrency?

Most cryptocurrency transactions are public by default, which makes it much easier to research money laundering compared to the fiat world, where most transaction and account details are recorded in private records. Thanks to cryptocurrency's transparency, we can analyze the data to show where money laundering occurs by looking at addresses linked to criminal activity funds.

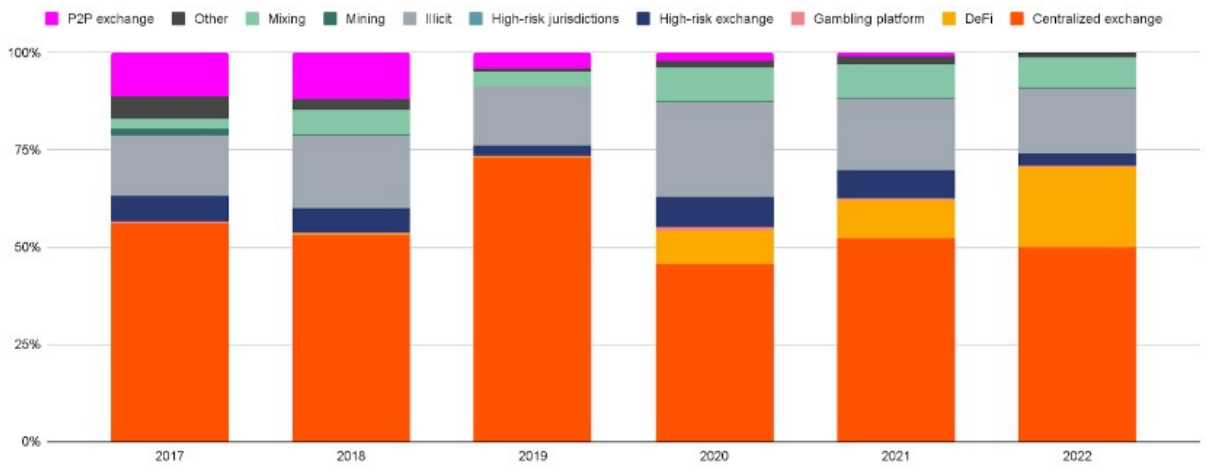

Figure 1. Destination of funds leaving illicit wallets, 2017 - 2022.

Overall, roughly half of the funds sent from illicit addresses went to the mainstream, centralized cryptocurrency exchanges. In recent years, DeFi protocols have become popular money laundering mechanisms, taking in 21% of all crypto sent by illicit addresses in 2022, up from 10% in 2021. 17% of the funds sent from illicit addresses went to other illicit services, such as darknet markets providing their own money laundering services in addition to

conventional products like drugs. Mixing services, which we will discuss in more detail later, received 8% of funds sent from illicit addresses.

If we get more granular, though, we can see that different types of cybercriminals favor different types of services for money laundering.

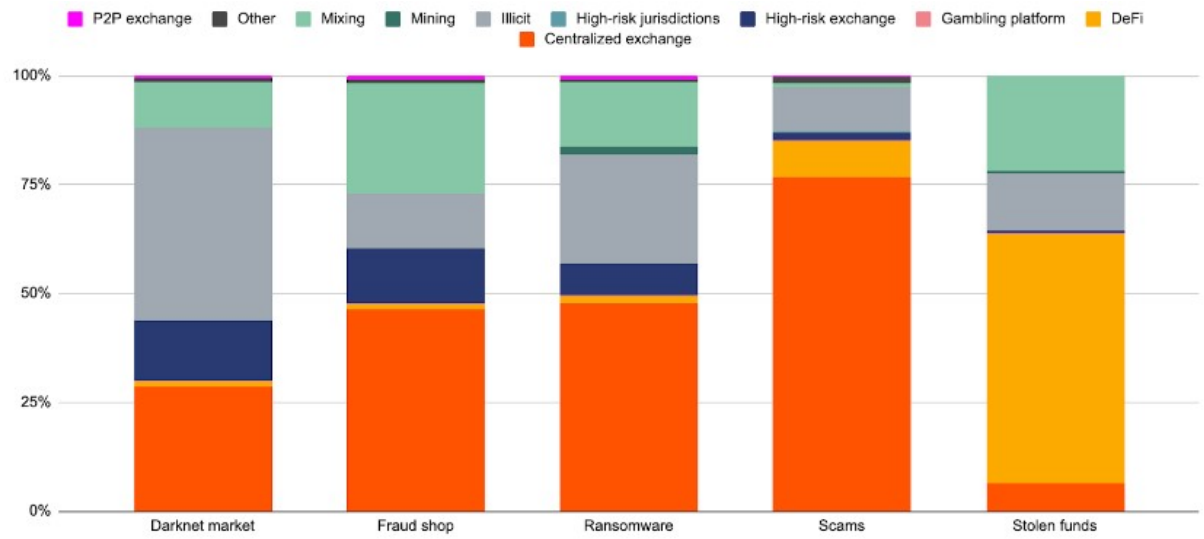

Figure 2. Destination of funds leaving illicit addresses by crime type, 2022.

For instance, cybercriminals who have stolen cryptocurrency send a disproportionately large share of funds to DeFi protocols compared to other types of crime. Fraud shop vendors, ransomware attackers, and especially scammers, on the other hand, favor centralized exchanges, with the former two also using mixers at a relatively high rate. Darknet market vendors, on the other hand, favor other illicit services for money laundering. It is important to remember, though, that not all of the service categories shown above allow for crypto to be converted to fiat currency. If we focus just on the C2F services that allow for fiat off-ramping — services that are crucial to criminals as they allow crypto to be moved into the traditional financial system — we see that concentration is even greater. We can see this in the graph below, which shows both the number of C2F services that received any illicit cryptocurrency in a given year alongside the share of all illicit funds that went to just the top five C2F services receiving the most illicit cryptocurrency.

In 2022, 915 C2F services received cryptocurrency from addresses linked to illicit activity. But just five of those services received 68% of those funds. In other words, if those five services implemented more effective compliance procedures or if law enforcement disrupted those five services, money laundering activity in 2022 would be reduced

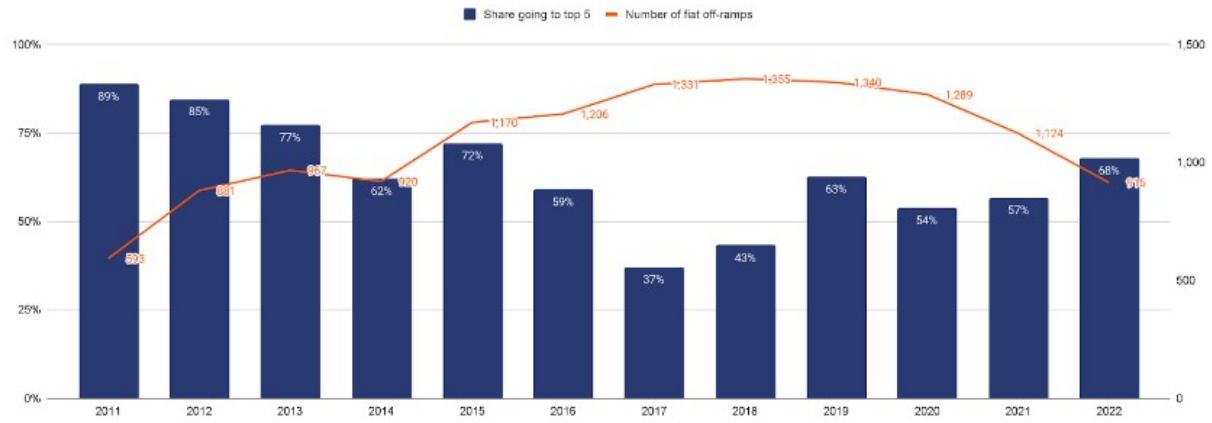

Figure 3. Share of illicit cryptocurrency moving to top five C2F services and total number of unique C2F services receiving illicit cryptocurrency, 2011—2022.

by more than half.

It is also valuable to analyze money laundering activity in terms of individual deposit addresses at C2F services. In this context, think of the deposit addresses as analogous to bank accounts, with the C2F services themselves being the banks. In the graph below, we look at all C2F service deposit addresses that received any illicit funds in 2022, broken down by the range of illicit funds received.

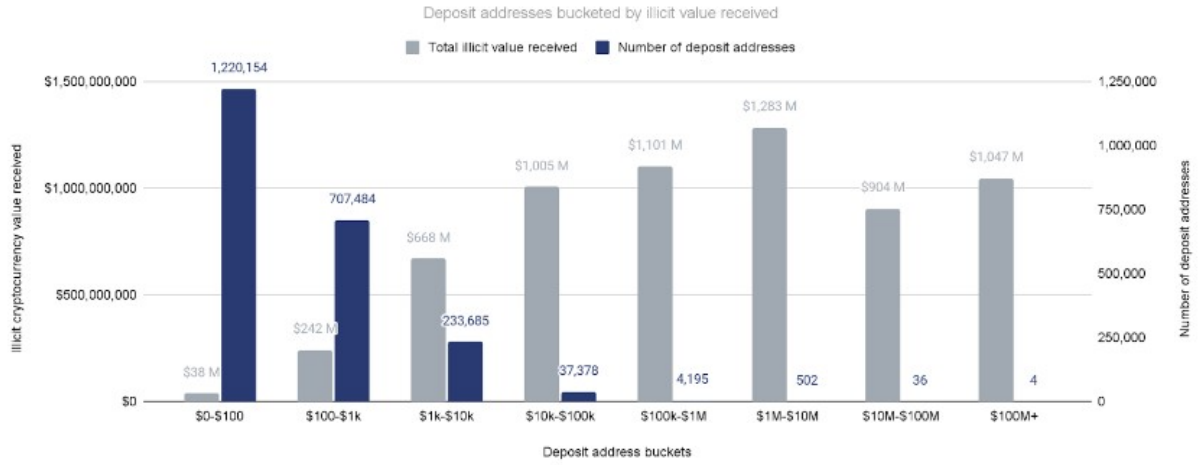

Figure 4. All illicit cryptocurrency received by C2F service deposit addresses, 2022.

Figure 4 shows service deposit addresses bucketed by how much total illicit cryptocurrency each address received individually in 2022. Each blue bar represents the number of deposit addresses in the bucket, while each grey bar represents the total illicit cryptocurrency value received by all deposit addresses in the bucket. Using the first bucket

as an example, we see that 1,220,154 deposit addresses received between $0 and $100 worth of illicit cryptocurrency, and together all of those deposit addresses received a total of $38 million worth of illicit cryptocurrency.

It can be seen from the figure that four deposit addresses at C2F services received over $100 million worth of cryptocurrency from illicit addresses in 2022. Taken together, those four deposit addresses received just over $1 billion worth of illicit cryptocurrency or 17% of the total sent from illicit addresses to C2F services in 2022. That is an astounding level of concentration! If we add in the next bucket of deposit addresses that received between $10 million and $100 million from illicit addresses, we find that the top 40 deposit addresses used for money laundering account for 31% of all illicit funds sent to fiat off-ramps in 2022, while the top 542 accounts for over half.

Who are the prolific money launderers behind the biggest money laundering deposit addresses? Only the exchanges hosting those deposit addresses could know for sure, though it is, of course, possible that the owners of those addresses provided false identity documents when creating their accounts. However, it is very likely that many of those deposit addresses are associated with nested services. Nested services are cryptocurrency businesses that run their operations on deposit addresses hosted by a larger service, usually exchange. This allows the nested service to tap into the liquidity and trading pairs offered by that exchange and also gives the nested service a secure place to store its cryptocurrency. OTC brokers especially often operate as nested services, and given the huge sums of money being handled by these 187 prolific money laundering deposit addresses, it is quite likely that many of them belong to an OTC broker. But we cannot say for sure, nor can we say how many individual OTC brokers or nested services account for these addresses. But what we can say is that if law enforcement or the compliance addresses at the services hosting these deposit addresses were to crack down on their activity, the crypto money laundering ecosystem as a whole would be severely hampered.

Luckily, this already appears to be happening. In 2021, the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) sanctioned two of the worst-offending money laundering services - Suex[2] (an OTC operating as a nested service) and Chatex[3] (a P2P exchange) - for accepting funds from ransomware operators, scammers, and other cybercriminals. In 2022, OFAC followed up by sanctioning Garantex[4], a Russia-based exchange found to have received cryptocurrency from a similar array of cybercriminals. More recently, January 2023 saw the shutdown of

[2]https://blog.chainalysis.com/reports/ofac-sanction-suex-september-2021/.
[3]https://blog.chainalysis.com/reports/ofac-sanction-chatex-revil-sodinokibi-november-2021/.
[4]https://www.techtarget.com/searchsecurity/news/252515668/US-sanctions-Garantex-for-laundering-over-100M.

Russia-based exchange Bitzlato, which according to Chainalysis data, received more than $646 million from illicit crypto addresses since 2019 — more than a quarter of its total value received. Bitzlato's founder was arrested as part of this law enforcement action, and while OFAC did not sanction the exchange, it was designated as a primary money laundering concern by the U.S. Treasury's Financial Crimes Enforcement Network (FinCEN), which prohibits U.S. firms from doing business with Bitzlato in a similar manner to an all-out sanctions designation.

3 Cryptocurrency mixers and their role in money laundering

As mentioned earlier, mixers are crucial to the cryptocurrency money laundering ecosystem. While they do not allow funds to be converted into fiat, mixers are important because they allow criminals to mitigate the default transparency of the blockchain and obscure the original source of cryptocurrency. Mixers do this by pooling together the funds of multiple users, mixing them up, and sending the funds to new addresses. Each user ends up with the equivalent amount of cryptocurrency they initially put in, except now, that cryptocurrency can only be traced on-chain to the mixer itself. That means the funds can then potentially be moved to a C2F service without raising alarm bells, though, of course, many services have compliance processes for dealing with funds sent from mixers, given their potential for criminality.

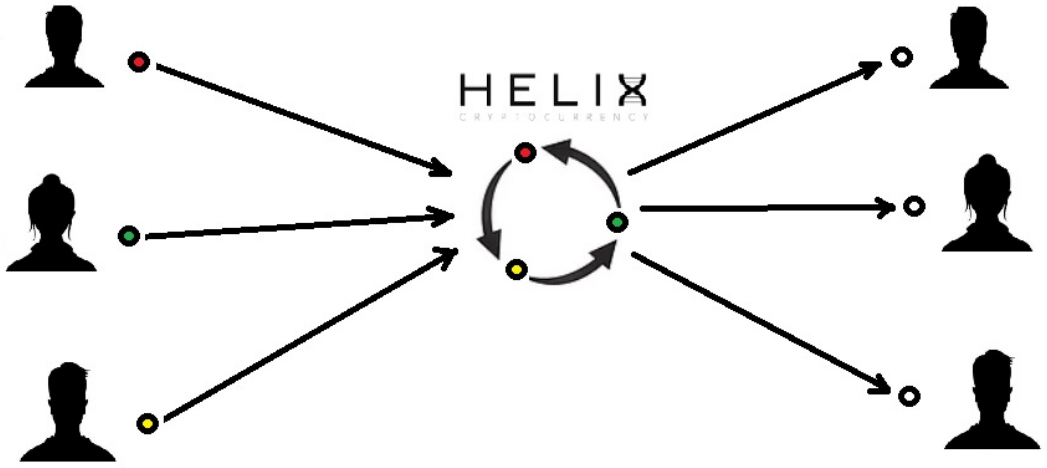

Figure 5. Mixer schematics.

It is important to remember that crypto mixers are not inherently criminal. Many people use mixers to preserve their financial privacy while using cryptocurrency. This is not entirely unreasonable — due to the transparency of blockchains, the entire record of a user's transactions is visible to anyone who knows that user's address. Somebody being paid for freelance coding work in cryptocurrency may opt to use a mixer so that their employer cannot find their wallet and see how much money they have. Still, mixers' enhanced privacy has made them attractive to cybercriminals, with roughly 10% of all funds sent to mixers in 2022 coming from illicit addresses.

4 How different types of cryptocurrency mixers work

Most mixers function according to the basic model outlined above, but different types achieve that function differently. Below is a rundown of the three most prevalent types of mixers and how they work.

- Centralized custodial mixers. Centralized custodial mixers temporarily take custody of users' funds before distributing them back to users. Though they can obscure the origin and destination of funds on the blockchain, users face privacy risks because the service operator may keep records of the details of each transaction. From a criminal's perspective, their transactions could be de-anonymized if police seize the service;
- **CoinJoins.** A CoinJoin is a process that essentially compresses the mixing process into a single, multi-party transaction. Many privacy-focused wallets offer CoinJoins as a built-in functionality and are non-custodial, meaning a third party never holds the user's cryptocurrency during the mixing process;
- **Smart contract mixers.** Smart contract mixers are also non-custodial, similar to CoinJoin wallets, but are different because their mixing process takes place over multiple transactions governed by a smart contract.[5] Smart contract mixers can only be used to mix cryptocurrencies on blockchains that support smart contracts, such as Ethereum and BNB Chain, but not, for example, Bitcoin. Smart contracts are self-executing and run on code hosted on distributed blockchains rather than centralized servers, meaning they can run perpetually without outside intervention or maintenance, making them impossible to shut down completely.

[5]https://www.coinbase.com/learn/crypto-basics/what-is-a-smart-contract.

We expect privacy-focused cryptocurrency developers to continue iterating and building new mixers more resilient to current investigative techniques and centralized, single points of failure.

5 Case study: The Tornado Cash situation—sanctioning a smart contract mixer

In August 2022, OFAC made waves when it sanctioned Tornado Cash, an extremely popular smart contract mixer built on the Ethereum blockchain. OFAC sanctioned the mixer due to its role in laundering cryptocurrency stolen by North Korea-affiliated hacking organization Lazarus Group, including U.S. $455 million stolen from Axie Infinity's Ronin Bridge protocol earlier in the year.[6] However, while Tornado Cash was sanctioned, its smart contract build can never be shut down. This has made the mixer a serious ongoing compliance risk for cryptocurrency services.

Tornado Cash is sophisticated and designed for maximum privacy. Users send the funds they want to mix to the Tornado Cash smart contract and receive a cryptographic note they can use to withdraw their mixed funds to a new address by sending a second transaction that references their note. Users can wait as long as they want to use their notes and receive their mixed funds after sending them to Tornado Cash. The mixer even has a mechanism for providing "clean" Ethereum to the user's withdrawal address so that they can pay any necessary gas fees without exposing it to another address they own.

Soon after OFAC's designation, the world received a real-time lesson in the difficulties of sanctioning a smart contract-based service, as several users began maliciously sending funds from Tornado Cash to addresses belonging to celebrities like Jimmy Fallon and Shaquille O'Neal, and crypto industry notables like Coinbase CEO Brian Armstrong and Andreessen Horowitz venture capitalist Ben Horowitz.

It is not just trolling — Tornado Cash continues to see significant usage even after being sanctioned, albeit at much lower levels than before the designation. The Tornado Cash situation exemplifies the difficulties in combating cryptocurrency-based money laundering involving distributed services that cannot be shut down like centralized services. Regulators will need to grapple with these difficulties as the DeFi ecosystem continues to grow and privacy

[6] https://coingeek.com/axie-infinity-ronin-bridge-hacked-for-over-600m-in-eth-and-usdc/.

Figure 6. Credit: @josephdelong on Twitter.

enhancements improve.

6 Underground money laundering services offer bespoke, mixer-like services to small networks of cybercriminals

In addition to popular, public-facing mixers like Tornado Cash, we have also recently observed the growth of underground money laundering services. These services behave similarly to mixers in that they obfuscate cryptocurrency transfers on behalf of cybercriminals looking to move funds to exchanges where they can be traded for cash. However, unlike those mixers, these services are typically only accessible through private messaging apps or anonymous web browsers like Tor, and are only advertised through darknet forums or even word of mouth.

These underground money laundering services can also vary greatly in their on-chain infrastructure and in many cases, differ significantly from standard mixers. Some function as networks of private wallets shuffling funds around, while others behave as instant exchangers and provide liquidity for users to swap funds on new blockchains. Some

do actually mix and re-distribute funds like a standard mixer, and some fall somewhere in between the models we've described. But generally, what links these services is that they act as an intermediary between cyber criminals and cryptocurrency exchanges and either facilitate cybercriminals' movement of funds to exchanges or move funds there themselves on cybercriminals' behalf and return clean cryptocurrency or fiat currency to the cybercriminal. Like the nested OTC services we discussed, many underground laundering services also source liquidity from exchanges.

We can see one example of an underground money laundering service on the Chainalysis Reactor graph below, with the names of the cybercriminal organization and exchange in question removed.

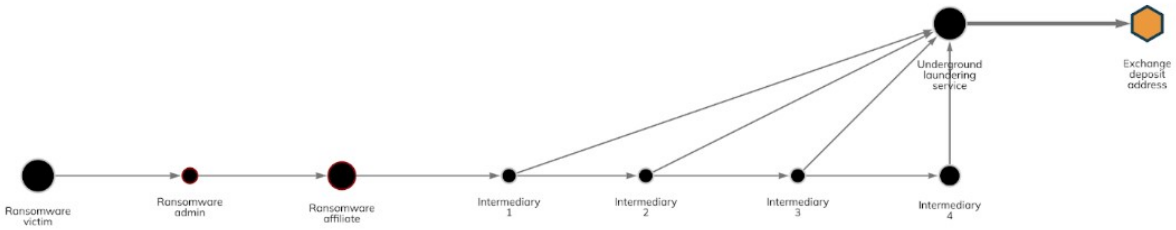

Figure 7. Underground money laundering service on the Chainalysis Reactor.

In this case, the underground laundering service functions similarly to a mixer and helped an affiliate for a large ransomware strain move funds to a deposit address at a centralized exchange. That deposit address is believed to be controlled by the laundering service itself.

Underground money laundering services are difficult to identify from on-chain activity alone, and identifying their addresses often requires extensive investigation and blockchain analysis techniques. That means it's difficult to definitively measure underground laundering services' activity at scale. However, we can estimate their activity by measuring the transaction volume of all wallets and networks of wallets that meet the following criteria:

- They've received large amounts of cryptocurrency from illicit services;
- They send large amounts of cryptocurrency to exchanges, allowing users to off-ramp into fiat currency.

The graph below shows the yearly cryptocurrency value received by wallets that fit those criteria.

Total cryptocurrency moving to wallets that fit our underground laundering heuristic has grown in the last four years, hitting $6 billion in 2022. Their growth may result from law enforcement action against larger services facilitating money laundering, such as the shutdowns of rogue exchanges like Garantex and Bitzlato, which may force

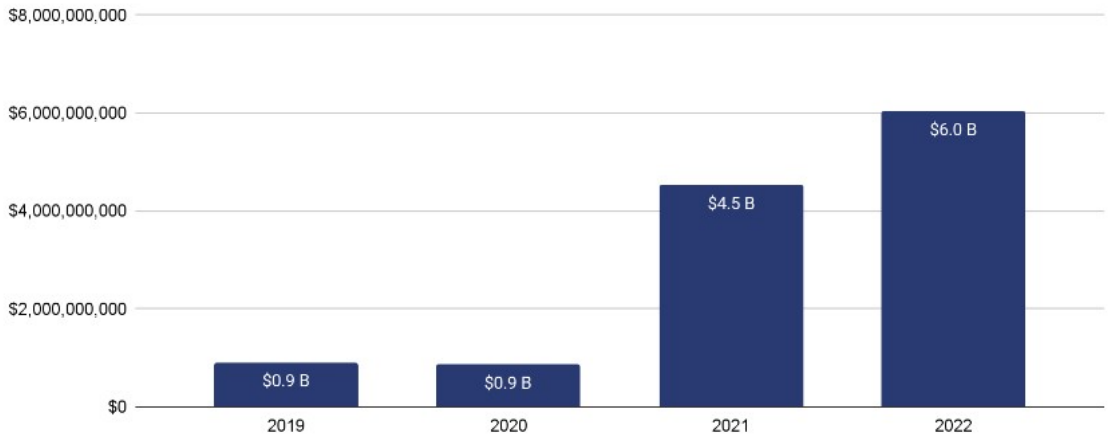

Figure 8. Total illicit value moving to suspected underground laundering services, 2019 – 2022.

cybercriminals to turn to smaller, harder-to-spot underground services.[7]

7 Case study: UK-Australia drug ring shows how criminals can use cryptocurrency to launder proceeds of traditional, offline crime

The money laundering figures we share in this chapter are all based on crime we can describe as "cryptocurrency native," meaning crime whose proceeds are derived in cryptocurrency, such as drug sales via darknet markets or crypto scams. We estimate money laundering activity by measuring transactions involving thousands of on-chain entities we have affirmatively identified as belonging to specific criminal groups or organizations. However, these measurements do not account for cryptocurrency usage to facilitate transactions and money laundering linked to traditional, offline forms of crime whose initial proceeds are in fiat currency, such as traditional drug trafficking.

While we cannot measure crypto-based money laundering of funds linked to traditional crime at scale the way we do the cryptocurrency-native crime, we know that many organized crime groups (OCGs) are laundering funds in this way. Below, we will share an example of how one drug trafficking OCG operated in the UK and Australia and

[7] See https://blog.chainalysis.com/reports/hydra-garantex-ofac-sanctions-russia/ and https://blog.chainalysis.com/reports/us-authorities-shut-down-high-risk-exchange-bitzlato/.

cryptocurrency to facilitate and conceal drug sales until it got busted.

7.1 How the Harrod's drug trafficking ring used cryptocurrency

In 2019, police arrested several members of a drug trafficking ring operating in the UK and Australia. The traffickers in this case had an unusual modus operandi for smuggling drugs: They would insert packers of cocaine into items at the department store Harrod's, then purchase them and have unwitting staff shop the items to addresses in Australia, where co-conspirators could collect them.

While that shipping method is interesting, our focus is on how the group used cryptocurrency to send money overseas to drug suppliers. Harrod's ring followed a common strategy that many criminal enterprises use:

1. The organized crime group (OCG) contacts a controller who is in charge of a money laundering operation and tells the controller how much illicit cash they need to move, the counterparty receiving it, and where that counterparty is located. In this case, Harrod's ring was the OCG and the counterparty was the drug supplier;
2. The controller will then contact a coordinator they work with whose job is to ensure the money gets to the counterparty;
3. The OCG will text a picture of a bill to the controller with the serial number visible. The controller will pass this image on to the coordinator, who passes it to the collector tasked with physically receiving the cash;
4. Through the controller, the coordinator will communicate to the OCG the location where the cash will be handed off. The two parties will share other details, such as the make and model of the vehicles the individuals making the exchange will be driving. This is done to limit the risk of the meeting being infiltrated by police;
5. The OCG will then pass the bill from the picture in step 4, along with the full amount of cash to be transferred, to a courier. The courier then meets the collector at the designated place and time;
6. Upon meeting, the courier will pass the bill from the picture to the collector. The collector then checks to make sure the serial number matches the one in the picture he received. The transaction will not take place if they do not match. This is done to ensure to the collector that the courier, whom he has never met, is the correct person;

7. If the serial numbers match, the courier will hand the full amount of cash to be transferred to the collector;

8. The collector will communicate to the controller that the cash has been handed over. At that point, the controller conducts a value transfer process, whereby money is transferred electronically to a coordinator in the OCG counterparty's location. Traditionally, electronic transfer is done through banks or traditional money services businesses (MSBs);

9. The controller and new coordinator then arrange for the same process described in steps 1-7 to be conducted in reverse in the OCG counterparty's location so that the counterparty receives an equivalent amount of cash — importantly, not the same cash handed over in the OCG's location.

We have condensed these steps in the diagram below:

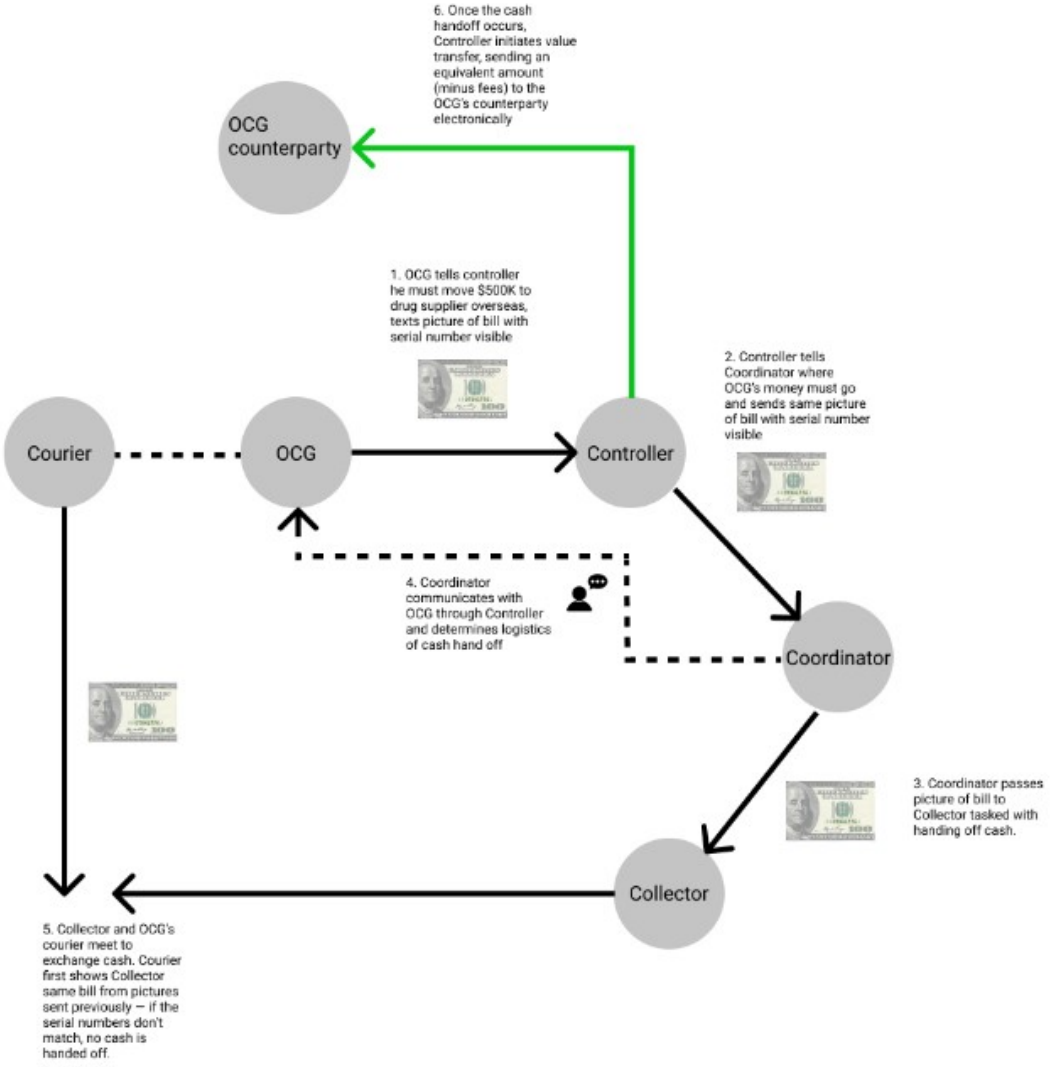

Figure 9. OCG drug trafficking ring cryptocurrency movement

The Harrod's drug ring followed this exact process, but with one twist: the value transfer process was conducted using cryptocurrency transactions rather than bank or MSB transfers. More specifically, the collectors were responsible for carrying out cryptocurrency transactions. Police tracking Harrod's drug ring's activity arrested one of these collectors after a cash handover, recovered the cash, and discovered evidence on his person identifying bill serial numbers described above, as well as a list of several Bitcoin addresses. Below is a Reactor graph showing some of the collector's Bitcoin transactions related to the money laundering ring's activity.

The coordinator on the UK side of the operation fled following the collector's arrest, but returned several months

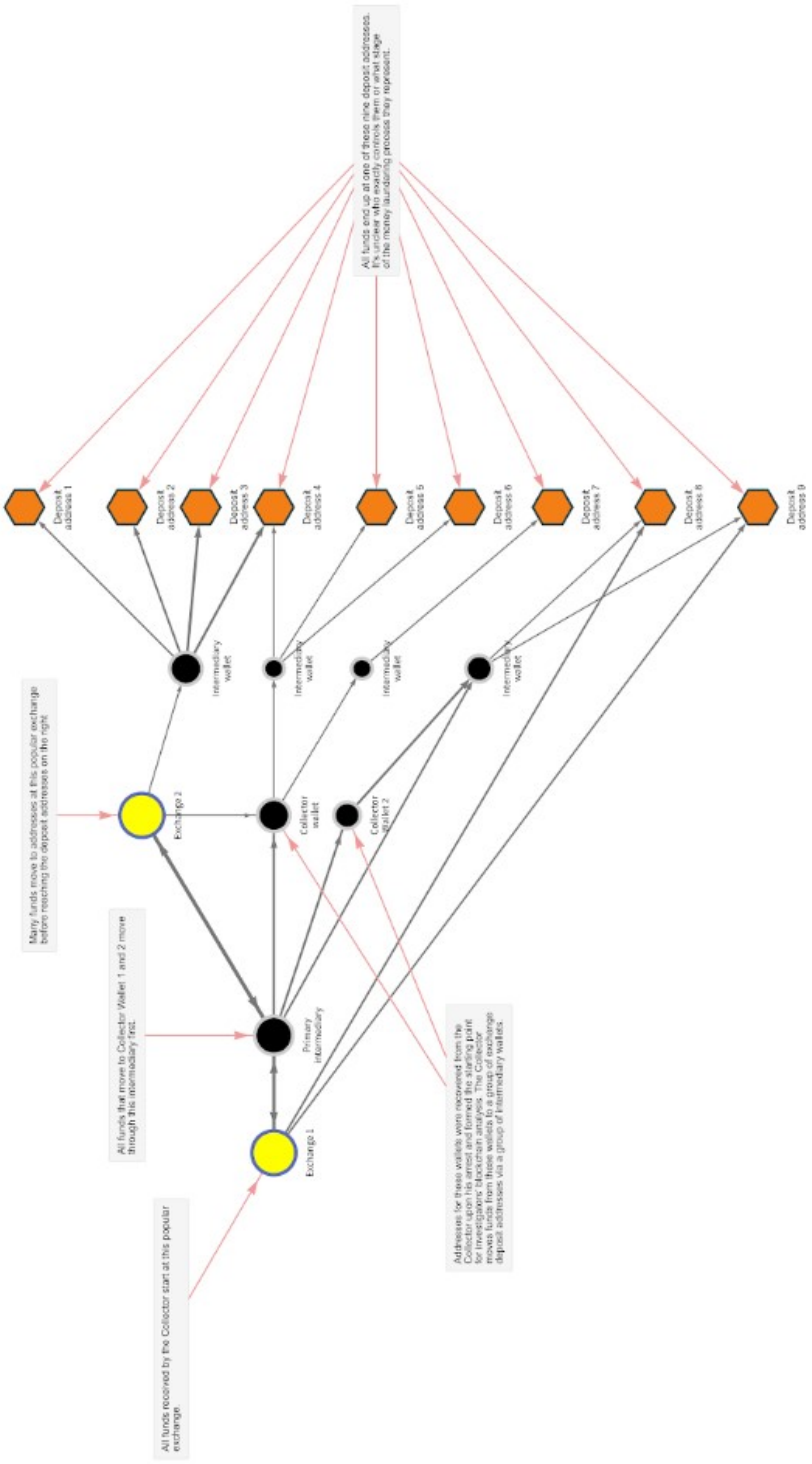

Figure 10. Tracking some of the collector's Bitcoin transactions related to the money laundering ring's activity.

later and was then arrested. Police recovered from him a hardware cryptocurrency wallet, whose transaction history showed £8 million worth of cryptocurrency being moved to a popular exchange within a six-month period. Because

these funds entered the cryptocurrency ecosystem as fiat currency, blockchain analysis alone would never allow an investigator or compliance officer to identify them as risky.

The Harrod's ring shows how OCGs not traditionally thought of as linked to cryptocurrency have embraced the technology as a means of money laundering. That means that any law enforcement agencies investigating these groups, and not just those responsible for cybercrime investigations, must become proficient in blockchain analysis and crypto investigations in order to do their jobs as effectively as possible.

References

Bryans, D. (2014). Bitcoin and money laundering: Mining for an effective solution. *Indiana Law Journal 89*, 441–472.

Campbell-Verduyn, M. (2018). Bitcoin, crypto-coins, and global anti-money laundering governance. *Crime, Law, and Social Change 69*, 283–305.

Comolli, Alexandra D.; Korver, M. R. (2021). Surfing the first wave of cryptocurrency money laundering. *Journal of Federal Law and Practice 69*, 183–236.

Dupuis, D. and K. Gleason (2020). Money laundering with cryptocurrency: open doors and the regulatory dialectic. *Journal of Financial Crime 28*, 60–74.

Kramer, J. A., A. A. J. Blokland, E. R. Kleemans, and M. R. J. Soudjin (2023). Money laundering as a service: Investigating business-like behavior in money laundering networks in the netherlands. *Trend in Organized Crime*.

Oad, A., R. Abdul, T. Askar, A. Munif, A. Bandar, and Z. Chenglin (2021). Blockchain-enabled transaction scanning method for money laundering detection. *Electronics 10*(15), 1766.

van Wegberg, R., J. J. Oerlemans, and O. van Deventer (2018). Money laundering with cryptocurrency: Open doors and the regulatory dialectic. *Journal of Financial Crime 25*(2), 419–435.

Wronka, C. (2022). Anti-money laundering regimes: a comparison between germany, switzerland and the uk with a focus on the crypto business. *Journal of Money Laundering Control 25*(3), 656–670.

Yining, H., S. Suranga, T. Kanchana, F. Kensuke, and S. Aruna (2019). Characterizing and detecting money laundering activities on the bitcoin network. *Computer Science*.