Trends in Organized Crime
https://doi.org/10.1007/s12117-023-09505-1

From payday to payoff: Exploring the money laundering strategies of cybercriminals

Mirko Nazzari[1]

Accepted: 31 August 2023

Abstract

Cybercriminals are commonly assumed to engage in cybercrime for monetary rewards. Like traditional offenders, they must launder their illicit proceeds to obscure the permanent trails in online environments. The mainstream narrative argues that these offenders engage in complex money laundering schemes because of the use of new technologies. However, empirical research on the money laundering activities associated with cybercrime has been scarce. To address this knowledge gap, the present study analyzes money laundering transactions from 182 Bitcoin addresses belonging to 56 members of the Conti ransomware group using blockchain analysis. The results show that offenders are quite unsophisticated when laundering their illicit proceeds. Most of the addresses transact directly with an entity (52%) and concentrate 80% or more of the illicit proceeds in one singular service (69%). In terms of destinations, exchanges and dark web services are the preferred choices, being involved in 71% and 30% of the transactions respectively. Conversely, the use of mixers is more limited (8%). There are significant differences in money laundering strategies used by offenders based on the amounts of illicit proceeds to launder. Implications for research and policy are discussed.

Keywords Money laundering · Ransomware · Bitcoin · Cybercrime · Blockchain

Introduction

Cybercrime has emerged as a major concern for national governments and international bodies over the last decade (Lavorgna 2020). With the increasing reliance of modern society on technology and digital infrastructures, tackling cybercrime has quickly become a top priority in the political agendas worldwide (Nguyen and Luong 2021). Despite the lack of consensus around its definition, the term

✉ Mirko Nazzari
mirko.nazzari@unicatt.it

[1] Università Cattolica del Sacro Cuore and Transcrime, Largo Gemelli 1, 20123 Milan, Italy

Published online: 20 September 2023

cybercrime identifies a wide array of cyber-dependent (e.g., hacking) and cyber-enabled crimes (e.g., online drug trafficking) (Caneppele and da Silva 2022).

Most of the criminological research suggests that monetary gain is the primary driver for cybercriminals (Hutchings 2014; Kerstens and Jansen 2016; Lusthaus 2018; Paquet-Clouston and García 2022). Like all the other profit-oriented offenders, cybercriminals must solve the financial bottleneck posed by money laundering to enjoy the fruits of their crimes. In fact, they even face additional challenges compared to traditional offenders because they must obscure the digital trails that inevitably connect their proceeds to the victims (Leukfeldt, Kruisbergen, et al. 2019; Levi 2015; van Wegberg et al. 2018).

The mainstream narrative argues that cybercriminals "make extensive use of obfuscation techniques to anonymize their financial activities" (Europol 2023, p. 11). In particular, cybercriminals are often assumed to be high-skilled offenders who engage in complex money laundering schemes by exploiting opportunities offered by new technologies (e.g., cryptocurrencies) (Europol 2021; Richet 2013; Wronka 2022). However, these claims are based on weak premises. First, several scholars showed that most cybercriminals do not have an extensive technical knowledge (Collier et al. 2020; Gundur et al. 2021; Lusthaus 2018). Second, empirical research on how cybercriminals launder their illicit proceeds has been surprisingly scarce to date (Kruisbergen et al. 2019; van Wegberg et al. 2018). The present study aims at addressing this knowledge gap by answering the following research question: *How do cybercrime actors launder their illicit proceeds?* To do so, it provides empirical insights into how 56 members of the Conti ransomware group laundered their illicit proceeds by analyzing through blockchain analysis transactions from 182 Bitcoin (henceforth BTC) addresses where they received their wages.

The present study is structured as follows. The next section reviews previous empirical literature that investigated how cybercriminals launder their illicit proceeds. Section "Current Study" illustrates the data and methodology. Section "Results" presents the main results of the analysis. The last section discusses the results together with the methodological limitations, policy implications and directions for future research.

Empirical literature on the money laundering strategies of cybercriminals

New technologies have been assumed to be facilitation tools for money laundering since the late 90s (Haines and Johnstone 1999). Over the decades, such concern has led to the rise of the "cyber-laundering" concept in both academic and policy debates (Filipkowski 2008; Handa and Ansari 2022; Wronka 2022). However, most of the scholars only analyzed new forms and typologies of money laundering in digital environments from a theoretical point of view (Albrecht et al. 2019; Campbell-Verduyn 2018; Dupuis and Gleason 2020; Handa and Ansari 2022). Conversely, despite the profit-oriented nature of most cybercrimes, empirical research on how cybercriminals launder their illicit proceeds has been limited to date (Custers et al. 2019; Kruisbergen et al. 2019).

To the best of my knowledge, only a few studies empirically investigated the specific money laundering strategies of cybercriminals. McGuire (2018) carried out 100 interviews with convicted or active cybercriminals, further enriched with information stemming from other data sources (e.g., dark web forums, court documents). The results show that 15% of cybercriminals spent most of their illicit proceeds on covering immediate needs (e.g., paying bills), 20% purchased illicit goods and services (e.g., drugs), 15% purchased assets (e.g., properties) while 20% reinvested at least some of their revenues in further criminal activities. Of note, cybercriminals attempted to convert their illicit proceeds into cash in at least 30% of the cases.

Kruisbergen et al. (2019) analyzed 30 cases of organized crime groups to understand the use of IT to handle illicit proceeds and identify potential similarities and differences between traditional offenders and cybercriminals. The results showed major differences in terms of money laundering methods between the two groups of actors. In the cases of offline organized crime, offenders almost exclusively used traditional methods and did not use cryptocurrencies which, on the contrary, were a routine money laundering tool for cybercriminals. However, of note, both groups of actors showed a striking similarity in the preference for cash.

Paquet-Clouston et al. (2019a) analyzed victims' payments to 35 ransomware families. Overall, results showed that ransomware actors tend to consolidate their illicit proceeds into one or more key addresses. Out of 2,077 key addresses identified, 163 had additional contextual information: 86 (53%) were related to known exchanges, another 47 (29%) to gambling websites and 12 (7%) to mixing services. In another study, Paquet-Clouston et al. (2019b) analyzed the money laundering of illicit proceeds stemming from more than 4 million sextortion spam emails. Results show that offenders entirely moved the proceeds to other wallets on average after 5.5 days. Within two hops, several exchanges were identified but they only received 3.82 BTC (about 0.14% of the total estimated sextortion revenues), suggesting that spammers do not necessarily cash out within the first hops.

Custers et al. (2019) analyzed how the profits of banking malware are laundered, identifying two main models. The former involves the use of money mules to quickly cash out the illicit proceeds. The latter involves the direct spending of illicit proceeds via (a) purchases of products online; (b) purchases of BTC via exchanges; or (c) purchases of luxury goods. BTC can be further laundered via mixers (also known as tumblers) which are privacy-enhancing services that improve the anonymity of BTC transactions by mixing coins of different users, thus breaking the traceable link between sender and receiver. In a related project, Custers et al. (2020) focused on the laundering of profits of ransomware based on desk research, 20 semi-structured interviews with experts from law enforcement and anti-money laundering obliged entities and the analysis of 4 police files. Also in this case, two main laundering strategies have been identified based on the specific form of payments requested in the ransom, namely vouchers or cryptocurrencies. In the former case, vouchers are sold for cash or cryptocurrencies, often via advertisements on the dark web. In some instances, vouchers are not sold but directly spent online service provider or stores, where they can be directly exchanged for products or services. In the latter case, cryptocurrencies are laundered via mixers and then sent to other addresses of the cybercriminals where they

can be exchanged in fiat currency via exchanges or individual BTC traders as well as being directly spent.

Trozze et al. (2023) used blockchain analysis to analyze money laundering strategies used to launder illicit proceeds originating from 6 fraudulent projects in the Ethereum ecosystem. Ethereum is a decentralized blockchain platform that enables developers to build and deploy smart contracts and decentralized applications. Overall, results showed that scammers engaged in relatively unsophisticated money laundering schemes, ultimately moving their illicit proceeds to centralized exchangers where they were likely withdrawn in exchange for cash.

Notably, several contributions on money laundering in digital environments come from the computer science domain. Lee et al. (2019) extracted over 10 million BTC addresses from over 2,800 dark web domains. Overall, 85 BTC addresses were classified as illicit. In total, 64% of the illicit proceeds were sent to exchanges while the remaining was unspent. Moreover, about 84% of the addresses have transferred more than 50% of their illicit proceeds to only one service. Oosthoek et al. (2023) analyzed around 13,500 ransomware payments to 87 criminal actors, distinguishing between commodity ransomware and ransomware-as-a-service (RaaS). Overall, results showed that commodity actors do not exhibit a specific laundering strategy, while RaaS actors primarily use fraudulent exchanges and mixers to make more difficult the tracing of illicit proceeds. Wang et al. (2022) investigated the laundering strategies associated to 22,717 BTC addresses belonging to 63 ransomware families from 2012 to 2021. Overall, the results showed that offenders prefer sending their illicit proceeds to exchanges and investment services while the use of mixers is minimal. Lastly, several studies analyzed the functioning of mixers by directly transacting with these services in experimental designs (De Balthasar and Hernandez-Castro 2017; Moser et al. 2013; van Wegberg et al. 2018).

Overall, empirical evidence on money laundering strategies of cybercriminals is still scarce, motivating the "need for exploration of the ways that members of cybercriminals networks spend their criminal earnings" (Leukfeldt and Holt 2022, p. 3). Addressing this knowledge gap is essential from a criminological point of view for both research and policy purposes. First, we still know very little about how difficult offenders find to launder their illicit proceeds (Levi 2015). Improving our understanding of cybercriminals' money laundering strategies is essential to infer their aims, preferences, and constraints. Empirical evidence on the behaviors of these offenders is also essential to guide efforts to automatically detect money laundering transactions via cryptocurrency (see, for example, Vassallo et al. 2021). Second, understanding how money laundering risks distribute across different Virtual Asset Service Providers (henceforth VASPs) as well as how offenders exploit vulnerabilities in the cyberspace are essential to identify potential areas of intervention and develop risk-based controls that can target more effectively these activities. VASPs are any natural or legal persons that conduct as business one of the following activities for or on behalf of another natural or legal person (FATF 2021): (a) Exchange between virtual assets and fiat currencies; (b) Exchange between virtual assets and fiat currencies; (c) Transfers of virtual assets; (d) Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; (e) Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

Current study

The empirical data consists of 182 BTC addresses belonging to 56 members of Conti, one of the most dominant ransomware criminal groups worldwide in 2021. The Conti group proved to be a suitable case study for two main reasons. First, among the wide array of cyber threats, ransomware has rapidly surged to be the prime concern across the European Union (ENISA 2022). Ransomware is a type of cyberattack in which threat actors take control of a target's asset (e.g., personal computer) and demand a ransom in exchange for the return of the asset's availability and confidentiality. Nowadays, offenders demand ransomware payments almost exclusively in cryptocurrencies because they offer pseudo-anonymous and cross-border transactions without requiring a central trusted party. In this regard, the Financial Action Task Force (henceforth FATF) has recently published a report on the financial flows associated with ransomware, stressing the need to investigate the main money laundering strategies used by these cybercriminals (FATF 2023a).

Second, the Conti group suffered a data breach in February 2022 which revealed its internal workings.[1] Following Conti's declaration of support to the Russian invasion of Ukraine, a Ukrainian researcher leaked on the surface web, along the source code of the Conti ransomware encryptor, over 170,000 internal private chat logs of the group members between June 2020 and March 2022. These chat logs were allegedly obtained from the servers of the two open-source platforms used by Conti for internal communications, namely Jabber and Rocket.chat. In particular, the private chat logs used in the present study have been retrieved from the GitHub page of NorthWave Cyber Security, a Dutch cybersecurity company that translated the chat messages in English using the paid Google API.[2]

Members of the Conti ransomware group discussed several topics in their chat logs, including their job responsibilities and earnings. The reading of the chat logs in the leak led to the identification of the internal financial flows of the group. Members had to write to either the boss or other high-rank members to collect their wages, after pointing out the work done and the amount due. Wages were paid in BTC twice per month (on the 1st and the 15th) at the addresses provided by the members. Out of the 243 BTC addresses identified in the leak, I only included in the sample those that, according to the content of the chat logs, were provided by members to collect their wages (182 amounting to 75% of the total).[3] Conversely, addresses related to payments for internal expenses of the group (e.g., servers, VPNs) were excluded. While still involving illicit proceeds of the group, financial flows from these addresses do not constitute money laundering from an analytical point of view.

Although the scope of the present study does not allow for an in-depth analysis of how BTC functions, a brief overview is necessary to better understand the

[1] The leak has allegedly disrupted the activities of the Conti group.

[2] Data are public and can be easily retrieved online.

[3] All the BTC addresses were identified in the Jabber leak. Rocket.chat messages were read but did not include any BTC addresses.

methodology used to investigate the money laundering strategies of these actors. BTC is a peer-to-peer cryptocurrency initially introduced in 2008 that enables users to conduct pseudo-anonymous transactions without the intermediation of a trusted third-party. All executed transactions, after being confirmed by selected nodes of the network (the so-called miners), are included and stored in a distributed ledger, also known as blockchain. It consists of all executed transactions in the network, including their time, transferred amount, origin and destination addresses. Of note, the blockchain is publicly accessible, allowing anyone to view and download the transactional data.

A BTC transaction consists of a list of addresses as inputs and outputs. BTC addresses are alphanumeric strings (34–62 characters) mathematically derived from the public key of an asymmetric key pair. Every user can hold multiple key pairs (and therefore addresses) in a wallet. The fundamental units of the BTC transactions are the Unspent Transactions Outputs (UTXOs), which represent the unspent outputs of previous transactions that can be used as inputs in new transactions. Each input consists of a reference to a previous transaction output and each output represents an amount of BTC that is sent to a new address. In addition to preventing the double-spending of the same amount of BTC, UTXOs link transactions together and can be used to reconstruct the transactional chain between different BTC addresses. As a result, it is possible to represent the entire BTC network as a transaction graph with input/output addresses as nodes and the transactions as directed edges (See 2023).

Over the years, a number of heuristic algorithms (e.g., multiple-input heuristics, change heuristics) have been developed to trace BTC transactions and cluster together addresses presumably controlled by the same entity (Ahmed-Rengers et al. 2019; Kim et al. 2022). The multi-input heuristic (also known as co-spending heuristic) assumes that two BTC addresses used as inputs in the same transaction are controlled by the same real-world actor. Indeed, a valid BTC transaction needs to be signed using the private keys associated with all the inputs and this feature can be used as evidence of common ownership (Meiklejohn et al. 2013). However, this heuristic can fail and lead to false positives in the case of CoinJoin transactions. A CoinJoin transaction is an aggregated transaction in which multiple users combine their funds, so it is no longer the case that all inputs are controlled by the same entity.

Change heuristic builds on how BTC functions. A UTXO is a unit of BTC in a specific address that can be spent as an input in a new transaction. If the total amount being spent is greater than the value of a single UTXO, the excess amount must be returned to the sender via a change address (Zhang et al. 2020). Instead of sending the change back to the sender's address, BTC wallets create a new address to receive the change amount. As a result, the new change address can be clustered with input addresses as they have common ownership.

When clusters of BTC addresses are matched with attribution data from external sources (e.g., websites, forums), it is possible to identify the real-world entities which control them and deanonymize the transactions on the blockchain (also known as tagging). Over the years, several blockchain analytics tools have been developed to provide VASPs and law enforcement agencies with clustering and

tagging activities. Notably, scholars have also successfully used these tools to analyze criminal activities for research purposes (De Balthasar and Hernandez-Castro 2017; ElBahrawy et al. 2020; Oosthoek et al. 2023).

In the present study, I used the blockchain analytics tool developed by Scorechain to process the blockchain data. Scorechain is a Luxembourg-based blockchain analytics company that uses state-of-the-art heuristics, coupled with proprietary off-chain information collected from open-sources, to support more than 200 clients in 40 countries. Access to the tool was granted to the partners of the EU-funded project CTC – Cut the Cord which aims at preventing the abuse of new technologies for financing terrorist organizations.[4] The use of a proprietary tool was additionally motivated by the fact that it represents a more powerful option compared to alternative open-source tools, especially in the collection and validation of attribution data (see, for example, Trozze et al. 2023).

First, given a BTC address as an input, the tool provides a wide range of information, including the type of address, the amount in BTC received, their countervalue in USD dollars and the timestamp of the wage transaction. The countervalue in USD dollars was calculated using the BTC-USD closing rate on the day of the transaction. Because of the volatility of BTC, this measure only approximates the criminal earnings and does not represent what they may have potentially profited at the end of the laundering process.

Second, the tool allows to track the money flows originating from the BTC addresses in the sample using state-of-the-art heuristics. While analyzing the direct counterparties of the BTC addresses would have been the best approach, it is important to note that money laundering through cryptocurrencies often involves routing illicit proceeds through multiple intermediary non-service addresses (commonly referred to as "hops") before ultimately sending them to a service. Offenders can easily create multiple self-hosted wallets and related addresses within seconds, using them as obfuscating layers in transactions with both licit and illicit services.

Therefore, in addition to analyzing direct exposure, it is crucial to consider indirect exposure as well. However, given the pseudo-anonymity of transactions, determining if (and when) the funds change ownership across several hops can be challenging. For example, criminal actors may exchange BTC for cash in face-to-face meetings with brokers who provide these services in return for a fee. Unfortunately, a similar hand-over would be undetectable on the blockchain without supplementary (off-chain) information.

As a result, building on previous literature (Oosthoek et al. 2023; Paquet-Clouston et al. 2019b), the present study looks at services and entities involved in both direct and indirect transactions with the deposit addresses in the sample. In particular, the former set of transactions (direct exposure) involves entities to which offenders directly transferred their wages after obtaining them. The latter (indirect exposure) accounts for the services and entities that are reached, within a maximum depth level of 10, after a first direct transaction with non-service addresses. The maximum threshold of 10 transactions has been chosen based on previous literature (see, for example, Lee et al.

[4] More information on the project can be retrieved here.

2019). It is worth noting that a service is used as a "stopping point" in tracing illicit proceeds through blockchain analysis. Once received, the service itself may move the funds among its internal wallets for operational purposes, making the tracing meaningless from an analytical point of view because the offender is not responsible for those transactions.

The tool provides an automatic display of the total count and type of entities that have received funds from the input BTC address, both directly and indirectly. These transactional data have been extracted from the tool and used to manually compile the database. In particular, for each BTC address in the sample, a set of non-mutually exclusive binary variables recorded the presence (1) or absence (0) of transactions towards relevant services, namely: (a) Exchange; (b) Dark web service; (c) Payment service; (d) Gambling website; and (e) Mixing service.

In addition, results from the blockchain analysis have been coupled with a selection of chat logs from the data leak to add nuance and qualitative depth to the analysis. In terms of ethics, some precautions have been adopted. While chat logs used in the present study are now publicly available on the surface web, they were not intended for public access. The personal identities of the offenders involved are still secret and protected using pseudonyms. Therefore, data are only analyzed at the aggregated level without referring to a specific individual's behavior. Second, I avoided displaying the unique pseudonyms found in the chat log files. Lastly, I partially paraphrased the statements included in the present study to prevent them from being easily associated with offenders through automated text searches in the chat logs.

The present study makes significant contributions to previous literature. First, contrary to most of the previous studies in the money laundering domain that analyzed police files, the present study uses a unique ground-truth data source to collect information on money laundering transactions. While police files offer valuable insights into criminal activities, research solely based on such data may inadvertently mirror the scope and the resources of the law enforcement agencies that carried out the criminal investigations (Roks et al. 2022). This observation holds true even when investigating cybercrime (Leukfeldt et al. 2019b; Werner and Korsell 2016). The issue is further exacerbated when it comes to the detection of illicit proceeds because law enforcement agencies often do not prioritize money laundering during the criminal investigations but rather focus on proving the connection between the offender and the predicate offence (Gundur et al. 2021).

Second, all previous studies that analyzed money laundering related to ransomware focused on the addresses used for receiving victim's payments (Oosthoek et al. 2023; Paquet-Clouston et al. 2019a; Wang et al. 2022). While correct, this approach has one main drawback. By default, it attributes the money laundering strategies to the criminal group as a whole ignoring, for example, potential differences that may exist in the behaviors of individual members. However, criminological research has not demonstrated yet if money laundering decisions are taken at the leader level or left to the single members of the criminal group (Levi and Soudijn 2020). As a result, the present study looks at the individual behaviors to avoid generalizing about the criminal group as a whole and to consider the potential role of individuals' psychological preferences on their money laundering strategies.

Results

A total of 411 BTC (equal to $287,995.81 at the time of the transfers) was sent to the addresses in the sample between June 2020 and February 2022, with an average wage payment of $1,582.39 (median = $834.05). At the time of writing, the same amount of BTC is worth more than $11 million ($11.472.777,30).[5] 91% of the addresses belong to non-custodial wallets (also known as cold wallets), namely BTC wallets where users have the exclusive control over their own private keys which are directly stored on a device (e.g., laptop, mobile phone, dedicated USB support). Conversely, in custodial wallets (hot wallets), users rely on a trusted third party (e.g., exchange) to store the private keys on their behalf.

Over time, several BTC address formats have been developed to deal with BTC increased use by providing users with more advanced security, additional privacy, higher scalability, and lower transaction fees. At the time of writing, there are four main types of BTC addresses (from the oldest to the most recent one): Legacy, Script, SegWit and Taproot. 20% of BTC addresses in the sample are Legacy which use the standard hash function Pay-to-PubKey (P2PKH) and start with the prefix 1. 25% are Script addresses that use the hash function Pay-to-Script (P2SH) and start with the prefix 3. Lastly, the remaining (55%) are SegWit that use the hash function Pay-to-Witness-Public and always start with the prefix bc1q. No BTC address in the sample adopted the Taproot format which is the most recent and advanced one. Introduced at the end of 2021, taproot addresses use the hash function Pay-to-Taproot (P2TR) and start with the prefix bc1p.

Overall, the addresses in the sample had a total of 3,732 transactions (mean = 20.5). 82% of the addresses only had two transactions, showing that most of the offenders preferred creating a new address for receiving each wage. The balance of all the addresses is equal to zero, meaning that all the offenders have moved their wages entirely to other addresses. Of note, almost all the offenders (98%) started laundering their illicit proceeds in one single transaction without breaking down the funds in multiple transactions over time. The speed with which this happened can be inferred from the time between the wage payment and the outgoing transaction from the deposit address. Overall, the mean holding period in the deposit address amounted to little more than 3 days (3 days, 3 h and 51 min) after illicit proceeds being deposited.

Offenders tend not to diversify: 80% or more of the illicit proceeds have been sent to one singular service in 69% of the transactions. This percentage raises to 87% when lowering the threshold to 50% of the illicit proceeds. Figure 1 shows the frequency of the services involved in the outgoing transactions from the addresses. Exchanges are the most preferred destinations (71%), followed by dark web services (30%), payment services (14%) and gambling websites (13%). Only 8% of the addresses transacted with mixing services. Notably, there are significant differences in the money laundering strategies used by offenders based on the amount of illicit

[5] One BTC is equal to $27.914,30 (01/05/2023).

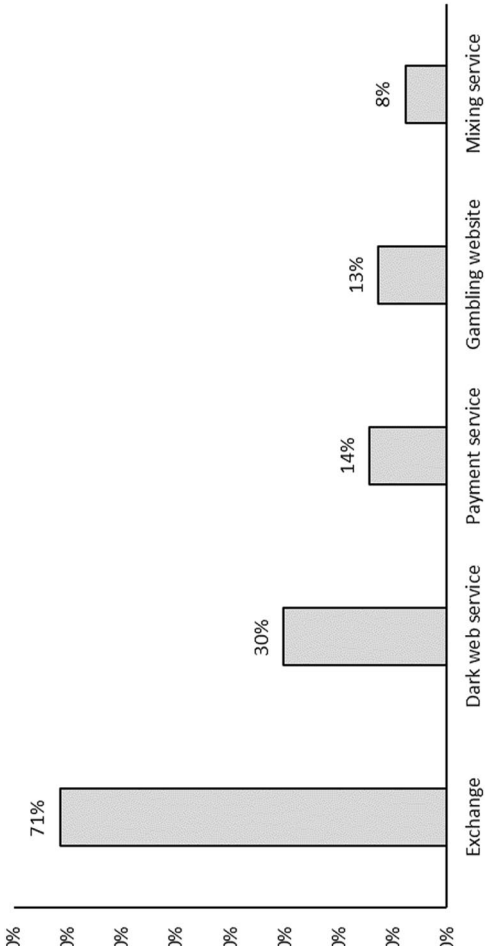

Fig. 1 Frequencies of services involved in money laundering transactions from BTC addresses in the sample ($N = 182$). *Note: Categories are not mutually exclusive*

proceeds that they must launder. Addresses receiving more than $1,000 are more likely to rely on mixers (26% vs 2%), dark web services (38% vs 27%) and payment services (21% vs 11%).

Most of the offenders (68%) transacted directly with an entity at least once. Of note, these offenders engaged consistently in direct transactions over time (74% of their transactions on average). Out of the 94 direct transactions, it was possible to identify the services involved in only 45 of them (48%). 62% of these transactions involved exchanges, followed by dark web services (18%), payment services and gambling websites (both 4%) and other entities (12%). While one would expect that offenders relied on high-risk services that do not perform any identity checks and are not likely to respond adequately to law enforcement subpoenas, this seems not to be the case. For example, high-risk exchanges were involved only in 20% of the transactions with exchanges.

Discussion, policy implications and limitations

Results show that offenders used good operational security practices when collecting their illicit wages. First, 91% of the addresses belong to non-custodial wallets which are not subject to typical compliance standards and are directly under the user's control. Conversely, custodial wallets rely on a third-party to store users' private keys. In addition to requiring a great level of trust from the user, services that host the wallets can also freeze funds in case of a motivated law enforcement request.

Second, most of the addresses (53%) adopt the SegWit standard. In addition to offering lower transaction fees, these addresses also have supplementary security features compared to Legacy and Script addresses. In particular, they contain only a single public key hash because users must provide proof of ownership of the corresponding private key to process transactions. This feature offers additional security and privacy as less data needs to be exchanged between different users. However, this additional security may come at the expense of the efficiency of the laundering process because several exchanges and wallet providers do not allow sending BTC to this type of address yet.

Third, 83% of the addresses had only two transactions (one incoming and one outgoing) with offenders receiving their illicit wages and moving them out entirely. This behavior is in line with the actual BTC design as "reuse of bitcoin addresses should be considered a deadly sin" (van Wegberg 2020, p. 77). Address reuse is the practice of receiving more than one transaction to a single BTC address. While being convenient, it is problematic because it reveals sensitive information about the users, such as the total amount of BTC they possess and the entities they transact with.

However, despite a visible preference for security over usability and convenience, cybercriminals tend to be surprisingly unsophisticated when it comes to money laundering, a characteristic that has been widely acknowledged among offline offenders as well (Berry and Gundur 2021; Levi and Soudijn 2020; Matanky-Becker and Cockbain 2021). While illicit proceeds are moved out from the deposit addresses quickly and in full, most of the addresses (52%) transact directly with an entity. This habit is highly insecure because it does not add any obfuscation layers between the illicit proceeds

and their criminal origin. Moreover, most of the offenders (73%), even when using multiple services, routed 80% of their illicit proceeds or more to one singular service. Such behavior inevitably requires a significant level of trust in these services, at least not to disclose their identities in case of law enforcement investigations.

For what concerns the typology of destinations, exchanges and dark web services are the most common services in terms of frequency (71% and 30% respectively). Offenders may use exchanges to convert illicit proceeds from BTC to other cryptocurrencies (the so-called chain-hopping) or in fiat currency that can be then rapidly transferred to bank accounts via wire transfers and withdrawn in cash (Moiseienko and Kraft 2018). As already pointed out by several studies (Kruisbergen et al. 2019; McGuire 2018; Soudijn 2019), cash is still king even for cybercriminals. It is a bearer negotiable instrument that guarantees anonymity and provides no information on its origin or its ultimate beneficiary, thus facilitating the laundering process and making the audit trail of money hard to follow for law enforcement (Riccardi and Levi 2018; Soudijn and Reuter 2016). Moreover, confiscation of cash not directly linked to a predicate offence also remains difficult in several jurisdictions (Custers et al. 2019).

An alternative to cashing out illicit proceeds via legitimate VASPs is the direct spending of cryptocurrencies to buy illicit goods and services. In this regard, dark web services enable offenders to directly spend their unlawfully earned BTC without a prior conversion in fiat currency. While money laundering services are also sold in the dark web, the high number of references for dark web marketplaces may suggest that a relevant share of cybercrime proceeds is reinvested into further criminal activities. Several studies already highlighted the rise of a specific underground economy for cybercrime where offenders buy and sell specific services/tools that can be used in larger cybercrime schemes (Hyslip 2020; van Eeeten and Bauer 2008). Alternatively, dark web marketplaces can also be used for hedonistic purchases (e.g., drugs). Overall, the frequency of dark web services show the relevance of what has been incisively defined as the "aquarium economy of the underground crime-community" (Van Duyne 1998, p. 363) where illicit proceeds keep circulating in the underground economy without ever entering the legal one.

The relatively unsophisticated money laundering strategies warrant further discussion. First, one could argue that the lack of complexity is the result of the small amounts of illicit proceeds involved. Indeed, results showed that, for example, transactions with larger amounts of illicit proceeds are more likely to involve mixers as well as being less likely to directly send funds to an entity. However, the extent to which these transactions are common in the cybercrime landscape is not easy to determine. While the early days of cybercrime were characterized by few high-profile offenders, nowadays it "has itself become industrialised, with boring tedious maintenance and infrastructure jobs outsourced to lowly paid contractors" (Collier et al. 2020, p. 1). In this regard, Conti adopted a successful "ransomware-as-a-service" business model where several members were responsible of completing repetitive tasks to maintain the infrastructure of the group. Most of the offenders in the sample (77%) received less than $1,000 every two weeks which can be easily laundered without engaging in complex money laundering schemes.

Moreover, if small amounts of illicit proceeds in the sample were the only determinant of unsophisticated money laundering schemes, we should observe complex

money laundering schemes to launder victims' ransomware payments – where often each victim pays hundreds of thousands of dollars—before they are used for internal expenses of the group. However, this is not the case. In one chat, N01 asked the boss: *"Shall we put it in the mixer? or pay as is, let them figure it out themselves?"*. Again, N01 asked N02: "*Does your team wash the cryptocurrencies before distributing them*?". To that question, N02 simply answered: "*No*". The lack of a standardized process for managing the illicit proceeds from victims' payments is clearly detectable in the incoming transactions of the addresses in the sample. In 22% of the transactions, offenders received wages that could be linked back to the group's addresses used to collect ransomware payments from victims, making them more vulnerable to detection.

Conversely, there are other factors that also seem to play a role in influencing cybercriminals' unsophisticated money laundering strategies. Despite the dominant narrative, not all members of cybercriminal networks are high-skilled (Gundur et al. 2021; Leukfeldt et al. 2019a; Lusthaus 2018). This lack of expertise seems to extend also to their knowledge of money laundering practices. Evidence from the chat logs suggests that offenders often are not familiar with tools available to disguise the origin of their illicit proceeds or lack knowledge of how to use them properly. For example, after the recruitment, N03 said to N04: *"Wages of course in BTC. Well, I recommend using a mixer"*. N04 answered: *"Well, there is an understanding with cryptocurrencies, but what is a mixer?"*. Similarly, N05 wrote to the boss: "*Hello, the exchange refused accepting the funds, they say that they come from unsafe sources. What should I do in such cases? […] I sent it to the mixer, I'm waiting, maybe it will help*".

Lastly, it is worth considering the wider regulatory environment as offenders need to be just as sophisticated as the anti-money laundering controls requires them to be (Levi 2015; Levi and Soudijn 2020). Cryptocurrency industry is among the latest entries under the umbrella of anti-money laundering controls. In October 2018, the FATF revised its Recommendation 15 (R.15 – Travel Rule) by requiring VASPs to be regulated as anti-money laundering obliged entities and later adopted an Interpretive Note to Recommendation 15 to further clarify how the FATF requirements apply to VASPs in June 2019 (see for a review FATF 2021). In May 2018, the EU published the Directive (EU) 2018/843 of the European Parliament and of the Council (AMLD5) (2018) which, in line with FATF Recommendations, extended anti-money laundering obligations to VASPs. EU efforts have been later coupled with Regulation 2023/1114 of the European Parliament and of the Council on markets in crypto-assets (MiCAR) (2023) – part of the larger EU's Digital Finance Package—which entered into force on 29 June 2023 and it will be directly applicable in all EU Member States by 30th December 2024. The regulation aims at harmonizing the framework regarding the authorization and operation of VASPs (CASPs – Crypto-Asset Service Providers in MiCAR's terminology) across the EU.

However, despite the significant regulatory progress, FATF found in its fourth targeted review of implementation of the standards on virtual assets and VASPs (June 2023) that 75% of jurisdictions assessed are either still non-compliant or only partially compliant (FATF 2023b). This lack of implementation generates significant opportunities for international arbitrage as offenders, for example, may simply use

"bitcoin exchange services that are located in jurisdictions that have no or less strict regulations" (van Wegberg et al. 2018, p. 432). Regulation represents a key tool in discouraging the misuse of cryptocurrencies for illicit purposes (Ahmed-Rengers et al. 2019; Moiseienko and Kraft 2018). Forcing offenders to rely on services subject to anti-money laundering obligations may significantly assist criminal investigations since law enforcement agencies can subpoena these services and obtain key offenders' information, such as personal bank accounts, e-mail addresses, phone numbers and even IP addresses. In this regard, it is imperative for international bodies and national governments to prioritize the proper implementation and enforcement of existing regulations in the next future to prevent the abuse of loopholes.

Limitation of the study, policy implications and future research directions

The present study has some limitations that need to be considered when interpreting the results. First and foremost, the sample only includes information on 56 members of Conti, namely one of the most dominant ransomware groups at the end of 2021. This choice inevitably raises the question to what extent the results can also be generalized to other threat actors, such as smaller ransomware gangs with different business models or even cybercriminals active in other domains (e.g., DDoS attacks). Different types of cybercriminals have different needs, expertise and constraints, thus likely engaging in different money laundering behaviors.

Second, information about money laundering strategies is limited by the extent and quality of attribution data collected by Scorechain. Even once identified, clusters of BTC addresses may be difficult to associate to a real-world entity because of the lack of attribution data, thus leading to the potential underestimation of certain money laundering strategies. In this regard, at least an unnamed cluster of addresses was identified in 72% of the transactions in the sample.

Lastly, tracing illicit proceeds through several hops requires necessary assumptions on the ownership of the funds. Looking at blockchain data alone is not enough to determine whether a change of ownership has occurred. For example, there is the risk of tracing funds that are no longer in the possession of the offenders because exchanged through in-person peer-to-peer transactions. While this risk surely exists, limiting the analysis only to direct transactions from the deposit address (direct exposure) would be too narrow of an approach, given the inherent nature of money laundering. Therefore, I decided to analyze both direct and indirect exposures, while setting up a maximum threshold of 10 transactions in the latter based on previous literature.

Despite the above-mentioned limitations, the present study provides valuable empirical insights into the money laundering strategies used by ransomware actors. Although cryptocurrencies provide new possibilities for money laundering, the behavior of cybercriminals seems to be surprisingly simple. The prevalence of basic money laundering schemes is a common finding in the literature (Levi and Soudijn 2020; Matanky-Becker and Cockbain 2021; Steinko 2012). However, most of the previous studies have been criticized for using law enforcement data. The assumption underlying these criticisms is that the lack of

complexity detected in money laundering activities is just the result of the priorities, constraints and resources of law enforcement agencies when investigating these cases. Moreover, it is unclear to what extent the detected patterns mirror the behaviors of those offenders who do not get caught (Cockbain et al. 2020).

Conversely, the results of the present study have been obtained by directly analyzing money laundering transactions, showing that simple money laundering schemes also emerge when looking at the behaviors of allegedly "successful" offenders. Results seem to confirm that the mainstream narrative on the money laundering activities suffers of the "ingenuity fallacy", namely when "the situation is imagined to be more complex than it really is" (Levi and Soudijn 2020, p. 6). While complex money laundering schemes certainly exist, they seem not to be the rule and may result in a distorted perception about the criminal phenomenon.

Future research should focus on further improving our understanding of money laundering associated with cybercrime. In this regard, the transparency of the blockchain offers a unique opportunity to criminologists interested in money laundering. For the first time, researchers can access data on financial transactions related to criminal activities without the intermediation of law enforcement agencies. To date, blockchain analysis has been almost exclusively the domain of computer scientists because of the necessary technical skills and computational resources to handle blockchain data on a large scale. However, it is of "fundamental importance for criminologists, and social scientists in general, to retain a role in these debates" (Lavorgna and Antonopoulos 2022, p. 146) and help computer scientists in critically interpreting data on criminal activities. The use of blockchain analysis tools – in particular open-source ones – may significantly lower the entry barriers from a computational point of view, opening new research avenues for criminologists interested in the financial investigation of both cyber-dependent and cyber-enabled crimes.

Acknowledgements I would like to express sincere gratitude to Peter Reuter for the valuable discussion on the topic and to Francesco Calderoni and Maria Jofre for the significant comments on an early draft of the manuscript.

Funding Open access funding provided by Università Cattolica del Sacro Cuore within the CRUI-CARE Agreement.

Data availability Data supporting the findings of this study are available upon request to the author.

Declarations

Competing interests The author has no competing interests to declare that are relevant to the content of this article.

References

Ahmed-Rengers, M., Shumailov, I., & Anderson, R. (2019). Tendrils of crime: visualizing the diffusion of stolen bitcoins. In G. Cybenko, D. Pym, & B. Fila (Eds.), Graphical Models for Security (Vol. 11086, pp. 1–12). Springer International Publishing, Cham. https://doi.org/10.1007/978-3-030-15465-3_1

Albrecht C, Duffin KM, Hawkins S, Morales Rocha VM (2019) The use of cryptocurrencies in the money laundering process. J Money Laund Control 22(2):210–216. https://doi.org/10.1108/JMLC-12-2017-0074

Berry M, Gundur RV (2021) Financial risk management strategies of small to medium illicit enterprises. Second international research conference on empirical approaches to AML and financial crime suppression, Nassau, The Bahamas. https://doi.org/10.21428/cb6ab371.a67fc4f3

Campbell-Verduyn M (2018) Bitcoin, crypto-coins, and global anti-money laundering governance. Crime Law Soc Chang 69(2):283–305. https://doi.org/10.1007/s10611-017-9756-5

Caneppele S, da Silva A (2022) Cybercrime. In: Nelken D, Hamilton C (eds) Research handbook of comparative criminal justice. Edward Elgar Publishing, Cheltenham, United Kingdom. https://doi.org/10.4337/9781839106385

Cockbain E, Bowers K, Vernon L (2020) Using law enforcement data in trafficking research. In: Winterdyk J, Jones J (eds) The Palgrave International Handbook of Human Trafficking. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-319-63058-8_100

Collier B, Clayton R, Hutchings A, Thomas D (2020) Cybercrime is (often) boring: infrastructure and alienation in a deviant subculture. Br J Criminol 61(5):1407–1423. https://doi.org/10.1093/bjc/azab026

Custers B, Pool R, Cornelisse R (2019) Banking malware and the laundering of its profits. Eur J Criminol 16(6):728–745. https://doi.org/10.1177/1477370818788007

Custers B, Oerlemans J-J, Pool R (2020) Laundering the profits of ransomware: money laundering methods for vouchers and cryptocurrencies. Eur J Crime Crim Law Crim Justice 28(2):121–152. https://doi.org/10.1163/15718174-02802002

De Balthasar T, Hernandez-Castro J (2017) An analysis of bitcoin laundry services. In: Lipmaa H, Mitrokotsa A, Matulevičius R (eds) Secure IT systems, vol 10674. Springer International Publishing, Cham. https://doi.org/10.1007/978-3-319-70290-2_18

Dupuis D, Gleason K (2020) Money laundering with cryptocurrency: open doors and the regulatory dialectic. J Financ Crime 28(1):60–74. https://doi.org/10.1108/JFC-06-2020-0113

ElBahrawy A, Alessandretti L, Rusnac L, Goldsmith D, Teytelboym A, Baronchelli A (2020) Collective dynamics of dark web marketplaces. Sci Rep 10(1):18827. https://doi.org/10.1038/s41598-020-74416-y

ENISA (2022) ENISA threat landscape for ransomware attacks. Publications Office. https://data.europa.eu/doi/10.2824/456263

European Parliament & Council (2018) Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018L0843. Accessed 30 Jul2023

European Parliament & Council (2023) Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R1114. Accessed 30 Jul 2023

Europol (2021) Cryptocurrencies: tracing the evolution of criminal finances. Publications Office. https://data.europa.eu/doi/10.2813/75468. Accessed 30 Jul 2023

Europol (2023) IOCTA, internet organised crime threat assessment 2023. Publications Office. https://data.europa.eu/doi/10.2813/587536. Accessed 30 Jul 2023

FATF (2021) Updated guidance for a risk-based approach to virtual assets and virtual asset service providers. FATF

FATF (2023a) Countering ransomware financing. FATF. https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Countering-Ransomware-Financing.pdf.coredownload.pdf

FATF (2023b) Targeted update on implementation of the FATF standards on virtual assets and virtual asset service providers. FATF. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2023.html. Accessed 30 Jul 2023

Filipkowski W (2008) Cyber laundering: an analysis of typology and techniques. Int J Crim Justice Sci 3(1):15–27

Gundur RV, Levi M, Topalli V, Ouellet M, Stolyarova M, Chang LY-C, Mejía DD (2021) Evaluating criminal transactional methods in cyberspace as understood in an international context. CrimRxiv. https://doi.org/10.21428/cb6ab371.5f335e6f

Haines J, Johnstone P (1999) Global cybercrime: new toys for the money launderers. J Money Laund Control 2(4):317–325. https://doi.org/10.1108/eb027198

Handa RK, Ansari R (2022) Cyber-laundering: an emerging challenge for law enforcement. J Victimol Victim Justice 5(1):80–99. https://doi.org/10.1177/25166069221115901

Hutchings A (2014) Crime from the keyboard: organised cybercrime, co-offending, initiation and knowledge transmission. Crime Law Soc Chang 62(1):1–20. https://doi.org/10.1007/s10611-014-9520-z

Hyslip TS (2020) Cybercrime-as-a-service operations. In: Holt TJ, Bossler AM (eds) The Palgrave Handbook of International Cybercrime and Cyberdeviance. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-319-78440-3_36

Kerstens J, Jansen J (2016) The victim-perpetrator overlap in financial cybercrime: evidence and reflection on the overlap of youth's on-line victimization and perpetration. Deviant Behav 37(5):585–600. https://doi.org/10.1080/01639625.2015.1060796

Kim M, Lee J, Kwon H, Hur J (2022) Get off of chain: unveiling dark web using multilayer bitcoin address clustering. IEEE Access 10:70078–70091. https://doi.org/10.1109/ACCESS.2022.3187210

Kruisbergen EW, Leukfeldt R, Kleemans ER, Roks RA (2019) Money talks money laundering choices of organized crime offenders in a digital age. J Crime and Justice 42(5):569–581. https://doi.org/10.1080/0735648X.2019.1692420

Lavorgna A (2020) Organized crime and cybercrime. In: Holt TJ, Bossler AM (eds) The Palgrave Handbook of International Cybercrime and Cyberdeviance. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-319-78440-3_14

Lavorgna A, Antonopoulos GA (2022) Criminal markets and networks in cyberspace. Trends Org Crime 25(2):145–150. https://doi.org/10.1007/s12117-022-09450-5

Lee S, Yoon C, Kang H, Kim Y, Kim Y, Han D, Son S, Shin S (2019) Cybercriminal minds: an investigative study of cryptocurrency abuses in the Dark Web. Proceedings 2019 Network and Distributed System Security Symposium. Network and Distributed System Security Symposium, San Diego, CA. https://doi.org/10.14722/ndss.2019.23055

Leukfeldt ER, Holt TJ (2022) Cybercrime on the menu? examining cafeteria-style offending among financially motivated cybercriminals. Comput Human Behavs 126:106979. https://doi.org/10.1016/j.chb.2021.106979

Leukfeldt ER, Kleemans ER, Kruisbergen EW, Roks RA (2019a) Criminal networks in a digitised world: on the nexus of borderless opportunities and local embeddedness. Trends Org Crime 22(3):324–345. https://doi.org/10.1007/s12117-019-09366-7

Leukfeldt ER, Kruisbergen EW, Kleemans ER, Roks RAR (2019b) Organized financial cybercrime: criminal cooperation, logistic bottlenecks, and money flows. In: The Palgrave Handbook of International Cybercrime and Cyberdeviance. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-319-90307-1_65-1

Levi M (2015) Money for crime and money from crime: financing crime and laundering crime proceeds. Eur J Crim Policy Res 21(2):275–297. https://doi.org/10.1007/s10610-015-9269-7

Levi M, Soudijn M (2020) Understanding the laundering of organized crime money. Crime Justice 49:579–631. https://doi.org/10.1086/708047

Lusthaus J (2018) Industry of anonymity: Inside the business of cybercrime. Harvard University Press

Matanky-Becker R, Cockbain E (2021) Behind the criminal economy: using UK tax fraud investigations to understand money laundering myths and models. Crime Law Soc Chang. https://doi.org/10.1007/s10611-021-09997-4

McGuire M (2018) Into the web of profit: understanding the growth of the cybercrime economy. https://www.bromium.com/wp-content/uploads/2018/05/Into-the-Web-of-Profit_Bromium.pdf. Accessed 30 Mar 2023

Meiklejohn S, Pomarole M, Jordan G, Levchenko K, McCoy D, Voelker GM, Savage S (2013) A fistful of bitcoins: characterizing payments among men with no names. Proceedings of the 2013 Conference on Internet Measurement Conference, 127–140. https://doi.org/10.1145/2504730.2504747

Moiseienko A, Kraft O (2018) From money mules to chain-hopping: targeting the finances of cybercrime [Occasion Paper]. Royal United Services Institute for Defence and Security Studies. https://static.rusi.org/20181129_from_money_mules_to_chain-hopping_web.pdf

Moser M, Bohme R, Breuker D (2013) An inquiry into money laundering tools in the Bitcoin ecosystem. 2013 APWG ECrime Researchers Summit, 1–14

Nguyen T, Luong HT (2021) The structure of cybercrime networks: transnational computer fraud in Vietnam. J Crime Justice 44(4):419–440. https://doi.org/10.1080/0735648X.2020.1818605

Oosthoek K, Cable J, Smaragdakis G (2023) A tale of two markets: investigating the ransomware payments economy. Communications of the ACM 66(8):74–83. https://doi.org/10.1145/3582489

Paquet-Clouston M, García S (2022) On the motivations and challenges of affiliates involved in cybercrime. Trends Org Crime. https://doi.org/10.1007/s12117-022-09474-x

Paquet-Clouston M, Haslhofer B, Dupont B (2019a) Ransomware payments in the bitcoin ecosystem. J Cybersecur 5(1):ty003. https://doi.org/10.1093/cybsec/tyz003

Paquet-Clouston M, Romiti M, Haslhofer B, Charvat T (2019b). Spams meet cryptocurrencies: sextortion in the bitcoin ecosystem. Proceedings of the 1st ACM conference on advances in financial technologies, 76–88. https://doi.org/10.1145/3318041.3355466

Riccardi M, Levi M (2018) Cash, crime and anti-money laundering. In: King C, Walker C, Gurulé J (eds) The Palgrave handbook of criminal and terrorism financing law. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-319-64498-1_7

Richet J-L (2013) Laundering money online: a review of cybercriminals' methods. Tools and resources for anti-corruption knowledge UNODC. https://arxiv.org/abs/1310.2368. Accessed 30 Mar 2023

See K (2023) The Satoshi laundromat: a review on the money laundering open door of Bitcoin mixers. J Financ Crime. https://doi.org/10.1108/JFC-11-2022-0269

Soudijn M (2019) Using police reports to monitor money laundering developments. continuity and change in 12 years of Dutch money laundering crime pattern analyses. Eur J Crim Policy Res 25(1):83–97. https://doi.org/10.1007/s10610-018-9379-0

Soudijn M, Reuter P (2016) Cash and carry: the high cost of currency smuggling in the drug trade. Crime Law Soc Chang 66(3):271–290. https://doi.org/10.1007/s10611-016-9626-6

Steinko AF (2012) Financial channels of money laundering in Spain. Br J Criminol 52(5):908–931. https://doi.org/10.1093/bjc/azs027

Trozze A, Davies T, Kleinberg B (2023) Of degens and defrauders: using open-source investigative tools to investigate decentralized finance frauds and money laundering. Forensic Sci Int Digit Investig 46:301575. https://doi.org/10.1016/j.fsidi.2023.301575

Van Duyne PC (1998) Money-laundering: Pavlov's dog and beyond. Howard J Crim Justice 37(4):359–374. https://doi.org/10.1111/1468-2311.00106

van Eeten MJG, Bauer JM (2008) Economics of malware: security decisions, incentives and externalities (OECD science, technology and industry working papers 2008/01). https://doi.org/10.1787/241440230621

van Wegberg R (2020) Outsourcing cybercrime [Delft University of Technology]. https://doi.org/10.4233/UUID:F02096B5-174C-4888-A0A7-DAFD29454450

van Wegberg R, Oerlemans J-J, van Deventer O (2018) Bitcoin money laundering: mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin. J Financ Crime 25(2):419–435. https://doi.org/10.1108/JFC-11-2016-0067

Vassallo D, Vella V, Ellul J (2021) Application of gradient boosting algorithms for anti-money laundering in cryptocurrencies. SN Comput Sci 2(3):143. https://doi.org/10.1007/s42979-021-00558-z

Wang K, Pang J, Chen D, Zhao Y, Huang D, Chen C, Han W (2022) A large-scale empirical analysis of ransomware activities in bitcoin. ACM Trans Web 16(2):1–29. https://doi.org/10.1145/3494557

Werner Y, Korsell L (2016) Cyber-OC in Sweden. In Bulanova-Hristova G, Kasper K, Odinot G, Verhoeven M, Pool R, de Poot C, Werner, Korsell L (Eds.) Cyber-OC: scope and manifestations in selected EU member states (pp. 101–164). Bundeskriminalamt, Wiesbaden

Wronka C (2022) Money laundering through cryptocurrencies—Analysis of the phenomenon and appropriate prevention measures. J Money Laund Control 25(1):79–94. https://doi.org/10.1108/JMLC-02-2021-0017

Zhang Y, Wang J, Luo J (2020) Heuristic-based address clustering in bitcoin. IEEE Access 8:210582–210591. https://doi.org/10.1109/ACCESS.2020.3039570