International Journal of Information Security (2024) 23:699–712
https://doi.org/10.1007/s10207-023-00766-z

REGULAR CONTRIBUTION

Cashing out crypto: state of practice in ransom payments

Constantinos Patsakis[1,2] · Eugenia Politou[1] · Efthimios Alepis[1] · Julio Hernandez-Castro[3]

Published online: 13 October 2023

Abstract
The fast pace of blockchain technology and cryptocurrencies' evolution makes people vulnerable to financial fraud and provides a relatively straightforward monetisation mechanism for cybercriminals, in particular ransomware groups which exploit crypto's pseudo-anonymity properties. At the same time, regulatory efforts for addressing crimes related to crypto assets are emerging worldwide. In this work, we shed light on the current state of practice of ransomware monetisation to provide evidence of their payment traceability, explore future trends, and—above all—showcase that over-regulating cryptocurrencies is not the best way to mitigate their risks. For that purpose, first, we provide an overview of the legislative initiatives currently taken by the USA, the EU, and the OECD to regulate cryptocurrencies, showing that strict laws and the divergences between the regulatory regimes can hardly efficiently regulate the global phenomenon of cryptocurrency, which transcends borders and states. Next, we focus on illicit payments in bitcoin to ransomware groups, illustrating how these payments are siphoned off and how criminals cash out the ransom, often leaving traceable evidence behind. To this end, we leverage a publicly available dataset and a set of state-of-the-art blockchain analysis tools to identify payment patterns, trends, and transaction trails, which are provided in an anonymised form. Our work reveals that a significant amount of illicit bitcoin transactions can be easily traced, and consequently, many cyber crimes like ransomware can actually be tracked down and investigated with existing tools and laws, thus providing fertile ground for better and fairer legislation on crypto.

Keywords Ransomware · Bitcoin · Taint analysis · Blockchain forensics · Cryptocurrencies · Regulation

1 Introduction

Since the advent of Bitcoin in 2008 (the first and most well-known cryptocurrency), cryptocurrencies and crypto-assets have been steadily in the spotlight of the media for their potential to create a fully decentralised economy by providing increased payment efficiency, transparency, reduced transaction costs, and the facilitation of international payments [1]. The inherent security and transparency of blockchain—the underlying technology of most cryptocurrencies—account for one of their most striking feature, their trustlessness, in which the need for third-party participation to guarantee trust among users in a decentralised environment is eliminated. In other words, as opposed to the central banks' centralised systems (which means that a monetary institution has privileged control over the production and distribution of money), cryptocurrencies can be completely independent of any intermediaries as they can be fully operable without intervention or control of any third-party entity, e.g. a bank. Justifiably, Bitcoin was born out of the 2008 financial crisis and the ensuing fundamental distrust in governments and financial institutions [2], whereas its price skyrocketed in 2017, resulting in the explosion of widespread media attention and consumer interest. With the rise of cryptocurrency as a popular investment, wallets and exchange platforms have advanced, providing online marketplaces for owners and investors to store and trade cryptocurrencies pseudonymously.

Even though cryptocurrencies' potential currently constitutes one of the most vividly discussed financial topics, they also occupy the media for their risks since they have been connected to financial crimes like money laundering, tax evasion, and ransom payments. To address the challenges posed by cryptocurrencies, policymakers push towards strictly regulating the crypto market. While to date there has not been

✉ Constantinos Patsakis
kpatsak@unipi.gr

[1] Department of Informatics, University of Piraeus, Karaoli & Dimitriou 80, 18534 Piraeus, Greece

[2] Athena Research Center, Marousi, Greece

[3] School of Computing, University of Kent, Canterbury, UK

any internationally coordinated regulation of blockchain and cryptocurrencies, several international bodies are working apace right now towards developing global standards and providing guidance for this purpose. At the same time, many governments worldwide respond to the emerging threats of the new crypto economy by introducing bespoke regulatory regimes to adjust current financial legal instruments to crypto-markets and crypto-assets, by entirely banning cryptocurrencies, or even by not dealing with them at all [3, 4]. There is also the exception of El Salvador, which became the first country in the world to recognise bitcoin as legal tender in 2021 [5].

Despite the above efforts over the past few years, the use of cryptocurrencies for ransomware attacks is on the rise [6, 7]. As it has been pointed out, the growth in ransomware is one of the "darker" activities that have been facilitated by the diffusion of cryptocurrencies [8]. Certainly, ransomware is not the sole nor the main illegal activity powered by cryptocurrencies, yet it is one of their top nefarious uses [9–11]. Cryptocurrencies, typically Bitcoin, have become a nearly universal form of ransom payment in ransomware attacks, in part because they enable criminals to extort huge sums of money from victims across diverse sectors with incredible speed [12]. Moreover, the pseudonymity that Bitcoin provides has supposedly given cybercriminals a way to monetise their actions without being traced. Their typical *modus operandi* is illustrated in Fig. 1. Depending on the group and their capabilities, they either use malspam campaigns to set a foothold on their victim's host or exploit a vulnerability on an internet-facing host. The dropped malware would then either try to leverage privileges and encrypt the host's files or connect to a command and control (C2) server allowing threat actors to manually hack their way through the victim's infrastructure while automating some tasks. Typically, they would try to locate and destroy backups and then encrypt the victim's files. In the past few years, threat actors have embraced the double extortion model in which the attackers encrypt the victim's data, exfiltrate sensitive information, and threaten to publish it. Further extortion tactics, e.g. providing deadlines, contacting the victim's clients, etc., have been leveraged to persuade the victim into paying the ransom, typically into a bitcoin address.

While the literature on ransomware focuses almost entirely on technical solutions, up to date, no simple technological "silver bullet" will wipe out the crypto ransomware threat [13]. Many works have experimented with machine learning, AI techniques, and behavioural analysis to detect ransomware [14, 15]. Still, preventing ransomware relies mostly on users' education and basic computing hygiene and best practices, whereas designing and deploying an effective and efficient detection solution against this particular malware category represents a formidable technical challenge [16]. Against this background, policymakers attempt to mitigate the effects of illicit cryptocurrencies transactions, including those associated with ransomware, by introducing domain-specific laws and regulations to constrain and control the cryptocurrency ecosystem, sometimes dramatically affecting the opportunities and promises offered by this new industry.

In this work, we attempt to shed light on the current state of practice and to demonstrate that laws alone—despite their strictly punitive and possibly universal character—cannot efficiently regulate and deter the crypto illicit usage when it comes to ransomware. Instead, we provide evidence and a methodology to prove that crypto ransomware can be tracked down by employing known tools and methods, to understand the cashing out methods used. The closest research to ours was published at the time of writing this article by [17], who performed a similar analysis to ours but over an older version of the dataset. Yet, they focus only on the first entity they can identify after receiving the payment transaction, whereas we follow the traces of the transactions up to the depth of five hops. Moreover, they do not discuss the common errors that are encountered nor the legal implications.

To prove our arguments, first we provide an overview of the legal framework regarding cryptocurrencies, illustrating how governments and international bodies try to address their use. Then, we focus on payments to ransomware groups, illustrating how they are siphoned off and how, despite the current legal restrictions, they frequently manage to cash out the ransom, often providing traceable evidence. To this end, we leverage a publicly available and recent dataset [18] and a couple of state-of-the-art blockchain analysis tools [19] to identify payment patterns, trends and transaction trails, which are provided in an anonymised form, and we demonstrate how these traces can be easily used to identify the illicit transactions.

The rest of this work is structured as follows. First, we introduce the background concepts used throughout this paper, such as mixers and tumblers, taint analysis, ransom payments, and cryptocurrency exchanges as cashing out mechanisms. In Sect. 3, we present the current legislative efforts by the USA, the EU, and the OECD to regulate cryptocurrencies, and we discuss their status and limitations. Next, in Sect. 4, we outline our methodology to identify payment patterns and reveal crypto transactions to ransomware groups. Our findings are described in Sect. 5, where we analyse the behaviour of the ransomware groups concerning their cashing-out practices. Finally, we conclude our paper in Sect. 6 by observing both the limitations and the benefits of our research to policymakers and by discussing future directions and challenges for the crypto ecosystem in terms of their regulation, risks, and opportunities.

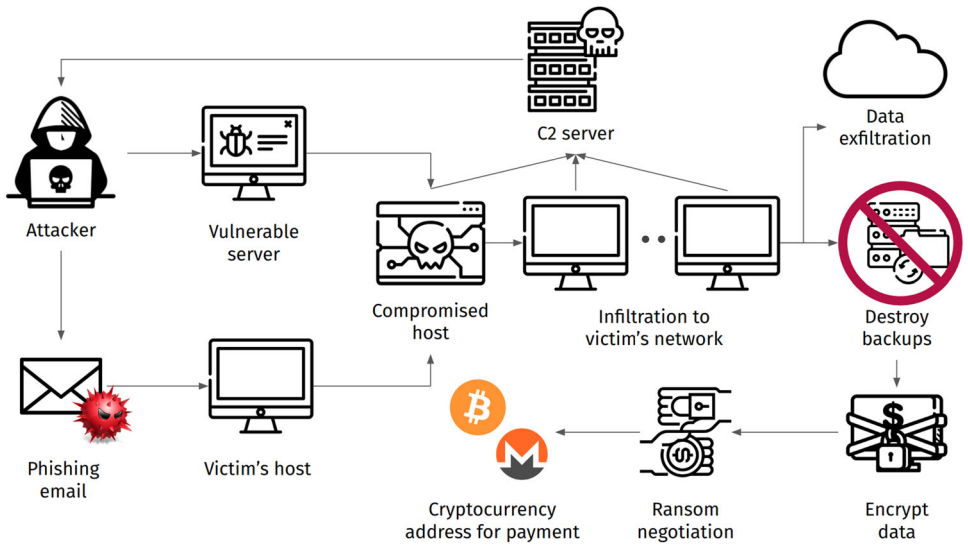


Fig. 1 The *modus operandi* of a ransomware attack

2 Background

To demonstrate the points of our paper, in this section, we outline some concepts regarding ransomware payments and other illicit crypto transactions.

2.1 Taint analysis

Taint in cryptocurrency refers to the concept that certain coins can be deemed riskier or less acceptable because of their previous owners' possible links to criminal activity. In this regard, taint analysis can inform us of how much of a coin comes from a given address and thus what percentage of a coin can possibly have illegal or uncertain origins associated with criminal activities.

To perform taint analysis, a starting point is typically chosen, frequently an address known to be associated with an illicit transaction. The transactions that are directly connected to this starting point are then analysed to identify their inputs and outputs, and any subsequent transactions that use these inputs and outputs are traced in turn. This process continues until all transactions that can be traced back to the starting point have been identified. Along the way, a variety of techniques can be used to filter out false positives and refine the analysis. For example, some transactions may involve multiple inputs and outputs, so it is important to distinguish between those that are truly connected to the illicit activity and those that are not. Other techniques, such as clustering, can be used to group together addresses that are likely controlled by the same entity, which can help identify the parties involved in the illicit activity. The basic methods are first-in-first-out (FIFO) [20] and last-in-first-out (LIFO) [21]. In the former, we assume that the earliest received coins are the first ones to be spent. On the contrary, in the LIFO method, we assume that the most recently received coins are the first ones to be spent.

2.2 Cashing out

Cashing out mechanisms, employed to transform crypto assets into fiat money, typically make extensive use of cryptocurrency exchanges, mixers, and tumblers.

Cryptocurrency exchanges, or simply exchanges, are platforms that facilitate the trading of cryptocurrencies, such as Bitcoin, Ethereum, and Litecoin, among many others.[1] They enable users to buy, sell, and trade digital assets, often for other cryptocurrencies or traditional fiat currencies like the US Dollar and Euro. Exchanges can be centralised or decentralised, with varying degrees of regulatory oversight and security features. Centralised exchanges (CEX) are managed by a central authority or company, which controls the platform's operations and holds users' funds in custody. They often provide features such as advanced trading tools, leverage trading, staking, and the ability to convert cryptocurrencies to a variety of fiat. However, users must trust the exchange with their private keys and personal information, which poses a serious security risk. On the contrary, decentralised exchanges (DEX) operate without a central authority, using smart contracts and blockchain technology to facilitate P2P transactions. Well-known examples are Uniswap, PancakeSwap, 1inch, dXdY, and JOE, to name but a few. They generally offer greater privacy, security, and control of funds but may have lower liquidity and fewer trading pairs than their centralised peers. They are also the target of frequent

[1] Including, in many cases, privacy-oriented ones such as Monero, Zcash and, to a certain extent, Dash, Secret, Horizen and Nym, to mention only a few. Privacy-oriented cryptos have been falsely accused of only serving to hide criminal activity and have been delisted in a number of exchanges to appease the regulators, e.g. the recent case of [22].

attacks which, however, typically focus on liquidity providers rather than normal users.

Mixers and tumblers are privacy-enhancing tools used by some cryptocurrency users to obfuscate the origin of their digital assets. These services work by pooling multiple users' coins together and then redistributing them in a way that breaks the link between the original addresses and the new (destination) ones. This process can potentially make it harder for third parties to trace transactions and determine the true owner and origin of the funds. Yet, it requires significant trust in the service provider who keeps an initially agreed share (typically anything between 5–10%) in exchange for the service.

Practically, when using a mixer or tumbler, users send their coins to a designated address managed by the service. The service then pools the coins with the ones coming from other users and redistributes them to new addresses, usually in multiple transactions and over a relatively long period of time. The redistributed coins are typically sent to new addresses, provided by the users or generated by the mixer itself. Users typically prefer to send their bitcoins to different addresses to prevent the detection of a single address. Depending on the number of users' transactions, used addresses, and amounts of exchanged cryptocurrencies, this shuffling can lead to numerous transactions where tainting is rendered less useful or even useless. While such services were created to provide individuals with greater privacy guarantees against, e.g. surveillance, in practice, mixers and tumblers are often associated with illicit activities. Since they obscure the source of funds, they are frequently exploited for money laundering, tax evasion, or other illegal transactions [23]. Thus, mixers and tumblers and their use are deemed illegal in numerous jurisdictions.

However, mixers often operate in a relatively unsophisticated way that leads to patterns which can help investigators limit their utility, particularly after carefully examining the transaction graphs they create. Thus, wallet addresses can be commonly linked with mixing services in various ways [24–28] and, in extreme cases, their mixing operation can be completely reversed [29].

3 Regulations

Several examples of regulating cryptos, i.e. their issuance, marketing and taxation, have emerged in many countries as governments desire not only to tax crypto profits but also to address related criminal operations. To this end, the EU, the US, and the OECD are currently pursuing global regulatory standards for cryptocurrency markets. In this section, first we succinctly present these legislative efforts, and then we discuss their limitations, particularly regarding attempts at regulating a constantly changing decentralised environment such as that of cryptocurrencies.

3.1 United States

The USA has no uniform regulatory approach for handling cryptocurrency exchanges and money transfer platforms. An early attempt to regulate the cryptocurrency market was the BitLicense law passed in 2015 by the state of New York. The law received harsh criticism from the cryptocurrency community for strangling all Bitcoin-related businesses since it led to the swift departure of many businesses from the state [1].

Since then, many policy-shaping organisations such as the Conference of State Bank Supervisors (CSBS) and the Uniform Law Commission (ULC) have initiated efforts to apply uniform cryptocurrency laws across all the US states [1], introducing the Uniform Regulation of Virtual-Currency Business Act (URVCBA).[2] The law provided guidance to virtual-currency businesses as to how they should operate and a three-tier licensing system. As expressed by the drafters, the goal of the URVCBA was not to regulate virtual currencies but rather to "regulate persons that issue virtual currencies or to provide services that allow others to transfer virtual currencies, provide 'virtual-currency' exchange services to the public, or offer to take custody of virtual currency for other persons". The disclosure obligations introduced by the URVCBA were limited only to large-scale transactions, whereas transactions below a given threshold would be exempt from all license-related compliance and disclosure requirements.[3] Even though the Act aimed at satisfying both policy-makers and crypto proponents by striking a balance between encouraging technological innovation, maintaining market stability, and ensuring consumer protection, it also received hard criticism.[4] As a result, and while the model law was under consideration by several states for adopting it in their own bills, in 2019 the ULC asked all states to refrain from enacting it.[5]

In the following years, there were many attempts by the US Congress to introduce laws to cover the crypto regulatory

[2] https://www.uniformlaws.org/viewdocument/final-act-154?CommunityKey=e104aaa8-c10f-45a7-a34a-0423c2106778.

[3] https://www.proskauer.com/blog/a-proposed-statutory-framework-for-state-regulation-of-virtual-currency-businesses-the-uniform-law-commissions-uniform-regulation-of-virtual-currency-businesses-act.

[4] https://www.forbes.com/sites/andreatinianow/2019/03/07/a-split-emerges-in-blockchain-law-wyomings-approach-versus-the-supplemental-act/?sh=68a51932719a and https://bitcoinist.com/nevada-scrap-cryptocurrency-bitcoin-regulations/.

[5] https://www.forbes.com/sites/caitlinlong/2019/03/25/seismic-news-about-state-virtual-currency-laws-ulc-urges-states-to-withdraw-model-act/?sh=218490335fda.

landscape in a variety of ways.[6] The Crypto-Currency Act of 2020 - which attempted to clarify which Federal agencies regulate digital assets and to require those agencies to notify the public of any Federal licenses, certifications, or registrations required to create or trade in such assets - failed to receive a vote[7] [30].

A federal regulation passed in November 2021 and known as the "Infrastructure Investment and Jobs Act", includes provisions for regulating crypto-assets and mandatory tax information reporting for some cryptocurrency transactions[8] [30]. The legislation increases reporting obligations and tax collections from digital brokers and requires them to undertake the same type of reporting currently required for traditional assets like stocks and bonds. The tax collection expands to digital assets as well since the law treats digital assets as cash and, therefore, a person who receives more than $10,000 of cash (including digital assets) in one or multiple transactions must file the relevant tax forms [31]. The type of information required to be reported includes the proceeds from taxable sales and exchanges of digital assets, the tax basis and holding period for digital assets sold, the transfers of digital assets to other exchanges, and the transfers of digital assets to wallet addresses that are not attributed to other exchanges (such as cold storage devices).

At the same time, the law greatly expands the definition of a broker to include "any person who is responsible for providing any service effectuating transfers of digital assets on behalf of another person". This wording, apart from including US cryptocurrency asset exchanges and digital wallet providers, would potentially implicate the extensive reporting obligations of cryptocurrency miners, software developers, and other entities who do not actually facilitate transactions.[9]

Not surprisingly, the law has raised serious concerns as it could potentially drive innovators and opportunities out of the USA. In this regard, politics and crypto advocates were urging for formal amendments of the law before its application in January 2023 to clearly exempt miners and developers from the reporting rules and to address the challenges regarding better reporting solutions[10] [31]. While the U.S. Treasury is proclaiming that the industry will need to comply, there have been more than five bills introduced in an attempt to modify or reverse the impact of the legislation, with the most recent one being a new bill claiming that will repeal the provisions of the "Infrastructure Investment and Jobs Act" regarding reporting requirements with respect to digital asset transfers.[11]

Other US bills on digital assets include, among others, the Central Bank Digital Currency Study Act,[12] introduced in 2021 to direct appropriate bodies to conduct a study on central bank digital currencies but did not receive a vote, as well as the Blockchain Regulatory Certainty Act which has been already introduced three times since 2018 in an attempt to protect blockchain developers or providers of a blockchain service from being treated as money transmitters or financial institutions unless they have control over digital currency.[13]

More recently, the partial victory for Ripple on its long-standing case against the Securities and Exchange Commission (SEC) has brought new hope to many US users and businesses that were worried about the very negative view of the SEC and its shortsightedness in trying to declare all cryptos other than Bitcoin as securities.

3.2 European Union

Nowadays, the regulating landscape for cryptocurrencies in the EU is fragmented as each EU country follows different and often diametrically opposed approaches when it comes to regulating these markets. Several European jurisdictions such as Germany, France, Lithuania, and Malta have been proactive and successfully designed their own national regulatory solutions to crypto assets, albeit with very different rules, whereas in many other jurisdictions, cryptocurrencies are largely unregulated[14] [32]. The European Commission, taking into account that crypto assets have become a worldwide phenomenon and a promising new type of financial asset and hence any regulatory gap may contribute to legal

[6] https://www.forbes.com/sites/jasonbrett/2022/05/19/congress-has-introduced-50-digital-asset-bills-impacting-regulation-blockchain-and-cbdc-policy/?sh=5fc921cc4e3f.

[7] https://www.congress.gov/bill/116th-congress/house-bill/6154/all-info and https://www.govtrack.us/congress/bills/116/hr6154.

[8] https://www.congress.gov/bill/117th-congress/house-bill/3684.

[9] https://www.dlapiper.com/en-gb/insights/publications/2021/11/infrastructure-bill-including-crypto-broker-rules-becomes-law.

[10] https://www.frazierdeeter.com/insights/infrastructure-bill-require-1099-cryptocurrency-reporting/ and https://taxbit.com/blog/the-infrastructure-bill-has-passed-whats-next-for-crypto#how-does-the-infrastructure-bill-change-the-definition-of-a-broker and https://www.warner.senate.gov/public/index.cfm/2022/8/warner-toomey-lummis-sinema-portman-drop-legislation-to-address-digital-asset-reporting-requirements-in-infrastructure-bill.

[11] https://www.congress.gov/bill/118th-congress/senate-bill/695?s=1&r=53 and https://www.forbes.com/sites/jasonbrett/2022/05/19/congress-has-introduced-50-digital-asset-bills-impacting-regulation-blockchain-and-cbdc-policy/?sh=3afc412d4e3f.

[12] https://www.congress.gov/bill/117th-congress/house-bill/2211/actions and https://www.govtrack.us/congress/bills/117/hr2211.

[13] See footnote 6 and https://www.fintechanddigitalassets.com/2023/03/blockchain-regulatory-certainty-act-would-protect-non-custodial-crypto-services/ and https://www.forbes.com/sites/jasonbrett/2022/05/19/congress-has-introduced-50-digital-asset-bills-impacting-regulation-blockchain-and-cbdc-policy/?sh=3afc412d4e3f.

[14] https://law.stanford.edu/2021/01/12/new-crypto-rules-in-the-eu-gateway-for-mass-adoption-or-excessive-regulation/ and https://complyadvantage.com/insights/cryptocurrency-regulations-around-world/.

uncertainty and weak investor protection, admitted for the first time in the Fintech Action Plan of 2018 the necessity to assess the suitability of the EU regulatory framework regarding these types of assets [32].

In September 2020, after a thorough consultation and review of the entire crypto assets ecosystem, the European Commission introduced a new comprehensive framework to regulate markets in crypto-assets, the Regulation on Markets in Crypto-Assets (MiCA), which establishes a uniform set of rules for crypto asset service providers and issuers.[15] MiCA aims to protect consumers and ensure financial stability and market integrity by establishing a digital single market and preventing further divergence between national regulatory regimes [32]. Following the final approval by the EU Council and Parliament and an 18-month period to allow foreseen measures to be adopted prior to its application, MiCA will come into force in the second half of 2024, and—being a regulation—once enacted will be directly applicable in all EU member states replacing any existing national frameworks for crypto assets[16] [32].

The scope of MiCA regulation is broad and covers issuers of crypto-assets and other service providers in crypto-markets, including trading platforms, crypto-asset exchanges, and custodian wallet providers. It also establishes specific rules for a relatively new subset of crypto assets called stablecoins [32, 33]. It also makes it a legal obligation for crypto projects to issue a white paper containing information about the project, including, among others, their main characteristics, rights and obligations, and submit it to the regulatory authorities.[17] Under the new rules, all types of crypto-asset service providers will need to obtain authorisation from a competent authority at the level of the member state and, more importantly, maintain a physical presence in the territory of the EU. Also, crypto-asset service providers need to set up sound and adequate systems and procedures for internal control and risk assessment. To ensure transparency and investor protection, additional disclosure requirements for issuers of stablecoins include disclosures on potential claims and conflict of interests and, more importantly, disclosure of the stabilisation mechanism [33]. As for crypto trading platforms, MiCA requires pre- and post-trade transparency as well as obligations in relation to the settlement of transactions. Exchange services are subject to requirements on non-discriminatory policy, price transparency as well as transparency on orders and transactions.

MiCA has been recognised as an ambitious legislative project that responds to an urgent policy need, whereas it has also been considered a unique opportunity for the EU to set global standards, attract innovation, and position its digital economy at the forefront as a top participant in the global crypto assets industry [32].

Nevertheless, it has been criticised for being far from conclusive, possibly not too effective and certainly not capable of providing legal certainty [34]. For instance, even though MiCA aims to regulate all types of crypto assets, it has been blamed for overregulating stablecoins, arguably aiming to deter investment of crypto profits in stablecoins, and, consequently, to prioritise protecting the interests of the European banking sector and national tax authorities [35]. MiCA also excludes from its application crypto assets that qualify as financial instruments under MiFID II [36]. However, MiCA is a regulation, and hence applied directly in all EU member states once enacted, as opposed to MiFID II, which, being a directive, will need to be transposed into national legislation, thereby possibly producing diverse definitions of financial instruments in each jurisdiction. Yet, since the remaining crypto assets will be governed by the uniform MiCA regulation, this divergence can potentially create discrepancies and regulatory arbitrage [32, 37].

Furthermore, it has been outlined that MiCA does not protect against all of the risks associated with cryptocurrencies [35]. More importantly though, the requirement to incorporate a single legal entity as a crypto-asset service provider and to register it with the EU member state in which it is headquartered seriously challenges the decentralised nature of cryptocurrency networks which are built on top of permissionless and trustless blockchains and hence lack centralised ownership and control from a single entity [33]. Inevitably, this constraint will create a significant compliance burden for some issuers of asset-referenced tokens, and it may hinder decentralised financial applications seeking out EU customers.

Overall, MiCA has been subject to strong criticism for creating barriers for new companies' market entrance, for building opportunities for regulatory arbitrage, for leaving out from the consultation process some of the largest market participants in the crypto-asset industry, for its encroaching approach to regulate the whole market of crypto-assets, and for trying to fit within the existing regulatory framework without even questioning whether that is the most appropriate and effective approach [37].

Given that MiCA does not provide a basis for tax authorities to collect and exchange the information needed in order to tax crypto-asset income, the EC launched in 2022 a public consultation for a new Directive on Administrative Cooperation (DAC), known as DAC8 [38], to combat international tax evasion by means of the automatic exchange of tax-related information, i.e. AEOI [39]. DAC8 aims to introduce uniform

[15] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593.

[16] https://www.consilium.europa.eu/en/press/press-releases/2022/06/30/digital-finance-agreement-reached-on-european-crypto-assets-regulation-mica/.

[17] https://medium.com/coinmonks/asset-referenced-tokens-under-the-eus-proposed-markets-in-crypto-assets-regulation-458c317577bb.

and mandatory disclosure requirements for crypto-assets service providers and thereby ensure that tax authorities across the EU have increased visibility with respect to crypto-assets. The directive, which final proposal has been tabled on 8 December 2022 and is to be enforced as of 1 January 2026 [40], aims to limit opportunities for bad actors to take advantage of potential loopholes in crypto-asset-related legislation within the EU [41, 42].

On top of the above, the European Parliament recently adopted a regulation on the transfer of funds that effectively extends to crypto-asset transfers the information-sharing duties applicable to wire transfers [43]. These requirements are commonly known as the "Travel Rule", and were originally designed to counter money laundering and terrorist financing, as well as to enhance the traceability of funds.

3.3 Organisation for economic co-operation and development (OECD)

The OECD raised awareness of tax evasion concerning cryptocurrencies in its report published in late 2020 [44]. The report offered an overview of the current tax treatments of virtual currencies worldwide and highlighted the need for greater transparency in this area, especially when considering crypto-assets.

Accordingly, the OECD conducted in 2022 the first comprehensive review of the Common Reported Standard (CRS)—under which countries currently implement the automatic exchange of information (AEOI) to fight against transborder tax evasion—to identify financial assets (such as e-money and crypto-assets), products, and intermediaries that should be included in the scope of the Standard and, thereby, to capture tax evasion facilitated through the use of cryptocurrencies and crypto-assets [31, 39, 45]. The work resulted in the publication of the Crypto-Asset Reporting Framework (CARF) and the amendments of the CRS to modernise the tax transparency instruments by including crypto assets in the OECD's tax reporting requirements [46]. The CARF defines the relevant crypto assets in scope, the intermediaries, and other service providers that will be subject to reporting. It also consists of several measures as rules and commentary that can be transposed into domestic law to collect information from crypto asset service providers [4]. To this end, the OECD is currently working on the legal and operational instruments needed to facilitate the international exchange of information collected based on the CARF to ensure its effective and widespread implementation [47].

3.4 Towards better and fairer regulations

As we have shown, various worldwide efforts towards regulating cryptocurrencies and controlling their illicit use are ongoing. Yet, they face criticism in terms of their applicability as well as their effectiveness towards constraining illicit crypto payments. In fact, it has been argued that regulating the inherently decentralised digital environment of cryptocurrencies by using traditional means may not be in the best interest of the digital economy and of the involved stakeholders. Above all, there are serious concerns that the regulating attempts across the USA, the EU, and the OECD, could potentially deter innovators and repel growth opportunities. Besides, this fragmented landscape of crypto regulations can hardly protect against all of the risks associated with cryptocurrencies.

In light of the above, we argue that over-regulating cryptocurrencies is not necessary to protect against crypto ransomware attacks. To this end, we provide below evidence and a method to demonstrate that crypto ransom payments can indeed be tracked down by solely exploiting current tools and behavioural models.

4 Methodology

In this section, we first present the dataset and the tools we used to identify ransom payment patterns, and then we provide an example to illustrate our methodology.

4.1 Dataset

To demonstrate our work, we use the publicly available dataset of J. Cable [18], which contains cryptocurrency addresses that ransomware victims sent ransom payments to, as reported by them. At the time of writing, the dataset contains data from about 10367 addresses belonging to 128 ransomware families. Table 1 illustrates the ransomware groups for which the reported ransom payments are above $1 m. Many of these groups used multiple Bitcoin addresses, e.g. Locky, while others used significantly fewer or just even one, e.g. MountLocker. This diversity is due to two factors. The first one is that not all victims report ransom payments. Thereby, even though, e.g. REvil had numerous victims, only 7 of the addresses are reported. Another factor is the *modus operandi* of the groups as, e.g. some groups targeted only a reduced number of high-profile organisations, while others may not have a specific target but attack "low-hanging fruit" and smaller organisations (usually called "spray and pray" attacks) or even use malspam campaigns to target random individuals.

In our work, we have been solely focused on groups with confirmed payments above $100.000 and less than 100 addresses so that the generated graphs are manageable. These restrictions resulted in 29 ransomware groups and 285 Bitcoin addresses of interest.

Table 1 Ransomware groups in the dataset with payments above $1 m

Ransomware group	Addresses	Ransom paid
Cuba	18	60150632.45
Netwalker (Mailto)	66	27477621.16
Conti	28	17426824.10
Locky	7037	14024715.95
REvil / Sodinokibi	7	12135784.74
RagnarLocker	4	10879014.96
DarkSide	3	9111317.45
Maui	39	8777233.40
Ryuk	40	7247659.18
MedusaLocker	20	5338914.69
Karakurt	19	5032602.57
MountLocker	1	4218728.14
BlackMatter	1	4070928.60
Egregor	9	3127036.56
DarkAngels	1	1514100.77
Bitpaymer / DoppelPaymer	1	1088792.44
DMALockerv3	9	1075195.34
HelloKitty	1	1072689.19

Fig. 2 Shatoshi's Nakamoto bitcoin address `1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa`, as illustrated in GraphSense. The left hand side shows incoming transactions, and the right hand side outgoing ones

4.2 Crypto analytics platforms

To identify payment patterns, trends and methods, we used Scorechain [48] and [19], an open-source crypto asset analytics platform. Such platforms use several machine-learning methods to cluster Bitcoin addresses and automatically illustrate in the form of a cluster as a single entity all the addresses provided by an investigator. This entity has a set of incoming transactions from various addresses and can have some outgoing transactions, as illustrated in Fig. 2. Some entities can be linked with thousands of addresses and incoming and outgoing transactions for which there is no additional intelligence; thus, the platform does not associate them with a named entity. Thankfully, GraphSense's combined with Scorechain' intelligence, can identify several major entities such as exchanges, mixers, or even dark web markets.

As part of our methodology, we use GraphSense and Scorechain to perform a taint analysis, exploiting the fact that Bitcoin does not actually provide any transactional privacy. On the contrary, all transactions are publicly available. To this end, we use the Bitcoin addresses of the various ransomware groups from the dataset as seeds, and we follow the transactions of the addresses that can be traceable, e.g. they have few incoming and outgoing addresses and hence their tainting has not been spread too widely, to the whole network. Starting from these addresses and using the intelligence obtained from the two platforms, we try to determine the receiving entities. However, when collecting further addresses, we exclude those with many and large inputs from other addresses since the latter ones fall beyond the scope of our investigation, e.g. they can be linked to other transactions and entities. We follow the traces of the transactions up to the depth of five hops, which is the maximum depth where the resulting graphs are still interpretable while traces remain reasonable.

4.3 Illustrating example

To illustrate our methodology, we provide an example using Fig. 3. Starting from address S (in red), we observe that it makes three transactions to addresses A, B, and C. However, A has inputs from other addresses and sends funds to others. Since we have no intelligence for the incoming addresses to A, and tainting the outgoing addresses may result in tainting a vast part of the graph, we consider these addresses out of scope (in yellow). Then, we notice that from B and C, one can reach an exchange (starting from S) in three and five hops, respectively; hops are counted in dark blue squares. Note that the transactions from and to the addresses in both these paths do not include other entities. One can observe two direct paths from S to the exchange E, namely $S \rightarrow B \rightarrow D \rightarrow E$, and $S \rightarrow C \rightarrow D \rightarrow E$. Similarly, there are paths from S to E'; however, since there is a shorter path to another exchange (E), we consider E' out of scope, so it is not reported. Hence, we report only three hops and all the exchanges at this depth.

5 Findings

Our aggregated results are illustrated in Fig. 5. In essence, our study involves the addresses of 29 ransomware groups whose transactions, surprisingly, after just 2.33 hops on average have reached an exchange for 27 of them (in two cases, this was not possible). Contrary to our first intuition, some of these addresses still contain bitcoins. For most of them, the amount is only a handful of satoshis that can be considered rounding errors in fees or the by-product of mental calculations when transferring the ransom to other addresses. However, a significant nine addresses do not fit this profile. Especially four of them contain quite a significant amount of money (more than ten bitcoins each), frozen for more than a year.

Obviously, one would expect the ransom to be transferred to other addresses shortly after payment. Indeed, that is the

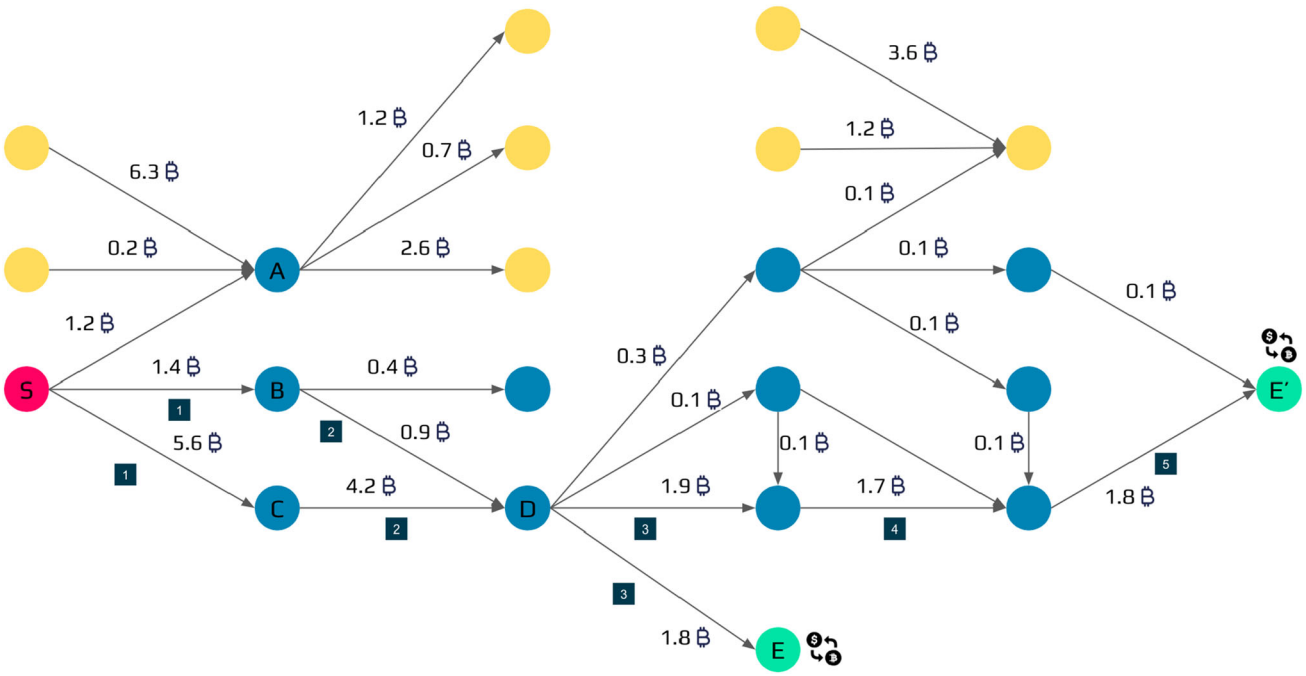


Fig. 3 An example graph illustrating traceability of transactions between addresses within and out of scope. The colour coding of the addresses is as follows: red is for a seed address, blue is for an address within scope, yellow is for out-of-scope addresses, and green denotes the addresses of known entities. The dark blue squares indicate the length of the shorter path to the seed address

case for almost all groups for which the amount of incoming transactions is almost the same as the number of outgoing ones. More precisely, the number of incoming transactions is 6861, and there are 6647 outgoing ones. Note that the difference in these 214 transactions is largely (around 76%) attributed to just one group, which seems to prefer to transfer some of the funds in bulk; another group is responsible for 15% of these transactions, whereas the remaining ones have a nonzero balance. The above makes us believe that the frozen addresses can be attributed to operational factors, such as the group losing access or, more likely, some legal intervention preventing them from transferring the funds.

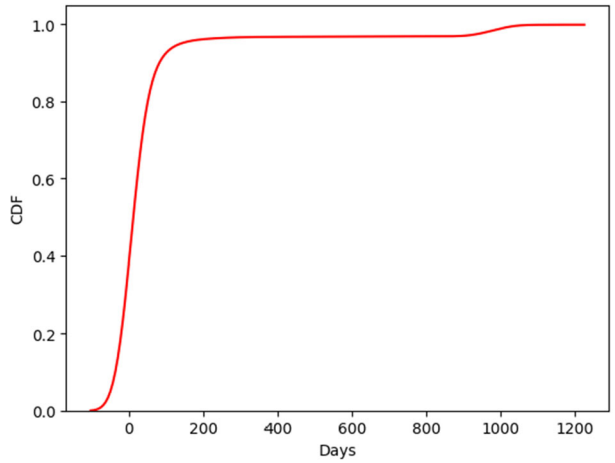
For addresses with zero balance, the time it takes for the ransom to be transferred to another address greatly varies. The cumulative distribution function (CDF) is illustrated in Fig. 4a with Fig. 4b showing that more than a third of the ransom payments are transferred to another address within half a day, whereas half of the payments are transferred to another address within two days. However, the remaining half of the ransom payments took up to three years to transfer the ransom. As a result, almost 95% of the ransom payments are siphoned off within three months of the payment. This is important because slower transfers make things easier for Law Enforcement.

In Table 2, we report the identified exchanges used on these cashing out transactions, their operating status, and the country in which they are based. Moreover, in Fig. 6, we provide a reduced and simplified version of the graph that we extracted regarding the payments for the infamous Wannacry ransomware [49] as analysed with our methodology. As one can observe, based on the intelligence we obtained, the threat actors behind Wannacry, attributed to the APT Lazarus group,[18] cashed out their loot just in two hops; however, the exchange used has not been identified. Nonetheless, after two more hops (four in total), the threat actors cashed out using five different well-known exchanges. This could have been discovered and stopped in near real-time with the current tools and techniques available to us.

As far as the mixers are concerned, only five mixer services were identified, as shown in Table 3. Among them is the notorious Bitcoin Fog (one of the most long-lasting mixers used for money laundering [50]) and [51], both of which have been shut down. The small number of mixers could be attributed to various platform constraints or, most probably, to limitations in the platform's intelligence since several entities up to this depth were not identified.

Finally, regarding the incoming transactions to these 27 ransomware groups, as expected, we identified a number of entities, far more than the ones used for cashing out. These entities range from exchanges to mining pools. In addition, we noticed that many of the incoming transactions were not directly made by the victims. For instance, one would expect

[18] https://attack.mitre.org/software/S0366/.



(a) Cumulative distribution of payments over days.

Period	Percent of transactions
1h	11.22%
12h	35.95%
24h	44.60%
48h	51.79%
Week	64.95%
Month	83.19%
2 Months	88.40%
3 Months	94.06%

(b) A descriptive analysis of the CDF of the ransom payments.

Fig. 4 Cumulative time results for ransom payments to be siphoned off

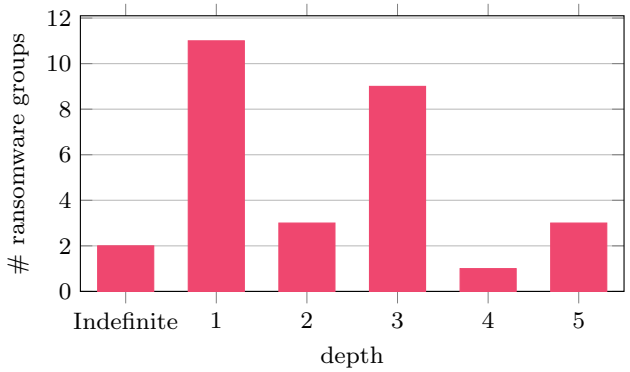


Fig. 5 Depth

a victim to buy some bitcoins directly from an exchange and then pay the ransom. However, in many cases, we noticed two or even three direct transactions before the ransom was paid. We believe this can be attributed to intermediary companies and consultants who negotiated with the ransomware groups for the payments and deliberately obscured the transactions so that victim organisations could not easily be linked to any ransom payment.

Table 2 Identified exchanges

Exchange	Country	Status
Bittrex	USA	Operating
Coinbase	USA	Operating
Bitzlato	Hong Kong	Closed
BTC	USA	Operating
BTC-e	Russia	Closed
CoinPayments	Lithuania	Operating
Epay		Closed
HitBTC	Chile	Operating
Huobi	Seychelles	Operating
Kraken	USA	Operating
Poloniex	USA	Operating
Tidex	UK	Operating
Mexc	Singapore	Operating
MtGox	Japan	Closed
Kucoin	Malaysia	Operating
Kuna	UK	Operating
LocalBitcoins	Finland	Closed
BitPay	USA	Operating
Cryptonator	Hong Kong	Operating
WebMoney		Operating
BitPay	USA	Operating
Exmo	UK	Operating
ChangeNOW	Seyhelles	Operating
QuadrigaCX	Canada	Closed
Cryptoprocessing	Estonia	Operating
YObit	Panama	Operating

6 Discussion and conclusions

Even though the global phenomenon of crypto is frequently described as the preferred tool for criminals such as terrorists, ransomware groups, and money launderers, it has also been argued that "*exaggerating the connection between crypto and crime neither helps to efficiently allocate law enforcement resources nor gives due to the great majority of crypto activity that is legitimate*"[52]. In this respect, it should be underlined that illicit crypto transactions such as ransomware payments constitute a very small fraction of all crypto transactions. Indeed, as illustrated in the latest report by Chainanalysis [10], in terms of all cryptocurrency transaction volume, illicit payments currently constitute only 0.24% of all. As Fig. 7 depicts, despite the peak in 2019, there is a decreasing trend. The latter contradicts [53] by two orders of magnitude, who estimated almost half of the transactions and a quarter of the users as illegal. Contrary to academia, other private sources such as Elliptic [11] and Ciphertrace [54] agree that the scale of illicit transactions is very low, differing slightly depending on the reporting, but with estimates on the scale of 0.5%

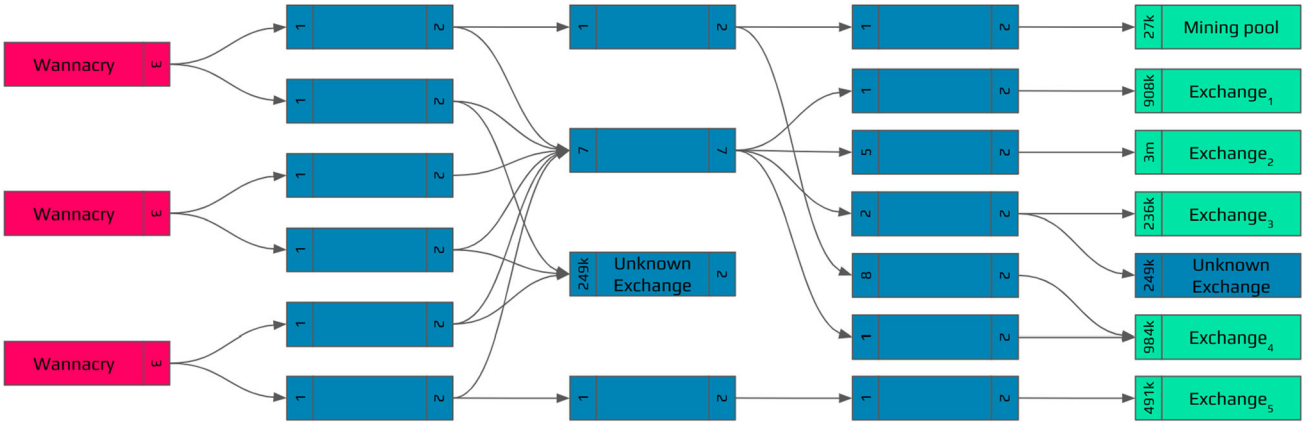


Fig. 6 Simplified version of the Wannacry ransom payments

to 1%. To put this into perspective, fiat money laundering activities annually are estimated by United Nations to be 2–5% of the global GDP [55], which accounts to around $800 billion - $2 trillion. Thus, since the illicit transactions with cryptocurrencies are, according to Chainanalysis' report, in the scale of $20.6 billion, this proportionally constitutes only a minuscule 1.03−2.6% of the total estimated money laundering volume.

Taking the above into account, it has been argued that overestimating cryptocurrencies' risks and ignoring their advantages will not lead to sound policies. Unquestionably, cryptocurrencies—and blockchains in general—like any other technological advancement, need to be carefully studied and regulated to wholly fulfil their promises, reveal all their benefits, and minimise their risks. And even though the pace of blockchain technology and cryptocurrencies' evolution keeps authorities in a permanent reactive position, internationally recognised standards towards their regulation should be appreciated, albeit not blindly.

Beyond any doubt, regulating the constantly changing environment of the cryptocurrency economy is not easy, and—according to several crypto advocates and blockchain experts—it may not even be feasible due to the inherently decentralised nature of blockchain technology based on which there is not any entity in control of their transactions. Obviously, just imposing legal obligations as taken from traditional financial markets may not be a viable option to regulate decentralised cryptocurrencies, which are designed to resist censorship and are antithetical to the existing structure of financial regulation. In addition, one-size-fits-all measures cannot adequately address the wide variety and heterogeneity of cryptocurrencies and the strategies of the businesses evolving around them (i.e. wallet providers, staking pools, exchanges) [1, 56, 57].

Crypto regulation requires a thorough understanding of the stakeholders involved, the kinds of activities carried out, the types of crypto-asset transactions that should be subject to reporting, and all the peculiar features that characterise the crypto-world. Current attempts at regulating this area seem to be impaired by a serious lack in this regard. Taking also into account the ambiguity of blockchain's immutable property compliance with the EU General Data Protection Regulation (GDPR), the efficient regulation of cryptocurrencies seems thus far to be a hard and complicated task [2, 32, 58].

Table 3 Identified mixers, tumblers, and other anonymising services

Service	Status
Bitcoin fog	Closed
BitMixer	Operating
ChipMixer	Closed
Cryptmixer	Operating
Hydra market	Closed
Wasabi wallet	Operating

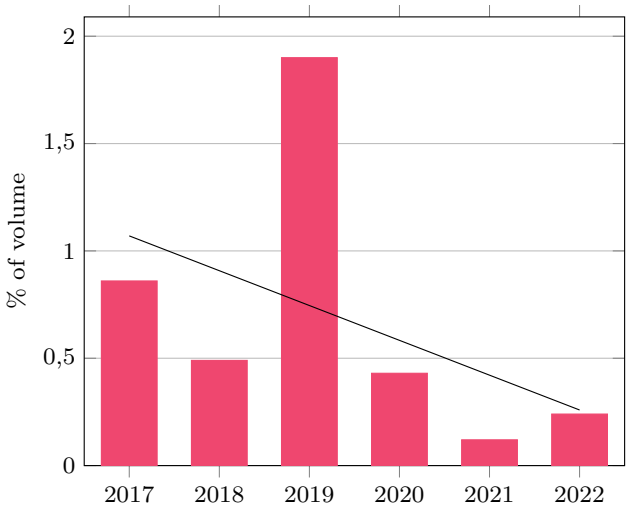


Fig. 7 Illicit share of all cryptocurrency transaction volume, 2017–2022, and the trend line. Adapted from [10]

Most of all, however, banning or aggressively regulating cryptocurrencies will likely only push users to the darker corners of the virtual world. As a matter of fact, pushing strict regulations towards cryptocurrencies bears the risk of cybercriminals shifting their operations to more secure and private alternatives such as Monero, ZCash, Grin, Verge [56, 59], etc. Notably, such a shift would, in some cases, render any traceability actions almost useless blockchain-wise. For instance, the shielded addresses of ZCash, despite their theoretical guarantees, provide some linkability [60, 61], yet it cannot be compared to the easy traceability of Bitcoin. Thus, by trying to strictly regulate cryptocurrencies, we may inadvertently shift illicit transactions to platforms with significantly fewer monitoring capabilities.

Bearing in mind the above considerations, we firmly believe that regulators should strike a better balance between over-regulation and crypto innovation. Towards this goal, in this work, we demonstrated how ransomware payments made in bitcoins can be easily traced and identified with existing tools and methods using real world data. However, one of the major limitations of this work is that the analysis is performed *a posteriori*. On the other side, it would have been quite difficult to perform it in real time, since cryptocurrency exchanges cannot, in many cases, known for certain at the time of payment whether a bitcoin address has been associated with a ransom payment, given that most victims would not have yet notified anyone. Using heuristics at this stage to match these addresses to other well-known payment addresses may be the only possible way to identify these ransom payments. In other words, even if an exchange can observe the same traces as those we used in this work, it is highly unlikely that it would be able to go some hops back and identify with certainty that an address is being used by a ransomware group. This limitation is also intensified by the victims' behaviour, who are often reluctant to report ransomware events, let alone the related addresses. Other limitations stem from the straightforward approach that we adopted in our methodology, for example, the maximum of five hops in our investigation. Although this can, of course, limit the applicability and scope of our findings, we found it to be a good compromise, in particular for improving the explainability of our results. If an exchange has a proper KYC policy in place, a request by Law Enforcement should quickly lead to the identity of the exchange customer involved in criminal activities. Finally, we should bear in mind that the identified entities from exchanges might be linked to straw men that the perpetrators use to withdraw the ransom, exploiting, e.g. gaps in the Know Your Customer processes.

Yet, the above shortcomings do not invalidate our results which attempt to shed light on some aspects of illegal activities exploiting the crypto ecosystem. In fact, one of the key outcomes of our study is that despite the impact of the ransomware groups, cyber criminals end up making the same mistakes that traditional ones make. The arrogance and greed to quickly get hold of the ransom money more than often lead to traceable transactions and entities in just a few hops. As a result, there is additional evidence that can be used not only in the prosecution of perpetrators but also in establishing robust regulations and policies. Above all, our findings underline the prospects for a fair and better regulation of the crypto ecosystem given that, as we have shown, with proper research and analysis, even the darkest corners of illicit activities can be exposed and—by extension—be justly regulated. Hence, regulators can greatly benefit from our analysis which demonstrates an alternative path to over-regulation by providing evidence towards tracing illegal crypto activities such as ransomware.

Acknowledgements This work was supported by the European Commission under the Horizon 2020 Programme (H2020), as part of the project HEROES (https://heroes-fct.eu/) (Grant Agreement No. 101021801) and under the ISF-P Programme, as part of the project CTC (https://ctc-project.eu/) (Grant Agreement No. 101036276). The content of this article does not reflect the official opinion of the European Union. Responsibility for the information and views expressed therein lies entirely with the authors.

Funding Open access funding provided by HEAL-Link Greece.

Data availability The used data are publicly available.

Declarations

Conflict of interest The authors declare no competing interests.

Ethical approval The authors declare full compliance with ethical standards. This article does not contain any studies involving humans or animals performed by any of the authors.

References

1. Alkadri, S.: Defining and regulating cryptocurrency: Fake internet money or legitimate medium of exchange? Duke L Tech. Rev. **17**, 71 (2018)
2. Politou, E., Casino, F., Alepis, E., Patsakis, C.: Blockchain mutability: challenges and proposed solutions. IEEE Trans. Emerg. Topics Comput. **9**(4), 1972–1986 (2019)
3. European Commission.: Eu regulatory framework for crypto-assets. https://ec.europa.eu/info/law/better-regulation/have-your-

say/initiatives/12089-Financial-services-EU-regulatory-framework-for-crypto-assets_en (2020)
4. Andersson, E.: A comparative analysis of the taxation of crypto currencies. Uppsala University, Master Thesis (2020)
5. Renteria, N.: Salvadoran lawmakers pass digital asset issuance law in bitcoin haven. https://www.reuters.com/technology/salvadoran-lawmakers-pass-digital-asset-issuance-law-bitcoin-haven-2023-01-11/ (2023)
6. Gonzalez, D., Hayajneh, T.: Detection and prevention of crypto-ransomware. In: 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), IEEE, pp 472–478 (2017)
7. Howcroft, E.: Crypto ransom attacks rise in first half of 2023, chainalysis says. https://www.reuters.com/technology/crypto-ransom-attacks-rise-first-half-2023-chainalysis-2023-07-12/ (2023)
8. Kshetri, N., Voas, J.: Do crypto-currencies fuel ransomware? IT Prof. **19**(5), 11–15 (2017)
9. Oosthoek, K., Van Staalduinen, M., Smaragdakis, G.: Quantifying dark web shops' illicit revenue. IEEE Access **11**, 4794–4808 (2023). https://doi.org/10.1109/ACCESS.2023.3235409
10. Chainalysis.: The chainalysis 2023 crypto crime report. https://go.chainalysis.com/2023-crypto-crime-report.html (2023)
11. Elliptic.: Financial crime typologies in cryptoassets. https://www.elliptic.co/resources/typologies-concise-guide-crypto-leaders (2020)
12. HSGAC Majority Staff Report (2023) Use of cryptocurrency in ransomware attacks, available data, and national security concerns. https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/HSGAC%20Majority%20Cryptocurrency%20Ransomware%20Report_Executive%20Summary.pdf
13. Connolly, L.Y., Wall, D.S.: The rise of crypto-ransomware in a changing cybercrime landscape: taxonomising countermeasures. Comput. Secur. **87**(101), 568 (2019)
14. Poudyal, S., Dasgupta, D.: Analysis of crypto-ransomware using ml-based multi-level profiling. Ieee Access 9:122,532–122,547 (2021)
15. Kok, S., Abdullah, A., Jhanjhi, N., Supramaniam, M.: Prevention of crypto-ransomware using a pre-encryption detection algorithm. Computers **8**(4), 79 (2019)
16. Olaimat, M.N., Maarof, M.A., Al-rimy, B.A.S.: Ransomware anti-analysis and evasion techniques: a survey and research directions. In: 2021 3rd international cyber resilience conference (CRC), IEEE, pp 1–6 (2021)
17. Oosthoek, K., Cable, J., Smaragdakis, G.: A tale of two markets: investigating the ransomware payments economy. Commun. ACM **66**(8), 74–83 (2023)
18. Cable, J.: Ransomwhere: a crowdsourced ransomware payment dataset. https://doi.org/10.5281/zenodo.6512123 (2022)
19. Haslhofer, B., Stütz, R., Romiti, M., King, R.: Graphsense: a general-purpose cryptoasset analytics platform. Arxiv pre-print (2021)
20. Reid, F., Harrigan, M.: An analysis of anonymity in the bitcoin system. Security and Privacy in Social Networks p 197 (2012)
21. Ron, D., Shamir, A.: Quantitative analysis of the full bitcoin transaction graph. In: Financial Cryptography and Data Security: 17th International Conference, FC 2013, Okinawa, Japan, April 1-5, 2013, Revised Selected Papers 17, Springer, pp 6–24 (2013)
22. Meichler, M.: Binance to delist privacy coins in european countries. https://decrypt.co/142973/binance-delist-monero-zcash-4-european-countries (2023)
23. Crawford, J., Guan, Y.: Knowing your bitcoin customer: money laundering in the bitcoin economy. In: 2020 13th International Conference on Systematic Approaches to Digital Forensic Engineering (SADFE), pp 38–45 (2020)
24. Möser, M., Böhme, R., Breuker, D.: An inquiry into money laundering tools in the bitcoin ecosystem. In: 2013 APWG eCrime researchers summit, Ieee, pp 1–14 (2013)
25. Wu, J., Liu, J., Chen, W., Huang, H., Zheng, Z., Zhang, Y.: Detecting mixing services via mining bitcoin transaction network with hybrid motifs. IEEE Trans. Syst. Man Cybernet. Syst. **52**(4), 2237–2249 (2022)
26. Seo, J., Park, M., Oh, H., Lee, K.: Money laundering in the bitcoin network: Perspective of mixing services. In: 2018 International Conference on Information and Communication Technology Convergence (ICTC), pp 1403–1405 (2018)
27. Hu, Y., Seneviratne, S., Thilakarathna, K., Fukuda, K., Seneviratne, A.: Characterizing and detecting money laundering activities on the bitcoin network. arXiv preprint arXiv:1912.12060 (2019)
28. Wu, L., Hu, Y., Zhou, Y., Wang, H., Luo, X., Wang, Z., Zhang, F., Ren, K.: Towards understanding and demystifying bitcoin mixing services. Procee. Web Conf. **2021**, 33–44 (2021)
29. Hong, Y., Kwon, H., Lee, J., Hur, J.: A practical de-mixing algorithm for bitcoin mixing services. In: Proceedings of the 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts, pp 15–20 (2018)
30. Matera, P.: Delaware's dominance, wyoming's dare: New challenge, same outcome? Fordham J. Corp. Fin. L **27**, 73 (2022)
31. Scarcella, L.: "atch me if i chain": Latest developments in extending reporting obligations and automatic exchange of information to cryptocurrency and crypto-asset transactions. Australian Tax Review-Blockchain Special Issue (2021)
32. Ferreira, A., Sandner, P.: Eu search for regulatory answers to crypto assets and their place in the financial markets' infrastructure. Comput. Law Secur. Rev. **43**(105), 632 (2021)
33. Pavlidis, G.: Europe in the digital age: regulating digital finance without suffocating innovation. Law Innov. Technol. **13**(2), 464–477 (2021)
34. Zetzsche, D.A., Annunziata, F., Arner, D.W., Buckley, R.P.: The markets in crypto-assets regulation (mica) and the eu digital finance strategy. Cap. Mark. Law J. **16**(2), 203–225 (2021)
35. Cengiz, F.: What the eu's new mica regulation could mean for cryptocurrencies. LSE European Politics and Policy (EUROPP) blog (2021)
36. European Parliament Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (recast) Text with EEA relevance. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0065 (2014). Accessed 26 July 2023
37. Mainz, J.: The regulation paradox of the crypto-asset industry: A critical analysis on how the european union is going to resolve the conflicts of interest and regulatory challenges when integrating the new asset class to the scope of regulation. Master's thesis, University of Helsinki, Faculty of Law (2022)
38. European Parliament Tax fraud & evasion- strengthening rules on administrative cooperation and expanding the exchange of information. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12632-Tax-fraud-evasion-strengthening-rules-on-administrative-cooperation-and-expanding-the-exchange-of-information_en (2023). Accessed 26 July 2023
39. Politou, E., Alepis, E., Patsakis, C.: Profiling tax and financial behaviour with big data under the gdpr. Comput. Law Secur. Rev. **35**(3), 306–329 (2019)
40. European Parliament Tax transparency rules for crypto-asset transactions (DAC8). https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2023)739310 (2023). Accessed 26 July 2023
41. Calleja, R.: DAC8 is coming-what crypto stakeholders need to know and do. https://news.bloombergtax.com/daily-tax-report-

international/dac8-is-coming-what-crypto-stakeholders-need-to-know-and-do (2022). Accessed 26 July 2023
42. Kerins S, Murphy B.: DAC8 is coming. https://www.grantthornton.ie/insights/factsheets/dac8-is-coming (2022). Accessed 26 July 2023
43. European Parliament 2021/0241 (COD) information accompanying transfers of funds and certain crypto-assets. https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2021/0241(COD)&l=en (2021). Accessed 26 July 2023
44. OECD.: Taxing virtual currencies: an overview of tax treatments and emerging tax policy issues. https://www.oecd.org/tax/tax-policy/taxing-virtual-currencies-an-overview-of-tax-treatments-and-emerging-tax-policy-issues.htm (2020)
45. Organisation for Economic Co-operation and Development (OECD) OECD seeks input on new tax transparency framework for crypto-assets and amendments to the common reporting standard. https://www.oecd.org/tax/exchange-of-tax-information/oecd-seeks-input-on-new-tax-transparency-framework-for-crypto-assets-and-amendments-to-the-common-reporting-standard.htm (2022). Accessed 26 July 2023
46. Organisation for Economic Co-operation and Development (OECD) Crypto-asset reporting framework and amendments to the common reporting standard. https://www.oecd.org/tax/exchange-of-tax-information/crypto-asset-reporting-framework-and-amendments-to-the-common-reporting-standard.htm (2022). Accessed 26 July 2023
47. Organisation for Economic Co-operation and Development (OECD) Oecd presents new transparency framework for crypto-assets to g20. https://www.oecd.org/newsroom/oecd-presents-new-transparency-framework-for-crypto-assets-to-g20.htm (2022). Accessed 26 July 2023
48. Scorechain (2023) https://www.scorechain.com/
49. Mohurle, S., Patil, M.: A brief study of wannacry threat: Ransomware attack 2017. Int. J. Adv. Res. Comput. Sci. **8**(5), 1938–1940 (2017)
50. Individual arrested and charged with operating notorious darknet cryptocurrency "mixer". https://www.justice.gov/opa/pr/individual-arrested-and-charged-operating-notorious-darknet-cryptocurrency-mixer (2021)
51. Sun, M.: ChipMixer is shut down for allegedly laundering $3 billion in crypto. https://www.wsj.com/articles/chipmixer-is-shut-down-for-allegedly-laundering-3-billion-in-crypto-325a55ee (2023). Accessed 26 July 2023
52. Roberts, D.: Jennifer j. schulp, jack solowey, nicholas anthony, nicholas thielman. https://www.cato.org/blog/overstating-crypto-crime-wont-lead-sound-policy (2023)
53. Foley, S., Karlsen, J.R., Putniņš, T.J.: Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? Rev. Financ. Stud. **32**(5), 1798–1853 (2019)
54. Ciphertrace.: Cryptocurrency crime and anti-money laundering report, February 2021. https://ciphertrace.com/2020-year-end-cryptocurrency-crime-and-anti-money-laundering-report/ (2021)
55. United Nations.: Money laundering. https://www.unodc.org/unodc/en/money-laundering/overview.html (2020)
56. Nabilou, H., Prum, A.: Central banks and regulation of cryptocurrencies. Rev. Bank. Fin. L **39**, 1003 (2019)
57. Nabilou, H.: How to regulate bitcoin? decentralized regulation for a decentralized cryptocurrency. Int. J. Law Inf. Technol. **27**(3), 266–291 (2019)
58. World Economic Forum.: Cryptocurrencies: A guide to getting started. World Economic Forum, Global Future Council on Cryptocurrencies. https://www3.weforum.org/docs/WEF_Getting_Started_Cryptocurrency_2021.pdf (2021)
59. Averin, A., Samartsev, A., Sachenko, N.: Review of methods for ensuring anonymity and de-anonymization in blockchain. In: 2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS), pp 82–87 (2020)
60. Kappos, G., Yousaf, H., Maller, M., Meiklejohn, S.: An empirical analysis of anonymity in zcash. In: Enck W, Felt AP (eds) 27th USENIX Security Symposium, USENIX Security 2018, Baltimore, MD, USA, August 15-17, 2018, USENIX Association, pp 463–477 (2018)
61. Quesnelle, J.: On the linkability of zcash transactions. CoRR abs/1712.01210, 1712.01210 (2017)