School of Informatics

Informatics Research Review
Blockchain and cryptocurrencies: a criminal's friend or foe?

[redacted]

[redacted]

Abstract

The advent of cryptocurrencies marked a new era, not only for the financial industry, but also for way that criminals around the globe operate. In this review, we expose the use and abuse of cryptocurrencies by illegal actors, as it has been recorded in the literature over the years, and then we explore recent academic advancements in the area of Blockchain Analytics, that prove how the same technology can be leveraged in order to detect or even prevent crime.

Date: [redacted] [redacted]

Supervisor: [redacted]

1 Introduction

It has been estimated that more than 20 billion US dollars worth of cryptocurrency were exchanged between criminal entities in 2019 alone.[1] Along with other alarming headlines, that makes one wonder whether this nascent technology is responsible for facilitating crime and, by extent, whether there are any the ethical implications for the people who support it.

Since the introduction of cryptocurrencies in 2008, the ecosystem that surrounds them has been evolving, promoting a libertarian financial system and embracing more and more people into its community. It is no secret though that criminals were among the first ones to adopt this new technology, as they saw it as an opportunity to move their operations online, saving time and effort, cutting back costs and reaching a bigger number of potential victims. Following its more recent mainstream adoption, sources agree that the proportion of blockchain-related criminal activity has been decreasing, but the absolute numbers are still on the rise. [6] [3]

Blockchain experts from both academia and industry have taken it upon themselves to find solutions to this problem, to ensure that this innovative technology can be used to its full potential, without posing a threat to society's public order. An analysis of the Bitcoin chain suggested certain patterns that a criminal is more likely to follow (more and lower-valued transactions than a lawful user, less holdings and repeated transactions with given counterparties), giving hope to the idea of building tools that can automatically tell apart illicit transactions from licit ones.[6]

Through extensive studies of different cryptocurrencies, the technology behind them, as well as the behaviour of their users, researchers from around the globe have come up with heuristics and techniques that can be used to investigate crime in the blockchain ecosystem. We shall shift our focus to the academic work, because of its unbiased and transparent nature, but we cannot disregard the contributions of private companies in the development of such forensic solutions, as their integrated platforms have been of great help to the authorities on several occasions.[2]

The aim of this review is therefore to shed light into *how* and *why* criminals use cryptocurrencies in their activities and evaluate whether the research community has equipped law enforcement with the right tools to battle them. In order to achieve that, we will examine two faces of the literature:

- In section 3, we will present an overview of the criminal activities that have been spotted so far in the blockchain ecosystem and give emphasis on the cryptocurrency properties that have facilitated their growth.
- In section 4, we will highlight that, contrary to popular belief, the use of cryptocurrencies leaves a certain trail behind and we will examine how researchers have leveraged data science, machine learning and behavioural science concepts in order to follow that trail and ultimately build tools that can hand blockchain criminals over to justice.

Section 5 presents our comments and conclusions, while the final section of the review serves as an inspiration towards future research.

We appreciate that technical solutions alone will not suffice in order to confront crime in the blockchain ecosystem; there are many legal aspects that arise in the fight against crypto-crime. It is deemed imperative that governments and regulatory bodies all over the world take action

[1] blog.chainalysis.com/reports/2021-crypto-crime-report

[2] Example of a Blockchain Intelligence product being used for the takedown of a child pornography website: wired.com/dark-web-welcome-to-video-takedown

to provide the institutional framework that is needed [4]; however, we will not cover such issues in our review. We will also not take into consideration criminal activities that don't make use of blockchain systems, but rather similar technologies, such as Tor. For example, a darknet market that uses voucher systems for its payments is out of our analysis's scope.

The review does not assume knowledge of blockchain systems, therefore, in the following section, we will provide some basic background knowledge that is necessary in order to understand the problem at stake and the solutions that are proposed. We do take for granted though that the reader is familiar with some Computer Science terms, such as certain data mining or machine learning techniques.

When it comes to the literature itself, all the papers that we analyse are peer-reviewed and have been presented at conferences or published in esteemed journals. We take special note of the work that has been presented at the USENIX Security Symposium or at the IEEE Symposium on Security and Privacy [7] [8] [18] [16] [15], as they seem to be the most influential conferences on Computer Security and Cryptography.[3] We subsequently follow the research groups behind these papers and discover more relevant, high-quality literature.[9] [11] For supporting facts, we also welcome information from intelligence agencies, such as Europol.[5] We don't find the need to impose restrictions on the papers' publication date, as we are exploring a relatively new field, but any work that is centred around outdated approaches has been intentionally left out. We also do not adhere to a strictly chronological order in our analysis, but rather group the papers based on their content.

2 Blockchain Technology & Cryptocurrencies

The reader of this review need not understand all the technical aspects behind cryptocurrencies. It is important, however, to gain an overview of their traits, in order to understand which of them make them attractive to criminals and which of them can better facilitate law enforcement during investigations. We shall provide a simplified description of how cryptocurrencies work and highlight the key characteristics that set them apart from traditional currencies.

The first cryptocurrency that was created, Bitcoin, was groundbreaking in the way that it used a *peer-to-peer network* in order to validate transactions between parties, eliminating the need for a centralised trusted authority, such as a bank [12]. Transactions in Bitcoin can be made between parties in any different places of the world; there are *no geographical restrictions* or any extra charges for cross-border payments. All transaction fees are determined by the free market and can therefore prove to be *less costly* than the ones imposed by central authorities. The currency is also *accessible* to anyone, regardless of their financial situation, as there are no prerequisites or arbitrary limits involved. In order to be validated, transactions are broadcast to the whole network, therefore all the details about them are *public*, including the sender, the receiver and the amount of the transaction. Once transactions are validated, they become *immutable*, stored in a distributed ledger, referred to as "the blockchain", where they reside everlastingly, without the option to be modified or deleted.

However, there is still assurance that the user's *privacy* is maintained, despite the public nature of the blockchain and its transactions. Figure 1 illustrates that in Bitcoin's privacy model a line is drawn between a user's actual identity and the transactions they make. Public transactions are linked to an identifier that is referred to as the user's address or public key, but they

[3] guide2research.com/topconf/computer-security-cryptography

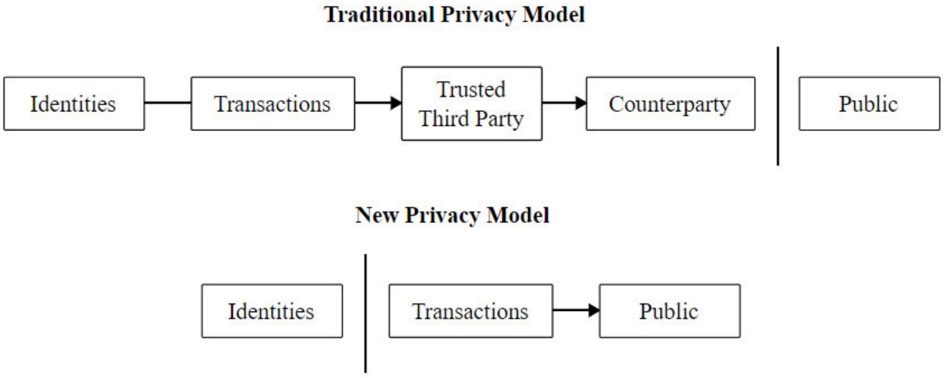

Figure 1: Bitcoin's Privacy Model [12]

are not in any way linked to the user's name, for example. In practice, Bitcoin is considered "pseudonymous", as the address of a user serves as a pseudonym which can be linked to many transactions, but it is often *perceived as anonymous*. Nakamoto in his whitepaper states that the users can maintain their privacy " by keeping [their] public keys anonymous". It is also worth specifying that a user can create an unlimited amount of public keys and use a different one every time, so that their transactions can not be directly linked to each other.

Even though some details vary from cryptocurrency to cryptocurrency, such as the *way* in which the network validates the transactions (referred to as the *consensus mechanism*), the properties we described for bitcoin can be generalised to most, if not all, existing cryptocurrencies, such as Bitcoin Cash, Ethereum and Litecoin.

3 Cryptocurrencies as crime facilitators

In this section, we will try to understand why cryptocurrencies are used by criminals and how they have influenced their activities over time. Countless acts of law violation involving cryptocurrencies have been reported since 2008, including but not limited to: scams and financial frauds, malware attacks, extortions, cybersex trafficking, sales of illegal goods and money laundering. We will go over some of the most common cases and, with the help of the literature, try to answer the following questions for each of them:

- Did this activity predate Bitcoin or was it enabled by this new technology? If it existed before, how has it evolved after the introduction of cryptocurrencies?
- Why do criminals prefer to use cryptocurrencies over traditional forms of payment to conduct this specific activity?

3.1 Ransomware

In its latest Internet Organised Crime Threat Assessment report, Europol identified ransomware as the number one threat in Europe and beyond, when it comes to cybercrime [5].

Ransomware is a type of malware that takes control over a user's personal or business data and asks for a certain ransom to be paid in order for the data to be released. The targets of these attacks are not only end users, but also private and public organisations, such as hospitals. The first reported cases of modern ransomware took place in 2005, years before the arrival of Bitcoin into the scene. Various methods of payments were used at first, such as SMS messages to premium rate numbers or voucher systems. It wasn't until late 2013 that criminals started to ask for the ransom to be paid in bitcoin. [14] Using cryptocurrencies instead of other forms of payment, ransomware criminals had the luxury of targeting any person in the world, regardless of their location, while maintaining their anonymity. [13]

Though we can see that the use of cryptocurrencies is not *essential* for the conduction of ransomware activities, it has been observed that since its adoption as the preferred method for payment, the sector has experienced tremendous growth. Paquet-Clouston et al estimate conservatively that from 2013 to mid-2017 about 23K BTC (more than USD 12M with the exchange rate of that time) was paid as a result of ransomware attacks. [13] At the time of their writing, the authors also reported the existence of 505 different ransomware variants, but, using their sources [4], we can see that the current number is 970, having almost doubled in less than three years' time.

3.2 Ponzi schemes

Another notable form of crime for which cryptocurrencies have been used in the past years is that of financial fraud, in particular through Ponzi schemes. With the promise of high returns on investment, Ponzi schemes aim to attract funds from users, which in turn are used to repay prior investors; when no more funds can be accumulated, the fraudsters run away with the users' investments, causing them severe financial damages.

Ponzi schemes are far from being an aftermath of cryptocurrencies, with their first recorded occurrence dating back to the 19th century. However, cryptocurrencies allegedly resurrected them, giving birth to a "new generation of Ponzi schemes" [5]. Bartoletti et al estimate that within a year's period (2013 - 2014), cryptocurrency Ponzi schemes generated more than USD 7M [2], while the latest report from Europol confirms that ICO scams [6] and Ponzi schemes were the most common cybercrime activities of the past year. Blockchain Analytics company Chainanalysis validates these statements and declares 2019 to be "The Year of the Ponzi Scheme". [3]

Cryptocurrencies are deemed ideal for Ponzi schemes because they remove all geographical barriers and allow the scammers to reach a plethora of potential victims.

3.3 Illegal trade and CaaS

The underground economy was a big problem for the authorities long before cryptocurrencies, or even the internet, came into the scene. Yet, it has been claimed that cryptocurrencies have radically influenced the black market landscape by "enabling black e-commerce". [6] Darknet markets, which in their majority run on cryptocurrencies, give people the opportunity to purchase illegal goods, such as drugs or weapons, from the comfort of their home, without having to reveal their identity.

Silk Road (2011 - 2013) was the first online marketplace to rely on Bitcoin as a form of payment,

[4] id-ransomware.malwarehunterteam.com

[5] wikipedia.org/wiki/Ponzi_scheme

[6] Initial Coin Offering (ICO) scams refer to cryptocurrency companies that raise money from users with the promise of building financial products, but in the end they run away with the money and never deliver on their promises. In some cases, ICO scams can be viewed as a specific category of Ponzi schemes.

but countless others have followed its example ever since, ensuring the overall resilience of online illegal trade, despite the frequent takedowns by law enforcement agencies all over the world. In fact, 2019 marked the year of the highest participation in darknet markets since their creation, resulting in a revenue of over USD 790M worth of cryptocurrency, while at the same time the share of cryptocurrency transactions associated with these markets doubled since 2018. [3]

However, through a specialised study into the effect of darknet markets on drug use, Barratt et al remark that the increased availability of illegal substances in online markets does not *necessarily* imply their increased use. [1] Foley et al build upon that statement and raise the (open) question of whether the overall increased activity that is observed in darknet markets reflects an increased illegal trade or a mere migration of street trading to the online world. In the latter case, one might argue that there are even positive sides of moving illegal activity online, such as decreased street violence or higher-quality (in the sense of safety) drugs. [6]

On another note, cybercriminals are now using dark markets to also sell "merchandise" such as malware, botnets and remote access tools (RATs), both to end users (B2C) and businesses (B2B). This practice has become known as *CaaS* (Cybercrime-as-a-Service) and it serves as an enabler for many aspiring criminals and criminal entrepreneurs, who lack the domain knowledge to implement their malicious ideas from scratch. Van Wegberg et al report that this commoditisation of cybercrime is not yet at alarming levels, especially in B2B contexts, yet they do find evidence that the reduced difficulty of engaging in cybercrime as a result of CaaS leads to increased criminal activity. [16]

We observe that most illegal activities were already well established before the introduction of Bitcoin, yet the adoption of cryptocurrencies opened up new avenues for them, by integrating them into a global market with more potential collaborators and victims and by promising a relatively high degree of anonymity. Although our analysis did not focus on that, we also need to note that, for all criminal activities that are conducted with cryptocurrencies, the greatest facilitator is in fact the inadequate regulation that surrounds them, which makes it easier for criminals to "launder" their acquired assets and get away with their crimes. The landscape could potentially be very different if the right regulatory framework was put in place, but we will leave that on the side for now [4].

4 Blockchains on the side of justice

Blockchain researchers are not oblivious to the alarming number of cryptocurrency transactions that have been linked to criminal activities. During the past few years, increasingly more effort is being invested from academics and industry leaders around the globe into detecting and preventing crime in the blockchain ecosystem. The transparency and immutability of the transactions in blockchains allow the researchers to collect an abundance of data, which can be used to analyse user activity and provide meaningful insights. In the words of Blockchain expert Sarah Meiklejohn, "however you move the money...it's going to be [in the blockchain] forever, so you're giving law enforcement a lot of time to figure it out" [7]

We shall examine the most common practices used to analyse blockchain data as part of an investigation, specifying the challenges that arise along the way and the methods that have been proposed to overcome them. In general, the approaches we will present try to find answers to the following questions:

[7] scientificamerican.com/article/the-imperfect-crime-how-the-wannacry-hackers-could-get-nabbed

- Given a known criminal transaction as a starting point, can we detect the related transactions on the blockchain and trace them all the way to the culprit's wallet? (address linking)
- Can we monitor all transactions on the blockchain and detect the ones that are most likely associated with criminal activity? (address / transaction classification)
- Given a known criminal address, can we prevent its owner from spending their illegally acquired assets? (blacklisting)

4.1 Address linking

One of the most crucial aspects of blockchain forensics is the ability to link users to their transactions. For example, starting from a transaction that pays ransom to a ransomware attacker, we would like to detect the attacker's address and link it to other transactions that might reveal some useful information about them. Initially, this may sound trivial, as we have established that all transaction data are publicly available on the blockchain. However, criminals will often go the extra mile in order to obscure their identity, for example by creating new addresses for each of their transactions.

Meiklejohn et al analyse the dynamics of Bitcoin transactions and come up with a set of heuristics that can be used to link together addresses that are controlled by the same user. Users that choose to receive all their coins in different addresses might end up with very small amounts in each one of them. Therefore, when making a larger payment, they will have to use coins from multiple addresses. The first heuristic takes advantage of this fact and states that when two or more addresses are used as input to a transaction, then they belong to the same user. Taking in one step further, the authors dissect Bitcoin's mechanism for giving back change and remark that the address where the change is sent (generally different from the input address) also belongs to the same user. [9]

Putting these heuristics into action, Kalodner et al integrate them and more in their general-purpose, open-source, blockchain-analysis platform, BlockSci, where they are used in combination with the union-find algorithm in order to produce address clusters in mere minutes. Investigators can use BlockSci to link criminals' addresses, not only in Bitcoin's blockchain, but also in all other cryptocurrencies that work in the same manner (Bitcoin Cash, Litecoin, Namecoin, etc). This constitutes a significant contribution to the research community and many have already adopted BlockSci in order to automate their workflows or to build their domain-specific applications on top of it [8]. [7]

However, the successful linking that can be achieved with the above techniques has led some criminals to abandon "mainstream" coins, such as Bitcoin, and turn their attention to the so-called *privacy coins*, such as Monero and Zcash [15]. This migration urged the academic community to better examine these cryptocurrencies, in order to understand the magnitude of the threat they present.

Researchers from UCL took a deep dive into the transaction chain of Zcash and proved that the majority of its users fail to maintain their anonymity, as they were able to identify more than two thirds of a set of "shielded" z-cash transactions, using a set of 5 heuristics [8]. Respectively for Monero, Möser et al discovered two vulnerabilities in its blockchain that can compromise the users' privacy and enhance the overall traceability of its transactions. They estimate that using

[8] For a complete list of papers and applications that have already integrated BlockSci in their workflows see section 3.5 of [7]

their heuristics, they can expose the obscured inputs of up to 80% of the total transactions in Monero. [11] However, all authors agree that there are measures than can be taken by the users of these cryptocurrencies, in order to increase their anonymity and possibly disrupt the address linking techniques that have been so far developed.

Another challenge arises in address clustering when criminals move their funds across different cryptocurrency ledgers (especially to privacy coin ledgers), in an attempt to conceal their source. Normally, that would not be a problem, as exchanges are now required by law to store their clients' identification data and could provide them to the authorities in the case of an investigation. However, new platforms have emerged that allow trading with decentralised exchanges, without revealing any personal data. [9].

Still, researchers from UCL [18] found that users who combine cross-chain transactions with privacy coins to enhance their anonymity usually do not take the necessary precautions (e.g. they use the same address more than once), thereby leaving trails behind and not achieving their purpose. Using data obtained from public APIs (1.3M cross-chain transactions) in combination with simple heuristics (matching exact amounts, similar timestamps, etc), they managed to link 76 - 90 % (depending on the involved coin) of input transactions to output transactions. More advanced heuristics linked input to output transactions even if they were products of more complex user behaviour, such as exchanging from currency A to currency B and then right back to A (referred to as a "u-turn" in the paper). It is worth noting that the authors used BlockSci in order to parse and analyse blockchain data.

4.2 Address classification

While clustering addresses can help investigators follow leads and gather information about suspects, it is not useful for determining whether an unknown transaction is in violation of the law or not. It would be very handy for the authorities to have tools that can monitor on-chain transactions and inform them about potential illicit activities.

The techniques we presented for address linking can not be directly generalised to fit this problem, but they can serve as the first step towards a solution. All the approaches we will discuss below use heuristics (either the ones that were mentioned above or similar ones) in order create clusters of addresses, which they later classify as licit or illicit. Overall, Random Forests seem to be the most successful classifiers for this task, but other methods are also proposed. A common problem found in this classification task is the inherent imbalance of the two classes, as illicit transactions, albeit plenty, only account for a small portion of the total cryptocurrency transactions (1.1% in 2019 according to Europol [5]). In order to deduce some ground truth for their respective datasets, the researchers used publicly available data, such as police reports of Bitcoin seizures.

Bartoletti et al applied data mining techniques for the automatic detection of Ponzi schemes in Bitcoin's blockchain. They experimented with multiple techniques, both for the classification itself and for overcoming the class imbalance problem and observed that the best performers were Random Forests that integrate a cost matrix in their learning that penalises false negatives 20 times more than false positives. This model successfully identified 31 out of 32 Ponzi schemes from a pool of more than 6K clusters of addresses. Proving that automatic Ponzi scheme detection is possible in the Bitcoin system, the authors make a significant contribution that could potentially be generalised to other cryptocurrencies, such as Ethereum, or other crimes, such as ransomware. [2]

[9] One such platfrom is Shapeshift: https://shapeshift.com/

Independently, researchers from MIT, in collaboration with Blockchain Intelligence company Elliptic, experimented with Graph Convolutional Networks (GCNs) for the classification of more than 150K Bitcoin transactions as *licit* or *illicit*. In order to overcome the class imbalance issue, they trained their model using a weighted cross entropy loss, thereby boosting the significance of the illicit samples in their training set. Despite promising results, GCNs did not perform as well as Random Forests, but the authors invite research in combining the two approaches for a potential performance gain. Another key takeaway from their work is the integration of temporal dynamics in the prediction model, as they split their data into distinct time steps, showing that information from the past can be used to predict the overall criminal activity in the future. Last but not least, the authors shared "The Elliptic Data set" with the research community, which is now the largest public dataset of bitcoin transactions with labels and handcrafted features.[17]

4.3 Towards Blacklisting

Once a cryptocurrency address has been declared as *illicit* (for example after a dark market shutdown by the police), ideally we would like to prevent the criminally-acquired money from getting spent, thereby lowering the criminal's incentive to commit anotherh crime. In order to accomplish that, the use of a *blacklist* has been proposed, where all illicit addresses would be registered and the funds they hold would be deemed *tainted* and subsequently refused by recipients. Platforms, such as EthProtect[10] and CryptoScamDB (formerly EtherScamDB)[11] are already doing something similar, by keeping track of known malicious cryptocurrency addresses and making them available to the public.

Aside from the controversy that surrounds blacklisting[12], there are some technical difficulties that are bound to emerge in an ecosystem that supports them. Möser et al explore the dynamics of a market where blacklisting Bitcoin addresses is the norm and observe that accepting non-tainted coins might still pose a threat, as there is a possibility that they will get tainted later on (e.g. following an investigation). They make the first steps towards a scoring scheme that aims to predict the risk of a certain coin to get blacklisted and therefore help the recipient of that coin make an informed decision on whether or not to accept it. As a first attempt, they used indicators, such as transaction values, obfuscation patterns and frequency of usage to allocate scores to clusters of transactions, but they only tested their model against 3 known occurrences of blacklisting, therefore leaving its validation subject to further research. [10].

5 Conclusion

After examining extensive literature on blockchain-related crime, we confirm that by enabling cheap and fast cross-border transactions, while guaranteeing their users a certain degree of anonymity, cryptocurrencies have facilitated the growth of certain illegal activities, such as cyber extortion or online illegal trade. It remains unclear whether crime in its entirety has been amplified as a result of this new financial system or merely transformed to fit in with the modern digital era.

In response to the association of blockchain technologies with illegal activities, experts around the globe have shifted their focus on devising forensic solutions that could aid law enforcement in

[10] info.etherscan.com/ethprotect

[11] cryptoscamdb.org

[12] coindesk.com/bitcoin-tracking-proposal-divides-bitcoin-community

their battle against crypto-crime. Using advanced heuristics and data mining techniques, they have managed to link cryptocurrency users to the ensemble of their transactions (even in cases of deliberate obfuscation), determine whether a given transaction is associated with criminal activity, and even propose pathways towards an ecosystem that prevents criminally-acquired assets from getting spent.

While there has been great success in tracing criminal activity linked to certain cryptocurrencies, such as Bitcoin, academic and industry leaders acknowledge that the emergence of new privacy-enhanced coins threatens to leave researchers and law enforcement one step behind criminals. Fortunately, preliminary research works suggest that there are hopes of extending the existing techniques to cover even such cases and help take the lead in this ongoing arms race.

Last but not least, we note that, even though a dedicated crime-tailored solution is yet to be introduced to the open-source community, the recent development of a general-purpose blockchain-analysis platform, namely BlockSci, already provides plenty of forensic capabilities and lays the foundations for more.

6 Future work

There are plenty of potential research topics that arise from our conclusions. We shall leave aside the obvious criminology-related question of better understanding the impact of blockchain technologies on the global illegal scene and rather focus on what can be done to tackle the technical challenges that have emerged.

As a first step, it would be useful to make a comprehensive comparison of the different techniques that have been proposed (e.g. for address clustering) and validate them against the same dataset, to make their performance differences more clear. A candidate dataset for this purpose would be the one provided by Weber et al, as it is currently the largest open-source dataset of Bitcoin transactions that includes labels and a multitude of useful features.

Additionally, we have seen that the majority of research work so far has been devoted specifically to Bitcoin, but as several other cryptocurrencies have gained significant popularity, it is deemed necessary to conduct more research around them, especially considering how a lot of the proposed methods can not be directly generalised to different blockchains. A useful application, for example, would be to extend BlockSci (or develop another general-purpose blockchain-analysis tool) to work with smart contract platforms, such as Ethereum.

Once the research around blockchain forensics fully matures, we also expect the open source community to be enriched with fully integrated, crime-tailored blockchain-analysis platforms, that will eventually help to reduce criminality levels in the era of cryptocurrencies.

References

[1] Monica J. Barratt, Simon Lenton, Alexia Maddox, and Matthew Allen. ‘What if you live on top of a bakery and you like cakes?’—Drug use and harm trajectories before, during and after the emergence of Silk Road. *International Journal of Drug Policy*, 35:50–57, 9 2016.

[2] Massimo Bartoletti, Barbara Pes, and Sergio Serusi. Data mining for detecting bitcoin ponzi schemes. In *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, pages 75–84. IEEE, 2018.

[3] Chainanalysis. The 2020 state of crypto crime, 2020.

[4] Primavera De Filippi De Filippi. *Blockchain and the law: The rule of code.* Harvard University Press, 2018.

[5] Europol. Internet organised crime threat assessment (iocta). *Europol European Police Office, Hague, The Netherlands, Tech. Rep*, 2020.

[6] Sean Foley, Jonathan R Karlsen, and Tālis J Putniņš. Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? *The Review of Financial Studies, Oxford University Press*, 32(5):1798–1853, 2019.

[7] Harry Kalodner, Malte Möser, Kevin Lee, Steven Goldfeder, Martin Plattner, Alishah Chator, and Arvind Narayanan. Blocksci: Design and applications of a blockchain analysis platform. In *29th {USENIX} Security Symposium ({USENIX} Security 20)*, pages 2721–2738, 2020.

[8] George Kappos, Haaroon Yousaf, Mary Maller, and Sarah Meiklejohn. An empirical analysis of anonymity in zcash. In *27th {USENIX} Security Symposium ({USENIX} Security 18)*, pages 463–477, 2018.

[9] Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M Voelker, and Stefan Savage. A fistful of bitcoins: characterizing payments among men with no names. In *Proceedings of the 2013 conference on Internet measurement conference*, pages 127–140, 2013.

[10] Malte Möser, Rainer Böhme, and Dominic Breuker. Towards risk scoring of bitcoin transactions. In *International Conference on Financial Cryptography and Data Security*, pages 16–32. Springer, 2014.

[11] Malte Möser, Kyle Soska, Ethan Heilman, Kevin Lee, Henry Heffan, Shashvat Srivastava, Kyle Hogan, Jason Hennessey, Andrew Miller, Arvind Narayanan, et al. An empirical analysis of traceability in the monero blockchain. *Proceedings on Privacy Enhancing Technologies*, 2018(3):143–163, 2018.

[12] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. Technical report, Manubot, 2019.

[13] Masarah Paquet-Clouston, Bernhard Haslhofer, and Benoit Dupont. Ransomware payments in the bitcoin ecosystem. *Journal of Cybersecurity*, 5(1):tyz003, 2019.

[14] Ronny Richardson and Max M North. Ransomware: Evolution, mitigation and prevention. *International Management Review*, 13(1):10, 2017.

[15] Eli Ben Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza. Zerocash: Decentralized anonymous payments from bitcoin. In *2014 IEEE Symposium on Security and Privacy*, pages 459–474. IEEE, 2014.

[16] Rolf Van Wegberg, Samaneh Tajalizadehkhoob, Ugur Akyazi, Carlos Hernandez Ganan, Bram Klievink, Kyle Soska, Carlos Gañán, Nicolas Christin, Michel Van Eeten, M J G Vanwegberg, r S and Tajalizadehkhoob, S T and Akyazi, U and Hernandezganan, C and Klievink, A J and Vaneeten}, and @tudelft Nl. *Plug and Prey? Measuring the Commoditization of Cybercrime via Online Anonymous Markets.*

[17] Mark Weber, Giacomo Domeniconi, Jie Chen, Daniel Karl I Weidele, Claudio Bellei, Tom Robinson, and Charles E Leiserson. Anti-money laundering in bitcoin: Experimenting with graph convolutional networks for financial forensics. *arXiv preprint arXiv:1908.02591*, 2019.

[18] Haaroon Yousaf, George Kappos, and Sarah Meiklejohn. Tracing transactions across cryptocurrency ledgers. In *28th {USENIX} Security Symposium ({USENIX} Security 19)*, pages 837–850, 2019.