RAND EUROPE

# Exploring the use of Zcash cryptocurrency for illicit or criminal purposes

Erik Silfversten, Marina Favaro, Linda Slapakova,
Sascha Ishikawa, James Liu, Adrian Salas

For more information on this publication, visit www.rand.org/t/RR4418

Published by the RAND Corporation, Santa Monica, Calif., and Cambridge, UK

RAND Europe is a not-for-profit research organisation that helps to improve policy and decision making through research and analysis. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

# Preface

Cryptocurrencies are currencies that only exist digitally, usually have no central issuing or regulating authority, and rely on cryptography to prevent counterfeiting and fraudulent transactions. While today they are increasingly used for legitimate purposes, cryptocurrencies have also attracted the attention of individuals and organisations that are engaged in criminal or illicit activities both on and off the dark web. To inform public debate, this report explores the illicit or criminal use of cryptocurrencies, with a particular focus on Zcash.

This independent research study was sponsored by the Electric Coin Company (ECC)—the creator of Zcash. It was conducted by the not-for-profit research institute RAND – comprising both RAND Europe and the US-based RAND Corporation. RAND is an independent, non-partisan research organisation that helps to improve policy and decision making through objective research and analysis. RAND's evidence-based publications do not reflect the opinions of its research clients and sponsors.

This report should be of interest to criminologists, law enforcement professionals, policymakers, regulators and others with an interest in cryptocurrencies.

For more information on the study, or RAND, please contact:

Erik Silfversten
Senior Analyst
RAND Europe
Westbrook Centre, Milton Road
Cambridge CB4 1YG
United Kingdom
erik_silfversten@randeurope.org
www.rand.org

# Summary

This measured and evidence-based study evaluates the potential risks and benefits of new and existing cryptocurrencies. A cryptocurrency is a form of currency that only exists digitally, usually without a central issuing or regulating authority, and which relies on cryptography to prevent counterfeiting and fraudulent transactions. The creation of cryptocurrencies has been recognised as a promising financial innovation and a potential new vehicle for increased economic freedom and opportunities, including facilitating global remittances and payments, preventing unlawful seizures of wealth, and helping to hedge against hyperinflation of local currencies.[1] However, cryptocurrencies have also been subject to criticism and recognised as a potential vehicle for fraud, organised crime and other illicit activities if the underlying technologies are not appropriately implemented and managed.[2] While there are widespread suspicions of the use of cryptocurrencies for illicit purposes, the specific nature and scale of the connections between cryptocurrencies and criminal or illicit use remain poorly understood both in research and the wider public awareness. As such, a proportional and evidence-based response is required to balance the potential risks and benefits of novel cryptocurrencies.

Within this context, the Electric Coin Company (ECC) commissioned not-for-profit research institute RAND – comprising both RAND Europe and the US-based RAND Corporation – to undertake a study exploring the use of its Zcash cryptocurrency for illicit or criminal purposes. Zcash is a digital currency invented and built with the stated aim to 'empower everyone with economic freedom and opportunity'. Since its launch in 2016, Zcash has become supported by several regulated exchanges and providers, including New York State Department of Financial Services-regulated Gemini, Coinbase and Bitgo.[3] The study focused on two overarching aspects to examine the evidence base on:

- **How cryptocurrencies may be used for illicit or criminal purposes**, and how this use materialises.
- **To what extent Zcash is used for illicit or criminal purposes**, and how such usage compares with other cryptocurrencies such as Bitcoin, Ethereum, Litecoin and Monero.

[1] Leonard & Treiblmaier (2019), Dorofeyev et al. (2018).

[2] Foley et al (2019), Aldridge & Décary-Hétu (2016).

[3] See https://z.cash/

The research included an extensive literature review of academic sources and news reports on cryptocurrencies and their illicit uses, as well as key informant interviews with a range of academic and industry cryptocurrency experts. In addition, the research team also collected and examined primary data on dark web[4] marketplaces and forums in order to identify ways in which cryptocurrencies are used for or in support of illicit activities, as well as to identify the nature and estimated scope of the illicit use of Zcash compared to other cryptocurrencies. Finally, factors that may influence future illicit use of Zcash were also identified and examined.

## Research into the use of cryptocurrencies for illicit or criminal purposes highlights its suitability for money laundering, trade in illicit goods and services, and terrorism financing

Research into the illicit or criminal use of cryptocurrencies is fundamentally challenged by the intrinsic characteristics of cryptocurrencies, and the concealed nature of the dark web in general and of many criminal activities in particular. Data are oftentimes difficult to access or insufficient, marketplaces may be taken offline due to law enforcement action, and privacy-preserving technologies may render users, transactions or other activities anonymous. By definition, too, the most successful illicit or criminal uses of cryptocurrencies or any other technology will be those that escape detection altogether by victims, law enforcement and the research community.

While the majority of transactions made with virtual coins are legitimate, this study has shown that cryptocurrencies are also used for a wide range of illicit or criminal purposes by a diverse group of malicious actors. Most commonly this includes:

1. **Money laundering:** Though national currencies and other digital technologies present equal if not greater money laundering challenges, cryptocurrencies are often perceived to represent attractive opportunities for money laundering. This is due to their decentralised and (pseudo-)anonymous characteristics. In contrast to conventional mechanisms, the benefit of cryptocurrency money laundering, or 'cryptolaundering', is that it circumvents geographic constraints and exploits the gaps or overlaps between heterogeneous regulatory frameworks.
2. **Trade in illicit goods and services:** The advent of dark web marketplaces has offered sellers of illicit goods and services new distribution channels that enable them to transact with customers globally online. These marketplaces have been found to offer a wide range of goods and services in exchange for cryptocurrencies, including drugs and controlled substances, explosives and weapons, ivory and wildlife trafficking, antiquities, and child sexual abuse material. Dark web marketplaces additionally offer opportunities to purchase a wide range of online 'crime-as-a-service' and cyber products such as exploit kits, Distributed Denial of Service (DDoS) services, or phishing tools.
3. **Terrorism financing:** The use of cryptocurrencies in terrorism financing

[4] The dark web is a part of the Internet that is not indexed by search engines. Specific browsers like Tor are required to access dark web sites, which contain anonymous message boards, online marketplaces for the purchase of illicit goods and services, exchanges for stolen financial and private data, and other illegal content.

has been a growing concern for regulators and for wider counterterrorism efforts. A number of terrorist organisations have been reported to have increased their interest in cryptocurrencies and to have used cryptocurrencies for soliciting funds from sponsors and supporters. Partly, the use of cryptocurrencies represents a new method of moving funds in a faster, more anonymous and global way that may be less constrained by international and national Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) regulation. However, recent research has shown that the use of cryptocurrencies for terrorist financing is largely episodic and not as widespread as could be assumed, as compared to more traditional means.

## Zcash is a cryptocurrency that uses zero-knowledge proofs to provide enhanced privacy for its users, however, there is little evidence that this is exploited by malicious actors

Zcash (ZEC) is a digital currency and so-called privacy coin launched in October 2016 as a code derivative of Bitcoin. Zcash operates in an 'opt-in' privacy construct where funds are either transparent or shielded, and the user can choose between the two options. Transparent funds are subject to similar privacy features to Bitcoin, whereas shielded funds feature stronger privacy-preserving features that seek to ensure that personal and transaction data remain completely confidential. The aim for privacy coins such as Zcash is to provide better privacy protections intended to benefit legitimate users who do not want their financial details made public. While intuitively it would seem likely that privacy coins would be the cryptocurrency of choice for malicious actors, due to their purported anonymity-preserving features, there has been little research or evidence to substantiate this claim.

This study explored how and the extent to which Zcash is used for illicit or criminal purposes (i.e. the scope, scale and nature of this phenomenon). In doing so, a number of key findings emerged:

- **Zcash is relatively unknown in the academic research community** and the links between Zcash and illicit or criminal activities have not been subject to substantial research. This may be due to a lack of awareness or understanding of Zcash from the research community or perhaps due to low levels of actual use of Zcash for illicit or criminal purposes, though both hypotheses remain untested. Crucially, the absence of evidence does not equal evidence of absence, meaning that the fact that there is little proof that Zcash is used for illicit or criminal purposes does not mean it is not happening; rather, this activity is simply not being detected.
- **This research has not identified any credible evidence pointing to large-scale use of Zcash for money laundering, terrorism financing or the trade in illicit goods and services.** While there are certainly some indications or anecdotal evidence that Zcash may have been used or advertised for illicit purposes, there is no evidence of widespread illicit use of Zcash. Of course, absence of evidence does not equate to evidence of absence, meaning that enduring vigilance against malicious use of this cryptocurrency is nonetheless important.
- **While previous research has shown clear links between cryptocurrencies and illicit activities on the dark web, Zcash has only a minor presence on the reviewed marketplaces and forums.** This does not

necessarily mean that Zcash is not used for illicit or criminal purposes on the dark web, but it indicates that Zcash is seen as a less attractive option to dark web users and is used less often compared to other cryptocurrencies, particularly Bitcoin and Monero.

- **Users engaged in illicit activities either may not fully understand the Zcash operating model,** the value in Zcash's privacy-preserving features, or else are not aware or confident in them.
- **Bitcoin is still perceived to be the dominant cryptocurrency** for illicit or criminal activities on the dark web, notwithstanding recent developments in the cryptocurrency environment, such as the advent of several more privacy-focused cryptocurrencies.

## There are a range of factors that may influence the future use of Zcash for illicit or criminal purposes

While there are few indications that Zcash is currently used for illicit or criminal purposes, this may change in the future – either as patterns of use change or as new data on those patterns comes to light. The academic research and interviewees consulted as part of this study presented a range of speculative factors that could affect the likelihood Zcash being used over other cryptocurrencies for illicit purposes in the future, including:

- **Bitcoin hegemony and network effects:** Notwithstanding the advent of privacy-preserving cryptocurrencies, criminals engaged in illicit activities are still primarily drawn to Bitcoin due to the structural incentives that the widely-used Bitcoin's critical mass creates for criminals.
- **Ease of use of Zcash:** While privacy coins may theoretically seem a boon to users engaged in illicit or criminal activities, various practical considerations may in fact make them less attractive for conducting illicit transactions on the dark web.
- **Degree of anonymity of Zcash:** There exists some public scepticism as to how anonymous Zcash truly is and whether future research will identify weaknesses in its privacy features.
- **Evolution of criminal behaviours:** Research suggests that Zcash's use for illicit or criminal purposes may in part be limited due to a lack of understanding of the underlying technology on the part of its users. As malicious actors become more sophisticated in their knowledge and skills regarding cryptocurrencies, or if wider exogenous changes in criminal tactics change (e.g. if for some reason there was an exodus from other cryptocurrencies or fiat currencies), it will presumably have a direct effect on Zcash.
- **Perceptions and branding of Zcash:** While different privacy coins may be perceived by criminals as offering similar levels of anonymity, the governance of Zcash and its branding by ECC as compliant with the relevant AML/CFT regulations may make it less susceptible to exploitation for illicit or criminal purposes.

Moreover, it seems that wider market conditions, rather than the specific characteristics of any one cryptocurrency, may also be a predominant driver for cryptocurrency adoption on the dark web. While it makes intuitive sense that privacy coins such as Zcash might be adopted en masse for criminal and illicit purposes, the limited research that exists in this space indicates that criminals are more likely to 'go where the money is'. That is to say that Bitcoin, which has to date captured the largest market share among cryptocurrencies, has reached a critical mass for both legitimate and illegitimate transactions. At the same time, actions by law enforcement, regulators and the ECC and others can also proactively shape both market and criminal behaviours. Effective action presumes a nuanced and up-to-date understanding of the dynamics of both. However, this study also found that analysis of the use of cryptocurrencies for illicit or criminal purposes remains an emerging field of research, particularly in relation to younger cryptocurrencies such as Zcash.

## Avenues for future research within this emerging field

Given that there has been little to no research on the use of the Zcash cryptocurrency for illicit or criminal purposes in the past, there are many potential avenues for further study. The following are a few examples of lines of inquiry that would augment the evidence base for future studies:

- **Improvements to mechanisms for data gathering and more accurate estimates of the extent of the use of cryptocurrencies** would enable a more robust and nuanced understanding of the scope of the issue, thereby facilitating the development of appropriate policy responses.
- **Transparency in methodological approaches** is crucial in different studies that examine the extent to which cryptocurrencies are used on the dark web. Continuing to enhance efforts to promote transparency and information sharing within the research community will be vital in establishing trustworthiness of a given source and triangulating information from various sources.
- **A stronger theoretical basis for research on cybercrime** is needed more widely including, for example, integration of relevant research and conceptual approaches from related fields such as criminology. This could include research around the behaviour of criminals, such as reluctance towards the early adoption of new technology or general adversity to risk.
- **A more sophisticated understanding of the suitability of privacy coins for conducting illicit and criminal activities** would also enable a more granular understanding of the different drivers that shape malicious actors' selection of one cryptocurrency over another for their purposes. This should include an examination of the numerous privacy coins and the variety in their suitability.

# Table of contents

# List of figures, tables and boxes

# Abbreviations

| | |
|---|---|
| AML | Anti-Money Laundering |
| BCH | Bitcoin cash |
| BTC | Bitcoin |
| CFT | Countering the Financing of Terrorism |
| DDoS | Distributed Denial of Service |
| DWM | Dark Web Monitor |
| DWO | RAND Dark Web Observatory |
| ECC | Electric Coin Company |
| ETH | Ethereum |
| FATF | Financial Action Task Force |
| ICO | Initial Coin Offering |
| KYC | Know Your Customer |
| LTC | Litecoin |
| UX | User experience |
| XMR | Monero |
| ZEC | Zcash |
| zk-SNARK | Zero-Knowledge Succinct Non-Interactive Argument of Knowledge |

# Acknowledgements

RAND reports typically draw on a wide collection of supporters and collaborators in their creation. The authors would first like to mention the invaluable insights provided by those who took the time to share their knowledge of the illicit use of cryptocurrencies and Zcash, many of whom are listed in the annex to this report. Within RAND, our reviewers, Jacopo Bellasio and James Black, offered insightful advice that improved the report, while Richard Flint assisted with data visualisation and Jess Plumridge helped to format and edit the final report document.

Finally, this study could not have been possible without the sponsorship and ongoing support of the Electric Coin Company, and in particular Josh Swihart and Jack Gavigan.

Despite these many valued contributions, any errors or omissions in the analysis presented in this report remain the sole responsibility of the authors.

# 1 Introduction

The creation of decentralised cryptocurrencies offers promises of digital currencies that can operate without a central bank and without the need for intermediaries, as well as bringing a number of potential security and privacy benefits. Recognised as a promising financial innovation and a potential new vehicle for increased economic freedom and opportunity, cryptocurrencies have been subject to significant media and investment attention and speculation (in all senses of the term).[5] However, they have also been subject to criticism and recognised as a potential vehicle for fraud, organised crime and other illicit activities if the underlying technologies are not appropriately implemented and managed.[6]

Many high-profile cryptocurrencies have become prominent payment methods on the dark web[7] and other illicit markets. In such marketplaces, users can buy and sell a wide array of illegal goods, including narcotic or other illicit substances, explosives, firearms, illegal pornography, fake or stolen identities, and hacking exploits. There have also been concerns that cryptocurrencies have been or might in future be used to support terrorist organisations in their efforts to finance, plan and perpetrate terrorist attacks.[8] However, while there are widespread suspicions of the use of cryptocurrencies for illicit purposes, the privacy-focused foundations of cryptocurrencies and the practicalities of their use (e.g. covertly through the dark web) make it challenging to truly understand the nature and scope of the problem, including the differences in criminal usage and perceptions of different types of cryptocurrency.[9] Indeed, by definition, the most successful illicit or criminal uses of cryptocurrencies or any other technology will be those that escape detection altogether by victims, law enforcement and the research community.

## 1.1. Focus of this report

As previously mentioned, this independent research study was commissioned by the Electric Coin Company (ECC), who developed

[5] Leonard & Treiblmaier (2019), Dorofeyev et al. (2018).

[6] Foley et al. (2019), Aldridge & Décary-Hétu (2016).

[7] The dark web is a part of the Internet that is not indexed by search engines. Specific browsers like Tor are required to access dark web sites, which contain anonymous message boards, online marketplaces for the purchase of illicit goods and services, exchanges for stolen financial and private data, and other illegal content.

[8] Dion-Schwarz et al. (2019).

[9] Foley et al. (2019).

and maintain Zcash. However, it is critical to note that RAND's publications do not reflect the opinions of its research clients and sponsors. Rather, this proportional and evidence-based report is intended to inform public debate and decision making with regard to the use of cryptocurrencies for criminal or illicit activities, both on and off the dark web. In particular, this study focuses on the use of the Zcash cryptocurrency for illicit or criminal activities, which addresses a significant gap in the existing evidence base. Intuitively, privacy coins such as Zcash would seem like an attractive vehicle for criminality, but this report will demonstrate that there is insufficient empirical research to test this hypothesis.

This report focuses on two key questions:

1. **How cryptocurrencies may be used for illicit or criminal purposes**, and how this use materialises.
2. **To what extent Zcash is used for illicit or criminal purposes**, and how such usage compares with other cryptocurrencies such as Bitcoin, Ethereum, Litecoin and Monero.

## 1.2. Research approach and methodology

To address these research questions, the study team leveraged the in-house expertise and toolkit of the RAND Dark Web Observatory (DWO).[10] This enabled the collection and examination of primary data on dark web marketplaces and forums. The research team used this data to identify ways in which cryptocurrencies are used for or in support of illicit activities. The data was analysed to identify the nature and scope of the illicit use of Zcash compared to other cryptocurrencies.

In addition, the team also conducted an extensive literature review of scholarly works and news reports on cryptocurrencies and their illicit uses. In total, 226 sources were shortlisted and reviewed. Furthermore, researchers also interviewed 15 academic and industry experts in the cryptocurrency field to capture their insights and perspectives. Based on all these inputs, the factors that may influence future illicit use of Zcash were also identified and examined.

A more detailed overview of the study methodology can be found in Annex A.

## 1.3. Structure of this report

This introductory chapter provides the study context as well as an overview of the specific research questions and approach undertaken. This report features four additional chapters:

- **Chapter 2:** The illicit use of cryptocurrencies
- **Chapter 3:** The use of Zcash for criminal or illicit purposes
- **Chapter 4:** Factors that may influence the future use of Zcash for illicit purposes
- **Chapter 5:** Conclusions

Finally, the report is complemented by a full bibliography and two annexes providing the reader with further information on the following:

- **Annex A:** Methodology
- **Annex B:** List of key informant interviewees

[10] Building on RAND's extensive research into the illicit use of dark web markets (e.g. for terrorism, narcotics  or the sale of illegal firearms and explosives ), the Dark Web Observatory (DWO) houses a primary data collection tool (i.e. a dark web crawler and scraper) and acts as a database and knowledge repository that RAND researchers can use to study the dark web.

# 2 The illicit use of cryptocurrencies

This report will first explore the evidence for the illicit use of cryptocurrencies broadly before focusing on Zcash specifically. In doing so, we will be in a position to identify the specific properties of Zcash which differentiate it from other cryptocurrencies when used for criminal or illicit purposes. This chapter, therefore, discusses the types of illicit uses of cryptocurrencies and the malicious actors who use cryptocurrencies for criminal or illicit purposes.

## 2.1. Cryptocurrencies have emerged as popular alternative payment mechanisms for both licit and illicit purposes

Since the introduction of Bitcoin, cryptocurrencies have emerged as popular alternative payment mechanisms. Cryptocurrencies refer to 'any form of currency that only exists digitally, that usually has no central issuing or regulating authority but instead uses a decentralized [sic] system to record transactions and manage the issuance of new units, and that relies on cryptography to prevent counterfeiting and fraudulent transactions'.[11] As of January 2020, there are over 2,000 publicly known cryptocurrencies with a combined total market capitalisation exceeding US$ 200 billion.[12]

While widely used for legitimate purposes, cryptocurrencies have also attracted the attention of individuals and organisations engaged in criminal or illicit activities on and off the dark web, though the extent of such usage  is uncertain.[13] The decentralisation that is an intrinsic part of cryptocurrency governance could allow individuals and organisations to engage in financial transactions without the supervision or interference of financial institutions; compliance with Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) regulation; or oversight by law enforcement agencies. Similarly, some analysts have cited the (pseudo-)anonymous features of cryptocurrencies as having the potential to increase the attractiveness of using

[11] Merriam-Webster (2020).

[12] CoinMarketCap (2020).

[13] The 'dark web' refers to the unindexed, unsearchable portion of the Internet that requires specific software packages to navigate. The Tor network enables access to the dark web – otherwise known as 'hidden services' – while concealing the user's identity and online activity from surveillance and traffic analysis. Entry points into the dark web can often be found on the Internet through traditional search engines. Persi Paoli et al. (2017).

cryptocurrencies for illicit purposes such as money laundering and terrorist financing.[14]

The intrinsic characteristics of cryptocurrencies have led many to assume intuitively that virtual currencies may be widely used for illicit transactions.[15] Some previous studies have begun to examine this topic, however there is not much agreement on the scope of the issue. Some studies estimate that as many as 25 per cent of Bitcoin users and as much as 44 per cent of Bitcoin transactions are involved in illicit activities.[16] These estimates place the total value of illicit Bitcoin transactions at around US$ 72 billion per year.[17] Other studies have, however, estimated that less than 1 per cent of Bitcoin transactions processed by exchange services can be determined as illicit.[18] Some researchers have also argued that the threat has been blown out of proportion, warning that overreaction from governments could stifle the positive benefits of new technology.[19] As with any other technology, a proportional and evidence-based response is required to balance the potential risks and benefits of cryptocurrency.

There is, therefore, significant disagreement concerning the extent to which cryptocurrencies are used for criminal intent. While it is clear that cryptocurrencies are accepted on dark web markets and could in theory be used for a range of illicit purposes, the reality of the connection between cryptocurrencies and criminal or terrorist use remains relatively unknown. To date, there has been little in the way of hard evidence gathering or detailed analysis on this topic.

Research into the illicit or criminal use of cryptocurrencies is fundamentally challenged by the concealed nature of the dark web and many researchers have expressed concerns about the validity and reliability of findings generated in dark web studies.[20] Data are often difficult to access or else insufficient, marketplaces may be taken offline due to law enforcement action, and privacy-preserving technologies may render users, transactions or other activities anonymous. While the extent of illicit activity involving cryptocurrencies is difficult to state with certainty, the use of cryptocurrencies for illicit and criminal purposes remains of significant interest to regulators and law enforcement. As authorities continue to grapple with the regulation of cryptocurrency-related activities, the methods with which actors use cryptocurrencies for illicit and criminal purposes also continue to evolve. Additionally, the rise of new cryptocurrencies with stronger anonymity features poses novel questions as to how actors may exploit privacy coins for criminal intent.

As part of this study, the research team conducted an extensive literature review of research into the use of cryptocurrencies. This search yielded an initial 1,599 sources, of which 119 sources were selected for in-depth data extraction. A detailed description of the literature process is included in Annex A. Among the research reviewed for this study (n=119), the largest proportion of sources (about 34 per cent) focused on the use of cryptocurrency for money laundering. The

[14] Dion-Schwarz et al. (2019).

[15] Albrecht et al. (2019), Carroll & Windle (2018).

[16] Foley et al. (2018).

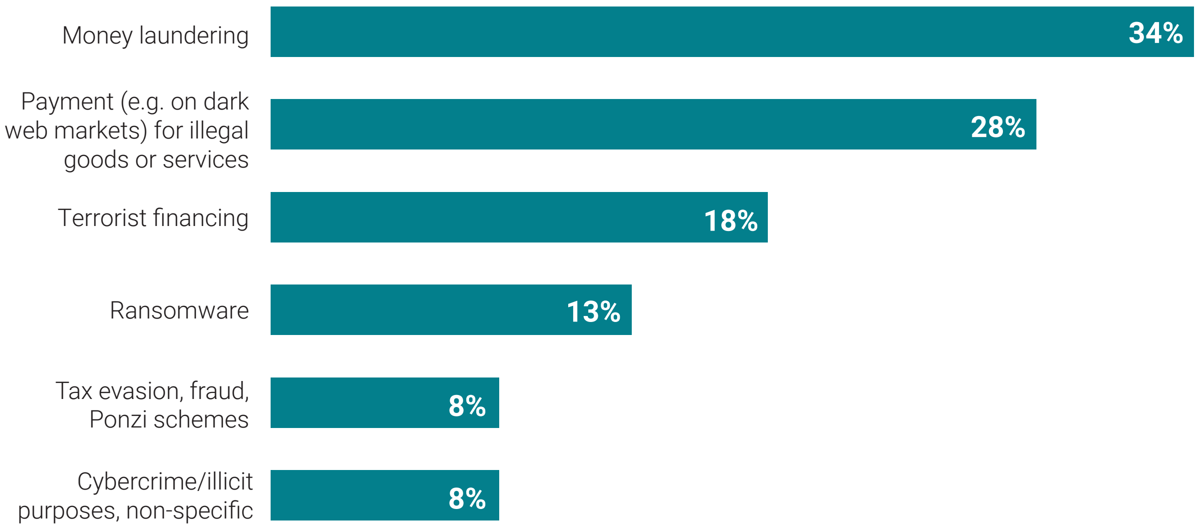
[17] Foley et al. (2018).

[18] Fanusie & Robinson (2018).

[19] Campbell-Verduyn (2018), Syska (2016), Chohan (2019).

[20] See for example Aldridge & Décary-Hétu (2015), Buskirk et al. (2015), Dolliver (2015), Munksgaard et al. (2016).

**Figure 2.1 Proportion of literature reviewed that specified a given illicit or criminal activity (n=119)**



*Source: RAND analysis (2020).*

second largest category (about 28 per cent) discussed the use of cryptocurrencies as payment mechanisms for illicit goods and services. Lastly, approximately 18 per cent of sources discussed cryptocurrencies in the context of terrorism financing. Other notable categories of uses which featured in the literature were in relation to ransomware (about 13 per cent of sources) and various forms of fraud or tax evasion, including Ponzi schemes (about 8 per cent of sources). It should be noted that a proportion of studies (8 per cent) did not focus on one category of uses exclusively but rather made mention of several, including cybercrime, and some studies discussed the use of cryptocurrencies for non-specified types of illicit or criminal purposes.

Interviews with cryptocurrency experts further emphasised that **money laundering, trade in illicit goods and services,** and **terrorism financing** as the criminal and illicit activities most often connected to the use of cryptocurrencies, both in relation to identified actual use and speculative use. The following sections go on to discuss the connections between cryptocurrencies and each respective illicit activity in order to highlight why cryptocurrencies may present an attractive option for malicious users engaged those activities.

### 2.1.1. Cryptocurrencies offer attractive money laundering mechanisms

Cryptocurrencies are judged by some to represent attractive money laundering mechanisms due to their decentralised and (pseudo-)anonymous characteristics.[21] In contrast to conventional money laundering mechanisms, cryptocurrency money laundering, or 'cryptolaundering', presents benefits in that it circumvents geographic constraints and exploits gaps and overlaps

[21] Barone & Masciandaro (2018).

between heterogeneous regulatory frameworks. Cryptolaundering is also faster than traditional money laundering services and has not required identity verification in contrast to the Know Your Customer (KYC) obligations of traditional financial institutions.[22]

Cryptolaundering may involve the profits not only from 'offline' crime but also from illicit activities conducted online. Cryptocurrencies are, for example, widely reported to be used as means of payment in ransomware attacks.[23] Moreover, virtual payment methods have been on the rise in the context of 'white collar crime' categories such as investment fraud and Ponzi schemes, representing a large proportion of the cryptomarket volume.[24] Frequently, profits from online fraud schemes go through several subsequent iterations of cryptolaundering to evade detection by law enforcement.[25]

The use of cryptocurrencies for money laundering is not determined solely by the purchasing and exchange of cryptocurrency coins. Criminals seeking to launder illicit transactions may make use of various other techniques and services in addition to traditional exchanges. In the case of illicit Bitcoin transactions, this often involves mixing services.[26] At the same time, various combinations of cryptocurrency transactions and long-chain transactions[27] may be used to obfuscate the money trail in money laundering schemes.[28] Existing studies indicate that the exchange of Bitcoins for alternative cryptocurrencies may increasingly be a preferred cryptolaundering mechanism over the use of traditional mixing services.[29]

However, the increasing acceptance and use of cryptocurrencies across society have also increased the regulatory attention on this new technology. Regulators and exchanges have been increasingly reviewing or requiring AML, capitalisation, consumer protection and cybersecurity standards. Some coins, such as Zcash, publicly state their compliance with global AML/CFT standards,[30] including the updated 2019 Financial Action Task Force (FATF) recommendations.[31] Lastly, despite the perceived attractiveness of cryptocurrencies for money laundering purposes, it is also worth noting that an estimated 99 per cent of cryptocurrency transactions are performed through centralised exchanges, which can be subject to AML/CFT regulation similar to traditional banks or exchanges.[32]

[22] Desmond et al. (2019).

[23] Ahn et al. (2016).

[24] Lee et al. (2019).

[25] Broadhurst et al. (2018).

[26] Cryptocurrency tumblers or cryptocurrency mixing services are services or software which mix potentially identifiable or 'tainted' cryptocurrency funds with others, so as to obscure the trail back to the fund's original source. Mixers have consistently processed about a quarter of incoming illicit Bitcoins per year. However, these mixers are not always reputable or trusted; van Wegberg et al (2018) reported being victims of scams with three out of the five mixers that they trialled. Fanusie & Robinson (2018), van Wegberg et al. (2018).

[27] A so-called 'long-chain' is a transaction chain whose growth rate appears to exceed a target value in a given 24-hour period. There are many legitimate reasons to create long transaction chains; however, they may also be caused by coin mixing or possible attempts to manipulate transaction volume. Blockchain (2020).

[28] CipherTrace (2019).

[29] Lee et al. (2019).

[30] Zcash (2019).

[31] FATF (2019).

[32] Moiseienko & Izenman (2019).

### 2.1.2. Cryptocurrencies have been used in the trade of illicit goods and services

As a payment mechanism, cryptocurrencies are widely used for purchasing illicit goods and services on dark web marketplaces. There are two main types of dark web marketplace:

1. **So-called cryptomarkets,** which bring together multiple sellers or vendors managed by marketplace administrators in return for a fee or commission on sales. Often compared to online marketplaces like eBay or Amazon, these markets often also provide additional services such as escrow (in which payment is released to vendors only after customers have received and are satisfied with their purchases) and third-party dispute adjudication. Cryptomarkets use cryptocurrencies for payment and maintain feedback systems that facilitate the selection of reliable vendors and highly rated products.[33]
2. **Vendor shops, or 'single-vendor markets',** are managed by a single vendor who sell directly to customers. Vendors typically maintain a vendor shop to avoid fees or commission structures imposed by cryptomarkets or other financial risks. Vendor shops typically specialise in a particular product and many vendor shop owners also trade on cryptomarkets.[34]

The advent of dark web marketplaces have offered sellers of illicit goods and services new distribution channels that enable them to transact with customers across larger geographical areas than they could previously using offline methods.[35] Dark web marketplaces have been found to offer a wide range of goods and services in exchange for cryptocurrencies, including drugs and illicit substances, explosives and weapons,[36] ivory and wildlife trafficking,[37] antiquities,[38] and child sexual abuse material.[39] Dark web marketplaces additionally offer opportunities to purchase a wide range of online 'crime-as-a-service' products such as exploit kits, Distributed Denial of Service (DDoS) services or phishing tools.[40]

The purchase of such goods and services with cryptocurrencies as opposed to other means may not only be motivated by the greater anonymity that they promise or the sheer availability of illicit goods and services on dark web marketplaces. Important also are practical factors including the speed of transactions and the lower fees compared to traditional payment systems. The exchange of goods and services on dark web marketplaces may also seek to circumvent traditional markets and institutions; for example, dealing in antiquities on the dark web has been in part motivated by efforts to disrupt traditional markets that are dominated by established auction houses.[41]

[33] Persi Paoli et al. (2017).

[34] Persi Paoli et al. (2017).

[35] Aldridge & Décary-Hétu (2016).

[36] Weimann (2018).

[37] Mead (2013).

[38] Paul (2018).

[39] Olson & Tomek (2017).

[40] Broadhurst et al. (2018).

[41] Paul (2018).

### 2.1.3. There is increasing concern about terrorism financing using cryptocurrencies

Further to money laundering and the procurement of illicit goods and services, the use of cryptocurrencies in terrorism financing has been a growing concern for regulators and to wider counterterrorism efforts. Terrorist organisations have made an increasing use of cryptocurrencies for two main related purposes.[42]

Firstly, cryptocurrencies have been used for soliciting funds from sponsors and supporters, and general fundraising activities. Terrorist organisations including the so-called Islamic State have been reported to direct online fundraising campaigns at cryptocurrency donations.[43] Apart from grassroots-style fundraising campaigns, cryptocurrencies may also be used by international actors and proxies in the context of state-sponsored terrorism. While there is precedent for such use, it is only supported by anecdotal evidence.[44]

Secondly, as terrorist groups are constrained by international and national AML/CFT regulations with regards to transferring funds, the use of cryptocurrencies is among new potential methods of moving funds in a faster, more anonymous and global way. Existing methods of terrorism financing range from traditional cash-based money transfer systems (e.g. hawala)[45] to formal banking.[46] Cryptocurrencies may appear as an attractive alternative to these existing systems as formal banking structures generally incorporate various KYC procedures, in contrast to some cryptocurrency exchanges. For some terrorist organisations, cryptocurrencies may also carry a perceived ideological benefit, as they circumvent the Western banking system.[47] While there is currently a lack of technical and telecommunications infrastructure in many locations in which terrorist organisations are most active, the development of sufficient infrastructure in regions such as sub-Saharan Africa and the Horn of Africa could lead to increased use of cryptocurrencies in this context.[48]

Based on these factors, existing studies show that the use of cryptocurrencies for terrorist financing has to date been largely episodic and is not as widespread as could be assumed.[49] A 2019 RAND study concluded that current concerns about cryptocurrency as a significant enabler of terrorist groups are almost certainly overblown.[50] However, methods of terrorist financing through cryptocurrencies are becoming more sophisticated.[51] For example, while terrorist organisations would previously publicise a single Bitcoin address to which supporters would be asked to donate, increasingly such

[42] Goldman et al. (2017).

[43] Interviewee 6, Weimann (2018).

[44] Interviewee 14.

[45] 'Hawala' refers to an informal cash-based person-to-person value transfer system often utilised by terrorist organisations including al-Qaeda for the purposes of transborder money transfers. Hawala takes place outside of conventional banking structures and institutions. Martis (2018), Dion-Schwarz et al. (2019).

[46] Freeman & Ruehsen (2013).

[47] Weinmann (2018).

[48] Goldman et al. (2017).

[49] Goldman et al. (2017).

[50] Dion-Schwarz et al. (2019).

[51] Interviewee 6.

fundraising methods have evolved to include an algorithm which generates new Bitcoin addresses periodically. This is intended to increase the difficulty of locating said Bitcoin addresses used for terrorist financing and their subsequent takedown by exchanges and relevant authorities.[52]

## 2.2. A wide range of actors use cryptocurrencies for criminal or illicit activities

The range of criminal and illicit purposes for which cryptocurrencies are or have been used is mirrored by the diversity of malicious actors known to be involved. This includes individuals, organised criminal groups, terrorist organisations and state actors. It should be noted that different types of actors may have different preferences for the use of cryptocurrencies, depending on the motivation of such actors for conducting illicit transactions, as well as the nature of their activities. Individual users can, for example, be expected to engage in large-scale money laundering less frequently than criminal organisations.[53] Conversely, they are more likely to purchase lower value illicit goods on dark web markets or hack cryptocurrency exchanges for personal enrichment.[54] Larger organised groups may, by contrast, be expected to engage in larger and more complex operations. The motivation of state actors – with Russia[55] and the North Korean regime[56] being prominent examples – may also differ, with the circumvention of international sanctions regimes eclipsing individual personal enrichment from cryptocurrency theft.[57]

Furthermore, criminal groups and terrorist organisations conventionally rely on different financial infrastructures and are defined by different 'business models'. Unlike many criminal organisations, terrorist organisations often seek to transfer funds outside of the physical location where they operate, e.g. in preparation for an attack elsewhere. The required financing infrastructure relies on a network of intermediaries. By adding additional layers of complexity and intermediaries, the necessity to transfer cryptocurrency transactions into fiat currencies may therefore represent greater operational risks to terrorist organisations than criminal groups.[58] On the one hand, the borderless nature of cryptocurrencies and their evasion of supervisory and regulatory frameworks make them pertinent for criminal groups and terrorism organisations, whereas on the other hand the operational risks and logistical difficulties are likely to depress demand from terrorism organisations for using cryptocurrency for these purposes.

Having examined the potential illicit or criminal use of cryptocurrencies in general, the following chapter explores the available evidence base on the illicit or criminal use of Zcash in particular.

[52] Interviewee 6.

[53] Fanusie & Robinson (2018).

[54] Kruithof et al. (2016).

[55] Matthews (2017).

[56] Carlisle & Izenman (2019).

[57] Interviewee 3.

[58] Goldman et al. (2017).

# 3 The use of Zcash for criminal or illicit purposes

Having examined the evidence base vis-à-vis the illicit use of cryptocurrencies more broadly, Chapter 3 will analyse the use of the Zcash cryptocurrency for criminal or illicit purposes, with particular focus on its adoption on the dark web.

## 3.1. Zcash is a cryptocurrency that seeks to provide enhanced privacy for its users

In response to a growing awareness that many popular cryptocurrencies, and particularly Bitcoin, do not possess as strong anonymity and privacy guarantees as previously thought, several alternative cryptocurrencies with privacy-enhancing or preserving features have been developed. This includes the altcoins Dash,[59] Monero,[60] Litecoin[61] and Zcash.[62]

Zcash (ZEC) is a digital currency and privacy coin publicly launched in October 2016 as a code derivative of Bitcoin. Similarly to Bitcoin, Zcash transaction data is posted to a public blockchain; but unlike Bitcoin, Zcash alleges that personal and transaction data can remain completely confidential.[63] This is reportedly accomplished through zero-knowledge proofs that allow users to spend coins without revealing which coins are being spent.[64] Zcash is the first widespread application of a novel form of zero-knowledge cryptography underpinned by what is considered state-of-the-art cryptographic research originating at MIT, Technion, Johns Hopkins, Tel Aviv University and UC Berkeley.[65]

While often assumed to be completely private, Zcash facilitates both shielded and transparent transactions on its blockchain through an 'opt-in' privacy model. The shielded transactions rooted in practical zero-knowledge proofs are called zk-SNARKs.[66] Zcash also offers transparent (i.e. public) transactions that are

[59] See https://www.dash.org/

[60] See https://www.getmonero.org/

[61] See https://litecoin.com/en/

[62] See https://z.cash/

[63] ECC (2020c).

[64] Kappos et al. (2018).

[65] Ben-Sasson et al. (2014), Miers et al. (2013).

[66] The acronym zk-SNARK stands for 'Zero-Knowledge Succinct Non-Interactive Argument of Knowledge', and refers to a proof construction where one can prove possession of certain information, e.g. a secret key, without revealing that information, and without any interaction between the prover and verifier. ECC (2020b).

not dissimilar to that of Bitcoin in that they reveal the pseudonymous addresses of the senders and recipients, as well as the amount being sent.[67] As of January 2020, 15.5 per cent of Zcash transactions were shielded, reflecting limited uptake of this particular functionality by the majority of users for the cryptocurrency.[68]

The following sections will interrogate to what extent Zcash is used for illicit purposes (e.g. the scope of the issue) and how Zcash is used for illicit or criminal purposes (e.g. for which purposes Zcash are used).

## 3.2. There is little evidence that Zcash is used for illicit purposes by malicious actors

As discussed in Chapter 2, some commentators believe that due to their privacy enhancing features, altcoins such as Zcash (as well as Monero, Dash and Litecoin) represent notable competitors for Bitcoin with illicit users on the dark web.[69] The expectation is that anonymity has played an important role in allowing the black market to flourish, as privacy-preserving cryptocurrencies could enable individuals to make illegal transactions that are difficult, and in some cases impossible, to track.[70] While this may appear intuitively persuasive, little empirical evidence or research exists in support of this claim.[71]

### 3.2.1. Zcash is relatively unknown in the academic research community and the links between Zcash and illicit or criminal activities have not been subject to substantial research

As discussed in Section 2.1, there is significant disagreement among researchers and practitioners as to the extent to which cryptocurrencies are used for illicit or criminal purposes. For example, when estimating the percentage of Bitcoin transactions made for illicit or criminal purposes, analysts' estimates range from 0.5 per cent[72] to 44 per cent.[73]

Similarly, the findings of this study are inconclusive with regard to the full extent of the use of Zcash for illicit or criminal purposes. While there is no analogous research that has been done to measure the percentage of Zcash transactions for illicit or criminal purposes, interviewees were able to speculate by using the numbers for Bitcoin as a point of departure.

This seems to be a result of a confluence of different factors. This includes broad unfamiliarity with Zcash in the research community and the practicalities of its privacy-preserving features. Challenging too are the opacity of the illicit use of cryptocurrencies and the barriers this creates for access to data. There is also a lack of focus in the research community on this specific use of Zcash. Where research on Zcash does exist, much of the literature focuses on the characteristics and technical aspects of Zcash, rather than its potential illicit or criminal uses. Overall, only

[67] Kappos et al. (2018).
[68] ZChain (2020).
[69] Todorof (2019).
[70] Albrecht et al (2019).
[71] Interviewee 7.
[72] Fanusie & Robinson (2018).
[73] Foley et al. (2018).

about 15 per cent of all sources reviewed as part of this study mentioned Zcash. Among those, where the source included a broader discussion of Zcash, the majority of sources (about 60 per cent, or less than 10 per cent of the total number of sources reviewed) focused on the characteristics of Zcash, particularly its privacy features. Only three sources included a discussion of the use of Zcash on the dark web, which may be due to Zcash's comparatively limited presence on the dark web (see Section 3.3). This may be due to a lack of awareness or understanding of Zcash from the research community or perhaps due to low levels of actual use of Zcash for illicit or criminal purposes.

### 3.2.2. There is limited evidence that Zcash is used for money laundering, purchasing illicit goods and services or terrorism financing

It bears repeating here that where research on Zcash does exist, most of the literature focuses on the characteristics and technical aspects of Zcash rather than on its potential illicit or criminal uses. However, some speculative or tenuous connections have been made between Zcash and the following:

- **Money laundering:** In the literature on the use of cryptocurrencies for illicit and criminal activities, their use throughout the money laundering process features most prominently (see Section 2.1.1). Anecdotally, there are indications of money disappearing into Zcash, in that the perceptible money or cryptolaundering trail stops at Zcash.[74] Albrecht et al (2019) highlight that Zcash is especially well-suited for money laundering, given that each individual financial transaction is impossible to trace and identify.[75] While the technical capabilities of Zcash could certainly in theory lend themselves to money laundering activities, there is no evidence of actual use for this purpose.[76]
- **Use in relation to illicit goods and services:** There are indications that Zcash is accepted or used for illicit goods and services. Previous research has shown that dark web marketplace AlphaBay was on the verge of accepting Zcash before its shutdown in July 2017.[77] It has also shown the Shadow Brokers hacking group to accept Zcash for their monthly release of data, but there is limited evidence as to the value of transfers into their wallet.[78] Additionally, two seizures of Zcash by law enforcement have come to light: one from the creator and administration of the AlphaBay market, and one from a criminal arrested by the UK police. AlphaBay was subject to a takedown by the US Department of Justice in 2017, which also resulted in the arrest of its creator and a civil forfeiture complaint against his assets, which included approximately 3,691.98 Zcash residing in a transparent address.[79] A subsequent investigation by the ECC traced these funds to the Bitfinex exchange, from which they were withdrawn shortly before AlphaBay announced the intention to support Zcash later that

[74] Interviewee 9.

[75] Albrecht et al. (2019).

[76] Interviewee 9.

[77] Buntinx (2017).

[78] Buntinx (2017).

[79] US DOJ (2017).

year.[80] This perhaps indicates that the owner of AlphaBay bought the Zcash in anticipation that this announcement would cause the price of Zcash to increase.[81] In September 2019, a small amount of Zcash (ZEC 34.89) was part of an auction of cryptocurrency seized from by UK police in the investigations of the hacking of UK Internet service provider TalkTalk.[82] These funds also appear to have been purchased from an exchange by the person from whom they were seized. Zcash's presence on the dark web is examined in greater detail in Section 3.3.

- **Terrorism financing:** Weinmann (2018) uncovered that a Telegram account entitled 'Technical Support of Afaq Electronic Foundation', a media group associated with ISIS, posed an answer to another user's question concerning whether Bitcoin purchases are secure. In this correspondence, the account offered a better alternative to secure online purchasing via Zcash.[83] Interviewees commented that they had not personally come across Zcash during the course of their research, though that does not necessarily mean that it is not being used for terrorism financing below the threshold of detection.[84]

These findings indicate only somewhat tenuous links between Zcash and illicit or criminal activities, while not discounting the possibility that these malicious uses could increase in scale and frequency in future. While it is feasible that Zcash could be used for illicit purposes similar to other cryptocurrencies, the currently available research does not present clear links between Zcash and illicit activities and there are no indications that Zcash is widely used for money laundering, terrorism financing, or for the trade in illicit goods and services.

## 3.3. The existing evidence points to a continued dominance of Bitcoin, so primary dark web marketplace data was collected to appraise Zcash on the dark web

Cryptocurrencies, and particularly Bitcoin, are often associated with the dark web following the widespread publicity and media attention surrounding the Silk Road investigation and other high-profile dark web marketplaces.[85] The connection between the use of cryptocurrencies for illicit purposes and the dark web has also been widely researched and documented.[86] Indeed, previous studies have shown that dark web marketplaces can be the predominant source for the illicit uses of this technology.[87]

Despite the intuitive benefits of privacy coins to conducting illicit or criminal transactions, the

[80] The seized funds had not been shielded following their withdrawal from the Bitfinex exchange, which made it possible to trace their provenance. ECC have asked us to make it clear that they have no privileged access to trace Zcash transactions.

[81] Zcash (2019b).

[82] BBC (2019).

[83] Weimann (2018).

[84] Interviewees 6 and 14.

[85] Kirkpatrick (2017).

[86] See for example previous RAND research such as Persi Paoli et al. (2017), Kruithof et al. (2016).

[87] Fanusie & Robinson (2018).

less anonymised Bitcoin is widely documented to be the most dominant cryptocurrency on the dark web. The emergence of alternative cryptocurrencies that are more opaque and better at concealing a user's activity through their privacy features have, however, recently led to a slight reduction in the illegal activity in Bitcoin.[88] However, given that researchers do not have full visibility into the use of cryptocurrencies for illicit or criminal purposes, these types of observations are often disputed and challenged.

Overall, existing evidence points towards a continued dominance of Bitcoin on the dark web, counter to expectations of the rise of privacy coins in this space, though the reasons for this may be poorly understood. To better understand the scope of the potential illicit use of Zcash, it is therefore necessary to examine Zcash's presence on the dark web and particularly on dark web marketplaces. As outlined in Chapter 1 and described in detail in Annex A, the study team used a combination of data sources for this investigation, including primary dark web marketplace data from RAND's DWO and secondary data from other dark web sources.

### 3.3.1. Using the RAND DWO for analysis of marketplaces enabled novel research findings in this study

Primary data was collected using the DWO in order to analyse the usage of cryptocurrencies across different dark web marketplaces. Box 1 provides an overview of the DWO.

**Box 1 The DWO**

Building on RAND's extensive research into the illicit use of dark web markets (e.g. for terrorism,[89] narcotics[90] or the sale of illegal firearms and explosives),[91] the Dark Web Observatory houses a primary data collection tool (i.e. a dark web crawler and scraper) and acts as a database and knowledge repository that RAND researchers can use to study the dark web.

The purpose of the DWO is to furnish researchers with up-to-date raw data scraped from cryptomarkets. Researchers can search for their own relevant dataset based on product information (e.g. drugs, guns and illegal electronic goods), vendor pages (i.e. suppliers on the dark web) and feedback on sales (i.e. used as a proxy for sales). Researchers can then use the data to make informed estimations of the size, scope and scale of illegal activity on different Internet-enabled black markets.

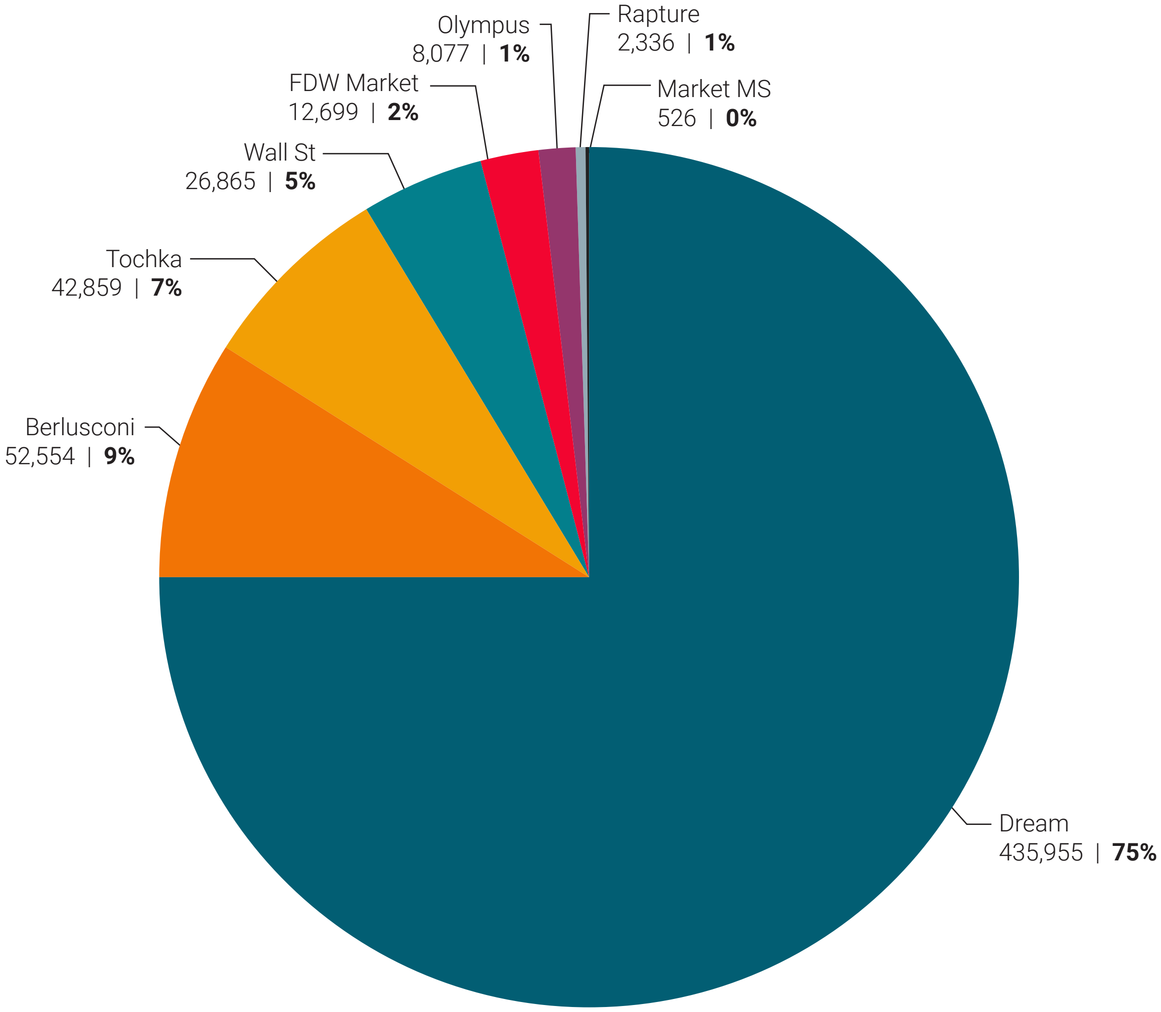
[88] Foley et al. (2018).

[89] Dion-Schwarz et al. (2019).

[90] Kruithof et al. (2016).

[91] Persi Paoli et al. (2017).

**Figure 3.1 Complete DWO listings by market**

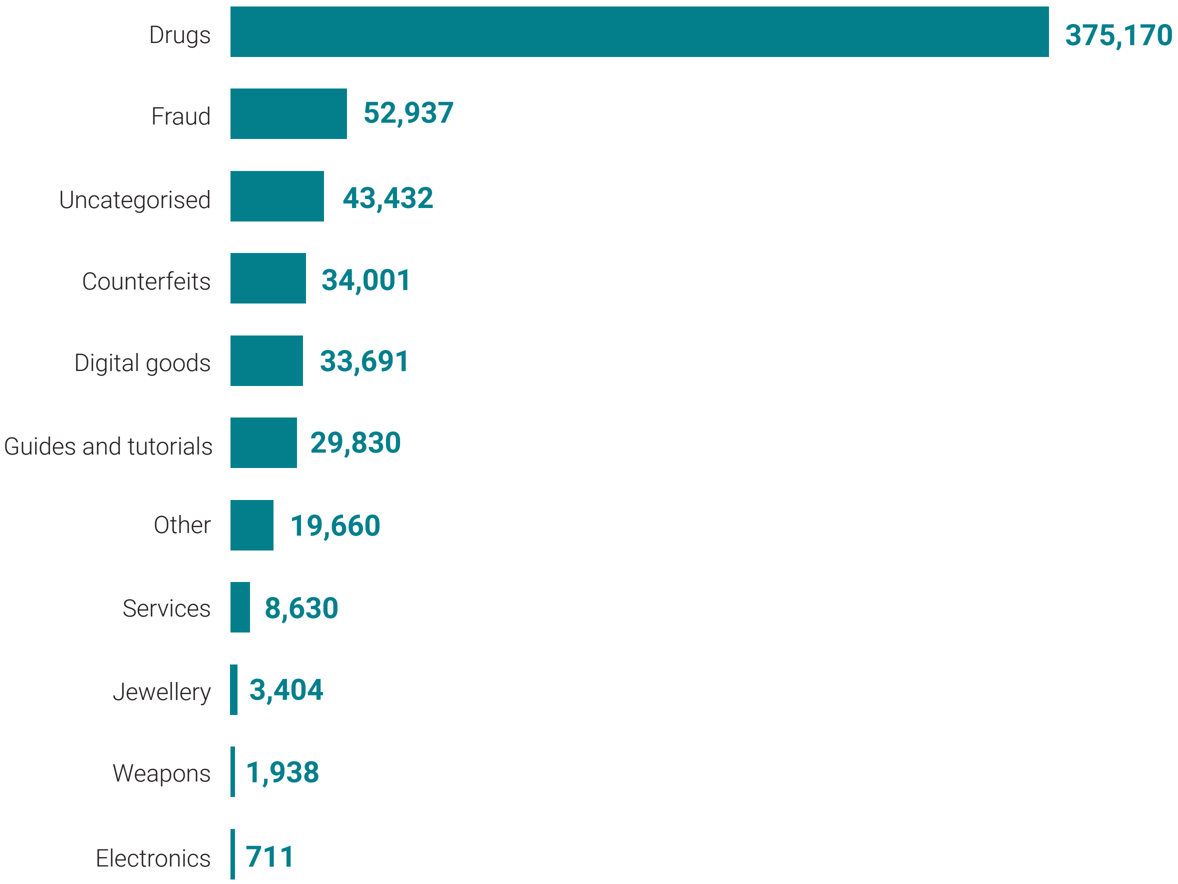


*Source: RAND DWO (2020).*

RAND's DWO comprises a database of scraped product listings and vendors from the dark web's top marketplaces. As of January 2020, it contains 581,871 listings across eight of the leading active and closed dark web markets scraped between 3 October 2017 and 27 April 2019. This is shown in Figure 3.1. The marketplace Dream is the largest included in the analysis by a significant margin (~436,000 listings), and the remaining markets are either medium-sized (Berlusconi, Tochka and Wall St) or significantly smaller (FDW Market, Olympus, Rapture and Market MS).

The 581,871 listings across these eight marketplaces can be categorised based on product type, as shown in Figure 3.2. Drugs represent the largest product category with over 60 per cent of total listings by volume (though not necessary value), whereas jewellery, weapons and electronics each represent less than one per cent of the total number of listings. It is also worth noting that uncategorised products (i.e. listings not designated to one of the other categories) represent a significant 7.5 per cent of listings.

**Figure 3.2 Overview of DWO listings by product category**



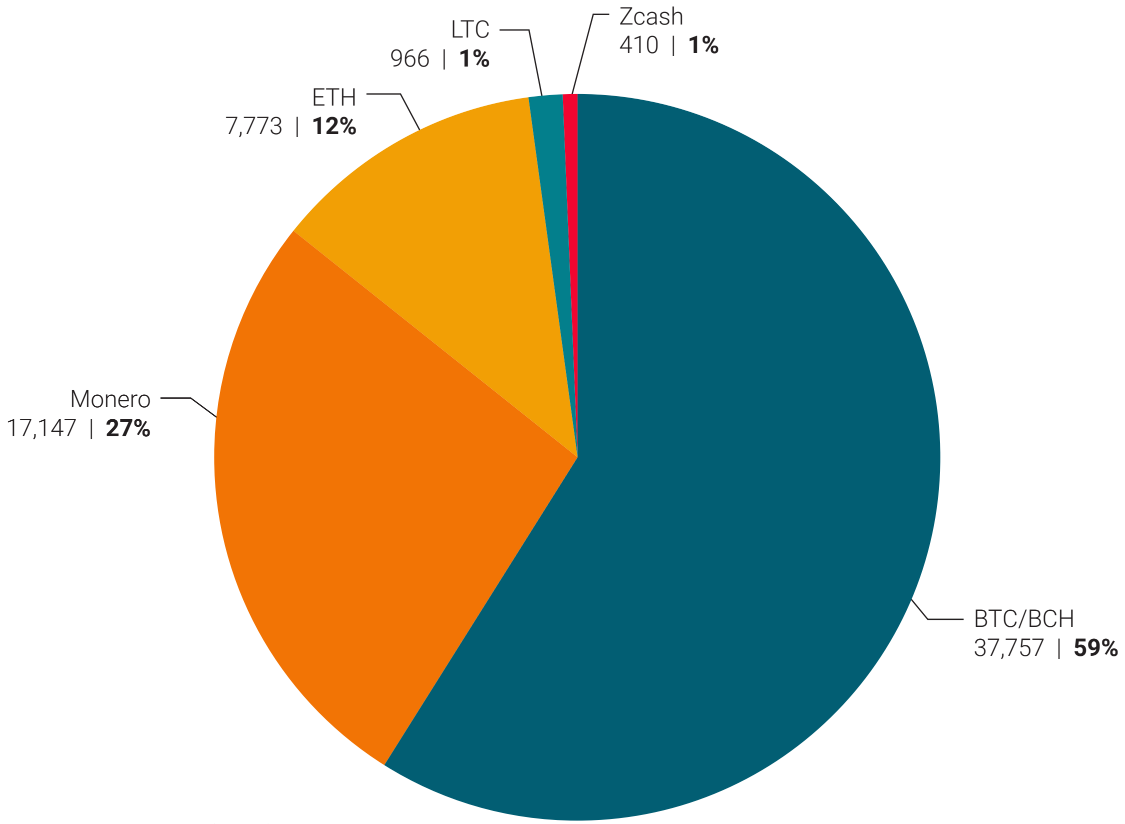
*Source: RAND DWO (2020).*

### 3.3.2. The DWO data was used to more accurately estimate the prevalence of Zcash and other cryptocurrencies on dark web marketplaces

To inform this study, the DWO data was used to better understand the presence of Zcash and other cryptocurrencies on dark web marketplaces, particularly as accepted methods of payment. The DWO aggregates listing descriptions into a single text-formatted field, which is often used by vendors to communicate accepted methods of payment. In this way, 'mentions' of select cryptocurrencies in these description fields were used as a proxy for 'accepted methods of payment' by vendors. The analysis included the following cryptocurrencies: Bitcoin and Bitcoin Cash (BTC, BCH), Ethereum (ETH), Litecoin (LTC), Monero (XMR, BitMonero) and Zcash (ZEC). A more detailed description of the research methodology is included in Annex A.

Overall, most markets only list exchange rates on their home page for cryptocurrencies that they accept. However, that does not necessarily indicate that all vendors accept all of the currencies that the market accepts and vendors can provide information regarding which of those they do accept. Some markets, like the now offline Tochka Market, list their accepted cryptocurrencies (Bitcoin, Bitcoin

**Figure 3.3 Cryptocurrency mentions in DWO listing descriptions**



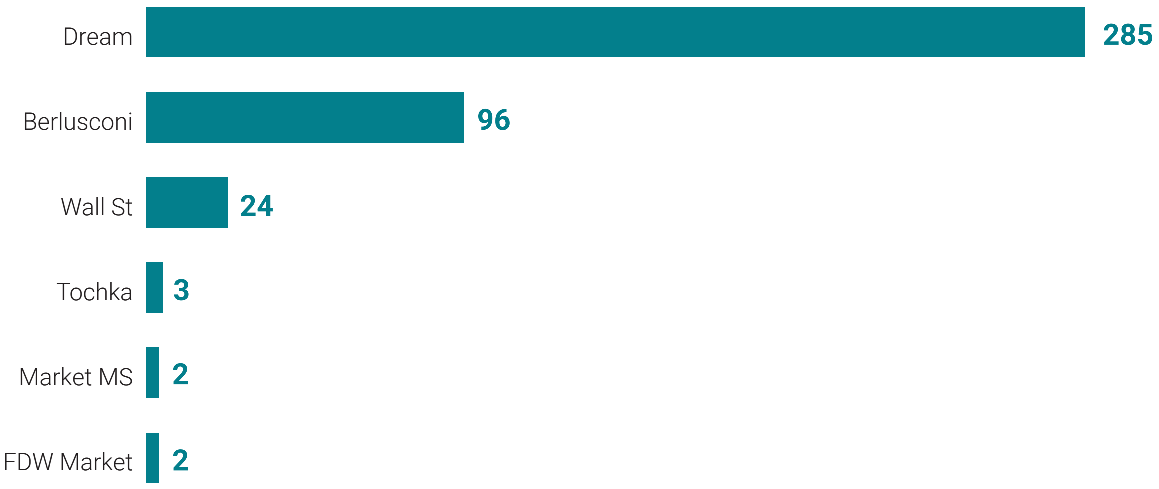
*Source: RAND DWO (2020).*

Cash and Ethereum in the case of Tochka), but also provide list pricing for individual items in US$. This makes it challenging to determine what the vendor would actually accept as payment without actually attempting to make a purchase.

Examining the DWO data, a search for mentions of the five cryptocurrencies examined in this study, including Zcash, returned a total of 64,053 matches to listing descriptions. The full breakdown is shown in Figure 3.3 below. The DWO data indicates that Bitcoin, Monero and Ethereum make up nearly all mentions (98 per cent) and indicates an overarching preference for these three currencies as payment methods across the eight dark web marketplaces reviewed. The significant presence of Monero (27 per cent) is consistent with a perceived shift from Bitcoin to cryptocurrencies with allegedly stronger anonymity and privacy-preserving features.[92] The results also indicate that Zcash does not have a significant presence on the dark web marketplaces, only appearing in 412 listings (less than 1 per cent). This also indicates that Zcash is not widely accepted or used as a method of payment on such markets.

[92] Interviewee 7.

**Figure 3.4 DWO listings with 'Zcash' mentions by market**



*Source: RAND DWO (2020).*

These results are largely in line with findings from other previous dark web research examining accepted payment methods. A 2019 Mosaic study found that 98 per cent of dark web marketplaces appear to accept Bitcoin, followed by 20 per cent of marketplaces accepting Monero. According to the Mosaic study, only two marketplaces were found to accept Zcash.[93] Similarly, the 2019 leak of the dark web marketplace Nightmare's sales data showed that Bitcoin accounted for 97.97 per cent of sales by US$ value, compared to Monero (1.13 per cent), Litecoin (0.46 per cent) and Zcash (0.05 per cent).[94]

Figure 3.4 shows that a majority of the 412 listings where Zcash was mentioned were found in the Dream (n=285) and Berlusconi (n=96) marketplaces, whereas the Wall Street (n=24), Tochka (n=3), Market MS (n=2) and FDW (n=2) marketplaces only had a small number of listings mentioning Zcash. The Olympus and Rapture marketplace listings did not feature Zcash at all.

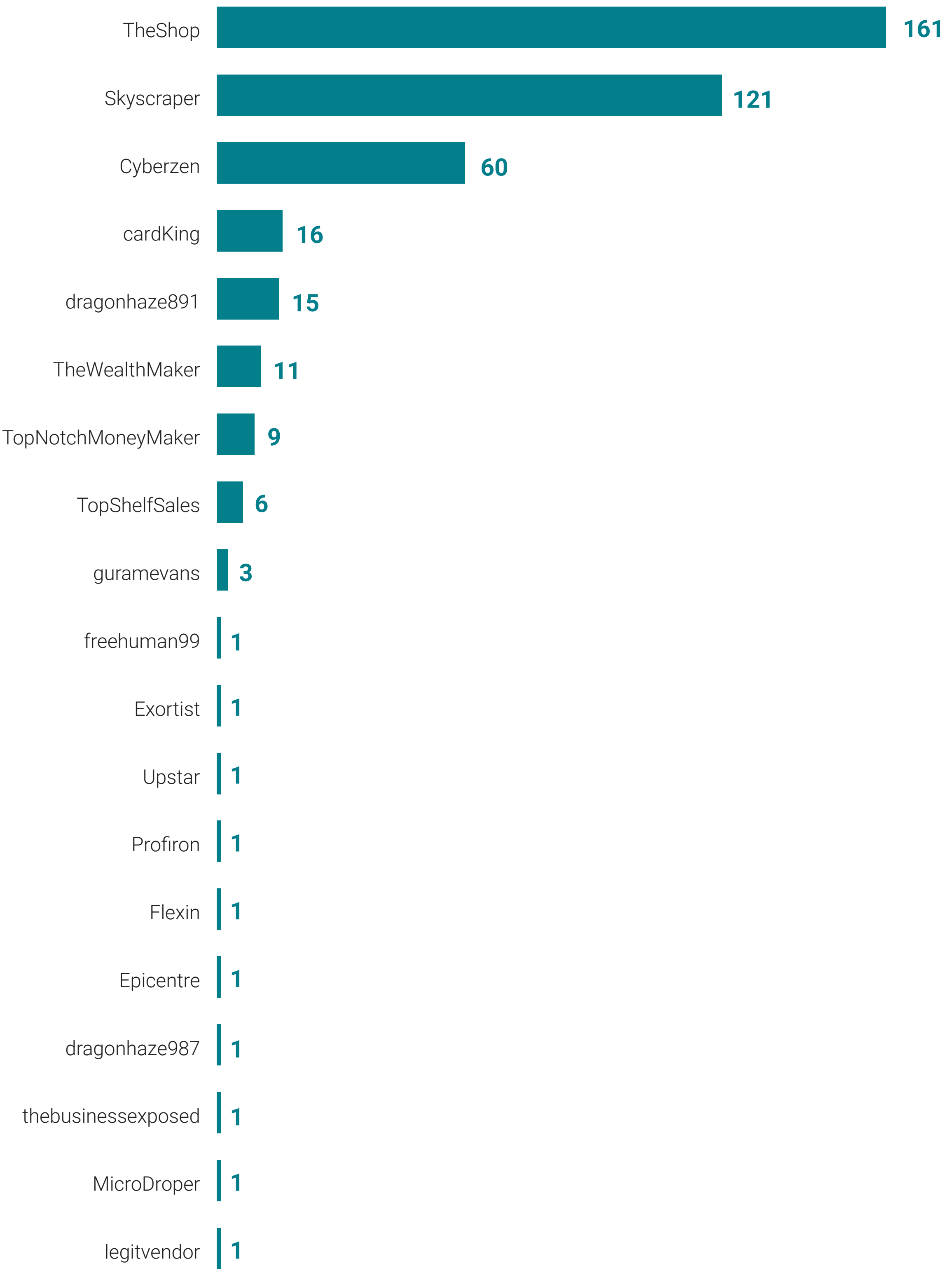
A further examination of Zcash mentions in marketplace listings reveal that a majority of mentions originate from just three sellers (TheShop, Skyscraper and Cyberzen), as shown in Figure 3.5.

While the description fields can be used as a proxy indicator for accepted payment methods, they can also mention cryptocurrencies in other contexts. For example, one listing that was particularly interesting (at least anecdotally) was for mining Zcash using other people's computers (see below).

[93] Ndinga (2019).

[94] Darknet Live (2019).

**Figure 3.5 Listings with 'Zcash' mentions by vendor**



*Source: RAND DWO (2020).*

**Box 2 Example of listing for Zcash miner**

★👑 2017 Miner (Active or Hidden Mode) $22,200+ VALUE - [Next 10 Orders Pay ONLY $10] 👑★

GPUs are so overpriced! Don't invest $10,000+ for decent returns when others can do the work for you for ONLY $10!

Description:
Mine tons of Zcash by infecting other computers without them knowing. Simply add your payment address and miner will run hidden on computers/servers.

Imagine 10, 20, 50, 100 infected computers MAKING YOU MONEY!!

ACT NOW and we will include a FREE BONUS!

LAST THING: To make sure we don't saturate this method, this price will go up by $10 after every 10 sales, so get in now cheap while you can.

*Source: RAND DWO.*

### 3.3.3. The study team augmented primary data collection with an examination of Zcash in other dark web datasets

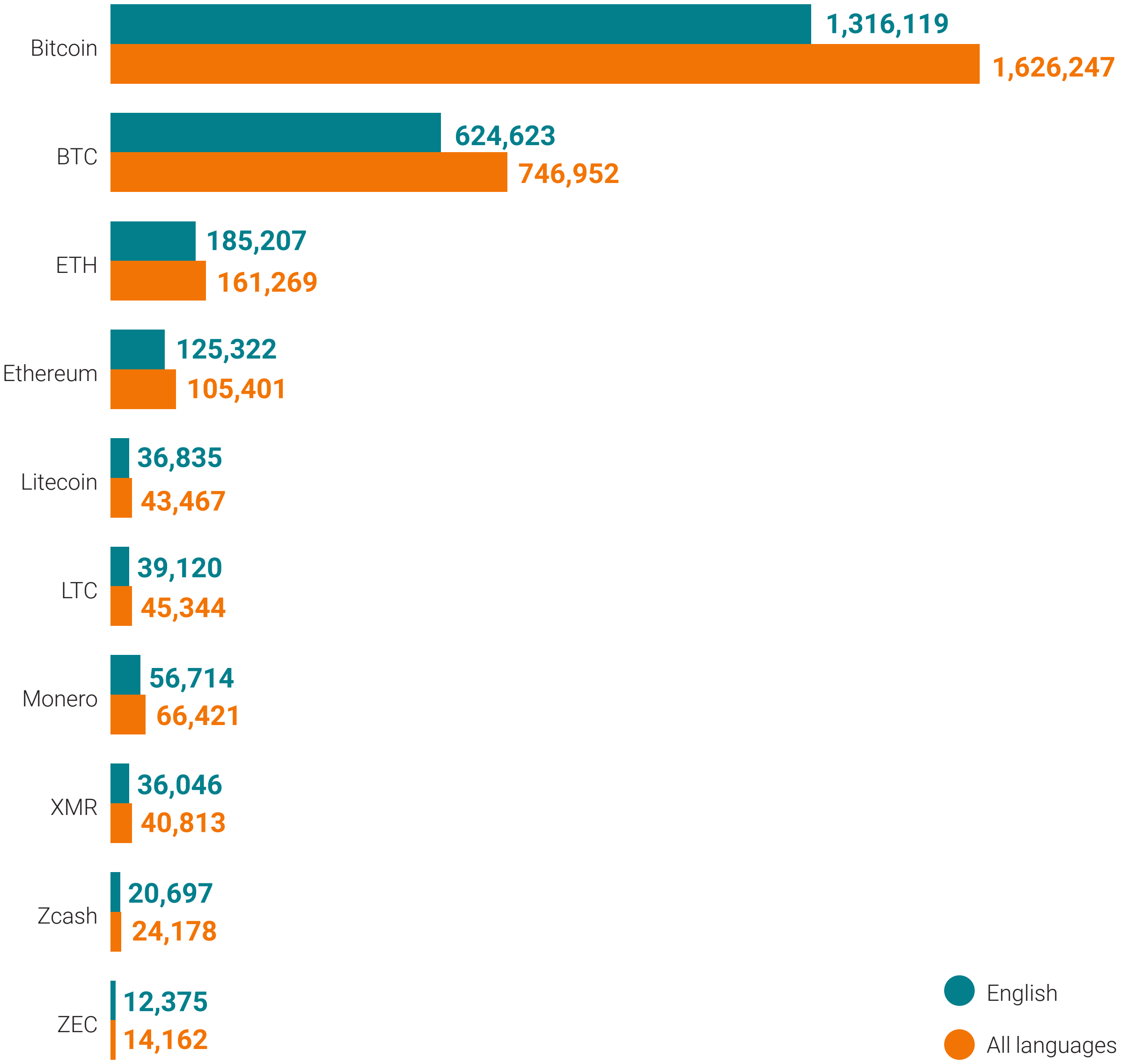
To compare the presence of Zcash on dark web marketplaces, or lack thereof, the study team also examined a secondary dark web dataset from the Dark Web Solutions Dark Web Monitor (DWM).[95] The DWM dataset contains two subsets of data: posts from dark web discussion forums (approximately 30 million) and cryptocurrency wallet addresses identified in dark web marketplaces or forums (approximately 30,000). The DWM dataset does not clearly show accepted payment methods for illicit goods and services on dark web marketplaces; however, it can be used to:

1. Show the presence of Zcash in dark web forum posts relative to other cryptocurrencies, which can be used as a proxy to measure general interest in a cryptocurrency by dark web forum users.
2. Show the frequency of Zcash cryptocurrency wallet addresses on dark web forums relative to other cryptocurrencies, which illustrates the prominence of cryptocurrency use by dark web users.

Figure 3.6 shows the distribution of the number of mentions in dark web forum posts by cryptocurrency. Similar to the results from the DWO analysis above, the DWM datasets also clearly shows the prominence of Bitcoin, followed by Ethereum and Litecoin. Compared to the DWO results, Monero seems to be less prominent in dark web forum posts than in dark web marketplaces. There is some presence of Zcash mentions in both English and other language posts, but overall mentions of Zcash only represents 0.23 per cent of total forum posts. This indicates that Zcash is not a prominent cryptocurrency of discussion among dark web forum users.

[95] The DWM provides data for different situations, leading to strategic insights, deep understanding of tactics or even operational support to identify actors based on mistakes made in the past. The DWM gathers information about online activities on crime areas as drugs, weapons, cybercrime and counterfeiting. Dark Web Solutions (2020).

**Figure 3.6 Number of forum post mentions in DWM dataset by cryptocurrency**

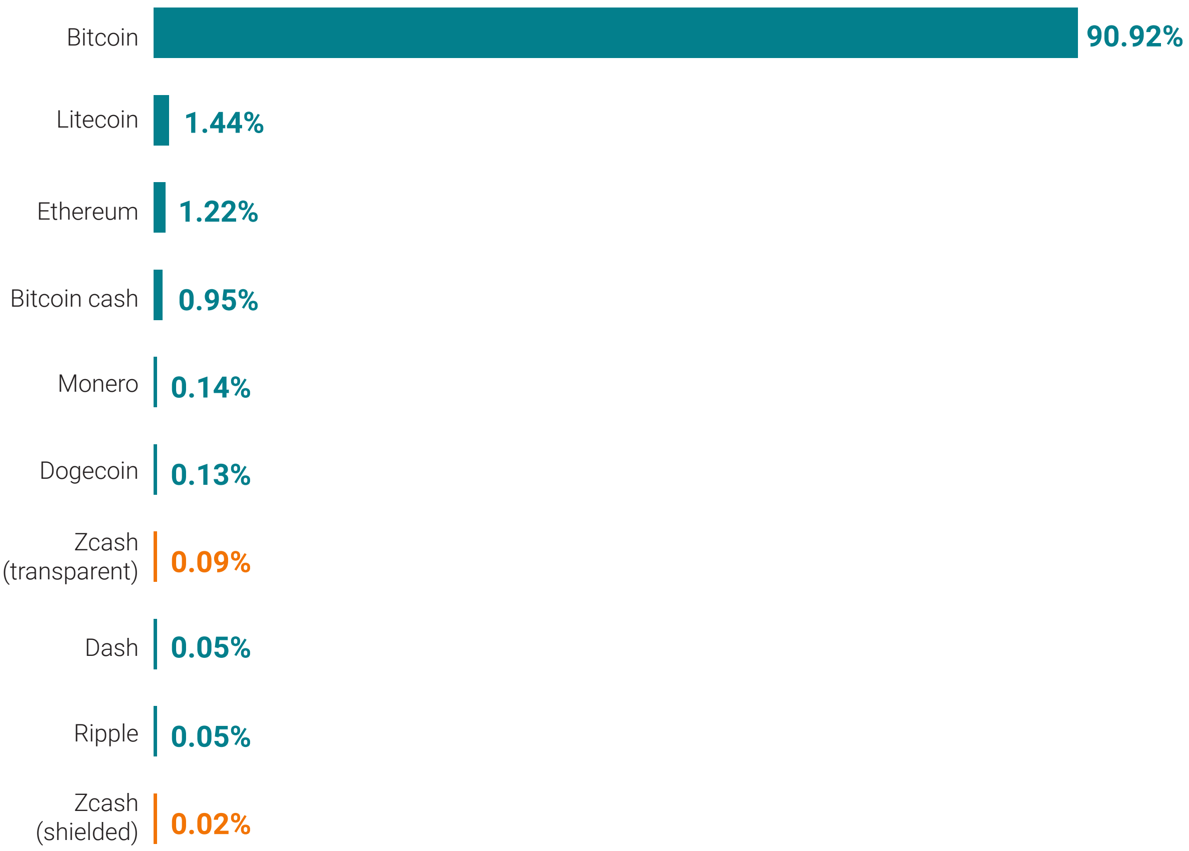


*Source: DWM (2020).*

The DWM also captures cryptocurrency wallet addresses mentioned in dark web forums or marketplaces. While the presence of a wallet address on the dark web does not translate to evidence of illicit activities, a high-level aggregation of identified wallets illustrates the general level of interest in particular cryptocurrencies by dark web users, some of whom may be engaged in illicit activities. Previous research has shown that 80 per cent of cryptocurrency wallets identified on the dark web were used with malicious intent.[96]

[96] Lee et al. (2019).

**Figure 3.7 Distribution of identified cryptocurrency wallets in DWM dataset**



*Source: DWM (2020).*

Figure 3.7 shows the distribution of identified cryptocurrency wallets in DWM dataset, which clearly illustrates the overarching number of Bitcoin wallets. Zcash wallets only make up 0.15 per cent (n=42) of the identified wallets, again indicating that Zcash is not a prominent cryptocurrency for dark web users. The data further emphasises that most users do not make use of Zcash's privacy features, as shielded wallets only represent 0.02 per cent (n=6) of all identified wallets.

These findings are largely in line with previous research, which has found that as many as 99.8 per cent of cryptocurrency addresses used on dark web marketplaces at the time of their research were Bitcoin addresses.[97] Similarly, other research shows that privacy coins are not widely used in such markets[98]; the proportion of illicit transactions for Monero and Ethereum on dark web marketplaces remains in the single digits, with 7 per cent for Ethereum and 4 per cent for Monero, in contrast to 76

[97] Lee et al (2019), Kethineni & Cao (2019).

[98] Ibid.

per cent for Bitcoin.[99] Similarly, Bitcoin remains the cryptocurrency most widely involved in malware and ransomware attacks. A recent report shows that whereas Bitcoin was used in 98 per cent of the malware and ransomware cases studied, Ethereum was only used in only 1 per cent of cases.[100]

In conclusion, this study has found that there is little evidence that Zcash is used for illicit purposes by malicious actors, and more specifically that:

- Zcash is relatively unknown in the academic research community and the links between Zcash and illicit or criminal activities have not been subject to substantial research.
- While it is feasible that Zcash could be used for illicit purposes similar to other cryptocurrencies, the currently available research does not present clear links between Zcash and illicit activities and there are no indications that Zcash is widely used for money laundering, terrorism financing, or for the trade in illicit goods and services.
- Zcash does not have a significant presence on the dark web marketplaces, only appearing in 412 listings (less than one per cent) across the eight marketplaces in the DWO.
- Zcash's limited presence on the dark web was further corroborated by other sources, which also indicate that Zcash is seen as a less attractive option to dark web users and is used less in dark web marketplaces compared to other cryptocurrencies, particularly Bitcoin and Monero.

In addition to the current use of Zcash, this study has also identified a range of factors that might affect the future scale of illicit or criminal uses of Zcash and how this develops as compared to other cryptocurrencies. These are discussed further in the following chapter.

[99] CipherTrace (2019).

[100] Ibid.

# 4 Factors that may influence the future use of Zcash for illicit purposes

Beyond examining the current levels of use of Zcash for illicit or criminal purposes, the academic research and interviewees consulted as part of this study presented a range of speculative factors that could affect the likelihood Zcash being used over other cryptocurrencies for illicit purposes in the future (see Table 4.1). The following five factors emerged most prominently from the literature and interviews:

- The Bitcoin hegemony
- The usability of Zcash
- The degree of anonymity of Zcash
- Evolution of criminal behaviours
- The perception and branding of Zcash.

These are presented in more detail in the following sections. All factors that may influence the future use of Zcash for illicit purposes are summarised in a table at the end of this chapter.

## 4.1. The Bitcoin hegemony offers a range of incentives to illicit users

Notwithstanding the advent of privacy-preserving cryptocurrencies, evidence suggests that users engaged in illicit activities are still primarily drawn to Bitcoin due to the relatively low friction of making international payments using only pseudonyms as identifiers.[101] This persistent dominance of Bitcoin may be due to its critical mass in terms of use, rather than the use of privacy overlays or mixing services to compensate for the lack of anonymity in Bitcoin.[102] Given the high volume of transactions made in Bitcoin, criminal and illicit activities are perceived to be more likely to be 'lost in the noise', with illicit transactions going unnoticed on the blockchain.[103] Additionally, Bitcoin can also regularly be accessed through cryptocurrency exchanges that do not comply with KYC regulation.

[101] Kappos et al. (2018).

[102] Interviewee 13.

[103] Interviewee 13.

One growing benefit for those engaged in illicit activities is the fact that cryptocurrencies as a whole are becoming more widely accepted as a form of payment amongst retailers.[104] However, this does not apply to all coins in equal measure. The high volume of transactions on the blockchain can help to obfuscate money laundering in Bitcoin, whereas single large transfers of value would be more prominent on the Zcash blockchain due to there being fewer overall transactions at present.[105] However, this is only applicable to transparent, and not shielded, Zcash transactions.

Additionally, Bitcoin's critical mass offers structural incentives for illicit users: it would be suboptimal for one individual to switch to a cryptocurrency that is less liquid or less frequently used even if that coin had more privacy-preserving features.[106] This in essence represents a network effect, whereby 'a service becomes more useful to all users the more people use it', reducing the incentive for users to switch to new, albeit theoretically more appropriate, technologies.[107] Overall, it appears the high levels of illicit use of Bitcoin may therefore predominantly be attributed to its market presence, suggesting that individual traits of cryptocurrencies are less important than the overarching nature of the market[108]; a shock to this market may therefore be required in order to disrupt the current levels of illicit use of cryptocurrencies and displace malicious users to others such as Zcash.[109]

## 4.2. The usability of Zcash may deter use for illicit purposes

While privacy-enhancing or preserving features are theoretically important, users (including those engaging in illicit or criminal activities) are often more concerned with the practicalities of the cryptocurrency such as its ease of usability. The user experience (UX) is therefore an important factor for cryptocurrency adoption on the dark web: cryptocurrency transactions that are faster, easier to carry out and do not require a substantial level of technical know-how are more likely to be used by illicit actors as much as any other type of user.[110] One prominent benefit of using cryptocurrencies is the ease with which funds can be moved. The user experience of sending funds via Zcash is not perceived as being as accessible as that of other cryptocurrencies. Additionally, according to two interviewees, the usability of Zcash is perceived as falling behind its peers.[111]

The prominence of usability concerns suggests that while privacy coins may seem like a boon to users engaged in illicit or criminal activities, various practical considerations may make them less attractive for transactions on the dark web.[112] The usability factor also interacts with the structural effects of the Bitcoin hegemony discussed in Section 4.1. If smaller cryptocurrencies are perceived as

[104] Albrecht et al. (2019).

[105] Interviewee 9.

[106] Interviewee 13.

[107] Goldman et al. (2017).

[108] Interviewee 8.

[109] Interviewee 13.

[110] Interviewees 6 and 9.

[111] Interviewees 6 and 9.

[112] CipherTrace (2019).

less user-friendly, they may also be less widely adopted in the market, reducing their value in the context of illicit activities such as ransomware where criminals are incentivised to demand cryptocurrencies that their victims will be using or at least familiar with. This creates a cycle – 'vicious' or 'virtuous' depending on one's perspective as either a proponent or opponent of illicit and criminal use of currencies such as Zcash.

## 4.3. Scepticism of Zcash's privacy-preserving functions may influence the use for illicit or criminal purposes

Cryptocurrencies are generally perceived to provide increased, rather than complete, anonymity.[113] The experience with Bitcoin has shown that while many popular cryptocurrencies may be assumed to provide a substantial level of anonymity upon launch, subsequent research can uncover weaknesses that reduce the level of anonymity or privacy.[114] Based on this trend, there is some scepticism as to how strong the privacy-preserving features of Zcash are and there are speculative doubts as to whether future research will provide insight into weaknesses of Zcash.[115]

Some of the technical privacy features of cryptocurrencies, including Zcash, may also be undermined by how users engage with and use the currencies. Recent research has shown that behaviour in and out of shielded pools can reveal information about Zcash users. Some participants in the relatively small shielded Zcash pool engage with the pool in a way that is identifiable, which significantly erodes the anonymity of other users.[116] Thus, a combination of users' unfamiliarity with the underlying technology and the blockchain itself may culminate in behaviour that undermines the technical privacy-enhancing or preserving features implemented by Zcash and other privacy coins.[117] However, as previously noted, privacy-preserving features do not seem to be the determining factor for cryptocurrency use for illicit purposes (see Section 4.1).

## 4.4. The evolution of criminal behaviour may alter the levels of illicit use of Zcash in the future

As discussed in previous sections, it is often not the technology itself but the understanding and perception of it that defines how the technology will be used. In the case of Zcash, it appears that its use for illicit or criminal purposes may also be limited due to a lack of understanding of the underlying technology and its functionality. Anecdotal evidence obtained through interviews showed, for example, that where transactions in Zcash are observed on the dark web markets, they are often unshielded; indicating that users may lack an understanding of the requirements of making shielded transactions in Zcash and may instead assume that all Zcash transactions are anonymous.[118] Cryptocurrencies that operate on an 'opt-in' privacy model, for example through the use of

[113] Carroll & Windle (2018).

[114] Interviewee 13.

[115] Tramer et al. (2019), Quesnelle (2017), Biryukov & Feher (2018), Biryukov et al. (2019).

[116] Interviewees 6 and 9, Kappos et al. (2018).

[117] Interviewee 14.

[118] Interviewee 6.

shielded payments, therefore require a more active engagement from its users.[119]

While there have been some signals of increasing sophistication of criminals and terrorist organisations in certain domains (e.g. Hamas' use of cryptocurrencies for financing),[120] individuals and organisations engaged in illicit or criminal activities are generally judged to be averse to adopting new technologies. Instead, they typically rely on technologies and methods that have been well tested.[121] This may also mean that the adoption of Zcash could increase in the future as the technology matures and awareness increases.

## 4.5. The perception and branding of Zcash can work to either deter or attract illicit use

There are several other factors, beyond its technical features, that underpin the consumer perception of Zcash and may influence its specific use for illicit or criminal purposes. This includes the perceived centralisation of Zcash compared to some competing cryptocurrencies, which may increase mistrust of its purported anonymity.[122] Perceptions of Zcash do not only evolve organically but are also proactively influenced by the public statements and branding efforts undertaken by the ECC and the Zcash Foundation. This may also provide opportunities for differentiation from cryptocurrencies that perhaps have similar anonymity features, such as Monero. Signalling compliance with AML/CFT regulation may, for example, reduce the perceived benefits of exploiting Zcash's anonymity features for money laundering and terrorist financing. While Zcash and other privacy coins may be perceived by criminals as ensuring similar levels of anonymity, the governance of Zcash and its efforts to showcase compliance with AML/CFT regulations may make it less vulnerable to exploitation for illicit and criminal purposes than other privacy coins.

## 4.6. Other factors influencing future illicit or criminal use of Zcash

Overall, this study has identified a range of factors that may influence the future use of Zcash of illicit purposes. This includes those already described as major considerations in Sections 4.1 to 4.5 but goes beyond with a number of other factors also being identified in the study.

The combined list of factors has been grouped in Table 4.1. This covers three categories:

1. Factors endogenous to Zcash
2. Exogenous and/or structural factors
3. Other factors that may influence the use of Zcash for criminal or illicit purposes.

[119] Interviewee 6.

[120] Interviewees 6 and 14, Carlisle (2019).

[121] Interviewee 9.

[122] Interviewee 11.

**Table 4.1 Factors that might affect the use of Zcash for criminal or illicit purposes**

| Category | Factor | Description |
|---|---|---|
| Endogenous factors | Perceived level of anonymity and users' familiarity with Zcash's anonymity features | There is a perception that emerging research may demonstrate, or is already demonstrating, various loopholes in Zcash's technical underpinnings. Secondly, there may be a lack of user familiarity with Zcash and its anonymity features.[123] Lastly, there may be reduced trust in Zcash's anonymity features due to the perceived centralised nature of Zcash's governance.[124] |
| | Usability of Zcash | Limited usability, or user-friendliness of cryptocurrencies, can present significant barriers to entry for cryptocurrencies, particularly for cryptocurrencies requiring higher levels of technical sophistication.[125] Various factors could influence the usability of Zcash, including attributes of the Zcash wallet, and the speed of transactions, especially shielded transactions.[126] |
| | Branding of Zcash | Clear branding of Zcash and the ECC as compliant with relevant regulations could reduce the incentives for its use in illicit purposes in contrast to other privacy coins.[127] Signalling compliance with AML/CFT regulation may be a key factor in differentiating Zcash from other privacy coins in the minds of criminal actors and refuting the reputation of privacy coins such as Zcash for harbouring illicit activities.[128] |
| | Protection from cyberattacks | Cryptocurrency users may be subjected to various attacks including cryptojacking or outright theft from cryptocurrency wallets. The degree of protection that Zcash provides to its users against attacks may be an important factor, particularly for criminal actors seeking to use Zcash for money laundering purposes or larger illicit transactions. The evidence base collected to date is weak on this issue, though one study suggests that Zcash has the perceived benefit of better protecting its users from cyberattacks relative to other privacy coins.[129] |

[123] Interviewee 9.

[124] Interviewee 9.

[125] Dion-Schwarz et al. (2019), Abrosimova (2019).

[126] Interviewees 6 and 9.

[127] Interviewee 14.

[128] Thibodeau (2019).

[129] Todorof (2019).

| Category | Factor | Description |
|---|---|---|
| Exogenous/ structural factors | Network effects and Bitcoin's hegemony | The dominant position of Bitcoin in the cryptocurrency market creates barriers for the adoption of other cryptocurrencies in both legitimate and illicit markets. It is possible that, should the volume of transactions in Zcash and its market share increase significantly, it would also become more widely adopted on the dark web.[130] Due to network effects, a technology becomes more useful to a user the more widely it is adopted, and it may be less attractive for illicit actors to switch to alternative cryptocurrencies, even if they provide better anonymity.[131] |
| | Price stability and reliability | Large swings in the value of a cryptocurrency may create doubts about its reliability. New cryptocurrencies may also be unreliable due to an existing trend of the majority of cryptocurrencies shutting down after being launched.[132] More stable cryptocurrencies are therefore assumed to be preferred for illicit projects requiring more long-term planning, as well as money laundering purposes, as significant value fluctuations would destabilise the movement of funds.[133] |
| | Changing practices and tech-savviness among illicit actors | The use of privacy coins may be conditioned on actors such as terrorist groups are becoming more sophisticated in their methods of using cryptocurrencies.[134] This implies that cryptocurrencies that require more sophisticated technical knowledge may be more likely to be used by more sophisticated actors (e.g. larger organised crime groups and state actors) rather than individual criminals seeking to use cryptocurrencies for payments for 'low-level' illicit goods and services.[135] |
| | Regulation | While regulation in the context of cryptocurrencies remains challenging, AML/CFT regulation has been observed to have a clear impact on privacy coins[136] and evolving regulatory practices may influence the adoption of specific cryptocurrencies (e.g. through regulating the 'middleman' or the use of on/off ramps).[137] |

[130] Interviewee 8.

[131] Interviewee 13, Goldman et al. (2017).

[132] Interviewees 1 and 13, Dion-Schwarz, Manheim et al. (2019).

[133] Interviewee 6.

[134] Interviewee 6, Dion-Schwarz et al. (2019).

[135] Interviewee 13.

[136] Interviewee 11, Auer & Claessens (2018).

[137] Interviewee 2.

| Category | Factor | Description |
|---|---|---|
| | Law enforcement | Even with more sophisticated techniques of obfuscating transactions, the blockchain provides rich opportunities for law enforcement to attempt and track illicit transactions.[138] This may be facilitated by increasing awareness of the risks posed by privacy coins and improved technological expertise among law enforcement agencies.[139] Adaptation and improvement of law enforcement practices, as well as improved cooperation between international law enforcement and intelligence agencies, may discourage the illicit use of cryptocurrencies, including privacy coins.[140] |
| Other factors | Attributes of the blockchain | Some cryptocurrencies may offer incentives for illicit/criminal purposes due to the range of opportunities provided by the underlying blockchain technology.<br>This concerns, for example, the difference between cryptocurrencies such as Bitcoin, designed as relatively simple payment mechanisms, and cryptocurrencies such as Ethereum with a wider range of blockchain applications that may be attractive for more sophisticated operations, Initial Coin Offering (ICO) fraud and market manipulation.[141] |
| | Resilience and stability of the cryptocurrency market | The perceived stability and resilience of the cryptocurrency market as a whole may be a factor in how criminal actors adopt and use cryptocurrencies. In theory, the nature of blockchain technologies provides considerable assurances against a system collapse. The resilience of the system against outside shocks and volatility may facilitate greater portability in the case of illicit transactions.[142] |

[138] Interviewee 6, Carroll & Windle (2018).

[139] Fanusie & Robinson (2018).

[140] Dion-Schwarz et al. (2019).

[141] Interviewee 1.

[142] Albrecht et al. (2019).

# 5 Conclusions

Cryptocurrencies can offer a number of potential security and privacy benefits and represent a promising financial innovation with a range of other economic opportunities.[143] However, they have also been perceived as a vehicle for fraud, organised crime and other illicit activities – and this perception will be matched by reality if the underlying technologies are not appropriately implemented and managed.[144] While the majority of transactions made with virtual coins are legitimate, this study has found that cryptocurrencies are also used for a wide range of criminal or illicit purposes by a diverse group of malicious actors. The main illicit and criminal purposes for which cryptocurrencies are most commonly used are i) money laundering, ii) purchasing illicit goods and services and iii) terrorism financing.

While privacy coins may intuitively appear likely to be preferred by malicious actors due to their purported anonymity-preserving features, there is little evidence to substantiate this claim. Zcash is a digital currency with optional features that enable privacy for transactions. Notwithstanding its privacy-enhancing features, the evidence base is lacking with regard to the full extent of the use of Zcash for illicit or criminal purposes. This study explored to what extent Zcash is used for illicit purposes (e.g. the scope of the issue) and how Zcash is used in these cases (e.g. for which purposes Zcash are used by malicious actors). In doing so, a number of key findings have emerged:

- Zcash is relatively unknown in the research community and the links between Zcash and illicit or criminal activities have not been subject to substantial research. This may be due to a lack of awareness or understanding of Zcash from the research community or perhaps due to low levels of actual use of Zcash for illicit or criminal purposes.
- There are three main illicit use cases for cryptocurrencies in general: money laundering, terrorism financing and trade in illicit goods and services. Our review has not identified any credible evidence pointing to large-scale use of Zcash for either of those purposes. While there are indications or anecdotal evidence that Zcash may have been used or advertised for illicit purposes, it is challenging to substantiate or quantify that evidence. Equally, it is important to note that absence of evidence does not equate to evidence of

[143] Leonard & Treiblmaier (2019), Dorofeyev et al. (2018).

[144] Foley et al. (2019), Aldridge & Décary-Hétu (2016).

absence, and so continuing research and vigilance against malicious use of Zcash is required.

- The dark web has been a prominent driver of the use of cryptocurrencies for illicit or criminal purposes and previous research has shown clear links between the presence and use of cryptocurrencies on the dark web and illicit activities. This study has found that Zcash has a minor to non-existent presence on the reviewed dark web marketplaces and forums. This does not mean that Zcash is not used for illicit or criminal purposes on the dark web, but it indicates that relative to other cryptocurrencies, particularly Bitcoin and Monero, Zcash is seen as a less attractive option for most dark web users.
- This analysis also found that where Zcash is used for illicit purposes, there are low levels of use of shielded Zcash payments on the dark web, which indicates that users engaged in illicit activities either do not understand the Zcash operating model or are not aware, in need of or confident in Zcash's privacy-preserving features. It may also suggest that illicit users of cryptocurrencies may not value the privacy features offered by Zcash, which would be supported by the continued use of Bitcoin.
- Notwithstanding recent developments in the cryptocurrency environment, such as the advent of several altcoins and privacy-focused cryptocurrencies, Bitcoin is still perceived to be the dominant cryptocurrency for illicit or criminal activities on the dark web.

While there are few indications that Zcash is currently extensively used for illicit or criminal purposes, this may change in the future. There are a range of factors that could affect the frequency, scale and impact of the use of Zcash for illicit purposes over other cryptocurrencies in the future, including:

- **Bitcoin hegemony:** Notwithstanding the advent of privacy-preserving cryptocurrencies, criminals engaged in illicit activities are still primarily drawn to Bitcoin due to the structural incentives that Bitcoin's critical mass creates for criminals.
- **Usability of Zcash:** While privacy coins may seem like a boon to users engaged in illicit or criminal activities, various practical considerations may make them less attractive for transactions on the dark web.
- **Degree of anonymity of Zcash:** There exists some scepticism as to how anonymous Zcash really is and whether future research will identify weaknesses in the Zcash anonymity features.
- **Sophistication of criminals:** It appears that Zcash's use for illicit or criminal purposes is in part limited due to a lack of understanding of the underlying technology on the part of its users.
- **Perceptions and branding of Zcash:** While privacy coins may be perceived by criminals as ensuring similar levels of anonymity, the governance of Zcash and its branding as compliant with AML/CFT regulations may make it less susceptible to exploitation for illicit or criminal purposes.

Moreover, it seems that market conditions, rather than specific characteristics of any one cryptocurrency, may be a predominant driver for cryptocurrency adoption on the dark web. While it makes intuitive sense that privacy coins such as Zcash would be adopted en masse for criminal and illicit purposes, the research that exists in this space indicates that criminals are more likely to 'go where the money is'.[145] That is to say that the Bitcoin cryptocurrency, which has captured the largest market share among cryptocurrencies,  has reached critical mass for both legitimate and illegitimate transactions. A shock to this market may therefore be required in order to disrupt the current levels of illicit use of cryptocurrencies and displace malicious users to others such as Zcash.

At the same time, actions by law enforcement, regulators and the ECC and others can also proactively shape both market and criminal behaviours. Effective action presumes a nuanced and up-to-date understanding of the dynamics of both. However, this study found that research into the use of cryptocurrencies for illicit or criminal purposes remains an emerging field, particularly in relation to younger cryptocurrencies such as Zcash. Given the paucity of data and analysis in this area, this report concludes with some avenues for future research.

### 5.1.1. There are several avenues for future research within this emerging field

Given that there has been little to no prior research on the use of the Zcash cryptocurrency for illicit or criminal purposes, there are many possible avenues for further research. The following are a few examples of lines of inquiry that would augment the evidence base for future studies:

- Improvements to mechanisms for data gathering and more accurate estimates of the extent of the use of cryptocurrencies would enable a more robust and nuanced understanding of the scope of the issue, thereby facilitating the development of appropriate policy responses.
- Transparency in methodological approaches is crucial in different studies that examine the extent to which cryptocurrencies are used on the dark web. Continuing to enhance efforts to promote transparency and information sharing within the research community will be vital in establishing trustworthiness of a given source and triangulating information from various sources.
- A stronger theoretical basis for research on cybercrime is needed more widely, including, for example, integration of relevant research and conceptual approaches from related fields such as criminology. This could include research around the behaviour of criminals, such as reluctance towards the early adoption of new technology or general adversity to risk.
- A more sophisticated understanding of the suitability of privacy coins for conducting illicit and criminal activities would also enable a more granular understanding of the different drivers that shape malicious actors' selection of one cryptocurrency over another for their purposes. This should include an examination of the numerous privacy coins and the variety in their suitability.

[145] Interviewee 13.

# References

Abrosimova, Tanya. 2019. 'Volatility and poor usability slows down crypto adoption - Charlie Lee.' FXStreet, 26 May 2019. As of 11 February 2020: https://www.fxstreet.com/cryptocurrencies/news/volatility-and-poor-usability-slows-down-crypto-adoption-charlie-lee-201903260934

Ahn, Gail-Joon, Adam Doupe, Ziming Zhao & Kevin Liao. 'Ransomware and cryptocurrency: partners in crime.' In *Cybercrime Through an Interdisciplinary Lens*, 119–140. London: Routledge.

Albrecht, Chad, Kristopher McKay Duffin, Conan Albrecht & Victor Manuel Morales Rocha. 2019. 'The use of cryptocurrencies in the money laundering process.' *Journal of Money Laundering Control* 22: 210–16. doi:10.1108/JMLC-12-2017-0074

Aldridge, J., & D. Décary-Hétu. 2016. 'Hidden Wholesale: The drug diffusing capacity of online drug cryptomarkets.' *International Journal of Drug Policy* 35: 7–15. doi:10.1016/j.drugpo.2016.04.020

Aldridge, Judith, and David Décary-Hétu. 2016. 'Cryptomarkets and the future of illicit drug markets.' *The Internet and drug markets* 23–32.

Auer, Raphael, & Stijn Claessens. 2018. 'Regulating cryptocurrencies: assessing market reactions.' *BIS Quarterly Review*. As of 11 February 2020: https://www.bis.org/publ/qtrpdf/r_qt1809f.pdf

Barone, Raffaella, & Donato Masciandaro. 2018. 'Cryptocurrency or Usury? Crime and Alternative Money Laundering Techniques.' Milan, Italy: Universita Bocconi. Working Paper No. 101. As of 11 February 2020: http://ssrn.com/abstract=3303871

*BBC*. 2019. TalkTalk hacker Elliott Gunton: Cryptocurrency auctioned by police. 30 September. As of 11 February 2020: https://www.bbc.com/news/uk-england-norfolk-49880630

Ben-Sasson, Eli, Alessandro Chiesay, Christina Garmanz, Matthew Greenz, Ian Miersz, Eran Tromerx & Madars Virzay. 2014. 'Zerocash: Decentralized Anonymous Payments from Bitcoin.' doi:10.1109/SP.2014.36 As of 11 February 2020: http://zerocash-project.org/media/pdf/zerocash-oakland2014.pdf

Biryukov, Alex, and Daniel Feher. 2018. 'Deanonymization of Hidden Transactions in Zcash.' University of Luxembourg.

Biryukov, Alex, & Daniel Feher. 2019. 'Privacy and Linkability of Mining in Zcash.' Washington, DC: 2019 IEEE Conference on Communications and Network Security (CNS). doi:10.1109/CNS.2019.8802711. As of 11 February 2020: https://ieeexplore.ieee.org/document/8802711

Biryukov, Alex, Daniel Feher & Giuseppe Vitto. 2019. 'Privacy Aspects and Subliminal Channels in Zcash.' In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, pp. 1813-1830. 2019.

*Blockchain*. 2020. 'Number Of Transactions Excluding Chains Longer Than 10.' As of 11 February 2020: https://www.blockchain.com/charts/n-transactions-excluding-chains-longer-than-10?

Broadhurst, Roderic G., David Rowan Lord, Donald Maxim, Hannah Woodford-Smith, Bianca Sabol, Ho Chung, Corey Johnston & Bryan Matamoros-Marcias. 2018. 'Malware Trends on 'Darknet' Crypto-markets: Research Review.' Canberra, Australia: ANU Cybercrime Observatory. doi:10.13140/RG.2.2.36312.60168. As of 11 February 2020: http://regnet.anu.edu.au/research/publications/7377/malware-trends-%E2%80%98darknet%E2%80%99-crypto-markets-research-review

Buntinx, JP. 2017. 'The Shadow Brokers Only Accept ZCash Payments for Their Monthly Dump Service.' The Merkle, 30 May 2017. As of 11 February 2020: https://themerkle.com/the-shadow-brokers-only-accept-zcash-payments-for-their-monthly-dump-service/

Buskirk, J., Roxburgh, A., Naicker, S., & Burns, L. 2015. 'A response to Dolliver's "Evaluating drug trafficking on the Tor network"'. *International Journal of Drug Policy*. 26(11), 1126–1127.

Campbell-Verduyn, Malcolm. 2018. 'Bitcoin, crypto-coins, and global anti-money laundering governance.' *Crime, Law and Social Change* 69: 283–305. doi:10.1007/s10611-017-9756-5

Carlisle, David, & Kayla Izenman. 2019. 'Closing the Crypto Gap Guidance for Countering North Korean Cryptocurrency Activity in Southeast Asia.' London: Royal United Services Institute. RUSI Occasional Paper, April. As of 11 February 2020: https://rusi.org/sites/default/files/20190412_closing_the_crypto_gap_web.pdf

Carlisle, David. 2019. 'Countering The Use Of Cryptocurrencies For Terrorist Financing.' Elliptic, 13 February 2019. As of 11 February 2020: https://www.elliptic.co/our-thinking/countering-terrorist-financing-cryptocurrency

Carroll, Paul, & James Windle. 2018. 'Cyber as an enabler of terrorism financing, now and in the future.' *Journal of Policing, Intelligence and Counter Terrorism* 13(3): 285–300. doi:10.1080/18335330.2018.1506149

Chohan, Usman W. 2019. 'Initial coin offerings (ICOs): Risks, regulation, and accountability.' In *Cryptofinance and Mechanisms of Exchange*, edited by Stéphane Goutte, Khaled Guesmi & Samir Saadi, 165–77. Springer, Cham.

Christin, Nicolas. 2013. 'Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace.' In *Proceedings of the 22nd international conference on World Wide Web*, 213–224. New York:ACM.

*CipherTrace*. 2019. Cryptocurrency Anti-Money Laundering Report, 2019 Q2. Report-CAML-20190812. As of 11 February 2020: https://ciphertrace.com/q2-2019-cryptocurrency-anti-money-laundering-report/

*CoinMarketCap*. 2020. All Cryptocurrencies. As of 11 February 2020: https://coinmarketcap.com/all/views/all/

*Dark Web Solutions*. 2020. Dark Web Monitor. As of 11 February 2020: https://dws.pm/tools/monitor/

Darknet Live. 2019. Potential 'Exit Scam' Imminent After Nightmare Market Breach. As of 11 February 2020: https://darknetlive.com/posts/nightmare-market-market-hacker-wreaks-havoc-on-the-darkweb/

Desmond, Dennis B., David Lacey & Paul Salmon. 2019. 'Evaluating cryptocurrency laundering as a complex socio-technical system: A systematic literature review.' *Journal of Money Laundering Control*. doi:10.1108/JMLC-10-2018-0063

Dion-Schwarz, Cynthia, David Manheim & Patrick B. Johnston. 2019. *Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats*. Santa Monica, Calif.: RAND Corporation. RR-3026. As of 11 February 2020: https://www.rand.org/pubs/research_reports/RR3026.html

Dolliver, D. S. 2015. 'A rejoinder to authors: Data collection on Tor'. *International Journal of Drug Policy***.** 26(11), 1128–1129.

Dorofeyev, M., M. Kosov, V. Ponkratov, A. Masterov, A. Karaev & M. Vasyunina. 2018. 'Trends and prospects for the development of blockchain and cryptocurrencies in the digital economy.' *European Research Studies Journal* 21(3): 429–45.

*ECC (Electric Coin Company)*. 2020a. Parameter Generation. As of 11 February 2020: https://z.cash/technology/paramgen/

———. 2020b. What are zk-SNARKs? As of 11 February 2020: https://z.cash/technology/zksnarks/

——— (homepage). 2020c. Zcash. As of 11 February 2020: https://z.cash/

Fanusie, Yaya J., & Tom Robinson. 2018. 'Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services.' Center on Sanctions and Illicit Finance & Elliptic. As of 11 February 2020: https://info.elliptic.co/whitepaper-fdd-bitcoin-laundering

FATF. 2019. The FATF Recommendations. As of 11 February 2020: http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html

Foley, Sean, Jonathan R. Karlsen & Tālis J. Putniņš. 2018. 'Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?' *The Review of Financial Studies* 32(5): 1798–853. doi: 10.1093/rfs/hhz015

Foley, Sean, Jonathan R. Karlsen & Tālis J. Putniņš. 2019. 'Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?' *The Review of Financial Studies* 32(5): 1798–853.

Goldman, Zachary K, Ellie Maruyama, Elizabeth Rosenberg, Edoardo Saravalle & Julia Solomon-Strauss. 2017. 'Terrorist Use of Virtual Currencies: Containing the Potential Threat.' Washington, DC: Center for a New American Security. As of 11 February 2020: https://www.cnas.org/publications/reports/terrorist-use-of-virtual-currencies

Kappos, George, Haaroon Yousaf, Mary Maller & Sarah Meiklejohn. 2018. 'An Empirical Analysis of Anonymity in Zcash.' Baltimore, MD: Proceedings of the 27th USENIX Security Symposium. As of 11 February 2020: https://www.usenix.org/conference/usenixsecurity18/presentation/kappos

Kethineni, Sesha, and Ying Cao. 2019. 'The rise in popularity of cryptocurrency and associated criminal activity.' *International Criminal Justice Review*. doi:10.1177/1057567719827051.

Kirkpatrick, Keith. 2017. 'Financing the dark web.' *Communications of the ACM* 60(3): 21–2. doi:10.1145/3037386 As of 11 February 2020: https://cacm.acm.org/magazines/2017/3/213816-financing-the-dark-web/fulltext

Kruithof, Kristy, Judith Aldridge, David Décary-Hétu, Megan Sim, Elma Dujso & Stijn Hoorens. 2016. 'Internet-facilitated drugs trade: An analysis of the size, scope and the role of the Netherlands.' Santa Monica, Calif.: RAND Corporation. RR-1607-WODC. As of 11 February 2020:
https://www.rand.org/pubs/research_reports/RR1607.html

Lee, Seunghyeon, Changhoon Yoon, Heedo Kang, Yeonkeun Kim, Yongdae Kim, Dongsu Han, Sooel Son & Seungwon Shin. 2019. 'Cybercriminal Minds: An investigative study of cryptocurrency abuses in the Dark Web.' San Diego, CA: Network and Distributed Systems Security (NDSS) Symposium. doi:10.14722/ndss.2019.23055.

Leonard, David, & Horst Treiblmaier. 2019 'Can cryptocurrencies help to pave the way to a more sustainable economy? Questioning the economic growth paradigm.' In *Business Transformation through Blockchain,* 183–205. Palgrave Macmillan, Cham.

Martis, Genesis. 2018. 'A guidance to understand hawala and to establish the nexus with Terrorist financing.' London: Association of Certified Anti-Money Laundering Specialists. As of 11 February 2020:
http://files.acams.org/pdfs/2018/A_Guidance_to_Understanding_Hawala_G_Martis.pdf

Matthews, Owen. 2017. 'Bitcoin and Blockchain: A Russian Money Laundering Bonanza?' Newsweek, 18 September. As of 11 February 2020:
https://www.newsweek.com/russia-finally-embracing-virtual-currencies-666794

Mead, Derek. 2013. 'The Rhino Horn Crisis and the Darknet.' Vice News, 24 January. As of 11 February 2020:
https://www.vice.com/en_us/article/vvvnj4/rhino-horn-crisis-and-the-darknet

*Merriam-Webster*. 2020. Cryptocurrency. As of 11 February 2020:
https://www.merriam-webster.com/dictionary/cryptocurrency

Miers, Ian, Christina Garman, Matthew Green & Aviel D. Rubin. 2013. 'Zerocoin: Anonymous Distributed E-Cash from Bitcoin.' 2013 IEEE Symposium on Security and Privacy. doi:10.1109/SP.2013.34. As of 10 January 2020:
https://ieeexplore.ieee.org/document/6547123

Moiseienko, Anton, & Kayla Izenman. 2019. 'From Intention to Action: Next Steps in Preventing Criminal Abuse of Cryptocurrency.' London: Royal United Services Institute. RUSI Occasional Paper. As of 11 February 2020:
https://rusi.org/sites/default/files/20190911_intention_to_action_web.pdf

Munksgaard, Rasmus, Jakob Demant, and Gwern Branwen. 2016. 'A replication and methodological critique of the study "Evaluating drug trafficking on the Tor Network".' *International Journal of Drug Policy*. 35: 92-96.

Ndinga, Eli. 2019. 'The State of Privacy Coins.' Mosaic, 3 July. As of 11 February 2020:
https://medium.com/@eliezer.ndinga/the-state-of-privacy-coins-b873982acbe4

Olson, Eric, & Jonathan Tomek. 2017. 'Cryptocurrency and the BlockChain: Technical Overview and Potential Impact on Commercial Child Sexual Exploitation.' Prepared for the Financial Coalition Against Child Pornography (FCACP) & the International Centre for Missing & Exploited Children (ICMEC). As of 11 February 2020:
https://www.icmec.org/wp-content/uploads/2017/05/ICMEC-FCACPCryptocurrencyPaperFINAL5-17.pdf

Paul, Katie A. 2018. 'Ancient Artifacts vs. Digital Artifacts: New Tools for Unmasking the Sale of Illicit Antiquities on the Dark Web.' *Arts* 7(2): 12. doi:10.3390/arts7020012

Persi Paoli, Giacomo, Judith Aldridge, Nathan Ryan & Richard Warnes. 2017. 'Behind the curtain: The illicit trade of firearms, explosives and ammunition on the dark web.' Santa Monica, Calif.: RAND Corporation. RR-2091-PACCS. As of 11 February 2020: https://www.rand.org/pubs/research_reports/RR2091.html

Quesnelle, Jeffrey. 2017. 'On the linkability of Zcash transactions.' arXiv preprint arXiv:1712.01210.

*Radiolab.* 2017. The Ceremony. WNYC Studios, 14 July. As of 11 February 2020: https://www.wnycstudios.org/podcasts/radiolab/articles/ceremony

Syska, Samantha J. 2016. 'Eight-years-young: How the New York BitLicense stifles Bitcoin innovation and expansion with its premature attempt to regulate the virtual currency industry.' *The Journal of High Technology Law* 17: 313.

Thibodeau, Mary. 2019. 'Will Privacy Coins like Monero Survive Regulation?' Hedge Trade, 25 February. As of 11 February 2020: https://hedgetrade.com/will-privacy-coins-like-monero-survive-regulation/

Todorof, Maria. 2019. 'FinTech on the Dark Web: the rise of cryptos.' *ERA Forum* 20: 1–20. doi: 10.1007/s12027-019-00556-y

Tramer, Florian, Dan Boneh & Kenneth G. Paterson. 2019. 'PING and REJECT: The Impact of Side-Channels on Zcash Privacy.'

*US DOJ.* AlphaBay, Largest Online 'Dark Market', Shut Down. 20 July. As of 11 February 2020: https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down

van Wegberg, Rolf, Jan-Jaap Oerlemans & Oskar van Deventer. 2018. 'Bitcoin money laundering: mixed results?' *Journal of Financial Crime* 25(2): 419–35. doi:10.1108/JFC-11-2016-0067

Weimann, Gabriel. 2018. 'Going Darker? The Challenge of Dark Net Terrorism.' Washington, DC: Wilson Center. As of 11 February 2020: https://www.wilsoncenter.org/publication/going-darker-the-challenge-dark-net-terrorism

Zcash. 2019a. Zcash Regulatory Brief. As of 11 February 2020: https://z.cash/wp-content/uploads/2019/09/Zcash-Regulatory-Brief-201909.pdf

———. 2019b. Zcash Draft Risk Assessment. Not publicly available.

ZChain. 2020. Total value exchanged over a given pool type. Zchain Explorer. As of 11 February 2020: https://explorer.zcha.in/statistics/values

# Annex A. Methodology

## A.1. Overview of approach

This study had two overarching research tasks, as shown in Table A.1. The following sections within this annex provide further information on each task, as well as underlying assumptions and limitations.

**Table A.1 Overview of approach**

| Research task | Research approach |
|---|---|
| Task 1: Identify the nature and scale of Zcash usage on dark web markets | Use the RAND Dark Web Observatory (DWO) to extract the number of markets and vendors accepting Zcash as form of payments. |
| Task 2: Examine other illicit uses of Zcash | Conduct literature review and key informant interviews. |

### A.1.1. Task 1: Identify the nature and scale of Zcash usage on dark web markets

Task 1 of this study entailed the primary exploration of which cryptocurrencies are most commonly accepted and used on dark web markets. The main purpose of this task was to gather and assess the available evidence regarding to what extent dark web marketplaces accept Zcash and how this compares to other cryptocurrencies. This was done using the tools of the RAND Dark Web Observatory (DWO). The DWO aggregates listing descriptions into a single text-formatted field, which is often used by vendors to communicate their accepted methods of payment. The research team began by using 'mentions' of select cryptocurrencies in these description fields as a proxy for 'accepted methods of payment'. For these purposes, a mention can be defined as a case-insensitive, whole-word match on the text content. As an example, consider the text 'Methamphetamine'. While it contains the correct letter sequence, E-T-H, a common abbreviation for the Ethereum cryptocurrency, it is not a whole-word match. On the other hand, the text 'bitcoin, eth, monero, cc' is a whole-word and case-insensitive match for ETH.

Additionally, the term 'unique' was used to describe a single listing with a unique 'Offer ID' field, of which there may be multiple observations. This typically occurs after multiple web scraping sessions where the same listing is re-scraped. These kinds of duplicate listings are treated collectively as a single listing and therefore counted only once. This study focused exclusively on a listing's 'description' field. For example, for a listing titled '250.000 Fullz records from Hospital' (presumably a dump of hacked hospital data), the description is shown in Box 3. The relevant cryptocurrency information that matches the search criteria has been highlighted. Note that, although additional cryptocurrency information (e.g. ccbtc, lbc) may be provided by the vendor, this is not detected by this search approach.

### Box 3 Example of listing description

FORMAT:

FIRST_NAME | MIDDLE_NAM | LAST_NAME | RACE | STATE | GENDER | SKIN | HAIR | EYE | BIRTH_DATE | SSN | BIRTH_CITY | HEIGHT | WEIGHT | STREET | CITY | STATE | ZIP | PHONE | DL_NR | DL_STATE

+ Financial info

Small sales will continue but for those who are interested in bigger database for themselves or for resell:

-250.000 Records from Hospital

-These will be all ages and no selection possible

Name address ssndob and much more is completed for all

The majority of these are able to pay for hospital and have good credit score all around

==========

SEARCHTAGS

==========

US, United states, USA fullz, Florida fullz, New jersey fullz, New york fullz, apple, vmware, coupons, moneybookers, Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Pennsylvania fullz, Illinois fullz, bitcoin, btc, verizon, twc, comcast, spectrum, xfinity, hulu, hbo, nba, premium, account, spotify, deezer, netflix, passport, mcdonalds, loan, fraud, watches, diamonds, lump sum, documents, carding tutorial, paypal to bitcoin, cc to bitcoin, cvv, cvc, vcc, virtual, credit, card, virtual credit card, cashoutmoneyteam, pp, id, identification, mdma, steam, origin, instagram, pediatrician, under 18, minor, kids, children, kids fullz, children fullz, kid profile, hospital, patient, facebook, crunchyroll, , cc to pp, cc to btc, ccbtc, cc2btc, refund, doubledip, amazon, ebay, paypal, skill, neteller, payza, coinbase, coinmama, freelancer, aliexpress, card, carder, carding, creditcard, cc, msc, vbv, visa, mastercard, discover, money making, money, followers, likes, youtube, scam, scamming, scams, dox, doxing, doxx, profile, profiles, full, fulls, fullz, fuls, cc fullz, ssndob, ssn, dob, date of birth, social security number, vpn, hbo, western union, WU, liqpay, flight, flights, hotel, hotels, bookings, expedia, transunion, experian, cyberteacher, banned, ebooks, bannedebooksewhoring, e-whoring, ewhore, kalashnikov, isellpizza, courvoisier, antonsen, expectus, hansa, euro, usd, scans, rdp, vps, server, remote, desktop, protocol, bangbus, brazzers, pornhub, playboy, hackpack, hacking, hackers, white hat, gray hat, grey hat, blackhat, black hat, giftcard, gift, card, voucher, funds, transfer, qvc, school of travel, groupon, nectar, british airways, deliveroo, subway, mcdonalds, data, cloud, service, hosting, socks, proxy, socks4, socks5, ssh, bitvise, antidetect, fraudfox, localbitcoins, lbtc, lbc, monero, zcash, payment error, phone, gva, google voice, google voice account, counterfeit, airbnb, crypto, template, w99, taxes, IRS, tax, skype, cheque, cheques, check, checks, secure, securing, security, keylogger, administrator, windows, hack, password, stealer, RAT, booter, access, trojan, PSD, PDF, fresh, tickets, shows, disney, theatre, concert, vip72, luxsocks, premsocks, xdedic, spambot, megapack, university, lessons, gmail, samsung, iphone, android, galaxy, note, s7, balance, cerified, certification, ceritfy, moneygram, fargo, wells, wells fargo, trick, suntrust, boa, bank of america, capital one, capone, cap1, citibank, schwabbs, fidelity, chase, chase bank, surveillance, camera, webcam, TD, SSN, social security number, valid_cc_info, st0ned, redson, GGMcloud, kriminal, pastebin, spider, theshop, thinkingforward, certificate, apple, vmware, coupons, moneybookers, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, New York, Nevada Fullz, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Utah, Vermont, Virginia, Washington, West Virginia, Wisconsin, Wyoming, California fullz, eastcoast, westcoast, skyscraper

=========

### A.1.2. Assumptions and limitations

The main assumptions that underpin this analysis are:

1. The use of 'mentions' of select cryptocurrencies as a proxy for 'accepted methods of payment'
2. A focus on the listings' 'description' field
3. The use of rudimentary 'regular expressions' for matching text.

These limitations have a number of implications on the robustness of the data gathered and the findings derived from analysis of that data. One is false positives. Since the approach uses cryptocurrency mentions as a proxy for accepted methods of payment, this will generate false positives. For example, a listing titled 'How to buy ETHERIUM with CC or PP 2017 new GUIDE' purports to sell a guide for purchasing Ethereum. There is no way to tell whether or not the vendor actually accepts Ethereum as payment. Similarly, the naïve whole-word matching for 'ETH' can still produce false positives. An example of this in action would be a listing for 'ETH-LAD Blotters' for LSD consumption.

Another challenge is capturing full context and detail for any listings. Focusing on the 'description' field is valid, for example, but may miss additional information by, say, ignoring a listing's title.

### A.1.3. Task 2: Examine other illicit uses of Zcash

Task 2 comprised the exploration of how cryptocurrencies are used for illicit purposes and how the use of Zcash compares to other leading cryptocurrencies. The primary purpose of this task was to understand the available evidence base on how different cryptocurrencies are used for illicit purposes, terrorist purposes and the laundering of funds from offline and online crime, as well as to examine estimates of how much cryptocurrency value is generated from illicit activities (e.g. as a result of hacking or theft).

This task was primarily carried out through a structured document and literature review activity. The aim of the literature review was to collect, analyse and synthesise scientific and 'grey' literature[146] about the use of cryptocurrencies, including Zcash. This review followed these seven steps:

1. Protocol development
2. Identification of relevant literature
3. Study selection
4. Data extraction
5. Quality assessment
6. Synthesis of the evidence
7. Interpretation of the findings.

The exact search protocol (Step 1) was developed at the start of the project alongside RAND's Knowledge Services team. The study team determined that the best way to identify relevant literature in this space would be by conducting two parallel searches: one that specifically focused on Zcash and research into the illicit use of Zcash, and one that compared the illicit use of Zcash with the illicit use of other cryptocurrencies, particularly Bitcoin, Ethereum, Monero and Litecoin. Search strings are illustrated in Box 4. Sources which discussed the technical underpinnings of these cryptocurrencies and the economics of cryptocurrencies (e.g. market cap, trade volume, etc.) were excluded from the search parameters. Other restrictions included only considering sources published from 2016 onwards and in the English language.

[146] Grey literature is documents and research produced by organisations outside of the traditional commercial or academic publishing and distribution channels.

**Box 4 Search strings**

TITLE-ABS-KEY ( ( cryptocurrenc* OR "crypto currenc*" OR "crypto market" OR "cryptocurrency market" OR "crypto currrency market" OR bitcoin OR ethereum OR monero OR litecoin ) AND ( malware OR illicit OR malicious OR criminal OR breach OR vulnerab* OR crime OR crimes OR "dark web" OR darkweb OR darknet OR onion OR tor OR "money laundering" OR terroris* OR cryptojacking OR "crypto jacking" OR "crypto-jacking" OR drugs ) ) AND ( LIMIT-TO ( PUBYEAR , 2020 ) OR LIMIT-TO ( PUBYEAR , 2019 ) OR LIMIT-TO ( PUBYEAR , 2018 ) OR LIMIT-TO ( PUBYEAR , 2017 ) ) AND ( LIMIT-TO ( LANGUAGE , "English" ) )

The search strings outlined in Box 4 were applied to title OR abstract OR keyword, thus casting the net for data capture as wide as possible within the limitations described above. Searches were conducted in SCOPUS, the largest of the academic literature databases, and Nexus, which indexes newspapers, blogs and press releases from around the world. The following document types were included in this search: peer-reviewed sources (journal articles, book chapters, books, or conference papers), newspapers, magazines and blogs. This search was conducted in 11 unique datasets:

- SCOPUS
- Web of Science
- Academic Search Complete
- Military Database
- Policy File
- Criminal Justice Abstracts
- Public Affairs International Service (PAIS) Index
- IEEExplore
- ACM Guide to Computing Literature
- Business Source Complete
- Business eBooks

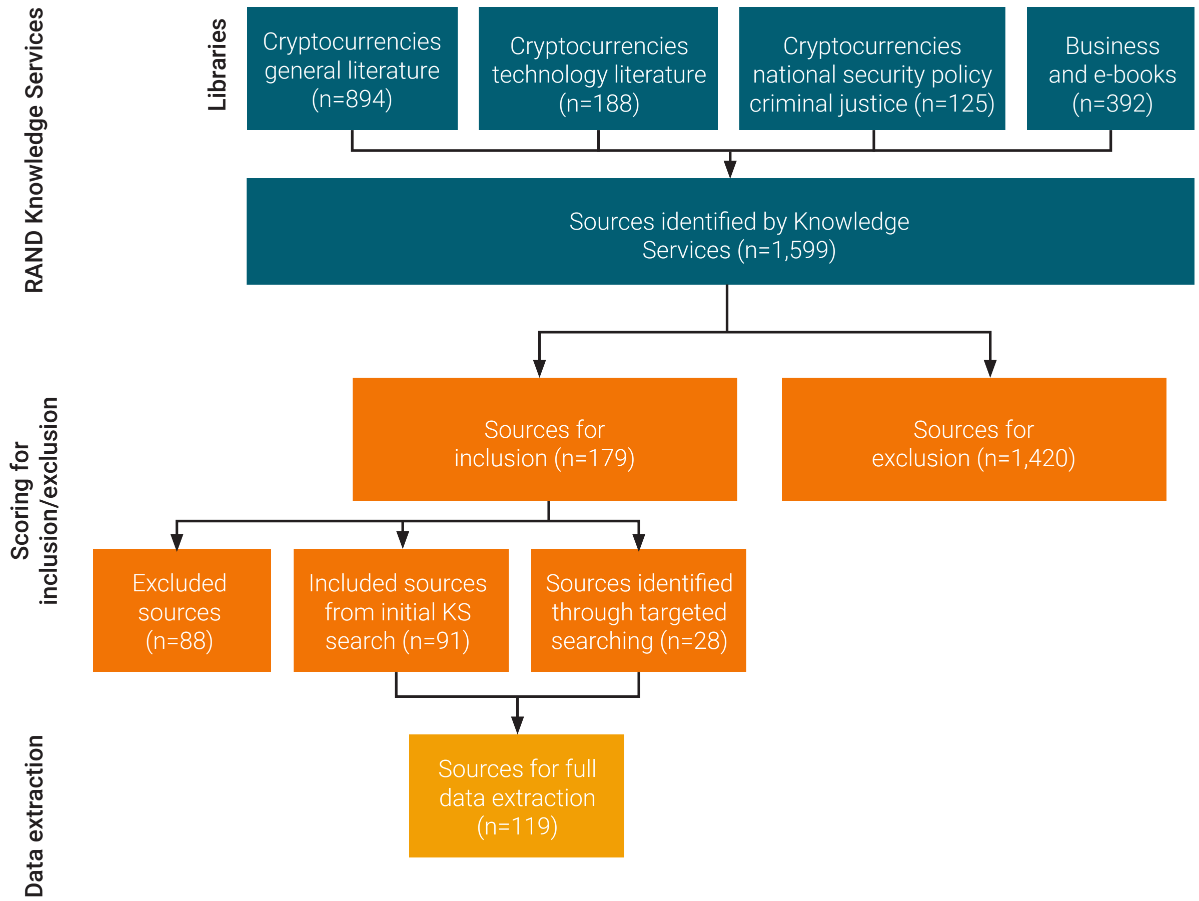
Upon completion of this search, a total of 2,479 sources were identified. Once duplicates were removed, 1,599 hit counts remained. These were subsequently filtered into four libraries. The study team went through all 1,599 sources in order to determine their relevance to the study. At this stage, the decision to include/exclude a given source was made on the basis of its title and abstract.

Of these 1,599 sources, 179 were assessed as being relevant to the study. These sources were then mapped against a data extraction matrix, which captured relevant information on the illicit use of cryptocurrencies, including Zcash, for a variety of criminal and terrorist purposes. Furthermore, 47 additional sources were included that had been identified through targeted searching and through referrals during our interviews. The total number of sources that were considered in the qualitative literature review was thus 226.

In addition to the collection and analysis of scientific and grey literature on cryptocurrency, the RAND team also conducted semi-structured key informant interviews[147] with experts such as law enforcement and private sector representatives (e.g. financial intelligence services, exchange service providers, etc.) in order to further examine the

[147] Semi-structured interviews allow more scope to explore interviewees' points of view in a more detailed manner. This type of interview uses a series of open- and closed-ended questions, providing the opportunity to respond, probe and follow-up the interviewees' answers.

Figure A.1 Sources considered for literature and evidence review


RAND Knowledge Services
Libraries
Cryptocurrencies general literature (n=894)
Cryptocurrencies technology literature (n=188)
Cryptocurrencies national security policy criminal justice (n=125)
Business and e-books (n=392)
Sources identified by Knowledge Services (n=1,599)
Scoring for inclusion/exclusion
Sources for inclusion (n=179)
Sources for exclusion (n=1,420)
Excluded sources (n=88)
Included sources from initial KS search (n=91)
Sources identified through targeted searching (n=28)
Data extraction
Sources for full data extraction (n=119)

characteristics of cryptocurrency use. A total of 61 experts were engaged by the study team, all of whom were identified through desk research and through snowball sampling.[148] Of these, 15 interviews were completed via telephone interviews, which captured expert views on and knowledge of the topic and complement and validate the literature review findings.

[148] Snowball sampling can be defined as a technique for finding research subjects whereby existing subjects recruit or refer future subjects from within their network. When applied to a literature review, one source leads to another and the effect is that the literature considered is said to grow like a rolling snowball.

# Annex B. List of interviewees

Please note that the list of interviewees below do not correspond to the references to anonymised interviewees throughout the report. No comments or quotations within the report are attributed to individual interviewees.

This annex lists those interviewees who have consented to be identified by name, role and/or organisation for their inputs throughout the course of this study.

**Table B.1 List of key informant interviewees**

| Name | Role | Organisation |
|---|---|---|
| Antoine Martin | Senior Vice President | Federal Reserve Bank of New York |
| Bernhard Haslhofer | Senior Data Analyst | Austrian Institute of Technology |
| David Jevans | Chief Executive Officer | CipherTrace |
| Jonathan Karlsen | PhD Candidate | University of Technology Sydney |
| Nick Furneaux | Managing Director | CSITech |
| Sean Foley | Senior Lecturer | University of Sydney |
| Tālis J. Putniņš | Professor | University of Technology Sydney |
| Yaya Fanusie | Adjunct Senior Fellow | Center for a New American Security |
| Anonymous | - | University College London |
| Anonymous | - | Elliptic |
| Anonymous | - | - |
| Anonymous | - | - |
| Anonymous | - | - |
| Anonymous | - | - |
| Anonymous | - | - |