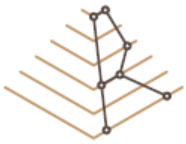

RAMSES

RAMSES

Internet Forensic platform for tracking the money flow of financially-motivated malware

H2020 - 700326

D6.2 Altcoins: Alternatives to Bitcoin and their increasing presence in Malware-related Cybercrime

Lead Authors:

Darren Hurley-Smith (UNIKENT), Julio Hernandez-Castro (UNIKENT)

With contributions from:

Edward Cartwright (UNIKENT), Anna Stepanova (UNIKENT)

Reviewers:

Luis Javier Garcia Villalba (UCM)

Deliverable nature:	Report (R)
Dissemination level: (Confidentiality)	Public (PU)
Contractual delivery date:	31/08/2017
Actual delivery date:	31/08/2017
Version:	1.0
Total number of pages:	36
Keywords:	Cryptocurrency, altcoin, malware, darknet market, privacy

Abstract

Bitcoin is a relatively well-known cryptocurrency, a digital token representing value. It uses a blockchain, a distributed ledger formed of blocks which represent a network of computers agreeing that transactions have occurred, to provide a ledger of sorts. This technology is not unique to Bitcoin, many so-called 'altcoins' now exist. These alternative coins provide their own services, be it as a store of value with improved transactions (lower fees, higher speed), or additional privacy. Malware and Dark Net Market (DNM) operators have used Bitcoin to facilitate pseudo-anonymous extraction of value from their victims and customers. However, several high-profile arrests have been made using Bitcoin transaction graphing methods, proving that the emphasis is on the pseudo part of pseudo-anonymity. Altcoins specialising in masking the users' identity – Monero, ZCash, and Dash – are therefore of interest as the next potential coins of choice for criminals. Ethereum, being the second largest crypto-currencies and imminently implementing its own privacy features, is also of interest. This report profiles the best-performing altcoins likely to be of interest to malware operators.

[End of abstract]

Executive summary

This report introduces the reader to altcoins, cryptocurrencies other than Bitcoin. These currencies vary in nature, from stores of value (like Bitcoin) to service-driven mini-economies. This leads to a dizzying array of different cryptocurrencies, some in competition, others existing (for now) in their own niche.

Altcoins have proven useful for many different tasks, but they have begun to become a notable component in cyber-criminal activity. This report assists readers in understanding the emerging role of altcoins in cybercriminal activity by:

- Outlining the highest-performing altcoins in terms of market capitalisation, social media commentary and proven criminal usage
- Drawing on the technical definitions of privacy-focused altcoins (Monero, ZCash, Dash) to outline how they resist current transaction graphic techniques, and where possible outline criticisms or potential vulnerabilities.
- Providing a technical, financial and criminological analysis of each discussed altcoin. Where possible, this includes examples of malware or Dark Net Market (DNM) activity related to the coins in question.

The key observations and findings of this report are:

- Monero and ZCash represent a significant roadblock for current blockchain analysis techniques. Transaction graphic as a form of data forensics is very effective on Bitcoin, Ethereum and transparent (instant send) Dash transactions. Such methods will remain relevant for a while yet, as public knowledge about Bitcoin vulnerabilities is irregular in its distribution: many communities who are otherwise privacy focused hold on to some incorrect perceptions of how Bitcoin protects their identities.
- Monero uses ring signatures to provide anonymity, masking public addresses and decorrelating inputs from outputs from the perspective of unprivileged observers. Only the endpoints have the privileged information required to gain further information about their transactions (and then only their portion of it). This makes blockchain analysis impossible with current techniques. Monero has been used to launder the proceeds of the Wannacry Ransomware attack of 2017, and is a listed currency option on several DNM (including the late Alphabay and Hansa markets).
- ZCash and Dash have little to no presence in social media and legal investigations of cybercriminal activity, but do offer significant improvements in terms of protecting user-data. There is some criticism in the Monero and Ethereum communities, as well as several prominent crypto-bloggers, regarding potential vulnerabilities in Dash. Specifically, there are fears of a potential double-spend vulnerability in the instant send functionality, and reports suggests that only 28|% of users make use of the privacy features. This may mean that Dash is popular for its cheap and faster transactions and that its privacy features are not as ‘use-tested as those of Zcash and Monero.
- Ethereum, although not a privacy-focused currency, is planning to implement privacy features. The ZCash team is working closely with Ethereum developers to introduce zK-Snarks, which will allow the use of zero-knowledge proofs to provide opaque transactions in the future. The foundations for this will be laid in the Metropolis hard-fork later this year. It is yet unknown as to what effect this will have on transaction fees and speeds. Currently, Ethereum runs a transparent blockchain in the same way as Bitcoin, but offers significantly lower fees and faster transaction speeds. It is the second most capitalised currency at present, at 38% of the Bitcoin market cap at time of writing.
- Ethereum and Monero have both appeared in ransomware demands, and have a small but growing DNM presence.

Document Information

IST Project Number	700326	**Acronym**	RAMSES
Full Title	Internet Forensic platform for tracking the money flow of financially-motivated malware		
Project URL	http://www.ramses2020.eu		
EU Project Officer	Nada Milisavljevic		

Deliverable	Number	D6.2	Title	
Work Package	Number	WP6	Title	

Date of Delivery	Contractual	M12	Actual	M12
Status	version 1		final x	
Nature	prototype □ report x demonstrator □ other □			
Dissemination level	public x restricted □			

Authors (Partner)	UNIKENT			
Responsible Author	Name	Darren Hurley-Smith Julio Hernandez-Castro	E-mail	Dh433@kent.ac.uk j.c.hernandez-castro@kent.ac.uk
	Partner	UNIKENT	Phone	07870806745

Abstract (for dissemination)	Bitcoin is a relatively well-known cryptocurrency, a digital token representing value. It uses a blockchain, a distributed ledger formed of blocks which represent a network of computers agreeing that transactions have occurred, to provide a ledger of sorts. This technology is not unique to Bitcoin, many so-called 'altcoins' now exist. These alternative coins provide their own services, be it as a store of value with improved transactions (lower fees, higher speed), or additional privacy. Malware and Dark Net Market (DNM) operators have used Bitcoin to facilitate pseudo-anonymous extraction of value from their victims and customers. However, several high-profile arrests have been made using Bitcoin transaction graphing methods, proving that the emphasis is on the pseudo part of pseudo-anonymity. Altcoins specialising in masking the users' identity – Monero, ZCash, and Dash – are therefore of interest as the next potential coins of choice for criminals. Ethereum, being the second largest crypto-currencies and imminently implementing its own privacy features, is also of interest. This report profiles the best-performing altcoins likely to be of interest to malware operators.
Keywords	Cryptocurrency, altcoin, malware, darknet market, privacy

Version Log			
Issue Date	Rev. No.	Author	Change
11/07/2017	0.1	Darren Hurley-Smith	Initial draft
31/07/2017	0.2	Darren Hurley-Smith	Changes due to significant developments in the target domain (Alphabay and Hansa shutdowns)
11/08/2017	0.3	Darren Hurley-Smith	Internal draft prior to submission to UCM: Further changes to incorporate discussion of Wannacry cash out via Monero.
14/08/2017	0.4	Julio Hernandez-Castro	Tracked changes: modifications and suggestions for improvement as part of UNIKENT internal review.
14/08/2017	0.5	Darren Hurley-Smith	Final draft prior to UCM proof read. Submitted to RAMSES consortium on date of authorship.
26/08/2017	0.6	Luis Javier Garcia Villalba	Review copy, including corrections and suggestions.
29/08/2017	1	Darren Hurley-Smith	Final copy, incorporating feedback and adding abstract and all relevant frontmatter.

Table of Contents

List of Figures

Abbreviations

BCH: Bitcoin Cash

BTC: Bitcoin

DNM: Dark Net Market

ETC: Ethereum Classic

ETH: Ethereum

XMR: Monero

ZEC: ZCash

Definitions

Blockchain: A type of distributed ledger, originally proposed by the pseudonymous Satoshi Nakamoto. It is the basis for Bitcoin and all cryptocurrencies use some derivative of this technology, with various technological improvements and additions entering the marketplace from, 2014 onwards.

Cryptocurrency: Digital currency, based on blockchain technology. The currency may be a derivative of an existing currency, a fork of an existing currency, or its own standalone blockchain. The currency aspect is represented by tokens, which usually have a cash value associated with them

Cryptocurrency Exchange: Used specifically to refer to currency exchanges like Poloniex, which allow the exchange of one cryptocurrency token for another. Many facilitate the exchange of cryptocurrencies for fiat currencies, with regulation playing an increasing role in their operation.

Dark Net: Websites beyond the control of standard internet service providers. There are several gateways and types of dark net. Tor is the most popular gateway and network of this kind, with examples like Zeronet providing an alternative means to resist DMCA takedowns by collaborative seeding of content. Advocates propose that the dark net is used by those seeking privacy, but criminal activity naturally benefits from this as well.

Dark Net Marketplace: Dark net markets are places on the so-called dark web, which facilitate the sale of illegal goods. Narcotics, firearms, and ransomware services are just a few examples. Many function similarly to markets on the surface web, such as Ebay, with individual retailers using a site to host their listed goods. Cyptocurrencies are the de facto tender accepted by such markets.

Initial Coin Offering: When putting a cryptocurrency on the market for the first time, an ICO, or initial coin offering, is launched. This is similar to an IPO in nature, though the volatility of cryptocurrency markets make it a highly unpredictable process.

Market Capitalisation: The sum of the number of all token's value for a given token, commodity or fiat currency.

Malware: Malicious software. Distributed for a variety of purposes, all of which are considered criminal.

Ransomware: Malware that aims to encrypt a victim's files. A ransom is demanded for the returnof these files, though their return is by no means guaranteed.

1 Introduction

Many types of malware, such as ransomware, focus on the extraction of cash value from their victims. The inherent traceability of fiat currencies, and the highly centralised nature of the banking system make demanding money in USD or Euros difficult. Charge backs, payment blocks and other tools exist to allow victims to fight back, requiring more sophistication and patience on the part of an attacker to ensure that they receive the payment. Most importantly, cash transfers, unless rigorously laundered are highly traceable, putting the perpetrators of cybercrime at risk of exposure and arrest [1].

Bitcoin provides a digital, decentralised and relatively anonymous alternative. This cryptocurrency was unveiled in 2009, with an initial market price of $0.008 and swiftly rising to $0.08 in 5 days. It's growth over the next few years would see it reach parity, then exceed, the USD in value. Today it trades at over $3100 per coin [2]. However, it is not merely cash value that attracts the attention of malware operators. Bitcoin, operating on top of blockchain technology, is a deregulated exchange medium. The blockchain does not exist in one central location but is instead a consensus of participating nodes, which forms a ledger of all transactions that have taken place. Individuals use public keys to identify their wallets, instead of personal details. Until one wishes to convert Bitcoin to fiat currencies, one may keep personal details separated from Bitcoin transactions.

In 2013, CryptoLocker made, probably for the first time, use of the Bitcoin digital currency platform to collect ransom money. The advantages of using cryptocurrency were made apparent in the aftermath, with a final sum of $3,000,000 [2] being credited to the operators (contrary to initial figures of $27 million). Though the ransomware itself was thwarted in early June 2014, the use of digital currency as a means of collecting ransoms on a large scale had been proven effective.

Since then, malware and digital currency have developed rapidly. Altcoins, or alternative coins, have sprung up in the digital currency market place. Initially copy cats of Bitcoin, with some serving as smaller stores of value, altcoins have quickly diversified to provide services of their own. A common approach is to use a given altcoin as fuel for a related service, for example, Siacoin is used as a medium of exchange for its distributed file storage contract system [4]. Bitcoin now trades at over $3100 per coin [2], but volatility is still a defining characteristic of most cryptocurrencies. One can argue that the value of cryptocurrency is secondary to its other attributes that lend themselves to nefarious activity: one can simply ask for more coins if the dollar value is too low, but it isn't possible to change the fundamental transaction model, blockchain or privacy features of the selected currency.

The anonymity of Bitcoin has been called into question repeatedly [5,6]. Currencies focusing on privacy and anonymity have arisen as a result. Zcash, Dash, and Monero have entered a marketplace that has an increasing demand for currencies resistant to observation. Usability is now a hot topic for many digital currency communities, who want to lower the barrier of entry for first time users. There have even been hypothetical discussions of smart contracts (an attribute of Ethereum and like-designed currencies) to automate ransom collection further, offering yet more benefits in scalability, speed and service for malware operators.

This report provides a contemporary and forwards-looking discussion of altcoins and their role in for-profit malware, with a focus on ransomware. Section 2 provides a breakdown of prominent altcoins, section 3 maps the attributes of these altcoins to malware usage (drawing on reports of attacks and academic literature), and discusses challenges to law enforcement (in terms of prevention of payment, outreach to victims, and detection/traceability of funds), section 4 concludes the report.

2 Altcoins

Altcoin is a somewhat contentious term in the cryptocurrency community, with some in the Ethereum and Monero communities arguing that it specifically refers to alternative coins built on the Bitcoin platform. For the sake of brevity, this report will use altcoin to refer to all post-Bitcoin cryptocurrencies, including those not based on the Bitcoin digital currency platform.

Altcoins have emerged for several reasons. Ethereum, with its distributed computing network providing a 'smart contract' service, has developed as a form of currency-fuelled service economy (with several of its own altcoin spin offs). Dash focuses on transaction speed (boasting near instant transactions) and privacy, remaining a store of value but with augmented capabilities.

It would be unwieldy to exhaustively list the motivations behind altcoin development (though most share a profit motive), just as it would be to list all altcoins that may have a potential use in for-profit malware. As a result, this section will focus on four of the leading altcoins that have a significant presence in malware-related literature and media. Each currency has its history, technical aspects, and services discussed briefly in the context of its use in malware. A more thorough exploration of for-profit malware and its relationship with specific altcoins will be provided in section 3.

A brief discussion of emerging currencies is provided to show the ongoing development of the cryptocurrency landscape. Exchange services, which are vital for conversion back to fiat, will also be discussed.

2.1 Monero (XMR)

Monero promotes itself as a secure, private and untraceable currency. Like many altcoins, it has a thriving Reddit community and social media presence, with a focus on espousing the benefits of privacy in civil society. It has also seen a high degree of media attention in the last year, due to its use as a medium for the exchange of criminal funds. Monero is a fork of the CryptoNote-based currency, Bytecoin.

The official Monero website correctly points out that many blockchain implementations offer security at the cost of anonymity, which is correct when discussing the observation of funds and transactions associated with a given address. The Bitcoin blockchain explorer allows one to explore the full history of any wallet if provided with the correct public key. Monero does not permit this, encrypting such information and making it privacy locked to the owner of the wallet.

It is claimed that it is 'extremely unlikely' that a transaction can be traced back to a specific user [7]. This is wise, as all decentralised digital currency platforms require peer consensus to resolve transactions. As a result, transaction metadata must be shared at some point, to obtain consensus. However, Monero is designed to ensure that this information, and the nodes performing consensus-operations on it, remains locked away from prying eyes.

Monero makes use of ring signatures to create ambiguity around which funds have been spent. Ring signatures allow a group of users, all holding their own private key, to endorse a given piece of information (digitally signing it). In an ideal ring signature system, it is not possible to determine which private keys have been used (all participating keys are equiprobable), only that a threshold value has been reached, indicated a consensus on the information present [8]. This allows Monero to maintain anonymity for the parties involved.

Keys are ephemeral, persisting for only one transaction at the receiver's end. This means that it is not possible to derive the address of the wallet that sent the transaction by compromising the recipient. Only recipients who are aware of the sender outside of the confines of the protocol itself have any knowledge of the specifics of a transaction beyond the amount received [9].

The final claim made by its creators is that all Monero remains fungible. This means that any given Monero coin is indistinguishable from the others, due to the service previously discussed. As a result, Monero that is blacklisted by exchanges or vendors is not locked out of the blockchain. In fact, the only way to keep Monero from being used is to sink it into burner wallets, which hold the coins and do not allow their use in further transactions. This means that event 'dirty' money is usable and extremely difficult to identify in the Monero digital currency platform.

These services are made possible by basing the currency on the CryptoNote protocol. Like Bitcoin, Monero uses a public ledger that is the product of distributed consensus on the transactions that have occurred using the target network. The difference lies in that CryptoNote does not allow transaction information to be followed through the blockchain. This protocol was not forked from the Bitcoin protocol, and as a result, it has many differing internal design choices.

Media attention around Monero has intensified from late 2016 through 2017. Alphabay, a notable DarkNet Market (DNM), adopted Monero at the end of august 2016. However, though the currency was allowed, individual sellers could choose whether they would accept the currency. The market cap of Monero did rise dramatically after the Alphabay announcement, from $25 million to $170, before dropping back to $110 million by the end of the year [10]. It is currently impossible to determine how much of this was driven by speculation, and how much was used in trade over this DNM. This information may become available in the future, as both Alphabay and Hansa were seized for some time prior to their shutdown in late July 2017.

Ransomware demanding payment in Monero has appeared recently, with Kirk being identified by Avast researcher Jakub Kroustek, in March 2017 [11]. Webroot's Tyler Moffit predicted in 2016 that Monero would either share or usurp the DarkNet Ransomware market soon [12], a prediction that we have yet to see come true, but which is being tested by individuals seeking lower costs and easier methods of laundering the proceeds of cybercrime.

Figure 1 demonstrates the effects of increased usage and media attention on Monero. With the late 2016 adoption of Monero by Alphabay, Monero spiked in both value and trade volume dramatically. Zion Market, Wall Street Market, Trade Route and Majestic Garden are other examples of DNMs which allow sellers to accept Monero. It is also possible to use xmr.to, a tool that allows you to make Monero payments to a Bitcoin address, effectively allowing trades for items demanding Bitcoin payment, to be fulfilled with Monero.

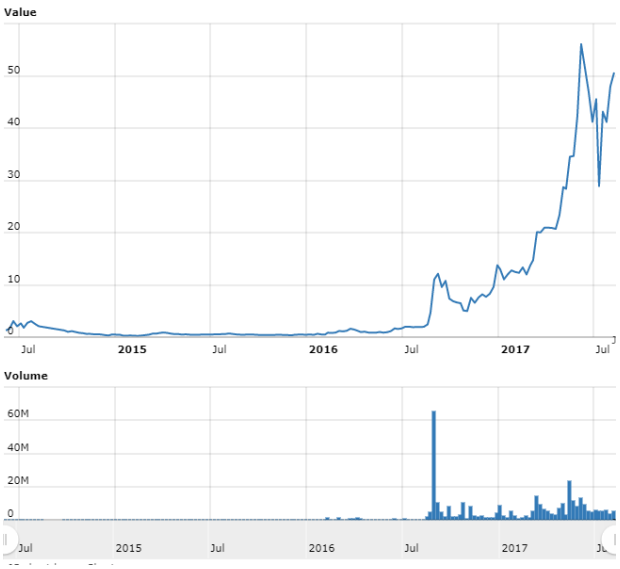

Figure 1 – World Coin Index Monero Price Chart (all time) [13]

2.2 Ethereum (ETH/ETC)

Ethereum itself is not a currency; it is a distributed network, described first in 2013 by Vitalik Buterin. Ether, the currency fuelling that network, is used to store value, which may be attached to so-called smart contracts [14]. These contracts are digital agreements, stored on the blockchain, which allow a variety of services to be exchanged for Ether. These services can include computational resources, storage, prediction markets and other digital services. There are already many cryptocurrencies based on the Ethereum paradigm, which provides specific services (Golem, Augur and Gnosis being prominent examples).

Ether is currently second only to Bitcoin in its value. Like Bitcoin, it uses a publicly accessible blockchain, which allows the values of wallets, transactions and contracts to be observed freely. Blocks of Ether can be created faster than those of Bitcoin, though in June 2017 there were significant congestion issues that led to scepticism regarding early claims that Ether would overtake Bitcoin in terms of network capacity and transaction speed [15]. The major point of differentiation lies in the smart contract system; applications can run on the Ethereum network, it is not just a store of value, like Bitcoin.

Ethereum has not been without controversy, with a hard fork in late 2016 that divided the community. The DAO hack resulted in 3.6 million Ether ($70 million at the time) being drained from the Ether balance associated with a specific smart contract. It is beyond the remit of this report to detail the specifics of this hack, but it was a pivotal moment in cryptocurrency self-regulation, as it was decided that to prevent the appropriated funds from being spent on the core chain, a hard-fork was required. This led to two divergent versions, Ethereum (ETH) and Ethereum Classic (ETC). Ethereum Classic still runs on the old chain, but Vitalik and many of the developers working alongside the Ethereum Foundation continue to work on the forked chain, referred to by many as Ethereum Core (or just Ethereum).

Ethereum has not escaped the attention of cybercriminals. CradleCore is an example of ransomware as a service, including the option to set up ransomware that allows payment in Monero and Ethereum [16]. The developers of CradleCore have not offered their software as a service, however. It appears that they intend to sell the software, so that others may operate the service. In April 2017, the source code was available for purchase at a price of 0.35 Bitcoin (starting bid). The fact that development kits like these are beginning to appear on DNM indicates that there is a demand for more diversity in the cryptocurrencies demanded by ransomware. This seems counter intuitive, as sticking with Bitcoin allows one to leverage the media attention and abundant available resources to help inexperienced users purchase Bitcoin for ransom. Adding more coins, many with their own wallets and technical requirements would appear to complicate matters (several articles made this observation about CradleCore and Kirk) and increase friction with the (unwilling) customer base.

The benefit, however, does not lie in the ability to ask for multiple currencies, but in what those currencies offer. Monero offers to increase anonymity and privacy, which is highly desirable when one's activities are considered illegal. Ether provides no such protection, but it does offer the smart contract system, which has its own appeal for ransomware and for-profit malware operators. Automated payment systems, secured using smart contracts, could increase the scale of ransomware attacks dramatically, as it would cut down on the need to manually handle the multiple wallets many ransomware operators tend to use. It could even associate a target with a unique identifier, thereby tying any transaction details to that instance of ransom, freeing operators to work at a higher level and oversee 'problem' cases, such as individuals finding it hard to pay the ransom due to technical inexperience. Though currently hypothetical, Mcafee and Avast have both expressed concerns that this could represent an avenue of ransomware development that should not be overlooked [17].

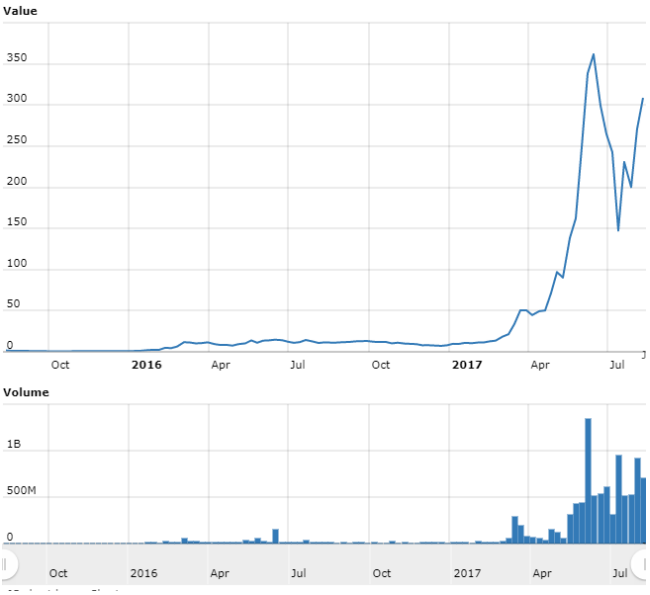

Figure 2 – World Coin Index Ethereum (ETH) Price Chart (all time) [13]

Figure 2 shows that Ethereum experienced a later spike than Monero, likely due to a lack of popular media attention. However, it has increased in value dramatically, to become the second most valuable cryptocurrency in the current market. As its many projects mature, and business-like Microsoft and the Ethereum Enterprise Alliance begin to push the technology further into the public domain, it is likely that this will only increase in value and intensity.

2.3 ZCash (ZEC)

Introduced in October 2016, ZCash claims to be the first open, permission less cryptocurrency that can fully protect the privacy of transactions using zero-knowledge cryptography. Like Monero, it provides additional privacy and anonymity services. In this way, the blockchain is protected against observation, all transactions are logged and verified by the consensus, but this consensus is achieved in a manner that allows both the recipient and sender to remain anonymous. The details of the transaction are also protected, remaining private [18]. Zcash supports both private and transparent addresses, allowing individuals to make public transactions on the blockchain.

ZCash has emerged from the development of ZeroCoin, as a product of the ZeroCash protocol. Zcoin is another anonymity focused cryptocurrency, but unlike ZCash, it does not hide transaction amounts, leaving it vulnerable to timing attacks that may derive transaction metadata. The transaction speed of Zcoin is also significantly lower, as it doesn't benefit from the far more efficient zK-SNARK implementation used by ZCash. As the ZeroCoin project officially endorses ZCash, our discussion will focus on the more favoured, higher value coin, ZCash.

Though Monero and Zcash both offer additional anonymity to users, they achieve this very differently. Zcash makes use of zK-SNARKs, which rely on zero-knowledge cryptography to function. ZK-SNARK stands for "Zero-Knowledge Succinct Non-Interactive Argument of Knowledge". This construct allows one to prove that one has knowledge of secret information without having to disclose said information. These zero-knowledge proofs can be verified in milliseconds, with only a single message required from the sender to the verifier [19, 20]. This is a marked improvement over previous interactive models, which required several rounds between the sender and verifier.

ZK-SNARKs are the foundation for protected transactions using Zcash. Bitcoin tracks unspent transaction outputs to determine if a transaction is spendable. Zcash calls these commitments, and requires that a nullifier is revealed to spent a given commitment. Both commitments and nullifiers are stored as hashes, to avoid disclosing any information related to these variables, or their relationships. Zcash nodes keep a list of all such variables that have been created or revealed. Most of the computation is offloaded to the creator of a transaction, taking 40 seconds to create a transaction but only milliseconds to verify it. The developers claim that it is theoretically possible to use zK-SNARKs to verify any relation without disclosing inputs or leaking information, though this is still too computationally intensive for many applications right now.

There are no current reported uses of Zcash in ransomware or ransomware-as-a-service (RaaS). Like Litecoin, it appears that currencies offering similar features have stolen the limelight, with Monero taking the lion's share of attention when considering for-profit malware. It is not, however, without its own cybercriminal ties.

Mining trojans, botminers and other malware has been reported as early as 2016, the aim being to procure sums of Zcash by seizing control of hardware that can be used to mine the currency. Zcash can be both GPU and CPU mined, making gaming, office and household PC's viable targets. As the attackers do not have to pay the energy cost of operating the mining software on infected devices, this is potentially lucrative, especially with growing, popular currencies that have not yet experienced a 'difficulty bomb' (rapid increase in difficulty of mining due to a high hash rate being directed towards it) [21].

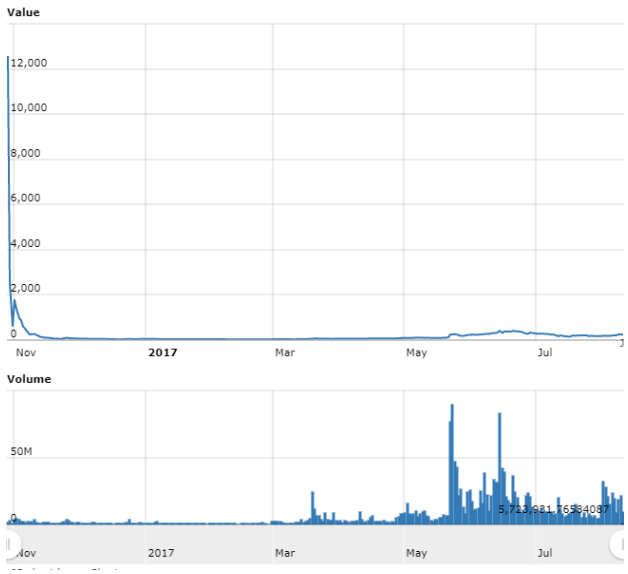

Figure 3 – World Coin Index ZCash Price Chart (all time)

Figure 4 – World Coin Index Zcash Price Chart (Feb-August 2017)

Figures 3 shows a marked difference when compared to the more typical currency growth patterns shown thus far. Zcash was in high demand on launch, and with only a few dozen coins in circulation, demanded a high price for those initial coins.

Figure 4 provides a somewhat less tumultuous (and recent) history. After an initial spike and drop, the currency began to grow from its $20-30 January 2017 price, with a spike in growth in May-June. The drop off in Zcash value in mid-June coincides with the rise of Monero value, possibly indicating a transfer of usage from one to the other. The dip in July is common to most cryptocurrencies, following the rapid drop, then recovery, of Bitcoin.

ZCash may not currently be as popular with the DNM and malware operators as Monero (due to a raft of trust issues, not least of which is their registration as a United States company), but it does offer a different

technological foundation. Should vulnerabilities be found in Monero, Zcash may fill the gap that will open in the privacy-seeking cryptocurrency market as a result.

2.4 Dash (DASH)

Dash has been previously known as DarkCoin and XCoin. Initially launched January 18, 2014 (as XCoin), its name was changed to DarkCoin in February 28 of the same year. The coin was finally renamed to Dash (Digital Cash) in March 25, 2015. The currency offers the same basic functionality as Bitcoin, alongside instant transactions, private transactions and decentralised governance.

The biggest structural difference between Dash and Bitcoin, is the two-tiered architecture it employs to enable 'Master Nodes' [22]. Miners, forming the baseline tier of a node, are tasked with creating new blocks. Master Nodes perform special functions, including PrivateSend (private transactions), InstantSend and governance functions. To mitigate Sybil attacks, a 1,000 Dash collateral payment must be made to take the role of a Mater Node. Both types of node split the block reward.

PrivateSend is a currency mixing technique, used to add additional privacy to transactions. Identical inputs from multiple users are added to a single transaction, with several outputs. Due to the identical transactions in the inputs, the outcome is obfuscated, making it difficult to trace the flow of funds (direct methods will not yield a solution). This is based on the CoinJoin method but is heavily modified. The maximum transaction size is 1000 Dash, and mixing is restricted the certain denominations (usually multiples or divisors of 10). A more advanced version, CoinShuffle, has been published by the University of Saarland, which does not require third-party governance, but this is currently not in use in the Dash protocol [23].

It is important to differentiate Dash from Dashcoin, a similarly named, but different protocol. Dash is based on the X11 hashing algorithm, while Dashcoin is a CryptoNight derivative (the same protocol from which Monero is derived) [24]. Both have privacy and anonymity features, though Dashcoin is more geared toward privacy from the outset. Dash, however, is by far the more capitalised currency, with greater trading volume and value at present.

Several DNMs accepted Dash until closure, including Nucleus. Community discussion regarding Dash usage in DNMs centres around a perceived preference for centralised and trusted mixing services using Bitcoin. A lack of promotion, and conscious effort on the part of the developers to disassociate themselves from the previous "dark" branding is also cited as reason for lack of adoption. Several cryptocurrency blogs, including Bitcoin Magazine, make another argument: the DNM community demands Monero over ZCash and Dash because they do not trust either of these alternative protocols [25]. Dash requires that users trust the Master Node network to not collude with authorities to trace transactions. ZCash is registered in the United States, combining concerns around that with the fact that mixing is done on an opt-in basis.

Despite this, Dash remains a valid alternative, decentralised means of laundering money associated with cybercriminals. Built in mixing and a decentralised approach means that trust needn't be placed in proven (and likely more expensive) mixing services, so long as one trusts the Dash network.

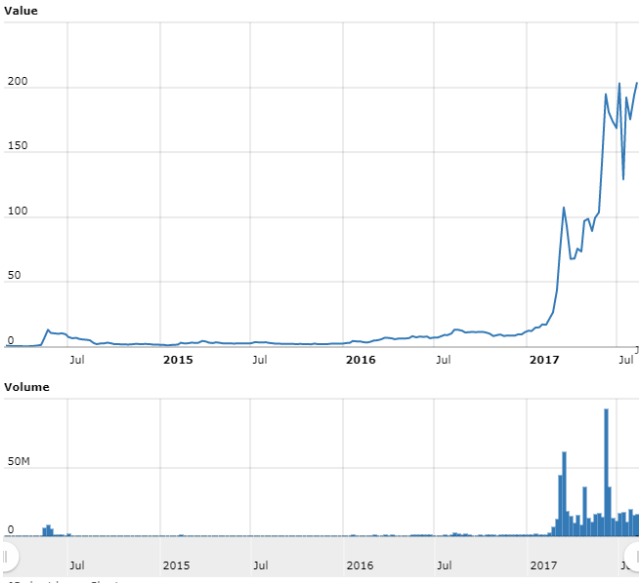

Figure 5 – World Coin Index Dash Price Chart (all time)

Figure 5 shows that like the other currencies reported on in this document, Dash experienced a significant period of growth this year. It is reported that at present less than 1% of users are operating Dash in PrivateSend mode, so it is likely that the instant transaction services it offers are a driving force in its uptake. 2017 is strongly suggested to be the second major cryptocurrency wave, in which altcoins start to pick up significant value and compete, if not with Bitcoin, then with each other to have a significant stake in their respective markets. Dash appears to be following that trend for now, and it is yet to be seen whether its role in malware monetisation will increase.

2.5 Other Relevant Currencies

There are several currencies that offer advantages in transaction speed, anonymity, and/or privacy that have either very small capitalisation or little coverage with regards to DNM and malware. Anoncoin and Litecoin are examples of such currencies. Zcoin is another, but as the ZeroCoin project now officially endorses ZCash, this has been briefly discussed as a part of that sub-section.

2.5.1 Anoncoin

Anoncoin has an exceedingly low market capitalisation of $225,568 as of august 10, 2017. It is only reported as trading via the Exchange.i2p exchange, with a volume of $1 [2]. To all intents and purposes, it is a defunct coin at present, with several grassroots efforts to revive it or appropriate the mature blockchain implementation.

The Anoncoin wiki states that Anoncoin was created out of a desire for a truly anonymous cryptocurrency [26]. It launched June 6, 2013, and has reached a current coin supply of 1,934,794 out of a possible 3,103,954. It represents one of the first attempts to implement an anonymous cryptocurrency.

A major criticism of the currency is its use of the dark net exchange Exchange.i2p. This exchange has exceptionally low trade volume and creates an environment in which this currency in not conducive to laundering. This prevents it from accruing sufficient community goodwill to be popular as a medium of legitimate or criminal exchange, at present. However, the currency has 1.9 million coins in circulation, and there is the outside possibility of one of the grassroots teams, or original developers, pushing a new direction for this coin.

With regards to contemporary DNM and for-profit malware, this coin is useful largely as a historical point, between the rise of Bitcoin and the emergence of the first true altcoin markets in 2015-2017. At present, it is a

concept that has survived its first implementation: Monero, ZCash and Dash all take lessons from the manifesto of the Anoncoin developers, but the coin itself is unlikely to play a much further role in the progression of the anonymous, private blockchain ideology.

2.5.2 Litecoin (LTC)

Litecoin has been referred to as the 'silver to Bitcoin's gold'. It is a smaller denomination currency, initially launched in 2011. It possesses a higher coin limit (84 million instead of Bitcoin's 21 million), uses the Scrypt algorithm, has a 2.5 minute (instead of 10) mean block time, and only halves emission rewards every 840,000 blocks [27]. This makes it easier to mine than Bitcoin, making for a currency with a larger number of coins and faster transaction processing rate (thanks to the faster block time).

Litecoin was developed by Charlie Lee, a former Google employee. As a fork of the Bitcoin Core client, it is heavily modified but retains the core functionality and feature of Bitcoin. As a result, it is primarily intended as a store of value. It does not currently boast any smart contract or service provision capabilities.

A variety of malware has targeted Litecoin throughout its years of existence. In 2013, malware was distributed through Litecoin community sites to take control of wallets and steal funds [28]. Another wave of attacks was reported in 2014 and 2015; this time used to mine Litecoin (and Dogecoin) instead of stealing it directly. This has been reported for other currencies (including Ethereum), but Litecoin has been a favourite for this form of malware, likely due to the low computational requirements required to contribute hash rate to the network (which is required to mine, or earn, coins) [29].

Litecoin is not well suited to traditional DNM activity. It is difficult to mix or 'tumble'. In a tumbler, Bitcoin is exchanged in decreasing amounts, splitting the value across multiple wallets and creating a complex chain of transactions that make mapping the flow of value from entry to exit point exceptionally difficult. This is not immune to sufficiently driven and sophisticated tracking, but it does increase the technical costs and time requirements of individuals trying to follow a Bitcoin transaction. Some services suggest that they are capable of mixing Litecoin, but it is not clear if these are legitimate, and many have shut-down after only a brief period of activity. As Litecoin doesn't provide privacy by design, the difficulties inherent in providing this service make it ill-suited to use in many DNM scenarios.

As previously mentioned, value storage isn't the only force informing the selection of cryptocurrencies for trading or ransom. One can always ask for a USD equivalent fraction of a given cryptocurrency, to achieve the same result. Bitcoin transactions may be slow, but in the case of ransomware, this is not a crippling issue, as the breadth of an attack is more important than the processing speed of any one transaction. Furthermore, in a DNM scenario, longer transaction times only mean longer waiting times for confirmation of an order: Bitcoin may be slower, but it is more widely accepted and doesn't require merchants to switch to a currency that only offers faster transaction times. As a result, Litecoin is an example of how extensions of the Bitcoin paradigm may not be successful in malware and DNM scenarios.

3 Altcoins and Cybercrime

Bitcoin is by far the dominant cryptocurrency, both in terms of market performance and in utilisation in cybercrime. Since CryptoLocker (2013), most ransomware families have made use of Bitcoin to receive ransom. The decentralised and deregulated nature of the blockchain makes it ideal for such nefarious activity, though it is not resilient against analytical tracking techniques.

As the Bitcoin blockchain is public in all respects, it is possible to trace transactions, even those that have been performed using mixing services. This has led to an interest in altcoins that boast improved anonymity and privacy features, although it is only recently that ransomware demanding such currency has come to light. To understand the motivations behind altcoin selection in for-profit ransomware, one must first explore the attributes of a currency that appeal to the target application.

3.1 Desirable Attributes of Altcoins

The desirability of a given currency is highly application-specific, especially with the current wave of app-focused altcoins. Malware and DNMs, however, do share several key interests: procurement, user experience, liquidity, exchangeability, and operational security.

3.1.1 Acquisition

The acquisition of Bitcoin, though arguably an element of the user experience, is a critical consideration for ransomware operators. Many ransomware operators have implemented a form of customer service, to assist individuals in the acquisition of Bitcoin, as it has been found that a lack of familiarity with the currency can prevent otherwise willing ransom payments [30, 31]. Adding additional currencies to the payment options, even if their acquisition is like that of Bitcoin, would complicate this already troublesome aspect of ransom payment.

There are two main hurdles a willing payer must overcome, assuming zero initial knowledge in cryptocurrencies. First, they must register with an exchange service (or find an unregistered venue from which to purchase coins). This can be a laborious process, requiring three forms of photo identification in the case of Poloniex [32] and Coinbase [33]. Alternatives, such as Bitcoin ATM, prepaid cards and arranging to meet someone to buy currency with cash exist, but bear their own complications and dangers [34]. Specific issues aside, they all share the common issue of being region-locked, Bitcoin ATMs just don't exist in many locations, nor do individuals willing to perform anonymous cash trades for Bitcoin. Exchanges are by far the most common method of acquisition, and these take time to get set up.

Time is not on the side of the ransomware operator or victim: the operator wants to accrue currency as quickly as possible to minimise risk of detection and arrest. The victim wants to pay to avoid any time-based penalties that many ransomware strains incorporate. Therefore, acquisition, or at least incentive to hold a balance of a given currency, is a consideration when selecting an appropriate currency for ransom. Many companies are now holding Bitcoin as a part of their security strategies, in the case of ransomware attacks that bypass their other security measures [35]. The fact that Bitcoin increases in value over time, as a general trend, makes this a more palatable strategy, than demanding a currency with a less favourable market performance (as the number of coins budgeted for will likely remain relevant to the typical ransom demand for longer).

Altcoins such as Ethereum are about as easy to acquire as Bitcoin. Poloniex, Coinbase and other major exchanges provide options to purchase Ethereum and Bitcoin with fiat currencies, usually Euros, US Dollars or Pound Sterling. Monero, however, suggests that the easiest way to acquire the currency is to purchase it with Bitcoin [36]. Using a service known as ShapeShift [37], one may exchange one currency for another simply, without registration and without the use of a traditional exchange service. Exodus, a wallet application, even provides such functionality built in, for a limited selection of currencies [38].

This additional step requires minimal time, so individuals holding Ethereum or Bitcoin can easily exchange for a wide variety of altcoins. The issue remains the payer's willingness to fulfil the ransom [39, 40]. Sufficient confusion and anxiety about the steps that they must go through to purchase a currency that they may have never heard of can skew the risk-reward equation that informs their willingness to pay. It is therefore important for ransomware operators that they weight the ease of acquisition and understanding of a given currency with the other benefits it may provide.

The second hurdle that must be overcome is the selection of an appropriate wallet, and subsequent transaction. This is the core of the user experience.

3.1.2 User Experience

To acquire a sum of cryptocurrency, one must have an appropriate wallet to store it. Most ransomware strains offer detailed information on how to do this for Bitcoin [30], but as altcoins enter this field, the issue of wallet selection becomes non-trivial for first time users.

Ethereum is fairly straightforward to set up: there are a variety of wallet applications that provide multi-currency support, all of which include Ethereum. Mobile applications are particularly common to this, though most exchanges also provide a basic form of wallet (which is likely to be the wallet used by less experienced individuals). Currencies that cannot be directly acquired through exchanges can be very confusing, however.

Monero, for example, strongly encourages users to run a full-node on the machine hosting their wallet. There are many configuration options which will be completely alien to someone who only wishes to pay a ransom and does not want to put time into exploring how to acquire, then pay, the ransom. Figure 6 shows an example of the Monero GUI wallet. The bottom left icon shows that the wallet is synchronised to the blockchain: achieving this state can be a lengthy process, requiring the download of the current blockchain. Services allowing one to connect to an existing full-node exist, but are unreliable and not new-user friendly.

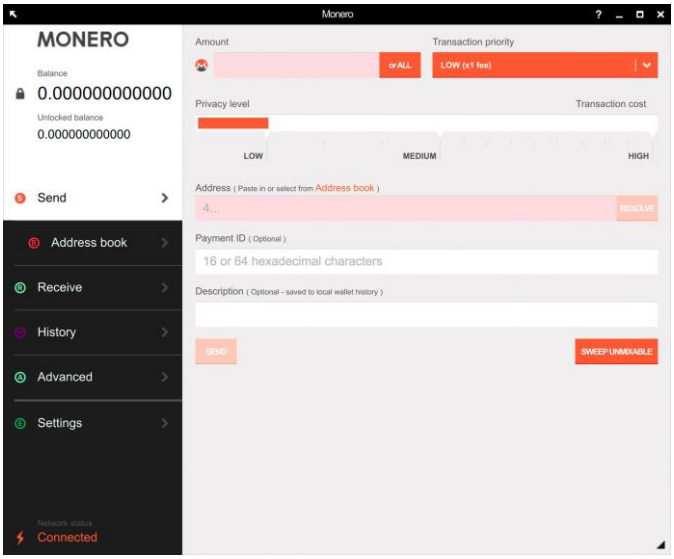

Figure 6 – Monero GUI Wallet

ZCash and Dash both offer currency specific wallets, though Dash is also supported by Exodus, which is exceptionally user-friendly. All the currencies discussed here are accessible through mobile applications like Coinomi [41]. The main consideration, on the part of ransomware operators, will be providing the support required to guide users to appropriate wallets in a timely manner, should they wish to mitigate the additional steps involved in using currencies other than Bitcoin and Ethereum.

3.1.3 Liquidity

This is not a major consideration for most cryptocurrencies, all of those listed in section 2 under their own sub-sections have more than sufficient capitalisation and trade volume to meet the demands of contemporary ransomware and DNM needs. However, it is important to distinguish projects that have since fallen out of favour.

Anoncoin [26] is widely discussed in pre-2015 literature, as a project that sought to provide a truly anonymous Bitcoin equivalent. Initially priced highly, it was plagued by low trade volume, a rapid decline in price and a catastrophic pump in mid-2017, leading to a spike in trade followed by the complete collapse of its value. With a market capitalisation of less than $210k, this coin is not suitable for any large-scale laundering or transactions. It is also only traded on a single exchange, making it exceptionally hard to acquire for first-time users.

For malware operators, and DNM merchants, it is important that a currency has sufficient capitalisation to facilitate its use. It is also beneficial for a currency to offer a high transaction rate, with low fees, to mitigate the effects of Bitcoin friction. When a currency is used as much as Bitcoin, the speed of transactions can slow down, as more highly valued (higher fee) transactions are favoured. This can be an issue for individuals wishing to make payments, as it will either take a long time (tens of minutes, possibly hours) to process transactions paying average fees, or cost significantly more to be facilitated in a reasonably time-frame.

Ethereum had similar issues aggravated by token-offerings in June: gas (transaction) fees went up dramatically, with some exchanges passing scaling fees onto users unexpectedly [42]. Some wallets became disabled during this time, to prevent overload of exchanges and mitigate the runaway transaction backlog on the chain. This is undesirable to malware operators, especially when considering a coin mixing service (which need to make many transactions). However, it is not a critical issue, providing that the currency is, on average, able to facilitate transactions in a timely manner.

3.1.4 Operational security

A long-desired feature, only recently incorporated into cryptocurrency alongside success in the marketplace, operational security is sought after by individuals of benign and nefarious intent alike. For malware operators and DNM merchants, currencies offering increased operational security capabilities are attractive, especially if they offer such services without the need to use third-party services like coin mixers.

Monero is the current darling of this attribute, providing anonymization and privacy services. It has already been incorporated into instances of ransomware uncovered by security professionals, though it has not yet been found in actual attacks. Monero has also proven attractive to DNM, with Alphabay officially listing it as an accepted currency until its closure in July 2017. Benign users of the currency have pointed out that a benefit, from their perspective, is that coins cannot be marked as ‘dirty’, a severe problem for law enforcement agencies wishing to seek or lock funds associated with cybercrime, but a driver for criminal and legitimate use to co-exist in the Monero market.

ZCash offers an alternative means of attaining similar operational security, and should vulnerabilities be found in Monero, then ZCash may not be compromised due to its very different zK-SNARK technology. However, its registration in the United States has led some communities to question its ability to honour claims of non-disclosure and a truly private blockchain. JP Morgan have announced that they wish to integrate ZCash technology into their Quorum enterprise. This demonstrates an interest in so-called privacy-coins, but official statistics suggest that only 18% of users are making use of private transactions: the majority are using transparent addresses [43].

Dash has received similar criticism, instead levelled against its use of master nodes. Requiring collateral to become a master node may put off casual attackers, but dissenting voices argue that state level actors can afford to fund either the collateral or the means to bypass it to perform a Sybil attack on the master node system.

There is no evidence for this claim, but it has been sufficient to cast doubt on whether the master node system is trustworthy.

Ethereum offers no advantages in terms of operational security, offering a full-disclosure blockchain explorer, much like Bitcoin. Mixing services, such as EtherMixer exist, but have the same issues with fees and transaction costs as Bitcoin mixers. A Zcoin tumbling service for Ethereum has been a topic of community discussion in May 2017, but currently there is no official disclosure of such a project reaching completion. Monero has been suggested as a means of performing mixing with a minimum of transaction fees (via ShapeShift). This will be discussed in more detail in sub-section 3.4.

3.2 Mining Malware

Botnets, associated with some strains of ransomware due to their use in malvertising and other saturation campaigns, have been used to mine illicitly using infected hardware. Bitcoin is exceptionally difficult to mine, and so this type of malware has focused on high-performing altcoins, notably Ethereum, ZCash, Monero and Dash. There have been some suggestions that these botnets are used for monetization during 'down time' (when the botnet isn't being used for other purposes). However, Kaspersky, Avast and McAfee [44] have all reported on malware that appears to be specifically set up for mining and little else, lacking the more sophisticated command and control elements seen in more direct strains.

Mining malware takes advantage of the usual points of ingress into computer systems: malvertising, exploits and poor security practices. Once installed on the target machine, it will direct computational resources to mine cryptocurrencies. The use of resources in this manner is rewarded whenever a block is found; such malware usually contributes its hash power (a measure of resources applied to the cryptographic puzzle that must be solved to find a block) to mining pools to guarantee some form of pay out. If they mined 'solo', the reward would only be paid if they were the first to find the block: which is unlikely unless one has a significant portion of the hashing power being directed to a given currency. McAfee went so far as to say that Bitcoin mining malware was 'a fool's errand' in 2014. In this, they remain correct, but ASIC resistant cryptocurrencies, and heightened awareness of new, low difficulty currencies as they emerge, has galvanised a new wave of mining malware.

Interestingly, many mining pools that have discovered evidence of mining botnets participating in their efforts have noted that many such botnets are 'good actors' from the perspective of the pool. Alpereum (a Swiss mining pool) received a portion of botnet hashing power in April of 2017, largely from devices that had individual contributions of less than 5MH/s [45]. Mobile phones, home PC's and other hardware were all directed to mine Ethereum in this manner, as the electricity costs of doing so are not of importance to the botnet operator. The botnet does not seek to overload the target network, though this example caused issues by registering many individual addresses to the pool, causing database load problems. These problems led to the discovery of the substantial number of low-rate miners, and the subsequent purge of those miners from the pool. Technical staff commented that the botnet appeared, in all other respects, to act like any other miner and accrue funds, without inconveniencing the pool.

Bondnet is an example of a diversified mining malware: it mines multiple coins but appears to favour Monero. In May 2017, it was reported as mining $1,000 a day in cryptocurrencies, the majority of which was derived from Monero proceeds [46]. Infecting over 15,000 windows servers, this malware has been active since December 2016. The primary impact on the victims is increased power costs, with quotes of $1,000-2,000 in additional electricity costs. It is strongly suggested that as well as frequent patching, companies monitor their energy and resource usage to spot any anomalous behaviour, such as intensive out-of-hours processing.

Mirai has been reported as mining Bitcoin in early 2017, but only for a few days. IBM X-Force reported that an unknown group (or individual) was experimenting with the computational power represented by the many IoT devices under the control of the botnet [47]. However, the mining difficulty of Bitcoin, long dominated by ASIC hardware optimised for low power and high return on investment, is so high that the return provided by

such a Botnet is exceptionally low. This does have implications for less hard currencies, however, and those that favour CPU mining over ASIC mining.

This is especially true of ASIC-resistant currencies, such as ZCash. The creators of ZCash have stated their conscious decision to veer away from a design that can be made more efficient on ASIC device, and instead, favour mining using CPU and GPUs that are commercially available and in high supply. This has drawn the attention of botnets seeking to enter a market in which they don't have to compete with highly specialised, efficient miners, and where even infected mobile phones can provide some return.

Not technically a botnet, the ZCash mining issues of December 2016 were caused by unscrupulous individuals installing ZCash mining software on devices without the consent of their owners, allowing them to indirectly benefit from the unused computational resources of the infected device until the owner noticed the software. Kaspersky labs are credited with the finding and the subsequent publication of figures suggesting that up to $6,200 a month may have been mined at the peak of this phenomenon [48]. As the software is installed under the guise of legitimate applications, their advice is only to install authentic, signed applications, and to check periodically for any odd drops in performance on your devices.

There are no evidence-backed reports of Dash mining botnets currently, though it is possible that they exist on a small scale. The ASIC resistance of Scrypt would place it in the category of crypto currencies that a botnet of commercial and standard computer hardware could compete in.

A crucial point to consider, when thinking of methods by which one may attempt to prosecute the operators of malware like this, is that there is no point of 'ingress' into the market. A ransomware transaction requires that a real identity is used to purchase some crypto currency (unless they find unique means of avoiding this requirement, like a face-to-face transaction). Mining malware mines directly to a wallet, which, if it is a Monero, ZCash (non-transparent) or private Dash wallet, will provide anonymity features as of the first transaction. Transaction graph techniques may work to follow Ethereum back to an identity once the operator attempts to convert their earning back to fiat, but more operationally secure currencies present a serious obstacle to traditional blockchain forensics.

3.3 Ransomware

Ransomware strains demanding payment in currencies other than Bitcoin are relatively new but are expected to rise in number sharply in the next few years. Monero has been an especially popular coin with many cyber criminals, though it has only appeared in a few ransomware strains to date. Ethereum has also caught the attention of some malware operators, despite its public blockchain. This sub-section will explore some examples of ransomware, which either demand ransom in altcoins or have a noted history of incorporating altcoins into its exit strategy.

There are few examples of ransomware using altcoins at present, but it is important to consider the potential that they offer to this form of malware. Wannacry and Kirk represent two implementations of altcoin use in ransomware, but are by no means exhaustive examples. They are merely the first reported to be using altcoins. Ethereum, Monero, Dash and ZCash all have their attractive qualities, but currently, it is Monero that has emerged as the first Altcoin to gain significant attention in the ransomware domain.

3.3.1 Wannacry

This ransomware hit the headlines in the first half of May 2017, by affecting the NHS, Telefonica and numerous other high profile European institutions [49]. It was extremely disruptive and garnered a significant portion of media attention for the scale and intensity of the campaign. However, its main aim was not lucrative, gaining little more than $140,000 worth of ransoms over its lifetime. Compared to the figures of CryptoLocker, this was far from a financial success (if that was the intent).

The attack struck more than 230,000 machines on its first day, in over 150 countries. Marcus Hutchins discovered that registering a domain name found in the code activated a kill switch, preventing the code from performing as intended [50]. The ransomware propagated via the EternalBlue exploit of the Windows Server Message Block (SMB) protocol. Emergency updates provided by Microsoft days after the initial attack brought the campaign to a close four days later.

Wannacry functions in much the same way as most ransomware. Once it has infected a machine, it will begin to encrypt files using public-key cryptography, before encrypting the key itself and storing it offsite (from the victim's perspective). To decrypt the files, the affected party had to pay $300 of Bitcoin within three days, or $600 within seven days [51]. Failure to pay in this time frame would result in the deletion of the decryption key. Three addresses were used, with payment being requested into one of the three addresses. A twitter bot, @actual_ransom, followed these wallets, providing real time updates [52]. This showcased the ability for sufficiently motivated individuals to follow Bitcoin blockchain activity.

The attack was deemed by Europol to be the largest scale attack thus far, but also noted that its impact was relatively small. Figure 7 shows the more-than 200,000 infected hosts, in over 150 countries. The scale of the attack was augmented by its potentially unexpected success in hitting major infrastructure, such as data centres, which went on to further propagate the malware.

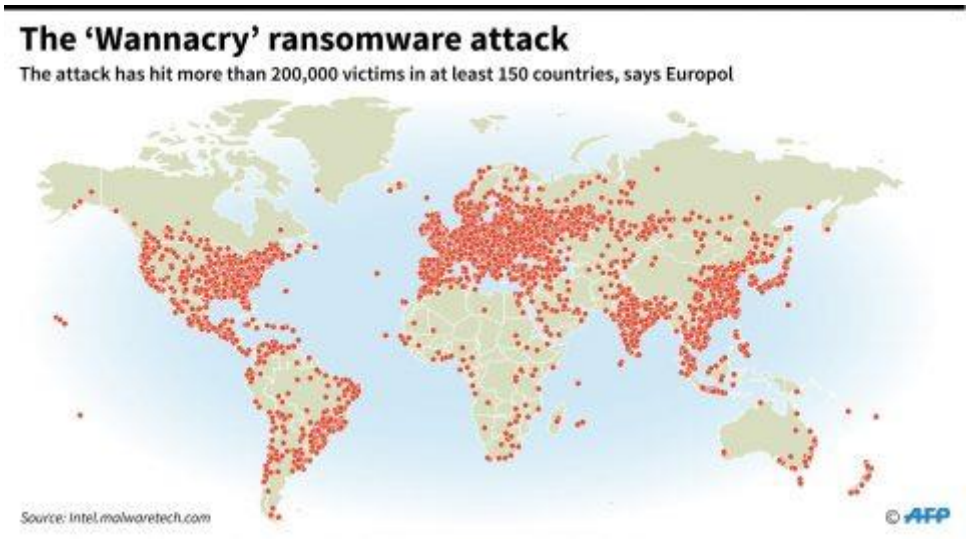

Figure 7 – Wannacry Ransomware Map [53]

The wallets associated with the ransomware went unattended until August 3 of 2017, at which time Bitcoin was withdrawn from the wallets in increments between 7 and 10 Bitcoin in size. Over nine transactions, the 55.2 Bitcoins in the wallet were moved to other Bitcoin addresses, before being moved into Monero [54]. The operators may have also benefitted from the Bitcoin fork, in which holders of Bitcoin received an equal amount of BitcoinCash. It is not clear, at this point, whether they have taken advantage of this, or whether it would be possible to trace the proceeds of the hard-fork.

The Wannacry operators have made use of a Swiss company called Shapeshift, to turn their Bitcoin into Monero. Shapeshift have made an official statement declaring these acts to be a breach of their terms of service, and pledging to cooperate with law enforcement in any manner possible. However, they can only blacklist wallets associated with Wannacry if they know about them, and the operators are free to conduct transactions on the Bitcoin blockchain until they manage to process a transaction for Monero through Shapeshift without them having yet identified that wallet [54]. Shapeshift is an easy-to-use service, requiring no sign-up. It allows the exchange of many types of cryptocurrency, with an intuitive interface. It's potential, and reported use in laundering will be discussed in sub-section 3.6.

The use of Monero as a means of laundering is an intuitive one. Instead of having to perform many transactions to launder Bitcoin through mixers, one may instead complete a transaction into Monero, perform one or more Monero transactions between several wallets, then exit back to Bitcoin to cash out to fiat. In this way, the complexity and cost of laundering are reduced, if one has sufficient knowledge of the current market environment (and doesn't trade into a falling currency). This is a strategy that may become increasingly common.

3.3.2 Kirk

Most ransomware families still demand payment in Bitcoin, but there have been recent developments including ransomware that gives the victim a choice of currencies that they may pay with. One example, is the Star Trek themed ransomware, Kirk, which explicitly demands Monero as payment [11]. This ransomware was discovered by Avast researcher Jakub Kroustek before it had the opportunity to propagate itself significantly. If allowed to propagate, it would have disguised itself as the Low Orbit Ion Cannon (LOIC) network stress testing program. Following infection, Kirk generates an AES password, which is encrypted with RSA-4096 public key encryption. It then uses this key to encrypt files on the host computer [55].

A time-based series of penalties are applied to anyone who does not pay within two days, raising the initial ransom of 50 ($1,100 as of 17 March 2017) Monero to 100, doubling again on the 8th day, then again on the 15th day. If after 31 days no ransom is received, the decryption key is permanently deleted. Payment allegedly results in a decryption program, Spock, being provided to release the files.

Figure 8 – Kirk Ransomware Splash Screen

The Spock program decrypts a file that is present on the infected machine. The file contains the encrypted password required to release the locked files: use of another password will corrupt files (as pointed out by the ransomware). Anyone wanting to pay the ransom will have to send this file, alongside their payment, to receive the appropriate Spock program for their unique infection. This is potentially the first ransomware to demand Monero, with any potential predecessors currently undetected by security professionals.

3.3.3 Ransomware as a Service (RaaS) and Associated Developments

Wannacry and Kirk are examples of how altcoins are being utilised in identified ransomware strains, but Ransomware-as-a-Service has its own criminal contributions to make. The advantages of conducting business

in Monero, ZCash or Dash are distinct, as they preserve the anonymity of both parties, allowing the sale of illegal software to benefit from an added layer of protection.

With the recent takedown of Alphabay and Hansa [56], cyber criminals have never been more aware of the open-book the Bitcoin blockchain provides to those that have the resources to look deep enough. One Bitcoin community commentator suggested that the blockchain was incorrectly assumed to be anonymous by many, but instead provided law enforcement officers with a ledger of criminal transactions. If a criminal gets caught selling illegal goods on the street, they can be charged with that crime, but if their ledger of criminal transactions is open for all to see, they can be accused of much, much more. This is evident incentive to use privacy focused currencies.

The development of ransomware capable of demanding ransoms in other currencies is also of interest. This is an emergent market niche, and enterprising cyber criminals are seeking the exploit this emerging market, trading on fears associated with Bitcoin traceability. CradleCore is an example of a multi-currency ransomware package, with the source code up for sale to the highest bidder [16]. This is not a service, like Satan, but a one-time sale of source code for ransomware. Such sales can be conducted like any other DNM trade, using any currency that is found to be mutually agreeable to both parties. There's no reason such a trade could not be conducted in Bitcoin, Ethereum, Monero or ZCash, regardless of the currency collected by the resultant ransomware.

Satan makes its money by charging a 30% fee on all Bitcoin transactions [57]. Though there are currently no known examples of this being done with altcoins, there is little reason why it could not be a feature in future implementations of RaaS products.

The Shadow Broker's, though not involved in RaaS directly, have been providing a subscriber-only dump of NSA cyber-tools and information since early 2017. Wannacry was reported to have used leaked NSA information regarding the EternalBlue Microsoft SMP exploit, and so interest in high amongst those looking to add an edge to their malware tools. Notably, The Shadow Brokers are requesting payment in ZCash as their currency of choice for this information. The veracity of their claims is, however, yet to be proven.

3.4 DarkNet Markets

DNM are black markets, associated with narcotics, firearms, stolen goods and malware-related trade. They exist on decentralised networks that operate on top of the standard Internet [58]. Many of these markets make use of the Tor network, and all of them use Bitcoin [59].

Late 2016, some market places announced that they would be integrating Monero and Ethereum payments. Foremost among these were Alphabay and Hansa, which at the time were considered the largest and most lucrative of their kind. Despite offering more secure altcoins, Bitcoin remained the most used currency, and it is still widely supported in most DNM, regardless of community (largely altcoin and darknet-affiliated subreddits) dissent on the issue [60].

Several notable DNM have accepted currencies other than Bitcoin [58], to promote privacy in the interests of obfuscating illegal transactions. There is not yet widespread adoption of altcoins; most markets support one or more mixing services alongside Electrum Lightweight Bitcoin wallets. A common criticism, specifically of Monero, is that it does not yet support multi-signature wallets. These are used heavily for Bitcoin transactions and offer advantages regarding transaction processing (avoiding the need for a traditional escrow system in many cases).

3.4.1 Alphabay

Alphabay Market was a Tor-based DNM. It opened in December 2014, after two previous 'soft-launch' phases in September and November respectively. At its peak (July 2017), Alphabay boasted more than 400,000 users.

In 2015, it was recognised as the largest DNM. It is most notable for being the first major DNM to implement multi-currency trading [58].

Initially, Bitcoin was the currency of choice, and this remains the case for most existing DNM. However, in late 2016, the operators of Alphabay announced that they would be accepting Ethereum and Monero transactions. May 2017 saw Ethereum go live on this DNM, with Monero having done so the previous year, in August 2016 [61]. The effects on Monero were marked, with a rapid increase in value perceived almost immediately after the announcement. A rise from $10 to $20 was observed in the six months after adoption by Alphabay.

Ethereum initially appears to be an odd choice for a DNM, as it doesn't offer any significant privacy benefits over Bitcoin. It does offer the possibility of more secure contracts. The Ethereum network can facilitate the automation of contracts that execute upon payments associated with them. In this way, a sufficiently sophisticated ransomware strain could use the Ethereum blockchain as a form of escrow – holding the means to decrypt files held to ransom, and releasing those means once payment is fulfilled. In a sector that requires trust despite engendering little to none, this could be an important step for ransomware operators who wish to increase their perceived legitimacy. This could lead to a higher willingness to pay, should the practice become commonplace and contracts prove trustworthy.

Beyond ransomware, Bitcoin friction, and interest in potential zK-SNARK implementation in the Ether currency, have been sufficient to drive its implementation in a number of DNM. The impact of this on the price of Ether is unclear, as the forces that have acted on it recently are complex, driven by Bitcoin apprehension around the hard-fork to Bitcoin Cash, amongst others. However, the possibility of using Ethereum smart contracts to provide a contractual basis for trust, using the smart-contracts system is a prospect that many DNM proponents appear to find exciting. In this way, trust-less contracts can be created, which enforce the honouring of payments for services, if the provision of said service (goods in this case) can be validated. This is appealing to individuals dealing with wholesale or other tasks that require a high volume of trades, to people with varying demands: it allows much of the formal element of a trade to be automated.

The adoption of these currencies does not appear to have played a role in the takedown of Alphabay as a part of Operation Bayonet of July 13, 2017. This multi-national effort seized control of the market and operated the site for several days prior to its closure. This was rapidly followed by the takedown of Hansa, billed to take over from Alphabay as the next biggest DNM [62]. Although cryptocurrencies played only a minor role in the identification and seizure of this DNM, they have been locked where authorities have seized wallets. In the case of Monero, this may not provide significant forensic evidence or leads to follow, but it will prevent the coins from re-entering the market, depriving vendors of their profits. At the time of seizure, Alphabay was stated to be ten times larger than Silk road.

Bitcoin and Ethereum wallets, if accessed by law enforcement, could provide a significant body of data for further prosecutions and investigations. It is likely that this will encourage the adoption of Monero, ZCash and Dash in other DNM, as they realise the benefits of preventing relationships between addresses being derived trivially upon seizure of a wallet associated with criminal activity [63].

Alphabay staffers have commented that the market is 'only temporarily offline', but it remains to be seen whether this is bravado or a commitment to reviving the brand. Silk road is currently in its third iteration but has not managed to match the success of the original since FBI intervention in 2013, indicating that reinvention of the brand is possible, but does not have a history of success.

3.4.2 Hansa

Hansa was billed as the successor to Alphabay and accepted Monero and Bitcoin at its time of closure. Taken down during Operation Bayonet, it was operated for several weeks by Dutch law enforcement agents, prior to

being taken offline, with an official police notice replacing its homepage. It has been claimed that over 10,000 addresses for Hansa buyers outside of Holland were obtained in this operation [64].

Monero proposed for Hansa only briefly, going live at the beginning of July 2017. It is likely that the reason for Monero not being accepted prior to the Hansa shutdown, is the non-existence of a multi-signature implementation of a Monero wallet at present. Though the XMR (Monero) project team suggests that they are close to completing a multi-signature wallet, Hansa was shut down before it got the chance to implement the currency.

Hansa and Alphabay are notable for being the largest DNM of their time. However, they are also noteworthy for their adoption (or proposal thereof) of Monero in the wake of the Oasis exit scam.

3.4.3 Oasis

Oasis was the first DNM to use Monero. The distinction between Alphabay holding the title of 'first major' and Oasis holding the title of 'first', is that Alphabay processed orders of magnitude more trade than Oasis. Oasis traded in narcotics, fraudulent documents and digital items (of which RaaS was undoubtedly an element). This DNM, however, set back Monero adoption in October 2016 by conducting an exit scam [65].

An exit scam relies on the DNM having direct access to a body of escrow funds, money that is being held prior to confirmation of contract fulfilment on the part of vendors. Oasis went offline, with the operators accused of taking 150 Bitcoin and an undisclosed quantity of Monero from the escrow wallets. Oasis did not come back online, although some community hopes that it was a technical or legal issue, not a scam.

Although Monero was, at the time, considered to have lost its foothold in the DNM domain, Alphabay and Hansa continued with their implementation and popularisation of Monero amongst their own vendors, with Monero seeing increased trade throughout 2017.

3.4.4 The Wall Street

The Wall Street DNM is still in operation and is currently highly listed among DNM ranking sites. It was founded on October 19, 2016, and accepts Monero as a form of payment [66]. It offers the now-standard suit of multi-signature capability, centralised escrow and customer support as a part of its operation. It also provides localisation in both English and German.

Wall Street is an open DNM, allowing anyone to register. All the previously listed DNM were also of this category. Some DNM are listed as Referral or Invite only, but none of these currently offer Monero payments. Wall Street also offers deposit fewer payments, allowing individuals to purchase using wallets outside of the marketplace. This is considered advantageous to those who do not want address details and other identifying information associated with a static wallet [58].

As with the previously discussed DNM, the Monero option is an opt-in service for vendors. It is not within the remit of this report to derive accurate numbers for Monero usage, but it is likely that usage is currently low-but-rising as more individuals become educated about the benefits of this technology regarding privacy and anonymity. Considering the amount of personal data derived from the Alphabay and Hansa takedowns, it is likely that DNM and their proponents will begin to emphasise the importance of global, self-enforcing operational security, as opposed to relying on individuals to handle it themselves.

3.5 Key Issues for Law Enforcement

The increased emphasis on operational security in DNM, ransomware and other criminal uses of cryptocurrency present significant challenges, both current and future, to law enforcement agencies (LEA). The usage of transaction graphing techniques [67, 68] has been a coup for those wishing to identify where Bitcoin and other public-chain altcoins are being spent and where the money goes on its way towards fiat

liquidation [69]. This has strong possibilities in the future, for the identification and arrest of the perpetrators of cybercrime.

Initial research into the Bitcoin transaction graph emphasised the anonymity of the transactions themselves while pointing out that the underlying structure of transactions could be traced from origin to destination, given sufficient time and resources [67]. With the addition of personal data, or other transaction metadata (such as records from the Hansa takedown), it is possible to turn such tracing activity into actionable evidence in cybercrime cases. It is in the interests of cyber-criminals, though, to avoid such outcomes.

The focus of any cryptocurrency related investigation is the flow of money [70]. At some point, the operators of a piece of malware or DNM will want to cash out their profits into fiat currency, to be spent in the mainstream economy. This can be achieved by exchange, or by purchasing goods for further resale, but the important consideration is the avoidance of detection. Particularly sophisticated criminals will also realise that as the blockchain is immutable, it is wise to proof yourself against any potential investigation in the future. This can be achieved in many ways: coin mixing (tumbling) and exchanging for an appropriately privacy-centric altcoin being the two most common strategies.

Bitcoin tumblers are an example of a coin mixing service, and there are many them in operation at present [71]. In theory, this can be performed by oneself, but this requires an intimate understanding of the Bitcoin blockchain and sufficient computational resources to perform the number of transactions required to obfuscate the final trade. It is important to note that tumblers that work by performing many transactions can be expensive, costing up to 4% of the laundered sum (2-3% is the normal range). It doesn't protect against derivation by sufficiently driven transaction graph attempts, which will eventually work through the transactions to derive a path followed by the currency to a given set of egress points.

CoinJoin and CoinShuffle [72] are two proposals, discussed previously in brief, which integrate a form of coin mixing into altcoins (Dash being notable for its incorporation of CoinJoin into PrivateSend) [71, 73]. Figure 9 provides a basic outline of the service and what it seeks to achieve.

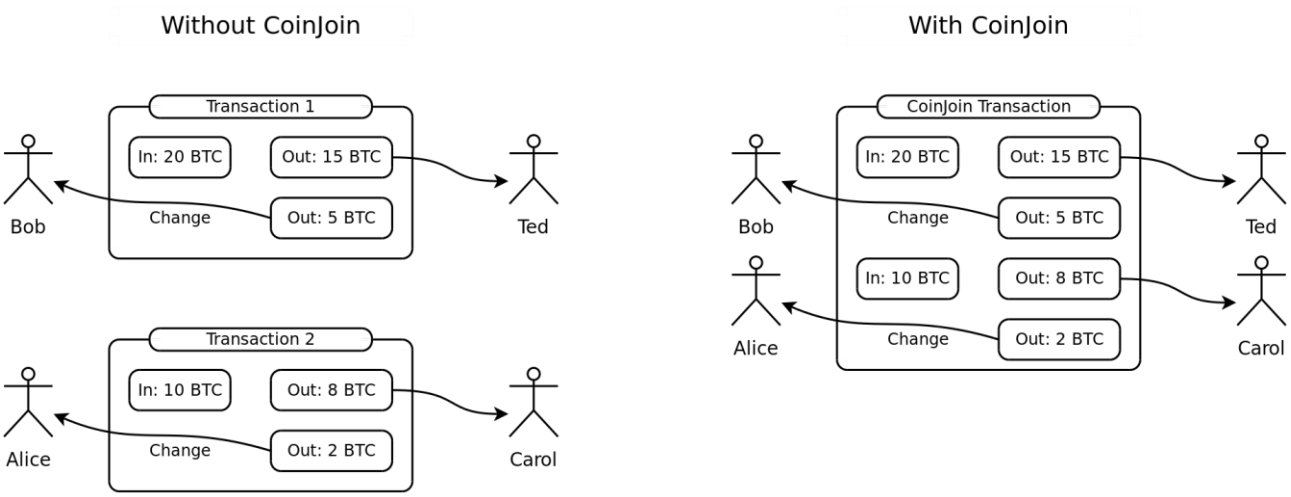

Figure 9 – CoinJoin basic concept

By associating transactions with others, it is possible to commit them to the same block, with their addresses being used interchangeably. In this way, a transaction is no longer tied to a single wallet, but to a set of wallets, which all contribute to the transaction pool. The path between the sender and recipient is thereby obfuscated, though in small-enough sets it is possible to derive relationships, given a sufficient sample set or associated metadata. It is for this reason that Dash uses master nodes to control the process of joining transactions, to ensure that a large enough set is generated and processed promptly. Dash is not currently adopted by any of

the major DNM, nor has it been incorporated into for-profit malware, but it does offer services that appear to be increasing in demand.

Coin mixing, when incorporated directly into the blockchain protocol used by a given currency, can defy existing transaction graph methods by prevent reliable association of addresses with a given transaction. It will still be possible to observe in and outgoing payments in a public blockchain, and it is for this reason that the protocols implementing CoinJoin or its equivalents, tend to favour private blockchains, encrypted so that even the developers cannot derive information about their currency.

Monero uses ring-signatures to provide a similar service, though it is a bespoke implementation [9], not associated with the CoinJoin, CoinShuffle or Dash projects. Unless LEAs can derive associated data, or break the ring-signature scheme itself, it will be exceptionally difficult to trace transactions. Transaction graph methods will not be effective against Monero, until this issue is resolved (if it can be). DNM takedowns have shown that it is possible to obtain rich sources of data that can be associated with cryptocurrency wallets [64], and although Monero protects its users by using stealth addresses for each transaction, ownership of multiple different wallets leaves cyber criminals only as protected as their operational security and least private wallets allow them to be. Where Monero and similar currencies are used, it is likely that such information will be required to make headway regarding the history of a given privacy-centric altcoin address.

A recently highlighted issue is the trivial way people with relatively little technical knowledge can exchange one cryptocurrency for another. Shapeshift allows the swift exchange of currencies, though not in substantial amounts. The current deposit cap for Bitcoin is 1.4234 ($4,920) [54], though this can be circumvented by splitting funds into multiple wallets or using multiple rounds of conversion to fully exchange the balance of Bitcoin into, for example, Monero. The Wannacry operators would likely have had to do something like this to transfer their Bitcoin into Monero, proving that it is possible, and that arbitrary caps can only complicate (and possibly slow) the process, not prevent it.

Despite cooperating with LEAs in the ongoing Wannacry investigation, it's hard to see what Shapeshift can do, other than blacklist wallets as they are reported. Unless these wallets are blacklisted from their own chains, it is possible for criminals to transfer funds to new wallets, possibly with sufficient speed to overcome observation attempts and exchange funds before they are noticed. If the blockchain in question belongs to Monero, Dash or ZCash, this becomes a whole lot harder, as the funds may remain obfuscated until they transfer into a public-chain currency like Ethereum or Monero. Increased cooperation with exchanges, especially ones that do not require users to identify themselves will be increasingly important, especially as the rate at which wallets needs to be blacklisted grows to exceed the feasible rate of doing so.

A final, more ephemeral consideration for LEAs, is the concept of trust-building between malware operators and their targets. The Ethereum smart-contract service, and the various iterations of this being created at an increasing pace, offers a potential way for cybercriminals to ‘legitimise’ themselves in the eyes of their victims [74]. By using the smart-contract system to secure payment and process the return/decryption of keys at a rate beyond the capability of manual services, it is possible that malware operators could create an environment of trust that has been denied to them by exceptionally bad actors (those who do not decrypt files – most ransomware operators). This is purely hypothetical at this point, but academics and cryptocurrency community commentators alike have proposed means by which this could be achieved.

4 Conclusion

This report has provided an overview of the current role of altcoins in cybercrime, specifically where malware and DNM-related. Four key currencies have been identified, for their attributes of market-value, privacy, anonymity and potential for further software development to extend the capabilities of malware operators.

Privacy and anonymity are sought after by malware operators and DNM patron/merchants alike, but the role of currencies like Monero, ZCash and Dash are still being defined. Monero has a significant lead on the other two regarding adoption by criminal enterprise and market capitalisation. There have been four major market proposals to incorporate Monero into DNM sites thus far, with three of them reaching deployment. Two of these have been taken offline, Alphabay to Operation Bayonet, and Oasis to an exit scam by its operators. However, with the increased capabilities of law enforcement agencies now apparent to the cryptocurrency community, especially with regards to the illusion of Bitcoin anonymity, it is not unreasonable to expect that an emphasis on privacy-centric currencies will emerge in the very near future. This may be through competition eliminating those markets that do not adopt such currencies, or by the DNM domain adopting one or more of the privacy-focused currencies.

Ransomware demanding payment in altcoins has been uncovered, a recently discovered strain Kirk, demands payment in Monero. CryptoCore has not yet been deployed, but has been offered for sale in exchange for Bitcoin. This ransomware source code provides the purchaser with the ability to deploy ransomware that requests payment in Monero or Ethereum. Wannacry, though typical in its Bitcoin ransom demands, recently has its balance removed from three Bitcoin wallets associated with it, and exchanged for Monero via the account-less exchange site, Shapeshift. These developments indicate an increasing awareness of the technological advances in cryptocurrency and the new possibilities for privacy and obfuscation. The Wannacry operators had considerable time to plan their exit strategy, indicating that they may have been considering the optimal way to obtain their funds for some time.

These findings lead to the inevitable conclusion that current methods of tracing transactions will continue to bear fruit, as Bitcoin is still by far the most popular medium of exchange for malware and DNM activity. Ethereum increasing in appeal in both domains doesn't offer any additional privacy features, but can be tumbled in much the same way as Bitcoin. Potential zK-SNARK integrations have been proposed, but have not yet been implemented, and it is unclear as to whether the developers will choose to provide a private Ethereum implementation on the core branch. However, this is a domain in a state of change, and that change will inevitably lead to those using Bitcoin and Ethereum being subject to the increasingly effective means of transaction derivation available to law enforcement. Transaction graph visualisation and other means of determining the link between originator and destination wallets will increase in efficiency and effectiveness. This will likely lead to increased LEA effectiveness in identifying cybercriminals associated with DNM and malware.

The adoption of Monero, and the existence of several alternative privacy/anonymity altcoins, indicates that success against traditional forms of malware and DNM payment will encourage adoption of alternatives. It is likely that the easiest to use of these options will take precedence, and currently that would indicate that Monero is likely to play an even larger role in the future of malware monetization. Should weaknesses be identified in the ring-signature scheme employed by Monero, Dash and ZCash both offer bespoke alternatives that may prove resistant to such countermeasures.

References

[1] Aurangzeb, S., Aleem, M., Iqbal, M.A. and Islam, M.A., 2017. Ransomware: A Survey and Trends. Journal of Information Assurance & Security, 6(2).

[2] World Coin Index. 2017. . August 10.

[3] Ward, M., 2014. Cryptolocker victims to get files back for free. BBC News, August 6.

[4] Sia Official Website. 2017. . August 10.

[5] Reid, F. and Harrigan, M., 2013. An analysis of anonymity in the bitcoin system. In Security and privacy in social networks (pp. 197-223). Springer New York.

[6] Reynolds, P., Reynolds, P., Irwin, A.S. and Irwin, A.S., 2017. Tracking digital footprints: anonymity within the bitcoin system. Journal of Money Laundering Control, 20(2), pp.172-189. Vancouver.

[7] Monero Home Page. 2017. . August 10.

[8] Noether, S., 2015. Ring SIgnature Confidential Transactions for Monero. IACR Cryptology ePrint Archive, 2015, p.1098.

[9] DeMartino,Ian. 2014. "CryptoNote Offers More Anonymity for The Future of Cryptocurrencies". CoinTelegraph. October 14.

[10] Bitcoin Magazine. “Alphabay Comments on Bitcoin Congestion, Monero Adoption and Zcash Possibilities”. 2016. . December 21.

[11] HotHardware. “Star Trek-Themed ‘Kirk’ Ransomware Beams Down With 'Spock' Decryptor”. 2017. . March 17.

[12] Allison, Ian. International Business Times. 2016. “Machine Learning Cybercrime Experts Tip Monero to join Bitcoin for Darknet Ransomware”. . September 8.

[13] WorldCoinIndex. 2017. . August 10.

[14] Ethereum Home Page. 2017. . August 10.

[15] Higgins, Stan. Coindesk. “Startups See Service Outages Amid Ethereum Blockchain Backlog”. 2017. . June 21.

[16] Buntinx, JP. The Merkle. 2017. “CardleCore may introduce new Monero and Ethereum Ransomware”. . April 18.

[17] Wuehler, Eric. McAfree, Securing Tomorrow. “Beyond Bitcoin for Ransomware”. 2017 . May 31.

[18] Zcash Home Page. 2017. . August 10.

[19] Ben-Sasson E, Chiesa A, Tromer E, Virza M. Scalable zero knowledge via cycles of elliptic curves. InInternational Cryptology Conference 2014 Aug 17 (pp. 276-294). Springer, Berlin, Heidelberg.

[20] Sasson EB, Chiesa A, Garman C, Green M, Miers I, Tromer E, Virza M. Zerocash: Decentralized anonymous payments from Bitcoin. InSecurity and Privacy (SP), 2014 IEEE Symposium on 2014 May 18 (pp. 459-474). IEEE.

[21] Spring, Tom. ThreatPost Blog. “Zcash Spurs Rash of Malicious Mining Software”. 2016. . December 13.

[22] Dash Home Page. 2017. . August 10.

[23] Ruffing, T., Moreno-Sanchez, P. and Kate, A., 2014, September. CoinShuffle: Practical decentralized coin mixing for Bitcoin. In European Symposium on Research in Computer Security (pp. 345-364). Springer, Cham. Vancouver.

[24] Torpey, Kyle. BitCoin Magazine. “Darknet Customers are Demanding Bitcoin Alternative Monero”. 2016. . August 26.

[25] Kouki Janika. Minergate Blog. 2016. . July 16.

[26] AnonCoin Wiki. 2017. . August 10.

[27] CoinDesk. “Comparing Litecoin to Bitcoin”. 2014. . April 2.

[28] Total Defense. “Litecoin is Targetted”. 2013. . July 8.

[29] Huang, D.Y., Dharmdasani, H., Meiklejohn, S., Dave, V., Grier, C., McCoy, D., Savage, S., Weaver, N., Snoeren, A.C. and Levchenko, K., 2014, February. Botcoin: Monetizing Stolen Cycles. In NDSS.

[30] F-Secure. The Customer Journey of Crypto-ransomware. 2017. . February 16.

[31] F-Secure. State of Cyber Security in 2017. 2017. . February 16.

[32] Poloniex Cryptocurrency Exchange. 2017. . August 10.

[33] Coinbase Cryptocurrency Exchange. 2017. . August 10.

[34] Beigel, Ofir. 99Bitcoins. “How to Buy Bitcoin Anonymously and without ID”. 2017. . September 25.

[35] McCausland, Phil. NBC News. “Companies Stockpiling Bitcoin in Anticipation of Ransomware Attacks”. 2017. . May 18.

[36] Monero Forums. “How to Obtain Monero”. 2016. . August 5.

[37] ShapeShift. Simple Coin Exchange. 2017. https://shapeshift.io/#/coins . August 10.

[38] Exodus. Multi-currency Wallet. 2017. . August 10.

[39] Hernandez-Castro, J., Cartwright, E. and Stepanova, A., 2017. Economic Analysis of Ransomware.

[40] Hernandez-Castro, J., Cartwright, E. and Stepanova, A., 2017. Ransomware and Game Theoretic Insights on Kidnapping.

[41] Coinomi. Mobile Multi-Currency Wallet. 2017. . August 10.

[42] Russo, Camila. Bloomberg. “Ethereum Slides as Network Backlog Points to Growing Pains”. 2017. . June 21.

[43] Shin, Laura. Forbes. “JPMorgan Chase to Integrate ZCash Technology to its Enterprise Blockchain Platform”. 2017. https://www.forbes.com/sites/laurashin/2017/05/22/jpmorgan-chase-to-integrate-zcash-technology-to-its-enterprise-blockchain-platform/#244fbeb77a33 . May 22.

[44] McAfee. McAfee Labs Tech Report. 2014. . June.

[45] Alpereum. News and Updates. 2017. . April 10.

[46] Gautham. News BTC. “Botnet Mines over $1,000 Worth of Cryptocurrency Everyday”. 2017. . May 5.

[47] Hertig, Alyssa. Coindesk Blog. 2017. . April 10.

[48] Gostev, Alexander. SecureList. “ZCash, or the Return of Malicious Miners”. 2016. . December 12.

[49] Symantec Security Response. "What you need to know about the WannaCry Ransomware". 2017. . May 14.

[50] Fox-Brewster, Thomas. Forbes #CyberSeucrity. "How One Simple Trick Just Put Out That Huge Ransomware Fire". 2017. https://www.forbes.com/sites/thomasbrewster/2017/05/13/wannacry-ransomware-outbreak-stopped-by-researcher/#520cc14974fc . May 13.

[51] Gallagher, Sean. Arstechnica. “Researchers say Wannacry Operator moved Bitcoins into “untraceable” Monero”. 2017. . August 5.

[52] Collins, Keith. @actual_ransom #wannacry. 2017. . August 10.

[53] Eagle News. "Map Showing the Extent of Wannacry Ransomware Attack". 2017. . May 15.

[54] Fox-Brewster. Forbes #CyberSecurity . "Wammacry Hackers are Using this Swiss Company to Launder $142,000 Bitcoin ransoms". 2017. https://www.forbes.com/sites/thomasbrewster/2017/08/03/wannacry-hackers-use-shapeshift-to-launder-bitcoin/#a202d783d0d2 . August 3.

[55] Abrams, Lawrence. Bleeping Computer. "This Week in Ransomware – March 17th 2017". 2017. . March 17.

[56] Leyden, John. The Register. "Dark web souk Alphabay shuts for good after police raids". 2017. July 14.

[57] Cylance Threat Guidance Team. Cylance. "Threat Spotlight: RaaS" 2017. .

[58] Deepdotweb. Dark Net Markets Comparison Chart. 2017. . August 10.

[59] Chaudhry, P.E., 2017. The looming shadow of illicit trade on the internet. Business Horizons, 60(1), pp.77-89.

[60] Kethineni, S., Cao, Y. and Dodge, C., 2017. Use of Bitcoin in Darknet Markets: Examining Facilitative Factors on Bitcoin-Related Crimes. American Journal of Criminal Justice, pp.1-17.

[61] Fawcett, J.P., 2017. Bitcoin regulations and investigations: A proposal for US policies (Doctoral dissertation, Utica College).

[62] Sterling, Bruce. Wired. "Alphabay as Described by the FBI". 2017. . July 21.

[63] Janze, C., 2017. Are Cryptocurrencies Criminals Best Friends? Examining the Co-Evolution of Bitcoin and Darknet Markets.

[64] Gibbs. S, Beckett, L. The Guardian. "Dark Web Marketplaces Alphabay and Hansa Shutdown". 2017. . July 20.

[65] Amani, Jelani. Cyptocoins News. "Has the Oasis run dry? Anatomy of a Dark Net Market Exit Scam.". 2016. . October 9.

[66] DeepDot.Web. "Wall Street Market adds Support for Monero". 2017. . July 7.

[67] Ron, D. and Shamir, A., 2013, April. Quantitative analysis of the full Bitcoin transaction graph. In International Conference on Financial Cryptography and Data Security (pp. 6-24). Springer, Berlin, Heidelberg.

[68] Ober, M., Katzenbeisser, S. and Hamacher, K., 2013. Structure and anonymity of the bitcoin transaction graph. Future internet, 5(2), pp.237-250.

[69] Neilson, D., Hara, S. and Mitchell, I., 2017, January. Bitcoin forensics: a tutorial. In International Conference on Global Security, Safety, and Sustainability (pp. 12-26). Springer, Cham.

[70] Narayanan, A. and Möser, M., 2017. Obfuscation in Bitcoin: Techniques and Politics. arXiv preprint arXiv:1706.05432.

[71] Heilman, E., Baldimtsi, F., Alshenibr, L., Scafuro, A. and Goldberg, S., 2016. TumbleBit: An Untrusted Tumbler for Bitcoin-Compatible Anonymous Payments. IACR Cryptology ePrint Archive, 2016, p.575.

[72] Ruffing, T., Moreno-Sanchez, P. and Kate, A., 2014, September. CoinShuffle: Practical decentralized coin mixing for Bitcoin. In European Symposium on Research in Computer Security (pp. 345-364). Springer, Cham.

[73] Bissias, G., Ozisik, A.P., Levine, B.N. and Liberatore, M., 2014, November. Sybil-resistant mixing for bitcoin. In Proceedings of the 13th Workshop on Privacy in the Electronic Society (pp. 149-158). ACM.

[74] Kaptchuk, G., Miers, I. and Green, M., 2017. Managing Secrets with Consensus Networks: Fairness, Ransomware and Access Control. IACR Cryptology ePrint Archive, 2017, p.201.