An Investigation into the Relationship Between Cryptocurrencies, Anonymisation Networks, and the Darknet Cybercrime Scene

(extended abstract of the MSc dissertation)

Angelos Velissaratos
Departamento de Engenharia Informática
Instituto Superior Técnico

Advisors: Professors Nuno Santos and Nelson Escravana

I. Introduction

The aim of this dissertation is to examine the Bitcoin cryptocurrency and the Tor privacy network and the different methods by which they can be used to facilitate criminal activities in the dark net. This thesis attempts to act as a comprehensive guide as to how an individual with both the legal and technical competence can attempt to pursue a forensics investigation in scenarios where Tor, Bitcoin or both in conjunction have been used by one or many individuals either as a means to commit a crime or as an accidental consequence if those systems were the targets of cybercrime themselves. For that purpose, it presents an up-to-date list of known vulnerabilities that are affecting both Tor and Bitcoin and methods by which one can extract digital artefacts from computer systems related to both technologies that could lead to de-anonymising their users and as a consequence aid in an investigation.

In recent years there has been an increase in the activity in the *dark net*, the section of the Internet that is not accessible normally without some sort of special software, in the form of concealed, digital marketplaces that are designed to privately deal with the selling of drugs and contraband medication, weapons, child pornography, among other things. The latest advancements in methods in which Internet users can conceal their true identities from the world and more importantly from the eyes of Law Enforcement Agencies on a worldwide scale helped in facilitating this trend [1]. Although techniques to provide anonymity while navigating public network are not a new concept and have in fact been around for quite some time, the advent of the Tor anonymity network with its ease of use and simplicity in the ways one can gain access to it and take advantage of its privacy-enabling features has allowed the facilitation of illicit storefronts in the bowels of the deep web. The Tor network and more importantly all the tools to gain access to it, including its official browser, are available to nearly every Internet user and are easily acquired from the so called clear web with little to no effort.

A close partner to Tor is a form of currency that is being used in order to facilitate the buying and selling of illicit goods online and that is the cryptocurrency that goes by the name Bitcoin or BTC for short. Since its release as open-source software back in 2009, this peer-to-peer system of transactions has created a new financial paradigm that nations and international markets are still trying to make sense of. Bitcoin and almost all other kinds of widely-circulated cryptocurrencies have one unique trait in common: they are not being issued by a centralised authority, such as a central bank or (supra) national governmental body, but instead are being created through a process that is referred to as *mining* [2]. Another unique aspect of Bitcoin is that transactions do not have to go through a bank or other financial network, but instead transfer from one party to another. Due to its reliance on cryptographic protocols in order to facilitate those transactions, Bitcoin offers at the very least a basic level of anonymity in transactions. Despite the fact that Bitcoin is relatively recent, a lot of research went into developing techniques that allow for de-anonymisation of transactions. Some of them, such as Reid and Harrigan's 2013 research into the subject [3] proved that anonymity is not guaranteed and that it is possible to link public keys (meaning users' wallets) with external identifying information, such as databases with recorded transactions.

When it comes to the matter of user anonymity in the Tor and Bitcoin networks the situation is further complicated if privacy-conscious users utilise techniques in order to further conceal their transactions and further remove the links that connect them to their activities. There is a plethora of options available, that can either be used individually or in conjunction with one another: Bitcoin mixers (or tumblers), online services that act as laundering services [4], [5], [6], and of course there is the combination of cryptocurrencies and anonymisation networks such as Tor. The latter is one of the most difficult situations to tackle, due to the fact that it provides Internet users with a way in which they can further remove themselves from their online activities by introducing several intermediate relay stations, that further confuse the digital tracks of a user.

This document was written with two very specific purposes in mind:

- As an attempt to complement existing literature in the fields of Tor, Bitcoin, Darknet Cryptomarkets by examining how those aforementioned systems work together in cyber-criminal activities.
- Act as a guide to help forensic investigators to locate digital artefacts generated by Tor and Bitcoin that could potentially be used as evidence in a court of law.

In addition, this dissertation is written for an audience with possibly no prior knowledge of the aforementioned systems and technologies. For this reason, it provides a very basic introduction for multiple aspects surrounding the the Bitcoin

and Tor systems, the dark net and cybercrime.

Note that this dissertation was not created with mobile or cloud computing forensic investigations in mind and focuses solely on traditional PC systems running some recent version of Microsoft Windows, Apple macOS, and GNU/Linux distributions such as Ubuntu. While the underlying operating principles of both the Bitcoin and Tor protocols respectively remain the same regardless of the device or operating system they are used on, mobile devices tend to differ significantly from personal computers in how they deal with issues such as file management, application file acquisitions and methods of installation. Perhaps more importantly, there is a significant level of difficulty involved in extracting the contents of mobile devices' storage media for reasons that range from enforced full disk encryption to the fact that getting physical access to their storage requires special tools and different methods of extraction from the ones that an investigator might be familiar with.

Main Contributions: This dissertation analyses and evaluates the core systems (namely Tor and Bitcoin) and it makes the following three main contributions:

- Perform a survey on existing literature that cover the subjects of Tor and Bitcoin de-anonymisation techniques and forensic artefact acquisition and combine their collective findings into a singular document.
- Analise the currently-known vulnerabilities and shortcomings that are affecting the security and anonymity-providing features of Tor and Bitcoin.
- Deliver a comprehensive and all-inclusive guide into forensically examining computer systems where Tor and Bitcoin were used and an analysis of the meaning of the recovered artefacts.

The remainder of this dissertation is organised as follows. Chapter 2 presents a quick introduction of all the different aspects covered by this dissertation. The operating principles of the Tor and Bitcoin protocols are presented in Chapters 3 and how they allow cryptomarkets to exist in the darknet. Known vulnerabilities that can lead to compromising users' anonymity is examined in greater detail in Chapter 4. A comprehensive guide to forensically examining all the systems discussed in this dissertation is presented in Chapter 5. Ultimately the dissertation is concluded in Chapter 6.

II. Related Work

Tor is a popular anonymization network which in simple terms allows an Internet user to hide their IP online. Bitcoin is the most widely-used cryptocurrency in circulation today. Together they are used by hundreds of thousands of people on a daily basis and they currently are the two most prominent ways by which crime is facilitated on the darknets. This chapter examines the basic components of both systems, followed by a description of the way they operate. But first, we provide an overview of the main cryptographic operations which are used in the design of these systems.

Of all major anonymity and privacy networks, Tor remains the most widely used [24]. This could be attributed to many different factors, potentially chief among them being the ease in which a person can access the network and utilise its services. From the end-user perspective, accessing the services offered by the network might be as easy as downloading and installing a modified version of the Firefox web browser1 from the Tor project's website. For individuals looking to offer private and anonymised services through the Tor network, the setting up process might be as simple as editing a few simple configuration files on their systems.

A typical Internet user has few options available to them if they want to hide their tracks when they are online. They can use Virtual Private Networks to route their network traffic through overlay networks or use intermediary, proxy servers to access information on their behalf. The problem with those solutions is that they generally tend to be centralised and fall under the control of authorities that keep logged entries of users and how those users are making use of them.

In the case of Bitcoin, the cryptocurrency first appeared on the scene with the introduction of a self- published paper by "Satoshi Nakamoto" back in October of 2008 [40] and was immediately followed by the project's launch on sourceforge as an open-source effort. The project's creator (or group of creators) simply known by the online moniker of "Satoshi Nakamoto" described it as a "purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution". Although the reasoning behind Nakamoto's decision to release the protocol specifications were never fully made clear, this paper's author's interpretation is that it has to do with the dismay the Bitcoin creators experienced with the way the international banking system operates and how susceptible it is to external influences that could threaten its very existence. In the Genesis Block of the Bitcoin's Blockchain (more on both in the following sections of this chapter), the following somewhat cryptic text is encoded in hexadecimal form: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks" This is a reference to the cover page of the British newspaper "The Times", dated 3rd of January 20092, that was promoting a news story in the same issue that was discussing the then Chancellor of the British Exchequer's Alistair Darling plan to issue another financial aid package to the banks after the worldwide economic crisis of 2007 - 2009. While this by itself does not reveal any actual informa- tion about the Bitcoin creators or their modus operandi, if it is taken into account in conjunction with the Bitcoin system's unregulated, de-centralised, peer-to-peer nature it allows a person to make some reasonable assumptions as to the reason why Bitcoin exists in the first place.

Since then, Bitcoin has become a worldwide phenomenon. In their highly cited report which exam- ines Bitcoin's meteoric rise in popularity, Barber et al. [8] go through the reasons why Bitcoin succeeded where other attempts throughout the decades failed in order to create a functional system that could serve as a large-scale e-payment system. Amongst the reasons listed in their paper, arguably the most prominent ones are:

- No central authorities and points of trust: As mentioned, the system relies entirely on a network of peer-to-peer nodes in order to function and on the assumed honesty of the majority of participant nodes in the network in order to validate transactions and to eliminate the problem of double spending and forgery.
- Predictable money supply: Bitcoins are currently gen-

erated in chunks of 12,5 per block and this aspect of the protocol is going to be examined in more detail in subsequent sections of this chapter. The amount of newly-created Bitcoins used to be 50 per block but the protocol has a hard-coded limiter to its supply algorithm [40, 8]3 halving the amount of Bitcoins per block once a certain threshold has been reached. In addition to that, there is also a hard-coded limit to the total number of coins that can ever be minted, at 21 million [40, 8]. For reference, at the time of the writing of this dissertation, there was a total of 16,820,025 Bitcoins in circulation4. Bitcoin's capped supply was conceived as a means to mirror the Gold Standard monetary model and to prevent spasmodic fluctuations in the market value of the cryptocurrency, something that traditional, fiat currencies suffer as a result of banking or political decisions.

- Creation of new businesses and business models: Being both a new type of currency and a new method of conducting financial transaction online, Bitcoin has enabled the creation of new types of businesses. Some legitimate, some not so much.

Discussion: Cryptomarkets are a byproduct of the tools and technologies made available freely to the general public by Tor and Bitcoin. By using Tor's hidden services, an individual can setup a server inside the Tor network that has its IP address and as a consequence its geographical location entirely hidden from individuals who try to communicate with it. Aided by Bitcoin's ability to provide its users the tools to conduct pseudo-anonymous monetary transactions online, this naturally makes those kinds of servers ideal breeding grounds for illegal activity. This chapter focuses specifically on the problem of cybercrime in the Internet, in particular on darknet cryptomarkets which leverage primarily Tor and Bitcoin as key enabler technologies.

Cybercrime, or computer-related crime is a form of criminal activity that involves the use of electronic equipment, such as personal computers (e.g. Windows and Linux-based PCs, Apple Macintosh, in both desktop or laptop configurations) and various other personal electronic devices such as mobile phones (smart phones), tablets and in the past Personal Digital Assistants, and potentially a use of a network, either local or wide-area such as the Internet with the ulterior motive of inflicting to a person or group of people physical or metal harm [38].

The Internet, and more specifically the World Wide Web is comprised of three distinct, layers that are often visualised in the form of an iceberg1 as seen in Figure 3.1. The iceberg is separated in three parts each one representing The Surface Web, the Deep Web and the darknet [12]. The analogy is as such: The part of an iceberg that is seen floating on the sea comprises only a small fraction of its true volume. The same can be applied to different layers that make up the Internet and the World Wide Web. The first layer, the Surface Web, is the one that is immediately available for observation and interaction. It is comprised of all the information that are available on the Internet and in the Web that can be indexed by a search engine (e.g. Alphabet's Google) and can be accessed by anyone using the Internet.

The second layer, is the one that is not immediately obvious to a normal Internet user and it is usually referred to as the Deep Web. While the name implies in a sense mystery and potentially hidden and concealed activities, it is actually the part of the Internet and the World Wide Web that exists behind log- in screens, news site paywalls (e.g. The Wall Street Journal), video-on-demand (e.g. Netflix), corporate Intranets, pages behind CAPTCHAs, and so on. Websites and other content on the Deep Web could potentially be accessed by knowledge of specific, hidden URLs via a normal web browsing application.

The third layer of the Internet is the darknet. Depending on the circumstance and situation, the terms Deep Web and Dark Web/Net are used interchangeably, but for the purpose of this report and to avoid a pointless semantic dispute it would suffice to describe it as its own layer in the triad, that also forms a symbiotic relationship with the second one. It is a part of the Internet that is built on top of either overlay networks or darknet networks and generally require specialised software in order for someone to gain access to them.

While their mere existence and method of acquiring access to them does not necessarily make them illegal in any way, the level of privacy they offer and the means by which one can successfully conceal their activities on them makes them a natural hotbed for the development of criminal activities. With that said, most of the interest in the darknet lies in the activities that are happening or have the potential to happen inside them than their technical aspects.

III. Darknet Cryptomarkets

Cryptomarkets are a byproduct of the tools and technologies made available freely to the general public by Tor and Bitcoin. By using Tor's hidden services, an individual can setup a server inside the Tor network that has its IP address and as a consequence its geographical location entirely hidden from individuals who try to communicate with it. Aided by Bitcoin's ability to provide its users the tools to conduct pseudo-anonymous monetary transactions online, this naturally makes those kinds of servers ideal breeding grounds for illegal activity. This chapter focuses specifically on the problem of cybercrime in the Internet, in particular on darknet cryptomarkets which leverage primarily Tor and Bitcoin as key enabler technologies.

Definition of Cybercrime: Cybercrime, or computer-related crime is a form of criminal activity that involves the use of electronic equipment, such as personal computers (e.g. Windows and Linux-based PCs, Apple Macintosh, in both desktop or laptop configurations) and various other personal electronic devices such as mobile phones (smart phones), tablets and in the past Personal Digital Assistants, and potentially a use of a network, either local or wide-area such as the Internet with the ulterior motive of inflicting to a person or group of people physical or metal harm [7].

While in years past, especially since the advent of the personal computer / microprocessor revolution in the mid 1970s, when personal computers started to became a household commodity, cybercrime was either not even a fully conceived idea or it was mostly encountered in cases where isolated computer systems were the victim of theft or the source of data breach. In recent years the definition of cybercrime has evolved in order to cover areas such as online abuse and harassment via email, message boards and chat

rooms, financial fraud and unauthorised access to computer systems and networks via means such as phishing and social engineering, etc.

Since the proliferation of Internet access and advancements in the field of computational technology and encryption, a different form of cybercrime has emerged. From the bowels of a certain area of the Internet simply described as the darknet has emerged a new kind of technology for enabling stealth criminal activities.

The Internet, and more specifically the World Wide Web is comprised of three distinct, layers that are often visualised in the form of an iceberg. The iceberg is separated in three parts each one representing The Surface Web, the Deep Web and the darknet [8]. The analogy is as such: The part of an iceberg that is seen floating on the sea comprises only a small fraction of its true volume. The same can be applied to different layers that make up the Internet and the World Wide Web. The first layer, the Surface Web, is the one that is immediately available for observation and interaction. It is comprised of all the information that are available on the Internet and in the Web that can be indexed by a search engine (e.g. Alphabet's Google) and can be accessed by anyone using the Internet.

The second layer, is the one that is not immediately obvious to a normal Internet user and it is usually referred to as the Deep Web. While the name implies in a sense mystery and potentially hidden and concealed activities, it is actually the part of the Internet and the World Wide Web that exists behind log-in screens, news site paywalls (e.g. The Wall Street Journal), video-on-demand (e.g. Netflix), corporate Intranets, pages behind CAPTCHAs, and so on. Websites and other content on the Deep Web could potentially be accessed by knowledge of specific, hidden URLs via a normal web browsing application.

The third layer of the Internet is the darknet. Depending on the circumstance and situation, the terms Deep Web and Dark Web/Net are used interchangeably, but for the purpose of this report and to avoid a pointless semantic dispute it would suffice to describe it as its own layer in the triad, that also forms a symbiotic relationship with the second one. It is a part of the Internet that is built on top of either overlay networks or *darknet networks* and generally require specialised software in order for someone to gain access to them.

While their mere existence and method of acquiring access to them does not necessarily make them illegal in any way, the level of privacy they offer and the means by which one can successfully conceal their activities on them makes them a natural hotbed for the development of criminal activities. With that said, most of the interest in the darknet lies in the activities that are happening or have the potential to happen inside them than their technical aspects.

Darknet Architecture Analysis: As the name of this dissertation implies, a large part of it is dedicated into examining darknets, how they operate and the kinds of illegal activities that either take place on them or can be enabled to take place. While the technical implementation is different for each one of them, for the most part all of the darknet platforms that are in use today, such as I2p (Invisible Internet Project) [9], Freenet [10] and Tor [11], all utilise a decentralised, peer-to-peer architecture in order to function as information exchange channels. What this means, in very generalised and simplistic terms, is that they forgo the traditional model of a centralised client-server architecture that serves as the focal point of a network, providing information to connected client machines and being responsible for the coordination of traffic. Instead, in the peer-to-peer model *peers* (meaning machines participating in the network) have equal privileges in how they tackle the assigned workload.

What is really interesting and noteworthy is that although these systems utilise the Internet in order to operate, they can be considered as different layers, or more specifically, Overlay Networks. That means that they are networking infrastructures that are built on top of other networking systems [12]. This gives overlay darknets several advantages, since they don't have to *obey* the rules of existing networks, especially in the way data is encoded when passed through their channels. For example, the Tor privacy network has support for its own top-level domain [11], .onion, which is not formally supported by the Internet's DNS (Domain Name Service).

As mentioned earlier, one of the main differentiating factors between the Surface Web and the darknet is the fact the access to the the latter requires the use of either special system software configuration, or entirely different software altogether than the ones the general Internet-browsing public uses. For example, in the case of all three major privacy / anonymity networks, when a user who needs to use their services in order to conceal their activities online, they would need to configure their applications in such a way for them to bypass the normal internet communications channels and to use the anonymity networks and the encryption that they provide. Alternatively, if a user's activities are isolated to web browsing they could download Tor's official web browsing bundle that facilitates the connection to the Tor network without any end-user meddling[1].

Online Trading and Darknet Marketplaces: This section deals with examining the history and background of online selling of goods and services and the recent approach of doing illegal transactions using the darknet marketplaces. A large part of this section will be dedicated to examining the case of *Silk Road*, a darknet marketplace that has cast a huge shadow on the cryptomarket industry and is still discussed to this day, years after its demise.

The first known online, "e-commerce"-like transaction was a 1971 marijuana exchange between students. As described on J. Martin's book [1], students of Stanford University and the Massachusetts Institute of Technology were using ARPANET, which was the predecessor to the modern Internet to make arrangements in order to exchange cannabis for money.

In recent times new platforms have emerged that allow buyers and sellers to facilitate the buying and selling of drugs and other illicit goods online. They are called darknet markets or most commonly Cryptomarkets. J. Martin [13] describes a Cryptomarket as a type of website that employs advanced encryption in order to protect the anonymity of users. In addition, Cryptomarkets tend to shy away from accepting fiat currencies as a form of payment and instead rely on Cryptocurrencies such as Bitcoin. Barratt and Aldridge [14] also add to the definition of the term Cryptomarkets that it is a marketplace that can host multiple sellers and that it

[1] https://freenetproject.org/pages/help.html

"provides participants with anonymity via its location on the hidden web" and "aggregates and displays customer feedback ratings and comments". It is mentioned how participation in such markets usually requires a certain level of technical competence, meaning that an individual wanting to buy or sell will need to be able to know how to use specialised software required to access the darknet URLs (i.e. Tor Browser Bundle), and the ability to own and use cryptocurrencies and digital wallets.

Most of these platforms act as the *middleman* of sorts between the two parties, meaning that they do not sell the illicit goods themselves, instead provide a platform in which sellers can reach a wider audience. They might make use of an escrow system, meaning that when a buyer buys something from a vendor, the funds are not transferred immediately to the vendors but the marketplace holds on to them until the transaction is complete. This has been exploited many times in the past with "exit scams".

While they differ in the good and services that they trade, darknet marketplaces have several characteristics in common: Firstly their design structure is reminiscent of legitimate big-name websites such as Amazon and eBay, giving users the ability to search via a search function and the ability to browser according to category. Second, they utilise the encryption methods that the darknet platform they operate provides them with in order to keep communications secret, and third, they forgo the use of fiat currencies and other traditional forms of monetary payment in order to avoid leaving a trace of financial transactions conducted on their systems [15]. Instead they employ the use of cryptocurrencies such as Bitcoin for preserving anonymity. A combination of all three previously-mentioned make darknet marketplaces a lucrative place for individuals who wish to do business of dubious legal nature away from the curious eyes, especially those of law enforcement.

Silk Road and other cryptomarkets that followed used mainly two payment systems: "Finalise Early" and the "Escrow system" and for the most part it was entirely left up to the buyer to choose which payment system they preferred to use. As mentioned, cryptomarkets act as intermediates between buyers and sellers. When a buyer makes a purchase they do not transfer the funds directly to the seller but to the marketplace. After the transaction has been completed and the buyer indicates to the seller that they have indeed received their order, then the marketplace releases the funds to the seller. If the vendor has a good reputation on the market and is well trusted by the community they can ask for an early release of the funds. As a general rule of thumb, it can be considered appropriate to Finalise the transaction early when the seller is entirely confident that the vendor will ship the product. Finalise early is generally avoided in the case there is not enough trust generated by the vendor.

Another benefit of vendors having a good reputation on the darknet is they can charge a premium price for their products. Purchasing illegal drugs from a faceless and anonymous dealer online will always carry the inherit risk of it being a scam, and in that case a vendor that has a stellar profile and they are reviewed well by members of the community will have their merchandise considered more valuable since it has a much higher probability of actually arriving at the buyer's door.

A major drawback when it comes to cryptomarkets' lack of legitimate operating credentials is that they can also be the targets of scams. Anyone with the means to replicate the design of an existing cryptomarket can do so and have it operational inside the Tor network as a Hidden Service. That would allow them to scam unsuspecting buyers and sellers. It falls onto the users and the community of legitimate cryptomarkets to police the landscape. Typically, in places like Reddit[2] users will report those scam websites to other cryptomarket users. Because users of those services cannot seek legal advice from the police or any law enforcement organisation, it is vital to them and their interests that they participate in the policing and observe news and developments in the cryptomarket world. With no centralised authority in place, users need to rely on each other in order to remain safe and secure while making use of those services. That is the main reason why, as it was clearly demonstrated by Silk Road, that buyers and sellers try to maintain their reputation high. A seller with a bad reputation (usually a low feedback score) will have trouble selling to prospective buyers. The same principle could also be applied to buyers. A buyer with a low score might potentially mean that they have tried to scam sellers by falsely reporting that the merchandise they have ordered has not yet arrived and so on.

- Cryptomarkets do not sell themselves drugs but for the most part act only as the middleman between buyers and vendors.
- There is well documented precedent where users (buyers and sellers) of one cryptomarket jumped to the next competing cryptomarket that offered features similar to their previous one.

It would appear that any attempt at law enforcement to shut down one or multiple cryptomarkets contributes to nothing in the grand scheme of things. In fact it might even have the opposite effect since traditionally it made people a a lot more innovative in their attempts to hide their tracks further. So the real question regarding attempts to shut down cryptomarkets is that if the ecosystem can be disrupted, what steps need to be taken in order to do so. It is an interesting question indeed and probably one with multiple answers and approaches to the subject. But, it is not this dissertation's design goal to answer it but only to make the question available to the reader.

According to darknet news reporting website deepdotweb.com[3], at the time of the writing of this thesis there were approximately 32 operational markets and vendor shops in the dark web. When arranged by the date of their creation, we can see that Dreammarket is the oldest remaining marketplace in the dark web, having been around since 2013 and still going strong[4]. When examined by other notable characteristics, such as user reviews and satisfaction of their services, Dream Market, Libertas Market, Wall Street Market, and CGMC are amongst the highest ranking in the darknet.

Cryptocurrencies and Anonymisation Networks: Cryptocurrencies, especially Bitcoin, are widely used in darknet

[2]https://www.reddit.com/r/DarkNetMarkets/comments/3l515f/dnm_here_is_a_list_of_confirmed_scam_sites_if_you/

[3]https://www.deepdotweb.com/about-deepdotweb/

[4]https://www.deepdotweb.com/dark-net-market-comparison-chart/

marketplaces to facilitate anonymous monetary transactions online [16]. Both Bitcoin and Tor have developed a somewhat symbiotic relationship with one another, in multiple ways. Assuming that neither the buyer and / or the seller avoid significant missteps that would compromise their anonymity while using a cryptocurrency, such as advertising in some capacity their Bitcoin wallet address and associating it with their real life name or their online moniker that could be traced back to their actual identities, or a transaction ID, it is extremely difficult if not outright impossible at times to link transactions to individuals.

Since the peer-to-peer architecture of cryptocurrencies make them a *community-operated* system, there is no central authority that keeps checks and records of real world names and activities that take place inside the system, making it impossible for law enforcement agencies to issue a subpoena to a governing body, when the need arises. That does not mean that there is not a ledger in which transactions inside the system are recorded, but what gets transcribed in there does not directly reference people, locations, Internet addresses or the type of goods or services purchased with the currency. Yet again that does not mean that the system provides full anonymity. As mentioned earlier, if for example a user of the currency advertises their wallet address in conjunction with elements that could lead to their actual identities, that immediately creates a significant opportunity for individuals looking to de-anonymise cryptocurrency users. Therefore, systems such as Bitcoin are considered "pseudo-anonymous" [17] and not fully anonymous.

There is another method in which cryptocurrencies and anonymity networks can work together to create what, in theory, can be described as a more secure method of performing financial transactions online. As mentioned, Bitcoins and similar electronic currencies exist solely as digital assets, therefore they rely on computer networks in order to circulate and be useable as a type of currency. Therefore, it is entirely possible to alter the way in which cryptocurrency wallets are connected to the network, in this case the Internet. There are methods in which a user can configure their wallet software to utilise one of the aforementioned privacy networks in order to further blur their online traces.

While utilising the encrypted and abstractly-conceived communications channels of anonymity networks does indeed sound like a good idea on paper, recent studies into the field of cryptocurrency usage over a privacy network (specifically Tor) has shown that their concurrent use is anything but safe and that users should be very careful about doing so [18], [19].

A. How to Set Up a Darknet Marketplace

As mentioned, the majority of darknet cryptomarkets today run on the Tor network. More specifically they make use of Tor's Hidden Services feature in order to be accessible only via the Tor Browser or any other browser that is configured to access the Tor network and keep their geographical location secret via the use of rendezvous points on the Tor network.

The process of setting up a darknet cryptomarket has been refined and it now exists in an almost standardised form since the days of Silk Road. As shown in the instructional manual released by TheOnionShop creators titled "Onionshop Installation Guide"[5], it is a fairly simple and straightforward action to create a Hidden Service inside the Tor network. The *steps* one must take in order to do are plenty and it includes:

- **Selecting an operating system:** The authors of the paper recommend an Open Source operating system instead of a closed one, such as Windows.
- **Self host or use a hosting service:** Having access to the server infrastructure gives the user a greater degree of autonomy and potentially privacy.
- **Fake identity setup:** In case a hosting service needs to be utilised in order to host the Hidden Service, it is highly recommended for obvious reasons that one does not provide their real identity. In addition it is recommended that they create an email address that does not draw suspicion.

Summary: This chapter provided an in depth analysis of cryptomarkets, which are a byproduct of the tools and technologies made available freely to the general public by Tor and Bitcoin. By using Tor's *Hidden Services* feature, an individual can setup a server inside the Tor network that has its IP address and as a consequence its geographical location entirely hidden from individuals who try to communicate with it. Aided by Bitcoin's ability to provide its users the tools to conduct pseudo-anonymous monetary transactions online, this naturally makes those kinds of servers ideal breeding grounds for illegal activity.

Silk Road, which is considered to be the first successful darknet marketplace, by utilising the technologies and anonymity features available through Tor and Bitcoin has created a paradigm shift in the methods by which illegal activities can escape the eye of law enforcement online and even though it has long been shut down, it has left behind a rich legacy by having spawned a variety of imitators and successors. In the following chapter, a more in-depth analysis of Tor and Bitcoin vulnerabilities will be provided. Such vulnerabilities can be used as potential sources of forensic evidence.

IV. Tor and Bitcoin Vulnerabilities

This chapter is devoted into examining known Tor and Bitcoin vulnerabilities that could be exploited for the purposes of de-anonymising the users of both systems. Likewise, such vulnerabilities can be used for forensic investigations.

There is a variety of reasons that define whether the Tor network and the randomly-generated circuits that users create are secure or not. Due to its nature and different methods of being used, Tor vulnerabilities can come in many different forms. This section reviews the literature that revolves around the field of known Tor security vulnerabilities and exploitations. Being a network that is designed to operate on top of infrastructure that is donated by people the world over, Tor is bound to be the target of intense scrutiny in order for potential vulnerabilities to be discovered.

As mentioned previously, Tor is built around a network of volunteer nodes, situated across different countries and different continents around the world. The primary operating principle of the system is to hide the tracks of its users online

[5]https://www.deepdotweb.com/2015/03/27/onionshop-guide-how-to-set-up-a-hidden-service/
http://thehub7gqe43miyc.onion/index.php?topic=7507.0;topicseen

by re-routing their traffic across a series of nodes before that traffic reaches its ultimate destination. There are a few known methods by which Tor-related traffic can be analysed in order to de-anonymise the network's users, but can for the most part be separated into three main categories:

- **Protocol-level attacks –** A protocol-level attack can occur when an attacker takes advantage of a shortcoming in the design of a specific protocol, or by taking advantage of an outdated or insecure implementation of it in order to be able to carry out an attack.
- **Traffic correlation attacks –** As it currently stands, Tor cannot protect against the monitoring of traffic at the fringes of the network (i.e., traffic entering through guard node and traffic that is leaving the exit nodes to reach its ultimate destination). While Tor employs the use of several techniques in order to mitigate traffic analysis (i.e. splitting the traffic in even-sized cells), it cannot prevent traffic confirmation.
- **Fingerprinting attacks –** Also referred to as "Traffic Fingerprinting" is a technique that can be used to identify web traffic and user behaviour while browsing the web.

Next, we present some relevant attacks from each of these categories.

A. Protocol-level Attacks against Tor

The Tor network is susceptible to a number of protocol-level attacks that can be broken down into two different categories:

- **Cell manipulation –** Consists of the purposeful manipulation of "cells", which are the transmission units of Tor, in order to correlate traffic as it enters and exits the Tor network.
- **Routing attacks –** Involves the manipulation of the Tor network's circuit building mechanisms in order to build a circuit that will include compromised nodes.

Bitcoin Vulnerabilities: There has been a plethora of papers that have been published regarding Bitcoin and its inherit security features, or lack thereof. The Bitcoin protocol while providing a high degree of confidentiality in transactions also keeps a record of every single one that has taken place since its activation in 2009. As stated in previous sections, those transactions are recorded in the network's Blockchain, a distributed ledger that is available to all participating nodes in the network. While the information transcribed there exist in an anonymous form (i.e. not tied with information that can trace them back to their users such as real names and IP addresses), by making use of information from outside the Bitcoin network, it has been proven that certain transactions can be linked back to their instigators. Furthermore, while the information inside the Blockchain does not exist in a *plain-text* format, there are utilities and even websites that can allow one to parse the contents of the Blockchain and search for records that contain specific Bitcoin addresses and even get a list of all transactions associated with them.

In addition, besides using external information to correlate users and their transactions, there are methods by which one can for example manipulate the protocol's built-in mechanisms against Denial-of-Service attacks (DoS) in order to route traffic via specific channels on the network. Furthermore, making Bitcoin wallets route their traffic over the Tor network, something that seemed like a good idea not that long ago, was recently discovered to have the potential to be catastrophic when it comes to maintaining Bitcoin users' anonymity, as explained below.

In this section Bitcoin vulnerabilities are classified in two different categories based on the factor that triggers them and allows them to be a liability:

- **User-induced –** Opportunities for exploiting aspects of the Bitcoin network based on actions performed by its users. Someone who can see all of your Internet traffic can easily see when you send a transaction that you didn't receive (which suggests you originated it). Bitcoin-QT has good Tor integration which closes this attack vector if used.
- **Architectural shortcomings –** Flaws or shortcomings presented in the Bitcoin protocol itself that would allow for deanonymisation.

Bitcoin over Tor: Since it has been demonstrated that Bitcoin transactions are not entirely anonymous but pseudo-anonymous and can be linked back to their issuers and receivers, Bitcoin users naturally have been trying to figure out different ways by which they can augment the protocol's privacy features and potentially build upon them in order to further conceal their anonymity online.

One such way was to connect their Bitcoin wallets online through the Tor network. While on paper it sounds like a great idea, recent research in the field has disproved it. The most widely-cited research was done by University of Luxembourg student and fuculty members Ivan Pustogarov, A Biryukov and D Khovratovich [19], [18]. Among their findings, we highlight the following:

- **Routing Bitcoin traffic through Tor –** The Bitcoin protocol has built-in anti-DoS algorithms that works with a reputation-based system. By making use of that system, when a malformed message is sent to a node on the Bitcoin network, the sender is afflicted with a score that varies depending on the type of message that was sent. When that score reaches a value of 100 then the sender's IP address is banned from the network for a 24-hour period.
  What this means in the context of Bitcoin usage over Tor is that it is theoretically possible for an attacker to ban clean and safe Tor exit nodes by making them send malformed messages to the Bitcoin network and then inject their own compromised exit nodes on the Tor network that Bitcoin users will have no option but to use unwillingly.
  The subject can be even further complicated and dangerous if the attacker also has the ability to ban "good" Bitcoin peers on the Bitcoin network. That would mean that the attacker would not only control the communications path to the Bitcoin network but also peers that can validate transactions. That would give the attackers the methods by which they can drop blocks and transactions which would in turn increase the probability of double spending, therefore compromising one of the Bitcoin's alleged innovations and key components. Traffic confirmation attacks could potentially also happen allowing opportunities for deanonymisation and transaction link-

ing.

- **Fingerprinting attacks –** By exploiting the Bitcoin peer discovery protocol it is possible to fingerprint users on the network. The idea is very simple: In order to get the list with the IPs of known Bitcoin clients on the network, clients send GETADDR messages to known peers on the network. In reply they receive ADDR messages with said list. If enough GETADDR messages are being sent, peers will willingly share the IP addresses of all clients that are stored in their database.
  An attacker can easily manipulate the list of known IP addresses that can be sent to other peers. They can include a variety of combination of IP addresses that do not necessarily belong to the Bitcoin network, for example Tor node addresses, VPN addresses, and so on. This effectively sends a *cookie*, as the researchers describe it that can be used to fingerprint the user. Later that Bitcoin client can be queried with a GETADDR message that will make them divulge its list of known IP addresses and in the process reveal that combination of selected IP addresses that were passed on to its database in the form of the afforementioned cookie.
  This method of fingerprinting has a problem though. Each client can have stored in their database 20,480 addresses at a time. Every time a client will resume operation on the network, they will automatically connect to eight peers simultaneously and will request typically 2500 addresses. What this means, that this cookie will have a limited lifespan before it becomes overwritten by new addresses.
- **Sybil Attacks –** By exploiting the design of the Hidden services feature of Tor, it is relatively easy for an attacker to initiate Sybil attacks. A Sybil attack can occur when a reputation-based system is fooled by forging identities in peer-to-peer networks. In the case of Bitcoin over Tor, something that could provide one with a possible for attack is to fill up all the good nodes' connection slots, so that new nodes can connect only to an attacker's nodes. A way to make this possible would be by broadcasting the IP addresses of legitimate Bitcoin network nodes, but provide fake port numbers, so that any broadcast of those same IP addresses with the real port numbers is rejected because a Bitcoin client, stupidly, only considers the IP address, which it thinks it already knows.

Summary: In this chapter we observed that the Tor and Bitcoin networks, while providing a certain level of confidentiality to their users, they can have their anonymity features compromised due to a variety of reasons. Chief among them is the fact that they both are decentralised networks that rely on user-provided infrastructure in order to operate. That fact alone could potentially allow the traffic that is being generated by said networks and their users through compromised channels. Although both systems' developers are quick to react to fix newly-discovered vulnerabilities, the ones that are presented in this chapter can not necessarily be patched out as they are inherent to the design of the system.

In the case of Tor, the protocol's vulnerable points are examined and separated into three categories: Attacks done at the protocol-level, attacks that can correlate traffic and fingerprinting. In the case of Bitcoin, two main kinds of vulnerabilities are looked into: ones that can be triggered as a result of the users' actions and underlying flaws or shortcomings in the design of the Bitcoin protocol itself that when exploited could compromise the anonymity of its users. On the subject of Bitcoin usage through Tor network, there is a variety of attacks that have proven to be possible and feasable, mostly through the research done by Pustogarov et al. [19]. An attacker that can a large number of nodes on the Tor network can route Bitcoin traffic due to shortcomings in the design of the latter's built-in, Anti-DoS protection mechanisms.

The ethical aspect of research done on methods by which the privacy and anonymity features of both Tor and Bitcoin has been the subject of many published papers. One thing that is always taken into consideration is how Bitcoin and even more importantly Tor do in fact have a legitimate *raison d'être*. Tor has been used extensively in regimes where freedom of speech and expression is forbidden or otherwise punished. As such, researchers that performing studies in the field of deanonymisation always make special mention of that fact and how they would generally shy away from performing tests on the live networks themselves. In their paper which focuses on Tor statistical data, Loesing et al. [20] ponder about the consequences of publishing data that are measured from the live Tor network and they propose a set of guiding principles which should be followed when measuring Tor data.

V. Tor and Bitcoin Forensics

This chapter examines the forensics artifacts left behind by the Tor and Bitcoin protocols and the most common front-end applications a typical user might use in order to take advantage of those two protocols. It should be reiterated at this point that this thesis is only concerned with investigations conducted on so-called *traditional* computer systems, i.e. personal computers running recent versions of Operating Systems such as Microsoft's Windows, Apple's macOS and different flavours or distributions of GNU/Linux. As such, the little-to-no mention is provided to new forms of computing equipment, such as tablets and smartphones, devices that are capable of running Tor and Bitcoin software.

The Microsoft Windows family of operating systems is the the most widely-used system software Personal Computers. According to statcounter global stats, as of January of 2018, Windows has 82,6% of the marketshare, followed by Apple inc.'s macOS at 13,06%. The rest 4,26% is spread among various other Operating Systems, including different versions of GNU/Linux[6]. As such, this chapter will focus on those three major desktop operating systems according to their market share.

Areas of Forensic Focus on Operating Systems: This section is meant to familiarise the reader with the most common areas in which modern Operating Systems might store user files, application files, configuration settings and so on that could potentially be used as evidence-related artifacts. Areas of focus include (but are not limited to):

- application installation directories;
- user home directories and user-specific configurations;
- operating system services that log user activities.

[6]https://statcounter.com/

Microsoft Windows: In Windows, there are numerous potential sources for evidence extraction. We highlight six relevant ones: application directory structure, Windows prefetch system, Windows Registry, Windows virtual memory and pagefile, Windows Search, and Cortana.

Apple macOS

As mentioned earlier, Apple Inc.'s macOS not only has a sizeable marketshare in the desktop Operating System market but all the tools required to use Bitcoin, Tor and get involved in the dark net cybercrime scene are also available for it as well. It shares many similar traits with Microsoft Windows but it also includes some key differences, such as that there is no centralised database that stores user and application information (i.e. Registry) and the directory structure where application settings are stored also differs from that of Windows. Areas of forensic interest in macOS include the Application Installation Directory, the Apple System Log Process, Crash Reporter and Diagnostic Messages, the service that monitors changes to a given directory tree.

GNU/Linux Running the GNOME Desktop Environment

On Linux and other Unix-like operating systems the situation is a bit more complex as there is a greater degree of variation in the naming and placement of system files and directories. As such, it would take a disproportionate amount of time to describe each different distribution's quirks compared to their marketshare. As such, this section will focus on the aspects that are common on most of them, especially when they utilise the GNOME desktop as their Graphical User Interface.

Bitcoin Specific Forensics

This section will focus exclusively on techniques that can be used in order to extract digital artifacts from the Bitcoin system. As was mentioned in chapter 3, in order for a user to begin making transactions inside the network, they will to have a piece of software called "wallet". Therefore, most of the focus will be on that area.

Tor-specific Forensics

As stated before, the Tor Browser Bundle is the easiest way one can gain access to the Tor network. The Tor Browser is based on a modified version of the Mozilla Firefox web browser with custom modifications to allow a user to access Tor and some additional plugins for extra security, such as forced HTTPS connections and the option to disable javascript entirely.

This section is going to be based on the papers by Runa A. Sandvik and Aron Warren entitled Forensic Analysis of the Tor Browser Bundle on OS X, Linux, and Windows and "Tor Browser Artifacts in Windows 10" [21] respectively. These two papers go through artifacts left behind by Tor on the three main operating systems and the authors present some investigation scenarios based on some assumptions as to how the user might make use of the browser bundle. Next, we present some of the most relevant artifacts in their own sections.

Summary: The aim of this chapter was to provide a technical guide as to how an investigator could This chapter we went through all the possible forensics places on a Windows, Mac or Linux personal Computer.

Security incidents can occur in the confidence that a system, either hardware, software or a combination of the two will function as intended (or as advertised) and would not fail under certain conditions. Both Tor and Bitcoin promise to hide the traces of user activities but as further examination on later parts of this dissertation will attempt to show, traces can be left behind unless paranoia on the part of the user makes them take additional steps in order to further hide their tracks.

In computers running Microsoft Windows as their Operating System a great deal of information related to user activity is recorded in the system Registry that upon examination could provide an investigator of clues as to what that activity was and even when it was conducted. Additionally, newer technologies introduced in recent versions of Windows that were meant to either improve the system's performance or aid users in their day-to-day tasks, can be a great source of information regarding user activities when examined from a forensic perspective.

VI. Conclusion

The main contribution that this thesis attempted to offer was the creation of a survey of existing literature in the field of Tor and Bitcoin vulnerabilities and then how a forensics investigator could make use of that information in order to examine those two systems in the event that they were used in some form of electronic crime. Bitcoin is the most widely-used alternative payment system, and Tor is the most widely-used anonymity network, used in many countries around the world, including those that prohibit freedom of speech.

Recent advancements in the fields of computer technology and cryptography have made the actions that take place in the darkest corners of the web almost invisible to prying eyes and more importantly when it comes to crime invisible to the eyes of law enforcement.

The examination of the literature in the field of Tor and Bitcoin forensics, reveals that the front-end software that is used to facilitate the connection to both networks can in certain cases leave behind digital artefacts that can be used to either deanonymise Bitcoin transactions and expose wallet addresses. The Tor Browser can under certain conditions leave behind a plethora of trails related to user activity in areas such as the Windows Registry, Page File and RAM.

While Tor and Bitcoin have shown to perform according to the intend of their respective designers, research conducted on examining the operating effectiveness of both systems has shown that their ability to provide anonymity to users while being used can be compromised. And while both systems promise to hide the traces of user activities, traces of their usage can be left behind on devices that their users install the necessary front-end software to make use of them.

Future Developments: According to a research conducted by Recorded Future, a company that specialises in real-time threat intelligence, Bitcoin is set to lose its place as the dominant payment system in the dark web in the near future[7]. The report entitled "Litecoin Emerges as the Next Dominant Dark Web Currency" argues that Bitcoin has simply become too popular in order to be effectively used as an efficient method of payment in the dark web, and that it will probably be replaced by other cryptocurrencies, such as Litecoin and Dash. The transition period from Bitcoin to other Cryptocurrencies will take place was estimated to be six to twelve months (as of February 2018).

[7] www.cnet.com/news/bitcoin-wont-be-the-dark-webs-top-cryptocurrency-for-long

The more traditional forms of computing, meaning desktop and laptop computers are declining in sales. If we were to count smartphones and tablets and potentially wearable devices such as smartwatches as "computers", Android is be the number one used operating system worldwide. Apple's iOS also has a small but measurable and consistent marketshare. iOS and Android are similar and different in how they handle things such as: file operations, filesystem journaling, temporary file creation, and most importantly "full disk" encryption on the devices that are installed on. As such, most of the architectural flaws and exploits and the forensic techniques discussed in this thesis do not apply to those operating systems and devices.

REFERENCES

[1] J. Martin, *Drugs on the dark net: How cryptomarkets are transforming the global trade in illicit drugs*. Springer.

[2] S. Nakamoto, *Bitcoin: A peer-to-peer electronic cash system*.

[3] F. Reid and M. Harrigan, "An analysis of anonymity in the bitcoin system," in *Security and privacy in social networks*. Springer, pp. 197–223.

[4] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S. Savage, "A fistful of bitcoins: characterizing payments among men with no names," in *Proceedings of the 2013 conference on Internet measurement conference*. ACM, pp. 127–140.

[5] M. Moser, R. Bohme, and D. Breuker, "An inquiry into money laundering tools in the bitcoin ecosystem," in *eCrime Researchers Summit (eCRS), 2013*. IEEE, pp. 1–14.

[6] S. Abramova, P. Schöttle, and R. Böhme, "Mixing coins of different quality: A game-theoretic approach," in *International Conference on Financial Cryptography and Data Security*. Springer, pp. 280–297.

[7] R. Moore, *Cybercrime: Investigating high-technology computer crime*. Routledge.

[8] M. K. Bergman, "White paper: the deep web: surfacing hidden value," vol. 7, no. 1.

[9] F. Astolfi, J. Kroese, and J. Van Oorschot, "I2p - the invisible internet project."

[10] Freenet. [Online]. Available: {https://freenetproject.org/whatis.html}

[11] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The second-generation onion router."

[12] What is the definition of overlay networking? [Online]. Available: https://www.sdxcentral.com/sdn/definitions/what-is-overlay-networking/

[13] J. Martin, "Lost on the silk road: Online drug distribution and the 'cryptomarket'," vol. 14, no. 3, pp. 351–367.

[14] M. J. Barratt and J. Aldridge, "Everything you always wanted to know about drug cryptomarkets*(* but were afraid to ask)," vol. 35, pp. 1–6.

[15] D. Gayle, "Online market 'is turning drug dealers from goons to geeks'." [Online]. Available: http://www.theguardian.com/world/2016/feb/11/online-market-turning-drug-dealers-goons-geeks-darknet

[16] J. Buxton and T. Bingham, "The rise and challenge of dark net drug markets," vol. 7.

[17] R. A. Hardy and J. R. Norgaard, "Reputation in the internet black market: an empirical and theoretical analysis of the deep web," vol. 12, no. 3, pp. 515–539.

[18] A. Biryukov and I. Pustogarov, "Bitcoin over tor isn't a good idea," in *Security and Privacy (SP), 2015 IEEE Symposium on*. IEEE, pp. 122–134.

[19] A. Biryukov, D. Khovratovich, and I. Pustogarov, "Deanonymisation of clients in bitcoin p2p network," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. ACM, pp. 15–29.

[20] K. Loesing, S. J. Murdoch, and R. Dingledine, "A case study on measuring statistical data in the tor anonymity network," in *International Conference on Financial Cryptography and Data Security*. Springer, pp. 203–215.

[21] A. Jeffries. FBI seizes underground drug market silk road, owner indicted in new york. [Online]. Available: https://www.theverge.com/2013/10/2/4794780/fbi-seizes-underground-drug-market-silk-road-owner-indicted-in-new