Silk Road - A Case Study of Anti-forensic Techniques for Internet Crime

Andreas Handal Hellesnes, Ole André Hauge, Sander Stamnes Karlsen & Sylwia Harewska
Department of Information Security and Communication Technology
Norwegian University of Science and Technology (NTNU)
Gjøvik, Norway

***Abstract*—This paper analyzed the dark website Silk Road and identified what anti-forensics techniques were employed to ensure anonymity. As the original Silk Road and its successors are no longer operational, this paper used a qualitative literature review to collect information about previous research and documentation of its functionality. The effectiveness, drawbacks, and use cases of the identified techniques, mainly the TOR network and cryptocurrencies, were discussed in further detail. The findings revealed that both TOR and Bitcoin contained design flaws that might be exploited by investigators to acquire evidence. Results also showed that human errors were a significant contributor to de-anonymization while accessing Silk Road-related services. Furthermore, cryptocurrencies and their transparent nature indicate that they might be the best economical platform for investigators as all transactions are publicly available. As forensic techniques improve, criminals may refrain from such applications in the future.**

***Index Terms*—Silk Road, anti-forensics, Internet forensics, Internet crime, cryptocurrency, Bitcoin, The Onion Router**

I. Introduction

The Internet makes use of network technology to connect devices in *local area networks* (LAN) to enable communication across long distances. The LANs are interconnected, allowing computers on one or more neighboring networks to communicate with one another. Routers and switches are responsible for data forwarding between devices. On a global scale, core services like the *Autonomous System* (AS), the *Border Gateway Protocol* (BGP), *Internet Service Providers* (ISP), and *Domain Name Systems* (DNS) are used to connect networks. The networks that are connected to other networks are grouped into autonomous systems i.e., the Internet's large networks. An AS enforces the same routing policy in its internal network(s). BGP allows ASes to communicate by sharing their IP address space and connections to other ASes. These are owned by businesses that provide services for accessing, utilizing, or participating in the Internet, known as ISPs. On top of that, DNS allows users to enter domain names rather than IP addresses into web browsers. The Internet's DNSes convert human-readable domain names into IP addresses, which are used by systems to communicate [1]. As a result, the Internet has evolved into the backbone of modern civilization, serving as a platform for conducting business, selling goods, communicating, and sharing data. Furthermore, because the Internet lacks two crucial qualities, anonymity and privacy, it has become a vital source for intelligence gathering.

Enter the dark web, a network that provides anonymity and protection from surveillance. It is an informational lifeline for people living under oppressive regimes as it provides access to information and safety from prosecution. On the other hand, it helps criminals sell drugs, stolen identities, child pornography, hacking for hire, malware, and other illegal goods and services through a marketplace. Criminals can more easily conduct anonymous business thanks to the emergence of cryptocurrencies, as the combination of the dark web's anonymity and cryptocurrency makes it difficult and resource-intensive to investigate and prosecute criminals [2].

The TOR network is the underlying technology that allows the dark web to operate in privacy and anonymity. Thousands of nodes make up the network, which is utilized to connect senders and recipients. The term *layer* refers to each of these connections. Each layer contains an encrypted payload as well as a destination endpoint. When an intermediate endpoint receives a request, the outer layer is removed and the remaining data is forwarded to the next endpoint until the last layer is uncovered and the request is routed to the intended destination. Hence, the name *The Onion Router* [3].

The TOR network anonymizes the source and receiver of data by routing it this way. Only the IP address of the last intermediate endpoint will be visible to the destination endpoint. The previous and next endpoints will be known to the endpoints. Furthermore, because of the encryption employed between the source and intermediate destinations, a passive listener can not tell where the packets are going. The TOR browser is available for free download and can be used to access a secret sector of the Internet that provides access to services that are only accessible through a network of intermediate endpoints. The Silk Road website is an example of such a service [3].

Silk Road was an anonymous online dark web marketplace for the sale and distribution of illegal substances, principally narcotics, that was founded in February 2011. It served as a TOR proxy, allowing users to browse the site anonymously and securely. Since its creation, the FBI and Europol have shut it down twice, and its inventor, Ross Ulbricht, has been arrested and convicted on seven charges, receiving a life sentence without the possibility of parole. The United States has seized more than $3.6 million in bitcoin linked to the Silk Road [4].

However, anonymity is not completely guaranteed. It is feasible to identify intermediate endpoints, destinations, and

what endpoint is linked to an onion router using well-applied Internet forensic techniques, a methodology used to investigate crimes done on and/or with the Internet, and combined cooperation. To oppose forensics procedures, criminals employ anti-forensics strategies aimed at limiting the availability and utility of digital evidence, as well as disturbing and/or destroying the evidence's scientific validity [3].

The goal of this study is to explain, analyze, and evaluate the anti-forensics strategy employed by dark web users to remain anonymous and hidden. It addresses the following question:

> "What anti-forensics techniques are utilized on the Silk Road dark web website to remain hidden and anonymous, and what are their efficacy, drawbacks, and how may they be improved?"

The rest of the paper is structured as follows: Section II covers the background and history of Silk Road, while Section III describes related work. Section IV explains the study's methodology. The findings are presented in section V, and they are addressed in section VI. Section VII brings the paper to a conclusion and suggests further work.

II. Background

Silk Road was the first multimillion-dollar illegal marketplace, founded and administrated by Ross Ulbricht. Ross had very liberal views which made him particularly opposed to the notion of the state law restrictions against freedom of individuals. The liberal vision of freedom advocated the removal of the state from citizens' affairs. That vision was implemented in Silk Road, where the community was free and could finalize transactions that the government would not allow [5].

Silk Road was launched on February 6, 2011, according to legal documents cited in the case against Ross Ulbricht. Ross began by selling psychoactive mushrooms that he had grown himself. Because the platform was only known to individuals who were already on the dark web, the number of users grew slowly. That changed quickly after a Gawker piece about the Silk Road was published in June 2011. The site received a lot of attention as a result of this story, which included prominent personalities and law enforcement authorities. United States Senator Chuck Schumer of the United States issued a comment regarding the dark web market shortly after the story was released, bringing even more attention to the site.

Silk Road grew in popularity over time, making it extremely difficult to manage. There were up to 150,000 active users at the peak of Silk Road's popularity [6], [7]. As indicated in Figure 1, the bulk of these users were from the United States.

Undercover operations began in November 2011, with DEA agents posing as buyers and vendors on Silk Road to obtain access to Ross Ulbricht. Carl Force, also known by the username *Nob*, among others, was the agent who made the crucial discoveries in this case. Ulbricht employed a group of two to five administrators to assist him in running the site. The administrators were responsible for handling complaints, moderating the forum, and keeping watch of law enforcement leaks.

Origin	
Country	**Pct.**
U.S.A.	43.83%
Undeclared	16.29%
U.K.	10.15%
Netherlands	6.52%
Canada	5.89%
Germany	4.51%
Australia	3.19%
India	1.23%
Italy	1.03%
China	0.98%
Spain	0.94%
France	0.82%

Acceptable destinations	
Country/Region	**Pct.**
Worldwide	49.67%
U.S.A.	35.15%
European Union	6.19%
Canada	6.05%
U.K.	3.66%
Australia	2.87%
World. excpt. U.S.A.	1.39%
Germany	1.03%
Norway	0.70%
Switzerland	0.62%
New Zealand	0.56%
Undeclared	0.26%

Fig. 1. **Top 12 most frequent shipping origins (left), and acceptable shipping destinations (right).** Certain sellers ship to multiple destinations, hence totals may exceed 100%. Source: Adapted from [7].

Ross Ulbricht knew the agents were pursuing him by January 2013, so he grew suspicious of his workers, especially when 350,000 USD vanished from Silk Road's accounts. When one of his employees, Green, was arrested by authorities, Ulbricht contacted the user called *Nob* and ordered a hit on Green. The DEA agent took advantage of the circumstances to get closer to the main administrator known as the *Dread Pirate Robert* (DPR), who, at that time, unknowingly was Ulbricht.

The investigators spent a long time attempting to identify the site's administrator, as it takes a lot of experience and effort to hunt down someone on the dark web. Many agents were involved in this case, and they pooled their resources to achieve a common goal: to find DPR. They tried looking through intricate bitcoin transactions but finally, a simple Google search revealed the name of Silk Road's genuine administrator. Ulbricht had used his Silk Road pseudonym on the public Internet while posting questions in forums and uploading movies to YouTube, where the entries included his Google account: *rossulbricht@gmail.com*. It was the case's most significant break.

Ross Ulbricht was finally tracked to San Francisco, where he was apprehended by the FBI in October 2013. He was caught red-handed, while he was working on Silk Road. The platform was shut down immediately, and up to $4 million in bitcoin was seized from the site. The FBI announced on the site that it was dedicated to exposing criminals on the dark web. Ross Ulbricht was sentenced to life in prison in May 2015 [8].

The Silk Road case, as well as the news of Ross Ulbricht's arrest, boosted the site's profile even more. TOR was being downloaded and accessed by new users. Due to the lack of an unrestricted platform on the market and high demand, Silk Road 2 was established to fill the void. A new URL address, redesigned login screen, and security features that allowed

users to utilize the *Pretty Good Privacy* (PGP) encryption key to increase the authentication measure were all important developments [9]. The new administrator of Silk Road 2 was 26-year-old Thomas White.

The FBI's Operation ONYMOUS brought down Silk Road 2.0, and the principal operator, Thomas White, was captured in November 2014 [10].

The *Diabolus Market* renamed itself as *Silk Road 3 Reloaded* mere hours after Silk Road 2.0 was shut down. In comparison to previous versions, the new version used the anonymous I2P peer-to-peer decentralized network instead of TOR. Unlike Silk Road 1 and 2, Silk Road 3 allowed users to deal in a variety of cryptocurrencies [11]. According to one report, the most recent version failed to attract enough clients and was shut down [12].

III. Related Work

Significant research related to the site's closure was investigated through content analysis of dark web market forums. The investigation yielded insights concerning the dark web market userbase's behavior and the marketplace's prospects [4].

Rita Zajácz's research examined whether a stable market could exist in the face of online anonymity, defying the state [13]. She demonstrated how Silk Road was founded on a paradox. On the one hand, robust cryptographic anonymity was employed to aid in the concealment of information from the authorities. The same cryptographic anonymity made it difficult to apply rules and develop a stable market. Furthermore, Silk Road attempted to create subcultural norms to assure good behavior in the face of anonymity, but these norms were insufficient to govern the behavior facilitated by the architecture.

Regarding Silk Road, Catalina Goanta authored an article about the private governance of identity, focusing on the crypto community's unique identity management system [6]. She discovered that the identity was dependent on the roles that individuals might perform on the site, as well as their actual rights and responsibilities. To do so, special attention was paid to key contractual paradigm documents such as the Seller's and Buyer's Guides, as well as the Silk Road Charter, which was all sources of regulations written by the Silk Road's administrator, Ross Ulbricht, within the Silk Road community.

A percolation paradigm was utilized by Louis M. Shekhtman et al. to investigate the boundaries of privacy in conspiracy, dark web, and blockchain networks [14]. They did so by considering what would happen if one (or more) people in such a network were to be de-anonymized by an external identity, as these compromised persons may leak information about others with whom they engaged. This could lead to the information of more and more nodes being released. They use their framework to analyze three real-world networks: a blockchain transaction network, a dark web network of interactions, and a political conspiracy network. They discover that starting with one compromised user, it is possible to de-anonymize a considerable portion of the network ($>$50%) in fewer than 5 steps in all three networks. Overall, these findings provide suggestions for investigators looking to identify actors in anonymous networks, as well as individuals looking to keep their identities private.

IV. Methodology

Because Silk Road is no longer operational, the paper used a qualitative literature review to collect information from existing research and documentation of its functionality. This entailed identifying relevant research papers, books, reports, and other textual publications and determining their relevance to the subject. Acknowledged online academic search engines and literary databases were used to locate relevant academic sources. Weaker sources, such as news articles, were used to add substance to some of the information presented in the results and discussion when research had not yet explored a topic in depth.

Using a VPN and the TOR web browser, an attempt was undertaken to determine the presence of current operational Silk Road dark web sites. The objective was to acquire access to internal documentation and chat groups to gain a better understanding of the situation. There were, however, no current reputable onion sites found. The legitimate sites were down, according to posts on the dark web, and users were urged not to use counterfeit scam sites.

This paper is based on a selection of the publications that were encountered. Because the purpose of this article is to look at the internet anti-forensics techniques used by Silk Road, an attempt was made to identify publications created during and after the arrest of the site's developer.

V. Results

The Silk Road website was a marketplace for the sale and distribution of illegal substances. Several steps had been taken to guarantee that both the customer and the distributor remained anonymous. The most crucial methods were found in network activity and payment methods, as well as in product delivery [7]. This section describes the main methods that were utilized to ensure network, exchange, and general anonymity.

A. Network Anonymity

To ensure network anonymity, Silk Road took advantage of onion routing through the software *The Onion Router* (TOR) and its hidden services, as well as *Pretty Good Privacy* (PGP). This allowed packets sent between clients and servers to be both unreadable (confidential) and untraceable (anonymous) over the network, in addition to authenticated. Onion routing, TOR software, TOR services, and PGP are all explained in this section.

1) Onion Routing: Onion routing was developed by the United States Naval Research Laboratory to protect U.S. intelligence communication online and is the technique of using intermediate endpoints to route internet traffic as shown in figure 2 [15]. Instead of sending internet packets directly to the receiver, onion routing uses several endpoints, also known as nodes, to relay traffic through the network. The message

sent from the user is being encrypted several times, like the layers on an onion. These different layers of encryption are illustrated by the dashed lines in figure 2. Each node will remove or add a layer of encryption, depending on whether the packet is being sent to the server or the client. The client possesses all the keys and will encrypt each message, shown with black arrows in figure 2, with all layers of encryption, and then forward this message to the first node. This node will remove one layer of encryption with the one key it knows, which reveals the next destination in the chain but nothing more. This process is then repeated until there are no layers of encryption left, and the next recipient will then be the final destination, the server. For packets sent in return, this process is repeated backwards, usually through the same intermediate endpoints [2].

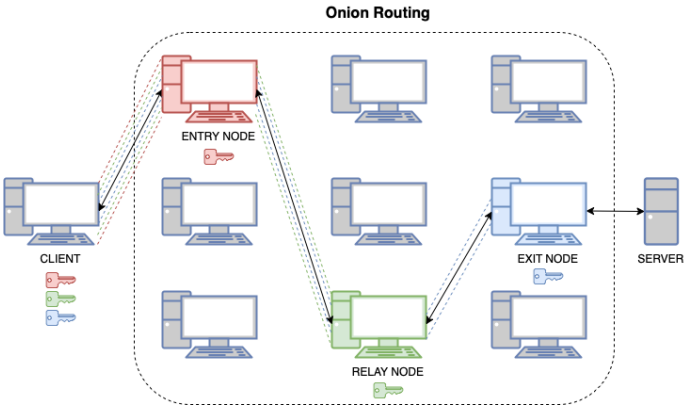

Fig. 2. Onion Routing

2) The Onion Router: The TOR software standardizes onion routing through a protocol that follows the same fundamentals as in the onion routing process. The TOR network consists of many publicly listed nodes. When a client wants to send a message, he first contacts a TOR directory, where he is by default distributed three nodes and a *circuit-ID* (CID). The CID will work as a public identifier to this client's chain of nodes. Further on, the client will establish an individual key with each node and inform about the distributed CID.

Messages sent will then be encrypted three times with these three keys by the client, and sent to the first endpoint. This entry node will decrypt the first layer of encryption, which reveals the next endpoint and leaves two layers of encryption. The packet, however, referred to as a cell, retains the same size despite the removal of a layer. This process is then repeated for the second endpoint, which sends its encrypted message to the final endpoint.

On the arrival at the final endpoint, only one layer of encryption remains. This layer will be decrypted by the final endpoint, leaving the message in cleartext. The packet will then be sent to the intended destination from this exit node. The response to the packet follows the same chain in reverse. This applies for a standard maximum of ten minutes before a new chain with a possible new CID is established. This whole process is then applied to each session. The protocol and nodes are what constitute the TOR network [3].

Onion routing through TOR provides several features. First of all, the final destination only knows about the last endpoint, which therefore in practice acts as a proxy for the client. Because this node could be placed at any location around the world, the client will also be able to act as if he was located at this geological location. While the final destination only knows about the final endpoint, all the endpoints only know about their previous and next endpoint.

As a result, no devices on the network know the entire chain, and none of them possess more than one key, making them incapable of reading the payload. In addition, the packets are all of the same size, which means it is impossible to see from the size of the packet wherein the chain the packet is currently at. Even the nodes themselves are not aware of which number they are in the chain. The nodes only know the CID, their corresponding key, their sender and receiver, and from that whether to decrypt or encrypt. Overall, this provides certain confidentiality over the network as well as anonymity for the client [16].

The anonymity is however not absolute, and TOR is vulnerable to different attacks. If the TOR directories were taken down, nobody would be able to access the TOR network, resulting in a denial-of-service. When it comes to anonymity, the client will ruin its anonymity if he were to log in with a personal account, use a credit card, or other information that can be used to identify a person. This would enable the server or final destination to identify who it is talking to. In addition, the last transmission between the exit node and the final destination is by design sent in clear text, meaning this transmission is vulnerable to man-in-the-middle attacks such as eavesdropping.

Therefore, it is recommended to also use some type of application-layer encryption, such as HTTP over TLS (HTTPS) or PGP, which encrypts the message itself between the applications on the client and the server, resulting in an encrypted message at the last transmission as well. Nevertheless, it is still theoretically possible to capture traffic between the client and entry node as well as between the exit node and server to then correlate this traffic and see whether the packet stream matches, in which case indicates that this client is accessing this server.

This is a weakness by design. However, it is also difficult to perform such an act, as these transmissions are difficult to locate and often change. On the other hand, these nodes are publicly listed, and the use of TOR often draws suspicious attention which motivates actors to go even further. The use of TOR is also distinguishable from different traffic, so if only one person is accessing the TOR network from a local network, it will be easy to locate which device is using TOR, which then removes the anonymity aspect of using TOR [16].

3) Onion Services: The Silk Road website itself also needs anonymity and is therefore set up as an onion service, formally known as a hidden service for the TOR network. These services are similar to regular websites but are only accessible

through the TOR network, and constitute what is often referred to as the dark web. In figure 2, with the use of HTTPS, there is still a security issue if an actor gets hold of the traffic in both ends. That is, between both the client and entry node as well as between the exit node and server.

By moving the server inside the TOR network, and hence becoming an onion service, this issue gets resolved and the server becomes hidden from the public. If a client now wants to talk to this hidden service, they will need to meet in the middle. This technique secures that neither the client nor the server knows who each other are, and thus achieves full anonymity.

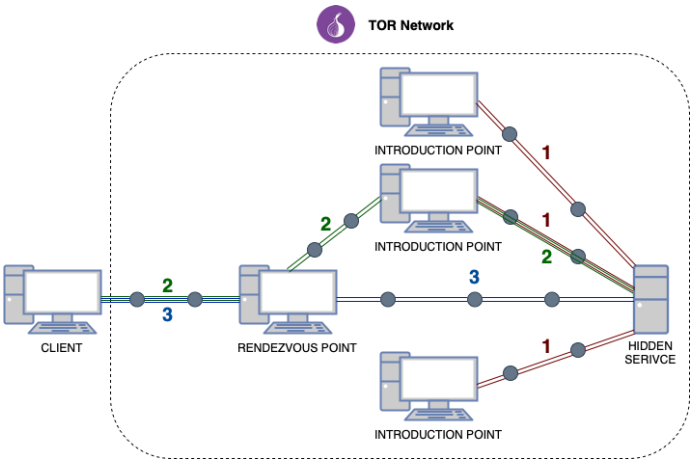

Fig. 3. Onion Service

To achieve full anonymity, the server first needs to set itself up as a hidden service, which is shown with red connections in figure 3. The server starts by picking out three nodes that will work as introduction points and then creates a full TOR circuit for each of these. Next, the server creates a hidden service descriptor, which includes the service's public key and the IP addresses of the introduction points. This descriptor will then be published to a distributed hash table, which is distributed throughout several TOR nodes. This means that all the nodes hold some information about the hash table, and when a client looks up a hidden service, the responsible node will provide the correct descriptor. The key to this hash table is what is called the onion address. This address is not publicly listed anywhere, and every client who wants to talk to this hidden service needs to know this onion address from somewhere else, which could be from a friend, specified TOR search engines, or somewhere on the public internet [15].

Clients wanting to connect to a hidden service needs to establish their connection by meeting the hidden service in the middle at some *rendezvous point* (RP). The client starts by knowing the onion address, from which it retrieves the addresses of the introduction points. Then, the client creates a full TOR circuit to an RP, telling it to connect to one of the introduction points, as shown with green connections in figure 3. In addition, the client includes a one-time password string, used to identify this session. The introduction point then forwards the message including the one-time password and the address of the RP to the hidden service through its TOR connection.

The server then decides whether it wants to establish a connection or do nothing. This could be based on the one-time password, making it an additional access password, but this is not a usual thing to do. If the server decides to establish a connection, it creates another full TOR circuit to the RP and sends over the given one-time password. The RP then checks for other connections with the same string, and if found, it bridges these connections and becomes another relay node in this session. This is shown with blue connections in figure 3. Because of this way of setting up the bridge, the one-time password also makes sure that no one else has gotten involved and tampered with the message.

The connection between the client and the server is then established, with a total of six intermediate endpoints which just forward packets like regular TOR traffic. Neither the client nor the server knows who each other are, and thus full anonymity is achieved. This process hides the server and makes them difficult to find, resulting in an unknown number of existing hidden services in the world [15].

4) Pretty Good Privacy: PGP is a program using public-key cryptography to provide asymmetric encryption of data ensuring privacy and authentication for secure communication. It can be used to sign, encrypt, and decrypt data like emails, files, and disk partitions. In essence, it allows the transmission of files and messages to be transported securely over the Internet without them being intercepted or deciphered. This was an important aspect for Silk Road helping users to stay anonymous and at the same time confirm that they were talking to the right person [17].

PGP was designed around the *Rivest–Shamir–Adleman* (RSA) algorithm introducing public key cryptography for secure data transmission. The RSA algorithm is asymmetrical using two keys: a public key and a private key. The public key is used to encrypt the message or data that the owner wants to send. He generates his pair of private and public keys, before sharing the public key, which is then used by those who want to communicate with him. As illustrated in figure 4, he is the only one who can decode the data as he is the only one who possesses the corresponding private key. Normally, the public key is distributed by email or made available on corporate- or personal websites.

OpenPGP is a PGP-based, cross-platform, open-source standard that is available to everyone, intending to allow the users to use their own cryptographic algorithms like AES, DSA, Triple DES, SHA-1, and ECC.

Although PGP implementations are extensively used, they have certain limitations in that users may struggle to understand the standard and how it might be utilized. Furthermore, Nemec et. al. discovered a vulnerability that affected RSA keys, which meant that PGP implementations that used an RSA key-pair were susceptible [18]. Owners of impacted

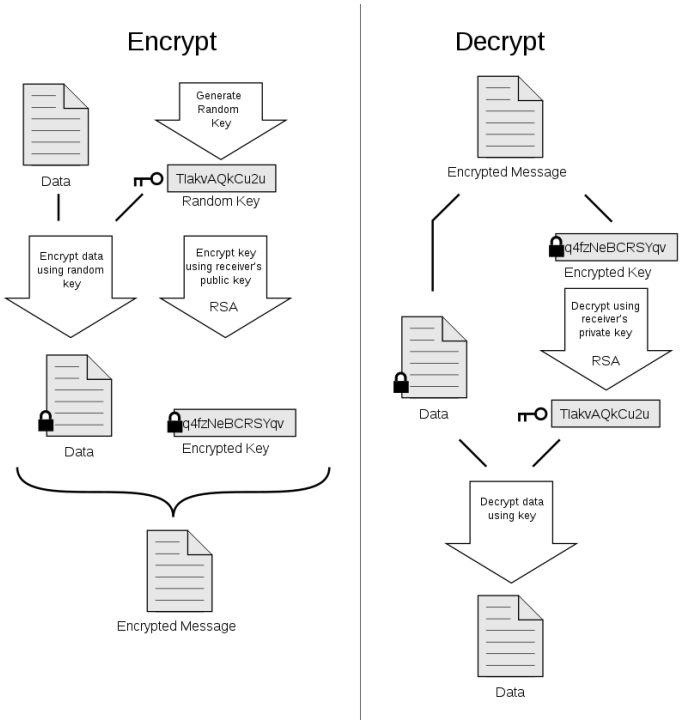

Fig. 4. **Diagram illustrating how PGP works.** Source: created by xaedes & jfreax & Acdx at https://commons.wikimedia.org/wiki/File:PGP_diagram.svg

implementations were required to alter their implementations and key pairs.

Although the ability to sign files and messages was necessary to establish that they originated from authorized administrators or drug distributors, it also assisted investigators in confirming Ross Ulbricht's identity as the *Dread Pirate Robert* (DPR), Silk Road's main administrator. After the physical capturing of Ross Ulbricht, his computer was seized and brought in for digital forensic investigation. Investigators discovered a journal on his computer, as well as a folder containing multiple keys, including his private PGP key. The investigators were able to corroborate that the uncovered private PGP-key was DPR's by using DPR's public PGP-key, confirming that Ross Ulbricht was the main administrator of Silk Road [19].

B. Exchange anonymity

The conventional banking systems and their transactions provide a record of every transaction containing personal information on each transaction. This paper trail of transactions is kept by the bank, whose services make the exchange, and is often accessed by law-enforcement agencies for investigations. For a hidden marketplace selling illegal goods, such as the Silk Road, to be sustainable over time it needs to ensure the anonymity of transactions for its users. By this logic, common bank transactions could not be used for Silk Road. Instead, they offered different solutions for payments such as PayPal, gift cards, cryptocurrencies, or even mailing money through postal services [20]. Because of the traceability of the other options, using cryptocurrencies for payments was by far the most popular amongst its users.

A whitepaper released in 2008 under the pseudonym *Satoshi Nakamoto* marked the inception of a new digital currency [21]. It detailed an open-source, peer-to-peer, decentralized payment system called Bitcoin. Bitcoin and digital currencies utilizing *blockchain* technology are now referred to as cryptocurrencies. Cryptocurrencies can be described as a set of cooperating ledgers, the blockchains, containing all past transactions and rules for validating new ones. The cryptocurrency's network creates blocks containing transaction data.

In the case of Bitcoin, the network takes approximately 10 minutes to create one block. It also limits the block size to 1MB. The nodes collect the new transactions that are being broadcasted into a block. Each node in the network tries to find the *proof-of-work* (POW) to validate its block. The first node that finds the POW for the current block broadcasts it to the rest of the nodes. POW is a complex algorithm that typically requires large amounts of computing power to complete, therefore *miners* lend computing power to the network for a reward, typically small amounts of bitcoins. When a POW hash for the block is found the validated block is added to the blockchain if the other nodes accept the block. The process is then repeated [21]. Figure 5 shows a simplified illustration of how one transaction on the network is being added to a block, validated, broadcasted, accepted, and added to the blockchain.

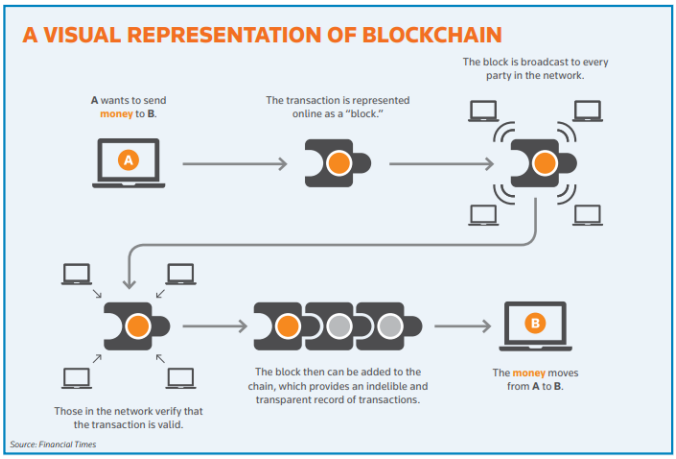

Fig. 5. **Visual presentation of the process of payments on a blockchain** Source: Thompson Reuters [22]

This system removes the need for an overseeing or *trusted* third-part, such as a bank. The data from transactions are accessible to the public and contains data like the receiver-, sender addresses, and amount, etc. These addresses do not have to be connected to any one person, and in many cases, this is where the privacy stems from. In the beginning Silk Road only accepted bitcoin for payments, which had almost complete market dominance, shown as orange in the graph below in figure 6. During the time in which the first iteration of

Silk Road was accessible on the dark web, bitcoin had nearly complete market domination in the cryptocurrency segment, as shown in figure 6.

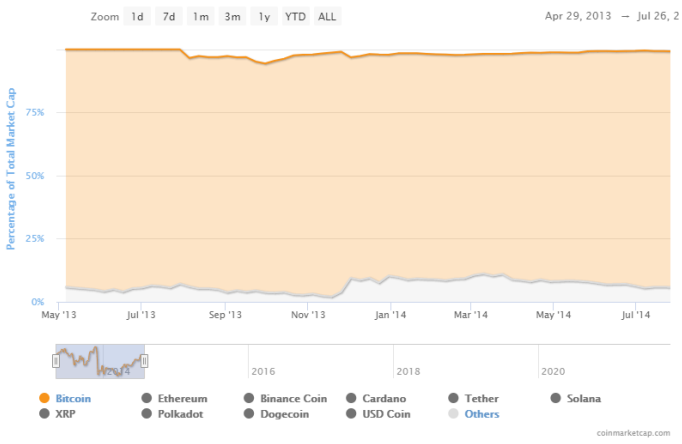

Fig. 6. **Graph presenting the Bitcoin's almost total marked-control in the period 2013 to 2014** Source: coinmarketcap.com

At the time of Silk Road 1, cryptocurrency exchanges lacked regulations regarding information kept on transfers from government-issued currencies, such as NOK, to cryptocurrencies. This meant that any person could purchase bitcoins on an online exchange, such as *Mt.Gox* or *Monero* with i.e. a gift card or PayPal transaction [20], [23]. That amount of bitcoins could from there be anonymously used as payment for illegal goods on Silk Road using their *escrow* system for securing deliveries.

The escrow mechanism could be used as a buffer account between the buyer and seller, instead of early finalization which was further described in the next section. The buyer will transfer the bitcoins to escrow and wait until the package is delivered before he finalized the purchase, thus providing a system of security for the buyer. Escrow also enabled the market operator to calculate their commission fees and was mandatory to use when conducting business on the website. Failure to follow this mandate would result in explosion [7].

C. Delivery of goods

In order to preserve the anonymity of the buyer and seller Silk Road recommended using a different delivery address from that of the buyer, thus creating a physical security buffer for the buyer. The more distinct the address was the safer for the buyer as it would be harder to link him/her to the delivery of the goods. Another normal approach was to have items delivered to a post box or someone else's house.

Once the seller shipped the item and marked it as sent on Silk Road, the delivery address was erased from all the site's records. After delivery, the buyer would finalize the purchase by telling Silk Road to release the funds held in escrow. The buyer could at the same time give the seller feedback, which enabled a mechanism similar to that of Amazon's star rating. This could in the future tell other buyers who the best-sellers were, as well as function as a thrust mechanism as an incentive for the seller to stay true and not scam their buyers. This final step referred to as finalizing was mandatory ensuring that the seller always gets paid for the service. If the buyer did not finalize the purchase within a given time, Silk Road automatically finalized the pending order. In addition to the feedback functionality, Silk Road had a mechanism for the sellers which allowed them to ask for an early finalization i.e., get feedback and payment before the buyer got the product. Sellers had to have been active for more than a month and have more than 35 successful transactions [7].

Nicolas C. found that the majority of the purchased items were shipped worldwide, despite the illegal nature of the item [7]. He discovered three reasons why the seller was not afraid of shipping across borders:

1) The use of early finalization meant that the sellers could get paid even if the shipment was stopped at the borders.
2) They sent small quantities which were harder to detect, in addition to using couriers thus making it harder to trace the package back to the seller.
3) The use of techniques to mitigate the risk of package inspection, like vacuuming sealing the drugs to hide the smell of the drugs, or having proper packaging to make the package look more professional

As a result, sellers were able to expand their operations with a relatively low personal risk.

VI. Discussion

From the results in section IV, it is evident that the main anti-forensics techniques utilized by Silk Road were a combination of the use of TOR and Bitcoin. Cryptocurrencies and TOR are indeed used for illicit activities, however, the reality is that the majority of both technologies are predominantly used for legal actions. Former *Central Intelligence Agency* (CIA) acting director Michael et al. conducted a study focusing on Bitcoin's use in illicit finance. They found that the use of bitcoin for money laundering and other illegal activities was relatively limited. They stated that "[I]llicit activity among all cryptocurrencies as a percent of total cryptocurrency activity from 2017 to 2020 was less than 1 percent", and that a mere 0.5% of the transaction volume of bitcoin was used for illicit financial activities [24].

This section further discusses how the identified anti-forensic techniques provided anonymity, how the anonymity could be broken, and how the techniques could be improved. The following subsections are in the same order as the findings were presented in section V.

A. Network Anonymity

In general, TOR provides the user with anonymity, but as previously mentioned, the service is not perfect and the anonymity can be broken. The security of the service is not stronger than its weakest link i.e., the human operator, implying that a user's mistake during use or implementation

most often is the reason for de-anonymization [25]. An example of this can be found in Norway where a student at a school sent a bomb threat to his school hoping to cancel the exams. The threat was sent via the TOR network to ensure his anonymity. However, he was foolish enough to send the threat while connected to one of the school's access points. When the police started the investigation they found that only one student had accessed the TOR service from the school at the time of the threat. As they were able to see who the student was via his login ID, they proceeded to arrest the student [26]. Thus, even though TOR can provide anonymity, users have to understand how it works to preserve the security the service provides. Below are techniques an investigator can use to counter the TOR-related anti-forensics techniques found in section IV, followed by a discussion on how the anti-forensic techniques can be improved.

1) TOR - De-anonymization: An investigator can employ various techniques to analyze anonymous communication networks. In general, there are two classes of attacks: single-end and end-to-end attacks [27].

To conduct a single-end attack the investigator has to control or monitor one of the exit nodes of the transaction. The goal is to compromise the communications security and privacy by either passively analyzing traffic pattern artifacts to infer information of what is happening at the application layer, or actively injecting data into the network traffic aiming to get the IP addresses of the users.

Single-end passive attacks focus on monitoring the traffic to deduce the accessed websites. This is accomplished by pre-collecting artifacts like network packet data i.e. fingerprints of how the traffic would look like if one accessed various websites [28]. Then, by comparing this collection of fingerprints to the monitored data, the investigator could identify what websites the users are accessing. With earlier versions of TOR, an investigator could try to determine the physical location of hidden services by injecting timing data in the log files of the client running the hidden service [29].

Single-end active attacks aim to perform *remote code execution* (RCE) at the victim's system by injecting malicious code into the network traffic. For this type of RCE attack, the goal is to bypass the encryption services, like TOR, and establish an unencrypted end-to-end connection with the host. After having established an unencrypted link the investigator can inject software that will be executed in the browser of the victim, bypassing the local proxy settings in the browser, and creating a direct connection to the investigator's system. Thus revealing the victim's IP address and potentially other artifacts. With various browser vulnerabilities, the investigator can in theory conduct further attacks to compromise the anonymity of the victim [27].

With end-to-end attacks, the goal is to correlate the network traffic between the end nodes and the server by controlling or monitoring the nodes at both ends of the communication.

End-to-end passive attacks focus on monitoring the traffic at both ends of the connection to correlate the outbound and inbound packets and identify or prove that a communication between two entities has taken place. With this attack, the investigators can look at timestamp artifacts combined with the number of sent and received packets in a given time interval to validate the communication [27].

End-to-end active attacks aim to modify the traffic between the targeted end nodes by injecting a packet sequence and monitoring both ends to prove that there is communication going between them. This type of attack can be conducted at different levels of the OSI model i.e. the network layer, protocol layer, and application layer. At the network layer, the investigator can implement a unique signal by exploiting timing features or packet sizes. At the protocol layer, the investigator could tamper with various protocol features to create a unique signal. An example of this would be to exploit the data integrity verification used between the hops in the network. With access to the entry node, the investigator can modify the contents of the ciphertext so that it is decrypted wrong at the receiving end and creates a decryption error that can be used as an artifact. Thus, indicating a relationship between the exit node and entry node. At the application layer, the investigator could simply inject certain content into the network traffic aiming to create a specific traffic pattern as a response and use that response to indicate the communication relationship [27].

With these attacks, investigators can try to identify and locate users and hidden services of the TOR network, given enough collected data and artifacts. Unfortunately, it is still difficult to pinpoint the exact location or identity as the hidden service or user might be using proxies to add more layers to their anonymity. Another approach is to take down the service altogether. This will be difficult as TOR has proven to be fairly resilient to attacks due to the decentralized design and academic support. Moreover, there is a moral issue weighing high collateral damage. This would mean that the agency has to take down every site run on TOR, which might not be beneficial to society. As mentioned earlier, TOR is mostly used for legitimate purposes like supporting oppressed individuals with means of communication. If an agency takes down the TOR network they will have to deal with a high collateral cost [7].

2) TOR - Anonymization: Investigators might try to de-anonymize the users of TOR during their forensic work, however, there are steps users can take to mitigate this effort. This paper has identified four main methods: human error, network layer, protocol layer, and application layer.

As aforementioned, the biggest weakness of TOR is its users. Kevin et al. discovered that both experts and non-experts show lacking knowledge of the TOR service which can lead to a breakage of the anonymity [25]. Their work shows that most users lack the proper understanding of how the technology works, and struggle to grasp the threat model for using TOR. A better design of the service could drastically improve the user's understanding of the service, like clearer stating the node paths and ownership to clearly state that it is a decentralized service. Further improvements like safe script execution and training and learning mechanisms can further improve the

user's knowledge, thus helping them stay anonymous.

At the network layer one can implement techniques for packet padding, introduce time delays, dummy packets, and traffic morphing, to obfuscate the data and make it harder for an investigator to analyze the data. By changing the length of packets, supplying wrong timestamps attacks like fingerprinting are less effective. Dummy packets and traffic morphing can be used to change the pattern of the transmitted data entirely making it near impossible to identify [27]. Similar techniques for dummy data and morphing can be applied at the protocol layer. A simple example can be to use SSH to implement packet padding and obfuscate data.

At the application layer techniques like HTTP pipelining can be used to modify the inbound and outbound traffics packet sizes. The signatures of the traffic can be changed by modifying the HTTP request data, as this is often used as a metric for traffic fingerprint monitoring. A third option aiming to cover the transmission data is to use a decoy website to create noise in the network. However, these techniques are limited to specific services running HTTP or similar protocols, while a deeper understanding of other applications is needed to apply obfuscation methods [27].

These techniques can be combined to better protect the anonymity of the TOR service. Yet, this might implicate even more performance deficits for the user.

B. Exchange Anonymity

In [24], Michael et al. state that:"[It] is easier for law enforcement to trace illicit activity using Bitcoin than it is to trace cross-border illegal activity using traditional banking transactions, and far easier than cash transactions". This statement was based on their findings of how expert investigators viewed and experienced the transparency of Bitcoin. Contradictory to traditional banking transactions where one can aim to hide transactions between parties, Bitcoin is open for everyone to see, as all transactions are stored on public ledgers. Since cryptocurrencies use a decentralized transparent design forensic data is easily available for investigators, and can be used to discover illicit transactions. Never before has there been an economical ecosystem with so much transaction data publicly available. This might implicate that criminals stay away from Bitcoin and other cryptocurrencies in the future as more advanced forensic techniques are developed and the governments start to regulate the space.

This subsection discusses the challenges of de-anonymizing the users of cryptocurrencies by focusing on bitcoin, and different obfuscation techniques the users can utilize to stay or become even more anonymous.

1) Bitcoin - De-anonymization: Cryptocurrencies like bitcoin provide pseudo-anonymity to its users [30]. Users obtain a unique identifier, a private key, connecting them to their transactions. These private keys are only accessible by the crypto exchanges where the transactions are made. The private key is a unique alphanumeric value generated for that user and is used when sending and receiving bitcoins, and thus also ends up on the blockchain [31]. Transactions have attributed an address of origin which also ends up on the ledger. Hence, all users can monitor a private key and see what addresses are connected to it to track what transactions that user has made. A common technique that is used by traders to analyze the market.

Despite the challenge of conducting forensics on bitcoin transactions, this pseudo-anonymity makes it easier for investigators as the user's public address can be traced back to the user's identity [32]. If a user's personal information like email address was attributed to the private key, everyone could be able to connect the transactions to the user. As Bitcoin has become less novel, more and more tools and methods like automatic clustering of Bitcoin addresses have been developed to stop the illegitimate use of the currency [33]–[35].

Common techniques for cryptocurrency forensics are based on blockchain-based transaction analysis and off-chain information. Blockchain-based information is often used for pattern analysis. The off-chain information is most often used to validate the findings, but can also be implemented in the pattern analysis to provide more accurate results [35]. The resulting patterns can be used by investigators to conduct better de-anonymizing analysis.

Sybil attacks, in regards to blockchains, are when an attacker runs several nodes in the blockchain network. These attacks are generally used to disrupt networks by blocking transactions or in the most extreme cases, if the attacker controls more than 50% of the nodes, take control of the network. They can also be used by investigators to monitor the transactions [36]. Not too dissimilar of a man-in-the-middle attack. This can in turn aid in the tracking of the expenditure of coins based on the timestamp mechanism enforced by Bitcoin. Using this timestamp feature investigators can break the pseudo-anonymity of the users and violate their privacy [37].

Investigators can use address clustering to make a one-to-many map from users to addresses and in doing so discover what users are connected to what addresses in the blockchain network. This is one of the most common ways of conducting high-level blockchain analysis where the investigators collect open-source information about the transactions to construct clusters. The effectiveness of this technique is due to the high reuse of addresses and merging of clusters. Here, the reuse of addresses means that an address is used for more than one transaction, which degrades the anonymity of the blockchain user. This reuse of addresses is also referred to as multi-input transactions, which occurs when a user performs a payment exceeding each of the available bitcoins in his wallet. A set of bitcoins are then selected from the wallet and sent as individual transactions. As Bitcoin does not allow for different users to participate in the same transactions, this artifact can be used to link various addresses to one owner [38]. The overlap in clusters indicates that new transactions are not getting new key pairs making it possible to link addresses to a single owner [39]. These two flaws are what make address clustering effective as a high-level tool.

Elli et al. used two artifacts, multi-input transactions, and

shadow addresses, to analyze the behavioral patterns of Bitcoin's users to de-anonymize them. Shadow addresses are used for collecting the change from the result of transactions. Based on shadow addresses investigators can differentiate two different transactions coming from a user since the public ledger will be updated with a never before seen address of that user. The researchers discovered that by using their methodology an investigator could construct a geographic view of the blockchains sub-network. Moreover, it can be used to reveal 40% of the profiles of Bitcoin users, even if the users ensure that they have a different address for each transaction [38].

Furthermore, J. Monaco shows in his research that one can identify long-time Bitcoin users by transaction behavior. He focused on the publicly available transaction artifacts: timing- and network features, of which he extracted random time-interval, hour of day, time of hour, time of day, coin flow, and input-output balance attributes. By using a Wald-Wolfowitz test to identify if two data sets stem from the same distribution, he was able to determine what addresses in the blockchain network belonged to what user. The findings indicate that longtime Bitcoin users can be tracked, despite implementing mechanisms for obfuscation [40].

2) Bitcoin - Anonymization: A bitcoin owner can use coin-mixing to increase his level of anonymity. Coin-mixing implies that owners group together in networks and starts to mix their coins with each other by continuously sending them around until they perform transactions [41]. A weakness found in this design is that the mixing server has access to the mapping of all the addresses. To improve upon this, Luke et al. implemented the use of a blind signature scheme with an append-only public log. With this solution, the authors claim the method to be: "[...] fully compatible with Bitcoin, forces mix to be accountable, preserves user anonymity even against a malicious mix, is resilient to denial of service attacks, and easily scales to many users" [42]. The name of the new implementation is *Blindcoin*.

Another technique for anonymization is the use of *decentralized anonymous payment* (DAP) schemes. Zero-cash is an example of how DAP can be implemented on top of Bitcoin or other altcoins to increase the user's anonymity by hiding the user's identities, transaction amounts, and their account balances [43].

A third novel technique is *Transaction Remote Release* (TRR), which is inspired by the TOR network. TRR uses nodes to encrypt and similarly forward transaction data as that of the TOR network. This technique has two goals. One is to render attacks like the aforementioned Sybil- and fake node attacks useless since it will be increasingly harder to link a user's address and transaction as both attributes are encrypted in the network. The other is to ensure the user's anonymity, even if the TOR network, which should be used as an underpinning, is disconnected. This is achieved by implementing transmission delays for the transactions so that an attacker cannot connect the time of the transaction to the address of the owner [44].

Lastly, technologies like the cryptocurrency Monero and storage wallet *dark wallet* incorporate aspects of the aforementioned techniques to further anonymize holdings and transactions [45]. Many dark web predecessors to the Silk Road, such as *AlphaBay*, have switched from accepting bitcoin to Monero based on the increased anonymity of the currency. Monero uses an *opaque blockchain* to hide transaction details, which is known to be a key information source for information in investigations [46].

The opaque blockchain is achieved using *stealth addresses* and *Ring Signatures* making it resistant to de-anonymization. Monero stealth addresses prevent outputs from being associated with the recipient's public address. This is accomplished by the use of one-time destination public keys. One-time public keys are only spendable by the recipient and only the recipient can detect their designated output on the blockchain. Since all outputs are unlinkable the privacy of the recipient is ensured.

On the input side of the transaction, the sender's privacy is protected with the use of ring signatures. A ring signature is a type of digital signature in which a group of possible signers are fused together to produce a distinctive signature that authorizes the transaction. This is analogous to the signing of a check from a joint bank account, but with the actual signer remaining unknown. The digital signature is made up of the actual signer combined with the non-signers to form a ring where all members are equal and valid. The actual signer is a one-time spend key that corresponds with an output being sent from the sender's wallet. The non-signers are passed transaction outputs pulled from the blockchain, which acts as decoys. These outputs together make up the input of a transaction. To a third party, all of the inputs appear equally likely to be the output being spent in the transaction. This feature helps the sender hide the origin of the transaction by making all inputs indistinguishable from each other.

Key images are used to prevent someone from spending the same output twice. A key image is a cryptographic key derived from an output being spent and is made part of every ring signature transaction. There can exist only one key image for each output on the blockchain. Yet due to its cryptographic properties, it is not possible to determine which output created which key image. A list of all key images is maintained on the blockchain, enabling miners to verify that no output is spent twice [47].

This enhances the anonymity and even makes it impossible for miners to determine who is transmitting or receiving the transactions or what the transactions contain. Cryptocurrencies like Monero hence have a huge use case on the dark web as it improves financial anonymity.

C. Delivery of goods

A general challenge in the fight against drugs is stopping the import. As the delivery model used by Silk Road abuses the regular post service it highlights a need for better detection and procedures regarding prosecuting the sellers or recipients.

As of today, the risk is too low of getting caught and the communication between government agencies is too slow.

As discussed in section IV, most shipments were international and across borders. For governments or law enforcement agencies to stop this flow of illegal goods, they can aim to attack the delivery model. Nicolas C. found that one method of attack would be to reinforce the controls at the post offices and border customs to prevent the illicit items to reach their destination.

He also found that most sellers did not worry about having the packages seized, as the sellers marked their packages as international shipping, as the risk of prosecution was low. This can be a result of improper communication between the agencies like customs, who are the ones with jurisdiction to inspect mail, and the *Drug Enforcement Agency* (DEA). As a result, if a package is seized by customs it is either destroyed or returned to the sender instead of reported to the DEA which might want to use the items as evidence in their cases [7].

Silk Road was meant to be an anonymous marketplace with few restrictions for its users. Built into the design of the site where the mechanism of *early finalization* as mentioned in section IV. Early finalization could only be used by seasoned sellers as it was not available for new users. A bit contradictory is the fact that the site discourages the use of this mechanism in general due to the potential abuse of trust. This raises the question of why the mechanism was implemented at all.

Rita Zajácz examined the site's failed attempt to create subcultural norms aiming to support the site's anonymity and trust, which can be one of the causes for such contradictions [13]. Moreover, it might be the result of how Ross Ulbricht's tried to implement his mixed libertarian ideals, aiming to give people their own choices and emphasizing the individual's right to non-interference, into built environments to create a freer digital economy. As Ramus et al. discuss in their paper, Ulbricht's seemed to have mixed political views and as many of the mechanisms of the site were updated after internal discussions on the site this might have resulted in less optimal functionality which in turn contradicted some of the ideals of the site trying to balance freedom and trust [48].

VII. Conclusion

This paper identified the use of the TOR network and services, and the cryptocurrency bitcoin as the main anti-forensics techniques employed to ensure network-, transaction-, and delivery-anonymity on the Silk Road dark web site, of which all utilizes the principle of decentralization. While TOR can be used to preserve the user's anonymity and Bitcoin provides pseudo-anonymity, there are some drawbacks. Mainly due to human error and vulnerabilities in the implementation of decentralized networks as well as the inherent transparency in cryptocurrencies. These weaknesses create opportunities for investigators to de-anonymize activity in connection with the Silk Road. The use of these services is mostly legitimate, hence investigators cannot prosecute and convict users solely based on them accessing TOR or making payments in bitcoin. Moreover, the transparency in cryptocurrencies might implicate that criminals stay away from bitcoin and other cryptocurrencies in the future as more advanced forensic techniques are developed and more government regulations are put in place.

Further work should therefore look into how more advanced forensic techniques can utilize the transparent nature of cryptocurrencies in general. This includes research on technologies like Monero and dark wallets aiming to improve privacy. There should also be continuous research on TOR and other decentralized networks to understand what forensic artifacts exist and how they can be utilized to identify criminals without disrupting the ethical and lawful use of the service.

References

[1] J. F. Kurose and K. W. Ross, *Computer Networking: A Top-Down Approach*. 80 Strand, London, UK: Pearson, 2013. ISBN: 9780132856201.

[2] A. Årnes, *Digital Forensics*. The Artium, Southern Gate, Chichester, West Sussex, PO19 8SQ, UK: John Wiley & Sons Ltd, 2018. ISBN: 9781119262381.

[3] T. T. P. Inc., "About tor browser." https://tb-manual.torproject.org/about/. [Accessed on: 23.10.2021].

[4] W. Lacson and B. Jones, "The 21st century darknet market: Lessons from the fall of silk road," *International Journal of Cyber Criminology (IJCC)*, pp. 40–61, 2016. DOI: 10.5281/zenodo.58521.

[5] J. Bartlett, *The Dark Net: Inside The Digital Underworld*. United States, Brooklyn, New York: Melville House, 2015. ISBN: 9781612194899.

[6] C. Goanta, "The private governance of identity on the silk road," *Frontiers in Blockchain*, vol. 3, p. 4, 2020. DOI: 10.3389/fbloc.2020.00004.

[7] N. Christin, "Traveling the silk road: A measurement analysis of a large anonymous online marketplace." https://www.andrew.cmu.edu/user/nicolasc/publications/TR-CMU-CyLab-12-018.pdf, 2012. [Accessed on: 01.11.2021].

[8] B. Storyville, "Silk road drugs death and the dark web documentary." Vimeo.com, August 2017. [Video recording]. Available: https://vimeo.com/230066610. [Accessed on: 12.11.2021].

[9] Wikipedia, "Pretty good privacy." https://en.wikipedia.org/wiki/Pretty_Good_Privacy, 11 2021. [Accessed on: 18.11.2021].

[10] Europol, "Europol's 20 most noteworthy operations." https://www.europol.europa.eu/about-europol/europol-20-years/europols-20-most-noteworthy-operations, 2019. [Accessed on: 12.11.2021].

[11] R. Price, "We spoke to the shady opportunist behind silk road 3.0." https://www.dailydot.com/debug/silk-road-3-blake-benthall/, 05 2021. [Accessed on: 12.11.2021].

[12] Trendmicro, "Dark web marketplace silk road 3.0 launched... again." https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/dark-web-marketplace-silk-road-3-0-launched-again, 05 2016. [Accessed on: 12.11.2021].

[13] R. Zajácz, "Silk road: The market beyond the reach of the state," *The Information Society*, vol. 33, no. 1, pp. 23–34, 2017. DOI: 10.1080/01972243.2016.1248612.

[14] L. M. Shekhtman, A. Sela, and S. Havlin, "Percolation framework reveals limits of privacy in conspiracy, dark web, and blockchain networks." https://arxiv.org/abs/2007.05466, 2020. [Accessed on: 13.10.2021].

[15] N. M. Roger Dingledine and P. Syverson, "Tor: The second-generation onion router." https://apps.dtic.mil/sti/pdfs/ADA465464.pdf, 2004. [Accessed on: 25.10.2021].

[16] T. M. Emin Çalışkan and A.-M. Osula, "Technical and legal overview of the tor anonymity network." https://www.ccdcoe.org/uploads/2018/10/TOR_Anonymity_Network.pdf, 2015. [Accessed on: 29.10.2021].

[17] M. Bishop, *Computer Security [Art and Science] Second Edition*. 80 Strand, London, UK: Pearson, 2019. ISBN: 978-0-321-71233-2.

[18] M. Nemec, M. Sys, P. Svenda, D. Klinec, and V. Matyas, "The return of coppersmith's attack: Practical factorization of widely used rsa moduli." https://crocs.fi.muni.cz/_media/public/papers/nemec_roca_ccs17_preprint.pdf, 2017. [Accessed on: 25.11.2021].

[19] S. Jeong, "The dread pirate's diary." https://www.forbes.com/sites/sarahjeong/2015/01/22/the-dread-pirates-diary/, 2015. [Accessed on: 25.11.2021].

[20] P. Bajpai, "Liquidity of bitcoin." https://www.investopedia.com/articles/investing/112914/liquidity-bitcoins.asp, 2021. [Accessed on: 22.10.2021].

[21] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system." https://bitcoin.org/bitcoin.pdf, 10 2008. [Accessed on: 15.11.2021].

[22] M. J.W., A. C. Rennock, and A. R. Butcher, "Blockchain technology and regulatory investigations." https://www.steptoe.com/images/content/1/7/v3/171269/LIT-FebMar18-Feature_Blockchain.pdf, 2018. [Accessed on: 15.11.2021].

[23] D. Adler, "Silk road: The dark side of cryptocurrency." https://news.law.fordham.edu/jcfl/2018/02/21/silk-road-the-dark-side-of-cryptocurrency/#_edn7, 2 2018. [Accessed on: 16.11.2021].

[24] M. Morell, J. Kirshner, and T. Schoenberger, "An analysis of bitcoin's use in illicit finance." https://cryptoforinnovation.org/resources/Analysis_of_Bitcoin_in_Illicit_Finance.pdf, 04 2021. [Accessed on: 08.11.2021].

[25] K. Gallagher, S. Patil, and N. Memon, "New me: Understanding expert and non-expert perceptions and usage of the tor anonymity network," in *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, (Santa Clara, CA), pp. 385–398, USENIX Association, 07 2017. ISBN: 978-1-931971-39-3.

[26] J.-P. Sandvik, "Lecture 9: Internet forensics." forelesning.gjovik.ntnu.no, 26.10.2021. [Video recording]. Available: http://forelesning.gjovik.ntnu.no/publish/1635264121-18d3c4b9ec51/screen.mp4. [Accessed on: 27.10.2021].

[27] M. Yang, J. Luo, Z. Ling, X. Fu, and W. Yu, "De-anonymizing and countermeasures in anonymous communication networks," *IEEE Communications Magazine*, vol. 53, no. 4, pp. 60–66, 2015. DOI: 10.1109/MCOM.2015.7081076.

[28] M. Yang, X. Gu, Z. Ling, C. Yin, and J. Luo, "An active de-anonymizing attack against tor web traffic," *Tsinghua Science and Technology*, vol. 22, no. 6, pp. 702–713, 2017. DOI: 10.23919/TST.2017.8195352.

[29] J. A. Elices, F. Pérez-González, and C. Troncoso, "Fingerprinting tor's hidden service log files using a timing channel," in *2011 IEEE International Workshop on Information Forensics and Security*, pp. 1–6, 2011. DOI: 10.1109/WIFS.2011.6123154.

[30] Q. ShenTu and J. Yu, "Research on anonymization and de-anonymization in the bitcoin system." https://arxiv.org/abs/1510.07782, 2015. [Accessed on: 05.11.2021].

[31] R. S. Shah, A. Bhatia, A. Gandhi, and S. Mathur, "Bitcoin data analytics: Scalable techniques for transaction clustering and embedding generation," 2021. DOI: 10.1109/COMSNETS51098.2021.9352922.

[32] J. Luu and E. J. Imwinkelried, "The challenge of bitcoin pseudo-anonymity to computer forensics." https://heinonline.org/HOL/LandingPage?handle=hein.journals/cmlwbl52&div=11&id=&page=, 2016. [Accessed on: 05.11.2021].

[33] S. Bistarelli, I. Mercanti, and F. Santini, "A suite of tools for the forensic analysis of bitcoin transactions: Preliminary report," in *Euro-Par 2018: Parallel Processing Workshops* (G. Mencagli, D. B. Heras, V. Cardellini, E. Casalicchio, E. Jeannot, F. Wolf, A. Salis, C. Schifanella, R. R. Manumachu, L. Ricci, M. Beccuti, L. Antonelli, J. D. Garcia Sanchez, and S. L. Scott, eds.), (Cham), pp. 329–341, Springer International Publishing, 2019. DOI: 10.1007/978-3-030-10549-5_26.

[34] H. Kuzuno and C. Karam, "Blockchain explorer: An analytical process and investigation environment for bitcoin," in *2017 APWG Symposium on Electronic Crime Research (eCrime)*, pp. 9–16, 2017. DOI: 10.1109/ECRIME.2017.7945049.

[35] D. Ermilov, M. Panov, and Y. Yanovich, "Automatic bitcoin address clustering," in *2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA)*, pp. 461–466, 2017. DOI: 10.1109/ICMLA.2017.0-118.

[36] J. R. Douceur, "The sybil attack," in *Peer-to-Peer Systems* (P. Druschel, F. Kaashoek, and A. Rowstron, eds.), (Berlin, Heidelberg), pp. 251–260, Springer Berlin Heidelberg, 2002. DOI: 10.1007/3-540-45748-8_24.

[37] F. Reid and M. Harrigan, "An analysis of anonymity in the bitcoin system." https://arxiv.org/abs/1107.4524, 2012. [Accessed on: 05.11.2021].

[38] E. Androulaki, G. O. Karame, M. Roeschlin, T. Scherer, and S. Capkun, "Evaluating user privacy in bitcoin," in *Financial Cryptography and Data Security* (A.-R. Sadeghi, ed.), (Berlin, Heidelberg), pp. 34–51, Springer Berlin Heidelberg, 2013. DOI: 10.1007/978-3-642-39884-1_4.

[39] M. Harrigan and C. Fretter, "The unreasonable effectiveness of address clustering," *2016 Intl IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld)*, Jul 2016. DOI: 10.1109/uic-atc-scalcom-cbdcom-iop-smartworld.2016.0071.

[40] V. Monaco, "Identifying bitcoin users by transaction behavior," 04 2015. DOI: 10.1117/12.2177039.

[41] J. Bonneau, A. Narayanan, A. Miller, J. Clark, J. A. Kroll, and E. W. Felten, "Mixcoin: Anonymity for bitcoin with accountable mixes," in *Financial Cryptography and Data Security* (N. Christin and R. Safavi-Naini, eds.), (Berlin, Heidelberg), pp. 486–504, Springer Berlin Heidelberg, 2014. DOI: 10.1007/978-3-662-45472-5_31.

[42] L. Valenta and B. Rowan, "Blindcoin: Blinded, accountable mixes for bitcoin," in *Financial Cryptography and Data Security* (M. Brenner, N. Christin, B. Johnson, and K. Rohloff, eds.), (Berlin, Heidelberg), pp. 112–126, Springer Berlin Heidelberg, 2015. DOI: 10.1007/978-3-662-48051-9_9.

[43] E. Ben-Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized anonymous payments from bitcoin." https://ia.cr/2014/349, 2014. [Accessed on: 03.10.2021].

[44] Q. ShenTu and J. Yu, "Transaction remote release (trr): A new anonymization technology for bitcoin." https://arxiv.org/pdf/1509.06160v1.pdf, 2015. [Accessed on: 05.11.2021].

[45] R. M. Nicolas T. Courtois, "Stealth address and key management techniques in blockchain systems." https://pdfs.semanticscholar.org/ba9b/fb3f7bed1aaadd008cff9351e2d98d76bb59.pdf, 2017. [Accessed on: 20.11.2021].

[46] A. Miller, M. Möser, K. Lee, and A. Narayanan, "An empirical analysis of linkability in the monero blockchain." http://arxiv.org/abs/1704.04299, 2017. [Accessed on: 25.11.2021].

[47] Monero, "Ring signature." https://www.getmonero.org/resources/moneropedia/ringsignatures.html, 2021. [Accessed on: 25.11.2021].

[48] R. Munksgaard and J. Demant, "Mixing politics and crime – the prevalence and decline of political discourse on the cryptomarket," *International Journal of Drug Policy*, vol. 35, pp. 77–83, 2016. DOI: 10.1016/j.drugpo.2016.04.021.