Alexander Hope Myhra

CRYPTOMARKETS: AN ACTOR-NETWORK PERSEPCTIVE ON DARK WEB BASED BLACK MARKETPLACES

A Qualitative Web Study on the Nature of Online Criminal Cryptomarkets on the Dark Web

Master's thesis in Sosiologi Master
Supervisor: Hendrik Storstein Spilker
Trondheim, October 2016

Norwegian University of Science and Technology
Faculty of Social and Educational Sciences
Department of Sociology and Political Science

NTNU
Norwegian University of
Science and Technology

Acknowledgements:

It is a strange sensation, that of finally delivering my master's thesis. I remember my second year at NTNU where the prospect of writing a master thesis seemed seemed like a time that would never come, that it seemed so far away. Yet in but the blink of an eye; here I am now, writing the preface of my thesis before delivery.

It is a moment of both joy, but also a small moment of sadness The joy of having finally completed my work, but also a sense of sadness to think that my time at NTNU now has come to an end, something it at times felt like it never would in my 5 years.

But those have been 5 good years that I do not regret, and I would like to give my thanks all my classmates who have been a great source of entertainment and made my experience here so much more, especially the other Sociology Master students from the 2015 batch! Also I want to thank the Department of Sociology and Political Science for its many great and knowledgeable teachers and lecturers who have continued to impress me throughout my time at NTNU.

And last but not least, I would like to thank my family for their generous support, and in particular my mother, for her great stubbornness is all the encouragement a student could ask for!

Abstract

The purpose of this qualitative study is to explore the challenge posed by the growth of so called 'cryptomarkets' on the dark web; sprawling black markets that evade the law and surveillance through the use of heavy encryption and untraceable cryptocurrencies, so as to create a better understanding of how cryptomarkets function in general, viewing them as unique networks. To do this, data was gathered from four major dark web cryptomarket websites and their forums, and data regarding the original Silk Road 1.0 cryptomarket was compiled. The following analysis and discussion lead to the understanding of cryptomarkets as sophisticated and technological networks whose existence is grounded in central elements of our modern society that explains why they are so difficult to defeat. This study is meant to add to the nascent discourse and literature on the subject of surrounding the security challenges posed by cryptomarkets, and help those seeking to counter them.

Table of Contents

Table of Figures

1. Introduction

Secret dark web based cryptomarkets pose a growing challenge for law enforcements across the globe. Vast networks of illegal traders, terrorists and criminals occupy the dark side of the web, or; put more precisely; the dark web (Chen, et al., 2008; Bradbury, 2014; Christin, 2014; Décary-Hétu & Giommoni, 2016; Martin J. , 2014). Now, sensationalism aside, what I am referring to are defined as cryptomarkets, online markets using multiple layers of encryption and crypto currencies to conceal themselves from the government, and include online black markets such as the Silk Road, Dream Market, Agora,

The central research question for this paper will be as follows.

"How are cryptomarkets formed, maintained and dissolved?"

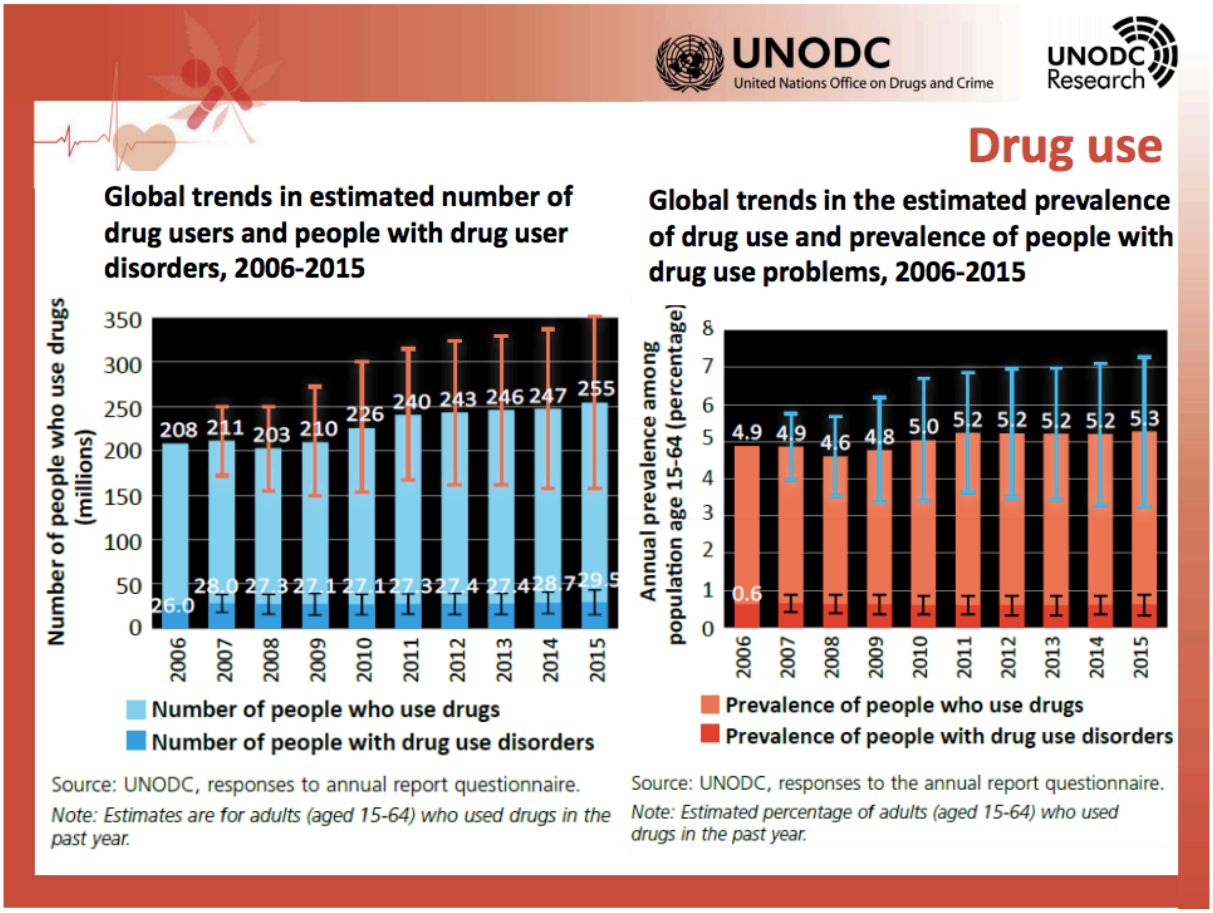
1.1 Framing the Issue

Our society is developing at an exponential rate, and in many simultaneous ways; technologically, culturally, socially. The world has changed radically since the innovations of the information revolution of the 1970s. Computers can be utilized to design ever more powerful computers, which in turn can be used to design even more powerful computers. As Castells (2010) noted in his book on the Rise of the Network Society: Any innovation system that innovates components of its own network will explode exponentially. We are witnessing a society that is ever more complex, ever spurred onwards by its technological advancement, taking new shapes and forms as it is. It is fair to say that we live in a society of interconnectedness, where physical space and time lose some of their original meaning, enabling for whole new of organization and cooperation to become possible. Entirely new arenas of play are created from out technological progress. The internet is perhaps one of the greatest symbols of our world's interconnectedness, a new media that connects billions of people from all over the world together in a digital society that ignores the boundaries laid by physical and geographical space. The benefits of this technology is available to every aspect of society, from business, learning, research, trade, and education. But while this

technological has the power to enhance elements of our existing society and transform it, this progress will also transform all elements of our society that it touches, both good and bad, and that includes criminality as well. Arriving at the backdrop of an increasingly complex world and technological society are a new generation of cyber criminals who transfer old practices such as drug trafficking and transfers the old drug trade into a new and more sophisticated digital format. While the online drug trade began almost as soon as the new technology and the internet was introduced, it was vulnerable on the surface web; existing currencies too controlled and regulated and the surface web unable to provide the true protection that the online drug market needed to grow to a significant. This would come to change. The change started as early as in 2008 once the possibilities presented by the dark web started to become first realized, culminating in the first major cryptomarket on the dark web in 2011, the Silk Road (Martin J. , 2014). The Silk Road's popularity experienced a significant growth, all up until the point in 2013 when the FBI shut down the site for good, arresting its secretive owner, Ross William Ulbricht; who was under the pseudonym of "Dread Pirate Roberts" (D.O.J., 2015). Until then, the Silk Road had at its registered peak an estimate of 900,000 estimate users, and during its two years generated sales of more than 80 USD in sales (Aldridge & Décary-Hétu, 2014; Dolliver, 2015; Flitter, 2013; Christin, 2014). For many people, the revelation of the Silk Road and the arrest of Ulbricht was their first wakeup call to the dark web, and even still it is a relatively new and often misunderstood phenomenon.

Attempts to slow stop the global drug trade has been met by negligible, and sometimes even opposite result (Wisotsky, 1986; Baum, 1996; Carpenter, 2003). In 2017, a report from UNODC shown below, the United Nations Office on Drugs and Crime, they highlighted how drugs are still a prevalent problem even in the modern day and age:

Figure 1. United Nations Office on Drug and Crime report on 2006-2015 drug use.



(UNODC, 2017)

Although 80 million USD may be a lot of money, I would like to put it context and remind the reader that the market value for cocaine alone in North America is estimated to be at 38 billion USD (UNODC, 2010). However, the drug market of the future is liable to change. Aldridge and Décary-Hétu (2014) suggested a trend or even paradigm shift in which the drug market goes digital, where cryptomarkets represent a evolutionary change of a criminal paradigm.

While individual markets may be taken down and defeated, such as Silk Road 1.0, Silk Road 2.0, BlackSheepMarket and so on, cryptomarkets as a general dark web phenomenon have proven resistant to government intervention and prone to reconstituting themselves after individuals are taken down. Décary-Hétu and Giommoni (2016) performed a study on the

effects of Operation Onymous, which was an international law enforcement operation targeting multiple different cryptomarkets and other hidden services operating on the TOR network, and resulted in 410 hidden services being taken down, 17 vendors and administrators arrested, and one million dollars worth of Bitcoins as well as 180,000 in cash, drugs and silver being seized. Yet they found that despite the large scope and extent of the operation, it had a negligible effect on online drug trafficking, wherein drug prices were not raised as a consequence of the operation (Décary-Hétu & Giommoni, 2016). This highlights the highly reflexive and adaptable nature of cryptomarkets on the dark web, where the loss of even major sites inflicts little perceptible damage. In a study done by Bahaskar, Linacre and Machin in 2017; the year of writing this paper; report the online drug trade having grown remarkably since 2011 (Bhaskar, Linacre, & Machin, 2017), while efforts attempting to stop drugs in general, such as the War on Drugs, have met with little effect or even the opposite of its original intent.

1.2 Past Literature on the Dark Web based Cryptomarkets

The Dark Web is a relatively new phenomenon, alongside the internet. Although it has existed ever since the creation of the internet itself, large scale and organized use of the dark web through encrypted browsers and anonymous networks such as TOR is a more recent phenomenon. This has naturally limited the amount of literature on the subject, but on the other hand; due to the significance of the Dark Web as a phenomenon, an unregulated blind-zone where criminals may operate relatively free from the law and the consequences such uncontained behavior might bring; much has still been written in the relative brief time that we have known about it. Granted, much of the scientific attention given to the Dark Web by researchers has often revolved around the spread and activity of dark web based terrorist and extremist groups whose activity has been located on the dark web. It is a problem addressed in a multitude of different studies: including Hsinchun Chen and colleagues case study on digital jihadism in 2008, Tianjun Fu's focused crawler dark web forum based study in 2010, and Gabriel Weimann's 2016 more recent article on the development of terrorism on the dark we, Going Dark: Terrorism on the Dark Web (Chen, et al., 2008; Fu, Abbasi, & Chen, 2010; Weimann, 2016). and they have been conducted with a multitude of different scientific methods and approaches, featuring data and text mining, networks analysis, networks typological analysis and data crawling. Because of the threat posed by terrorism in the age that we live in (U.S. Department of State, 2017), and the boundless opportunities and freedom

provided by the dark web, it may come as no surprise that such a significant proportion of resources be devoted to learning and understanding the nature of terrorists on the dark web as it is a matter of national security. But despite the attention put on terrorists on the dark web due the large threat they may pose, it does not mean that illegal dark web based black markets have been given much leeway. The early phenomenon of the Silk Road 1.0 that was closed down in 2013 opened the eyes for many to the world of large scale black markets existing on the dark web, and also helped garnered attention from researchers as well. Observations of the site and associated forums related to the infamous Dark Web online marketplace 'Silk Road' combined with anonymous interviews with its users has been conducted by Marie Claire Van Hout and Tim Bingham on the user experiences, providing us with a qualitative view into the workings of the dark web drug trade (Hout & Bingham, 2013). The Silk Road was eventually closed on October the third 2013 by the FBI, and the reaction of the online drug market was then observed by Joe Van Buskirk, Amanda Roxburg, Michael Farrel and Lucy Burns. In their research they found that the closing off the by-then largest online black market had a brief and confusing effect on the online criminal userbase, yet forums and discussions were noted to appear immediately in the wake of the event; discussing alternative sites and platforms, and it did not take long before sites such as 'the Black Market Reloaded' and 'Sheep Marketplace' were identified and saw a significant surge in users (Buskirk, Roxburgh, Farrell, & Burns, 2014). Even though the currency, Bitcoin, suffered a temporary drop in value immediately following the takedown, it has since recovered and is stronger now than before the closure (Buskirk, Roxburgh, Farrell, & Burns, 2014). The results of their article and monitoring has therefore helped point out the highly reflexive and malleable nature of the dark web, as the black marketplaces on the dark web employed by a large number of often unaffiliated and disparate individuals that will merge, move to or create a new site or marketplace if the current site is removed or taken down. In addition to the merely technical and practical issues of dealing with dark web based marketplaces, the dark web also comes with its own share of ethical and political issues, as noted by Eric Jardine (2015), wherein Eric argues that TOR and the Dark Web; while they may be considered a positive and valued asset to freedom and expression in more authoritarian societies; can be considered a liability in already free existing liberal democracies where their use takes a far more dark turn, such as towards the trafficking of illegal goods and services or spreading extremist and hateful views. TOR and the Dark Web are new technologies brought about by the exponential technological development that we experience all around us in our modern society, where laws, regulations and nation states may struggle to keep up with the significant development; and the risk of our

current laws and procedures lagging behind the social and digital reality of the world that we live is ever a possible threat. This is a dearth that I have also found within my own field of sociology. The internet has been around for a notably longer time than the dark web; at least to public use and is far more understood by the general public; and has been used both as a primary and secondary source of data by researchers within the discipline, but the Dark Web has mostly been untouched so far as I browsed through existing sociological literature across a variety of search engines, including ERIC; Google Scholar and Sociological Abstract. I can only speculate at this point that this dearth of literature on the dark web might be explained by how the dark web might be viewed as primarily a technological and security challenge for the computer and information sciences, coupled with it being a relatively new phenomenon, not really playing an active role for a significant number of private users until 2008 and really gaining its notoriety in 2013 with the closure and reveal of the large scale cryptomarket Silk Road 1.0. It is therefore the promise of scratching new ground within my discipline that drives this research, hoping to contribute something meaningful to something that I see as a very important subject in our increasingly digitalized world (Castells, 2010).

1.3 The Purpose Statement of this Study

The purpose of this internet based qualitative dark web study is to explore with the help of perspectives offered by Actor Network Theory the social phenomenon of criminal actors on so called 'cryptomarkets'; online black markets based on the dark web accessible through encrypted services such as TOR and using private, non-state owned cryptocurrencies such as BitCoin to avoid tracking and detection by law enforcement. Through examining the users, sites and related documents the goal is to ultimately create a better understanding of how such cryptomarkets function, an understanding that will allow us to better deal with them in the future. Below I will give a definition of cryptomarkets from which we can work.

> *"Cryptomarkets are defined as a type of website that employs advanced encryption to protect the anonymity of users."*
>
> (Martin, 2013, p. 351).

In our case, Martin's definition of cryptomarkets is a good starting point, but it could use some further work in our case. In our case, we are interested in cryptomarkets based on the Dark Web specifically, and in addition, they also use cryptocurrencies such as BitCoin which are more than merely just encryptions, but an entirely new currency altogether. So, let's modify the original definition a bit.

"Cryptomarkets are defined as a type of website based on the dark web that employs advanced encryption and cryptocurrencies to protect the anonymity of users."

This current definition for Cryptomarkets will suit our subject far more. Now, Cryptomarkets more narrowly define the type of dark web black based marketplaces that we are interested in for this paper, with the added benefits that it will be a lot easier to say "cryptomarkets" rather than "dark web based online black marketplaces", and so whenever I then refer to Cryptomarkets again in this paper, I will be referring to the new definition that I developed here. To further illuminate so that all my readers will be perfectly clear on what I mean with this; cryptomarkets refer specifically to dark web based markets, most well known of them being the Silk Road 1.0, but will also include sites such as a Dream Market, Tochska Market, Wall Street Market; the dark web kind; both new and old sites that fit the requirement.

1.4 The Structure of this Paper

This paper will be divided into seven different parts, with a bibliography at the end with reference to all related material and other authors referred to. This first chapter has been the introduction, where I introduced the reader to the topic, the research question, familiarized the reader with the literature on the subject and gave the purpose statement for this research. The second chapter will be the theory chapter, where I will familiarize the reader with Actor-Network Theory and its oddities and explain why I chose to use it, and then go on to explain and elaborate on the original research question. The third chapter will be a general explanation how the Dark Web and Cryptomarkets to give the reader a better understanding of the subject. The fourth chapter will be the method chapter, where I will explain and elaborate on methodological decisions, research approach, as well as reflect on my role as a researcher, qualitative considerations and possible ethical concerns surrounding my research.

The fifth part will be the discussion chapter, where I will go through the implications of my findings on the current situation with the Cryptomarkets and past research. The sixth chapter will be relatively short and it will be there that I present the findings of my research and give advice to future approaches and research.

2. Theory: Actor-Network Theory

2.1. Why Actor-Network Theory

When approaching this subject, Actor-Network Theory was far from the only network theory available to choose from. Indeed, ever since the first methodologies were developed in the 1930s; albeit to a not so-successful reception; there has been a growing number of new methodologies developed in the past years (Scott, 2000). These include Social Network Analysis, American Social Network Analysis, Castell's Networked Society, Post-Structuralist Internet Theory, as well as various different approaches from researchers such as Hardt & Negri and Deleuze & Guattari (Cavanagh, 2007). One of the chief objections to using ANT in general is its unwieldiness. The methodological challenge presented by employing constructionist methodologies is not the understated and ANT is a particularly high-investment method, yet in turn, as argued by Cavanagh (2007). That we understand the internet as a thing is something that ANT would describe as a network effect in itself. The primary question for instance in say, a question about the internet from an ANT perspective would be to question how the internet came to be a thing in the first place, or whatever else the object of the study may be did. ANT's capacity to allow us to disintegrate the object and rendering it ontologically strange can give a purchase for a deeper analytical insight into what the object actually is (Cavanagh, 2007; Krieger & Belliger, 2014), which is why I see the theory as a suitable pick for the task.

2.2 Actor Network Theory

Actor Network Theory; or 'ANT' for short, sometimes known as the 'sociology of translation'; is an increasingly influential method has been rooted in the studies of science society and technology (Dankert, 2012; Callon M. , 1984). As a method for in-depth research; and despite its heavy sociological background; ANT has been used in studies related to

international relations and the *political sciences* as well (Dankert, 2012). Although ANT carries the word 'theory' in its name, it can be looked at just as much as a method for doing research (Dankert, 2012). Actor Network Theory, in short, can generally be defined as a research method and/or theory where the focus is laid on the connections between both human and non-human entities, wherein it describes how these connections sometimes lead to the creation of new entities that do not necessarily practice the total sum of characteristics of the original constituent entities that made it up (Dankert, 2012; Spöhrer, 2016). The central and methodological concept of ANT is to treat the distinction between the "social", "nature" and "technology" not as explanans, but as explanandum (Latour, 2007). Because of this, the premise of every actor-network theory is to avoid any explanation of nature via social factors as well as any explanation of society via natural or technological factors; instead, concepts such as nature, technology and society need to be understood as the co-constitutive result of networking of heterogeneous entities and cannot be reduced or at least solely attributed to one kind of these factors alone. An example of this can be the gunman that was made by Latour, where it is stated that a man and a gun can form a new entity when the two of them are connected to a third entity; the gunman. In spite of what may have been argued by the pro-American gun lobby, man cannot shoot another man by himself. Yet in turn, it cannot neither be said that that gun is the cause of all problems. Guns that shoot someone all by themselves are quite uncommon; it is here that ANT wants its adherent researchers to focus on the connection that brings the man and the gun together, and thus creates this third entity, the gunman; which is different from both man and gun in in that the gunman can shoot someone, whereas the man and the gun cannot (Dankert, 2012). This example, as it was presented by Latour, also shows how ANT research can come up with unexpected conclusions. In Latour's example, we can conclude that war is caused neither by men or by guns, but the connection between the two entities that we have to blame for all the cruel incidents that happen with it every day (Dankert, 2012). This focus on connections shows how ANT is a *constructivist* theory. Even though the word of '*actor*' may suggest that the method is about networks of people, this is not the case. As we have seen from the example of the gunman as presented previously, an actor can also be non-human (Dankert, 2012). This is where a new term associated with Actor Network Theory comes into play, that of the '*actant*', a central term in ANT that is used to describe ANT's unique view of both human and non-human as valid actors. During fieldwork, connections between humans and non-humans can be traced during the research, and only traceable connection from the empirical data will be part of the descriptions that is made by the ANT researcher. This description then reveals all the

connections that eventually lead to the creation of a certain entity, such as the third entity from the earlier example from Latour that was the gunman (Dankert, 2012; Latour, 2007). ANT also seeks to reveal how connections were established in the first place, something that can only revealed through fieldwork because the exact way connections are established can vary from instance to instance (Dankert, 2012). For ANT, *existence* is first, *essence* is second. In Actor Network Theory with our example of the gunman, the gunman only existed after the constituent elements were connected, and therefore ANT does not search for essences, but rather for the connecting and reconnecting of different entities that eventually shape and reshape the essence of a certain entity or phenomenon (Dankert, 2012; Callon, 1984). In order for us to fully grasp how this really works also requires us to understand the underlying concept of truth of Actor Network Theory in general. In philosophy there exists a division between modernist and postmodernist thinking with regards to the definition of truth; yet Actor Network Theory rejects both of these camps (Dankert, 2012). For ANT's understanding of truth, truth should be understood as a state of affairs that under no circumstances cannot be denied in a practical sense (Dankert, 2012; Latour, 2007; Cavanagh, 2007). To give an example of this, in western societies, a statement that people don't need houses to exist would therefore be regarded as not true. For ANT, truth does exist, yet it can also change over time; not being fixed (Dankert, 2012). Essence can change, which means that when we focus on ANT, we focus on the conception of truth. It is merely logical that ANT does not want to focus on truth or essences themselves, rather, it should be the forces that shape or reshape the true essences that the researcher discovers when doing their fieldwork (Dankert, 2012). To give give an example in a contrast between Actor-Network Theory and Social Network Theory: while Social Network Theory begins by trying to understand the forms and variety of social structure, ANT's approach would be an investigation the nature of power in society, the way actions, beliefs and opinions are formed and developed. For ANT, a central starting position is a critique of traditional understandings of power within sociology. Thus, for in Actor-Network Theory, power becomes an explanatory variable, and therefore when we seek to understand how things come to be, we will seek out the source of the social power which has enabled this to occur. In an example given by Cavanagh, if we were to say explain Microsoft's dominance as a software supplier, we could do so in reference to its ability to control and direct the world market for software, but for ANT, this is unacceptable for ANT as power cannot be the cause of power, for that would be a circular argument. Instead, from ANT's perspective, we must seek to understand how power is developed in the present, because in its perspective, power, social order and society are continuously being developed

(Cavanagh, 2007). In addition, Michel Callon's introduced three ANT principles; Agnosticism, generalized symmetry and free association. These demand the researcher be impartial towards any scientific or technological arguments used by the actors when they should speak about themselves or their environment. And because this is ANT, it also applies animals, technical objects, discourses, media and any living and inanimate material or ideational entity in the research. The research must abandon all a priori distinctions between natural and social event, and reject the hypothesis of a definite boundary which separates the two.

Within ANT there exists some basic principles and terms associated with it, that are necessary to clarify in order to understand Actor Network Theory and use it to any meaningful extent, which I will summaries below.

2.2.1 Ant Networks and Group Formation

Network formation is a central aspect of Actor-Network Theory. When a network is fully formed and functional, the fact that it is a network can easily be completely missed.

> *All phenomena are the effect of the product of heterogeneous networks. But in practice we do not cope with endless network ramification. Indeed much of the time we are not in a position to detect network complexities. So what is happening? The answer is that if a network acts as a single block, then it disappears to be replaced by the action itself and the seemingly simple author of that action.*

(Law, 1992, p. 5)

When a network is fully formed; or so to say *naturalized* or *punctualized* as it is often referred to in Actor-Network Theory; it finally disappears from view. To give an example of how networks work from say research in housing, the focus is often on groups, that being for example possibly the departments, the homeowners, or the housing associations, and, because this is ANT, even an entity like a house could be regarded as a group as well. These are all groups of both human and non human entities, such as employees, building materials and

computers as well (Dankert, 2012). In adherence with constructivism, within the focus of Actor Network Theory, these groups are often deconstructed in order to see what is going on inside of them, and thus, it becomes clear that every single entity is a group of entities. For ANT, the point is that groups are not stable, in that they can be remade over and over again (Dankert, 2012). In fact, this continual remaking, or renewal, of the group and entities are necessary for their continued existence, because if workers stop going to work anymore, then the department does not exist anymore, and when the walls of a house falls down, then the house does not exist anymore (Dankert, 2012). This is why networks are sometimes said to be '*performative*' within Actor Network Theory, and that is because they have to be constantly acted upon and renewed, lest the networks cease to exist, for they are not stable, unending things, but are made in the moment, and disappear when discontinued (Latour, 2007). The networks of Latour's Actor-network theory is in this sense similar American communicative networks, in that they are temporally situated rather than eternal things. Networks are constantly activated, deactivated, dynamically created and re-created.

However, in order to create a functional network, proper enrollment of the different actants is necessary, often involving a process of transformation of the various parts of the network so that they may work together in unity, where various parts are locked into certain roles (Cavanagh, 2007). The process of locking parts in is referred to as 'interessement', the process by which the actors are enrolled into the network.

> *Each entity enlisted by the problematization [the original definition of the situation] can submit to being integrated into the initial plan, or inversely, refuse the transaction by defining its identity, its goals, projects, orientations, motivations or interests in another manner … Interressement is the group of action by which an entity attempts to impose and stabilize the identify of the other actors.*
>
> (Callon, 1986, p. 208)

The process of forming a network, the identity of the elements from which the network is comprised is subservient to the problematization, the overriding definition of the situation (Latour, 2007). To again contrast with Social Network Theory, when a network is formed, its elements are not stable nodes and dynamics links, as in social network theory, but are dynamically defined the network, and what emerges then is a network that behaves as a thing.

It serves to be said however that in Actor-Network Theory, networks function by exclusion and can be defined as particular rather than universal. What is meant with the former, that ANT networks are working by exclusion; is that in principle they are exclusionary so far as the constitution of a network depends on differentiating those elements which are part part of on network from one another. As Callon (1986) would go on to explain, the process of interessement is the process of defining the identify of the enrolled participants in such a way as to build devices which attach the participant to your group but detach and isolate him/her/it from other groups who would seek to define its identity otherwise and in oppositional terms.

2.2.2 Actants with agency.

For ant, the social is nothing other than patterned networks of heterogeneous materials (Law, Notes on the theory of the ator-network: Ordering, strategy and heterogeneity, 1992). Human social relations rarely take the form of the following:

> *Interaction between unmediated human bodies [therefore] … If human beings form a social network it is not because they interact with other human beings. It is because they interact with human beings and endless other materials too. And, just as human beings… prefer to interact in certain ways rather than others – so too do the other materials that make up the heterogeneous networks of the social.*
>
> (Law, 1992, p. 3)

Actors form groups that ANT calls actor-networks. However, although it lies in its name, ANT does not use the word ‘actor’ in general because of the aforementioned reasons, preferring to use the term ‘actants’ instead. An actant is that which accomplishes: or undergoes: an act (Dankert, 2012). Actants differ from actors because they can be humans so well as animals, objects or even concepts; the commonality being that they all can accomplish or undergo an act (Dankert, 2012). There can be huge differences between actants, and in ANT, actors can have the power to change other actors; a power which is referred to as ‘*agency*’ (Dankert, 2012). When we act we always act with others, and it is during these interactions that we change other actants, whilst at the same time, we are being changed by other actants. This can include human so well as non human actors, as some people simply

have to watch whenever a TV screen should be turned on nearby, a crashing computer can make someone truly desperate. And people influencing objects can take the example of people turning a television on or off, or me influencing this computer when typing in this paper. At the core, objects and non-human actants may structure social relations. For example in a when it comes to a phone call, the call and the conversation on it is structured by the technology as much as by the two parties on the either end of the conversation.

2.2.3 Difference between objects and things & Radical Relationality

Because ANT does not make any analytical distinctions between humans and non-human actors, it is sometimes regarded as weird or faulty by critics; a point sometimes raised by critics of ANT, yet this often stems from a faulty view of ANT in general, because whilst there is no analytical distinction, ANT does not neglect the potential differences between human and non-human entities, even though they do not have any a priori relevance for ANT based studies (Dankert, 2012). To many people, an object might be viewed as a stable thing, such as a chair or rock, but the term itself, 'things', is abstract, for it can also include something that is not as stable in the traditional definition (Dankert, 2012). In the perspective of ANT, 'objects' are things that are the temporary result of a set of multiple connections, and as long as these connections are held and not severed, the object has the same essence. One of the core commitments which distinguish ANT from earlier views of networks is what is called '*radical relationality*', the principle that there is no necessary a priori significance or relevance attached to a given object, person or idea. This notion was touched upon in our previous discussion on Actants, as in ANT, there is no necessary difference between the social and the natural. The implications of this equality on networks can be seen in Callon (1984) and his analysis of experiments performed at St Brieuc Bay, where a group of researchers sought to establish different methods of clam fishing in order to solve the problem of dwindling effects on the network created by the researchers, fishermen, and the clams, upon whom the livelihood of the fishermen depended, and whose behavior is the subject of the studies performed by the researchers (Cavanagh, 2007).

2.2.4 Translation and Transformation

Interaction is essential between actants in order to create and hold any connections between them, and in order to establish the connections in the first place, the actants must be displaced and transformed so that they may fit into an *actant-network* (Dankert, 2012). The work that is

necessary to displace and transform is then called *'translation'*, and in ANT, translation is all of the intrigues, negotiations, acts of persuasion, violence and calculations through with an actant is changed (Dankert, 2012). Should actants for instance not have been translated, or in alternate case; not translated themselves; they are then not a part of the actant-network (Dankert, 2012). Going back to our discussion about housing; when implementing housing management plans, thorough translation connections have to me made between the original visions of the alderman and the director that is working for the housing association, so well as connections between the rule of law and the floor plan (Dankert, 2012). When translation is successful, the actants will work together in order to change the actor-network from something that was originally just the plans for a house of stone, and ultimately into an actual house of stone (Dankert, 2012)). On the other end, if actants are not translated; such as when they are displaced and transformed; the actor-network cannot be established, or, in other words; if all the actants stick to their original characteristics they will not be able to connect to each other in such a way that a new actant-network with different characteristics is created (Dankert, 2012). Thus in ANT, change can be presented in many forms, such as if an architect changes his drawings, he comes a different architect; or if the housing association agrees to a suggestion of the architect, that housing association in question has become a different constituents. Michel Callon (1984) identified four so-called 'moments of translation' when exploring the scientific and economic controversy around the decline in the population of scallops in St. Brieuc Bay. The first stage was Problematization, which involves the the actor seeking to make themselves indispensable to the rest of the network. The second moment was called Interessement, in which the actor sought to lock the other actors in the roles of the network that had been proposed for them The third moment was called Enrollment, and involved a set of strategies in which the actor sought to define and interrelate the various other roles now taken up by the others. And the fourth moment was called Mobilization of allies, which involved a set of methods used by the actor, wherein the actor seeks to mobilize and set their allies into action whilst ensuring their internal cohesion and seeking to prevent backstabbing (Callon M. , 1984). Alternatively; and building from Callon's initial work; Rodger, Moore and Newsome (2009) identified six phases of translation. In the problemisation phase, the focal actor identifies the nature of a problem and identifies both human and nonhuman actors (Law, 1986). To be effective, the actor must define the problem in a way that the identified actors would find compelling (Woods, 1997). The next phase is called the Obligatory Passage Point, or OPP. It is the phase in which the actor defines the non-negotiable aspects of the idea, vision or approach that they wish to to embrace in

resolving the problem. The third phase is called the interessement. It is the phase in which the actor tries to convince them to them that it is their; that being the focal actor's; vision or idea is the better way forward (Kitchen, 2000). It is also in this phase of interessement that is likely to reveal any potential resistance, whether it is expected or not. In the fourth phase, the enrollment of actors occurs. Enrolment occurs when potential participants embrace and adopt and enroll to help achieve the mission and OPP of a principal actor. In this phase, the persuaded actors communicate and negotiate with the principal actor about what they could contribute towards the achieve of the of the obligatory passage point vision or purpose. In this, the scope, nature, content and duration of collaborations are discussed and the potential outcomes are communicated. In the fifth phase, the mobilization of alliances and networks occurs. Typically, this phase marks the beginning of the execution of actions that were negotiated in phase four, which was the enrollment of actors. The sixth phase is is called black Boxing, and it is during this phase that the network institutionalizes practices and actions that have become essential to its identity and performance of the network (Fountain, 1999).

2.2.5 Immutable Mobiles.

One may view interaction much like a flow, that flows from one actor-network to another actor-network, and in ANT-driven research, the goal is to track these flows (Dankert, 2012). For something to flow from one actant-network to another actant-network in requires that it be put in form first, and this can be for example information (Dankert, 2012). So if we want to for instance to have the flow of information from the working researcher's desk and on to the desk of the management team that is in charge of the vital decision making, it is necessary that we first put the information in a form that can be understood by the managers that will be receiving the information; an 'immutable mobile', which could in this case be a research report (Dankert, 2012).

After the research question has been set, and ANT has been picked to be the research method, the first step from there on out is going to be choosing a starting point; that is, to choose the actant from where the research departs (Dankert, 2012). Whilst there exist few common rules, theories and other presumptions are best avoided in the early stages of the research in order for the widest amount of involved entities can be explored and considered during an ANT research (Dankert, 2012). An example of such a starting actant could be when researching the

implementation of a policy, the document containing the policy in question could be such an actant; or, for the purposes of this paper, the Dark Web; or perhaps more specifically, one of the black market websites; or cryptomarkets as well call them in this paper; could be our actant. Starting from the original actant, the researcher would begin to first explore and unravel it, so well as both the human and non-human actants related to the original actant((Dankert, 2012). This exploration can be done through qualitative data such as interviews, document analysis, diary keeping and observation.

ANT based research has three requirements; first, it should be acknowledged that ANT is a holistic approach without boundaries, thus context as such does not exist; secondly, that all actants that leaves traces should be regarded in the same way, such as how new regulations from the central government that affect a building project could be analyzed in just the same way as a group of tenants that have influence on a building project; and thirdly, during fieldwork an emphasis must be made on connections, as in it should be made clear in just what way the regulation from the central government connects to a specific building project, so well as what the effect of this connection is (Dankert, 2012).

After the fieldwork has been completed, a new phase will start, yet which data that will remain useful to the research depends on the research in question (Dankert, 2012). If the goal of the researcher is to tell a story, then almost all of the gathered data may be useful and there may be no concluding article in the end, yet if the goal was to create a kind of model or to learn something from the research, or even make recommendations, not all the that will be useful.

There are a number of reasons why I choose to use Actor-Network Theory in this case. The main reason for choosing Actor-Network Theory as the main theoretical approach in this study was because of its emphasis on the importance of non-human actors as significant ‘actors’, or rather, ‘actants’. It is indeed a non-human actant will be one of the largest objects of focus in this paper, that being the dark web itself, and how it affects and shapes the behavior of other human actants, that being criminals in this case. The dark web may have no will or inherent prerogative in and of itself, indeed it is the amalgamation of numerous human advances within the information and computer sciences, a veritable platform of communication that is but a sub-section on an even larger platform. Yet its existence is enough to present new opportunities to human actors who come into contact with it, opportunities and paths that can reshape the old social dynamic of actors, possessing a powerful transformative effect on its users that can change old rules on conduct. In addition to

this, the world wide web, or more specifically, the dark part of the world wide web cannot be understood in isolation. It is an interactive platform that is the continues product of its users, and grows and changes only through use. Neither the internet user or the internet in and of itself mean anything without the other, and this is an aspect that ANT concerns itself with greatly, wherein networks are performative; and the various actants that make up the network, whether human or otherwise; have an ability to effect each others. This study is going to have a noticeable technological theme going through it, even if I will not go so deep into the minute, technical details of the web nor the esoteric intricacies of its unique design and operation. Because of its expanded view on actors and background in the lab and technology studies, I have therefore chosen ANT to serve as the primary theoretical approach.

2.2 Elaboration on Research Question & Musings on the Use of Theory in a Qualitative Study

Although the inductive and deductive approach to data analysis may be commonly associated with a Qualitative or Quantitative design respectively, there exists no strict line limiting neither of them to either approaches, as they can both have a place in Qualitative Design (Bryman, 2012). Qualitative researchers build their patterns, categories and themes from the bottom up by organizing the data into increasingly more abstract units of information. This inductive process illustrates working back and forth between the themes and the database until the researchers have established a comprehensive set of themes (Creswell, 2014). Then deductively, the researcher looks back at their data from the themes to determine if more evidence can support each theme and whether they need to gather additional information (Creswell, 2014). Thus, while the process begins inductively, deductive thinking also plays an important role as the analysis moves forward (Creswell, 2014). Thus, when it comes to Qualitative Research Designs, theory can function much like that of a lens through which the researcher may view the data material and make sense of it (Bryman, 2012). Yet, the connection and flow between empirical data and the given theory is not necessarily a straightforward process, and increasing levels of generalization will often mean that greater levels of abstraction of the data is necessary on the researcher's part in order for links to be made between the empirical data and theoretical concepts and models. In this respect, it is important to note that Actor-Network Theory is a very general type of theory as well as methodology that can be applied to a very large number of different problems and research

questions across a number of different disciplines and fields, including medicine, sociology, political science.

The central research question of this paper is as follows:

"How are cryptomarkets formed, maintained and dissolved?"

With this research question, we assume Actor-Network Theory's definition of networks. This means that networks are to be understood as constantly performative, they are not permanent but must be constantly remade lest they dissolve, and they are made up of both human and non-human actors called actants, wherein we do not limit ourselves to just human actors, but can also include objects and things as well. Therefore, the network that we are seeking to explore consists of both non-human and human actors that each can play a significant role. New technology could for instance occupy the role of one such *actant*. We do not look for permanent or universal networks and structure, but we will seek to explore the specifics of the problem at hand.

We are not interested in particular actants, because in actor network theory, actants gain their meaning in relation to the networks they are connected to. Actants not connected to the network are therefore irrelevant, and the power of individual actants will be understood only in relation to one another.

3. The Dark Web

3.1 The Dark Web

To many, the Dark Web may be a nebulous term shrouded in confusion, rumors and misinformation, often used interchangeably with Darknet or Deep Web. Although I will not give a complete breakdown of the Dark Web, mainly due to the fact that the dark web is a subject large enough to span multiple book series; let alone a master thesis; I will attempt to give the reader a cursory introduction to the basics of Dark Web, its relation to the Internet,

Deep Web, its special traits and quirks, and try to dispel some of the most common misconceptions about it. First off, when we are referring to the Dark Web, we should recognize it to be a part of the World Wide Web, also known as the Internet, which in turn has three different layers, with the *Surface Web* on top, the larger *Deep Web* below, and the *Dark Web* below the deep web once again (Chen, 2012; Bradbury, 2014). Below is a visual illustration of the layering of the three different webs.

Figure 2. Visual Illustration of the Dark Web in relation to the World Wide Web.

The Surface Web is the part of the internet that you and me use for 'normal' searches and browsing, including going pages such as Google, Yahoo, Dagbladet, Wikipedia, It's Learning and other similar pages that are readily available through common search engines on the surface web (Chen, 2012; Bradbury, 2014). The second layer, known as the Deep Web, is the largest and most expansive part of the world wide web (Chen, 2012). The deep web, like the dark web, is not discoverable by means of standards search engines such as google, and can

include password protected or dynamic pages, encrypted networks, webmail pages, registration-required web forums, and pages behind paywalls (Chen, 2012). If you use an online banking account, your password-protected bits will be on the deep web (Chen, 2012). The deep web is by far the largest of the three layers, and also includes the dark web, which is the hidden layer underneath. The dark web, in turn, is the lowest and most secretive layer of the three.

The dark web is generally accessed through special router, an example being a popular and heavily encrypted dark web browser known as Tor. Tor, originally an acronym for The Onion Router, is an anonymity network that has been designed to keep your identity and location hidden and secured behind layers of encryption, and is primarily used to browse and navigate the dark web (Bradbury, 2014). Almost all sites on the Dark Web hide their true identity using the TOR encryption tool, which has the powerful ability to hide your identity so well as internet activity, allowing you to use it to confuse your location through bouncing your IP address through several layers of encryption, creating the technical illusion of appearing at a different location and with the different IP address than what you in truth are (Chen, 2012). This is one of the reasons why it can be hard to track users across the dark web, and why is often used by individuals pursuing ends not sanctioned by most government laws, such as illicit drug trafficking, illegal weapon sales, proliferation of weapon and bomb schematics and recipes, organizing terrorism and jihadist activities, the sale of humans, so well as human body parts and flesh (Chen, 2012). Granted, not all users of the dark web use it for nefarious purposes, as the dark web may also provide citizens of strict, totalitarian or oppressive regimes the ability come together, interact with the world and circumvent government sanctions and restrictions (Chen, 2012; Bradbury, 2014). Yet despite of the technological complexity behind the networks and the seemingly endless possibilities of the dark web, accessing the dark web, from a technological perspective, is relatively easy, requiring the simple installation of Tor in a single download and installation procedure, where the user can then type in the address of whichever web page that they wish to visit. TOR will encrypt the users IP address, and then bounce that encryption through a network of routers so that the users browsing is virtually untraceable (Bradbury, 2014; Christin, 2014). For a time, this was a challenge in that the dark web did not have a good search engine such as Google that is readily available on the surface web, and so users wishing access certain sites had to gather the links and information on the surface web or through contacts before they would be able to find them on the dark web by directly typing in the link (Bradbury, 2014). This is something

that is slowly changing however with the continued developed of search engines such as DuckDuckGo, Torch and Ahmia Deep Web Search Engine that can be used on the dark web. However, these search engines are far from perfect, and so bringing pre known links to the sites that you wish to visit while on the dark web is still the par for the course. Using pre-existing links comes with its own dangers however, as many of them are what's known as phishing links (Stockley, 2015; Bradbury, 2014; Ramzan, 2010)

3.2 Cryptomarkets

As I have just explained the dark web in general detail, I will use this sub chapter to go into further details on the cryptomarkets themselves, and covering what actually makes them cryptomarkets in the first place, unique features and elements with the websites, as well as payment and deliver methods used.

3.2.1 The Cryptomarkets themselves.

In the first chapter; building on Martin's (2013) earlier definition; we defined Cryptomarkets for the purpose of our study as the following:

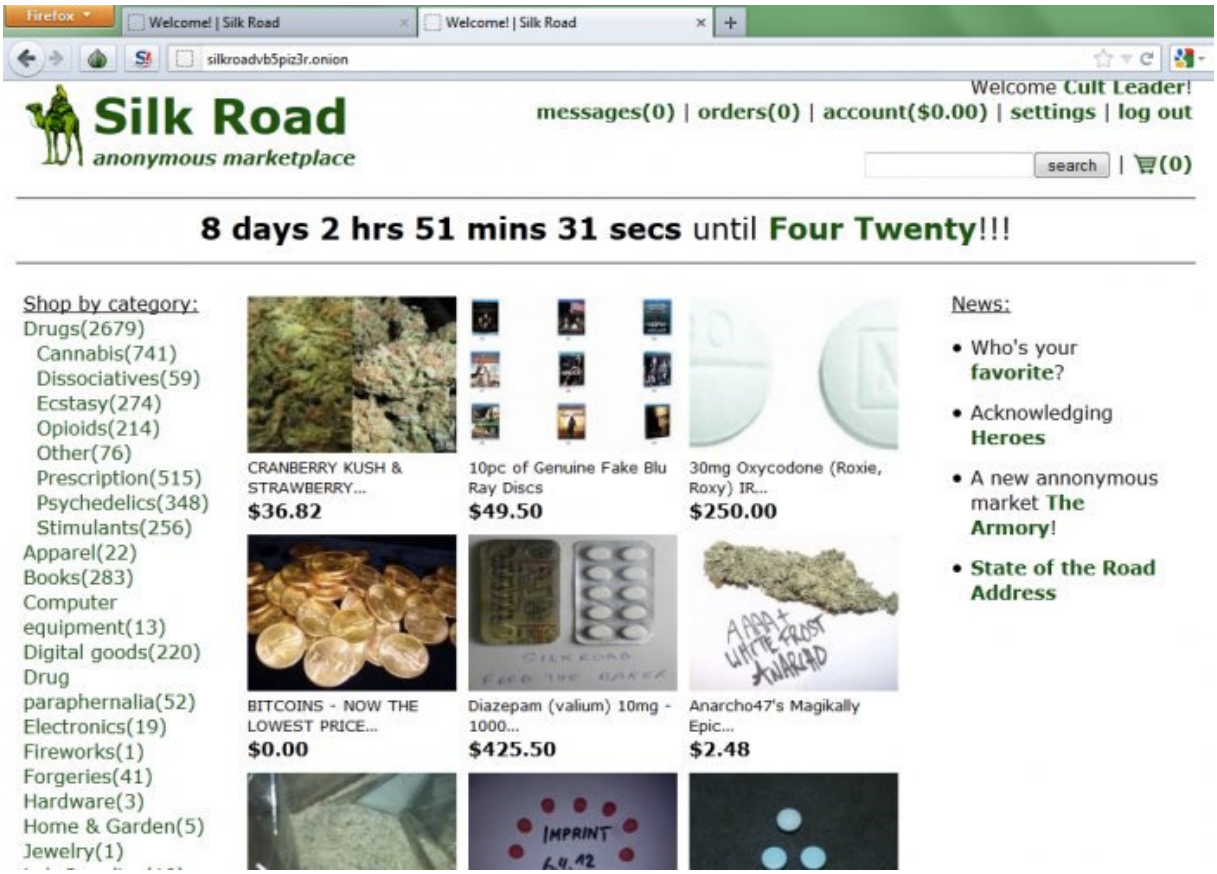
> *"Cryptomarkets are defined as a type of website based on the dark web that employs advanced encryption and cryptocurrencies to protect the anonymity of users."*

Characters of Cryptomarkets include: reliance on the TOR network; use of cryptonyms to conceal user identity; use of traditional postal systems to deliver goods; third-party hosting and administration; decentralized exchange networks; use of encrypted electronic currency, aka cryptocurrency (Martin J. , 2014). Searching through the dark web site, Hidden Wikipedia, whish is another website available through TOR; we can find ready access to hundreds of websites. Alternative, surface websites such as www.DeepDotWeb play host to online communities centered around Cryptomarkets, featuring regular listings of poplar Cryptomarkets, their status and allowing users to create reviews, as well as featuring a host of different guides and tutorials for both new and experienced users to become familiar with the art of dark web cryptomarkets. The Silk Road is not really a shop per say, but more like an

open market similar to E-bay, allowing for an online and anonymous transacting infrastructure, and similar to E-bay with regards to visibility of vendor, buyer and product ratings to assist in member transaction decision-making (Hout & Bingham, 2013).

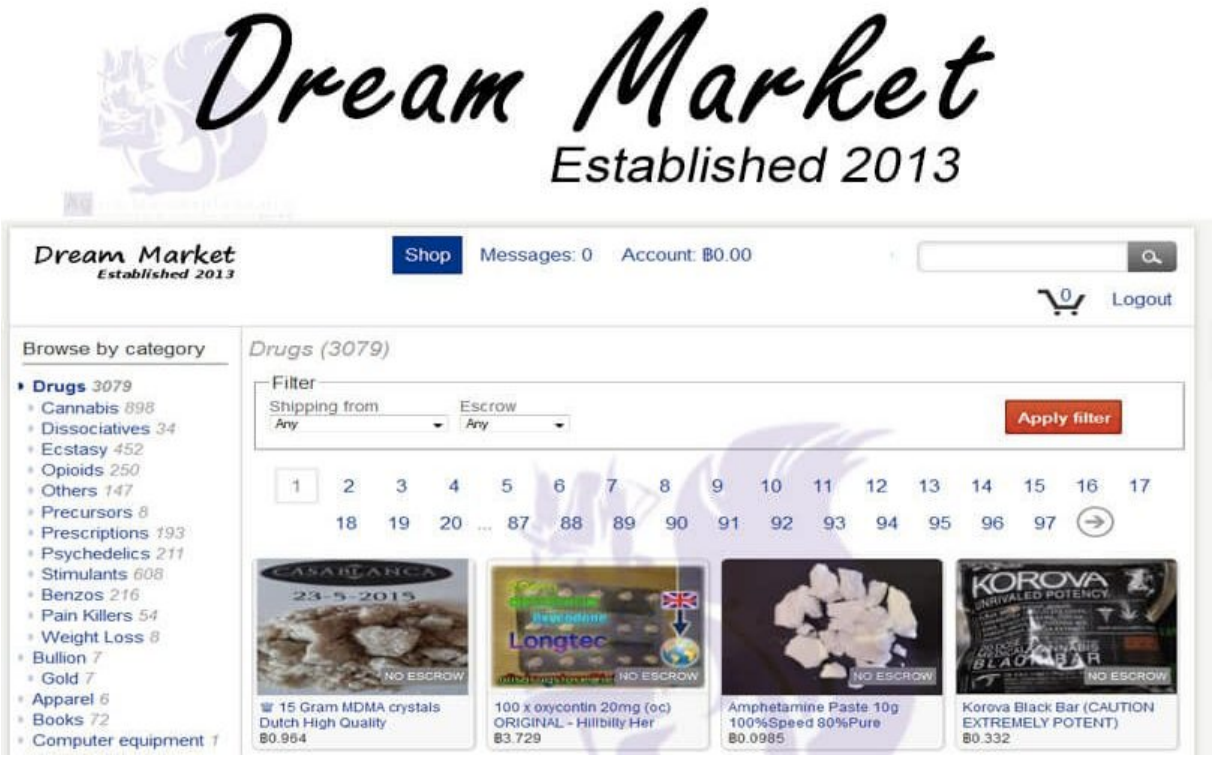
We build and take our conceptual model of Cryptomarkets from the original Silk Road 1.0, which was the first significant true dark web cryptomarket that both conquered and established the drug trade on the dark web (Hout & Bingham, 2013; Dolliver, 2015). From its inception in January 2011, the silk road ran for two and three quarter years. From the first data point of May 5, 2011, where the site had 343 drugs listings, to just before the shutdown the number of drugs listing rose a phenomenal early 3700%, reaching 13000 on October 1 2013 (Digital Citizen's Alliance, 2014). The FBI referred to the first Silk Road as “the most sophisticated and extensive criminal marketplace on the internet”. Inspired by the success of the Silk Road, many of the Silk Road’s successors took inspiration from and built on its image. Compare here two pictures, one taken from the old Silk Road:

Figure 3. Image of the cryptomarket Silk Road 1.0 store page.



Below is another screenshot taken from the still popular Dream Market

Figure 4. Image of the cryptomarket Dream Market store page.



Each site maybe different to a lesser extent in terms of looks, categories, types of products sold, but they are each closely based off on Ulbricht's first model introduced in the original Silk Road 1.0, which in turn was based on legal marketplace sites such as Ebay.com. Do note that I use Ebay.com as an example and not Amazon.com. This is because cryptomarkets, such as Silk Road 1.0, Dream Market and Tochka Market are more in line with Ebay.com, which functions as a virtual market ground, whereas Amazon is a direct provider of goods that maintains its own inventory in its large network of warehouses (Hout & Bingham, 2013).

3.2.2 Unique Features of the Cryptomarkets

Many features that we have come to expect from our legal marketplaces available on the surface web such as E-bay and the like; including rating and review systems; have found their way onto the new and innovating cryptomarkets as well (Hout & Bingham, 2013; Martin J. , 2014). As briefly mentioned in the previous section, mechanisms of trust came to take on an important role on cryptomarkets (Bhaskar, Linacre, & Machin, 2017). This mechanism of

trust would come to be expressed through rating systems found on cryptomarkets, such as the Silk Road 1.0 (Hout & Bingham, 2013). This proved to be a very important function on sites based around anonomity.

3.2.3 Cryptomarket Business, Payment and Delivery Methods

Cryptomarkets are good business. That much is evident from their growth as indicated by the studies done by Bhaskar and his colleagues (2017). Different cryptomarkets can employ different business models. The platform owner makes money from collecting a commission from sales made on the website, often through commissions and vendor bonds. Vendor bonds are fixed sums required to pay in order to become a vendor on a marketplace. Some sites employ a subscription system, or an initial entrance fee, although the most popular of them allow free access for the normal buyer.

A number of different payment methods exist for cryptomarkets to use, but they are all based around cryptocurrencies, some of the more popular examples being BitCoin, Ethereum, Ripple, Bitcoin Cash, Dash, Neo, Nem, Monera and LiteCoins (Gandal & Halaburda, 2016; Market Cap, 2017). Cryptocurrencies are decentralized, privately owned currencies lacking a centralizing authority, institution or owner and popular on the dark web or amongst those who do not wish to have their transactions tracked (Bradbury, 2014; Gandal & Halaburda, 2016). According to Market Cap (2017), there are no less than 1234 existing cryptocurrencies available in the world as of October 2017. The Silk Road made good use of the so called ‘escrow system’. In an escrow system, the funds deposited by the buyer are withheld from the seller, and held by the platform until receipt of the goods is verified by the buyer. In principle the escrow system mitigates the seller moral hazard, since the seller cannot just make away with the funds without sending the good, a real possibility when the transaction is illegal. Granted, this does not prevent the risk of the platform moral hazard, such as if the platform owners themselves should steal the funds held in escrow, which happened to the cryptomarket called Evolution in 2015 (Bhaskar, Linacre, & Machin, 2017). One solution to this problem would have been by using a so called ‘multi signature’ escrow system, where signatures from the buyer, platform and seller would all be required, but this solution did not popular, possibly due to the increased transactions costs involved (Bhaskar, Linacre, & Machin, 2017).

The most common method used for the delivery of goods on cryptomarkets is through the use the already perfectly legal postal system, where drugs are shipped and transferred from vendor to buyer through mail (Martin, 2014). Not only does this method provide a very convenient and easy method for delivery, but it is also relatively safe. This is because while it can be argued that inspecting their mail would be an easier way to detect and capture users on cryptomarkets than trying to catch them while they are online and heavily encrypted on the dark web, inspecting all the mail is an increasingly impossible proposition in our day and age (Martin, 2014). There are a number of benefits to this new form of distribution, especially when compared to previous methods (Dorn, Murji, & South, 1998), especially as there are no need for physical interaction or any contact between parties. One notable feature with this new platform for distribution lies in the potential for cutting out the links that go in the middle, such as drug traffickers, brokers, wholesalers, street retailers and other intermediary links (Martin, 2014). This can have a positive effect on the buying drug consumer, and further explain the qualitative advantages when it comes to user experiences that cryptomarkets can possess over alternative solutions (Dorn, Murji, & South, 1998; Hout & Bingham, 2013). One of the core weaknesses of the digital distribution networks that are enabled by cryptomarkets is that they are limited by the available digital infrastructure (Martin, 2014), yet this is something that is changing over time as the world is becoming increasingly modernized (Castells, 2010).

4. Method

In this chapter I will be detailing the methodology of my research. I will be describing and explaining my choice of methods, discussing the peculiarities of doing internet research in general, sampling, selection and talking about the thoughts behind the analysis of the data. Data quality considerations will be examined and I will explain my own precautions, in addition to talking a little bit about the researcher's role, possible effects and personal biases I may have on the research and finally I will go through a number of ethical considerations for this paper.

4.1 Method & Choice

The main method of data collection in this research is a qualitative document analysis.

A document analysis entails the in-depth study of various forms of documents (Bryman, 2012; Tjora, 2012). Documents are varied in that they can take many different forms, such as auto-biographies, letters, diaries, newspapers and even non-textual forms such as photographs (Bryman, 2012; Tjora, 2012). Neither are they limited to merely physical forms, but can also exist in nonphysical forms as well. An example of such a nonphysical form are documents on the internet, which can be referred to as *Virtual Documents* (Bryman, 2012). A distinguishing characteristic of documents is that they have not been originally produced at the behest of the researcher conducting the document analysis, but for some other original purpose, only to then be analyzed by the researcher at a later date (Bryman, 2012). In 1990, J. Scott defined four criterion to the analysis of documents, as well as creating the distinction between *Personal Documents* and *Official Documents*, and has further classified the latter; Official Documents; in terms of Private Documents as opposed to State Documents. His four Criterion are as follows (Scott, 1990). First: *Authenticity***.** Is the evidence genuine and of unquestionable origin. Second: *Credibility***.** Is the evidence free from error and distortion? Third: *Representativeness***.** Is the evidence typical of its kind, and, if not, is the extent of its untypicality known? Fourth: *Meaning***.** Is the evidence clear and comprehensible? Scott's four criterion for document analysis are applicable to physical and virtual documents as well, and hence invites the analysist during internet based document analysis to consider questions such as the following; why was the website constructed in the first place? Why is it there at all? Is it there for commercial reasons? Or does it have an axe to grind (Bryman, 2012)? These criterions will help with the quality assessment which I will go into later in this chapter. In addition, I have chosen to use a hermeneutic approach to the analysis of the various forms of document data gathered throughout my research. Hermeneutics refers to the long tradition in the history of ideas that has examined principles and procedures for interpreting texts, originally within religion and law, but has since grown increasingly with reference to texts of any kind and even human experience as well (Consalvo & Ess, 2011; Bryman, 2012). The central idea of hermeneutics is that when studying a text one must seek out to bring out the meaning of a text from the perspective of its author, which will entail a grasp of the historical and social concepts in which the text was produced. An approach to the analysis of text like qualitative content analysis can be hermeneutic when it is sensitive to the context within which the texts were originally produced. As I mentioned before about the nature of documents in a document analysis, hermeneutics is not exclusively confined to merely analyzing texts only, and it can even extend to social actions and other phenomenon.

Analyzing documents is not a straightforward matter however and I took multiple precautions when analyzing them, as I will go deeper into in the next chapter.

4.2 Doing Internet Research

The internet; also known as the World Wide Web or WWW for short; is in a constant state of flux, defined by its continuous change (Bryman, 2012). It constitutes a historically unique configuration of informational and communicative resources, being the digital marriage of a massive information archive with high-speed communications, accessible and applicable; in theory; anywhere and anytime (Consalvo & Ess, 2011). In today's digitalized world, people habitually provide; more or less willingly or knowingly; information onto operational systems the sort of information about themselves and their encounters that previously had to be sampled and documented for the distinct purposes (Consalvo & Ess, 2011). An example of this would I for instance be Gordon Bell's MyLifeBits project of documenting each and every aspect of his interactions with the world around him (Bell & Gemmel, 2007). New websites and pages are continuously being made, changed or discarded at a growing rate correlating to the exponential growth of the internet itself and its userbase (Bryman, 2012) (Internet World Stats, u.d.). Conducting an internet based research presents the researcher with a slew of new possibilities and avenues of approach to research, yet it also comes with its own set of unique challenges. Because of its constantly changing and evolving nature, the researcher may find that a website that they visited mere months ago has been significantly changed or altered, possibly carrying no true resemblances to its previous iteration, or it may have been removed or taken down altogether (Bryman, 2012). Unless the research is specifically aimed at observing the change and evolution of a certain part of the world wide web, the researcher may want to conduct the research within a short and concise time frame as to reduce the changes to the original research object (Bryman, 2012). Alternatively, if the researcher is analyzing a certain website or online forum, they may want choose to download and store the entire site from a given point in time onto their own computer through the use of programs such as the free HTTrack Website Copier (HTTrack, 2017). This allows the researcher to create an offline mirror of the website in question, allowing them to 'browse' its content offline without the need of a steady internet connection, or worry about their access to the site being revoked, or the site itself being removed or closed down (HTTrack, 2017; Cavanagh, 2007). I considered using such a method, but the file sizes were too large and the

download too slow. NVivo, the CAQDAS I used during my data collection and analysis allowed me to store individual websites and texts far more easily and quicker.

I would like to make a note on some methodological confusion when it comes to internet based studies, and that is that it can sometimes blur the line between observation based and document based studies. Internet studies are a relatively new methodological subject (Bryman, 2012), and Eun-Ok Im and Wonshik Chee (2012) have mentioned on how only a comparatively small amount of practical guidelines have been written about them. The interaction on the internet today is very different from the interaction presented in the movie TRON, and despite how cool it might have been for a researcher to don a fancy suit and observe a connected community in realtime, such is not the case. Although there exist numerous interactive groups and communities that can be observed on the web, most of these communities interact through text based means, and forums function very much like bulletin boards where people leave text messages upon text messages for the researcher to later rifle through, much like going through a correspondence of letters between persons. It is because of this that I chose to label this as a document study, as much of the data is already laid out there in ready text and image based form, and much of it still will continue to do so.

4.3 Data Selection and Sampling

I will be limiting myself to three sources of data in this project. The first of these is the websites themselves that will become objects in my analysis. The second source of data will be the comments and the feedback in various threads and comment sections by the users of these sites. The third source of data will be from various documents pertaining to aspect of the dark web, as well as measuring the growth and statistics of various sites when applicable. This collection of data from multiple different sources is known as triangulation, and is defined as the collection of data from more than one source so that it may be cross-checked (Bryman, 2012). This is a useful technique and strategy in ensuring the quality and validity of the data material, and reduce the risk of false or misleading data (Creswell, 2014).

Clear criterions for data material are an important aspect when it comes to ensuring the validity of our data collection and research collection. Even thought ANT may be envisioned as a boundless and holistic approach to a phenomenon, case or research question, a truly boundless research is never going to be either practical nor possible for a mortal researcher to

accomplish, as to examine the endless data available on a topic in a detailed and qualitative manner; especially a phenomenon that is constantly growing and evolving, as in the case of our research; will not be possible. It is therefore necessary to establish clear boundaries for my research. Thus, all data gathered must pertain to or all be based on the Dark Web. They must all be accessible through The Onion Router, TOR, if they are located on the dark web. They must all be primarily involved in the transaction of illicit drugs, which will be the largest unifier. Categories such as guns, hacking services or stolen credit cards are irrelevant and do not affect choice. Cryptomarkets involved with items such as human trafficking or pedophilia are off limits in this study due to ethical concerns, and while they may be mentioned, will not be studied in-depth. All sites must be relatively easily discoverable and accessible to the general public; such as their address being available on the surface web and accessible through TOR without any major hurdles. Whether the primary incentive behind the cryptomarket in question is idealistic, monetary or something else is irrelevant. They will be collected in order from largest to smallest in terms of popularity and size. Because of the secretive nature of the Dark Web and the sites located on it, it is not possible for me to guarantee that I should find the most popular sites, and some of these sites may be closed off, requiring Registration or that I be given access by certain 'Gatekeepers' of the site. Because such a level of interaction would break with my zero-interaction rule, these websites will be off-limits for my research, therefore cryptomarkets requiring registration such as CGMC are off limits.

4.4 Data Collection & Processing

Data was collected from four main sites; Dream market, Wall Street Market, Tochka and Libertas Market and their attached and separate forums and comment fields.

Collection of data from main sites; Dream Market, Tocka Market, Libertas Market and Wall Street Market was problematic due to their frequent downtime, meaning access to the sites was difficult and unreliable. However, no such issues were encountered with their respective forums, where the forums remained up and stable throughout the entire research process whenever I visited them.

A CAQDAS, or computer-assisted-qualitative-data-analysis-software was used in the analysis of the data material gathered during this research. The program in question was NVivo. It was

chosen because it was the only CAQDAS available from NTNU's software page for students, and because of its ability to handle a variety of files and formats, including audio, photos, pictures, word files, PDF, web and social media data. It proved itself valuable in storing and analyzing the large amounts of data gathered during my research. The actual utility of CAQDAS is at times questioned (Bryman, 2012; Tjora, 2012). Based on my experience, I cannot say for sure whether my interpretation or judgement would have been any different had I not used the software. What I do know for sure on the other hand is that it saved me a lot of time, and I like to believe that the less time I spend on shuffling through mounds of paper, the more time I will have for the actual analysis. NVivo comes equipped with a lot of advanced options that could take some time getting used to, but these are not required, as the basic options are intuitive and more than enough for regular coding, which meant that knowing the advanced options is more of a luxury than a necessity in order to use the program.

4.5 Data Quality Considerations

Controlling for the quality of the data material in a qualitative study poses a unique set of challenges for the qualitative researcher. Generally, some of the main considerations for data quality control pertains to following: *Reliability*, which has been defined as the extent to which a measure procedure yields the same results on repeated trials (Carmines & Zeller, 1979). *Validity* which refers to the extent to which an empirical measure adequately reflects what humans agree on as the real meaning of a concept (Babbie, 1995). Generally, it is addressed with the following question: "Are we really measuring what we want to measure?" (Babbie, 1995; Bryman, 2012; Tjora, 2012). *Generalizability*, and *Replicability* often play an important role as well. *Generalizability*; sometimes called *external validity*; refers to the degree to which findings can be generalized across social settings; however, LeCompte and Geotz (1982) do problematize the generalizability in qualitative researchers due to their tendency to employ case studies or small samples. And replicability refers to the extent to which the research in question can be replicated by future researchers who come after (Bryman, 2012). Thagaard (1998) explains that questions with regards to reliability and validity tend to be rooted in the quantitative methods, and their applicability then becomes problematic for mixed methods studies, and even more so for the purely qualitative studies.

Although this presents problems for the qualitative researcher, it is not grounds for throwing away quality concerns, and so Lincoln and Guba (1985) propose an alternative to the conventional reliability and validity: that of *trustworthiness* and *authenticity* (Guba & Lincoln, 1994). I will present these in the following sections.

4.5.1 Trustworthiness

As it is presented by Lincoln and Guba, trustworthiness is made up of four criteria, each of which has an equivalent criterion in quantitative research. They are as follows: 1. *Credibility*, which parallels internal validity. 2. *Transferability*, which parallels external validity. 3. *Dependability*, which parallels reliability. 4. *Confirmability*, which parallels objectivity. The first, credibility, presses the significance of multiple accounts on social reality. Examples of credibility techniques are *respondent validation;* sometimes called member validation is the process whereby the researcher provides the people on whom he or she has conducted the research with an account of his or her findings and requests feedback on that account; and *triangulation;* which refers to the use of more than one method or source of data in the study of a social phenomenon so that findings may be cross-checked (Bryman, 2012). The second, transferability, concerns the fact that qualitative research typically entails the intensive study of a small group or event in depth rather than in breadth. In response to this, Geertz (1973) suggests to qualitative researchers to produce so-called "thick descriptions" as he names them. That being rich accounts and details in their research, which according to Lincoln and Guba will provide others with a database from which to make judgements abut the possible transferability of findings. Dependability, as a parallel to reliability in quantitative research; but also a less popular qualitative assessment criterion in the qualitative tradition (Bryman, 2012); where Guba (1994) proposes an 'adutiting' approach where the researcher should keep a total record of all phases of the research: problem formulation, fieldwork notes, data analysis decisions, fieldwork, interview transcripts and so on so that they may be reviewed by peers. Because of the extreme amounts of data that qualitative research tends to generate, this would put an equally extreme amount of pressure on said peers, and is presumably one of the reasons why this technique is not as often used. The criterion of *confirmability* is concerned with ensuring that; while recognizing that complete objectivity is impossible in social research; the researcher can be shown to have acted in good faith. In other words, it should be apparent that he or she has not overtly allowed personal values or theoretical inclinations manifestly to sway the conduct of the research and finding derived from it (Bryman, 2012).

4.5.2 Authenticity

The concept of *authenticity*, as proposed by Lincoln and Guba (1985), raises a wider set of implications regarding the political aspect of research, and divides these concerns into five criterions: Fairness, which asks whether the research fairly represents the different viewpoints among members of the social setting. *Ontological authenticity*, which asks whether the researcher help members to arrive at a better understanding of their social milieu. Educative authenticity, which asks whether the researcher helped members appreciate better the perspectives of other members of their social setting. *Catalytic authenticity*, which asks whether the research acted as an impetus to members to engage in action to change their circumstance. *Tactical authenticity*, which asks whether the research empowered members to take the steps necessary for engaging in action.

4.5.3 Quality Assessment precautions taken.

In dealing with the criterion of credibility as we discussed above, I will first acknowledge that the notion of respondent validation as explained in section 4.6.2 is not applicable to this study because I do not have contact with any particular, and am observing networks based around anonymity and documents. However, Triangulation is still valid a technique in this research thanks to the wide array of available data on the subject matter, and is something that I will use throughout the analysis, the same as I will with the use of thick descriptions whenever possible to appease the transferability criterion.
The challenge of confirmability in my research is something that I have attempted to address in in the introduction, the previous, the sub chapter of the researcher's role and the analysis as well, and while I have a problematic view of the subject of the matter, i.e the dark web and cryptomarkets, it is not something that I have any real stakes or involvement in, nor any strong feelings. The impetus behind this paper is to divided equally between my curiosity on the subject matter and a wish to learn, and to write a good paper that I can be proud to deliver.

As for research replicability. Due to the nature of qualitative research, replicability is often compromised, as unlike quantities methods, there is no set mathematical formulate or strict, unwavering method. Qualitative research often involves a degree of interpretation, and is therefore inherently subjective and possibly different from researcher to researcher. In

addition, the phenomena's and objects examined during qualitative studies are often fleeting, and the people and places used in the research will change over time, and so if a researcher should repeat a previous study on a group or area, they may be entirely different from what they were during the original research.

Internal Validity is the concern with the question of whether a finding that incorporates a causal relationship between two or more variables is sound, and external validity is a concern with the question of whether the results of a study can be generalized beyond the specific research context in which it was conducted (Bryman, 2012).

4.6 The Researcher's Role, Effect and Personal Bias

One of the previously benefits with digital document based studies is that it is a very unobtrusive method. This works well in avoiding what is commonly referred to as the Observer Effect. When performing interviews, or observing individuals in an environment, they researcher may; intentionally or not; affect the the subject(s) of the research. The subjects may act differently, all depending on the researcher's looks, physique, size, gender, class, race, ethnicity, dialect, occupation or even their mere presence, and each of every variable may have a different effect from individual subject to subject. A prime example of the observer effect is the study at the Hawthorne Works in Cicero, Illinois, where the observed increases in productivity amongst the works had less to do with the changes made to the workplace, but more with the direct fact that they were visibly being observed, and thus production slumped when the study ended (Tjora, 2012; Bryman, 2012). With a digital document study, the observer's role will for all intents and purposes be effectively nil, in that no proximity or interaction is required with any subjects of the research; it being fully possible to conduct the entire research from a single office room provided you have the proper access and internet connection.

The dark web is a relatively new subject in the social sciences, and for myself as well. Although I; like so many of my generations that were born in the 1990; am a daily user of the internet and has been familiar with it through a large portion of my childhood, I have never had the need to hide neither my political views or activities, and never touched upon the dark web until I chose it as the topic for my research project. I will say that when it comes to the dark web; even though I have no real stakes in it myself; that I approach it with a negative

disposition. All forms of human inquiry is inherently subjective, and I will not claim that my choice was a purely objective one, ordained by some bias free machine logic that transcends the limits of the human mind. No, in my case, I chose the topic of the Dark Web; and later narrowed down on Cryptomarkets; because I was initially lured in by talk of the dark web, both on online forums and poorly researched clickbait articles talking about the dark web as it was some ominous, evil valley of the internet. I have since done my own research, and attended a seminar held at Samfundet in Trondheim on the Dark Web, featuring Britta Hale of the Institute for Information Security and Communication Technology here at NTNU, and Inger Marie Sunde, a professor at the Oslo Police Academy. Though I have learned much more since back then when I first started, my original disposition; while now more informed; has not changed much. Although I will never refute the value the dark web when it comes to helping oppressed groups in authoritarian societies come together and express themselves, I also recognize the dark web as a security challenge in already liberal and democratic societies, where the freedom and anonymity provided by the dark web is not necessary for the already given right of self expression, but can instead be used as a cloak by criminals and terrorists alike to shield their activities from the law. But even though I may view the dark web as problem to be solved, I will still to the best of my ability not let my bias interfere with my own judgement as a researcher. The hallmark of good research in general; both qualitative and quantitative; is the ability of the researcher to acknowledge all empirical data material that comes up during their research and that is relevant to their research question, and data material does not become irrelevant just because the researcher may not agree with it or because it refutes their cause.

4.7 Ethical Considerations

There exists a number of ethical considerations to take into account when doing research. Often, these can be divided into four principles (Diener & Crandall, 1978). First, there is the question of whether there is a risk of harm to participants. Harm in this sense is not just understood as merely direct physical harm, such as a stab wound; for while it is included, it harm can also involve harm to the participant's self esteem, social position, or making the subjects perform reprehensible acts. Second, there is the concern of whether or not there is informed consent on part of the research participants. Third is concerned with the invasion of privacy. And fourth is concerned with the possibility of deception or duping participants.

Since the the method of data collection in this research paper is a document analysis on content available in open or relatively open channels and site accessible to the general public, it also naturally solves many of the ethical challenges associated with doing research. Because the only interaction that takes place is between the researcher and the document data, there is a minimal level of intrusion. Due to the secretive nature of the dark web based online marketplaces and its associated forums, it would not be possible for me to identify users, sellers and buyers that I came across even if I had wanted to. My own presence would also be entirely unnoticed by all except those who intentionally set out to look for me, which given TOR is not an easy thing to do in itself for reasons explained earlier in the Dark Web and TOR section. To risk sounding melodramatic; I would for all intents and purposes be as a ghost. Because I would never meet anyone associated with the objects of my study, interact with any participants or tell them to come to place X or do action Y, I will state that there is no risk of harm to anyone involved in this research, which is usually one of the benefits of doing a document analysis. Even though the users of dark web have already anonymized themselves by using pseudonyms and revealing no information about themselves; I will still whenever I use, mention or describe dark web users who have been active on various sites, comment fields or forums refer to them with an alias, and not their site name. The only exception to this rule are prolific actors who have already been revealed in the media public, such as Ross William Ulbricht, aka “Dread Pirate Roberts” of the Silk Road. I would like to remind any reader however that that does not mean it is impossible to harm someone as a result of doing a document analysis. Bear in mind that people may still be harmed or come into trouble if you write something that may involve or highlight them.

With regards to the second principle of informed consent, I would like to preface this by saying that it is still a hotly debated topic due to its vast nature, and that no full consent or agreement as been reached (Bryman, 2012). But still, the core of the issue is still very real and can not be ignored. And at this core, the question of informed consent is concerned with whether or not participants are fully informed about their role in the research, so well as their right to withdraw and quit at any moment when they feel like it. And note when I say ‘fully informed’, because if the participant has only been given part of the information of the research, they will still count as not having been informed and thus violate the ethical principle of informed consent. Yet, as with a statement given by the British Sociological Association, consent from recipient is to be attained only insofar as it is practical; a fact acknowledged in their statement about covert research that condones ignoring this ethical

principle only when there is no other option available (British Sociological Association) (Bryman, 2012).

This research has no direct participants per say; and is a document analysis, not an observation; concerned with analyzing data already existing on the dark web and available to normal users without any kind of special clearance or access beyond TOR and a simple internet connection. Because of the vast user base of the various sites and forums explored during this study and the inherent secretive and paranoid nature of the dark web, which I went into further detail in the earlier chapter about the dark web; attaining consent from the sites would be impractical, intensely disruptive and or even impossible. In addition, the issue if consent is alleviated in a sense that the documents exist within a public domain accessible by the general population; and users of the various sites and forums that are not closed off can expect their content to be read by anyone.

5. Analysis

In this chapter I will be analyzing the gathered data, starting by showing themes and traits found throughout my coding and then analyzing the Data in the perspective of Actor-Network Theory. I will also repeat the original research question of this paper, which will guide the next chapters, and that is as follows:

"How are cryptomarkets formed, maintained and dissolved?"

Those who want the short answer can skip to section 5.4 The Nature of the Network, where I will give the final answer to this question.

5.1 Central Themes around Cryptomarkets

The dark web and the cryptomarkets represent a new form of evolution on already an already existing problem: drug traffic. The cryptomarkets that we know today are the result of the joining of elements both old and new. Drugs and their users, as well as superior information and encryption technology to introduce actants such as TOR, the Dark Web and cryptocurrencies such as BitCoin that enter together in a new and cohesive type of network

that stands to change the face of the drug trade as we know it. Libertarian and utilitarian views are often expressed together by users, and rather than

5.1.1 Low Risk

When we discuss risk, we will be referring to the user's chance of either being involved in violence or being caught, tracked or identified by the police. According to the World Health Organization (2014), violence can be defined as the intentional use of physical force or power, threatened or actual, against oneself, another person, or against a group or community, which either results in or has a high likelihood of resulting in jury, death, psychological harm, maldevelopment or deprivation. One of the benefits often highlighted with the use of online cryptomarkets such as the Silk Road 1.0 is that it takes the crime off the street and into the digital world, thereby reducing the risk that of violence. It is argued that it is therefore less likely that innocent bystanders may get caught up in any exchange, wherein the views of many users coincide with Jardine's (2015) own evaluation. Because of the physical and geographical distance between the involved parties, the buyer and the seller, there is a significantly reduced risk of exchanges turning violent, wherein one party might attempt to rob or assault the other, which was ever a risk with the conventional, old drug trade (Dorn, Murji, & South, 1998). However, the absence of direct physical violence might conceal other forms of violence, such as threats, coercion or blackmail that may take place around these cryptomarkets, and is hard to track or observe as they can take place in private and encrypted channels between individual users.

5.1.2. Efficiency and Innovation

Perhaps one of the stronger themes discovered during my research was the generally positive feedback towards the new form of drug trade offered by cryptomarkets. Cryptomarkets, whether they are referred to as black market, darknet markets, there was a general agreement amongst the users that the new form of trade offered by cryptomarkets were a welcoming change indeed, even if there were still the occasional minor technical complaint from users who did not agree with the design of the interface or with the layout, as observed wherein a large portion of the forums were devoted discussions or questions regarding technical problems and solutions. Yet those were minor compared to the general positivity towards the new form of drug trade in general. One of the users told the following story.

... it kinda hard to describe the difference. I remember back before I tried the silk road. It was just me, a couple of friends and a dealer down the road. In just two years, I came close to being busted three times! And our dealer wasn't even there. Then it all changed when heard about the Silk Road. We were hesitant at first, unsure about the move. But then we finally got around to make the first purchase, and then just a few days later, we got the shipment problem free. I couldn't believe how easy it was. Suffice to say it was easy sailing since and we never needed our old dealer.

These was a familiar story repeated in multiple instances, often told directly from user to user, but with the common theme that the utility and service provided by the new platform for drug trading was something to be cherished and welcomed.

5.1.3. Caution Advised

Much of my writing so far I realize may have painted a picture of drug trafficking on the dark web as an elegant and smooth operation without major hurdles. This is not my intention, as say is not entirely true, and I would like to remind the reader that it is anything but safe or guaranteed to succeed. While cryptomarkets in general definitely feature significant advantages and evolution on the original drug trade (Aldridge & Décary-Hétu, 2014), through minimizing contact; and thus chance for being caught or exposed to violence; gathering a greater number of buyers and sellers together to create a better qualitative experience for the user of these cryptocurrency sites, cryptomarkets are not without their own risks. And these risks do not solely lie with the authorities or the risk of being caught by the police. Cryptomarkets are sites run exclusively by private individuals and groups. Due to the secretive nature of these sites in general, the actual knowledge that the customer has of the owner of the sites is very small. There is in essence nothing to stop the user of the site from one day deciding to bail without a moment's notice, shutting the entire page down and leaving with all attached bitcoins. The users would receive no warning in this case, and their only real knowledge of site's owner would be the pseudonym that they used, such as the Dread Pirate Roberts of the Silk Road that remained anonymous until the FBI caught him. The cryptomarkets' owners suddenly bailing and running off with the money is a very real

possibility that users of these dark web black markets must acknowledge. That is not to give the impression that this has lead to mere blind trust is to be the only recourse left for users of these dark web based cryptomarkets. Given the illegality of their activity, the possibility of losing their own money, and even ending up in jail; users have more or less developed indicators of trustworthiness of different sites, some intentional, and some less intentional. An example of one of the intentional indicators of trustworthiness involves practices taken from already existing, legal websites such as Ebay.com; wherein review and rating systems are implemented so that users may review sellers and their products for other users of the site to see. This becomes a valued indicator of trustworthiness, wherein the suspicious environment inherent of these sites means that new and unknown buyers will struggle to gain traction for their wares and products on the site, while well known and established buyers will enjoy greater attention and business because of their positive rating and reviews. Marking certain users as trustworthy; whether it be through user ratings and reviews, or special titles or insignias given to them by the site's administrators, is not a new phenomenon exclusive only to dark web based cryptomarkets, but was also a practice on websites on the surface web such as The Pirate Bay that identified that marked certain, veteran users as more trusted based on their history on the site. Trust is a crucial aspect both on a dark web based cryptomarket as well as on a surface web page such as The Pirate Bay, and dealing with an untrusted source can be a risky endeavor for the user. In the case of The Pirate Bay, downloading from an untrusted and new source may result in the user downloading unwanted, dangerous or malicious files onto their computer. A similar situation goes for users of cryptomarkets, such as the Silk Road. Dealing with a new and yet untrusted seller can lead the user to receive a bad product, or a bad service; assuming they received either of them at all. Or it may even be a ruse and ploy to snare them into a trap.

An example of a more thought out but no less tried and true approach to evaluating trustworthiness amongst users has tended to be to follow a sort of pack mentality. Just like users of The Pirate Bay have a tendency to prefer well known, well used and popular sources; users dark web based cryptomarkets follow a similar kind of mindset when choosing both their sites and their buyers. Sites will therefore see an exponential growth the larger and more popular they get, wherein users will tend to flock towards the largest and most popular site available, provided its available categories match the user's interests. The bigger sites does therefore in effect only get bigger, at least up until a point. There does exist a duality in this, as noted by commenters on the various forums; where users express a level of concern when

the site grows too big, as the larger the site is, the more attention it will garner from the authorities, which in turn increases the risk of a crackdown or takedown of the site.

5.1.4 Driven by ideology.

One theme that occasionally came up from time to time among the users was their referrals to libertarian thought and ideology. This was often used as a justification and argument and for the activity on the site. However, this was not an attitude held by the large majority of the members; or at least not expressed frequently; but when it appeared, it typically did so from a certain sub-group of the users. These users were noted to be far more politically minded than the rest, often citing Libertarian ideology in numerous discussions, especially those revolving around the activity on the site. The use of ideological sentiment is nothing new when it comes to dark web cryptomarkets, with Ulbricht of the Silk Road 1.0 being often referred to as having a strong ideological side, and for even running hos own book club the site when it was still active.

However, these more strongly minded political users; although they were often far more active than regular users and veterans on the site; appeared to be be in the minority on the sites that they occupied. In one event, one of them came into an argument with a far more critical and pessimistic user who ruminated on how it was all to get the best fix, not a moral crusade. This exchange, although prolonged, was mostly ignored by the rest of the users on the site, until one of the moderators closed the thread.

5.1.5 Networks of Crime or Communities

Different dark web cryptomarkets were observed to foster a degree of loyalty and attachment amongst its user base, despite their anonymous nature. Users would express their preference for one site or another, arguing why a specific site was better than the other available alternatives, and users were at times even observed to get into arguments with one another should their opinion on a set if sites differ. It was not unusual for sites to be more than just functional marketplaces for the selling and buying illegal goods and services. They often featured comment fields, discussion boards and forums where users could interact and talk, even in anonymity. The Silk Road, the most successful and largest of the first cryptomarkets, did make sure to include just such social features for their users. Discussion forums hosted by

the Silk Road became grounds where users could meet, talk, converse, discuss transactions and give each other tips and advice. The Silk Road did, for all intents and purposes, seem to foster a community around it. But is community the right term? Lori Kendall would draw attention to the meaning of the word community as a possessing a certain unique characteristics that may not necessarily be applied to online communities (Consalvo & Ess, 2011). The word Community tends to evokes ideas of empathy, affect, support, consensus, shared values and interdependence, yet these are contrasted against the Networked Individualism as described by Barry Wellman, and his description of people in the developed world abandoning the old community for a new, so called networked community (Wellman, 2002). As its name might suggest, Wellman's concept is highly individualistic in nature, and lacking the traditional sense of collectivity that was found in earlier conceptions of community (Consalvo & Ess, 2011). In networked individualism, individuals remain connected, but as individuals rather than being rooted in a home base of work unit or household. Individuals will switch rapidly between their networks, working with them in order to information, collaborations, orders, support, sociability and a sense of belonging, and instead of identifying with a single close-knit community, each individual is at the center of a set of personal networks (Wellman, 2002). The implications of this modus operandi for the user is that that sites gain a far more ephemearal and fleeting meaning to them, and are viewed in a more utilitarian fashion. This makes sites more of a purely go-between between the user and their goal, i.e. to buy or sell drugs. The site loses any significance to the individual, the user feeling no attachment to the site itself, may be more likely to leave on a moment's notice. On the subject of user attachment to a site, the users themselves express sentiments of either position. A number of users, including those who have been observed to defend the given site in earlier arguments, have expressed the belief that they are happy to support their affiliated site, even though they may receive no apparent benefits in return from doing so. Users who voice a different opinion, not having a real sense of affiliation or belonging to the site in question, typically calls the former out for being naïve or short sighted, usually with a bit harsher words. Those feeling nor expressing no special attachment to the site tend to cite liberal market theories as arguments for why people should not grow too attached to a particular site, claiming that it diminishes the natural competition between them; a competitiveness that is argued and held to be good for vast majority of the users.

5.1.6 Flexible users and communities.

The closure of networks is an inevitable threat to the users of cryptomarkets on the dark web. As one user commenting on a discussion thread comparing different sites said:

> *you gotta have a plan A, B or C. if you invest too heavily in one site it'll hurt the most when it goes down. I got a bunch of friends who always keep an eye out on the next big hit, so that once it happens you know where to go next and so on.*

As mentioned previously in the beginning, Décary-Hétu and Giommoni (2016) would go on to observe the negligible impacts that Operation Onymous had had on the online drug trade. One of the causes for this has been identified as the flexible nature of the the dark web markets and their users. Potentially anyone with the prerequisite technical knowledge could create a new cryptomarket with but a minimal crew, and following the closure of one site, the remaining or new sites will often see a surge of new users. Cryptomarkets consistent of multiple different constituent elements that are brought together by the challenge normally presented by the old, conventional drug trade that often revolves around local markets. When an individual network is removed, it is typically done so through the removal of a single actant, i.e the administrators and the seizing of their assets. The remaining elements and actants that come together to form the network, the user base, their desire for a more safe and efficient drug trade, the technology and the problemisation that drives the entire network still persists. Because the role of administrator could be filled by a number of different people, new networks are easily formed and strengthened by elements of previous networks when the previous networks are destroyed. The information technology available in our time and digital age serves the rapid spread of information (Castells, 2010), combined with the fact that the average dark net use are young and relatively savvy technology users (Barrat, 2016), means that in the event that once a user's favorite marketing site is shut down, they are quick to locate the next, second best site. Surface forums and web sites such as www.DeepDotWeb often serve as spreaders of information regarding the status and availability of various different dark web markets, giving free access to introductions on how to use and best operate the dark web, as well as commenting fields and arenas for discussion where potential users can share reviews and discuss various sites on the surface web. Because of the the internet's disregard for physical space and borders, and the wide diffusion of digital communication technology in the modern day an age, the obstacles for moving to or establishing new

cryptomarkets are minimal, to the point that new sites often pop as a direct response to the closure of a previous site shortly after. The structuring elements of dark web based cryptomarkets, the underlying technology; both the software and hardware; the internet, TOR and cryptocurrencies such as BitCoins persist through interventions by national governments and law enforcement agencies and across national borders.

In a forum thread about the cryptomarket known as Wall Street Market, one user remarked about how many of the old vendors he knew from a different cryptomarket known as TradeRoute had found their way over to the Wall Street Market. This sort of market migration is a common story from many different users in relation to the closure of old markets across different sites. Because of the difficulty presented by tracking individual users using the dark web, when a cryptomarket is taken down or seized by the government, the administrator some goods and bitcoins are seized, but the users and vendors themselves are often left untouched by the event. This means that when a network is shut down, large parts of the previous network are already ready to be enrolled into a new one. One user, when commenting on the number of different cryptomarkets that they had been through, choose to describe the attempts as a 'whack-a-mole' game by the law.

> *... you know, whenever they shut us [The Cryptomarket] down, it doesnt really matter. the vendors, the goods, the buyers, nothings stopping us from just moving on to the next place. its just a stupid whackaamole game. i dont know why they bother.*

Whack-a-mole; for those not familiar; is an old arcade game where a single player whacks a number of fake moles to send them back into their holes. This is not a perfect analogy, as in a game of whack-a-mole, the moles will disappear on their own if you are not fast enough. Cryptomarkets, on the other hand, tend stay around if they are not taken down. But it is a good description of the efforts of many law enforcements, where taking down a single network often leads to another one popping up or an already existing network growing in response, turning the efforts of law enforcements into a Sisyphusian work, and critiqued by Christin (2014).

The establishment of a cryptomarket like Silk Road 1.0 and Dream Market or Tochka is not a straightforward process, and even though the sites may operate illegally, they are still beholden to the black market that is available on the Dark Web, and many of the same rules and elements typical of normal markets still apply even there. There exists only a limited number of buyers and sellers available on the dark web. Most of the largest sites available are mainly run as hosted marketplaces that are openly accessible through free registrations for both buyers and sellers, others may require a small entrance fee whilst others again are more gated, requiring invitations from people within the site. The owners of the first type of sites don't necessarily peddle any significant amount of products themselves, but instead take their profit in small sums from the deals that take place on the various sites. Because of this, the larger the site becomes, the larger the income of the people who run it. This creates a natural competition amongst the various cryptomarkets on the dark web for the available and limited traffic. Each

5.1.7 The price of anonymity

Anonymity has been regarded as one of the greatest challenges for law enforcement and one of the greatest strengths of cryptomarkets. However, during my analysis, it was also found to be one of the challenges that the sites themselves had to face with, where the great anonymity provided by the cryptomarkets and their operation became a double edged sword. Trust became a precious commodity on the site, as it was what ruled many of the transactions that took place, and their scale. Many users give cautioning tales and advice across different forums.

> *… don't store your money on any site, and don't trust a site you haven't heard of. Same with vendors. If you haven't heard of it, its not worth the risk*

Rita Zajácz (2017) identified the challenges posed by anonymity on the Silk Road 1.0 cryptomarket, wherein she remarked how the sites such as the Silk Road was built on a contradiction. The very same cryptographic anonymity made it difficult to impose rules and create a stable market, where the Silk Road had sought to impose rules and create a stable market. These internal problems did little to stop the silk road's growth however (Aldridge &

Décary-Hétu, 2014; Dolliver, 2015; Barrat, 2016), and so the impact of what disorder the anonymity may have introduced seems to not have had a significant effect. While internal problems relating to anonymity were discussed by many of the users, it was never pointed out as a major hurdle for their activity, but rather something that could be overcome through good judgement on part of the individual user.

5.2 The Six Phases of Network Translation

A translation is the process of establishing identities and the conditions of interactions among the different actors, consisting of displacing and transforming actors in order to make them fit into the actant-network (Dankert, 2012; Ritzer, 2005). This is essential for the function of the network. If the process of translation fails, it could spell the end for the network itself (Cavanagh, 2007). In Actor-Network Theory, networks are continuous things that have to be constantly performed, and so the process of translation is a process that takes place continuously, and is never fixed nor solid, even if it may seem so when the network is working coherently. Below I will walk through the six phases of translation as identified by Rober and colleagues (2009) for the network of the cryptomarket.

5.2.1 First Phase Translation: Problemisation

As we mentioned previously in the second chapter, problemisation is the first phase of translation and is where the principal actor identifies the nature of a problem as well as the available human and nonhuman actor. In our analysis, the principal actor will be identified as the Site Administrator. To clarify, the Site Administrator need not necessarily be a single individual, but can also consist of a smaller group of people who came together to run the site. The most important characteristic of the Site Administrator is that they act as a single actor, or a complete network if we were to use Actor-Network Theory terminology. In the case of the Silk Road 1.0 that launched 2011 and ran to 2013, it was Ross William Ulbricht who was identified as the Site Administrator. We need not know the real identity of the Site Administrator in order to identify them, such as how we can still identify “Tochka” who runs another Cryptomarket called Tochka Market, just as how we would still have Ulbricht by his pseudonym of “Dread Pirate Roberts” if he had still been anonymous.

When it comes to problemisation, it can be found in the contrast between drug trade on the street and drug trade on the cryptomarkets. The conventional drug market on the street was fraught with numerous challenges for buyers and sellers alike. The threat of both capture by police and violence, threats or robbery from different involved parties was ever present due to the physical proximity often required for transactions to occur where the different parties had to expose themselves. The use of the regular internet was not much of an improvement, where sites often lay out on the open web like isles in the ocean, often using standard currencies such as USD or EURO, and it was generally a matter of time before they were eventually come upon by law enforcement agencies. Ulbricht, in being the first Site Administrator of Silk Road 1.0 was in this sense the first pioneer to truly utilize the potential of the dark web.

Tochka, Site Administrator for Tochka Market, in an interview with authors from the site DeepDotWeb, told them the following about how Tochka Market got started:

> *At the start I was just interested in this topic as it often happens. Then when I was digging into the topic I came to realization that dakrnet is great opportunity to create community of like-minded people. Fastest way to achieve this in my opinion was to create such a platform that corresponds to my moral and sensual perception of the world.*

Tochka has strong biases, as they have a name that is known on the dark web community that they seek to uphold; even if just a pseudonym; and Tochka knew that the interview was going to be open, and so when interpreting it we should assume a certain degree of presentation and promotion on Tochka's part. Yet Tochka's explanation as to how he first became aware of the phenomenon is a story that is mentioned by multiple users and comments. The problemisation is not new, but to find a way to structure it as to make it approach is, and this is where Ulbricht's pioneering work with the Silk Road opened the way for many like minded sites to follow.

5.2.2 Second Phase of Translation: Obligatory Passage Point

As we mentioned previously in the second chapter, the Obligatory Passage Point is the second phase of translation, and is the phase in which the focal actor defines the non-negotiable

aspects of their idea, vision or approach. These are found in rules established for the site, business and payment models that will structure the design of their network. Yet across different networks and cryptomarkets, they seem to converge on a similar model, taking much inspiration from Ulbricht's first work with the Silk Road with only minor alterations to the sites.

5.2.3 Third Phase of Translation: Interessement

As we mentioned previously in the second chapter, interessement is the third phase of translation, and it is where the actor communicates their solution and ideas and as well as the obligatory passage point from phase two to the other actors, but it is also in this phase that the greatest risks of resistance appearing also lie. In the case of the silk road, Ulbricht had the necessary skills to integrate the technological elements of the Silk Road into his network, TOR, the Dark Web and BitCoin, but he still lacked another component necessary to complete it. Yet, there were also multiple factors working for Ulbricht's acquisition of the most important element of his site; namely the users, the sellers and buyers that would keep his site flourishing. In addition to the purely technological function and efficacy of his practical solution, he attempted to rally interest for his site through two primary ways; advertising through social media and contacts, and an ideological call inspired by Ulbricht's own inclination towards libertarianism. In the beginning, growth was slow for the Silk Road, yet it saw a steady increase over time as more people caught on and word began to spread at an exponential rate. In a 2014 study done by Judith Aldridge and Décary-Hétu , sales on Silk Road increased from an estimate of $14.4 million in mid 2012 to $89.7 millions, which is an increase of 600% in just over a year (Aldridge & Décary-Hétu, 2014).

5.2.4. The Fourth Phase of Translation: Enrollment

As we mentioned previously in the second chapter, enrollment is the fourth phase of translation, and it occurs when potential participants embrace and adopt the original mission and BPP of the primary actor, and negotiate with the principal actor about how they could contribute towards the achievement of their goal. This was a continuous progress in the case of the Silk Road, where the initial recruitment of users started off slow. This was a progress we could see on the Silk Road during its exponential growth, where at times it saw a growth

as large as 600%, and a continuous growth without too much disruption until its final shut down by the FBI during 2013 (Aldridge & Décary-Hétu, 2014; FBI, 2015).

Multiple users who said that they had been there during the beginning of Silk Road back in 2011-2013 explained their first experience as meeting something new for the first time, that the services and selection offered by the silk road was something that they had never before seen.

> *... it [Finding Silk Road] was like going into an entirely new world, kinda like a child in a candyshop. You've heard about these things but you don't really get it until youre in it. And that's how it started, once I was in, I stayed.*

5.2.5 The Fifth Phase of Translation: Mobilization of allies.

As we mentioned previously in the second chapter, mobilization is the fifth phase of translation, where allies are mobilized and committed to the fulfillment of the original goal of the principal actor. The goal of creating a large and thriving community in the case of Ulbricht and the Silk Road 1.0. This process unfolded in two places, and not at the same time. The full full establishment of the site required heavily on the technical knowledge of the Site Administrator in the beginning, and later on the recruitment of further administrators to aid in the running of the site. The increased growth of the marketplace over time demanded a growing number of operators, which was something that became a reality for Ulbricht in running the silk road. The extension of co workers presented a security challenge for the Site Administrator, yet in the case of Ulbricht he continued to maintain an anonymous relationship even with his fellow colleagues.

5.2.6 The Sixth Phase of Translation: Black-Boxing.

As we mentioned previously in the second chapter, black-boxing is the sixth and final phase of the translation process, and it is during this phase that the network establishes and institutionalizes the practices and actions that have become essential to the network's identity. Despite its criminal nature cryptomarkets such as the silk road often feature numerous rules

governing the site and its use that are laid down by the Site Administrator and his assistants. These rules govern things such as what's acceptable behavior and what is not acceptable behavior, and institutes a degree of order on what might otherwise have been chaos. This is evident in the cryptomarkets response to scammers or vendors who are associated with particularly poor services or quality products, where through the rating system introduced by many of these sites; cryptomarkets including those such as Tochka Markets, Silk Road 1.0 and Wall Street Market; where harmful actors to the network are identified. Forum threads have been established on forums attached to these sites in order to identify untrustworthy members and vendors and spot them, shunning and removing them from the cryptomarket. These rules, more or less established, are important for the continuation of the cryptomarket network. It is important because many of these sites rely on their innovation and customer experience in order to retain their users. Actor-Network Theory networks are exclusive in their nature, and such is the case with cryptomarkets as well. Users are displaced and transformed into their networks so that they may allow the network itself to grow and function. Cryptomarkets are not vendors themselves, but rather a host for multiple different vendors and buyers that constitute them, and these can be lost at any moment to other competing networks at any time even if the original network is not taken down, such was the case with the Silk Road 1.0 back in 2013 by the FBI (2015).

5.3. Constructing the Network: The Cryptomarket

The cryptomarket is a new type of network that has come to be commonplace on the dark web and a familiar aspect of its underside. It is a network that is built up from both new and old parts. The drug trade is something that has existed for a long time, yet with the advent of the internet, or more specifically the dark web; and aided by the inclusion of technologies such as TOR and cryptocurrencies such as BitCoin, it has taken on a new form in our digitalized society, and that form is the cryptomarket, self generating networks that are difficult to defeat due to the challenges posed by the new technological reality of the dark web.

The most central elements or actants of the Cryptomarket have been identified as the Site Administrator; The Internet, or more specifically the Dark Web; Encrypted Browsers, such as TOR; Cryptocurrencies, such as Bitcoin, and finally, the Users, the vendors and buyers that make use of the site, driven by the problemisation and need for a superior type of drug trade.

Each of these elements are necessary for the function of the network. If one of them are removed, the rest of the network would cease to function, and it would collapse.

The most common way of dealing with Cryptomarkets used by government and law enforcement agencies around the world has been to go after the Site Administrator, which was the method used against the original Silk Road 1.0 and Ulbricht. The result of such an action was the immediate disintegration of the network, and so has proven itself to be a very effective method against single networks. However, the remaining elements of the network, the User, the Dark Web, Encrypted Browsers and Cryptocurrencies were left for the most part untouched. Currency may be seized and occasional users may be caught, but never in a volume large enough to cause significant change (Décary-Hétu & Giommoni, 2016). There are a number of reasons for this. As we mentioned in chapter three, tracking down users on the dark web is not an easy process due to the nature of the dark web and the heavy use of encryption and private cryptocurrencies by the users, and requires considerable time and effort, which makes tracking and apprehending large numbers of users difficult. And so the network could reform itself if it was simply introduced to a new Site Administrator who could bring it all together, as Ross Ulbricht and his Silk Road 1.0 showed the world the solution to an old problem. Targeting individual networks seem to yield little significant effect when it comes to stopping the drug market on the dark web, as discovered by Décary-Hétu and Giommoni (2016) in their study on the effects of Operation Onymous, and certain users have thus described government actions against sites as a game of whack-a-mole.

5.4 Answering the Research Question: The Nature of the Network.

And so, to summarize everything so far and answer the original research question.

Networks are formed through the recruitment by the principal actor; the Site Administrator; of the technological actors that are central to its structuring; TOR, Dark Web and Bitcoins. The process is not a straightforward one, but the necessary network between the technological actors and site administrator is necessary before the network can function.

Networks are maintained and motivated by the initial and continued need and problemisation that first brought them into being. The desire for a more an easier sand safer drug trade. Trust

is important in maintaining sites, and is reinforced through rules and systems, such as vendor rating and review systems. Networks that fail to generate trust are less likely to be successful.

Networks are dissolved when one of the central actors are removed upon which its entire function is based upon. This is typically the Site Administrator, the principal actor of the network. The other parts of the network are generally too difficult to eliminate in any practical way. This, however, means that a large portion of the original network elements remain intact if diffused, and the network can therefore easily reconstitute itself once introduced to a new Site Administrator, which is incidentally also the actor that is the easiest to replace.

6. Discussion: The Nature of the Network

In this chapter I will discuss my findings and their implications for the original issue posed by cryptomarkets, following the conclusion of the analysis.

6.1 Dark Web Activism

Although it has been claimed that that ideology and politically activism plays an important in the formation of cryptomarkets on the dark web, I was unable to find any heavy indication of that. Alexia Maddox (2015) and her colleagues performed anonymous interviews with previous users of the original silk road to find their political inclination behind it all. Personally none of my findings turned up any significant proof to hint at a strong libertarian ideology functioning as a motivating factor for cryptomarkets in general. I did come across multiple discussion and book groups who were indeed interested in political discussion around state intervention, legalization of drugs and libertarianism, but these groups appeared to always be the minority in all sites I found, similar in ways to Ulbricht's own book group was more of a side note in his large and expansive black marketplace. Having browsed the available discussion forums surrounding the cryptomarkets, I have encountered users who show significant political motivation in their actions and thinking, and regularly participate the political discussions. Although these tend to be the vast minority, with the large majority of the forums typically devoted to answering more practical and instrumental questions on how to operate and use the site, a subject that vastly overshadows any other. Politically motivated actors raising libertarian ideals may add a superficial charm to the activity, but it is

doubtful that the cryptomarket itself would suffer any change should the politically minded actors disappear. Harkening back to some of the previous user comments that I mentioned, the first reaction many of them had with their introduction to cryptomarkets was more in line with that of a child who just stumbled across the candy shop rather than a political activist who saw his belief vindicated. It seems it is the cryptomarkets' utility and efficiency in serving different drug buyers and traders that is the most important driving factor for them.

6.2 Reconstituting Networks

Perhaps one of the chief threats of the cryptomarket as a dark web phenomenon lies in its ability to reform and reconstitute itself after having been damaged. This coincides with previous research on the dark web. When I talk about reconstitution, I am not referring to the same networks as were taken down by law enforcement agencies pulling themselves together to become exactly the same network as they were before. We have seen that such is not the case, wherein networks that 'reform' tend to do so in a very different way, and often featuring a significantly reduced user base, which is mainly because people are likely to jump over to different platforms when the original network went down. The two main reasons for this is because the individual user is either not attached enough to the site to warrant waiting around for the site to come back, and the fact that when a site is taken down, other sites will often pop up in its place to fill the vacuum and demand of the users. Silk Road 1.0 is not the same as Silk Road 2.0, and so on. The principal actor, the Site Administrator, exert a significant effect on the rest of the network, and the networks often come to take on a shape of their own throughout their existence. When a site then is taken down, it often returns with a new Site Administrator, and although they may share the same or similar problemisation as with the previous Site Administrator, the exact details of how these networks go about solving them may differ. Granted, individual users tend to be attracted to networks similar to their previous ones, like how some users of the original Silk Road mentioned that even though they still needed their fix, they would avoid certain marketplaces that dealt in things such as child pornography and human trafficking.

6.3 Cryptomarkets

Cryptomarkets based on the dark web still present a significant challenge to law enforcement agencies across the world, and they will probably continue to do so into the foreseeable

future. This is because they are composed of a very tricky mix of different actors, none of which can easily be removed from the equation. The closest that the cryptomarkets come to a vulnerability lies with the Site Administrator. Seizing and removing the site administrator has so far proven to be the best way to eliminate individual sites (FBI, 2015; Décary-Hétu & Giommoni, 2016). However, the technological elements associated with cryptomarkets, such as the dark web, TOR and BitCoins are all still readily accessible to the average internet user, and information regarding how to use it has been steadily spreading across the internet since the first major news of Ulbricht's Silk Road 1.0 began to spread, with DeepDotWeb (2017) releasing a guide on how to start your own Black market business online if you so wished. And the need the initial problemisation that lies at the bottom of cryptomarkets; the desire for a safer and more convenient illegal drug trade and profit; are still despite the takedown of an individual site. I believe the earlier comment one of the users made about efforts to shut down individual sites being akin to that of an endless game of whack-a-mole, it is a fitting analogy if we are referring to the approach of targeting and eliminating the Site Administrator. But what can then be done if that is the case? Could we target another part of the network? I briefly mentioned some of those points in the analysis chapter, but I feel I can go further into them in this section.

Let us start with the first and obvious aside from the Site Administrators; namely the Users, the common vendors and sellers that make up the majority of the network. There are two issues that crop up in this scenario with going after the vendors. The first is encryption; as we mentioned in chapter 3; as Dark Web users employ a strong layer of encryption to keep themselves safe. The second is scale, which compounds the first issue of encryption. The Silk Road had an estimated 900,000 registered users that bought and sold illicit products (Flitter, 2013; Dolliver, 2015). Capturing a single user involved with a cryptomarket often comes down to either great effort by the authorities, or great carelessness by the user in question. Christin (2014) highlights this issue, critiquing the ability of law agencies to deal with the challenge posed by online drug trafficking. But what about going after the structuring technology in the network? Cryptocurrencies such as BitCoin lack any centralizing authority from which it can be controlled. According to the European Central Bank (European Central Bank, 2012), traditional financial sector regulation is not applicable to bitcoin because it does not involve traditional financial actors. If cryptocurrencies were to be centralized under a responsible institution, it might be possible. Granted, this brings us back to another problem, as we mentioned before, and that is the sheer number of different cryptocurrencies available. As stated before in chapter 3, Market Cap (2017) lists no less than 1234 different

cryptocurrencies available throughout the world, and much of their value is generated and maintained through their private use and popularity, variables that are outside the ability for any government to directly control. The Dark Web is another structuring technological actant in the cryptomarket. However, as we went through in chapter 3 on the dark web, it is not so much an individual thing that can be removed than it is the backdrop of the entire world wide web (Bradbury, 2014). Therefore, removing the dark web as a platform for operation on which the network is dependent upon is an impossible task short of taking down the entire dark web, and renders it as a solution impractical. Judging by the poor success of the war on drugs (Wisotsky, 1986; Baum, 1996; Carpenter, 2003), it is doubtful that we will be able to remove the drug trade in the foreseeable. Granted, cryptomarkets are criminal networks that rely on the illegal status of drugs to flourish. Legalizing drugs would undermine the largest source of business for the cryptomarkets that we have examined in this paper. However, whether or not the societal impact such a legalization would have is worth the weakening of illegal cryptomarkets is a question for law & policymakers.

7. Conclusion

Central findings of the study pertain to cryptomarkets proving to be flexible networks that while vulnerable individually due to their reliance on a principal actor; the Site Administrator; to hold the network together, they are also resilient as a whole in that the removal of a single network paves the room for the growth of other similar networks as the remaining components of the original cryptomarket still remains; the structuring technology; BitCoin; Dark Web; TOR, as well as the old elements; the Users and the Drugs. Unlike the Site Administrator, these remaining elements are difficult to remove, which means that cryptomarkets are symptomatic of our digitalized society. Government and law actions against individual cryptomarkets have only had a negligible effect on cryptomarkets in general as the majority of central elements of the original network remains unaffected after individual network takedown. The notion that cryptomarkets were a form of online political activism was examined but political ideology was not found to have a significant effect on the network. In addition, the literature review revealed that due to the newness of the subject, the literature on the subject is relatively shallow. Most of the available literature revolve around the original Silk Road 1.0, but scarce any of it refers to its successors and the multitude of different cryptomarkets that have appeared in its wake. Recommendation for future research

in order to answer the problem posed by cryptomarkets is to examine the dark web and anonymizing encryption technologies such as TOR, as current methods and technologies are unable to effectively handle cryptomarkets. Alternatively, comparative or longitudinal studies of the development of cryptomarkets to identify and detect trends, evolutions or patterns of behavior within cryptomarkets.

Bibliography

Aldridge, J., & Décary-Hétu, D. (2014). *Not an 'Ebay for drugs': The Cryptomarket 'Silk Road' as a Paradigm Shifting Criminal Innovation*. Retrieved from SSRN: https://ssrn.com/abstract=2436643

Babbie, E. (1995). *The practices of social research* (7th ed.). Belmont, CA: Wadsworth.

Barrat, J. M. (2016). Safer scoring? Cryptomarkets, social supply and drug market violence. *International Journal of Drug Policy*.

Baum, D. (1996). *Failure, Smoke and Mirrors: The war on Drugs and The Politics of.* Waltham, MA: Little, Brown and Co.

Bell, G., & Gemmel, J. (2007). *A digital life.* Retrieved 10 10, 2017, from www://www.sciam.com/article.cfm?id=a-dgitial-life

Bhaskar, V., Linacre, R., & Machin, S. (2017). *The economic functioning of online drugs markets.* Retrieved October 24, 2017, from http://dx.doi.org/10.1016/j.jebo.2017.07.022

Bradbury, D. (2014). Unveiling the dark web. *Network Security, 2014*(4), 14-17.

British Sociological Association. (n.d.). *Statement of Ethical Practice.* Retrieved October 21, 2017, from https://www.britsoc.co.uk/media/23902/statementofethicalpractice.pdf

Bryman, A. (2012). *Social Research Methods* (4th ed.). Oxford: Oxford University Press.

Buskirk, J. V., Roxburgh, A., Farrell, M., & Burns, L. (2014). The closure of the Silk Road: what has this meant for online drug trading? *Addiction, 109*(4), 517-518.

Callon, M. (1984). Some Elements of a Sociology of Translation: Domestication of the Scallops and the Fishermen of St Brieuc. *The Sociological Review, 32*(1), 196-233.

Callon, M. (1986). Some elements of a sociology of translation: domesitcation of the scallops and the fishermen of St Brieuc bay. In J. Law, *Power, Action and Belief. A new sociology of knowledge.* (p. 207). London: Routledge and Kegan Paul.

Carmines, E. G., & Zeller, R. A. (1979). *Reliability and validity assessment. .* Beverly Hills, CA: SAGE.

Carpenter, T. G. (2003). *Bad Neighbor Policy; Washington's Futile War on Drugs in Latin America.* Hampshire: Palgrave Macmillan and Houndmills.

Castells, M. (2010). *The Rise of the Network Society.* Oxford: Wiley-Blackwell.

Cavanagh, A. (2007). *Internet, Sociology in the Age of the.* Maidenhead: Open University Press.

Chen, H. (2012). *Dark Web.* New York, NY: Springer.

Chen, H., Chung, W., Qin, J., Reid, E., Sageman, M., & Weimann, G. (2008). Uncovering the dark Web: A case study of Jihad on the web. *59*(8), 1347-1359.

Christin, N. (2014). Operation cyber chase and other agency efforts to control internet drug trafficking the "virtual" enforcement initiative is virtually useless. *Journal of Legal Medicine, 27*(2), 207-224.

Consalvo, M., & Ess, C. (2011). *The Handbook of Internet Studies.* Oxford: Blackwell Publishing.

Creswell, J. W. (2014). *Research Design* (4th ed.). Dorchester: SAGE Publications. Inc.

Dankert, R. (2012). *Actor-Network Theory.* Retrieved May 22, 2017, from ScienceDIrect: http://www.sciencedirect.com/science/article/pii/B978008047163006068

D.O.J. (2015). *Roos Ulbricht, the Creator And Owner Of The "Silk Road" Website, Found Guilty In Manhatten Federal Court On All Counts*. Retrieved October 22, 2017, from United States Department of Justice: https://www.justice.gov/usao-sdny/år/ross-ulbricht-creator-and-owner-of-silk-road-website-found-guilty-manhatten-federal-court

Décary-Hétu, D., & Giommoni, L. (2016). Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous. *Crime, Law and Social Change, 67*(1), 55-75.

DeepDotWeb. (2017). *Starting Your Black-Market Business*. Retrieved October 20, 2017, from https://www.deepdotweb.com/2017/10/29/starting-black-market-business-digital-era/

Diener, E., & Crandall, R. (1978). *Ethics in Social and Behaviorial Research.* Chicago: University of Chicago Press.

Digital Citizen's Alliance. (2014). *Busted, but not broken. The state of silk road and darknet marketplaces.* Retrieved from https://media.gractions.com/314A5A5A9ABBBBC5E3BD824CF47C46EF4B9D3A76/5f8d4168-c36a-4f78-b048-f5d48b18dc0a.pdf

Dolliver, D. S. (2015). Evaluating drug trafficking on the Tor Network: Silk Road 2, the sequel. *International Journal of Drug Policy, 26*(1), 1113-1123.

Dorn, N., Murji, K., & South, N. (1998). *Traffick: Drug markets and Law Enforcement.* London: Routledge.

European Central Bank. (2012, October). *Virtual Currency Schemes.* Retrieved October 2012, 2017, from Frankfurt am Main: European Central Bank.

FBI. (2015). *Ross Ulbricht, the Creator and Owner of the Silk Road Website, Found Guilty in Manhatten on federal Court on All Counts*. Retrieved October 22, 2017, from https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/ross-ulbricht-the-creator-and-owner-of-the-silk-road-website-found-guilty-in-manhatten-federal-court-on-all-counts

Flitter, E. (2013). *FBI shuts alleged online drug marketplace, SIlk Road.* Retrieved from Reuters: http://www.reuters.com/article/2013/10/02/us-crime-silkroad-raid-udUSBRE9910TR20131002

Fountain, R. (1999). Socio-scientific issues via actor network theory. *Journal of Curriculum Studies, 31*(3), 339-358.

Fu, T., Abbasi, A., & Chen, H. (2010). A focused crawler for Dark Web forums. *Journal of the Association for Information Science and Technology, 61*(6), 1213-1231.

Gandal, N., & Halaburda, H. (2016). Can We Predict the Winner in a Market with Network Effects? Competition in Cryptocurrency Market. *Games, 7*(3), 16.

Geertz, C. (1973). Thick Description: Toward an Interpretative Theory of Culture. In C. Geertz, *The Interpretation of Cultures.* New York, NY: Basic Books.

Guba, E. G., & Lincoln, Y. S. (1994). Competing Paradigms in Qualitative Research. In N. K. Denzin, & Y. Lincoln, *Handbook of Qualitative Research.* Thousand Oaks, CA: SAGE.

Hout, C. V., & Bingham, T. (2013). 'Surfing the Silk Road': A study of users' experiences. *International Journal of Drug Policy, 24*(6), 542-529.

HTTrack. (2017). *HTTrack Website Copier*. Retrieved October 17, 2017, from https://www.httrack.com

Im, E.-O., & Chee, W. (2012). Practical Guidelines for Qualitative Research Using Online Forums. *Computers, Informatics, Nursing: CIN, 30*(11), 604-611.

Internet World Stats. (n.d.). *Internet Users in the World by Regions - June 30, 2017*. Retrieved October 17, 2017, from http://www.internetworldstats.com/stats.htm

Jardine, E. (2015). *The Dark Web Dilemma: Tor, Anonymity and Online Policing.* Retrieved October 22, 2017, from Center for International Governance Innovation: https://www.cigionline.org/sites/default/files/no.21.pdf

Kitchen, L. (2000). Environmental policy and the differentiation of of rural Space: An actor-network perspective. *Journal of Environmental Policy and Planning:, 2*(2), 135-147.

Krieger, D. J., & Belliger, A. (2014). *Interpreting Networks : Hermeneutics, Actor-network Theory & New Media.* Bielefeld: transcript.

Latour, B. (2007). *Reassembling the Social: An Introduction to Actor Network Theory.* Oxford: Oxford University Press.

Law, J. (1986). The heterogeneity of texts. In M. Callon, J. Law, & A. Rip, *Mapping the dynamics of science and technology.* Basingstroke: Macmillan Press.

Law, J. (1992). Retrieved August 22, 2006, from Notes on the theory of the ator-network: Ordering, strategy and heterogeneity: www.comp.lancs.ac.uk/sociology/papers/Law-Notes-on-ANT.pdf

LeCompte, M. D., & Goetz, J. P. (1982). Problems of Reliability and Validity in Ethnographic Research. *Review of Education Research, 52*(1), 31-60.

Lincoln, Y. S., & Guba, E. (1985). *Naturalistic Inquery.* Beverly Hills, CA: SAGE.

Madox, A., Barratt, M. J., Allen, M., & Lenton, S. (2015). Constructive activism in the dark web: cryptomarkets and illicit drugs in the digital 'demimonde'. *Information, Communication & Society, 19*(1), 111-126.

Market Cap. (2017). Retrieved October 23, 2017, from Cryptocurrency Market Capitalizations: https://coinmarketcap.com/all/views/all/

Martin, J. (2013). Lost on the Silk Road: Online drug distribution and the 'cryptomarket'. *Criminology & Criminal Justice, 14*(3), 351-367.

Martin, J. (2014). *Drugs on the dark net: how cryptomarkets are transforming the glboal trade in illicit drugs.* New York, Ny: Palgrave Macmillan.

Ramzan, Z. (2010). Handbook of Information and Communication Security. In P. Stavroulakis, & M. Stamp, *Handbook of INformation and Communication Security.* Berlin, CA: Springer.

Ritzer, G. (2005). *Encyclopedia of social theory.* London: Sage Publishers.

Roger, K., Mooe, S., & Newsome, D. (2009). Wildlife Tourism, science, and actor-network theory. *Annals of Tourism Research, 36*(4), 645-666.

Scott, J. (1990). *A Matter of Record.* Cambridge: Polity.

Scott, J. (2000). *Social Network Analysis: A Handbook.* London: SAGE.

Spöhrer, M. (2016). *Applying the Actor-Network Theory in Media Studies.* Hershey: IGI Global.

Stockley, M. (2015). *Hundreds of Dark Web sites clonsed and "booby trapped".* Retrieved October 22, 2017, from Naked Security: https://nakedsecurity.sophos.com/2015/07/01/hundreds-of-dark-web-sites-cloned-and-booby-trapped/

Thagaard, T. (1998). *Systematikk og Innlevelse: en innføring i kvalitativ metode.* Bergen: Fagbokforlaget.

Tjora, A. (2012). *Praksis, Kvalitative Forsknings Metoder i* (2nd ed.). Oslo: Gyldendal Norsk Forlag.

U.S. Department of State. (2017). *Country Reports on Terrorism 2016.* United States Department of State. Bureau of Counterterrorism.

UNODC. (2010). *The globalization of crime: A transational organized crime threat assessment.* United Nations Office on Drugs Crime. United Nations Publication Sales.

UNODC. (2017, June 16). *World Drug Report 2017.* Retrieved October 22, 2017, from United Nations Office on Drugs and Crime: https://www.unodc.org/wdr2017/field/WDR_2017_presentation_lauch_version.pdf

Weimann, G. (2016). Going Dark: Terrorism on the Dark Web. *Studies in Conflict & Terrorism, 39*(3), 195-206.

Wellman, B. (2002). Little boxes, glocalization, and networked individualism. In M. Tanabe, P. v. Besselaar, & T. Ishida, *Digitial Cities II. Computational and Sociological Approaches.* Berlin: Springer.

Wisotsky, S. (1986). *Breaking the Impasse in the War on Drugs.* Westport, CT: Greenwood Publishing Group.

Woods, M. (1997). Researching rural Conflicts: Hunting, local politics and actor-networks. *Journal of Rural Studies, 14*(3), 321-340.

World Health Organization. (2014). *Health topics: Violence*. Retrieved October 22, 2017, from www.who.int/topics/violence/en/

Zajácz, R. (2017). Silk Road: The market beyond the reach of the state. *The Information Society, 33*(1), 23-34.