**Abstract**

Team DIRE’s research involves investigating the socio-cultural interactions of various sectors of the Dark Internet. This proposal aims to demonstrate the applicability of Dark Internet markets and currency to the world marketplace. It also provides a collection of current information about the Dark Internet that has been gathered to justify the need for further research in order to expand upon the relatively small assemblage that exists thus far. Specifically utilizing the Tor Browser, Team DIRE plans to study this correlation by analyzing three overlapping subjects of the Dark Internet: marketplace communication trends during key moments and times of normalcy, marketplace consumer experience, and Bitcoin. The overarching goal of this paper is to outline the methodology by developing new knowledge about the unique culture and community of marketplaces of the Dark Internet.

**Introduction**

As the Internet has continuously developed as the world’s main source for information and communication, online security of the individual has become all the more necessary. Tor, otherwise known as”the onion router”, is a virtual privacy network that enables the user to operate online under heightened anonymity. Any website that is accessible on the public Internet that the average person might use everyday is also accessible on Tor. Tor is a network host on the Dark Internet, which is comprised of all of the websites and network hosts that have intentionally been hidden and are accessible *only* through networks such as Tor (McCoy et. al 2008). By using Tor to access the Dark Internet, users are able to browse the Web while equipped with more security than they had likely ever experienced before. Our team plans to utilize the unique functions provided by Tor to explore the Dark Internet in order to better understand Dark Internet users as a community culture in their response to times of crisis, as well as analyze economic aspects of the Dark Internet in regards to Dark markets and the use of Bitcoin as a cryptocurrency.

The Dark Internet’s degree of anonymity results in increased personal privacy and freedom for the user. Just as different cultures develop over geographically distinct regions, so do discreet cultures emerge on different virtual segments of the Internet. The unique characteristics of the Dark Internet have facilitated the development of a distinctive community culture. The Dark Internet has expanded the freedom of Internet users in several ways: it provides the ability to surpass censorship by citizens living under oppressive governments, and gives others the opportunity to act as whistleblowers and dissidents that expose corruption, all while maintaining elevated anonymity and personal privacy. Economic developments have occurred alongside the expansion of the Dark Internet as well; online cryptocurrencies and expansive marketplaces have flourished, attracting buyers and sellers from all over the world. Despite the progress these economic innovations have facilitated in recent years, little conclusive research has been done on their significance to society, and thus the future of these online marketplaces and currencies and their potential impact on society remains unclear. Bitcoin, the anonymous cryptocurrency, is becoming increasingly prevalent in mainstream commerce, and has recently become available on many popular public Internet services, such as Newegg and Overstock.com, despite its turbulent history and tendency to succumb to inflation.

Maintaining the stability of the Dark Internet has proven to be a challenge, since its anonymous nature has resulted in its use for criminal activity, which has led to numerous conflicts with law enforcement. Numerous Dark Internet marketplaces have been shut down by the Federal Government for their prevalence in the buying and selling of illegal goods and services, but to no avail: these marketplaces have simply reemerged soon after their shutdowns, or others have quickly come forth in their place (Bartlett, 2014). The Dark Internet economy has proven to be extremely resilient, as it has persistently continued to expand in both size and popularity in spite of major current events that have threatened to undermine its security and existence as a network and resource.

Team DIRE plans to analyze themes prevalent on the Dark Internet and Bitcoin’s use as a form of currency in the Dark Internet market experience, and to draw comparisons between Dark and traditional Internet marketplaces. Our research will be conducted through an economical and sociocultural lens, which will allow us to analyze the impact of Dark Internet developments on its culture through analyses of online web forums as well as firsthand experience on Dark Internet marketplaces to determine the functionality of its marketplaces and their practicality for consumers.

**Literature Review**

**Introduction**

The Dark Internet is a form of Internet based in anonymity that operates on a user-run, decentralized network. The concept of browser anonymity attracts a variety of people looking to keep their identities private in any cyberspace interaction. As this technology continues to develop and expand, it is likely to transform society as any major development in exchange has throughout history. The powerful capabilities and rich culture of the Dark Internet are the result of numerous components that contribute to the overall anonymity it provides. One of its most significant features is the Tor browser, the primary method for accessing sites on the Dark Internet itself. Among the many uses of the Dark Internet, 15.4% of its hidden services are comprised of illegal marketplaces, creating a haven for the trade of illegal drugs (Owen, 2015). The online drug trade has been revolutionized by the Dark Internet as it offers mass accessibility and relative anonymity compared to conventional markets for secure transactions. Another important area that should be considered for analysis is the role of Bitcoin, the first online currency to attain widespread adoption (Miers et al., 2013). Bitcoin’s ability to anonymize trade means that it has found natural and widespread usage when used for illegal transactions. While the Dark Internet is a relatively new and complex development, understanding various aspects of its functionality is the first step to creating valuable knowledge on the ways in which it affects society.

**Background**

**Structure.** Onion Routing was developed in 1995 by the Naval Research Lab as a model for anonymous Internet usage (Dingledine et al., 2004). The routing technology was then adopted by civilians to create Tor, which uses layers of encryption in order to conceal the identities of both the sender and receiver in any Dark Internet exchange. The layers of encryption are used to create circuits that can step from one anonymous source or “node” to another. This method of routing became known as “onion routing,” comparing the layers of encryption to the layers of an onion (Dingledine et. al, 2004). When using onion routing, one takes a pathway that goes through the network, building a circuit that will connect from one’s router (or node) to the next, but prevent the ability to identify any other nodes within the circuit (Dingledine et al., 2004). The original Onion Router was created with the intent to protect U.S. intelligence agents working out of dangerous territories. In an article on the effectiveness of the Tor network David Gingrich notes that the problem with this strategy was that agents were still easily identifiable because the only traffic known to be moving through the Onion Router was coming from U.S. intelligence (Gingerich et. al 2014). Therefore, in order effectively to hide themselves, the U.S. opened the Onion Router to the public (Gingerich et. al 2014). With continued development and the publication of the article, “Tor: Second-Generation Onion Router,” by original Onion Router developers Roger Dingledine, Nick Mathewson, and Paul Syverson, the Onion Router evolved into a completely anonymous network that went by “Tor,” which stands for “the onion router” (Gingerich et. al 2014).

Though there is existing research into specific facets of the Dark Internet as well as its technical makeup, there still lacks substantial academic literature and research pertaining to the Dark Internet and its community of users as a whole, aside from the notable book “The Dark Net” by Jamie Bartlett, which explores various subcultures that have flourished through the lack of censorship present on the Dark Internet. It should be noted that the Dark Internet is a different entity than the Deep Web, which is well known and heavily researched. In particular, the Deep Web refers to a web server that cannot be found using typical search engines, such as Yahoo or Google (Everett, 2009). The Dark Internet, on the other hand, is composed of servers that are more difficult to connect to, requiring special browsers such as Tor (Everett, 2009). These special browsers are able to access any website available on the traditional Internet, but Dark websites cannot be accessed through the traditional Internet. While the difference between these two terms is minute, it is a key distinction to make, as it is the Dark Internet, in particular the Onion Network, that is the focus of our research. The Dark Internet in its entirety is a large forum of anonymous exchange in many forms and as it expands it will inevitably influence the future of society.

Innovations in technology have the ability to transform society as a whole because they enable new and innovative forms of human interaction. In order to predict and analyze how Dark Internet markets will impact society, research into its community as a whole must be done. Team DIRE plans to investigate how these markets affect current forms of exchange, tradewise and culturally, and how user participation is affected by major events.

**Crisis Response**

**Shutdown of Silk Road and Silk Road 2.0**

On June 1, 2011, an article was published that would soon draw much attention to the infamous “Silk Road” (Chen 2011). It was described as a hidden website on the Dark Internet where users can anonymously buy many drugs and services. First founded in February of 2011 by Ross William Ulbricht, then known under the alias of “The Dread Pirate Roberts”, the Amazon-like marketplace went relatively unnoticed by the mainstream public at first (Chen, 2011). However, revenues of the Silk Road rapidly grew and became responsible for over USD$1.2 billion in sales and USD$80 million in commision (2013, MarketWatch). Days after the article was posted, the Silk Road gained the attention of the Drug Enforcement Administration (DEA) and other law enforcement agencies.

Although the DEA requested to have the Department of Justice (DOJ) seize the website domain, as an operator on the Tor Network, it became difficult to trace. After over two years, it took the combined efforts of the DOJ, Federal Bureau of Investigations (FBI), DEA and other agencies to eliminate the Silk Road and arrest the owner, Ross Ulbricht. Simultaneous with Ulbricht’s arrest, the United States government attacked the Silk Road website itself. Throughout 2013, the Federal Bureau of Investigation seized thousands of bitcoin worth millions of dollars from Silk Road accounts, and ultimately shut down the entire website. The sudden seizure of the Silk Road created a crisis in search for new marketplaces for its faithful users.

While the FBI hoped that the shutdown would heavily diminish online drug sales, it appeared that the opposite had actually taken place. Led by a new pseudonymous Dread Pirate Roberts, administrators from the original Silk Road re-launched the site in November 2013 just a month after its shutdown (Buskirk et. al 2014). This revitalization was named Silk Road 2.0 with the same setup as the original, but also with the promise of improved security. The new site nevertheless had its share of turbulence, most notably in the form of vulnerability in the site’s “Refresh Deposits” function. As a result of this, $2.7 million in bitcoin were stolen in February 2014. Administrators were able to use their commissions on sales to refund hack victims, with 50 percent being completely repaid as of April 8. However, Silk Road 2.0 was eventually shut down a year after its development, as a result of efforts by US and European agencies. It's alleged administrator, who went under the pseudonym “Defcon”, was arrested, and additional markets such as Cloud 9 were also targets of this operation.

Once the Silk Road and Silk Road 2.0 were taken offline, several other online marketplaces stepped in to consume the displaced customer traffic. In an analysis conducted by Dolliver (2015), the Agora, Pandora, Evolution and The Cannabis Road online marketplaces showed the highest increase in traffic after the Silk Road shut down. In terms of the most prominent Tor Network marketplace to purchase drugs, Agora was the leading site.

**Agora Goes Offline**

Whereas the Silk Road and the Silk Road 2.0 were externally shut down by the U.S. Federal government, the shutdown of the Agora network was an internal decision. On August 26, 2015, Agora’s anonymous administrators announced on their site’s page and in the “darknetmarkets” Reddit forum that they will temporarily take their site offline due to a detection of “suspicious activity” on their servers. Because of the events surrounding the seizure of the Silk Road 2.0, the Agora admins claimed to have taken the site offline in order to increase the site’s anonymity and security. Even though the admins keep their online following updated through Reddit forums, they have not announced when the site will be relaunched.

When Agora was taken offline, the Dark Internet drug market took a major hit. Agora had become the largest site for drug trade with over 17,000 listings of drugs for sale (Dolliver, 2015). In a recent study conducted by Carnegie Mellon researchers, it was estimated that the Agora marketplace was making USD$150,000 a day in sales in February 2015 (Soska & Cristin, 2015). At this time, Agora was the second largest online drug trade site, only eclipsed by Evolution. However, after Evolution went offline in March 2015 due to its exit scam - stealing the buyers’ and sellers’ bitcoins - most of the market share shifted over to Agora (Soska & Cristin, 2015).

According to Christin (2015), during this lapse in major online marketplaces, other lesser known sites - such as Abraxas, Alphabay, and Nucleus - might attempt to pick up the customers. “I don’t know who will be the new crowned king, but people will pick up the pieces,” he says. “The demand is here and people aren’t going anywhere. They want their drugs and people will find ways of selling to them.” Christin also states that these events should be taken as a security reality check for all of the site owners and that “Tor is not a magic box that provides you a cloak of invisibility, Harry Potter style.”

**Current Traffic**

Due to the increased notoriety the original Silk Road has gained over the last few years, many Dark Internet users have stopped using the Silk Road brand. Only a month after the original Silk Road was seized in October of 2013, the Silk Road 2.0 was launched. The Silk Road 2.0 could be thought of as genuine because the original staff of the Silk Road (sans Ross Ulbricht) created it. However once the Silk Road 2.0 shut down, copycats (with no link to the original staff and community members) created the Silk Road Reloaded in early January 2015. This site was not hosted on the Tor Network, but rather another anonymous Dark Internet browser, I2P.

More recently, someone renamed a marketplace called Diabolus Market to the Silk Road 3.0 (Kushner, 2015). On the site’s homepage, it reads, “Welcome to Silk Road 3.0. We are an anonymous, professional and peaceful marketplace selling all sorts of goods and services. I am honored to welcome you to our community.” The site’s unnamed owner also decided to take the original moniker of the Silk Road’s owner and call himself Dread Pirate Roberts.

Even though the talk surrounding the arrests and seizures of the Silk Road and the Silk Road 2.0 increased the amount of traffic towards Dark Internet marketplaces exponentially (Christin, 2015), little interest has been shown in the new versions of the Silk Road. Over the past two years, consumers of the Dark Internet markets have been shaken by the cryptographic disruptions of nearly all of the popular online marketplaces. In the scramble of the Silk Road sites, Evolution and Agora shutdowns, many users have raced to lesser known sites such as Abraxas, Amazon Dark, Black Bank, and Middle Earth. Subsequently, all of these sites have been taken offline, likely as a product of their own exit scams (Reynolds, 2016).

Currently, the most prevalent marketplace, Alphabay, is not gaining any popularity among users. Members of Reddit’s “darknetmarkets” page and Alphabay’s Tor-protected user forums, accuse Alphabay of intermittently stealing users’ bitcoins. However, even with all of the marketplace chaos, the online traffic has not been deflected back to “street” dealers. Nicolas Christin, a computer science researcher from Carnegie Mellon states that the overall anonymous online drug trade fluctuates around USD$100 million a year regardless of government involvement or exit scams. The resilience of Dark Internet marketplaces demonstrates its value as a subject of academic research.

**Bitcoin.** The Dark Internet has a role in numerous economic innovations that are transforming online commerce. Bitcoin is one such development; invented by Satoshi Nakamoto in October 2008, it is a relatively new form of virtual currency (Nakamoto, 2008). Bitcoin is the first open-source, decentralized cryptocurrency ever created (Ong, 2015). Since its release in January 2009, Bitcoin has now emerged as a major form of capital in online marketplaces, with over 15 million bitcoins in circulation as of January 2016 (CoinDesk, 2016). One major reason that we have seen Bitcoin gain such popularity is because of its format: Bitcoin is a cryptocurrency, or an alternative to traditional government-issued money. It utilizes cryptography in order to ensure the security of online transactions, prevent users from spending the same digital notes more than once, and to govern and monitor the supply of these notes in circulation (Luther, 2013). It should be noted that Bitcoin is not the only cryptocurrency in circulation on online markets. Several competing currencies, such as Dogecoin and PotCoin, have been introduced over the years, but none have attained the same popularity as Bitcoin (Ong, 2015). The Silk Road, an anonymous online marketplace that could only be accessed on the Dark Internet, accepted Bitcoin as its sole exchange currency until it was shutdown in October of 2013 (Greenberg, 2013). Cryptocurrencies such as Bitcoin effectively allow international online trade to commence with ease, which has led to the creation of numerous marketplaces on the Dark Internet.

**Online markets.** By far the most famous of the Dark Internet’s marketplaces, the Silk Road was initially founded in February of 2011. Its operator then went by the alias of “The Dread Pirate Roberts”, and was already well known for possessing strong libertarian and anti-regulation viewpoints. The site acquired notoriety only a few months after its founding, when the blog Gawker featured it in an article that emphasized its potential for drug purchasing and trafficking. Not long after this shot of publicity, the U.S. Government began a campaign to shut the website down, and ultimately arrested several drug dealers and purchasers who had been operating through the Silk Road. In October of 2013, the U.S. Department of Justice arrested a San Francisco man named Ross William Ulbricht, alleged to be the true identity of “The Dread Pirate Roberts”. As of this writing, Ulbricht has confessed to none of the charges the federal government has brought against him; his trial is currently scheduled for January of 2015. Simultaneous with Ulbricht’s arrest, the United States government attacked the Silk Road website itself. Throughout 2013, the Federal Bureau of Investigation seized thousands of bitcoin worth millions of dollars from Silk Road accounts, and ultimately shut down the entire website.

While the FBI hoped that the shutdown would heavily diminish online drug sales, it appeared that the opposite had actually taken place. Led by a new pseudonymous Dread Pirate Roberts, administrators from the original Silk Road re-launched the site in November 2013 just a month after its shutdown. This revitalization was named Silk Road 2.0 with the same setup as the original, but also with the promise of improved security. The new site nevertheless had its share of turbulence, most notably in the form of vulnerability in the site’s “Refresh Deposits” function. As a result of this, $2.7 million in bitcoin were stolen in February 2014. Administrators were able to use their commissions on sales to refund hack victims, with 50 percent being completely repaid as of April 8. However, Silk Road 2.0 was eventually shut down a year after its development, as a result of efforts by US and European agencies. It's alleged administrator, who went under the pseudonym “Defcon”, was arrested, and additional markets such as Cloud 9 were also targets of this operation. Although law enforcement agencies sought to publicize their success, numerous other prominent markets such as Evolution were unaffected, likely due to the professionalism of their operations as well as more advanced security. Agora already contained more listings than Silk Road 2.0 before the shutdown, with Evolution also expected to overtake Agora. Since then, Agora has also shut down of its own accord before receiving action by the FBI in order to avoid compromising the personal information of its users.

**Significance.** The 21st century has been a time of exponential acceleration in the growth of technology. These developments include many tools and resources that can improve societies through a wider spread of new knowledge or advanced cyber security. Nevertheless, the amount of information that we are lacking is far greater than the information that we know and comprehend. The Dark Internet consists of 5-25% of the total net - depending on who was asked- and has been increasing at the rate of about 2% each year (Everett, 2009). To date, there are few individuals (including government officials) that thoroughly comprehend the concept of the Dark Internet. The gap in knowledge and current information surrounding the Dark Internet unnerves society and prevents its potential benefits from being explored and exploited thoroughly. For these reasons, it is important that our team research the sociological and cultural interactions of the Dark Internet, especially as it becomes more relevant to daily life.

It is important to note that there are varying levels of awareness of the Dark Internet: (1) people who are completely unaware of its existence, (2) those who might only know facts about it through what has been said throughout the news or when it has been referenced in pop culture, and (3) those that have an in-depth familiarity with the Dark Internet who use it regularly. The obstacle that society needs to overcome is their lacking of general knowledge of the Dark Internet. The media mainly focuses on the darker side of the Dark Internet--the side that contains illegal pornography, black market trading and terrorist activity. Despite these criticisms, there are copious amounts of legal reasons that draw people to utilize the Dark Internet, such as personal online security and anonymity.

One of the fundamental reasons civilians use the Dark Internet is to ensure personal online security (Dingledine et al., 2006). It is a common desire held by individuals to keep their usage on the Internet free from tracking, however, this does not necessarily mean these users are participating in illegal acts. For example, there are times when someone needs to reveal vital information about potentially dangerous parties. These situations can include an individual acting as a “whistleblower” speaking up against his or her corporation, or even a criminal informant divulging information to a journalist.

Websites such as *The New Yorker*’s Songbox, allow users to exchange secure information without the fear of being tracked (Aked et al., 2013). However, the United States government has demanded control and/or unlimited access to these websites, to ensure privacy and protection of their assets. A momentous example of a recent exchange of secure information was when a former National Security Agency (NSA) subcontractor, Edward Snowden, published mass surveillance programs run by the NSA and the Government Communications Headquarters (GCHQ). Although Snowden later revealed himself to be the source of the leak, he was able to anonymously report information that revealed concerns about domestic surveillance and information security.

Higher authorities are not the only reasons why users might feel as though they are in danger: another major use of the Tor browser is to prevent third parties from discovering individual activity. This is essential for victims of domestic abuse or stalking to achieve a greater level of security from threats. Through anonymity achieved by the use of the Tor Network, victims are able to use the Internet safely without being tracked by potential assailants.

Many people use the Dark Internet as a crucial tool to allow one to safely bypass the censorship that oppressive governments impose on their people. However, the Great Firewall of China (GFC) prevents Chinese users from accessing the public Tor network (Winter & Lindskog, 2012). The chances of bypassing the GFC are minuscule, meaning that those who choose to utilize the Internet are forced to sacrifice their privacy. Personal safety, Internet security and censorship bypass are among many significant examples of how the Dark Internet can be exploited to benefit the general public.

**Gaps in Current Research**

Despite numerous advances in the Dark Internet’s popularity and mainstream usage, specific parts of it remain a great mystery to most. In particular, bitcoin usage and the marketplaces on the Dark Internet continue to suffer from lack of study. Further research is required in order to provide documentation for information and make it readily available. This needs to be done so its potential benefits can be exploited, and possible threats avoided or mitigated. The mystery surrounding these specific parts of the Dark Internet, from the average person’s perspective, is not unwarranted, as gaps in existing research of these specific parts leave knowledge on the topic with many unanswered and unexplored questions.

The Dark Internet’s massive amount of data has proven to be challenging for researchers to explore and exploit due to technical challenges that arise when attempting to locate, access, and index available Dark Internet data (Rocco et al., 2005). Various specialists have explored the development of possible research tools, which would enable any web-based information-seeking individual to be able to navigate the Dark Internet with ease in order to gain access to the vast masses of data available and determine the relevant data of their choosing. Prototypic methods of achieving these aims have been developed, such as the DynaBot, which aims to circumvent the difficulties experienced while operating under the Dark Internet by a systematic method of matching, probing, and ranking discovered sources (Rocco et al., 2005). The DynaBot, which utilizes a service class description-matching module and a source-based analysis module for probing and ranking, still requires further research devoted to its enhancement in order to successfully operate as an efficient method of Dark Internet data extraction, data which includes but are not limited to: news-related information made unavailable by government or corporate censorship, political discussion, and access to online markets. Increased ease and accessibility to data of the individual user as the result of some developed information-sorting method would likely result in a great increase in Dark Internet usage, allowing more people to access information that remains unavailable on the public Internet.

Our team will attempt to fill a crucial gap in the current research of the Dark Internet by analyzing the use of Bitcoin and other cryptocurrencies and their overall effectiveness and usage among online marketplace users. As of right now, significant studies have already been conducted on bitcoin and their value. We plan on building off of these studies in order to create new knowledge specifically on how bitcoin affect transactions on the Dark Internet. All transactions on Dark Internet Marketplaces require that some type of cryptocurrency be used instead of recognized currency, and there is a lot to be researched on how this affects the large amount of transactions that occur daily on the Dark Internet.

Although previous research has been done to analyze specific groups of people such as the case study done on cyber terrorism (Chen et al., 2008), our group could adapt this research in order to study the exact groupings of individuals who use the Dark Internet and also establish knowledge in the public about the topic and use by the general public. Pre-existing analyses of different (but similar) online marketplaces such as the Silk Road could be taken advantage of as resources to adapt to our research goals of understanding how different levels of anonymity affect the behaviors of users on the Dark Internet. In order to take it one step further, we can compare the user interactions of Dark Internet marketplaces to other competitive online marketplaces such as Amazon to see how behaviors on the Dark Internet vary from the public Internet where there is no anonymity at all in order to create a bridge between the Dark and public Internet (Christin, 2012).

Textual analysis of communication on the Dark Internet can be directly compared to communication using conventional browsing. In addition, we can gain knowledge on the communication norms of Dark Internet communities. As a prominent example, marketplaces such as the Middle Earth have thriving forums where users can congregate to discuss the site, its services, and other activities specific to the Dark Internet.

Additional gaps in research (that are not solely exclusive to the Dark Internet) exist due to the fact that interactions are taking place over a digital medium. One of these major differences between online and face-to-face communications is the lack of a shared physical area where interaction takes place. This results in the changing of social boundaries, such as the difference between personal and mass communication or the distinction of time at home as separate from time at the office. Users can post messages in secure private locations, but can communicate on an open public message board. This hybridization of the public and private spheres (Arendholz, 2013) creates new social spheres separate and apart from real life contexts. The nature of online communication enables people to feel anonymous but also connected to a heterogeneous global village. Since users feel that their interactions cannot be traced back, they can communicate on a personal level to a completely anonymous public. This is also a result of the ease in registering or leaving online communities, which makes online communication perceived as having less social obligations. However, people that consider themselves part of a close electronic community , affecting their behavior online.

**Potential Impact**

The Dark Internet has become a prevalent global topic and has received a substantial increase in attention by major news outlets almost daily, especially as it pertains to the development of online cryptocurrencies. The bitcoin’s emergence as the most widely used form of cryptocurrency has lead to various developments in the Dark Internet; copious amounts of drugs and other illicit materials have been bought on Dark Internet Marketplaces using bitcoins (Levin et al., 2014). Those who profited off of selling these illegal goods have been able to then successfully launder their profits on the Dark Internet using bitcoins. Despite the illegality of much of the online commerce conducted through the use of the bitcoin, the cryptocurrency is projected to continue to grow in popularity and widespread usage (Darlington, 2014). For instance, during his 2016 presidential campaign, Republican presidential candidate Rand Paul accepted donations in the form of bitcoins (Lichtblau, 2015).

It is not simply the development of the bitcoin that has brought attention to the Dark Internet; the wide variety of innovative ways for which the Dark Internet can be used has given it a major boost in media attention. For example, the 2016 Golden Globe winning television series *Mr. Robot*, has made constant reference to the existence of the Dark Internet throughout its first season. Additionally, Dark Internet marketplaces have seen a steady increase in users as of recently. After the FBI raid of the original Silk Road, the number of sellers on Silk Road doubled after six weeks following the release of Silk Road 2.0 (Buskirk et al., 2014). As the Dark Internet continues to develop and expand, the number of overall users and different applications of it will most likely increase. Significant academic researched conducted on the Dark Internet could possibly hold value in both the academic and public world. Now is the opportune time for our team to capitalize on the current situation and conduct an in-depth research study dedicated to the Dark Internet, as it still remains a new and enticing topic to most.

The research being done by this team additionally holds the potential to open doors to other areas of research into the culture of the Dark Internet. Our research can establish how the culture of the Dark Internet proceeds in the forums that we gather data on, but in order to truly establish the culture of the Dark Internet, we will need to rely on the expansion of our project by future researchers.

**Conclusion**

The Dark Internet is a forum for anyone who wishes to maintain privacy and anonymity within the cyber world. It is a steadily growing innovation used for the distribution of information, market transactions, and cultural connectivity, not unlike the public Internet. The distinction between the two is that all these actions may be done in complete privacy of the user on the Dark Internet, which makes all the difference, as people are prone to behave much differently under the cover of anonymity. Consequently, studying the Dark Internet can enable our team to view an altered subculture in which people engage in discussion and commerce unlike anywhere else, as many are completely comfortable in their ability to do or say whatever they want without fear of retribution. As Dark Internet usage expands, its shadowy culture that appears foreign and mysterious to us now may soon become customary and indisputably affect society. Therefore, it is of the utmost importance to study the Dark Internet and its users as it stands in order to enable our team to draw conclusions and make inferences about the culture as a whole and forecast its future impacts on our society.