# A DEEP DIVE INTO THE DARK WEB

CS625 Business Data Communication and Networks

Final Term Project | Spring 2019

By Alisha Peermohamed

## Table of Contents

# A Deep Dive into the Dark Web

CS625 Final Project: Spring 2019

Alisha Peermohamed

## I. Introduction: The Web as We know it and What lies Beyond

Most of us today thoroughly rely on the internet. Whether it is to navigate the fastest route on google maps, chat with friends on social media, purchase our groceries from Amazon Fresh, or even access our financial information through online banking portals. People use and trust the internet blindly to carry out many of life's essential activities. With only 1 website in 1991 to over about 1.9 billion websites today[1], the internet has been growing to all corners of the earth at a rapidly exponential rate. As of March 2019, over 4.3 billion people access to the world wide web for myriads of activities[2]. We believe the internet is so vast that you could practically find anything on there as it continues to document information and provide services for us. Yet, what we see is actually only the tip of the iceberg – it is the surface web (As shown in Figure 1). In reality the World Wide Web has several layers beneath, including the deep web and the dark web. This paper will take a deep dive on the deepest part of the internet iceberg: The Dark Web, notoriously known as the 'Criminal's playground', where underground activities such as terrorist communications, illicit drug trafficking, and several other illegal transactions regularly take place.

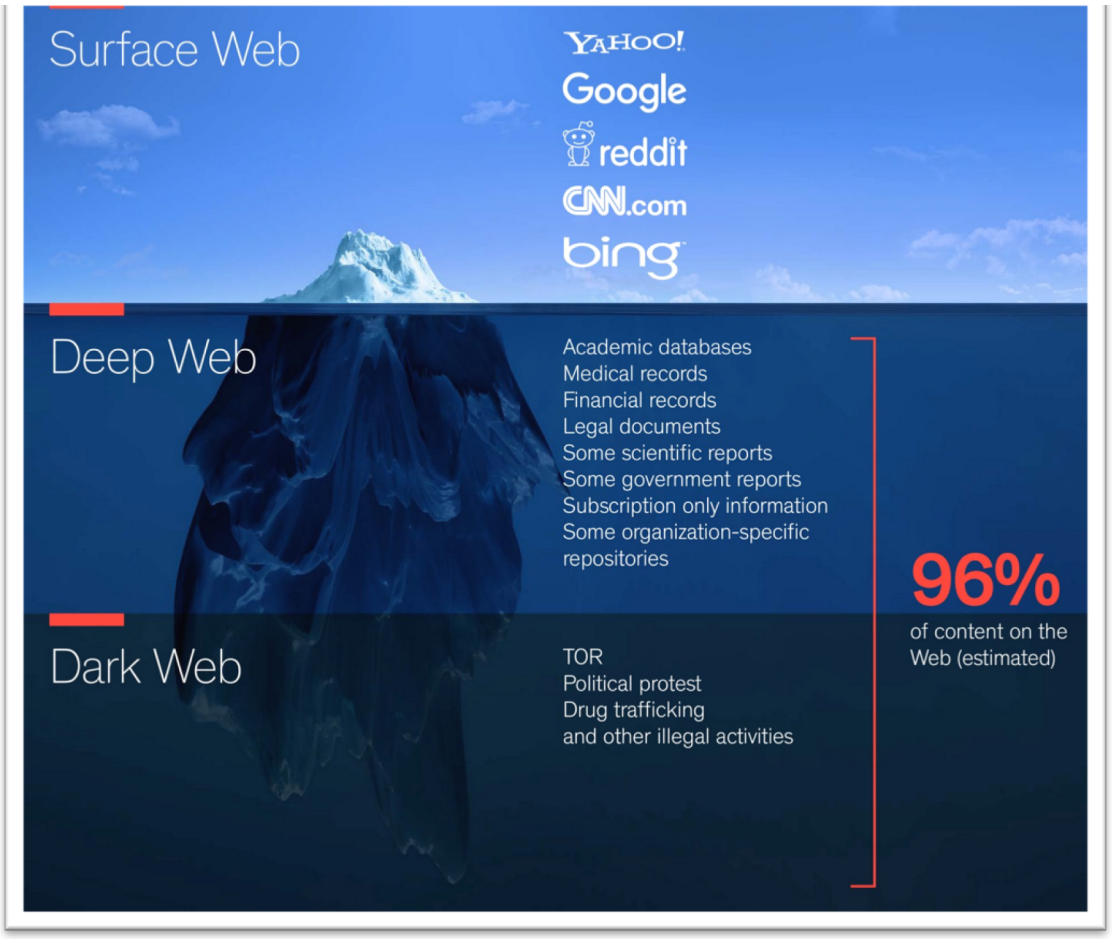
### Background on the World Wide Web:

The World Wide Web is composed of three primary layers: The Surface web, the Deep web, and the Dark web: **The Surface Web** (also known as the Clear Net) is any website that can be found using search engines, such as Google and Yahoo!. This would be your Google maps app, searches on

[1] Liedke, Lindsay. 2019. "100+ Internet Statistics & Facts For 2019 You Should Know About". *Website Hosting Rating*. https://www.websitehostingrating.com/internet-statistics-facts/

[2] "World Internet Users Statistics And 2019 World Population Stats". 2019. *Internetworldstats.Com*. https://www.internetworldstats.com/stats.html

*Figure 1: The Internet Iceberg*
*https://cdn-images-1.medium.com/max/1600/1*cr-gQUcV5TQLU83ZWdNVPA.jpeg*




Wikipedia, and public databases. It constitutes the hundreds of indexed websites and apps publicly accessible to everybody and can be discovered using search engines[3]. To briefly touch upon how search engines work: Search engines, such as Google and Yahoo!, use web crawlers, which are basically internet bots or web spiders, to find content and websites that are new or different to the internet. These web spiders periodically 'crawl' an already known web page and build an index on their search engine server of the words on a page: their content, organization and where to find it on that webpage. The web crawler then visits all the hyperlinks on that page to extract and discover new webpages it may not have

[3] "What Is Surface Web, Deep Web And Dark Web?". 2019. *Medium*. https://medium.com/@hackersleague/what-is-surface-web-deep-web-and-dark-web-cdbaf71b30d5

already found and loads that webpage's content into its search engine index as well[4]. Page by page, search engines are able to track and index all the webpages that 'want' to be discovered by everyone in the public, and form the 'Surface' Web. Since they are public, all surface web sites are under high constant surveillance by the government and include websites such as Youtube.com, CNN News, or Amazon.com. This is the portion of the ice-berg above the water. Although it appears massive to us, spanning over 20 Terabytes of information, it is actually a very small portion of the entire ice-berg. In fact, the surface web constitutes only 4% of the entire world wide web[5].

**The Deep Web** is, by definition, the collection of websites that are not accessible to the public by means of search engines and is estimated to constitute 96% of the entire internet, nearly 500 times larger than the surface web[6]. The deep web includes 2 types of websites: The first, websites with privacy protection – These are websites that are password protected for safety or privacy such as your online financial banking account, your personal email account, your Wall Street Journal subscription, subscription based online libraries, or classified databases. Second, websites that are not hyperlinked and thus cannot be reached by search engines. As mentioned above, web crawlers can only 'find' a website if they come across its hyperlink on another website. If a website is not hyperlinked, search engines will not be able to find it. This does not mean these websites are 'off limits' to users. Users may still access the website publicly if they have its exact URL[7]. An example of such a website may be an organization's intranet system, an online database that may requires digging through that organization's website to access, or

4 "How Does A Web Crawler Work? - Wp Themes Planet". 2019. *Wp Themes Planet*. https://www.wpthemesplanet.com/2009/09/how-does-web-crawler-spider-work/
5 "What Is Surface Web, Deep Web And Dark Web?". 2019. *Medium*. https://medium.com/@hackersleague/what-is-surface-web-deep-web-and-dark-web-cdbaf71b30d5
6 Rowe, Adam, and Adam Rowe. 2019. "What Is The Deep Web And How Can You Access It?". *Tech.Co*. https://tech.co/news/what-is-the-deep-web-2018-05
7 "Clearing Up Confusion - Deep Web Vs. Dark Web - Brightplanet". 2019. *Brightplanet*. https://brightplanet.com/2014/03/clearing-confusion-deep-web-vs-dark-web/

various community groups (A reading group's secret Facebook group). Although the deep web is commonly mistaken for the dark web, its uses are heavily integrated in our day-to-day internet use and for the most part, are perfectly legal. The exact size of the deep web is difficult to measure accurately as a majority of the information is restricted from public users and inside databases.

Finally, the last layer of the Internet, **The Dark Web** is a portion of the Deep Web. It lies at the lowest point of the iceberg at the bottom of the internet's deep abyss. While the dark web only actually constitutes about 0.03% of the World Wide Web, it is notorious for its ability to provide a secure platform where users may communicate anonymously without having to worry about government surveillance and regulations. The dark web can only be accessed using specific software, such as the Tor network, I2P, or Freenet[8]. Essentially, these software mask user identities and locations by bouncing their address requests through multiple distributed network clients and encrypting their IP source addresses at each stop before it reaches its final destination. This process wraps each transmission into multiple layers of encryption, thereby making it very difficult (but not impossible) to decrypt the user's IP source address. Neither are users able to narrow in on other users' IP address, nor are the websites that users visit or browse[9].

While the dark web is growing in popularity as an attractive and relatively safe platform to browse the web whilst maintaining user privacy, it is now also nefariously being used as a platform for underground and 'hush' transactions including the smuggling and trade of illegal drugs, arms and ammunitions, financial data, terrorist communications, hired assassinators, and illicit pornography. Since all of these activities would be subject to intervention on the Surface Web, they are executed over the Dark web where users may completely mask their identity. The primary payment for transactions is

[8] "The Dark Web & Deep Web: How To Access The Hidden Internet Today". 2019. *Digital.Com*. https://digital.com/blog/deep-dark-web/.
[9] "The Tor Network - FAQ". 2019. *Wordfence*. https://www.wordfence.com/learn/the-tor-network-faq/

through the use of popular cryptocurrency, Bitcoin[10]. Throughout this paper, we will take a deep dive on the Dark Web's History and Establishment, Technologies and Software, Popular Usages, and Future outlooks for the Dark web.

## II. History and Establishment

The Early days of the internet and the Growing Need for an Uncensored Web:

In the early days of the public internet, the 1990's, every site was publicly indexed, every email address recorded and government regulations tightly tracked and screened all message transactions. The World Wide Web was available, yet central authorities could easily identify who was sending what information and to whom. This led to the beginnings of the Dark Web. In 1995, members of the US Naval Research Laboratory: Paul Syversion, David Goldschlag, Mike Reed, developed the first prototype of the Onion Router. The Onion Router is the primary routing technology that facilitates the functionality of the dark web and is known for its layered IP encryption technology[11]. We will go into how these technologies work in greater detail later on in the paper. Initially, the primary purpose was only to permit US government agencies to scan sensitive information in foreign countries without being discovered and to help the US Military communicate with field agents internally[12]. In 1997, the US Defense Advanced Research Project Agency joined in to provide funding for Onion Routing and the technology was later patented in May 1998 by the US Secretary of Navy[13]. The official public patent can be found here.

Later in 2002, Roger Dingledine and Nick Matthews, both recent MIT graduates at the time, began working with Paul Syversion (a member of the US Naval Research Lab) to further develop the

[10] Naseem, Iflah, Ashirr K. Kashyap, and Dheeraj Mandloi. "Exploring Anonymous Depths of Invisible Web and the Digi-Underworld." *International Journal of Computer Applications (0975 – 8887)*: 21-24.
[11] "The Tor Project | Privacy & Freedom Online". 2019. *Torproject.Org*. https://www.torproject.org/about/history/
[12] "The US Government Has Been Funding the Gateway to the Dark Web." Home. November 05, 2017. Accessed April 28, 2019. https://www.thesiriusreport.com/technology/us-government-funding-gateway-dark-web/.
[13] Dark Web Academy, "History of the Dark Web/Deep Web," YouTube, March 26, 2016, , accessed April 28, 2019, https://www.youtube.com/watch?v=kPkKGzPTqGU

Onion Router project. To distinguish it from other projects, they called it the Tor Project, which stands for 'The Onion Router' project[14]. While the primary purpose was still to allow the secret exchange of information within the US government, they realized "the more people using the system, the harder it would be to separate a government's own messages from the general noise. You can't be anonymous on your own."[15]. Thus, in 2003, the team launched the Tor browser publicly as open source, establishing the first public platform for the Dark web[16]. Still today, Tor is the most commonly used software to access the Dark web where users may browse the web whilst masking their identity.

In 2004, the Electronic Frontier Foundation (EFF) began funding the Tor project[17]. EFF is a non-profit organization that fights for the civil liberties of users on online platforms, especially for emerging technologies. They are seen as an independent voice to ensure that the rights of users are preserved as new technologies are established. Naturally, as strong proponents of 'open source software, encryption, security research, … fight[ing] illegal surveillance and freedom-enhancing technologies'[18], EFF took a keen interest in maintaining and managing the Tor Project. Later in 2006, the Tor Project, Inc. filed as a 501(c)3 non-profit organization and rapidly started to garner attention and users[19].

## Rise of the Dark Web's Nefarious Reputation

It was only in 2008 when Satoshi Nakamoto created Bitcoin that made payment based transactions possible on the Dark web and gave rise to the numerous illegal transactions that the Dark web is known for today[20]. As a brief overview, Bitcoin is one of the most popular decentralized cryptocurrencies used

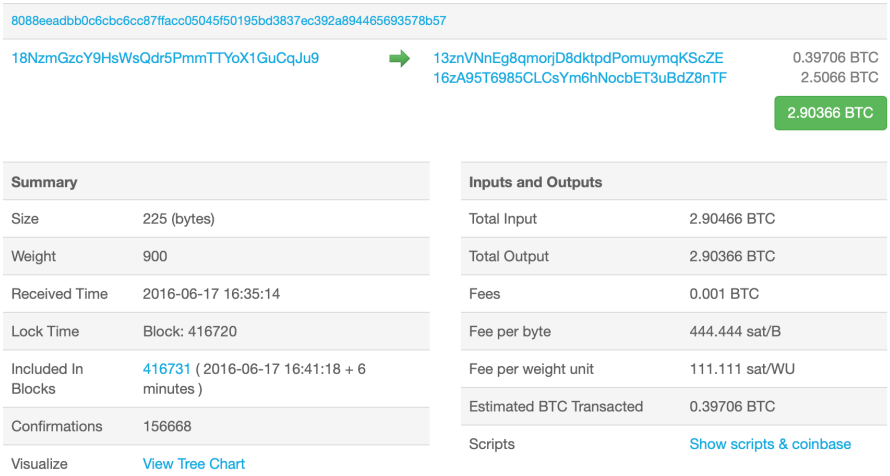
[14] "The Tor Project | Privacy & Freedom Online". 2019. *Torproject.Org*. https://www.torproject.org/about/history/
[15] "What Is The Dark Web And Is It A Threat?". 2019. *BBC Guides*. http://www.bbc.co.uk/guides/z9j6nbk
[16] "The Tor Project | Privacy & Freedom Online". 2019. *Torproject.Org*. https://www.torproject.org/about/history/
[17] Ibid
[18] "A History Of Protecting Freedom Where Law And Technology Collide". 2019. *Electronic Frontier Foundation*. https://www.eff.org/about/history
[19] "The Tor Project | Privacy & Freedom Online". 2019. *Torproject.Org*. https://www.torproject.org/about/history/
[20] McCormick, Ty. "The Darknet: A Short History." Foreign Policy. December 09, 2013. Accessed April 28, 2019. https://foreignpolicy.com/2013/12/09/the-darknet-a-short-history/

for payments of electronic transactions. Bitcoin transactions are executed without the need for a central regulatory authority through the use of Blockchain technology. Essentially, before a transaction is executed, each transaction is required to be verified by bitcoin 'miners' on the peer-to-peer network. Miners are essentially distributed users that voluntarily provide services to maintain and operate Bitcoin's payment technology. Once a transaction is confirmed, it is recorded in a universal and permanent Blockchain ledger, which is a publicly accessible database of all transactions ever occurred[21]. The process of verifying and recording each transaction upholds the integrity of the currency and eliminates the need for a central authority: each user can check their remaining balance in their 'Bitcoin wallet' and future transactions can be verified to ensure that the cryptocurrency has not been digitally copied or fraudulent. Like any currency, Bitcoin is a medium of exchange of goods, it holds no intrinsic value, no physical shape, but functions on the integrity of Blockchain technology[22].

So how does Bitcoin fuel illegal transactions on the Dark Web? By nature, the dark web protects users from government eavesdropping. This means there are no laws to ensure the trust and quality of good exchanges on the dark web. Bitcoin and Blockchain technology, on the other hand, solve this problem by providing a secure medium to exchange goods whilst keeping the seller and buyer identities anonymous: Each Bitcoin transactions, as recorded on the Blockchain ledger, only indicates the number of bitcoins exchanged, the sender address and the receiver address[23]. Please see an example of a bitcoin transaction shown in a blockchain ledger shown in Figure 2. No Personal information about neither the sender nor receiver is given:

[21] "How Does Bitcoin Work?" Bitcoin. Accessed April 28, 2019. https://bitcoin.org/en/how-it-works.
[22] PricewaterhouseCoopers. "Making Sense of Bitcoin, Cryptocurrency and Blockchain." PwC. Accessed April 28, 2019. https://www.pwc.com/us/en/industries/financial-services/fintech/bitcoin-blockchain-cryptocurrency.html.
[23] "Transaction View Information about a Bitcoin Transaction." Bitcoin Block Explorer and Currency Statistics. Accessed April 28, 2019. https://www.blockchain.com/btc/tx/8088eeadbb0c6cbc6cc87ffacc05045f50195bd3837ec392a894465693578b57

*Figure 2: Sample Bitcoin Transaction*
*https://bit.ly/2UHLyx2*



8088eeadbb0c6cbc6cc87ffacc05045f50195bd3837ec392a894465693578b57

| | | |
|---|---|---|
| 18NzmGzcY9HsWsQdr5PmmTTYoX1GuCqJu9 | 13znVNnEg8qmorjD8dktpdPomuymqKScZE | 0.39706 BTC |
| | 16zA95T6985CLCsYm6hNocbET3uBdZ8nTF | 2.5066 BTC |
| | | 2.90366 BTC |

| Summary | |
|---|---|
| Size | 225 (bytes) |
| Weight | 900 |
| Received Time | 2016-06-17 16:35:14 |
| Lock Time | Block: 416720 |
| Included In Blocks | 416731 ( 2016-06-17 16:41:18 + 6 minutes ) |
| Confirmations | 156668 |
| Visualize | View Tree Chart |

| Inputs and Outputs | |
|---|---|
| Total Input | 2.90466 BTC |
| Total Output | 2.90366 BTC |
| Fees | 0.001 BTC |
| Fee per byte | 444.444 sat/B |
| Fee per weight unit | 111.111 sat/WU |
| Estimated BTC Transacted | 0.39706 BTC |
| Scripts | Show scripts & coinbase |

Bitcoin was the first trailblazer in enabling transactions on the Dark web and accounted for 47% of transactions on the dark web at its peak[24]. However, recently, researchers at Qatar University have been able to unmask users' identity by tracking the sender address through several transactions on the public ledger and linking them to public accounts on forums such as BitcoinTalk: 'More disturbingly, 22 were payments to the Silk Road. Though they don't reveal many personal details of those 22 individuals, the researchers say that some had publicly revealed their locations, ages, genders, email addresses, or even full names.'[25]. Consequently, several other cryptocurrencies are rising to safely and anonymously exchange goods, including: Monero, Litecoin, & Dash[26]. The introduction of Bitcoin sparked a new generation of Dark web users who use the currency for the trade of illegal services and commodities, including the sale of illegal drugs, hired assassinators, prohibited pornography, illegal arms, and of fake passports or credit cards. Thus, giving the Dark Web it's notorious reputation as the 'Terrorist's Safe Haven'.

[24] DashMagazine. "Immunity on the Dark Web as a Result of Blockchain Technology." Codeburst. June 19, 2018. Accessed April 28, 2019. https://codeburst.io/immunity-on-the-dark-web-as-a-result-of-blockchain-technology-6693eb087bdd
[25] Greenberg, Andy. "Your Sloppy Bitcoin Drug Deals Will Haunt You for Years." Wired. February 01, 2018. Accessed April 28, 2019. https://www.wired.com/story/bitcoin-drug-deals-silk-road-blockchain/.
[26] DashMagazine. "Immunity on the Dark Web as a Result of Blockchain Technology." Codeburst. June 19, 2018. Accessed April 28, 2019. https://codeburst.io/immunity-on-the-dark-web-as-a-result-of-blockchain-technology-6693eb087bdd

## Who is Funding the Dark Web?

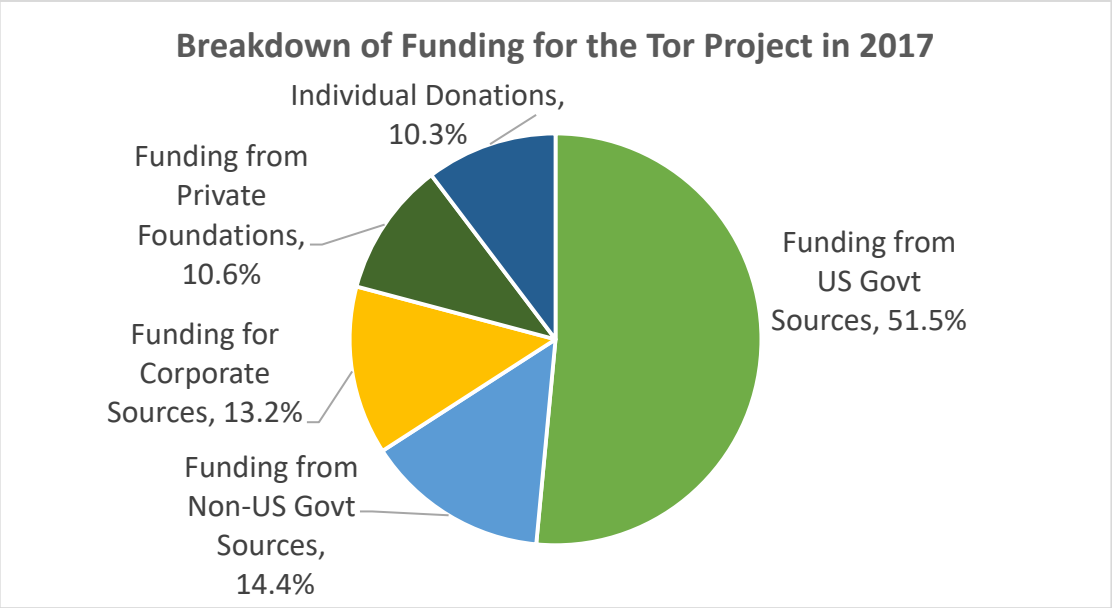
Now you might ask, given these illegal activities and lack of government surveillance, why hasn't the Dark Web been shut down and who is still funding the dark web? Interestingly, as of 2017, the United States government still provides majority funding for the Tor Project and is the organization's largest supporter. Please find a detailed breakdown of the Tor Project's total funding for 2017 based on its 2017 IRS Form 990 Report, their latest publicly released report in the Table 1[27]. Figure 3 also shows a breakdown of each category by percentage. The US Government still funds 51.5% of total Tor funding. Other interesting sources are the Swedish Government (14.4%), Mozilla, and DuckDuckGo. The main reason why organizations, such as the US government, continue to support the Tor Project and the dark web, is that the it provides a platform where individuals may anonymously (and thus freely) express opinions, exercise their fundamental human rights, and speak against oppression whilst maintaining anonymity[28]. The benefits to the Dark Web are many and more clearly delineated in the next section.

Table 1: The Tor Project 2017 Funding Sources:

| Source | Amount Funded |
|---|---|
| **Funding from US Government Sources:** | |
| US State Dept – Bureau of Democracy, Human Rights, and Labor | $133,061 |
| National Science Foundation | $548,151 |
| SRI International | $635,504 |
| Radio Free Asia/Open Technology Fund | $798,029 |
| ISC Counterpart International | $12,500 |
| **Funding from Non-US Government Sources** | |
| Swedish International Development Corporation Agency (SIDA) | $594,408 |
| **Funding from Corporate Sources** | |
| Mozilla Foundation | $522,188 |
| DuckDuckGo | $25,000 |
| **Funding from Private Foundations** | |
| New Venture Fund | $347,325 |
| Other Private Foundations | $89,007 |
| **Individual Donations** | $425,709 |
| **Total** | **$4,130,882** |

[27] "The Tor Project | Privacy & Freedom Online." Torproject.org. Accessed April 28, 2019. https://www.torproject.org/about/reports/
[28] Dark Web Academy, "History of the Dark Web/Deep Web," YouTube, March 26, 2016, , accessed April 28, 2019, https://www.youtube.com/watch?v=kPkKGzPTqGU

*Figure 3: Funding for the Tor Project 2017*




## Benefits of the Dark Web

While the Dark web may be known as the Criminal's playground, it offers valuable benefits for users that may be oppressed or wish to communicate anonymously. **Whistleblowers and Journalists** often use the Dark web as a platform to anonymously reveal fraudulent activity within government or private organizations and to report a news story. Not only do Whistleblowers put their lives, finances, physical safety, and well-being at risk but also those of their family and loved ones. The Dark web offers several dedicated whistleblower websites called anonymous forums, the most famous being WikiLeaks and Dead Man Zero, where whistleblowers or journalists may share tips or stories. If a story appears to have credibility, it eventually spreads till it reaches the hands of mainstream media. Additionally, major media sites, such as The New York Times and The Guardian, have also developed onion sites (dark net websites) where users may leave tips anonymously[29].

[29] "How Whistleblowers Use the Darknet for Good." Dark Web News. February 27, 2018. Accessed April 28, 2019. https://darkwebnews.com/dark-web/how-whistleblowers-use-the-darknet-for-good/

**Resistance fighters** and **human rights activists** in oppressive regimes may also use the Dark Web as a medium of anonymous communication with the outside world. For example, the Dark Web had a prominent role in facilitating communication during the Arab Spring in 2011. When repressive Egyptian president, Hosni Mubarak had censored several media websites on the clear net, activists and journalists used the Tor browser to communicate with Tunisia and Libya to set the Arab Spring into motion[30]. The Dark web is also frequently used in countries with limited or completely restricted access to the clear net, such as North Korea and Russia. Users in China use the dark web to access foreign (but perfectly legal) websites that are blocked by the 'Great Firewall'; websites such as Facebook, Youtube, and the New York Times[31].

**Private Organizations** and **Governments** are also one of the most frequent users of the Dark web. Just as the Dark Web was founded by the US Naval Research Lab to facilitate private communication between the US military, private organizations and governments now use the dark web as a secure platform to communicate without government eavesdropping and to store databases of private or censored information[32]. Lastly, the dark web provides a secure place for **everyday users** to browse sensitive topics on the web and express their opinion without government eavesdropping.

## III. The Tor Project – The Foundational Backbone Behind the Dark Web

### General Overview

The Tor Project, short for 'The Onion Router', was developed in 2002 as one of the first platforms for the Dark Web where users could browse and communicate on the internet without revealing their identity or location. It has since become the foundational backbone behind the Dark Web as the most

[30] Peace and Conflict Monitor, Tor, Anonymity, and the Arab Spring: An Interview with Jacob Appelbaum. Accessed April 28, 2019. http://www.monitor.upeace.org/innerpg.cfm?id_article=816
[31] Cox, Joseph. "What Firewall? China's Fledgling Deep Web Community." Motherboard. February 25, 2015. Accessed April 28, 2019. https://motherboard.vice.com/en_us/article/d735aa/what-firewall-chinas-fledgling-deep-web-community
[32] Sameeh, Tamer. "Research: Threats Vs Benefits of the Deep and Dark Web." Deepdot.web. October 28, 2018. https://www.deepdotweb.com/2018/10/28/research-threats-vs-benefits-of-the-deep-and-dark-web/

popular software used to access the dark web using the onion routing technology on a peer-to-peer routing structure[33]. The Tor Browser itself is a modified version of Mozilla Firefox and is used as a proxy to communicate and browse the web for regular browsers. So, its interface is not any different to use than a regular browser such as Google Chrome or Safari[34]. Additionally, the Tor network is not for the exclusive use of the Tor Browser. Other applications may also connect to the Tor network using the SOCKS protocol, although complete anonymity is not guaranteed. The Tor Browser was created by the Tor Project in 2008 to increase usability and ease for their less tech-savvy users. Users may also use the Tor Browser to access sites on the Clear Net as well as those exclusively on the Dark net. The only difference is that Tor processes all requests using the Tor Network[35].

The Tor Network is a collection of over 7000 volunteer computer servers distributed around the world[36]. Using the Onion Router technology, each user request is wrapped in multiple layers of encryption as is bounced through several computer servers on the Tor network. At each server, a layer of encryption is pealed until the request reaches its final destination, just like the layers of an onion[37].

## Onion Routing

Let's walk through an example of how a user sends a transmission over the Tor Network using Onion Routing. Suppose a user wishes to connect with a web server using Tor, the source computer will first establish a connection with a Tor server requesting a list of all available nodes (also called Relays) on the Tor Network. Each node or relay is a volunteer computer server or device which helps to form the Tor Network. There are currently over 7000 Tor nodes on the Tor network and any computer or routing

[33] "What Is Tor - How Does Tor Work - How to Use Tor." Tom's Guide. October 23, 2013. Accessed April 28, 2019. https://www.tomsguide.com/us/what-is-tor-faq,news-17754.html
[34] "The Ultimate Guide to Tor Browser (with Important Tips) 2019." VpnMentor. Accessed April 28, 2019. https://www.vpnmentor.com/blog/tor-browser-work-relate-using-vpn/
[35] "The Tor Network - FAQ." Wordfence. Accessed April 28, 2019. https://www.wordfence.com/learn/the-tor-network-faq/
[36] "Servers." Tor Metrics. Accessed April 28, 2019. https://metrics.torproject.org/relays-ipv6.html
[37] "The Tor Network - FAQ." Wordfence. Accessed April 28, 2019. https://www.wordfence.com/learn/the-tor-network-faq/

device has the capability to function as a Tor node. The Tor Browser then determines a random path of various nodes which the transmission will pass through and lastly the final destination. The complete chosen path for that transmission is also called the Tor circuit[38].

Based on the Tor circuit, the transmission is bundled into a packet of encrypted layers, similar to an onion, and is routed to the entry/guard node. The entry or guard node is the gateway into the Tor network and sets the transmission packet into Relay Mode. Entry nodes are significant because they can identify the IP address of the source computer that is sending the packet, however, they cannot see the final destination of the packet. Each node is only able to decrypt enough of the packet to determine where the transmission came from and where to send the packet to next in the entire circuit. Not one node knows both the source and destination address of a given transmission packet[39]. Thus, with the growing number of available nodes on the Tor network, there are myriads of combinations of nodes a single packet could take before it reaches its final destination. It is virtually impossible to track a packet's exact route from source to destination. This essential quality is what makes the Tor Network so difficult to monitor and what conceals user identity and location on the network.

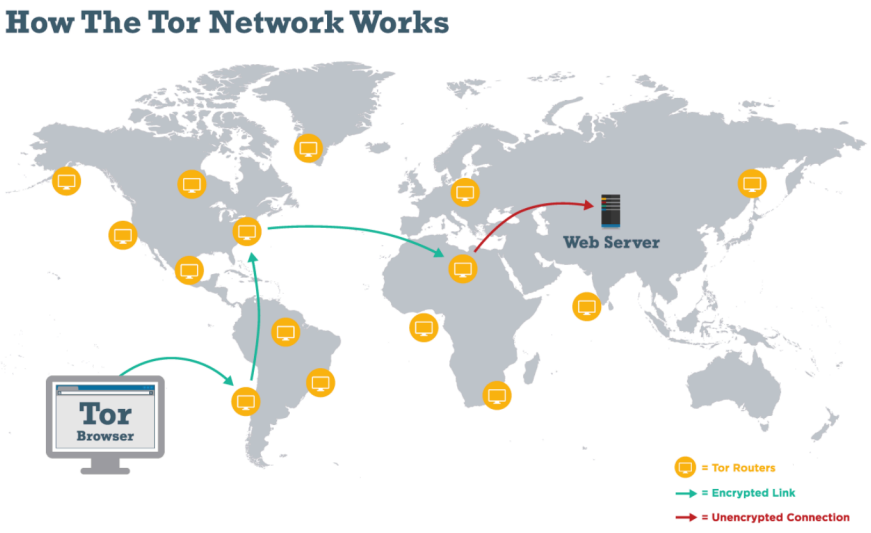
Next, the entry/guard node removes the first layer of encryption from the transmission packet, identifies the IP address of the next node in the Tor circuit and transmits the packet to the next node, a Middle node. Middle nodes are nodes within the Tor network through which packets are passed along and usually span the majority of a Tor circuit. Middle nodes cannot identify the original source of the packet nor the destination, they simply know the address of the previous node and that of the next node in the circuit. Middle nodes are commonly used by users who run Tor at their home or office as they do not have much responsibility other than passing the packet along the circuit. The Middle node will rarely

[38] "The Tor Network - FAQ." Wordfence. Accessed April 28, 2019. https://www.wordfence.com/learn/the-tor-network-faq/
[39] Srivathsav, Raja, and Raja Srivathsav. "TOR Nodes Explained!" Medium. April 14, 2018. Accessed April 28, 2019. https://medium.com/coinmonks/tor-nodes-explained-580808c29e2d

be scrutinized for suspicious activity as it does not know the source address nor the destination address of a transmitting packet[40]. Like the layers of an onion, a layer of encryption is peeled off at each node until the packet reaches its final destination. So, all packets being passed between Middle nodes will have some layer of encryption.

The last relay in every circuit is called the Exit node. That is, when a packet leaves the Tor network and is sent to its destination address, it is sent from an Exit node. The Exit node removes the last layer of encryption on the transmitting packet and sends the packet to the destination address in unencrypted format. Since Exit nodes are listed as the source address of transmissions using the Tor network to the destination address, they are the riskiest type of node as they are the first place investigators and legal authorities check to scrutinize any suspicious activity[41]. Overall, the packet is passed from source browser to an entry node, to multiple middle nodes, to an exist node, and finally the destination address, as multiple separate transmissions. Please find a simple depiction of the Onion routing technology shown in Figure 4.

*Figure 4: Onion Routing https://bit.ly/2N9aPBb*

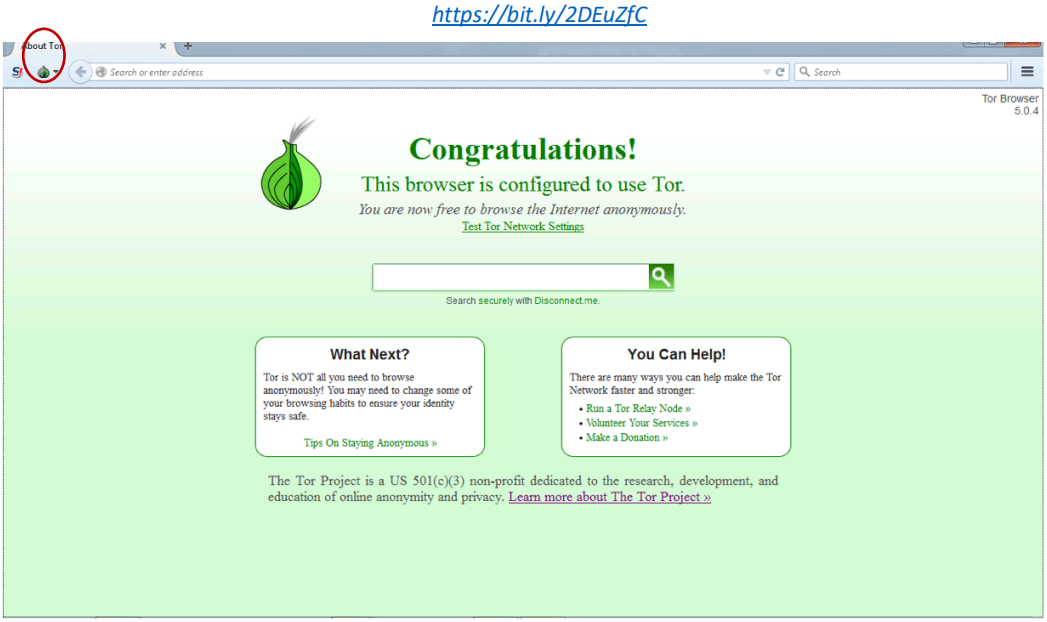



[40] Srivathsav, Raja, and Raja Srivathsav. "TOR Nodes Explained!" Medium. April 14, 2018. Accessed April 28, 2019. https://medium.com/coinmonks/tor-nodes-explained-580808c29e2d
[41] Ibid

## Accessing and Navigating Around the Tor Browser:

Accessing the Tor Network using the Tor browser is a relatively fast and intuitive process. Unlike what users may initially think, using the Tor Browser is very similar to using regular web browsers such as Google Chrome and Mozilla Firefox. If you wish to use Tor, simply download the Tor Browser Bundle from the Tor Project website: https://www.torproject.org/download/ and run through the installation process. The Tor Browser will require 120 MB on your device[42]. For detailed instructions, you can find a clear walk through of setting up the Tor here. Once you have fully installed the Tor Browser and run it, the Tor Browser should appear as shown in Figure 5. Voila! You are ready to use the Dark web!

*Figure 5: Tor Browser Configuration Page*
*https://bit.ly/2DEuZfC*




**Important things to note about the Tor Browser:** As shown above, the Tor browser appears just like a Mozilla Firefox browser would, except there is an onion icon in the menu bar. Clicking on the onion icon allows you to see your Tor circuit and the nodes your request is passing through in the Tor network before

[42] "The Ultimate Guide to Tor Browser (with Important Tips) 2019." VpnMentor. Accessed April 28, 2019. https://www.vpnmentor.com/blog/tor-browser-work-relate-using-vpn/

reaching its final destination[43]. For example, in Figure 6 below, this specific site request passed through a Bridge Node, France, & the Netherlands. It is interesting to note that the requested server returns back your site request as if the exit node were requesting it. So, in Figure 6, the returned Tor site states 'Your IP address appears to be: 5.79.68.161'. However, this is actually the IP address of the exit node in the Netherlands. This is because, according to the destination server, the exit node is the source address for that site request[44].

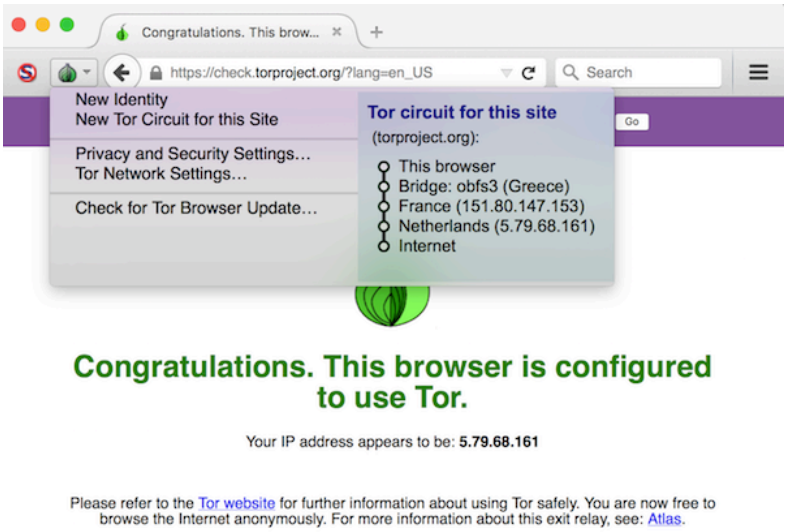
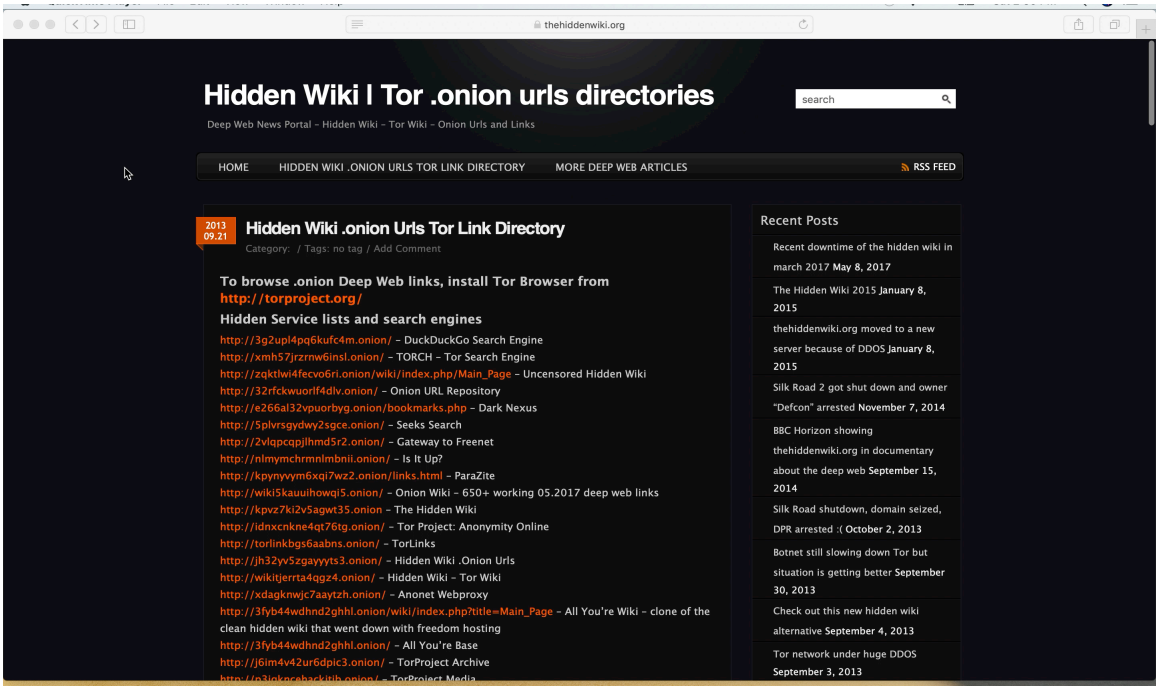



*Figure 6: Accessing your Tor Circuit https://bit.ly/2PziLcT*

**Onion Links:** So, we have set up the Tor Browser and are ready to explore the Dark web. Now what? Navigating on the Tor Browser is more complex than surfing on the clear net. The primary reason being that popular search engines such as Google and Yahoo! cannot crawl the dark net; users must know the exact links of the websites they wish to access. Additionally, all websites on the Dark net end in the onion suffix domain (.onion). Hidden Wiki is a commonly used website where Tor users can look up the latest onion link for popular websites exclusive to the Dark web services[45]. A video of the Hidden Wiki links site (clear net version) is attached in Figure 7. Please double click to view video. As shown, links for a variety of illegal services are available, including marketplace drugs, hitman services, fake certifications, Bitcoin laundering, and much more. We will go deeper into popular Dark web websites and services later on in this paper.

[43] Academy, Dark Web. "Using Tor." YouTube. March 27, 2017. Accessed April 28, 2019. https://www.youtube.com/watch?v=gHjYpxdCQvU
[44] Ibid.
[45] Ibid.

*Figure 7: Navigating Onion Links Using Hidden Wiki*
*https://thehiddenwiki.org*




## Tor Vulnerabilities

While the Tor Project claims to provide secure and anonymous user connectivity, it is important to highlight the strong efforts that government agencies having been putting in to track and de-anonymize cyber criminals on the Tor Network. Unsurprisingly, the Tor system does have flaws, primarily sourced from the exit node. As mentioned before, the exit node removes the last layer of encryption on the packet and transmits the packet to the destination address in unencrypted format[46]. Some web servers have their own added layer of encryption called an SSL certificate that prevents hackers from intercepting messages sent between web browsers and that web server. Other web servers that do not carry the SSL certificate transmit messages in unencrypted format, which may allow hackers and

[46] Sameeh, Tamer. "Is The Tor Browser Fully Anonymous? (The Myth and Reality)." Deepdot.web. March 30, 2017. Accessed April 20, 2019. https://www.deepdotweb.com/2017/03/30/tor-browser-fully-anonymous-myth-reality/

government authorities to intercept your message content even on the Tor Network[47]. Thus, whenever you visit an already unencrypted website using Tor, the exit node *can* track your previous browsing requests, searches, or messages transmitted. Many government agencies run their own exit nodes to keep an eye on dark web traffic as well as to trace users. There have been several cases where user identities have been unmasked: "In 2007, a security evangelist managed to intercept email messages and passwords for 100 email accounts via running an exit node on Tor's network. The users, whose emails and passwords were intercepted, made a mistake of not using encryption for their email communications, as they thought that Tor could shield them via its internal encryption protocol, but the reality is that this is not how Tor works."[48].

Additionally, in 2014, researchers at Carnegie Mellon University monitored enough entry and exit nodes to be able to track transmission timings and packet volume from node to node and identify which nodes belonged to the same Tor circuit. By identifying the Tor circuit, the group of researchers were able to track the IP source addresses of users as well as their destination addresses[49]. This experiment was later renamed to 'Operation Onymous' as the FBI was able to use the findings to arrest 17 cyber criminals and to seize 414 dot onion domain links, including Silk Road 2, Cannabis Road and Cash Machine[50]. We will go in deeper detail of popular and notorious dark websites later in this paper.

Significant research has also been conducted to analyze the effectiveness of fingerprinting on the Tor Browser. Essentially, when a user requests information from a server that enables fingerprinting, the

[47] "What Is Tor - How Does Tor Work - How to Use Tor." Tom's Guide. October 23, 2013. Accessed April 28, 2019. https://www.tomsguide.com/us/what-is-tor-faq,news-17754.html

[48] Sameeh, Tamer. "Is The Tor Browser Fully Anonymous? (The Myth and Reality)." Deepdot.web. March 30, 2017. Accessed April 20, 2019. https://www.deepdotweb.com/2017/03/30/tor-browser-fully-anonymous-myth-reality/

[49] "Is Tor Safe? Learn How Secure Tor Is." ProtonVPN Blog. February 27, 2019. Accessed April 28, 2019. https://protonvpn.com/blog/is-tor-safe/

[50] Greenberg, Andy. "Global Web Crackdown Arrests 17, Seizes Hundreds Of Dark Net Domains." Wired. June 03, 2017. Accessed April 28, 2019. https://www.wired.com/2014/11/operation-onymous-dark-web-arrests/

server collects information on the user's browser configuration, such as window size, font, font size, screen resolution, color depth, selected browser extensions/plug ins, use/lack of cookies, system language, system platform, system time-zone, and much, much more. The collection of these browser characteristics can be used to create a unique 'fingerprint' for the user's browser, gauge and predict user activity, and possibly identify the user if their browser fingerprint is unique[51]. In 2010, the Electronic Frontier Foundation (EFF) launched the Panopticlick research group to examine how unique an individual's browser configurations are and found that 94.2% of all browsers (excluding Tor Browsers) on the entire internet have a unique fingerprint. That is 94.2% of users may be identified based solely on their browser configuration[52]. Wow! Tor aggressively tries to block all known fingerprinting technologies in their Tor browser by implementing the HTTPS everywhere and the NoScript plugins. However, it is not completely immune to browser fingerprinting. A research group in the Department of Science and Engineering at Meiji University, Japan, conducted a study to test how vulnerable the Tor browser version 5.5 (the latest version in 2016) is to browser fingerprinting. The study concluded that 14.28% of users may be identified within 2 weeks of transmission using the latest version of the Tor Browser and 70.0% of users may be identified within 2 week of transmission using older versions of the Tor browser[53]. A detailed report of the study may be found here.

[51] "About." Panopticlick. Accessed April 28, 2019. https://panopticlick.eff.org/about
[52] Sameeh, Tamer. "Tor Fingerprinting – Is the Tor Browser Immune Against Browser Fingerprinting?" Deepdot.web. October 25, 2017. Accessed April 20, 2019. https://www.deepdotweb.com/2017/10/25/tor-fingerprinting-tor-browser-immune-browser-fingerprinting/
[53] Saito, Takamichi, Kazushi Takahashi, Koki Yasuda, Kazuhisa Tanabe, Masayuki Taneoka, and Ryohei Hosoya. "Tor Fingerprinting: Tor Browser Can Mitigate Browser Fingerprinting?" SpringerLink. August 24, 2017. Accessed April 28, 2019. https://link.springer.com/chapter/10.1007/978-3-319-65521-5_44

## Other Popular Dark Net Network Offerings

While Tor is the most popular and first network that comes up with reference to the Dark web, other networks are also available offering Dark Web services as well. In this section, we will go over two other dark web networks: I2P and Freenet, and how they differ from the Tor Project.

**I2P**, which stands for the **Invisible Internet Project**, is similar to Tor as an anonymous relay network. However, unlike Tor, I2P was designed to be exclusively used for Dark net services by limiting traffic flow to within the bounds of the I2P network. So, there exist very few exit nodes on the I2P network that provide access to sites outside the Dark web. As a result, security on I2P is a lot stronger than that of the Tor Browser and de-anonymizing a user is much more difficult[54].

I2P implements garlic routing, which is similar to Tor's onion routing in that it implements layered encryption by bouncing a packet through several nodes before it reaches its destination address. However, instead of circuit based, I2P implements packet-based routing. This means that packets may be dynamically routed to avoid congestion and latency. Similar to the clear net, network traffic in garlic routing is constantly shared between routers to form optimal network routes. Additionally, the sender may choose the number of nodes in their transmission circuits, allowing users to choose a comfortable balance between anonymity and speed. Increasing the number of nodes substantially increases browsing speed because the routing structure is simpler, however, also compromises user anonymity as there are fewer combinations of routes the packet could have traveled[55].

Another major difference between I2P's garlic routing and Tor's onion routing is that garlic routing implements simplex circuits, using only one-way traffic, while onion routing implements half-duplex circuit, using two-way traffic. This means that in onion routing, a packet returns back to the

[54] Holden, Ed. "An Introduction to Tor Vs..." IVPN. March 27, 2018. Accessed April 28, 2019. https://www.ivpn.net/privacy-guides/an-introduction-to-tor-vs-i2p
[55] Ibid.

source along the same circuit that it had travelled on the way to its destination address. In I2P's garlic routing, there are double the amount of circuits that a packet could have travelled since it could have travelled along any of the other nodes to reach its source address[56]. Lastly, unlike the Tor Project's Tor Browser, I2P offers a variety of applications specifically for access to the I2P network, including email, instant messaging, file-sharing, and distributed storage options[57].

**Freenet**, developed by Ian Clarke at the University of Edinburg in 1999, is a P2P network that allows users to anonymously share files/databases, send messages, or publish websites with other trusted users. Freenet enforces tight security measures within its network boundaries. That is, only users on the Freenet network may access the available files and resources - these include private websites, chats, forums, and databases. Users cannot use Freenet to access sites outside the Freenet network, such as regular sites on the Internet: Google or Youtube. Upon joining, each user gets a cryptographic identifier which allows them to identify and connect with other trusted users on the Freenet network but which maintains their anonymity for other users they do not know or trust[58].

The Freenet platform functions on a distributed data storage system where each client computer on the network allocates a portion of their hard drive for encrypted file storage. Each client computer also acts as a router to navigate the stored files through the network if another client computer has requested them. Each client computer cannot access nor manage any of the data stores on their computer. Similar to I2P, network traffic is shared frequently to allow computers to route requested data through an optimal route. This means the Freenet platform is completely decentralized so that there isn't one single point of failure. Due to this decentralized structure, Freenet is far more secure than Tor as

[56] Holden, Ed. "An Introduction to Tor Vs..." IVPN. March 27, 2018. Accessed April 28, 2019. https://www.ivpn.net/privacy-guides/an-introduction-to-tor-vs-i2p
[57] Ibid.
[58] "Freenet – Another Secure Anonymity Browser." Dark Web News. January 14, 2018. Accessed April 28, 2019. https://darkwebnews.com/anonymity/freenet-secure-anonymity-browser/

information is only known and accessible by the trusted users on the network. Unlike Tor, The Freenet network and its resources can never fully be shut down unless all the client computers have been identified, located, and shut down[59].

## IV. Popular Dark Web Services

In this section we will discuss popular onion sites exclusive to the Dark Web, including various search engines, illegal marketplaces, other platforms open to human activists and proponents of free-speech, and the rise and fall of Silk Road.

### Dark Web Search Engines

Since regular search engines such as Google and Yahoo! cannot crawl over Dark Web sites, the Dark web has its own search engines built to help new users navigate around the dark web and discover onion links. Some unique search engines include:

- **DuckDuckGo** – After DuckDuckGo invested in the Tor Project, it has since become the default search engine for the Tor browser. Users can use DuckDuckGo as an all-purpose search engine to access websites both on the clear net as well as the deep web. DuckDuckGo has risen to popularity primary because it supports user anonymity and does not keep track of user search history or activity. However, it is unlikely that you will find censored websites or illegal activities in their search results[60].
- **Torch** – One of the longest lasting and popular search engines, the Torch search engine boasts to have found over a million censored websites on the Dark web. However, unlike DuckDuckGo,

[59] Buckelew, Joanne, Corben, and CaesarMK. "TOR vs The Freenet Project." SnapMunk. December 18, 2016. Accessed April 28, 2019. https://www.snapmunk.com/tor-vs-the-freenet-project/

[60] "Best Uncensored Search Engines for Anonymous Searching." Deep Web Links | Deep Web Sites | The Deepweb 2018. March 30, 2019. Accessed April 28, 2019. https://www.deepwebsiteslinks.com/uncensored-search-engines-for-anonymous-searching/

which does not collect user search history nor display any Ads, Torch's homepage is inundated with hidden Ads which may easily get clicked if users are not careful[61].

- **NotEvil** – The simplest and most efficient search engine on the Dark web, NotEvil is aimed solely at censored websites and has an index of over 2.5 million hidden onion links. Users are also able to chat anonymously with other users across the globe through the search engine[62].
- **Hidden Wiki** – Known as the beginners guide to nefarious activity on the dark web, Hidden Wiki provides a complete breakdown of all exclusively dark web services and their latest onion links from hacking services, drug market places, fake passports, financial databases, email messaging services, to child pornography websites[63].

## Illegal Market Places and Hidden Services:

The Dark web is inundated with numerous online black-market places and services to get just about anything. Some of the most popular or interesting markets or services still running on the Dark web today include Dream Market, the Wall Street Market, CGMC (Cannabis Growers and Merchants Co-op), & BitBlender.

- **Dream Market**, founded in 2013, is the largest and most trusted general Darknet marketplace currently available. The site offers a total market listing of 146,987 products. However, recently, Dream Market has announced that they will be shutting down on April 30th 2019 and transferring to a new platform to protect their identity after a bust of opioid trafficking[64].

---

[61] "Best Uncensored Search Engines for Anonymous Searching." Deep Web Links | Deep Web Sites | The Deepweb 2018. March 30, 2019. Accessed April 28, 2019. https://www.deepwebsiteslinks.com/uncensored-search-engines-for-anonymous-searching/
[62] Ibid.
[63] Ibid.
[64] "Dream Market Review and URL." Deep Web Links | Deep Web Sites | The Deepweb 2018. April 03, 2019. Accessed April 28, 2019. https://www.deepwebsiteslinks.com/dream-market-url/

- Established in 2016, the **Wall Street Market**, is a newer and modern general purpose darknet market place offering over 15,000 product listings from 3500 vendors to over 700,000 customers. It offers a large variety of products. However, it strongly restricts the sale of certain types of pornography, weapons, and live animals[65].
- **CGMC (Cannabis Growers and Merchants Co-op)** is an invite-only marketplace specializing in cannabis and psychedelics. The platform offers a total of 1927 product listings such as Flowers, Edibles, Shrooms. Users that request an invite to purchase or sell are scanned for their scam history and theft on the tor network. CGMC is known for its professional user-interface and efficient product browsing options[66].
- **Bitblender** – Launched in 2014, Bitblender is one of the oldest and popular bitcoin mixers available. Bitcoin mixing is essentially the process of using a dedication and trusted third party (BitBlender) between a bitcoin transaction's sender and receiver. Similar to onion routing, this breaks the link between sender and receiver on the public blockchain ledger and adds a second layer of security for anonymous transactions[67]. Bitblender charges a 1-3% service on each transaction and additional security features such as a 99-hour delay to frustrate central authorities[68].

Due to the nature of the transactions, illegal marketplaces are often tracked and shut down soon after gaining popularity. Some of popular and noteworthy services on the Dark web that were recently shut down include AlphaBay, Russian Anonymous Marketplace, and Grams:

---

[65] "A Guide to Wall Street Market (Dark Net Market/DNM)." Explore Psychedelics. December 06, 2018. Accessed April 28, 2019. https://explorepsychedelics.com/markets/wall-street-market/
[66] Ciphas. "CGMC Review." Dark Web Reviews. January 23, 2018. Accessed April 28, 2019. http://darkweb.reviews/cgmc-review/
[67] WeUseCoins. "A Simple Guide To Effectively And Safely Mixing Bitcoins." What Is Bitcoin? Introductory Video and Current Bitcoin Price. Accessed April 28, 2019. https://www.weusecoins.com/a-simple-guide-to-effectively-and-safely-mixing-bitcoins/.
[68] Kptx. "BitBlender Review." Dark Web Reviews. February 14, 2017. Accessed April 28, 2019. http://darkweb.reviews/bitblender-review/

- **AlphaBay** – Launched in December 2014, AlphaBay was the reigning black-market place for all kinds of goods for several years and pioneered innovative website services such as digital contracts[69], escrow systems, and trade using other cryptocurrencies, aside from bitcoin. Known for its steady growth rate, Alpha Bay was at one point 10 times larger than the notorious, yet sophisticated, Silk Road (which we will soon discuss)[70]. By the time it was seized and shut down on July 4 2017, AlphaBay had over 400,000 users and bought in over $23 million in revenue[71].
- **Russian Anonymous Marketplace (RAMP)** is one of the longest lasting online market places in the history of the dark web. RAMP provided a platform for buyers and sellers specifically in Russia and other Eastern European countries to meet but did not act as a commissioning middleman in the trade. Buyers that wished to purchase goods simply posted their interest on the RAMP forum and sellers were required to reach out to them and independently negotiate the terms of trade from there. RAMP highly encouraged the 'dead drops' delivery method, whereby buyers leave the cash payment at one location and pick up their purchased goods at another so that both the buyer and the seller remain anonymous[72].
- **Grams** – Grams was one of the first search engines on the dark web that allows users to search for specific drugs across various illegal marketplaces. Intended to mimic Google on the Surface Web, Grams is seen as the Google for drugs across the Tor network. The Grams search engine was shut down in December 2017[73].

---

[69] Cox, Joseph. "This Dark Web Market Just Started Offering Contracts for Anything." Motherboard. May 01, 2015. Accessed April 28, 2019. https://motherboard.vice.com/en_us/article/mgbwea/alphabay-contracts

[70] Aliens, C. "AlphaBay and Oasis Markets to Begin Accepting Monero for Payments." Deepdot.web. August 23, 2016. Accessed April 24, 2019. https://www.deepdotweb.com/2016/08/23/alphabay-oasis-markets-begin-accepting-monero-payments/

[71] Cimpanu, Catalin. "AlphaBay Dark Web Market Taken Down After Law Enforcement Raids." BleepingComputer. July 14, 2017. Accessed April 28, 2019. https://www.bleepingcomputer.com/news/security/alphabay-dark-web-market-taken-down-after-law-enforcement-raids/

[72] Venkat. "Top 10 Popular Dark Websites." BLEEDBYTES. February 02, 2019. Accessed April 28, 2019. https://bleedbytes.in/top-10-popular-sites-in-the-deep-web/

[73] Academy, Dark Web. "Using Tor." YouTube. March 27, 2017. Accessed April 28, 2019. https://www.youtube.com/watch?v=gHjYpxdCQvU

Although each of these websites provide slightly different business propositions and specializations, across all these websites, ensuring security, usability, and the product variety are the most important factors in order to maintain user attraction and credibility.

- **Product Variety** - While some illegal marketplaces specialize in the sale of certain goods or restrict certain kinds of goods, several offer a variety of products that may other be illegal elsewhere. Products generally fall into four main categories[74]:
  - Illegal drugs (of a large variety) – eg. Cannabis, opioids, intoxicants, psychedelics
  - Criminal Services – hacked bank accounts, counterfeit monies, firearms, hitmen
  - Forgeries – fake licenses, passports, stolen SSNS
  - Digital Goods – hacked social media, Netflix, & amazon accounts.
- **Security** – several popular online black-market places enforce strong security measures to maintain the integrity of transactions. Some features include Two-Factor Authentication and trusted escrow services for each transaction. Additionally, each vendor must pay a Vendor Bond ranging from $200 - $500 (based on the specific marketplace) to even begin selling on the platform. Some online market places also pull vendor ratings from other co-existing market places so that customers may view vendor ratings before committing to a transaction[75]. Additionally, some illegal marketplaces require vendors to pay a 2.0% to 5.5% commission per transaction to the platform. The commission percentage is based on the vendor ratings so vendors are encouraged to provide a professional standard of services as well[76].

[74] Spencer, Wes. "The Silk Road: The Rise and Fall of the World's Largest Online Black Market." YouTube. October 11, 2013. Accessed April 28, 2019. https://www.youtube.com/watch?v=LkRhBOZSw38
[75] "Dream Market Review and URL." Deep Web Links | Deep Web Sites | The Deepweb 2018. April 03, 2019. Accessed April 28, 2019. https://www.deepwebsiteslinks.com/dream-market-url/
[76] "A Guide to Wall Street Market (Dark Net Market/DNM)." Explore Psychedelics. December 06, 2018. Accessed April 28, 2019. https://explorepsychedelics.com/markets/wall-street-market/

- **Usability** – Unlike most of us may think, the dark web provides a variety of simple, no-nonsense websites as well. This is because customers appreciate websites that are easy to navigate, hassle-free, and sophisticated. Several online black-market places allow users to pay in multiple cryptocurrencies such as Bitcoin, Bitcoin Cash, Monero and enable Bitcoin mixing[77]. Websites are usually Ad free and provide a sophisticated search filter to help users find the exact products they are looking for. Several online black marketplaces also practice prompt and proactive customer service whereby disputes are responded to and resolved quickly[78].

## Websites for Beneficial Causes

Apart from its array of nefarious websites, the Dark web also has sites for beneficial causes such as whistleblowing platforms, forums for free-speech, and databases for censored information. A few examples are WikiLeaks, Sci-Hub, SoylentNews, and Pro-publica.

- **WikiLeaks** – Developed by Julian Assange in 2012, WikiLeaks is used to spread information provided by whistleblowers, journalists, or anyone that wants to speak out in the name of public knowledge. Since 2012, WikiLeaks has been exposing classified information and was heavily involved in leaking private emails during the 2016 Presidential Elections. The .onion platform allows users to upload content anonymously and aims to get the truth to mainstream media[79].
- **Sci-Hub** - Developed by Alexandra Elbakyan in Kazhakhstan in 2011, Sci-Hub provides free-access to online research papers and literary works to all. Elbakyan believed that publishers and journals were hoarding subscription fees at the expense of public knowledge everyone ought to

[77] Ciphas. "CGMC Review." Dark Web Reviews. January 23, 2018. Accessed April 28, 2019. http://darkweb.reviews/cgmc-review/
[78] "A Guide to Wall Street Market (Dark Net Market/DNM)." Explore Psychedelics. December 06, 2018. Accessed April 28, 2019. https://explorepsychedelics.com/markets/wall-street-market/
[79] "WikiLeaks Fast Facts." CNN. April 11, 2019. Accessed April 28, 2019. https://www.cnn.com/2013/06/03/world/wikileaks-fast-facts/index.html

have access to. She believed knowledge and information should be available to all, regardless of funding or location restrictions[80].

- **SoylentNews** – One of the many websites for free-speech, Soylent News is a volunteer driven news posting forum focused on the topics of technology and science. It is a platform where users can openly and anonymously share and discuss their opinions and even react to other members' comments by becoming either 'Friends', 'Foes', or 'Fans' of other users, all done anonymously[81].
- **Pro-Publica** is a popular non-profit news forum in the public sphere that aims to 'expose abuses of power and betrayals of the public trust by government, business, and other institutions, using the moral force of investigative journalism'[82]. Recently, Pro-Publica launched their own dot onion site on the dark web to provide users a platform to anonymously browse sensitive news media without the government authorities standing over their shoulders. More importantly, Pro-Publica launched this site to allow users to anonymously tip stories if they felt governments or powerful organizations were unfairly benefiting from the public[83].

## The Rise and Fall of the Silk Road

**The Origins of Silk Road:** Silk Road is till date, the most well-known and first popularized illegal marketplace on the dark web, notoriously known for selling a wide collection of illegal drugs and services. Silk Road was originally founded in February 2011 when libertarian, Ross Ulbricht wanted to experience a truly free market place without regulations from a governmental authority. Prior to Silk

[80] Zhukova, Anya. "The Best Dark Web Websites You Won't Find on Google." MakeUseOf. March 02, 2019. Accessed April 28, 2019. https://www.makeuseof.com/tag/best-dark-web-websites/
[81] Ibid.
[82] "About Us." ProPublica. Accessed April 28, 2019. https://www.propublica.org/about/
[83] Ibid.

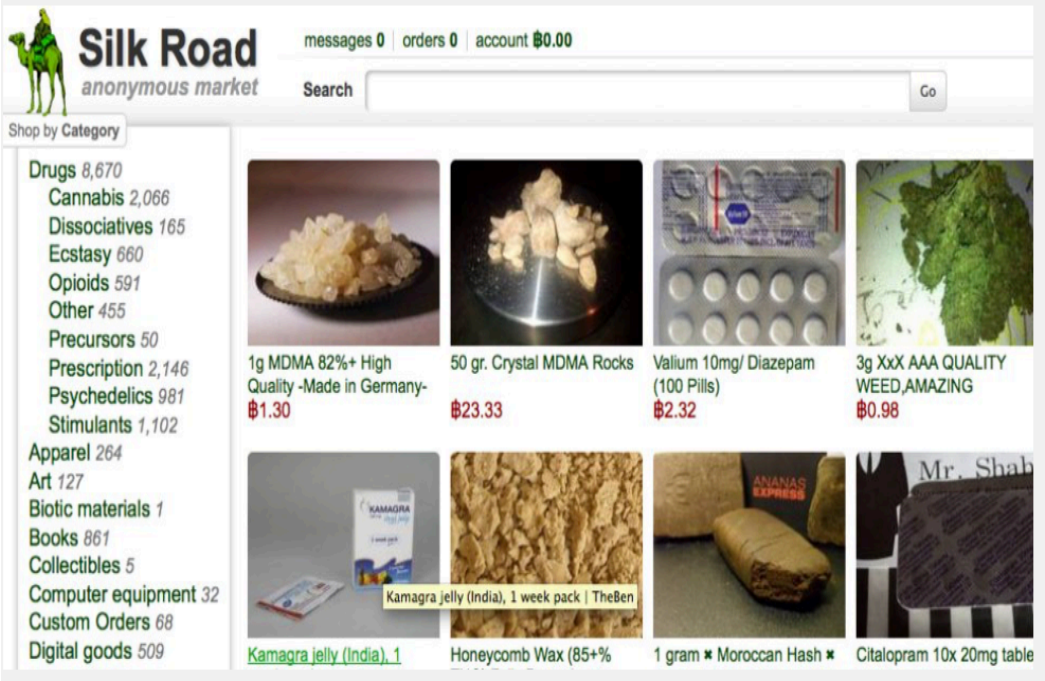
Road, Ross Ulbricht, a native-born Texan, had attempted day trades at the stock market, later started a multiplayer online video game company, and had also partnered with a friend to develop an online bookstore for used books, Good Wagon Books[84]. However, after completing his Master's degree at Pennsylvania State University, he developed an interest in libertarian economic theory, which formed the backbone of the Silk Road marketplace. He was skeptical of government authority and believed that people should be able to purchase and sell whatever goods they like as long as it doesn't inflict harm on others. He believed an anonymous userbase was the only way to achieve a truly free-market without government intervention. Using the Tor network, Ulbricht developed the Silk Road market as the first market place on the Dark web where users could use Bitcoin to anonymously purchase whatever goods they like. The only products Ulbricht was strictly against were child pornography, money scams, weapons, and the sale of any good that could harm others[85]. Ulbricht named the marketplace, Silk Road, after the historical trade networks spanning from East Asia, Africa, to Europe and operated the site under his pseudonym, 'Dread Pirate Roberts'[86].

**The Rise of Silk Road**: Soon after launching in January 2011, the site rapidly grew in popularity, which helped fund features for further development such a scalable server, an escrow service for buyers, and a ratings page for buyers and sellers[87]. The biggest advantage that Silk Road had over other marketplaces was the level of trust users had on the platform as well as in Ross Ullbricht. Ullbricht emphasized the importance of the Silk Road community as a platform for users could honestly and freely purchase

[84] "Drugs, (Non)Violence, and Video Games: A Brief History of Silk Road." CoinCentral. August 25, 2018. Accessed April 28, 2019. https://coincentral.com/silk-road-history/
[85] "The History of Silk Road: A Tale of Drugs, Extortion & Bitcoin." Blockonomi. November 20, 2018. Accessed April 28, 2019. https://blockonomi.com/history-of-silk-road/
[86] "Drugs, (Non)Violence, and Video Games: A Brief History of Silk Road." CoinCentral. August 25, 2018. Accessed April 28, 2019. https://coincentral.com/silk-road-history/
[87] "Drugs, (Non)Violence, and Video Games: A Brief History of Silk Road." CoinCentral. August 25, 2018. Accessed April 28, 2019. https://coincentral.com/silk-road-history/

whatever goods they want. He also developed several forums for users to openly discuss their core values without threatening their safety. Ulbricht made sure Silk Road operated efficiently and securely: Orders were fulfilled quickly, disputes resolved fairly, and escrow services were secure[88]. At its peak, Silk Road is said to have had over 1 million users with almost 1400 transactions a day and revenues ranging from $2 million to $7million per month[89].

*Figure 8: The Silk Road Forum https://bit.ly/2ULA9MH*

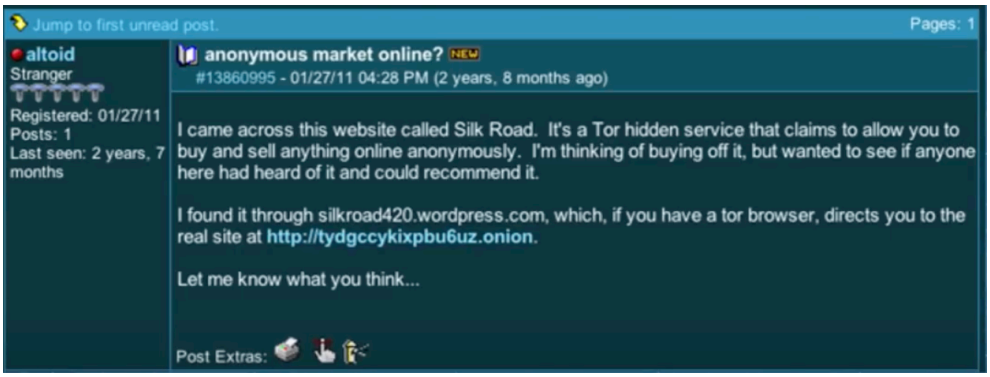



**Rough Waters for Silk Road:** It was only in June 2011, when journalist, Adrian Chen, from Gawker, a Manhattan based news blog, stumbled upon the Silk Road website and published a story about it, that brought Silk Road to the public sphere. Consequently, Senator Charles Schumer ordered the Drug Enforcement Agency (DEA) and Department of Justice to track and shut down the Silk Road platform. Several regulatory agencies such as the department of homeland security, the IRS, and FBI began

[88] "The History of Silk Road: A Tale of Drugs, Extortion & Bitcoin." Blockonomi. November 20, 2018. Accessed April 28, 2019. https://blockonomi.com/history-of-silk-road/
[89] "Drugs, (Non)Violence, and Video Games: A Brief History of Silk Road." CoinCentral. August 25, 2018. Accessed April 28, 2019. https://coincentral.com/silk-road-history/

scrambling to track the source of this underground marketplace[90]. Silk Road first hit rough waters on July 23rd 2013 when a reddit thread leaked a potential Silk Road user's IP address which allowed the FBI to track the server used to host Silk Road's website in Iceland[91]. They found that in January 2011, a Silk Road user, 'altoid', had posted on the shroomery.org forum asking if anyone had ever heard about Silk Road, that he is thinking of buying off of it, and whether anyone can recommend it. Interestingly, he also gave the web address to reach the Silk Road forum[92], as shown in Figure 8 :

*Figure 9: 'altoid' posts on shroomery.org https://bit.ly/2GO2ezc*




Only three days later, the same user, 'altoid' posted the same peculiar message on Bitcointalk.org using the same essential questions and some of the same script, 'Let me know what you guys think'[93]:

*Figure 10: 'altoid' posts on Bitcointalk.org https://bit.ly/2vqKDGS*


[90] "Drugs, (Non)Violence, and Video Games: A Brief History of Silk Road." CoinCentral. August 25, 2018. Accessed April 28, 2019. https://coincentral.com/silk-road-history/
[91] Ibid.
[92] Spencer, Wes. "The Silk Road: The Rise and Fall of the World's Largest Online Black Market." YouTube. October 11, 2013. Accessed April 28, 2019. https://www.youtube.com/watch?v=LkRhBOZSw38
[93] Ibid.

Since ‘altoid’ used the exact script in both messages as well as provided the link of Silk Road forum on both posts, it appears as though ‘altoid’ is trying to attract more attention and users to the Silk Road forum as a marketing tactic. The FBI now have a lead that ‘altoid’ may be associated with or a member of the Silk Road administration team.

Skipping ahead to October 11, 2011, the username ‘altoid’ posted again on the Bitcointalk.org forum seeking an IT pro ‘to be the lead developer in a venture backed bitcoin startup company’. However, this time ‘altoid’ left his public username, rossulbricht@gmail.com [94].

*Figure 11: 'altoid' reveals his Personal Email Address https://bit.ly/2vpfmUL*


At the same time in June 18th 2011, Silk Road’s website was updated from administrator ‘sr_admin’ establishing himself as the founder and man behind Silk Road[95]. He posted:

“Who is Silk Road? Some call me SR, SR admin or just Silk Road. But isn’t that confusing? I am Silk Road, the market, the person, the enterprise, everything. But Silk Road has matured and I need an identity separate from the site and the enterprise of which I am now only a part. I need a name.”

[94] Spencer, Wes. "The Silk Road: The Rise and Fall of the World's Largest Online Black Market." YouTube. October 11, 2013. Accessed April 28, 2019. https://www.youtube.com/watch?v=LkRhBOZSw38
[95] Spencer, Wes. "The Silk Road: The Rise and Fall of the World's Largest Online Black Market." YouTube. October 11, 2013. Accessed April 28, 2019. https://www.youtube.com/watch?v=LkRhBOZSw38

Later in February of 2012, 'sr_admin' posted again establishing his new name to the Dark web as, 'Dread Pirate Roberts'[96], the founder of Silk Road:

"Drum roll please… my new name is 'Dread Pirate Roberts"

The FBI began to investigate the connection between 'Dread Pirate Roberts', the owner of Silk Road, and 'altoid', also known as Ross Ullbricht. They found that DPR frequently posted YouTube videos about the Austrian free-market economist, Ludwig Von Mises, on the Silk Road message forum. Interestingly, they found the very same YouTube videos on Ludwig Von Mises on Ross Ulbricht's Google Plus+ site[97]. This gives a very strong lead on the Silk Road owner, but it's not enough to arrest Ross Ulbricht.

**'Dread Pirate Roberts' goes to Jail:** Hereon forth, the FBI began to closely monitor Ulbricht's every move. Using access to the Silk Road server, the FBI traced that a user accessed the Silk Road server from an internet café in San Francisco. Records from a Google Subpoena also showed that Ulbricht regularly logged into this own Gmail account less then 500ft away from this very same internet café[98].

Later in July 2013, the US Customs and Border Protection randomly intercepted a mail package coming in from Canada as part of routine checking to find 9 different forged identifications, all with Ross Ulbricht's picture, but all using different names. When questioned about the above, Ross Ulbricht confidently responded, 'Hypothetically, anyone could purchase these documents on a website called Silk Road'[99]. The FBI now had evidence that Ross Ulbricht at least knows about the Silk Road forum.

[96] Ibid.
[97] Ibid.
[98] Ibid.
[99] Spencer, Wes. "The Silk Road: The Rise and Fall of the World's Largest Online Black Market." YouTube. October 11, 2013. Accessed April 28, 2019. https://www.youtube.com/watch?v=LkRhBOZSw38

The final piece of evidence came on March 5th 2012 when a new user posted on stackoverflow.com using the username 'Ross Ulbricht' asking for help on how to connect a Tor hidden service. Only hours later, he realized his mistake and changed the username to 'frosty' with email address: frosty@frosty.com. In September 2013, when the FBI began to scrutinize data from the Silk Road server, they identified the substring 'frosty@frosty.com' in the server's SSH Public keys, which they knew was Ross Ulbricht[100]. The FBI now had enough evidence against Ross Ulbricht to arrest him. On October 1st 2013, the FBI arrested Ulbricht in the San Francisco Public library for money laundering, computer hacking, and trafficking of fraudulent identity documents and of illegal narcotics[101]. The same day, the Silk Road forum was seized and shut down. At the time of site seizure, Silk road had traded goods with total value of over $1.2 billion USD and Ulbricht received around $28 million of that in trade commissions[102].

What next? The Silk Road Forum and Ross Ulbricht only carved the trail for the numerous other online black-market places to follow. Since the Silk Road's seizure, numerous online black markets such as Silk Road 2.0 and now Silk Road 3.0[103], have risen and fallen only to reinvent themselves with a new name within a few days. The trade of illegal goods has been around in society for many years, whether it is in the dark alley ways of sketchy neighborhoods or from forged prescriptions for over-the-counter drugs, the dark web simply facilitates a new platform to bring buyers and sellers together. The FBI's hunt for cybercriminals continues onward.

[100] Ibid.
[101] Ibid.
[102] "The History of Silk Road: A Tale of Drugs, Extortion & Bitcoin." Blockonomi. November 20, 2018. Accessed April 28, 2019. https://blockonomi.com/history-of-silk-road/
[103] Ibid.

## V. The Future of the Dark Web

Much debate has taken place regarding the future and sustainability of the dark web. Some say Dark networks need to make significant changes in order to sustain and peacefully co-exist with government authorities. Others say the Dark web is only getting started and that we are the brink of rapid user expansion. Below are just a few of *my* predictions for the future of the Dark web:

The Dark Net will become much more mainstream as a medium of internet browsing. Over the past two to three years, people are generally becoming more aware of and much less forgiving for leaked personal data. Most value their personal privacy highly and prefer to be able to browse the internet freely without having Internet Service Providers, Search Engine cookies, and government authorities constantly following their every click. Given this day in age where new stories on data breaches surface the web every week, the Dark web is exactly what users need to carelessly browse all kinds of knowledge on the web and debate with different minded individuals. With the increased number of books, TV shows, and public news talks relating to the Dark web, user interest is currently higher than ever before[104]. People are naturally curious, they are learning and opening up to the many benefits the Dark web provides. Over the next few years, the Tor Project will see a substantial spike in customer base and network traffic.

Additionally, as several existing Dark marketplaces shut down every day, new marketplaces surface the web and the FBI's continues to track down cybercriminals. However, with every marketplace that falls, all other market places will grow smarter, more decentralized, and more

[104] "The Future of the Darknet: 9 Critically Important Predictions." Futurist Speaker. January 23, 2019. Accessed April 28, 2019. https://futuristspeaker.com/business-trends/the-future-of-the-darknet-9-critically-important-predictions/

determined to establish a secure libertarian trading platform[105]. Dark market operators will find new and innovative ways to cast a veil on government authorities and skillfully hide user footprints.

In an effort to maintain the highest standards of security and anonymity, the public blockchain ledger will become obsolete and more secure cryptocurrencies will rise. The problem with Bitcoin comes in the use of a public blockchain ledger, which gives authorities *some* ability to track senders and receivers, if they are really determined. Currently, tumbling and mixing services do blindfold and frustrate transaction trackers but these are only short-term fixes, in my opinion. A more secure system of processing transaction payments will arise and markets will gradually accept various other cryptocurrencies such as Litecoin, Ethereum, Dash, and more.

Reputation will be king – The Dark web currently has no form of a justice system and individuals cannot be charged for deceit. In the future, dark markets will function reliably based solely on user reputation. If a user has traded goods fairly in the past, their reputation will speak and they will attract more business. Conversely, a user with a reputation of malpractice and deceit will automatically be thrown out from all marketplaces and left with no place for themselves on the platform. A person's reputation will act as the main justice system on the Dark web and will become their ticket to sustaining on Dark markets.

[105] Naseem, Iflah, Ashirr K. Kashyap, and Dheeraj Mandloi. "Exploring Anonymous Depths of Invisible Web and the Digi-Underworld." *International Journal of Computer Applications (0975 – 8887)*: 21-24.

## VI. Closing Statements

As you may have guessed by now, the Dark web is a fascinating, profound, and ever-growing portion of the Internet iceberg. There are vast amounts of information available on the sophisticated technologies used to maintain user anonymity and the potential it has to tangibly impact society. From facilitating the Arab Spring revolution in 2011 to exposing the Democratic National Committee's emails during the 2016 Presidential Campaign, the Dark Net has substantial power to challenge overpowering government authorities and large private organizations. Representative of the truth, the people, and the free, the Dark web is where decentralized free-markets thrive, human rights activists promote free-speech, and where individuals speak out to reveal hidden truths. The Dark net's sophisticated infrastructure keeps investigative authorities on their toes to develop new and unorthodox ways to track down this new wave of tech-savvy cyber-criminals. Yet underneath this anarchist utopia, is it really beneficial for us to promote the freedom of knowledge for all? That too, at the cost of numerous money laundering, drug trafficking criminals on the loose? That discussion is for another research paper at another time.

## VII. Bibliography


"About." Panopticlick. Accessed April 28, 2019. https://panopticlick.eff.org/about

"About Us." ProPublica. Accessed April 28, 2019. https://www.propublica.org/about/

Academy, Dark Web. "Using Tor." YouTube. March 27, 2017. Accessed April 28, 2019. https://www.youtube.com/watch?v=gHjYpxdCQvU

"A Guide to Wall Street Market (Dark Net Market/DNM)." Explore Psychedelics. December 06, 2018. Accessed April 28, 2019. https://explorepsychedelics.com/markets/wall-street-market/

"A History Of Protecting Freedom Where Law And Technology Collide". 2019. *Electronic Frontier Foundation*. https://www.eff.org/about/history

Aliens, C. "AlphaBay and Oasis Markets to Begin Accepting Monero for Payments." Deepdot.web. August 23, 2016. Accessed April 24, 2019. https://www.deepdotweb.com/2016/08/23/alphabay-oasis-markets-begin-accepting-monero-payments/

"Best Uncensored Search Engines for Anonymous Searching." Deep Web Links | Deep Web Sites | The Deepweb 2018. March 30, 2019. Accessed April 28, 2019. https://www.deepwebsiteslinks.com/uncensored-search-engines-for-anonymous-searching/

Buckelew, Joanne, Corben, and CaesarMK. "TOR vs The Freenet Project." SnapMunk. December 18, 2016. Accessed April 28, 2019. https://www.snapmunk.com/tor-vs-the-freenet-project/

Cimpanu, Catalin. "AlphaBay Dark Web Market Taken Down After Law Enforcement Raids." BleepingComputer. July 14, 2017. Accessed April 28, 2019. https://www.bleepingcomputer.com/news/security/alphabay-dark-web-market-taken-down-after-law-enforcement-raids/

Ciphas. "CGMC Review." Dark Web Reviews. January 23, 2018. Accessed April 28, 2019. http://darkweb.reviews/cgmc-review/

"Clearing Up Confusion - Deep Web Vs. Dark Web - Brightplanet". 2019. *Brightplanet*. https://brightplanet.com/2014/03/clearing-confusion-deep-web-vs-dark-web/

Cox, Joseph. "This Dark Web Market Just Started Offering Contracts for Anything." Motherboard. May 01, 2015. Accessed April 28, 2019. https://motherboard.vice.com/en_us/article/mgbwea/alphabay-contracts

Cox, Joseph. "What Firewall? China's Fledgling Deep Web Community." Motherboard. February 25, 2015. Accessed April 28, 2019. https://motherboard.vice.com/en_us/article/d735aa/what-firewall-chinas-fledgling-deep-web-community

Dark Web Academy, "History of the Dark Web/Deep Web," YouTube, March 26, 2016, , accessed April 28, 2019, https://www.youtube.com/watch?v=kPkKGzPTqGU

DashMagazine. "Immunity on the Dark Web as a Result of Blockchain Technology." Codeburst. June 19, 2018. Accessed April 28, 2019. https://codeburst.io/immunity-on-the-dark-web-as-a-result-of-blockchain-technology-6693eb087bdd

"Dream Market Review and URL." Deep Web Links | Deep Web Sites | The Deepweb 2018. April 03, 2019. Accessed April 28, 2019. https://www.deepwebsiteslinks.com/dream-market-url/

"Drugs, (Non)Violence, and Video Games: A Brief History of Silk Road." CoinCentral. August 25, 2018. Accessed April 28, 2019. https://coincentral.com/silk-road-history/

"Freenet – Another Secure Anonymity Browser." Dark Web News. January 14, 2018. Accessed April 28, 2019. https://darkwebnews.com/anonymity/freenet-secure-anonymity-browser/

Greenberg, Andy. "Global Web Crackdown Arrests 17, Seizes Hundreds Of Dark Net Domains." Wired. June 03, 2017. Accessed April 28, 2019. https://www.wired.com/2014/11/operation-onymous-dark-web-arrests/

Greenberg, Andy. "Your Sloppy Bitcoin Drug Deals Will Haunt You for Years." Wired. February 01, 2018. Accessed April 28, 2019. https://www.wired.com/story/bitcoin-drug-deals-silk-road-blockchain/

Holden, Ed. "An Introduction to Tor Vs..." IVPN. March 27, 2018. Accessed April 28, 2019. https://www.ivpn.net/privacy-guides/an-introduction-to-tor-vs-i2p

"How Does A Web Crawler Work? - Wp Themes Planet". 2019. *Wp Themes Planet*. https://www.wpthemesplanet.com/2009/09/how-does-web-crawler-spider-work/

"How Does Bitcoin Work?" Bitcoin. Accessed April 28, 2019. https://bitcoin.org/en/how-it-works

"How Whistleblowers Use the Darknet for Good." Dark Web News. February 27, 2018. Accessed April 28, 2019. https://darkwebnews.com/dark-web/how-whistleblowers-use-the-darknet-for-good/

"Is Tor Safe? Learn How Secure Tor Is." ProtonVPN Blog. February 27, 2019. Accessed April 28, 2019. https://protonvpn.com/blog/is-tor-safe/

Kptx. "BitBlender Review." Dark Web Reviews. February 14, 2017. Accessed April 28, 2019. http://darkweb.reviews/bitblender-review/

Liedke, Lindsay. 2019. "100+ Internet Statistics & Facts For 2019 You Should Know About". *Website Hosting Rating*. https://www.websitehostingrating.com/internet-statistics-facts/

McCormick, Ty. "The Darknet: A Short History." Foreign Policy. December 09, 2013. Accessed April 28, 2019. https://foreignpolicy.com/2013/12/09/the-darknet-a-short-history/

Naseem, Iflah, Ashirr K. Kashyap, and Dheeraj Mandloi. "Exploring Anonymous Depths of Invisible Web and the Digi-Underworld." *International Journal of Computer Applications (0975 – 8887)*: 21-24.

Peace and Conflict Monitor, Tor, Anonymity, and the Arab Spring: An Interview with Jacob Appelbaum. Accessed April 28, 2019. http://www.monitor.upeace.org/innerpg.cfm?id_article=816

PricewaterhouseCoopers. "Making Sense of Bitcoin, Cryptocurrency and Blockchain." PwC. Accessed April 28, 2019. https://www.pwc.com/us/en/industries/financial-services/fintech/bitcoin-blockchain-cryptocurrency.html

Rowe, Adam, and Adam Rowe. 2019. "What Is The Deep Web And How Can You Access It?". *Tech.Co*. https://tech.co/news/what-is-the-deep-web-2018-05

Saito, Takamichi, Kazushi Takahashi, Koki Yasuda, Kazuhisa Tanabe, Masayuki Taneoka, and Ryohei Hosoya. "Tor Fingerprinting: Tor Browser Can Mitigate Browser Fingerprinting?" SpringerLink. August 24, 2017. Accessed April 28, 2019. https://link.springer.com/chapter/10.1007/978-3-319-65521-5_44

Sameeh, Tamer. "Is The Tor Browser Fully Anonymous? (The Myth and Reality)." Deepdot.web. March 30, 2017. Accessed April 20, 2019. https://www.deepdotweb.com/2017/03/30/tor-browser-fully-anonymous-myth-reality/

Sameeh, Tamer. "Tor Fingerprinting – Is the Tor Browser Immune Against Browser Fingerprinting?" Deepdot.web. October 25, 2017. Accessed April 20, 2019. https://www.deepdotweb.com/2017/10/25/tor-fingerprinting-tor-browser-immune-browser-fingerprinting/

Sameeh, Tamer. "Research: Threats Vs Benefits of the Deep and Dark Web." Deepdot.web. October 28, 2018. https://www.deepdotweb.com/2018/10/28/research-threats-vs-benefits-of-the-deep-and-dark-web/

"Servers." Tor Metrics. Accessed April 28, 2019. https://metrics.torproject.org/relays-ipv6.html

Spencer, Wes. "The Silk Road: The Rise and Fall of the World's Largest Online Black Market." YouTube. October 11, 2013. Accessed April 28, 2019. https://www.youtube.com/watch?v=LkRhBOZSw38

Srivathsav, Raja, and Raja Srivathsav. "TOR Nodes Explained!" Medium. April 14, 2018. Accessed April 28, 2019. https://medium.com/coinmonks/tor-nodes-explained-580808c29e2d

"The Dark Web & Deep Web: How To Access The Hidden Internet Today". 2019. *Digital.Com*. https://digital.com/blog/deep-dark-web/

"The Future of the Darknet: 9 Critically Important Predictions." Futurist Speaker. January 23, 2019. Accessed April 28, 2019. https://futuristspeaker.com/business-trends/the-future-of-the-darknet-9-critically-important-predictions/

"The History of Silk Road: A Tale of Drugs, Extortion & Bitcoin." Blockonomi. November 20, 2018. Accessed April 28, 2019. https://blockonomi.com/history-of-silk-road/

"The Tor Network - FAQ". 2019. *Wordfence*. https://www.wordfence.com/learn/the-tor-network-faq/

"The Tor Project | Privacy & Freedom Online". 2019. *Torproject.Org*. https://www.torproject.org/about/history/

"The Tor Project | Privacy & Freedom Online." Torproject.org. Accessed April 28, 2019. https://www.torproject.org/about/reports/

"The Ultimate Guide to Tor Browser (with Important Tips) 2019." VpnMentor. Accessed April 28, 2019. https://www.vpnmentor.com/blog/tor-browser-work-relate-using-vpn/

"The US Government Has Been Funding the Gateway to the Dark Web." Home. November 05, 2017. Accessed April 28, 2019. https://www.thesiriusreport.com/technology/us-government-funding-gateway-dark-web/

"Transaction View Information about a Bitcoin Transaction." Bitcoin Block Explorer and Currency Statistics. Accessed April 28, 2019. https://www.blockchain.com/btc/tx/8088eeadbb0c6cbc6cc87ffacc05045f50195bd3837ec392a894465693578b57

Venkat. "Top 10 Popular Dark Websites." BLEEDBYTES. February 02, 2019. Accessed April 28, 2019. https://bleedbytes.in/top-10-popular-sites-in-the-deep-web/

WeUseCoins. "A Simple Guide To Effectively And Safely Mixing Bitcoins." What Is Bitcoin? Introductory Video and Current Bitcoin Price. Accessed April 28, 2019. https://www.weusecoins.com/a-simple-guide-to-effectively-and-safely-mixing-bitcoins/

"WikiLeaks Fast Facts." CNN. April 11, 2019. Accessed April 28, 2019. https://www.cnn.com/2013/06/03/world/wikileaks-fast-facts/index.html

"What Is Surface Web, Deep Web And Dark Web?". 2019. *Medium*. https://medium.com/@hackersleague/what-is-surface-web-deep-web-and-dark-web-cdbaf71b30d5

"What Is The Dark Web And Is It A Threat?". 2019. *BBC Guides*. http://www.bbc.co.uk/guides/z9j6nbk

"What Is Tor - How Does Tor Work - How to Use Tor." Tom's Guide. October 23, 2013. Accessed April 28, 2019. https://www.tomsguide.com/us/what-is-tor-faq,news-17754.html

"World Internet Users Statistics And 2019 World Population Stats". 2019. *Internetworldstats.Com*. https://www.internetworldstats.com/stats.html

Zhukova, Anya. "The Best Dark Web Websites You Won't Find on Google." MakeUseOf. March 02, 2019. Accessed April 28, 2019. https://www.makeuseof.com/tag/best-dark-web-websites/