

The Dark Web: Regarding The concealed Past of The Onion Router

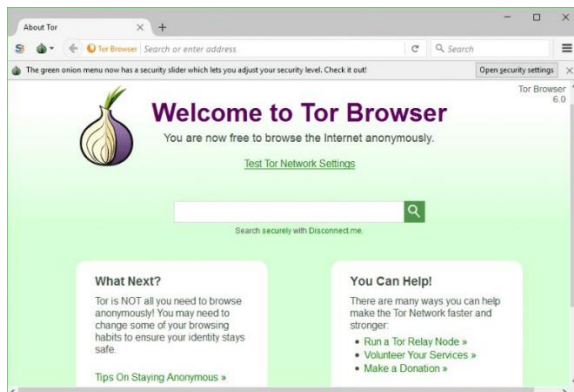
Kamile Simkute

Table of Contents

1	<i>Introduction to Tor</i>
1.1	Introduction
1.2	Timeline to map the historical period.....
2	<i>Tor and it's evolution</i>
2.1	Development
2.2	Changes
2.3	Concept to Existence.....
3	Technological Foundations of Tor
3.1	Blockchain.....
3.2	Networking Protocols.....
4	Other Actors Influence on TOR's Development
4.1	Government and State Actors.....
4.2	Funding and Regulation.....
5	Features of the TOR Browser
5.1	Browser Design and comparison with other Internet Browsers.....
6	How Tor can be measured
6.1	Network Performance Metrics.....
6.2	User Anonymity Metrics: Efficiency of Privacy.....
6.3	User Traffic.....
7	Contributors in the History of TOR
7.1	Individuals and Groups
8	The Technical Milestones and Challenges in TOR's History
8.1	List of Technical Advancements.....
8.2	Challenges and Solutions
9	Community and Open-Source Contributions to TOR
9.1	Achievements in Open Source Approach.....
10	Political Landscape in TOR Browser's historical Development
10.1	Digital Rights, Web Freedom in different parts of the world, Lobbying.....
11	Social and Cultural Dynamics of Tor
11.1	User Identity.....
12	Societal Impact of TOR
12.1	Consequences of TOR'S Development.....
12.2	Global.....
13	Conclusion
14	Bibliography

1 Introduction to Tor

1.1 Introduction



The TOR Browser webpage in 2020 [98]

The US Naval Research Laboratory launched the Tor project in 1995 with the goal of protecting users' internet privacy and anonymity [1]. The project's goal was to create an anonymous communication network for military use and to decouple identification from routing [2]. To safeguard confidential communications, the U.S. Navy created the Onion Router (TOR) network in the 1990s. TOR was first developed to safeguard U.S. intelligence communications, according to researchers Paul Syverson, Michael G. Reed, and David M. Goldschlag of the U.S. Naval Research Laboratory [3]. The initial alpha version was made available to the public in 1996, expanding its application past the Navy [3].

When TOR was made open source in 2002, anyone in the world could help to improve its security and privacy [3]. The Tor Project was formed in 2002 by Roger Dingledine, Paul Syverson, and Nick Mathewson to carry on the network's development [3]. By 2004, TOR was functioning as a stand-alone not-for-profit and in 2007 it started building bridges to assist users in getting around censorship [3]. Current data show that the network can accommodate over 6,000 nodes offering 25.5 Gbps of bandwidth in addition to over 2.5 million people using the network. Based on Mozilla Firefox, the Tor browser has features including HTTPS-Everywhere, NoScript, the Tor button, and the Tor launcher. By default, it runs in private mode and deletes browsing history when it closes [4].

1.2 Timeline to map the historical period

Oct. 29, 1969: Charley Kline, a UCLA student, transmits the first message via the ARPANET, but Stanford only receives the first two characters of "LOGIN". ARPANET is shortly followed by other "darknets," or clandestine networks [5].

1980s: The emergence of the contemporary web and the 1982 Internet protocol standard bring attention to the problem of unlawful or sensitive data storage. Physical "data havens" for illicit content exist in the Caribbean as early remedies [5].

Late 1990s: As the Internet expands, users are sharing copyrighted content on the darknet due to cheaper storage costs and file compression. Peer-to-peer networks give rise to open platforms such as Napster and hidden top sites [5].

March 2000: Ian Clarke launches Freenet, enabling anonymous access to pirated media. Clarke describes it as "a near-perfect anarchy" and suggests that businesses that are attempting to halt file-sharing [5].

September 20, 2002: Tor, an IP address-hiding program, is released by the U.S. Naval Research Laboratory. Although it was originally intended to protect operatives and dissidents, it also draws users of the darknet [5].

October 2002: Tor is initially used [6].

2003: About a dozen volunteer nodes, primarily in the United States but also one in Germany, are part of the Tor network [6].

2004: Roger and Nick's Tor work receives funding from the EFF for its usefulness in digital rights [6].

2006: The Tor Project, Inc. is incorporated as a 501(c)(3) nonprofit [6].

2007: The company starts building bridges to get across restrictions and reach the public internet [6].

2008: Tor Browser development gets underway [6].

January 3, 2009: The first Bitcoin is mined by Satoshi Nakamoto, and due to its secrecy and potential for criminal usage, it immediately becomes popular in the darknet [5].

2010: By safeguarding identities and getting around restrictions, the Tor Browser helps users during the Arab Spring [6]. According to ProCysive, there are 300 terrorist forums and 50,000 radical websites on the darknet, and terrorism is financed by pirated content [5].

June 1, 2011: Silk Road, a covert drug market accessible only to Tor and Bitcoin users, is revealed by a Gawker site. The value of Bitcoin jumps from \$10 to over \$30 as traffic increases [5].

August 1, 2013: Eric Eoin Marques, dubbed the FBI's top child porn facilitator, is taken into custody by Irish authorities. Due to an FBI sting utilising a Firefox breach to identify Tor users, his arrest and the closure of the darknet occur at the same time [5].

August 4, 2013: Ayman an-Zawahiri and Nasir al-Wuhayshi's al Qaeda discussions are intercepted by the United States, resulting in the closure of 21 embassies. Discussions had place on the "darknet" [5].

October 1, 2013: Ross Ulbricht, the man suspected of operating Silk Road, is taken into custody by the FBI. Between 2011 and 2013, the website brought in over \$1.2 billion [5].

October 4, 2013: According to The Guardian, the NSA was able to de-anonymize only a small portion of Tor users by taking advantage of technical weaknesses [5].

2 Tor and it's evolution

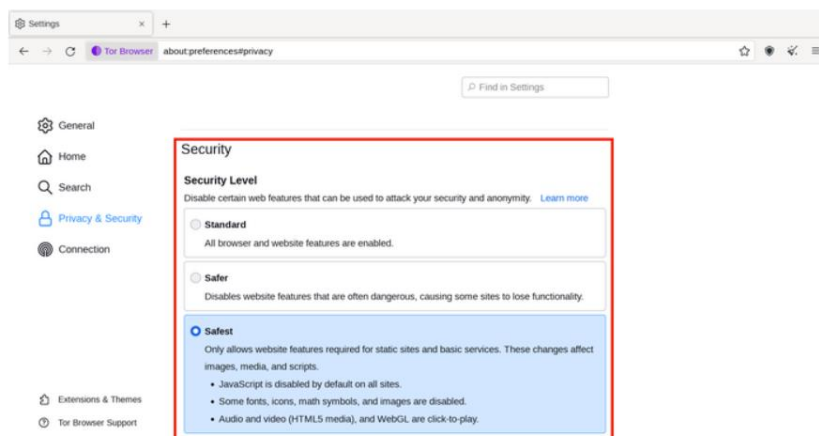


Figure 1: Website Features [7]

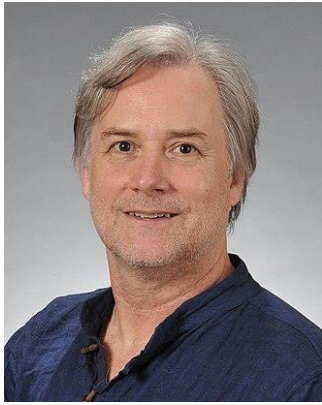
Tor Security

The Tor Browser instantly deletes cookies and history and isolates websites to prevent trackers and advertisements [7]. Additionally, it masks browsing behaviour so that external monitors only see Tor usage [7]. Users can further improve security by modifying site features in the Security Levels [7], even after Tor encrypts data. Click the Shield symbol next to the URL bar [7] to change these settings.

The Onion Service

Operating inside the Tor network, the Onion Service can only be reached by way of a three-hop Tor circuit that passes via three introduction points [8]. In order to conceal its location, it uses an anonymised circuit to upload a signed descriptor to a Tor distributed hash table [8]. The service then sends a "one-time secret" and establishes an anonymised circuit connection with a rendezvous location [8]. By matching strings between the client and the service, the rendezvous point confirms this secret [8]. Between the client and the service, it then passes encrypted messages [8]. Six relays are used by the Onion Service: three are selected by the client (which includes the rendezvous point) and three are selected by the service, which helps to protect location privacy [8].

2.1 Development



Paul Syverson [92]



David Goldschlag [93]

The pioneering research of Paul Syverson, David Goldschlag, and Mike Reed at the U.S. Naval Research Laboratory (NRL) is responsible for the creation of Tor. They laid the groundwork for onion routing, which subsequently functioned as Tor's architectural backbone [90].

Subsequently, the seminal paper "Anonymous Connections and Onion Routing" was released in 1998, offering more proof for Tor's conceptual basis [91]. Furthermore, the academic legitimacy of the thirteenth USENIX Security Symposium in 2004 was aided by its papers [94].

Following the release of its alpha version, which marked its first entry into public accessible, Tor began a significant shift from military restriction to public availability in 1996 [96]. The goal of Tor expanded transcend armed forces usage to let people to get around internet restrictions and navigate websites anonymously, led by Dr. Paul Syverson and a team of researchers who also included Roger Dingledine and Nick Mathewson [96].

The USA's government first sponsored Tor, but it gained notoriety after its alpha software was published in 2002 [96]. However, a significant transformation took place in 2004 when Tor broke away from its ties to the US governance to become The Tor Project, a nonprofit organisation devoted to independent advancement and the improvement of protections for privacy and security [96].

The evolution of Tor from a tool largely employed by the armed forces to a free to use network was marked by notable phases. Tor was first designed to protect American intelligence communications, but it soon became clear that it might have a wider social influence [96]. The non-profit Tor Project was established in 2002 with the goal of promoting anonymous online communication by making open-source and free software available. The launch of Tor's campaign for open online privacy was marked by this occasion [96].

2.2 Changes

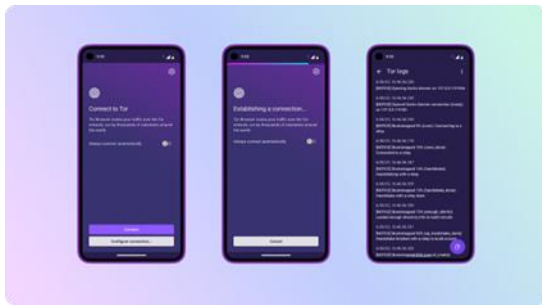
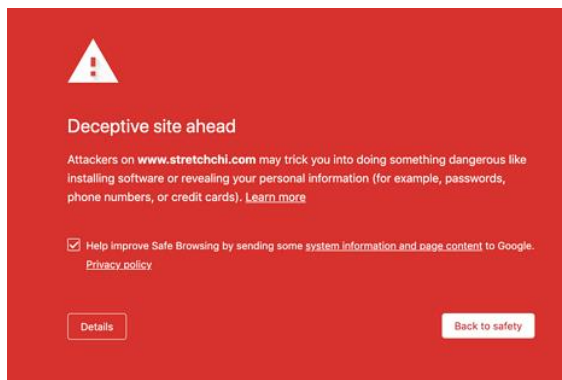


Figure 2: Connecting Tor on a smartphone [16].



Red Screen of Death Error [99]

More than four years ago, a community poll was utilised to choose the latest Tor Browser icon, sometimes known as the "onion logo," to replace the previous purple and green globe that was used in Tor Browser 8.5 [11]. The long-standing internal page referred to as "about: Tor," that hadn't been modified in a while, may also be redesigned thanks to this change [11].

The homepage of Tor Browser 13.0 has been updated with new program icons, a more straightforward layout, and the ability to redirect searches to the DuckDuckGo onion site [12]. Additionally, the updated homepage eliminates the prior "red screen of death" problem and enhances screen reader accessibility [12].

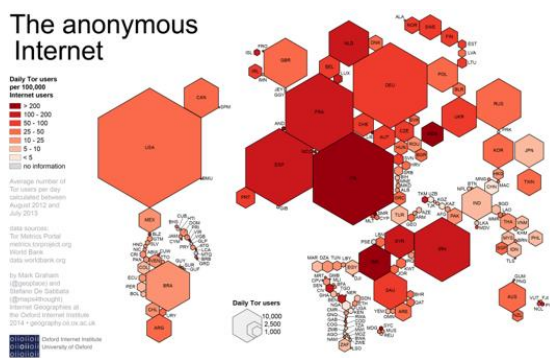
The Mullvad Browser logo has been integrated into a variety of materials, and new icons have been created for the Tor Browser [13]. "Letterboxing" was added to Tor Browser 9.0 to standardise viewport sizes and reduce the possibility of fingerprinting [13].

Enhanced native connectivity panels added to Tor Browser for Android improve user experience and set the stage for future developments such as Connection Assist [13]. Before the logs are relocated to "Connection Settings" in the Settings menu, matching the desktop version, users can auto-connect based on previous settings, access complete settings, and view new Tor logs [13]. Regardless of the state of their connection, users can now read Tor logs at any moment [13]. Additionally, an option to "copy all logs" at once removes the need for users to manually pick text.

The bridge card layout that was first presented in Tor Browser 11.5 has been replaced by a "compact card" style [13]. Pre-labels like "built-in," "sought from Tor," or "added by you" [13] identify the provenance of these additional bridge cards. Furthermore, users can now share all bridge cards simultaneously rather than one at a time when they have three or fewer [13].

2.3 Concept to Existence

The anonymous Internet



Daily Tor Users in 2014 [100]

volunteer TOR nodes, most of which were in the US and one node in Germany [290]. This unofficial spread represented the early stages of Tor's growth and community involvement.

The Tor Project, Inc. was founded in 2006 as a 501(c)(3) nonprofit company, driven by the realisation of the importance of ongoing progress [90]. This organisation laid the groundwork for organised efforts to increase Tor's functionality and accessibility.

The Tor Browser was developed in 2008 as part of a deliberate attempt to improve user experience and make the Tor network easier to use [90]. This project demonstrated a commitment to increasing Tor's usefulness and accessibility and marked a significant turning point in the project's development.

3 Technological Foundations of Tor

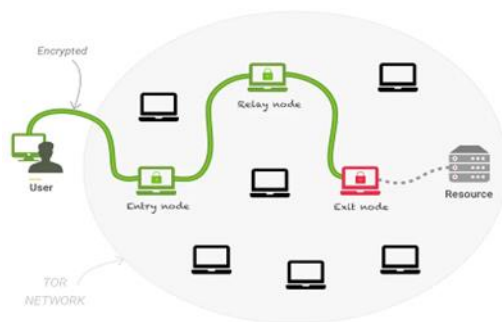


Figure 3: A simplified Tor Network [20]

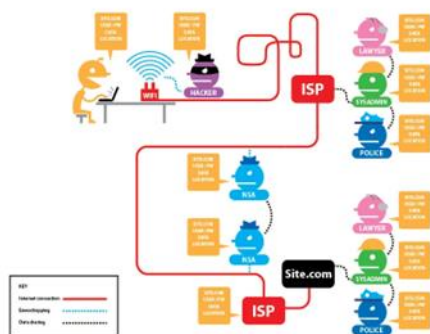


Figure 4: Information visible to eavesdroppers without HTTPS encryption [20]

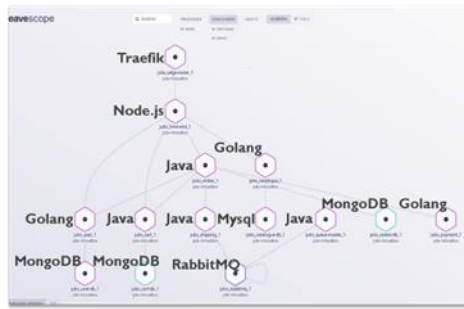


Figure 5: Virtual Private Network (VPN) [23]

● dizum (2)	17.28 MiB/s	12d 8h		45.66.33.45	-			443	80	Relay
● Serge (1)	939.28 KiB/s	33d 11h		66.111.2.131	2610:1c0:0:5::131			9001	9030	Relay
● moria1 (1)	500 KiB/s	15d 5h		128.31.0.34	-			9101	9131	Relay
● tor26 (1)	75 KiB/s	14d 22h		86.59.21.38	2001:858:2:2:aabb:0:563b:1526			443	80	Relay
● bastet (1)	50 KiB/s	13d 12h		204.13.164.118	2620:13:4000:6000::1000:118			443	80	Relay
● maatуска (8)	50 KiB/s	15d 8h		171.25.193.9	2001:67c:289c::9			80	443	Relay
● dannenberg (1)	40 KiB/s	14d 16h		193.23.244.244	2001:678:558:1000::244			443	80	Relay
● Faravahar (1)	40 KiB/s	1d 14h		154.35.175.225	2607:8500:154::3			443	80	Relay
● gabelmoo (1)	40 KiB/s	14d 20h		131.188.40.189	2001:638:a000:4140::ffff:189			443	80	Relay
● longclaw (1)	38 KiB/s	4d 9h		199.58.81.140	-			443	80	Relay

Figure 6: IP addresses [24]

A portion of the internet known as the "dark web" may only be accessed anonymously with the use of specialised browsers like Tor or I2P (Invisible Internet Project) [17]. Despite being frequently linked to illicit activity, intelligence services, media outlets, whistleblowers, and those subject to government limitations all utilise it [17]. Users simply need a specific browser to access the dark web; sophisticated hacking abilities or specialised OS systems are not necessary [18]. ". onion" links, which are unique to Tor and inaccessible through conventional browsers, are used by dark web sites [18].

To maintain anonymity, the Tor network distributes communication across a network of relays and employs three layers of encoding [18]. This system is intended to safeguard the locations, actions, and identification of its users. For even more anonymity, a lot of people additionally use VPNs [18]. Tor and related networks are not intrinsically linked to illegal activities, even though their purpose is to encrypt communications over the internet [18].

Every node in the overlay network that Tor builds keep a TLS connection open with every other node [20]. Tor creates a random circuit with a few nodes (usually three or more) to transport data [20]. Data transport may be slowed significantly when using more than three nodes [20].

An attacker may employ "traffic confirmation" to try to correlate entry and exit traffic if they examine unprotected communication coming into and going out of the Tor network [20]. Users using Tor are recommended to visit "HTTPS" websites in order to keep data leaving the exit node encrypted, which can assist prevent surveillance [20].

By distributing data across numerous randomly chosen nodes, Tor seeks to guarantee anonymity by preventing any one node from knowing a user's IP address and browsing history [20]. There are variations in price, efficiency, and security between Tor and VPNs, but both provide levels of secrecy and security [20]. Online anonymity is improved by using Tor [20].

By relaying encrypted data packets, the dispersed architecture of the Tor Network and its worldwide volunteer population promote privacy [20]. The network grows more resilient the more users there are that host relay nodes and use Tor [20].

The only long-term public deployment of the Onion Routing network was a short-lived, flimsy proof-of-concept [21]. Layered public-key cryptography and "mixes" are used by contemporary anonymity systems, such as Chaum's Mix-Net, to obfuscate sender-recipient relationships [21].

Together with other systems, Tor facilitates perfect forward secrecy and constructs circuits piecemeal [21]. While Tarzan and MorphMix utilise resource constraints to help prevent network control by attackers, Tor uses directory servers to govern node participation [21]. Participants in P2P schemes like Tarzan and MorphMix are responsible for both producing and relaying traffic to hide request origins [21]. To further obfuscate communication, "hordes" and systems such as Herbivore and P5 employ broadcast and multicast techniques [21].

Similar to how residences utilise mailing addresses, the protocol employs IP addresses to uniquely identify devices connected to the Internet [22]. A computer sends a message and contains its own IP address for a reply in addition to the recipient's [22]. IP addresses are broken down into binary numbers that are represented by decimal numbers, each of which represents a value according to bits [22]. These are referred to as "octets," and IPv4 addresses are conceivable [22]. Your IP address is detected by Google when you visit google.com [22]. As a result of ISPs assigning unique addresses—known as "dynamic IP addresses"—your IP address may vary every day [22]. Your IP address varies when you switch Wi-Fi networks since every provider has a different address range [22].



Figure 7: Diffie-Hellman key exchange [24]

The client and the starting node first build a TLS encrypted circuit, known as "CircID1," by using the Diffie-Hellman key exchange to generate a red AES key. [24]



Figure 8: Diffie-Hellman key exchange [24]

After, a blue key is generated by the client and the second node via the first node, with the first node creating "CircID2" and linking "CircID1" to "CircID2" [24].

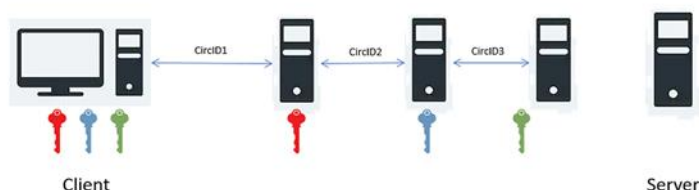


Figure 9: Diffie-Hellman key exchange [24]

Lastly, the client and the third node establish a green key using the first and second nodes; the second node establishes "CirclD3" and connects "CirclD2" to "CirclD3" [24].

Is worldwide web overlayed on top of internet?

Although they are different, the "Internet" and the "World Wide Web" (the Web) are sometimes confused.[25] The physical infrastructure of computer networks connected by wireless, fiber-optic, or copper wires is referred to as the "Internet". [25] The Web, on the other hand, is the software that runs on this infrastructure and is made up of URLs and hyperlinks that connect different web pages. [25] In essence, email, chat, file transfers, and the Web are just a few of the numerous services offered by the Internet [25].

The National Science Foundation (NSF) established the NSFnet in 1983, marking the start of the Internet's development. [25] Following 1985, several subnetworks came together and were enhanced by new TCP/IP (Transfer Control Protocol) protocols [25]. When he first suggested the idea in March 1989, Sir Tim Berners-Lee created the Web itself.[25] On November 12, 1990, he formalised the Web with assistance from Robert Cailliau. Berners-Lee created the first web browser, web server, and web pages by Christmas 1990 [25]. On August 6, 1991, Berners-Lee made the announcement of the Web's public launch on the alt. hypertext newsgroup [25].

Incorporating "hypertext" with the Internet to create "Uniform Resource Identifiers" (URIs) was Berners-Lee's revolutionary achievement [25]. The Web just needed "unidirectional links," which let users link to resources without the resource owner having to take any effort.[25] Compared to previous systems, this design made the construction of web servers and browsers simpler, but it also brought about the problem of "link rot." [25] The Web was non-proprietary, allowing independent creation of servers, clients, and extensions without licensing constraints, in contrast to proprietary systems like HyperCard [25].

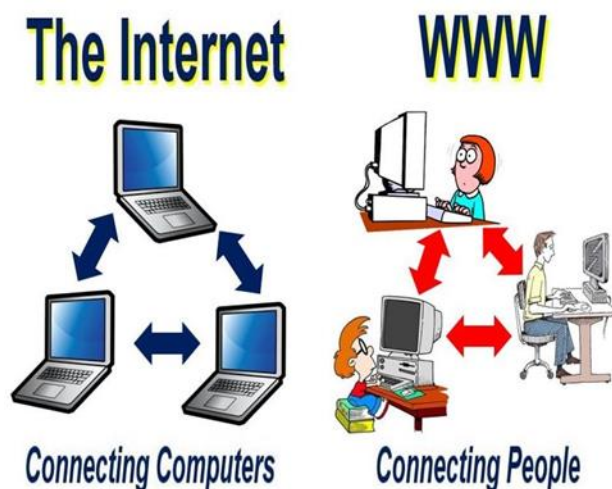


Figure 10 The Internet vs The World Wide Web [26]

How network overlays work:

Overlays provide extra functionality by making use of the underlying network's features. They can improve scalability, performance, and availability by caching static content [28]. When compared to the public Internet, a "routing overlay" offers wider-area connectivity with better throughput, reduced latency, and increased reliability [28]. These overlays are used for non-caching dynamic online content and live streaming [28]. Services such as those provided by

Akamai are prime examples of the "overlay philosophy" that aims to improve the underlying network by including new features [28]. This strategy seeks to enhance bandwidth and overall performance while lowering latencies and packet loss [28]. For instance, the overlay system optimises content delivery for a more seamless online page experience when a user inputs a URL [28].

3.1 Blockchain

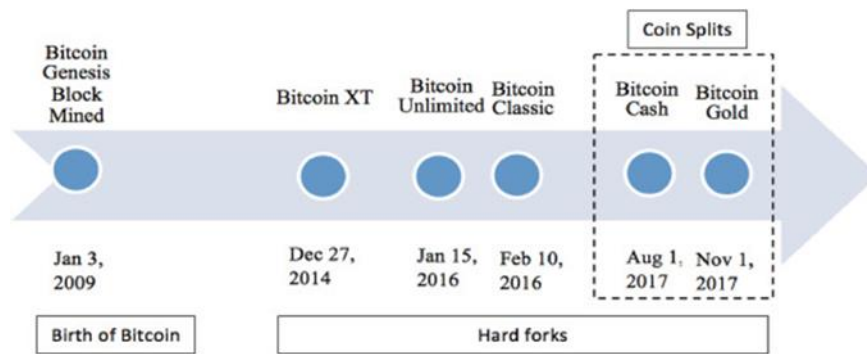


Figure 12: Bitcoin Timeline

[30]

Blockchain Technology

A "blockchain" system disperses confidence among numerous nodes as opposed to depending on one central authority, with each peer maintaining a copy of the ledger [29]. A "blockchain" is made up of connected blocks that are secured with public keys and contain transaction data, hashes, private keys, and nonces. Through hashes and nonces, each block keeps track of transaction times and refers to the one before it. By means of a consensus method, blocks are added [29].

With respect to the platform's configuration, blockchains can hold different kinds of data. Data integrity is ensured by cryptographic security and hash immutability [29]. "Smart contracts" carry out agreements, manage access, and automate processes [29].

The architecture and access mode of blockchains are used to classify them [29]. "Public blockchains" ensure openness by allowing for the open construction and validation of blocks, but they may also give rise to privacy problems [29]. Access is restricted to authorised individuals on "private blockchains" [29]. A consensus mechanism on a "consortium blockchain" is managed by a certain set of nodes [29].

Bitcoin and Blockchain Evolution

The first blockchain-based application was called "Bitcoin" [30]. According to popular belief, "Satoshi Nakamoto" [30] is an unknown person or group that created it. January 2009 saw the appearance of its genesis block. A decentralised digital currency called "Bitcoin" was created [30]. The project is a community-managed "open source" endeavour [30].

Through community discussion, blockchain applications like as "Bitcoin" can change, with significant modifications needing widespread support [30]. Conflicts may result in splits, and if both blockchains have enough support from the community, they may produce incompatible blockchains [30]. Notable coin splits like "Bitcoin Cash" and "Bitcoin Gold" have occurred for "Bitcoin," and the cryptocurrency has undergone several significant modifications or "hard forks" like "Bitcoin XT," "Bitcoin Unlimited," and "Bitcoin Classic" [30].

The blockchain, miners, core developers, exchange/marketplace operators, investors, merchants, hardware producers, and wallets are some of the major participants in the Bitcoin network [30]. By facilitating trade and promoting newly forked coins, exchanges and marketplaces can impact splits by bringing buyers and sellers together [30]. Depending on their position about the split, they can decide not to release new coins to traders in the event of a split [30].

Blockchain in Tor

"Blockchain" links each block to the preceding one cryptographically, ensuring data continuity and integrity [31]. By requiring most peers to act, "permissioned blockchain" systems can strengthen trust in "**Tor nodes**" through reputation evaluations, assisting in the defence against 51% attacks [31]. Many absentee peers may cause problems. Each peer adds an "empty block" to the committee to remedy this without affecting performance [31]. Due to resource limitations, a "Proof-of-Work blockchain" is inappropriate for Tor [31]. Rather, a "public permissioned blockchain" is suggested, in which every peer has an equal vote power. 14% and 5% of onion services, respectively, reference highly connected nodes, like hosting services and bitcoin explorers [85].

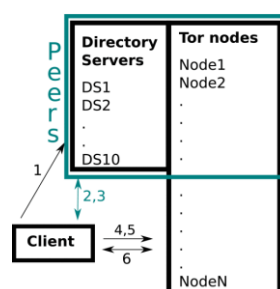


Figure 13: Nodes in Blockchain [31]

3.2 Networking Protocols

In "e-commerce," "financial transactions," and "government communications," network protocols safeguard critical data [32]. Violations of these protocols may result in serious repercussions [32].

As a result of the expansion of the Internet and the "World Wide Web (WWW)," three categories of networks have arisen: the "Surface Web," which is defined as websites that search engines index [33], the "Deep Web," which consists of websites that search engines do not index, like

medical information [33], and the "Dark Web," which can only be accessed with specialised software and includes websites on the Tor network [33].

The architecture of the Tor system, which was unveiled by the U.S. Naval Research Laboratory in 2004, is intended to conceal data [33]. An entry node allows data to enter, after which it is encrypted and transmitted over several internal nodes before leaving through an exit node. Detecting Tor traffic and identifying activities is made more difficult by this routing topology [33].

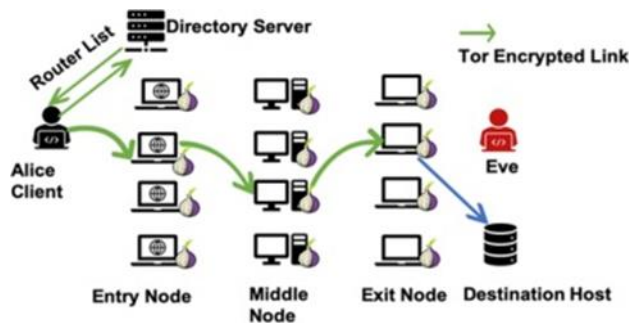


Figure 14: Tor Network Traffic [33]

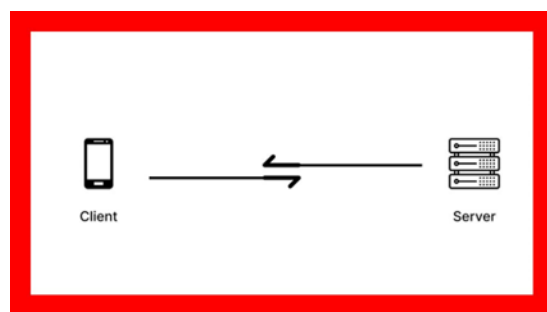


Figure 15: How HTTP protocol works [34]

IP addressing (IPv4) is used for site and machine identification and addressing on networks. To convert the domain name into an IP address, the request uses Domain Name Resolution (DNS) [35]. The client uses the IP address to establish a connection to the server using the service's address and port number [35]. Through this socket and protocol, data exchange takes place [35]. To keep the IP address anonymous and the connection encrypted, the client routes the request through several Tor relays and a Rendezvous Point (RP) [35].

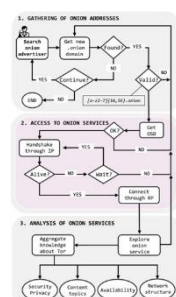


Figure 16: Flowchart of interaction with Tor onion services [35]

Users on the Tor network may be exposed by deanonymization techniques like network traffic analysis and vulnerability-exploiting [35].

Operating a Tor exit relay necessitates adjusting the Tor software bundle's settings [36]. Environment-related problems can include setting a recognisable DNS name, maintaining ISP

relationships, and configuring server settings [36]. The Tor community recommends identifying a good hosting site and alerting ISPs to possible problems [36]. Tor exit relays appear to be the source of abusers' and spammers' activities frequently [36]. It may be preferable to host the Tor relay through a hosting firm as opposed to at home [36].

Tor is a worldwide overlay network that establishes a virtual circuit with a minimum of three randomly chosen relays for every communication, thereby guaranteeing privacy and anonymity for user Internet traffic [36]. A directory server provides information on these relays, and the "Diffie–Hellman key exchange protocol" is used to share encryption keys [36]. At the source node, data packets are encrypted several times. As the packet moves forward, the matching relay node decrypts each layer of encryption [36]. Relays keep their privacy until the very last hop, only knowing about the relays that come before and after them [36]. The innermost layer of encryption is broken at the "exit node," after which the unencrypted data is sent to its intended location [36].

"HTTPS" over the Tor network preserves encryption of data between the final hop and the destination [36]. To maintain anonymity, the Tor browser modifies its path every 10 minutes [36]. Fig. 1 shows routing through the Tor network [36].

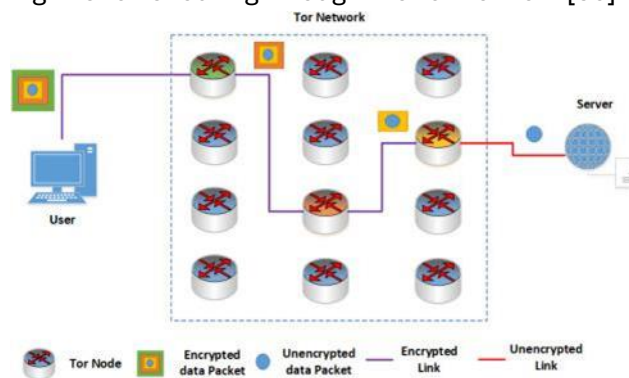


Figure 17: Onion routing [36]

The Tor Network powers connections made via it. 'Onion Routing,' which proxies requests through other Tor devices and shields a user's true IP address from exposure, is how Tor IP addresses are tunnelled through other devices on the network" [37]. Online activity is anonymised when requests are made via the Tor browser or network, which encrypts and routes them across several servers. Page loading speeds are slowed down by this mechanism [37]. Moreover, Tor can host hidden webpages that are only reachable via its network [37]. Every few seconds, IPQS updates its database of all active IP addresses in the Tor network [37].

Data interchange between computers is made possible by TCP/IP communication on the internet, which depends on the IP datagram [38]. It supports TCP and UDP protocols, among others, to guarantee dependable and effective data transfer [38]. Through intermediary routers, the network layer enables data transfer between hosts [38]. Information is encoded in an IP datagram and sent from host A to host B [38]. An IP address is a numerical identification that is assigned to every machine on an IP network and indicates its location [38]. Assigning addresses—which are often encoded as bit sequences—is necessary for node identification in a network [38]. The usage of fixed-length addresses is widespread [38].

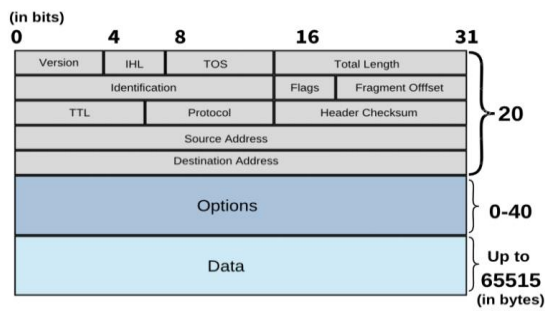


Figure 18: An IP Datagram [38]

Network Parameters	Class A	Class B	Class C
First Octet Range	1 to 126	128 to 191	192 to 223
Valid Network Numbers	1.0.0.0 to 126.0.0.0	128.1.0.0 to 191.254.0.0	192.0.1.0 to 223.255.254.0
# of Networks in Class	$2^7 - 2$	$2^{14} - 2$	$2^{21} - 2$
# of Hosts per Network	$2^{24} - 2$	$2^{16} - 2$	$2^8 - 2$
Size of Network Part of Address (bytes/bits)	1/8	2/16	3/24
Size of Host Part of Address (bytes/bits)	3/24	2/16	1/8
Default Mask	255.0.0.0	255.255.0.0	255.255.255.0

Figure 19: IPv4-Addresses [38]

4 Other Actors Influence on TOR's Development

The core concerns of Internet privacy, ownership, and governance were addressed in the initial stages of creation of Tor in the 1990s and early 2000s [39]. The Internet turned into a battleground between freedom and control following the fall of the Soviet Union, exposing conflicts within the neoliberal paradigm that supported free markets but opposed national sovereignty [39]. Dubbed as the "Crypto wars," this time concentrated on how encryption hampered security and law enforcement [39]. While cyberpunks and civil society organisations pushed for greater privacy, American policymakers sought to limit encryption to use by the government [39].

The sensitive nature of metadata—which may be used to identify trends and set control points—was also brought to light by the Crypto Wars [39]. The U.S. Navy created "Onion Routing," which combined military and civilian requirements to resolve privacy issues [39]. Its open-source architecture played a key role in encouraging a range of uses and trust [39]. On the other hand, timed attacks could be used by international enemies to uncover user patterns. Tor implemented "padding traffic" to obscure data patterns to prevent this, albeit system speed was occasionally impaired [39]. One important discussion during Tor's development concerned the inclusion of padding traffic [39].

4.1 Government and State Actors

Tor's development was greatly aided by DARPA, the State Department, and the Naval Research Laboratory, demonstrating the complex relationship between state interests and the network's inception [97]. These organisations had a key role in the development and funding of Tor, and

they made use of it in noteworthy occasions like the release of classified information by WikiLeaks, demonstrating the platform's typical application for activist and governmental purposes [97].

As part of its "Internet Freedom" effort, the State Department continues to fund Tor after its inception to aid political dissidents in nations such as Iran and Myanmar [97]. Tor's anonymity allowed the U.S. military to obtain sensitive material in a covert manner for covert intelligence operations [97].

The diverse user base of Tor, which includes activists and other groups in addition to intelligence agencies, was a major factor in the network's success as an anonymity source [97]. This widespread involvement was essential to maintaining the network's efficiency and guaranteeing strong privacy safeguards [97].

Early support from the Navy and DARPA was essential in turning Tor from a side project into a widely used technology [97]. By providing financing for the development of more user-friendly versions of Tor, the Electronic Frontier Foundation significantly contributed to the expansion of its usage [97]. Additional support from the State Department and the Broadcasting Board of Governors enabled the creation of the Tor Browser Bundle, which greatly increased the number of users of Tor and simplified installation [97].

As Tor gained popularity, it came under attack from several governments, including China, which attempted to stifle its use by blocking Tor relays [97]. Tor responded by using tactics like publishing bridge addresses to get around restrictions and keep its network operational, guaranteeing anonymity despite constant threats from state actors [97]. In addition to funding from the U.S. State Department and the National Science Foundation, the United States government provided significant financial support for the Tor project in 2012 [94].

The Russian government awarded a contract in 2014 to look at how to use the anonymous Tor network to obtain technical information about users and their devices [95]. The complicated nature of Tor's interactions with governments around the world came to light with this occurrence.

By encouraging corruption and fostering an atmosphere that encourages cybercrime, the Putin regime has promoted this network [40]. Comprehending this network is crucial to thwart Russian cyber operations. Russia's economy, which is impacted by sanctions and a downturn in the economy, is aided by cybercriminals [40]. The network's incentive structures, actors, and connections to the Russian government should all be examined by the United States and its allies. [40]

4.2 Funding and Regulation

Research funding from organisations such as the National Science Foundation goes towards "fundamental research on privacy and censorship," which includes developing new censorship circumvention techniques and enhancing Tor's performance and safety [41]. The goal of "building safer tools" for Tor Browser is accomplished by R&D support from institutions like DARPA and Radio Free Asia [41]. Funding for deployment and instruction from organisations such as the US State Department and the Swedish Foreign Ministry is allocated to "in-country security training," user-focused material, and helping activists globally to improve their online safety [41].

Major funding sources for the organisation are individual gifts and the Mozilla match. \$36,000 of the \$2,684,390 in revenue for the 2020–2021 fiscal year came from individual donors in the form of one-time gifts and monthly contributions [42]. Ten different cryptocurrencies were changed to USD as part of the donations. Contributions differ; some people donate once, while others give frequently or generously each year [42]. Unrestricted contributions from individual donations are crucial for developing tools, responding against censorship, and keeping emergency reserves [42]. Support from Sida, a Swedish government agency, allows for training, usability improvements, localisation, research with users, and support [42].

5 Features of the TOR Browser

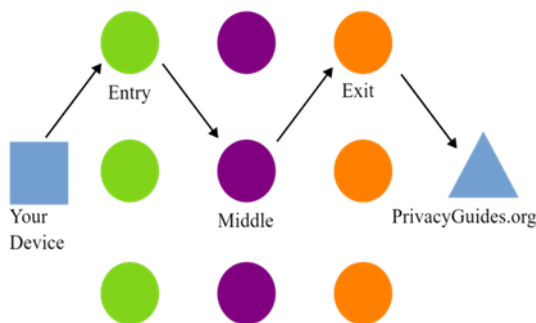


Figure 20: Tor Exit node [43]

A server that links the Tor Network to the internet is known as an exit node. [43] When utilising Tor, your data travels over three servers, creating a circuit, before arriving at its destination. [43] Your IP address is protected because websites you visit see the IP address of a Tor exit node. [43]

Tor makes use of a technique called "Onion routing," which is a multi-layer encryption scheme modelled after the structure of an onion. [44] These layered layers in onion routing are in charge of transferring data over virtual circuits and encrypting it many times. [44] Each layer on the client side decrypts the data before sending it to the next level, and the last layer decrypts the last bit of encryption to send the actual data to its intended location. [44] This procedure aids in hiding the user's IP address and location. [44]

By directing online traffic through many nodes, the Tor browser secures it. But since the exit node decrypts the communication, anyone keeping an eye on it may be able to see what users are doing [44]. Tor's security and privacy can be improved by using a VPN [44].

Onion addresses and the Onion Location functionality were promoted by the current #MoreOnionsPorFavor campaign [79]. This campaign gathers sysadmin requirements for simpler onion site deployment and management while showcasing the many applications of Tor [79]. With the privacy benefits of Tor, onion services provide HTTPS-like security for safe client-service interactions [79]. Tor is being added by numerous providers to improve privacy, security, and fight censorship [79]. Tor facilitates organisations and technology devoted to censorship avoidance, privacy, and anonymity [79]. A letter supporting the importance of digital trust and security was presented to the UN General Assembly, indicating the rising understanding of Tor's function in ensuring user security and trust [79].

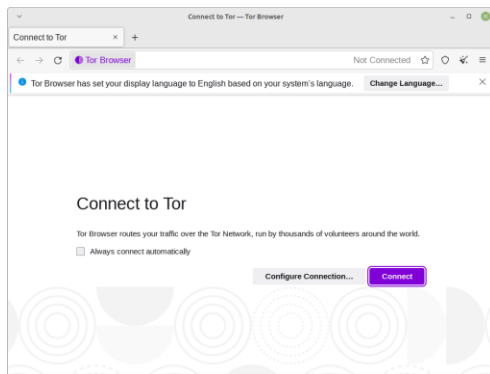


Figure 21: Connect tor network [44]

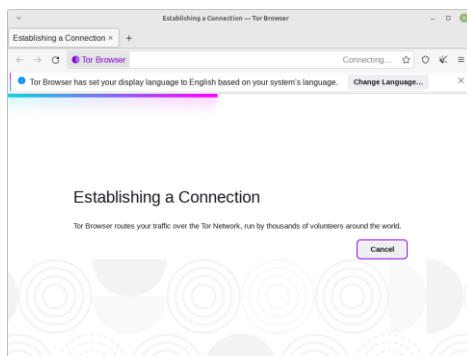


Figure 22: Establishing tor network [44]

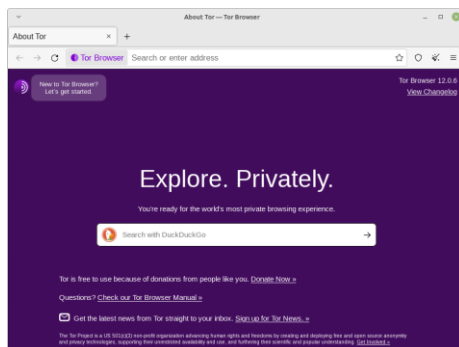


Figure 23: The welcome window/tab [44]

5.1 Browser Design and comparison with other Internet Browsers

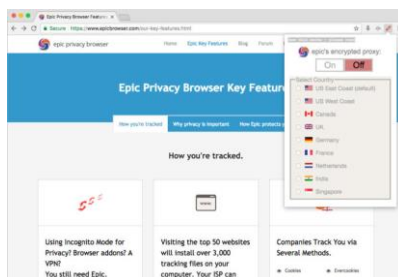


Figure 24: Epic Browser [46]

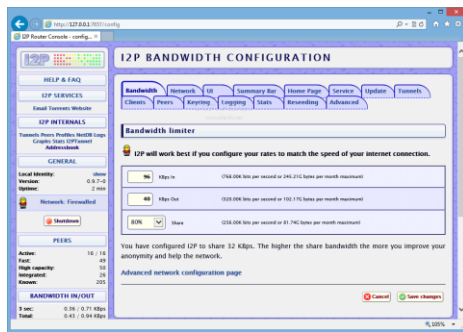


Figure 25: I2P Browser [46]

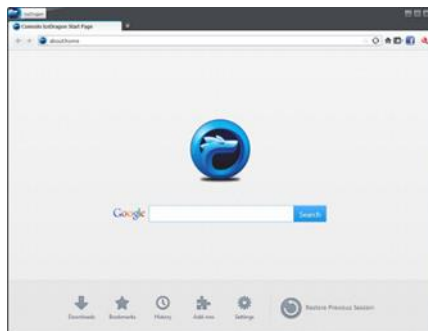


Figure 26: Comodo IceDragon [46]



Figure 27: Subgraph [46]

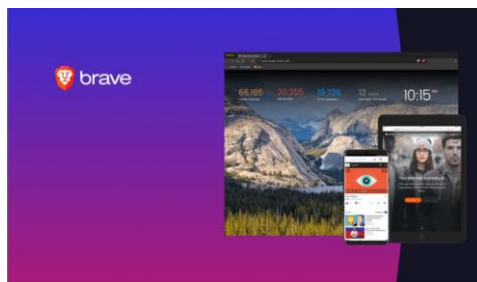


Figure 28: Brave [46]

Other services that are similar to Tor are Epic Browser, which is built on the source code of Chromium and has capabilities similar to those of Chrome. By default, it disables web trackers, scripts, advertisements, and other material. Plugins are supported to increase its capabilities. iOS and Android are two mobile operating systems that support Epic Browser [46].

The Invisible Internet Project, or I2P for short, uses Darknet technology to encrypt internet traffic and is designed to provide faster hidden services than Tor. To improve anonymity, traffic is routed through dispersed computers [46].

Comodo Ice Dragon has several features designed to increase security and privacy. It has an integrated ad blocker and VPN, as well as a site inspector that checks websites for viruses [46].

Brave is a web browser that works with a variety of operating systems, such as Linux, Mac, Android, and iOS. Users can enable a Tor connection within a tab using the Private Window feature of the most recent version, which also provides a Tor Onion service for increased security [46].

DuckDuckGo is a privacy-focused web browser that disables invasive advertisements, eliminates data collecting, and blocks trackers. In order to safeguard connections, it employs encryption and has a "privacy meter." Major devices and operating systems are compatible with it [47].

A Chromium-based browser called Iridium reroutes traffic from unsafe websites and prevents cookies and trackers. It works with Mac and Windows and supports Qwant or DuckDuckGo as the default search engines [47].

Puffin Browser offers encrypted cloud protection, private surfing, and proxy services to conceal IP addresses. Tox is an instant messaging program that offers safe communication with open-source encryption [47].

Freepto is a Linux program that uses encryption to improve privacy online and get around internet censorship. Peer Blocks is helpful for torrenting because it conceals IP addresses and blocks malicious ones [47].

6 How Tor can be measured

More than 3,000,000 users and more than 6,500 volunteer-run relays make up the Tor network [48]. Serving more than 40,000 users, it consists of more than 1,900 volunteer-run bridges that assist users in accessing the network in restricted regions [48]. Tor Metrics offers statistical analysis to comprehend the network's scalability, blocking attempts, and performance [48]. These statistics and query tools allow relay and bridge operators to view their contributions within the network [48]. Tor developers can learn more about network security and performance with the use of metrics [48].

To safeguard privacy, Tor relays and bridges only provide country-specific information when providing aggregated statistics on bandwidth and use [49]. CollecTor archives and forwards these statistics to directory authority [49]. The metrics-lib Java package can be used to analyse the public archive [49]. Customisable historical data visualisations, including relay, bridge, download, traffic, user, and traffic statistics, are available on the Tor Metrics website [49].

6.1 Network Performance Metrics

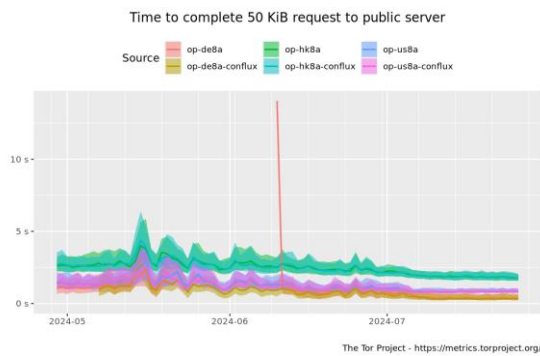


Figure 29: downloading static files Graph [50]

The performance of downloading static files of different sizes via Tor, from onion servers and public internet servers, as depicted in this graph [50]. It shows the range from the first to third quartile, highlights the median, and excludes the slowest and fastest quartiles. It contains times for both whole and partial downloads of larger files [50].

Every fifteen minutes for a whole day, relays and bridges gather statistics on bytes transported; this data is included in extra-info documents submitted to directory authorities [51]. In order to detect load-balancing problems, exit nodes report bytes and streams by leaving port, whereas relays are required to send statistics on bytes and cells in local queues [51].

6.2 User Anonymity Metrics: Efficiency of Privacy

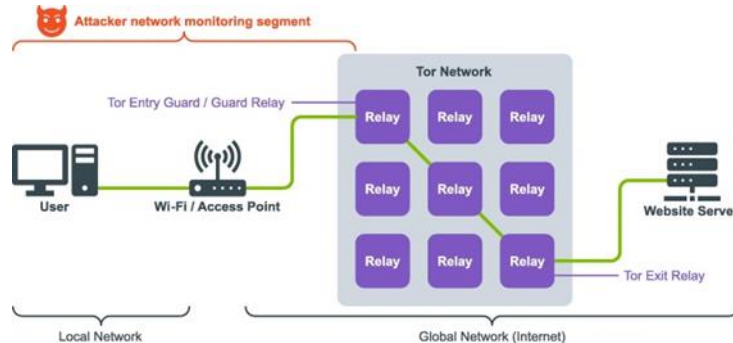


Figure 30: Global Network [52]

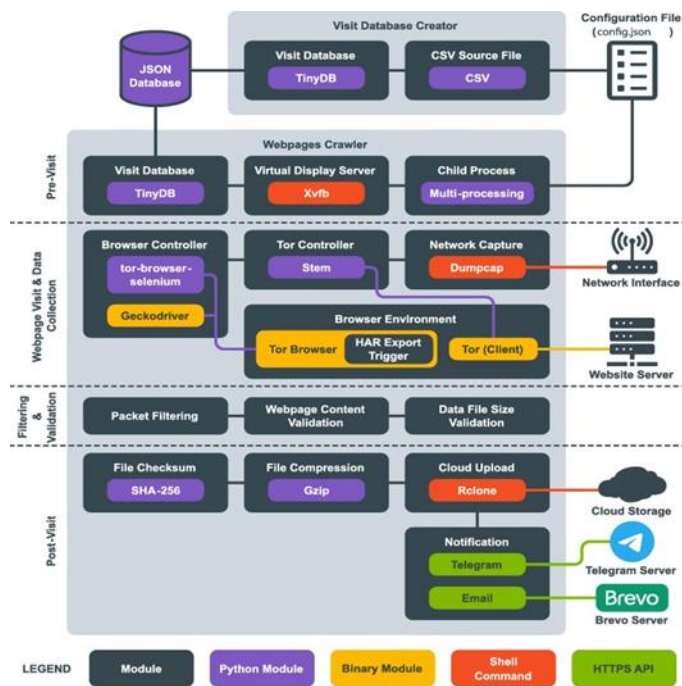


Figure 31: The WFP-Collector's main architecture [52]

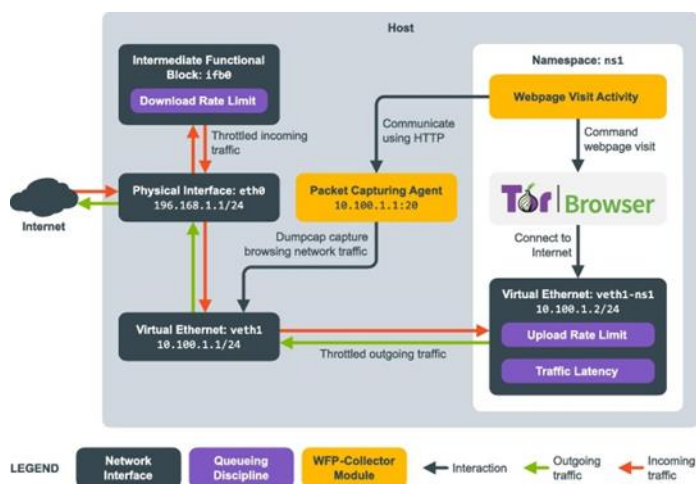


Figure 32: Network throttler implementation in WFP-Collector [52]

By providing anonymity and concealing users' online activities, the Tor Browser is intended to improve privacy [52]. Tor's multi-layer encryption and relay architecture is complicated, making it difficult to follow user behaviour [52].

By examining network packet metadata, a technique known as Website Fingerprinting (WFP) has aimed to identify the websites that are visited [52]. Because WFP may influence Tor's anonymity and privacy, it is a topic of investigation [52]. Other privacy solutions can also benefit from the use of effective WFP techniques [52].

Attackers utilise machine learning algorithms developed on massive datasets to identify and classify webpages while keeping an eye on network activity in order to carry out WFP assaults [52]. These days, machine learning advances include training on 90 out of every 100 observed webpages [52].

Using Selenium, the tor-browser-selenium library automates Tor Browser functions, enabling headless operation and automated surfing [52]. Because this library is compatible with the security characteristics of the Tor Browser, it is utilised in WFP experiments [52].

The Network Monitor tool provides access to the network throttler feature in the Tor Browser, which lets you set upload and download limitations [52]. Dumpcap is used by WFP-Collector to record network traffic, including the impact of outgoing traffic throttling [52].

Before viewing a webpage, users must open the Network tab of the Tor Browser and access the Developer Tools to get HTTP Archive (HAR) data, which includes webpage asset information [52].

Tor provides web anonymity with a second-generation onion router system [53]. The Tor network encrypts data at various layers and routes it through onion routers that are chosen at random, making it impossible for a single node to know the source and destination IP addresses [53]. Tor is intended to shield users against censorship, tracking, and surveillance [53]. It boasts 3 million users globally and more than 6,000 intermediary nodes [53].

6.3 User Traffic

Every day, the Onion Router (Tor) manages massive amounts of data and allows anonymous internet use [54]. Tor poses a problem to network managers in corporate settings. Effective traffic monitoring and threat identification are made more difficult by Tor's multi-layered encryption [54]. Because of its anonymity, there is a greater chance of malevolent activity, and it is more challenging to identify individuals who are engaged in illegal activity [54]. Tor's decentralised architecture creates security flaws as well, necessitating ongoing monitoring and possibly increased resource allocation and bandwidth utilisation [54]. Because Tor traffic is anonymous, it is difficult to enforce policies and restrict it [54].

Different kinds of encrypted communications are recognised using methods like encrypted traffic classification based on path signatures [54]. Techniques for separating Tor traffic from other network traffic, such as Support Vector Machines (SVM) and Long Short-Term Memory-based Recurrent Neural Networks (LSTM-RNN), function well [54]. Time-based features also help in detecting Tor traffic, and deep learning enhances accuracy by exposing better data linkages; performance metrics such as classification time are critical in assessing efficacy [54].

Label	Motivations for using the Tor network	# Answers	(%)
MOT_01	I want to protect my data from systems and organizations that evaluate personal information and/or pass it on to third parties.	101	84.17
MOT_02	I use Tor for political reasons.	35	29.17
MOT_03	I would like to offer and/or consume material that is potentially illegal.	25	20.83
MOT_04	I would like to have an informative exchange on topics with a specific target group.	20	16.67

Figure 33: Motivations [55]

7 Contributors in the History of TOR

7.1 Individuals and Groups



Figure 34: United States Naval Research Laboratory (NRL) [56]



Figure 35: Open Technology Fund [59]



Figure 35: Sida [59]



Figure 36: Fastly [59]



Figure 37: U.S. Department of State Bureau of Democracy, Human Rights, and Labor [59]

Craig Newmark
Philanthropies

Figure 38: Craig Newmark Philanthropies[59]



Figure 39: Zcash Community Grants [59]



Figure 40: [59] Ford Foundation

#start small

Figure 41: [59] #StartSmall



Figure 42: [59] Omidyar Network

OPEN SOCIETY
FOUNDATIONS

Figure 43: [59] Open Society Foundations



Figure 44: [59] Wasabi



Figure 45: [59] Open Net Fund

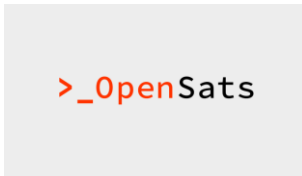


Figure 46: [59] OpenSats

People and Organisations Endorsing Tor

The Open Technology Fund (OTF) finances initiatives aimed at assisting individuals in using Tor to elude censorship and shield themselves from surveillance, as well as technology-centric solutions for censorship and surveillance problems [59].

The Tor Project received an unrestricted donation from **Craig Newmark Philanthropies** [59].

A initiative to develop "Arti," a Rust version of the Tor protocols, is supported by the **Zcash Community Grants (ZCG)** [59].

Jack Dorsey's charitable endeavour, **#StartSmall**, has given the Tor Project a general support donation [59].

The Tor Project has received general support funding from the **Ford Foundation** [59].

Founded by Pam and Pierre Omidyar, **Omidyar Network** is funding an initiative to share user stories regarding the value of encryption [59].

George Soros funded the **Open Society Foundations**, which provide funding for Tor to teach activists and human rights defenders in digital safety and security [59].

The Onion Service Resource Coalition is sponsored by **Wasabi and zkSNACKs**, the Wasabi-developing research and development business [59].

A grant from **OpenNet.fund (ONF)** was given to enhance the Tor infrastructure and bridge distribution tools [59].

Two onion service developers received funding from **Open Sats Initiative, Inc.** [59].

8 The Technical Milestones and Challenges in TOR's History

Configuring v3 Onion Services

Service side

To configure client authorization on the service side, the

`<HiddenServiceDir>/authorized_clients/` directory needs to exist. Following the instructions described in the section [Setup](#) will automatically create this directory. Client authorization will only be enabled for the service if tor successfully loads at least one authorization file.

Contribution from Open Source

Because TOR is open source, it has encouraged community involvement and ongoing development. The resilience of TOR against censorship and surveillance has been strengthened by contributions from volunteers around the world [60].

Bridging

Relaying Information in TOR makes it easier to access “.onion” websites, which search engines do not index, and it helps get over regional limitations to access content that is restricted globally [60].

Defending Privacy and Combating Surveillance

By encrypting data and passing it across several relays, TOR protects privacy by making it impossible for outside parties to track down online communications. For consumers under repressive regimes or under monitoring, this is essential [60].

Current Difficulties and Upcoming Advancements

Even with its popularity, opponents trying to take advantage of weaknesses pose a threat to TOR. New solutions such as "Tor Hidden Services v3" promise to improve security and overcome previous shortcomings, demonstrating the importance of ongoing research [60].

8.1 List of Technical Advancements

Enhanced Security and Encryption

To protect user privacy, TOR has continuously improved its encryption, making it harder for outside parties to track or intercept activity [63].

Improved Network Efficiency

As TOR gained mainstream, developers implemented relay bridges and optimised bandwidth to address latency and congestion, resulting in a notable increase in network speed and dependability [63].

Taking Scalability into Account

The Tor cloud was introduced by TOR in response to growing user demand, allowing users to build virtual bridges that balance network traffic and improve resilience [63].

Support for Mobile

Recognising the popularity of mobile devices, TOR created applications for them, such as the Android version of Tor Browser, which enables safe mobile browsing on tablets and smartphones [63].

Scholarly Investigation and Cooperation

Because TOR is open source, it encourages international research and collaboration, which leads to ongoing innovation and a better comprehension of its advantages and disadvantages [63].

Continuous Assistance and Updates

To fix vulnerabilities and defend against new threats, the TOR community provides frequent updates and patches [63].

8.2 Challenges and Solutions

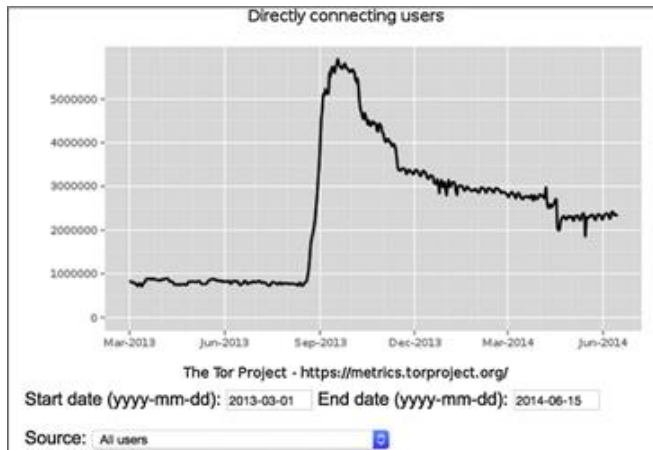


Figure 48: The presumed number of connecting users on the Tor Network from March 1st, 2013, to June 15th, 2014. [65]

Challenges

Access and Censorship: Censorship is a problem for the Tor Network, especially in nations with stringent internet laws. The Great Firewall (GFW) in China can censor access to Tor sites, including those with the “. onion” name [Christin, 2012]. [64].

Resolutions

Obfs4 Bridges: Users can utilise obfs4 bridges, which are accessible via the Tor Browser, bridges.torproject.org, or by sending an email to bridges@torproject.org, to get around censorship. Another alternative is to build bespoke obfs4 bridges, albeit many of these might not function in China. The Salmon system contributes to the difficulty of the GFW blocking obfs4 bridges [66].

Snowflake

More resilient alternatives, such as Snowflake, which currently has over 6,000 proxies and is almost ready for stable release, are the focus of efforts to overcome obstacles. To enhance bridge distribution, plans call for swapping out BridgeDB for a more adaptable system [66]. Included in the alpha version of the Tor Browser, Snowflake is an experimental mechanism meant to enhance performance in environments with restrictions, such as China. Its efficacy has increased with recent versions, which include new STUN servers [66].

Meek-Blue

Traffic caps cause Meek-azure, which operates internationally and is intended to operate behind the GFW, to operate slowly [66].

Endpoint security and protocol

A dependable endpoint (such as Snowflake proxy) and a resistant protocol (such as WebRTC or obfs4) are needed for effective circumvention. The GFW has trouble with obfs4, but it can identify previous protocols. BridgeDB is still useful, but securing bridge distribution is still difficult [66].

9 Community and Open-Source Contributions to TOR

9.1 Achievements in Open-Source Approach



[105]

Its open-source nature has brought to light some flaws and made major accomplishments possible. Because Tor is run by volunteers rather than by a single organisation or government, one of its main advantages is that it is resistant to shutdowns [72]. By directing requests via several levels, it successfully masks users' IP addresses, guaranteeing anonymity and privacy [72]. Furthermore, Tor's privacy features are widely accessible due to its free usage [72]. Additionally, it aids users in getting around geographic limitations, enabling access to content that could be prohibited where they are [72].

10 Political Landscape in TOR Browser's historical Development



[104] Arab Spring, 2010

Widespread demonstrations in support of political change and democracy took place throughout the Middle East and North Africa during the Arab Spring, which started in late 2010 [73]. TOR was essential to activists during this turmoil because it gave them a way to organise, communicate, and share information without being recognised. Information flow and solidarity among protestors were greatly aided by activists' ability to get around censorship, access prohibited websites, and establish safe communication channels thanks to TOR's encryption and routing [73]. Despite its importance, TOR's efficacy differed by location as authorities looked for more ways to monitor and identify users [73].

The 2019 Hong Kong demonstrations against a planned extradition bill demonstrated the ongoing significance of TOR. Protesters got beyond China's "Great Firewall" and surveillance by using TOR to share material, organise covertly, and hide their identities while accessing restricted websites and becoming visible worldwide [73]. Activists, however, continued to confront difficulties as Chinese authorities adjusted to resist TOR [73].

The fact that TOR is a part of these initiatives emphasises how important it is to promote free speech and avoiding censorship. Although TOR has proved helpful for identity protection and encrypted communication, there are still a lot of obstacles to overcome due to growing government awareness and surveillance capabilities [73]. In an age of growing censorship and surveillance, the continued development of TOR and related technologies is essential to maintaining online freedom [73].

10.1 Digital Rights, Web Freedom in different parts of the world, Lobbying



Kyoto 2023 [103]

The Tor Project seeks to advance technology that protects privacy, like encryption, in order to improve human rights [74]. Over the years, they have actively taken part in lobbying activities to support encryption and oppose government efforts to abolish it. This means composing letters, supporting ally organisations, and stepping up outreach and education [74]. The Tor Project had held a workshop at the UN-established Internet Governance Forum (IGF), a forum for multi-stakeholder discussion on internet public policy.

The panel "Encryption's Critical Role in Safeguarding Human Rights," which included experts from the domains of technology, non-profits, policy, human rights, and advocacy, discussed striking a balance between national security, privacy protection, and international human rights [74]. Details on the ideas the panel considered for creating an encryption regulatory framework with a human rights focus can be found in the session report [74].



Help Censored Users

The "Help Censored Users, run a Tor Bridge" campaign has been introduced by Tor to get more volunteers to build bridges. 200 additional obfs4 bridges were successfully installed during this campaign, increasing the total to almost 400 new bridges [76]. To preserve access for customers in Russia, more bridges might be required if censoring practices from a few Russian ISPs became widespread [76]. Researchers have discovered that in some regions of Russia, the default bridges in the Tor Browser—such as the Snowflake and obfs4 bridges from Moat—do not function [76].

12 Societal Impact of TOR

Definition of Sybil Attack

- In this paper**
 - A malicious device illegitimately takes on multiple identities.
 - The additional identities are called *Sybil nodes*.
- Question:**
 - How does an attacker create Sybil nodes and use them?



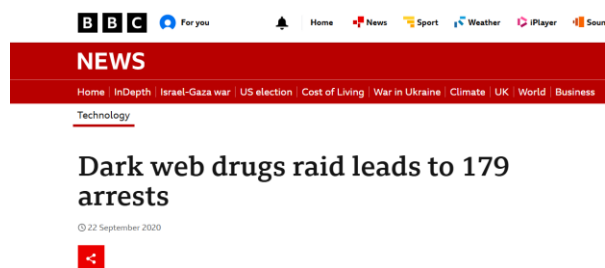
An attacker can create various identities [102]

Pfritzmman and Köhntopp (2001) and Reiter and Rubin (1998) formalised the mainstream definition of network anonymity, which emphasises keeping the states and attributes of communicating entities identical to prevent communication links from being identified [81].

By enabling anonymous communication via multi-hop pathways and tying anonymity to participating nodes, the Tor network has had a profound impact on society [80]. Assessing the anonymity of individual nodes is essential to comprehending how modifications to node states impact the network as a whole [80]. To reflect how changes in node anonymity affect the network dynamically, our evaluation integrates network-level measures with a variety of feature indicators to capture representative and real-time changes in node anonymity [80].

Tor's role in safeguarding online privacy is indicative of its societal significance, even in the face of increasingly sophisticated assault techniques aimed at anonymity networks. Among the notable risks are denial-of-service attacks, which prevent communication and allow traffic analysis, and the Sybil attack, which obscures high-performance nodes to interfere with node selection [81]. The efficacy of anonymity systems and their capacity to protect users are at stake due to these attacks [81].

12.1 Consequences of TOR'S Development



179 people arrested in EU and US [101]

The Way Tor Affected Other Domains

To get around restrictions and maintain their anonymity, activists utilise Tor [9]. Tor is used by the military for planning and secure communications [9]. Families utilise Tor as a privacy

safeguard [9]. Journalists use Tor to securely communicate with sources and conduct story research [9].

According to the Tor Project website, Tor is not a significant instrument for illegal behaviour. The website claims that thieves frequently make use of additional instruments like malware, botnets, stolen devices, and identity theft [9]. Furthermore, Tor can aid in defending against certain criminal strategies like identity theft and online stalking [9].

Security engineer Alec Muffett, a board member of the Open Rights Group, pointed out that onion addresses, which are used on the Silk Road and the dark web, lessen the possibility of censorship because they do not save identifying information [10]. He went on to say that the Tor network links participant computers into what is referred to as Onion Space, creating a different network space from IPv4 and IPv6 [10].

The dark web has provided access to both legally held and black-market firearms, frequently at lower prices than those found on the street, so facilitating a range of illicit operations, including arms dealing [82]. Though Europe is the main market with substantially higher profits than the US, the US is still a key source of firearms posted on the dark web [82].

42% of dark web listings are for firearms, with digital products related to weaponry coming in second at 27% and ammunition at 22% [82]. Because of the anonymity of the dark web, people and organisations looking for guns and ammunition are drawn to it, which presents serious difficulties for law enforcement [82].

Analysis of Tor sites is done to find illicit activity [83]. On 45% of onion services, automated content analysis detects illicit content including child sexual abuse, hacking services, or black-market items [83]. Nonetheless, it was discovered that 47% of these websites, which included file sharing and discussion boards, were moral [83].

During an Austrian police raid on William Weber's flat in Graz in 2012, gear for controlling Tor exit nodes overseas was taken. Weber's false suspicion was caused by the fact that some Tor users have downloaded child pornography using these nodes [84]. After being found guilty on June 30, 2014, of assisting in the distribution of child pornography, Weber was sentenced to three months of suspended jail time and three years of supervision [84]. He declined to appeal, giving personal and financial justifications, which stopped the case from being further reviewed by the courts [84].

12.2 Global



[107] *The great firewall of China*

With thousands of new nodes throughout the world, the Tor network has grown dramatically, improving anonymity and privacy [87]. Computers known as nodes are used to transmit

encrypted data, enhancing network security [87]. Using unlisted bridges, Tor has proven essential in getting beyond censorship, including China's Great Firewall, in order to access content that is forbidden [87]. Tor allowed activists to safely exchange information and communicate during government surveillance during the 2010 Arab Spring [87]. In 2019, Tor allowed protestors in Hong Kong share material, get around security measures, and access websites that were restricted while still protecting their identities [87].

13 Conclusion

Tor has advanced significantly in tackling issues with online surveillance and censorship, making it a trailblazing instrument in the field of digital privacy and anonymity. Internet freedom has been significantly impacted by its growth and worldwide reach, especially under repressive governments and during pivotal events like the Arab Spring and the uprisings in Hong Kong [87]. As a result of its ability to facilitate safe communication and access to content that is forbidden, Tor has grown to be a vital tool for privacy advocates, journalists, and activists everywhere [86].

Even with its achievements, Tor still must contend with growing government monitoring programs and changing attack techniques [81]. The network's critical role in preserving online privacy is highlighted by its capacity to uphold anonymity while fending off these threats. Tor's contributions to digital rights and global information access are still essential as it continues to develop with features like enhanced encryption and scalability solutions [87]. Tor is a prime example of how cooperative technology may be used to protect basic human rights because of its ongoing community involvement and open-source contributions [74].

14 Bibliography

Jadoon, A. K., Iqbal, W., Amjad, M. F., Afzal, H., & Bangash, Y. A. (2019a). Forensic Analysis of Tor Browser: A Case Study for Privacy and Anonymity on the Web. *Forensic Science International*, 299, 59–73. <https://doi.org/10.1016/j.forsciint.2019.03.030>[1]

Jadoon, A. K., Iqbal, W., Amjad, M. F., Afzal, H., & Bangash, Y. A. (2019b). Forensic Analysis of Tor Browser: A Case Study for Privacy and Anonymity on the Web. *Forensic Science International*, 299, 59–73. <https://doi.org/10.1016/j.forsciint.2019.03.030>[4]

McCormick, T. (2013, December 9). The Darknet: A Short History. *Foreign Policy*; Foreign Policy. <https://foreignpolicy.com/2013/12/09/the-darknet-a-short-history/>[5]

Mehta, S., & Upadhyay, D. (n.d.). A Review on Classification of Tor-Nontor Traffic and Forensic Analysis of Tor Browser. Retrieved August 1, 2024, from <https://www.ijert.org/research/a-review-on-classification-of-tor-nontor-traffic-and-forensic-analysis-of-tor-browser-IJERTV9IS040701.pdf>[2]

Quintin, C. (2014, July 1). 7 Things You Should Know About Tor. Electronic Frontier Foundation. <https://www.eff.org/deeplinks/2014/07/7-things-you-should-know-about-tor>[9]

SECURITY SETTINGS | Tor Project | Tor Browser Manual. (n.d.). [Tb-Manual.torproject.org](https://tb-manual.torproject.org/security-settings/). <https://tb-manual.torproject.org/security-settings/>[7]

The History and Evolution of the TOR Network - Anonymity Anywhere. (2023, May 29). <https://anonymityanywhere.com/the-history-and-evolution-of-the-tor-network/>[3]

The Tor Project. (2010). The Tor Project | Privacy & Freedom Online. Torproject.org.
<https://www.torproject.org/about/history/>[6]

Tor Project | How do Onion Services work? (n.d.). Community.torproject.org.
<https://community.torproject.org/onion-services/overview/>[8]

Amanda_James_Min. (2020, April 18). Understanding the Tor Network. Systems and Network Security. <https://medium.com/systems-and-network-security/understanding-the-tor-network-b9bf5ffca226>[20]

Kobie, N. (2019, May 19). What is the dark web? How to use Tor to access the dark web. Wired.
<https://www.wired.com/story/what-is-the-dark-web-how-to-access/>[10]

New Release: Tor Browser 8.5 | Tor Project. (n.d.). Blog.torproject.org. Retrieved August 1, 2024, from <https://blog.torproject.org/new-release-tor-browser-85/>[11]

New release: Tor Browser 13.0. (2023, October 12). Tor Project Forum.
<https://forum.torproject.org/t/new-release-tor-browser-13-0/9703>[12]

New release: Tor Browser 13.0 | Tor Project. (n.d.). Blog.torproject.org.
<https://blog.torproject.org/new-release-tor-browser-130/>[13]

Quintin, C. (2014, July 1). 7 Things You Should Know About Tor. Electronic Frontier Foundation.
<https://www.eff.org/deeplinks/2014/07/7-things-you-should-know-about-tor>[9]

What is the Dark Web? How to Access and Other Risks | CrowdStrike. (n.d.). Crowdstrike.com.
<https://www.crowdstrike.com/cybersecurity-101/the-dark-web-explained/>[17]

What Is the Dark Web? Myths and Facts About the Hidden Internet. (n.d.). Dataprot.
<https://dataprot.net/articles/what-is-dark-web/>[18]

Files and File Systems. (n.d.).<https://www.baeldung.com/cs/files-file-systems>
[27]

Galán-Jiménez, J., & Gazo-Cervero, A. (2010). Overlay Networks: Overview, Applications and Challenges. IJCSNS International Journal of Computer Science and Network Security, 10(12), 40. http://paper.ijcsns.org/07_book/201012/20101206.pdf[23]

IP addresses (article) | The Internet. (n.d.). Khan Academy.
<https://www.khanacademy.org/computing/computers-and-internet/xcae6f4a7ff015e7d:the-internet/xcae6f4a7ff015e7d:addressing-the-internet/a/ip-v4-v6-addresses>[22]

Jasuja, N. (2018). Internet vs World Wide Web - Difference and Comparison | Diffeen. Diffeen.com; Diffeen. https://www.diffeen.com/difference/Internet_vs_World_Wide_Web[25]

Murdoch, S., & Syverson, P. (n.d.). <https://murdoch.is/papers/tor14design.pdf>[21]

wang, H. (2020, April 4). Peeling the Onion: Demystify How Tor Enables Anonymous Communications. Medium; Systems and Network Security. <https://medium.com/systems-and-network-security/peeling-the-onion-demystify-how-tor-enables-anonymous-communications-9744db3abe61>[24]

(2024). Bing.com.
<https://th.bing.com/th/id/R.e0709fb8f2e0385bdfccfd7c84c35c3c?rik=I%2baiBjMg0RV6bw&riu>

[=http%3a%2f%2fmarketbusinessnews.com%2fwfp-content%2fuploads%2f2016%2f08%2fThe-Internet-versus-World-Wide-Web.jpg&ehk=u0Mly01fC45twvUDzM1bouEf9PGZl7mDp1MwZKbT7w4%3d&risl=&pid=ImgRaw&r=0](http%3a%2f%2fmarketbusinessnews.com%2fwfp-content%2fuploads%2f2016%2f08%2fThe-Internet-versus-World-Wide-Web.jpg&ehk=u0Mly01fC45twvUDzM1bouEf9PGZl7mDp1MwZKbT7w4%3d&risl=&pid=ImgRaw&r=0) [26]

Al-E'mari, S., Sanjalawe, Y., & Fraihat, S. (2023). Detection of obfuscated Tor traffic based on bidirectional generative adversarial networks and vision transform. *Computers & Security*, 135, 103512. <https://doi.org/10.1016/j.cose.2023.103512>[33]

Increasing Trust in Tor Node List Using Blockchain.
(n.d.).<https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8751340>
[31]

Islam, A. K. M. N., Mäntymäki, M., & Turunen, M. (2019). Why do blockchains split? An actor-network perspective on Bitcoin splits. *Technological Forecasting and Social Change*, 148, 119743. <https://doi.org/10.1016/j.techfore.2019.119743>[30]

Mustapha, R. (2023, April 6). What Is HTTP? Protocol Overview for Beginners. *FreeCodeCamp.org*. <https://www.freecodecamp.org/news/what-is-http/>[34]

Ottakath, N., Al-Ali, A., Al-Maadeed, S., Elharrouss, O., & Mohamed, A. (2023). Enhanced computer vision applications with blockchain: A review of applications and opportunities. *Journal of King Saud University - Computer and Information Sciences*, 101801. <https://doi.org/10.1016/j.jksuci.2023.101801>[29]

Overlay Networks: An Akamai Perspective.
(n.d.).<https://www.akamai.com/site/en/documents/research-paper/overlay-networks-an-akamai-perspective-technical-publication.pdf>
[28]

Sangeetha, K., & Ravikumar, K. (2018). Defense Against Protocol Level Attack in Tor Network using Deficit Round Robin Queuing Process. *Egyptian Informatics Journal*, 19(3), 199–205. <https://doi.org/10.1016/j.eij.2018.03.005> [32]

Brown, G., Zhu, H., Huffman, M., & Mitra, R. (n.d.). The Network Layer I | Addressing. *Utsa.pressbooks.pub*. <https://utsa.pressbooks.pub/networking/chapter/the-network-layer-addressing/>[38]

Collier, B., & Stewart, J. (2021). Privacy Worlds: Exploring Values and Design in the Development of the Tor Anonymity Network. *Science, Technology, & Human Values*, 016224392110390. <https://doi.org/10.1177/01622439211039019>[39]

Jadoon, A. K., Iqbal, W., Amjad, M. F., Afzal, H., & Bangash, Y. A. (2019). Forensic Analysis of Tor Browser: A Case Study for Privacy and Anonymity on the Web. *Forensic Science International*, 299, 59–73. <https://doi.org/10.1016/j.forsciint.2019.03.030>[36]

Pastor-Galindo, J., Mármol, F. G., & Pérez, G. M. (2023). On the gathering of Tor onion addresses. *Future Generation Computer Systems*. <https://doi.org/10.1016/j.future.2023.02.024>[35]

Sherman, J. (2022, September 19). Untangling the Russian web: Spies, proxies, and Spectrums of Russian Cyber Behavior. *Atlantic Council*. <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/untangling-the-russian-web/>[40]

Team, S. N. (n.d.). 4 Sources of Income: Who Pays to Keep the Tor Browser Going? Www.secureworld.io. Retrieved August 1, 2024, from <https://www.secureworld.io/industry-news/tor-government-funding-numbers>[41]

Tor Detection Test | Tor IP Address Check | Tor IP Test. (n.d.). Www.ipqualityscore.com. Retrieved August 1, 2024, from <https://www.ipqualityscore.com/tor-ip-address-check>[37]

23 Best Tor Alternatives For Browsing The Web Or Deep Web. (2023, October 5). PrivacyCrypts. <https://privacycrypts.com/privacy/browsing/best-tor-alternatives/>[47]

About – Tor Metrics. (n.d.). Metrics.torproject.org. <https://metrics.torproject.org/about.html>[49]

Aragon, J. (2023, April 18). What are exit nodes? Tor circuits explained. Privacy Guides. <https://share.privacyguides.org/glossary/exit-node/>[43]

Chakraborty, A. (2024, March 8). 10 Best Tor Browser Alternatives In 2024 [Anonymous Browsing]. TechViral. <https://techviral.net/best-tor-browser-alternatives/>[46]

Is the Tor Browser Really Private? [Privacy Features and Concerns]. (n.d.). Techjury. Retrieved August 1, 2024, from <https://techjury.net/blog/is-the-tor-browser-really-private/>[44]

Transparency, Openness, and Our 2020-2021 Financials | Tor Project. (n.d.). Blog.torproject.org. Retrieved August 1, 2024, from <https://blog.torproject.org/transparency-openness-and-our-2020-and-2021-financials/>[42]

Welcome to Tor Metrics. (n.d.). People.torproject.org. Retrieved August 1, 2024, from <https://people.torproject.org/~irl/metrics/>[48]

Your Ultimate Guide to Tor Browser - All you Need to Know. (2024, June 22). Www.privacyaffairs.com. <https://www.privacyaffairs.com/tor-guide/>[45]

Mohamad, & Zarul Fitri Zaaba. (2023). WFP-Collector: Automated dataset collection framework for website fingerprinting evaluations on Tor Browser. Journal of King Saud University - Computer and Information Sciences, 35(9), 101778–101778. <https://doi.org/10.1016/j.jksuci.2023.101778>[52]

Performance – Tor Metrics. (n.d.). Metrics.torproject.org. Retrieved August 1, 2024, from <https://metrics.torproject.org/torperf.html>

[50]

Performance measurements and blocking-resistance analysis in the Tor network | Tor Project. (n.d.). Blog.torproject.org. <https://blog.torproject.org/performance-measurements-and-blocking-resistance-analysis-tor-network/>

[51]

Raju Gudla, Satyanarayana Vollala, Srinivasa K.G, & Amin, R. (2024). A novel approach for classification of Tor and non-Tor traffic using efficient feature selection methods. Expert Systems with Applications, 249, 123544–123544. <https://doi.org/10.1016/j.eswa.2024.123544>[54]

Xiao, X., Zhou, X., Yang, Z., Yu, L., Zhang, B., Liu, Q., & Luo, X. (2024). A comprehensive analysis of website fingerprinting defenses on Tor. Computers & Security, 136, 103577. <https://doi.org/10.1016/j.cose.2023.103577>

[53]

(n.d.). Users' Privacy Literacy, Motivation to Use Tor and Further Privacy Protecting Behavior. https://www.researchgate.net/publication/372303474_Users%27_Privacy_Literacy_Motivation_to_use_Tor_and_Further_Privacy_Protecting_Behavior#pf4

[55]

(2024). Bing.com. https://th.bing.com/th/id/OIP.diHdA2fsHhT2A8v_w3JmrQHaHa?rs=1&pid=ImgDetMain

[56]

---What is Tor and how does it advance human rights? (2024, February 1). Amnesty International. <https://www.amnesty.org/en/latest/campaigns/2024/02/what-is-tor-and-how-does-it-advance-human-rights/>[86]

Challenges, priorities, and progress in anti-censorship technology at Tor | Tor Project. (n.d.). Blog.torproject.org. Retrieved August 1, 2024, from <https://blog.torproject.org/anti-censorship-challenges-priorities-progress/>[66]

Chaudhry, A. (2020, February 21). How to use the Tor Browser's tools to protect your privacy. The Verge. <https://www.theverge.com/2020/2/21/21138403/tor-privacy-tools-private-network-browser-settings-security>[77]

Cui, J., Huang, C., Meng, H., & Wei, R. (2023a). Tor network anonymity evaluation based on node anonymity. *Cybersecurity*, 6(1). <https://doi.org/10.1186/s42400-023-00191-8>[80]

Cui, J., Huang, C., Meng, H., & Wei, R. (2023b). Tor network anonymity evaluation based on node anonymity. *Cybersecurity*, 6(1). <https://doi.org/10.1186/s42400-023-00191-8>[81]

Dolliver, D. S. (2015). Evaluating drug trafficking on the Tor Network: Silk Road 2, the sequel. *International Journal of Drug Policy*, 26(11), 1113–1123. <https://doi.org/10.1016/j.drugpo.2015.01.008>[65]

How Tor improves usability without compromising user privacy — Free Software Foundation — Working together for free software. (n.d.). [Www.fsf.org](https://www.fsf.org). Retrieved August 1, 2024, from <https://www.fsf.org/bulletin/2020/fall/how-tor-improves-usability-without-compromising-user-privacy>[79]

Lee, J. R., Holt, T. J., & Smirnova, O. (2022). An assessment of the state of firearm sales on the Dark Web. *Journal of Crime and Justice*, 1–15. <https://doi.org/10.1080/0735648x.2022.2058062>[82]

Lee, M. (2017, January 4). The U.S. Government Thinks Thousands of Russian Hackers May Be Reading My Blog. They Aren't. *The Intercept*. <https://theintercept.com/2017/01/04/the-u-s-government-thinks-thousands-of-russian-hackers-are-reading-my-blog-they-arent/>[75]

MANAGING IDENTITIES | Tor Project | Tor Browser Manual. (n.d.). [Tb-Manual.torproject.org](https://tb-manual.torproject.org/managing-identities/). <https://tb-manual.torproject.org/managing-identities/>[78]

Minárik, T., & Osula, A.-M. (2016). Tor does not stink: Use and abuse of the Tor anonymity network from the perspective of law. *Computer Law & Security Review*, 32(1), 111–127. <https://doi.org/10.1016/j.clsr.2015.12.002>[84]

- Pastor-Galindo, J., Mármol, F. G., & Pérez, G. M. (2023a). On the gathering of Tor onion addresses. *Future Generation Computer Systems*.
<https://doi.org/10.1016/j.future.2023.02.024>[64]
- Pastor-Galindo, J., Mármol, F. G., & Pérez, G. M. (2023b). On the gathering of Tor onion addresses. *Future Generation Computer Systems*.
<https://doi.org/10.1016/j.future.2023.02.024>[70]
- Pastor-Galindo, J., Mármol, F. G., & Pérez, G. M. (2023c). On the gathering of Tor onion addresses. *Future Generation Computer Systems*.
<https://doi.org/10.1016/j.future.2023.02.024>[83]
- Pastor-Galindo, J., Mármol, F. G., & Pérez, G. M. (2023d). On the gathering of Tor onion addresses. *Future Generation Computer Systems*.
<https://doi.org/10.1016/j.future.2023.02.024>[85]
- Right now, Tor is protecting the privacy of millions of people like you! (n.d.). Newsletter.torproject.org. Retrieved August 1, 2024, from
<https://newsletter.torproject.org/archive/2023-10-30-tor-is-protecting-the-privacy-of-millions/>[74]
- The History and Evolution of the TOR Network - Anonymity Anywhere. (2023a, May 29).
<https://anonymityanywhere.com/the-history-and-evolution-of-the-tor-network/>[57]
- The History and Evolution of the TOR Network - Anonymity Anywhere. (2023b, May 29).
<https://anonymityanywhere.com/the-history-and-evolution-of-the-tor-network/>[60]
- The History and Evolution of the TOR Network - Anonymity Anywhere. (2023c, May 29).
<https://anonymityanywhere.com/the-history-and-evolution-of-the-tor-network/>[62]
- The History and Evolution of the TOR Network - Anonymity Anywhere. (2023d, May 29).
<https://anonymityanywhere.com/the-history-and-evolution-of-the-tor-network/>[63]
- The History and Evolution of the TOR Network - Anonymity Anywhere. (2023e, May 29).
<https://anonymityanywhere.com/the-history-and-evolution-of-the-tor-network/>[67]
- The History and Evolution of the TOR Network - Anonymity Anywhere. (2023f, May 29).
<https://anonymityanywhere.com/the-history-and-evolution-of-the-tor-network/>[73]
- The History and Evolution of the TOR Network - Anonymity Anywhere. (2023g, May 29).
<https://anonymityanywhere.com/the-history-and-evolution-of-the-tor-network/>[87]
- The Tor Project. (2010). The Tor Project | Privacy & Freedom Online. Torproject.org.
<https://www.torproject.org/about/history/>[58]
- The Tor Project | Privacy & Freedom Online. (n.d.). Torproject.org. Retrieved August 1, 2024, from
<https://www.torproject.org/about/supporters/>[59]
- Tor blocked in Russia: how to circumvent censorship. (2021, December 3). Tor Project Forum.
<https://forum.torproject.org/t/tor-blocked-in-russia-how-to-circumvent-censorship/982>[76]
- What is Tor (The Onion Router) and How Does It Work? (2023, July 17).
 Www.knowledgehut.com. <https://www.knowledgehut.com/blog/security/what-is-tor-in-cyber-security>[71]

What is Tor? - zenarmor.com. (n.d.). Www.zenarmor.com.

<https://www.zenarmor.com/docs/network-security-tutorials/what-is-tor>[72]

The History and Evolution of the TOR Network - Anonymity Anywhere. (2023, May 29).

<https://anonymityanywhere.com/the-history-and-evolution-of-the-tor-network/>[61]

Beginner's Guide to Tor: What It Is and How to Safely Use It 2024. (n.d.). WizCase.

<https://www.wizcase.com/blog/ultimate-guide-to-using-tor/>[105]

Bowen, J. (2021, February 12). Arab Spring: How the uprisings still echo, 10 years on. BBC News.

<https://www.bbc.co.uk/news/world-middle-east-56000950>[104]

claywilliams. (2020, January 6). PPT - The Sybil Attack in Sensor Networks: Analysis & Defenses PowerPoint Presentation - ID:9638793. SlideServe.

<https://www.slideserve.com/claywilliams/the-sybil-attack-in-sensor-networks-analysis-amp-defenses-powerpoint-ppt-presentation>[102]

Dark web drugs raid leads to 179 arrests. (2020, September 22). BBC News.

<https://www.bbc.co.uk/news/technology-54247529>[101]

Darknet 150531165004-lva1-app6892. (2015, June 2). SlideShare.

<https://www.slideshare.net/slideshow/darknet-150531165004lva1app6892/48889156>[100]

David Goldschlag - BankInfoSecurity. (2024). Bankinfosecurity.com.

<https://www.bankinfosecurity.com/authors/david-goldschlag-i-1676>[93]

Forum, I.-I. G. (2022, November 29). 352A3345. Flickr.

<https://www.flickr.com/photos/185833270@N04/52575724338>[103]

Greenberg, A. (2012). This Machine Kills Secrets. Random House.[97]

How to Fix Red Screen of Death On Windows 10/11 | Driver Talent. (n.d.). Www.drivethelife.com.

Retrieved August 1, 2024, from <https://www.drivethelife.com/how-to-fix-red-screen-of-death-on-windows-10-11/>[99]

Paul Syverson. (2023, May 30). Wikipedia. https://en.wikipedia.org/wiki/Paul_Syverson[92]

Reed, M. G., Syverson, P. F., & Goldschlag, D. M. (1998). Anonymous connections and onion routing. IEEE Journal on Selected Areas in Communications, 16(4), 482–494.

<https://doi.org/10.1109/49.668972>[91]

Singh, M. (2020, September 17). How To Change Your IP Address in Windows & MAC. TechViral.

<https://techviral.net/change-your-ip-address/>[98]

The History and Evolution of the TOR Network - Anonymity Anywhere. (2023, May 29).

<https://anonymityanywhere.com/the-history-and-evolution-of-the-tor-network/>[96]

The Tor Project. (2010). The Tor Project | Privacy & Freedom Online. Torproject.org.

<https://www.torproject.org/about/history/>[90]

The Tor Project. (2021, December 8). Wikipedia.

https://en.wikipedia.org/wiki/The_Tor_Project[94]

Tor hidden service V3 stealth mode · Issue #104 · hassio-addons/addon-tor. (n.d.). GitHub.

Retrieved August 1, 2024, from <https://github.com/hassio-addons/addon-tor/issues/104>[106]

Wikipedia. (2021, July 18). Tor (network). Wikipedia.

[https://en.wikipedia.org/wiki/Tor_\(network\)](https://en.wikipedia.org/wiki/Tor_(network))[95]

Economy, E. C. (2018, June 29). The great firewall of China: Xi Jinping's internet shutdown. The

Guardian. <https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown?ref=hir.harvard.edu>[107]