Anonymous P2P

An **anonymous P2P** communication system is a peer-to-peer distributed application in which the nodes, which are used to share resources, or participants are anonymous or pseudonymous.[1] Anonymity of participants is usually achieved by special routing overlay networks that hide the physical location of each node from other participants.[2]

Interest in anonymous P2P systems has increased in recent years for many reasons, ranging from the desire to share files without revealing one's network identity and risking litigation[3] to distrust in governments, concerns over mass surveillance and data retention, and lawsuits against bloggers.[4]

Motivation for anonymity

There are many reasons to use anonymous P2P technology; most of them are generic to all forms of online anonymity.

P2P users who desire anonymity usually do so as they do not wish to be identified as a publisher (sender), or reader (receiver), of information. Common reasons include:

- Censorship at the local, organizational, or national level
- Personal privacy preferences such as preventing tracking or data mining activities
- The material or its distribution is considered illegal or incriminating by possible eavesdroppers
- Material is legal but socially deplored, embarrassing or problematic in the individual's social world
- Fear of retribution (against whistleblowers, unofficial leaks, and activists who do not believe in restrictions on information nor knowledge)

A particularly open view on legal and illegal content is given in The Philosophy Behind Freenet (https://web.archive.org/web/20090627205546/http://freenetproject.org/philosophy.html) .

Governments are also interested in anonymous P2P technology. The United States Navy funded the original onion routing research that led to the development of the Tor network, which was later funded by the Electronic Frontier Foundation and is now developed by the non-profit organization The Tor Project, Inc.

Arguments for and against anonymous P2P communication

General

While anonymous P2P systems may support the protection of unpopular speech, they may also protect illegal activities, such as fraud, libel, the exchange of illegal pornography, the unauthorized copying of copyrighted works, or the planning of criminal activities. Critics of anonymous P2P systems hold that these disadvantages outweigh the advantages offered by such systems, and that other communication channels are already sufficient for unpopular speech.

Proponents of anonymous P2P systems believe that all restrictions on free speech serve authoritarian interests, information itself is ethically neutral, and that it is the people acting upon the information that can be good or evil. Perceptions of good and evil can also change (see moral panic); for example, if anonymous peer-to-peer networks had existed in the 1950s or 1960s, they might have been targeted for carrying information about civil rights or anarchism.

Easily accessible anonymous P2P networks are seen by some as a democratization of encryption technology, giving the general populace access to secure communications channels already used by governments. Supporters of this view, such as Phil Zimmermann, argue that anti-surveillance technologies help to equalize power between governments and their people,[5] which is the actual reason for banning them. John Pilger opines that monitoring of the populace helps to contain threats to the "consensual view of established authority"[6] or threats to the continuity of power structures and privilege.

Freedom of speech

Some claim that true freedom of speech, especially on controversial subjects, is difficult or impossible unless individuals can speak anonymously. If anonymity is not possible, one could be subjected to threats or reprisals for voicing an unpopular view. This is one reason why voting is done by secret ballot in many democracies. Controversial information which a party wants to keep hidden, such as details about corruption issues, is often published or leaked anonymously.

Anonymous blogging

Anonymous blogging is one widespread use of anonymous networks. While anonymous blogging is possible on the non-anonymous internet to some degree too, a provider hosting the blog in question might be forced to disclose the blogger's IP address (as when Google revealed an anonymous blogger's identity[7]). Anonymous networks provide a better degree of anonymity. Flogs (anonymous blogs) in Freenet, Syndie and other blogging tools in I2P and Osiris sps are some examples of anonymous blogging technologies.

One argument for anonymous blogging is a delicate nature of work situation. Sometimes a blogger writing under their real name faces a choice between either staying silent or causing a harm to themselves, their colleagues or the company they work for.[8]

Another reason is risk of lawsuits. Some bloggers have faced multimillion-dollar lawsuits[9] (although they were later dropped completely[10]); anonymous blogging provides protection against such risks.

Censorship via Internet domain names

On the non-anonymous Internet, a domain name like "example.com" is a key to accessing information. The censorship of the Wikileaks website shows that domain names are extremely vulnerable to censorship. Some domain registrars have suspended customers' domain names even in the absence of a court order.

For the affected customer, blocking of a domain name is a far bigger problem than a registrar refusing to provide a service; typically, the registrar keeps full control of the domain names in question. In the case of a European travel agency, more than 80 .com websites were shut down without any court process and held by the registrar since then. The travel agency had to rebuild the sites under the .net top-level domain instead.[11]

On the other hand, anonymous networks do not rely on domain name registrars. For example, Freenet, I2P and Tor hidden services implement censorship-resistant URLs based on public-key cryptography: only a person having the correct private key can update the URL or take it down.

Control over online tracking

Anonymous P2P also has value in normal daily communication. When communication is anonymous, the decision to reveal the identities of the communicating parties is left up to the parties involved and is not available to a third party. Often there is no need or desire by the communicating parties to reveal their identities. As a matter of personal freedom, many people do not want processes in place by default which supply unnecessary data. In some cases, such data could be compiled into histories of their activities.

For example, most current phone systems transmit caller ID information by default to the called party (although this can be disabled either for a single call or for all calls). If a person calls to make an inquiry about a product or the time of a movie, the party called has a record of the calling phone number, and may be able to obtain the name, address and other information about the caller. This information is not available about someone who walks into a store and makes a similar inquiry.

Effects of surveillance on lawful activity

Online surveillance, such as recording and retaining details of web and e-mail traffic, may have effects on lawful activities.[12] People may be deterred from accessing or communicating legal information because they know of possible surveillance and believe that such communication may be seen as suspicious. According to law professor Daniel J. Solove, such effects "harm society because, among other things, they reduce the range of viewpoints being expressed and the degree of freedom with which to engage in political activity."[13]

Access to censored and copyrighted material

Most countries ban or censor the publication of certain books and movies, and certain types of content. Other material is legal to possess but not to distribute; for example, copyright and software patent laws may forbid its distribution. These laws are difficult or impossible to enforce in anonymous P2P networks.

Anonymous online money

With anonymous money, it becomes possible to arrange anonymous markets where one can buy and sell just about anything anonymously. Anonymous money could be used to avoid tax collection. However, any transfer of physical goods between two parties could compromise anonymity.[14]

Proponents argue that conventional cash provides a similar kind of anonymity, and that existing laws are adequate to combat crimes like tax evasion that might result from the use of anonymous cash, whether online or offline.[15]

Functioning of anonymous P2P

Anonymity and pseudonymity

Some of the networks commonly referred to as "anonymous P2P" are truly anonymous, in the sense that network nodes carry no identifiers. Others are actually pseudonymous: instead of being identified by their IP addresses, nodes are identified by pseudonyms such as cryptographic keys. For example, each node in the MUTE network has an overlay address that is derived from its public key. This overlay address functions as a pseudonym for the node, allowing messages to be addressed to it. In Freenet, on the other hand, messages are routed using keys that identify specific pieces of data rather than specific nodes; the nodes themselves are anonymous.

The term *anonymous* is used to describe both kinds of network because it is difficult—if not impossible—to determine whether a node that sends a message originated the message or is simply forwarding it on behalf of another node. Every node in an anonymous P2P network acts as a universal sender and universal receiver to maintain anonymity. If a node was only a receiver and did not send, then neighbouring nodes would know that the information it was requesting was for itself only, removing any plausible deniability that it was the recipient (and consumer) of the information. Thus, in order to remain anonymous, nodes must ferry information for others on the network.

Spam and DoS attacks in anonymous networks

Originally, anonymous networks were operated by small and friendly communities of developers. As interest in anonymous P2P increased and the user base grew, malicious users inevitably appeared and tried different attacks. This is similar to the Internet, where widespread use has been followed by waves of spam and distributed DoS (Denial of Service) attacks. Such attacks may require different solutions in anonymous networks. For example, blacklisting of originator network addresses does not work because anonymous networks conceal this information. These networks are more vulnerable to DoS attacks as well due to the smaller bandwidth, as has been shown in examples on the Tor network.

A conspiracy to attack an anonymous network could be considered criminal computer hacking, though the nature of the network makes this impossible to prosecute without compromising the anonymity of data in the network.

Opennet and darknet network types

Like conventional P2P networks, anonymous P2P networks can implement either opennet or darknet (often named friend-to-friend) network type. This describes how a node on the network selects peer nodes:

- In opennet network, peer nodes are discovered automatically. There is no configuration required but little control available over which nodes become peers.[16]
- In a darknet network, users manually establish connections with nodes run by people they know. Darknet typically needs more effort to set up but a node only has trusted nodes as peers.

Some networks like Freenet support both network types simultaneously (a node can have some manually added darknet peer nodes and some automatically selected opennet peers) .

In a friend-to-friend (or F2F) network, users only make direct connections with people they know. Many F2F networks support indirect anonymous or pseudonymous communication between users who do not know or trust one another. For example, a node in a friend-to-friend overlay can automatically forward a file (or a request for a file) anonymously between two "friends", without telling either of them the other's name or IP address. These "friends" can in turn forward the same file (or request) to their own "friends", and so on. Users in a friend-to-friend network cannot find out who else is participating beyond their own circle of friends, so F2F networks can grow in size without compromising their users' anonymity.

Some friend-to-friend networks allow the user to control what kind of files can be exchanged with "friends" within the node, in order to stop them from exchanging files that user disapproves of.

Advantages and disadvantages of opennet compared to darknet are disputed, see friend-to-friend article for summary.

List of anonymous P2P networks and clients

Public P2P clients

- Classified-ads - an open source DHT-based decentralized messaging and voice app. Allows users to not expose any personal details but does not hide network addresses of nodes.
- DarkMX[17] - a file-sharing client modeled on WinMX/Tixati with a built-in implementation of Tor.
- DigitalNote XDN - an open-source anonymous decentralized encrypted messaging system based on blockchain technology

- Freenet - a censorship-resistant distributed file system for anonymous publishing (open source, written in Java)
- GNUnet - a P2P framework, includes anonymous file sharing as its primary application (GNU Project, written in C, alpha status)
- Perfect Dark - a Japanese file-sharing client based on a distributed data store. One can see the IP address of connected nodes, but not what they are up or downloading. Amoeba[18] is a similar client/network.
- Tribler - an open source BitTorrent client. It can be set to have neighboring nodes act as proxies between one's client and the torrent swarm. The proxy can see what file is being uploaded, but most nodes in the swarm only see the exit node.
- ZeroNet - a decentralized Internet-like network of peer-to-peer users. Allows tunneling of HTTP-traffic through Tor.

I2P clients

- I2P - a fully decentralized overlay network for strong anonymity and end-to-end encryption, with many applications (P2P, browsing, distributed anonymous e-mail, instant messaging, IRC, ...) running on top of it (free/open source, platform-independent)
- I2P-Bote an anonymous, secure (end-to-end encrypted), serverless mail application with remailer functionality for the I2P network
- I2P-Messenger an anonymous, secure (end-to-end encrypted), serverless instant messenger for the I2P network
- I2PSnark - an anonymous BitTorrent client for the I2P network
- I2Phex - a Gnutella client which communicates anonymously through I2P
- iMule - an aMule port running under I2P network
- Robert (P2P Software) - another anonymous BitTorrent client for the I2P network
- I2P-Tahoe-LAFS - a censorship-resistant distributed file system for anonymous publishing and file sharing (open source, written in Python, pre-alpha status)
- Vuze (formerly Azureus) - a BitTorrent client with the option of using I2P or Tor (initially open source, written in Java)
- BiglyBT - a successor to Vuze. A BitTorrent client where downloads can be routed through I2P, and searches carried out through Tor (open source, written in Java)

- MuWire[19] - is a filesharing software, with chat rooms. Even if running inside the I2P network, it is not called a 'I2P client' because it has a I2P router embedded, so this makes it a standalone software. The project got shut down on 14 February 2023[20] but recently it seemingly got unarchived on Github, the developer said that it is possible to import connections from a .txt file for MuWire to work, which is now provided in the releases.[21]

Defunct (Public P2P clients) or no longer developed

- Bitblinder (2009–2010) - file sharing
- Bitmessage - an anonymous decentralized messaging system serving as a secure replacement for email
- Cashmere (2005) - resilient anonymous routing[22]
- Entropy (2003–2005) - Freenet compatible
- EarthStation 5 (2003–2005) - anonymity controverted
- Herbivore (2003–2005) - file sharing and messaging. Used the Dining cryptographers problem.[23]
- MUTE (2003–2009) - file sharing[24]
- NeoLoader - a filesharing software compatible with bittorrent and edonkey2000. Anonymous when used with the "NeoShare" feature (that use the proprietary "NeoKad" network)[25]
- Netsukuku - a peer-to-peer routing system aiming to build a free and independent Internet
- Nodezilla (2004–2010) - an anonymizing, closed source network layer upon which applications can be built
- Osiris (Serverless Portal System) - an anonymous and distributed web portals creator.
- OFF System (2006–2010) - a P2P distributed file system through which all shared files are represented by randomized data blocks
- RShare (2006–2007) - file sharing
- Share - a Japanese filesharing client modeled on Winny
- Syndie - a content (mainly forums) syndication program that operates over numerous anonymous and non-anonymous networks (open source, written in Java)
- StealthNet (2007–2011) - the successor to RShare
- Winny - a Japanese filesharing program modeled on Freenet which relies on a mixnet and distributed datastore to provide anonymity

Private P2P clients

Private P2P networks are P2P networks that only allow some mutually trusted computers to share files. This can be achieved by using a central server or hub to authenticate clients, in which case the functionality is similar to a private FTP server, but with files transferred directly between the clients. Alternatively, users can exchange passwords or keys with their friends to form a decentralized network.

Examples include:

- Syncthing - is a free, open-source peer-to-peer file synchronization application. It can sync files between devices. Data security and data safety are built into the design of the software.
- Resilio Sync - a proprietary alternative to Syncthing

Private F2F (friend-to-friend) clients

Friend-to-friend networks are P2P networks that allows users only to make direct connections with people they know. Passwords or digital signatures can be used for authentication.

Examples include :

- Filetopia - not anonymous but encrypted friend-to-friend. File sharing, chat, internal mail service
- OneSwarm - a backwards compatible BitTorrent client with privacy-preserving sharing options, aims to create a large F2F network.
- Retroshare - filesharing, serverless email, instant messaging, VoIP, chatrooms, and decentralized forums.

Hypothetical or defunct networks

Hypothetical

The following networks only exist as design or are in development

- anoNet - extensible IP anonymizer with steganography support (in development)
- Crowds - Reiter and Rubin's system for "blending into a crowd" has a known attack
- P2PRIV - Peer-to-Peer diRect and anonymous dIstribution oVerlay - anonymity via virtual links parallelization - currently in development and has significant, unsolved problems in a real world environment
- Phantom Anonymity Protocol - a fully decentralized high-throughput anonymization network (no longer in development)[26]

- Race (Resilient Anonymous Communication for Everyone) - A project by DARPA to build an anonymous, attack-resilient mobile communication system that can reside completely within a network environment, capable of avoiding large-scale compromise by preventing compromised information from being useful for identifying any of the system nodes because all such information is encrypted on the nodes at all times, even during computation; and preventing communications compromise by virtue of obfuscating communication protocols.

Defunct or dormant

- Bitblinder - a decentralised P2P anonymity software program which included Tor but with increased speed.[27] Website is down and clients are no longer functional.
- Invisible IRC Project - anonymous IRC, inspired by Freenet, which later became I2P (Invisible Internet Project).[28]
- Mnet (formerly MojoNation) - a distributed file system[29]

Anonymous P2P in a wireless mesh network

It is possible to implement anonymous P2P on a wireless mesh network; unlike fixed Internet connections, users don't need to sign up with an ISP to participate in such a network, and are only identifiable through their hardware.

Protocols for wireless mesh networks are Optimized Link State Routing Protocol (OLSR) and the follow-up protocol B.A.T.M.A.N., which is designed for decentralized auto-IP assignment. See also Netsukuku.

Even if a government were to outlaw the use of wireless P2P software, it would be difficult to enforce such a ban without a considerable infringement of personal freedoms. Alternatively, the government could outlaw the purchase of the wireless hardware itself.

See also

- Anonymity application
- Anonymous remailer
- Anonymous web browsing
- Comparison of file sharing applications
- Dark web
- Data privacy

- Internet privacy
- List of anonymously published works
- Personally identifiable information
- Privacy software and Privacy-enhancing technologies
  - FLAIM
  - I2P
  - I2P-Bote
  - Java Anon Proxy
    - Free Haven Project
- Secure communication

Other

- Crypto-anarchism
- Cypherpunk
- Digital divide
- Mesh networking
- Wireless community network
- Torrent activity indexing

References

1. Kobusińska, Anna; Brzeziński, Jerzy; Boroń, Michał; Inatlewski, Łukasz; Jabczyński, Michał; Maciejewski, Mateusz (2016-06-01). "A branch hash function as a method of message synchronization in anonymous P2P conversations" (https://doi.org/10.1515%2Famcs-2016-0034) . *International Journal of Applied Mathematics and Computer Science*. **26** (2): 479–493. doi:10.1515/amcs-2016-0034 (https://doi.org/10.1515%2Famcs-2016-0034) . ISSN 2083-8492 (https://search.worldcat.org/issn/2083-8492) .
2. Endsuleit, Regine, and Thilo Mie. "Censorship-resistant and anonymous P2P filesharing". *First International Conference on Availability, Reliability and Security*.

3. Electronic Frontier Foundation (2005). RIAA v. The People: Five Years Later (https://www.eff.org/wp/riaa-v-people-five-years-later) Archived (https://web.archive.org/web/20120606204216/https://www.eff.org/wp/riaa-v-people-five-years-later) 2012-06-06 at the Wayback Machine. Retrieved March 5, 2008.
4. Pain, Julien, ed. (September 2005). "Handbook for bloggers and cyber-dissidents" (https://web.archive.org/web/20070215022127/http://www.rsf.org/rubrique.php3?id_rubrique=542) . Reporters Without Borders. Archived from the original (http://www.rsf.org/rubrique.php3?id_rubrique=542) on 2007-02-15.
5. Russell D. Hoffmann (1996). Interview with author of PGP (Pretty Good Privacy) (http://www.animatedsoftware.com/hightech/philspgp.htm) Archived (https://web.archive.org/web/20190416085355/http://www.animatedsoftware.com/hightech/philspgp.htm) 2019-04-16 at the Wayback Machine. Transcript of a radio interview, retrieved 2008-01-21.
6. John Pilger (2002). Impartiality of British Journalism (http://www.zmag.org/znet/viewArticle/11340) . ZNet article, retrieved 2008-02-11.
7. Declan McCullagh (2007). Google: We had no choice in Israel ID request (https://archive.today/20121208200015/http://www.news.com/8301-13578_3-9824638-38.html) . CNET News.com article, retrieved 2008-02-11.
8. Bill Vallicella (2004). Reasons for 'Anonyblogging' (https://maverickphilosopher.blogspot.com/2004/07/reasons-for-anonyblogging.html) Archived (https://web.archive.org/web/20060514095855/http://maverickphilosopher.blogspot.com/2004/07/reasons-for-anonyblogging.html) 2006-05-14 at the Wayback Machine. Maverick Philosopher blog, retrieved 2008-02-11.
9. Media Bloggers Association (2006). MBA Member Hit With Multi-Million Dollar Federal Lawsuit (https://web.archive.org/web/20070630182947/http://www.mediabloggers.org/mba-news/mba-member-hit-with-multi-million-dollar-federal-lawsuit) . Retrieved 2008-02-11.
10. Associated Press (2006). Ad agency drops lawsuit against Maine blogger (http://www.boston.com/news/local/maine/articles/2006/05/06/ad_agency_drops_lawsuit_against_maine_blogger/) . Retrieved 2008-02-11.
11. Adam Liptak (2008). A Wave of the Watch List, and Speech Disappears (https://www.nytimes.com/2008/03/04/us/04bar.html) Archived (https://web.archive.org/web/20170407043030/http://www.nytimes.com/2008/03/04/us/04bar.html) 2017-04-07 at the Wayback Machine. *The New York Times*, 2008-03-04. Retrieved 2008-03-09.

12. Dawinder S. Sidhu (2007). The chilling effect of government surveillance programs on the use of the internet by Muslim-Americans (https://ssrn.com/abstract=1002145) Archived (https://web.archive.org/web/20220205032803/https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1002145) 2022-02-05 at the Wayback Machine. University of Maryland Law Journal of Race, Religion, Gender and Class.

13. Daniel J. Solove (2006). "I've got nothing to hide" and other misunderstandings of privacy (https://ssrn.com/abstract=998565) Archived (https://web.archive.org/web/20220205032806/https://papers.ssrn.com/sol3/papers.cfm?abstract_id=998565) 2022-02-05 at the Wayback Machine. San Diego Law Review, Vol. 44.

14. Rob Thomas, Jerry Martin (2006). The underground economy: priceless (http://www.usenix.org/publications/login/2006-12/openpdfs/cymru.pdf) Archived (https://web.archive.org/web/20080511154350/http://www.usenix.org/publications/login/2006-12/openpdfs/cymru.pdf) 2008-05-11 at the Wayback Machine. Retrieved 2008-01-20.

15. "Technology and Privacy Policy" (https://www.ntia.gov/page/chapter-5-technology-and-privacy-policy) . Archived (https://web.archive.org/web/20220205032759/https://www.ntia.gov/page/chapter-5-technology-and-privacy-policy) from the original on 2022-02-05. Retrieved 2020-11-07.

16. Gill, Phillipa; Crete-Nishihata, Masashi; Dalek, Jakub; Goldberg, Sharon; Senft, Adam; Wiseman, Greg (2015-01-23). "Characterizing Web Censorship Worldwide: Another Look at the OpenNet Initiative Data" (https://doi.org/10.1145/2700339) . *ACM Transactions on the Web*. **9** (1): 4:1–4:29. doi:10.1145/2700339 (https://doi.org/10.1145%2F2700339) . ISSN 1559-1131 (https://search.worldcat.org/issn/1559-1131) . S2CID 16660905 (https://api.semanticscholar.org/CorpusID:16660905) . Archived (https://web.archive.org/web/20220205032758/https://dl.acm.org/doi/10.1145/2700339) from the original on 2022-02-05. Retrieved 2021-03-20.

17. "DarkMX" (https://darkmx.app/) . Archived (https://web.archive.org/web/20220210110604/https://darkmx.app/) from the original on 2022-02-10. Retrieved 2022-03-29.

18. "Amoeba 5.1.8 (The next generation P2P file sharing software)" (https://archive.org/details/amoeba_5.1.8) .

19. "MuWire - Easy Anonymous File Sharing" (https://muwire.com/) . *muwire.com*. Archived (https://web.archive.org/web/20200823094455/https://muwire.com/) from the original on 2020-08-23. Retrieved 2020-08-22.

20. "Shutdown notice and Java I2P warning (#178) · zlatinb/Muwire@8dbd094" (https://github.com/zlatinb/muwire/commit/8dbd0944ff07780a73d6895f8455e1da0e60db61) . *GitHub*.

21. "Update README.md with instructions to import connections from a friend · zlatinb/muwire@651c9f3" (https://github.com/zlatinb/muwire/commit/651c9f3e944b07adf92fb2ac6d74eaa31423eff5) . *GitHub*. Retrieved 2024-08-23.

22. Zhou, Ben Y. (5 May 2015). "Cashmere: Resilient Anonymous Routing" (https://web.archive.org/web/20161230125920/http://current.cs.ucsb.edu/projects/cashmere/) . UC Santa Barbara. Archived from the original (http://current.cs.ucsb.edu/projects/cashmere/) on 30 December 2016. Retrieved 31 January 2007.

23. "Herbivore" (https://www.cs.cornell.edu/People/egs/herbivore/) . Archived (https://web.archive.org/web/20090307101334/http://www.cs.cornell.edu/People/egs/herbivore/) from the original on 2009-03-07. Retrieved 2009-03-19.

24. "MUTE: Simple, Anonymous File Sharing" (https://mute-net.sourceforge.net/) . *mute-net.sourceforge.net*. Archived (https://web.archive.org/web/20200731101420/http://mute-net.sourceforge.net/) from the original on 2020-07-31. Retrieved 2020-08-22.

25. "NeoLoader" (http://neoloader.com/anonymity.html) . *neoloader.com*. Archived (https://web.archive.org/web/20180101150202/http://neoloader.com/anonymity.html) from the original on 2018-01-01. Retrieved 2017-03-08.

26. "Google Code Archive - Long-term storage for Google Code Project Hosting" (https://code.google.com/archive/p/phantom) . *code.google.com*. Archived (https://web.archive.org/web/20190228102158/https://code.google.com/archive/p/phantom) from the original on 2019-02-28. Retrieved 2019-03-17.

27. Bauer, Kevin & Mccoy, Damon & Grunwald, Dirk & Sicker, Douglas. (2008). BitBlender: Light-weight anonymity for BitTorrent. 10.1145/1461464.1461465.

28. Gehl, Robert W. (2018), "Archives for the Dark Web: A Field Guide for Study" (https://dx.doi.org/10.1007/978-3-319-96713-4_3) , *Research Methods for the Digital Humanities*, Cham: Springer International Publishing, pp. 31–51, doi:10.1007/978-3-319-96713-4_3 (https://doi.org/10.1007%2F978-3-319-96713-4_3) , ISBN 978-3-319-96712-7, archived (https://web.archive.org/web/20220205032801/https://link.springer.com/chapter/10.1007%2F978-3-319-96713-4_3) from the original on 2022-02-05, retrieved 2020-11-14

29. Rhea, Sean, Chris Wells, Patrick Eaton, Dennis Geels, Ben Zhao, Hakim Weatherspoon, and John Kubiatowicz. "Maintenance-free global data storage". *IEEE Internet Computing 5*.

External links

- Planet Peer Wiki (http://www.planetpeer.de/wiki/) - a wiki about various anonymous P2P applications
- A survey of anonymous peer-to-peer file-sharing (http://www.lix.polytechnique.fr/~tomc/P2P/index.html) (2005)
- Anonymous, Decentralized and Uncensored File-Sharing is Booming (https://torrentfreak.com/anonymous-decentralized-and-uncensored-file-sharing-is-booming-120302/) by TorrentFreak (2011)