Hyphanet

Hyphanet (until mid-2023: **Freenet**[4]) is a peer-to-peer platform for censorship-resistant, anonymous communication. It uses a decentralized distributed data store to keep and deliver information, and has a suite of free software for publishing and communicating on the Web without fear of censorship.[5][6]:151 Both Freenet and some of its associated tools were originally designed by Ian Clarke, who defined Freenet's goal as providing freedom of speech on the Internet with strong anonymity protection.[7][8][9]

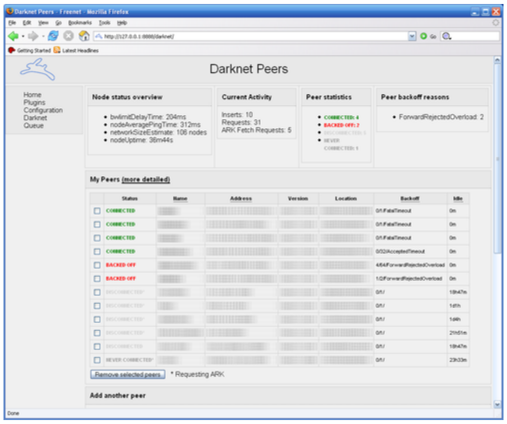
The distributed data store of Freenet is used by many third-party programs and plugins to provide microblogging and media sharing,[10] anonymous and decentralised version tracking,[11] blogging,[12] a generic web of trust for decentralized spam resistance,[13][14] Shoeshop for using Freenet over sneakernet,[15] and many more.

History

The origin of Freenet can be traced to Ian Clarke's student project at the University of Edinburgh, which he completed as a graduation requirement in the summer of 1999.[16][17][18] Ian Clarke's resulting unpublished report "A distributed decentralized information storage and retrieval system" (1999) provided foundation for the seminal paper written in collaboration with other researchers, "Freenet: A Distributed Anonymous Information Storage and Retrieval System" (2001).[19][20] According to CiteSeer, it became one of the most frequently cited computer science articles in 2002.[21]

Freenet can provide anonymity on the Internet by storing small encrypted snippets of content distributed on the computers of its users and connecting only through intermediate computers which pass on requests for content and sending them back without knowing the contents of the full file. This is similar to how routers on the Internet route packets without knowing anything about files — except Freenet has caching, a layer of strong encryption, and no reliance on centralized structures.[20] This allows users to publish anonymously or retrieve various kinds of information.[6]:152

Release history



Darknet Peers - Freenet - Mozilla Firefox

File Edit View Go Bookmarks Tools Help
http://127.0.0.1:8888/darknet/
Getting Started Latest Headlines
Home
Plugins
Configuration
Darknet
Queue
Remove selected peers
Done

Darknet Peers

Node status overview

- bwlimitDelayTime: 204ms
- nodeAveragePingTime: 312ms
- networkSizeEstimate: 106 nodes
- nodeUptime: 38m44s

Current Activity

Inserts: 10
Requests: 31
ARK Fetch Requests: 5

Peer statistics

- CONNECTED: 4
- BACKED OFF: 2
- DISCONNECTED: 5
- NEVER CONNECTED: 1

Peer backoff reasons

- ForwardRejectedOverload: 2

My Peers (more detailed)

	Status	Name	Address	Version	Location	Backoff	Idle
□	CONNECTED	[redacted]	[redacted]	[redacted]	[redacted]	0/1/FatalTimeout	0m
□	CONNECTED	[redacted]	[redacted]	[redacted]	[redacted]	0/1/FatalTimeout	0m
□	CONNECTED	[redacted]	[redacted]	[redacted]	[redacted]	0/1/FatalTimeout	0m
□	CONNECTED	[redacted]	[redacted]	[redacted]	[redacted]	0/32/AcceptedTimeout	0m
□	BACKED OFF	[redacted]	[redacted]	[redacted]	[redacted]	4/64/ForwardRejectedOverload	0m
□	BACKED OFF	[redacted]	[redacted]	[redacted]	[redacted]	1/2/ForwardRejectedOverload	0m
□	DISCONNECTED*	[redacted]	[redacted]	[redacted]	[redacted]	0/1/	18h47m
□	DISCONNECTED*	[redacted]	[redacted]	[redacted]	[redacted]	0/1/	1d1h
□	DISCONNECTED*	[redacted]	[redacted]	[redacted]	[redacted]	0/1/	1d4h
□	DISCONNECTED*	[redacted]	[redacted]	[redacted]	[redacted]	0/1/	21h51m
□	DISCONNECTED	[redacted]	[redacted]	[redacted]	[redacted]	0/1/	18h47m
□	NEVER CONNECTED*	[redacted]	[redacted]	[redacted]	[redacted]	0/1/	23h33m

* Requesting ARK

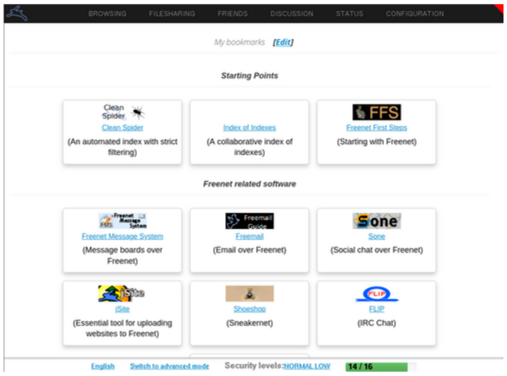
Add another peer

The Freenet 0.7 darknet peers list.

Freenet has been under continuous development since 2000.

Freenet 0.7, released on 8 May 2008, is a major re-write incorporating a number of fundamental changes. The most fundamental change is support for darknet operation. Version 0.7 offered two modes of operation: a mode in which it connects only to friends, and an opennet-mode in which it connects to any other Freenet user. Both modes can be run simultaneously. When a user switches to pure darknet operation, Freenet becomes very difficult to detect from the outside. The transport layer created for the darknet mode allows communication over restricted routes as commonly found in mesh networks, as long as these connections follow a small-world structure.[22]:815–816 Other modifications include switching from TCP to UDP, which allows UDP hole punching along with faster transmission of messages between peers in the network.[23]

Freenet 0.7.5, released on 12 June 2009, offers a variety of improvements over 0.7. These include reduced memory usage, faster insert and retrieval of content, significant improvements to the



My bookmarks [Edit]

Starting Points

Clean Spider
(An automated index with strict filtering)

Index of Indexes
(A collaborative index of indexes)

Freenet First Steps
(Starting with Freenet)

Freenet related software

Freenet Message System
(Message boards over Freenet)

Freemail
(Email over Freenet)

Sone
(Social chat over Freenet)

jSite
(Essential tool for uploading websites to Freenet)

Shoeshop
(Sneakernet)

FLIP
(IRC Chat)

English Switch to advanced mode Security levels:NORMAL LOW 14 / 16

FProxy index page (Freenet 0.7)

Developer	[1]
Initial release	March 2000
Stable release	0.7.5 build 1503[2] / 6 July 2025
Repository	https://github.com/hyphanet/fred
Written in	Java
Operating system	Cross-platform: Unix-like (Android, Linux, BSD, macOS), Microsoft Windows
Platform	Java
Available in	English, French, Italian, German, Dutch, Spanish, Portuguese, Swedish, Norwegian, Chinese, Russian[3]
Type	Anonymity application, peer-to-peer, friend-to-friend, overlay network, mix

FProxy web interface used for browsing freesites, and a large number of smaller bugfixes, performance enhancements, and usability improvements. Version 0.7.5 also shipped with a new version of the Windows installer.[24]

As of build 1226, released on 30 July 2009, features that have been written include significant security improvements against both attackers acting on the network and physical seizure of the computer running the node.[25]

	network, distributed data store
License	GNU General Public License version 3 only
Website	www.hyphanet.org (https://www.hyphanet.org)

As of build 1468, released on 11 July 2015, the Freenet core stopped using the db4o database and laid the foundation for an efficient interface to the Web of Trust plugin which provides spam resistance.[26]

Freenet has always been free software, but until 2011 it required users to install Java. This problem was solved by making Freenet compatible with OpenJDK, a free and open source implementation of the Java Platform.

On 11 February 2015, Freenet received the SUMA-Award for "protection against total surveillance".[27][28][29]

Features and user interface

Freenet served as the model for the Japanese peer to peer file-sharing programs Winny, Share and Perfect Dark, but this model differs from p2p networks such as Bittorrent and emule. Freenet separates the underlying network structure and protocol from how users interact with the network; as a result, there are a variety of ways to access content on the Freenet network. The simplest is via FProxy, which is integrated with the node software and provides a web interface to content on the network. Using FProxy, a user can browse freesites (websites that use normal HTML and related tools, but whose content is stored within Freenet rather than on a traditional web server). The web interface is also used for most configuration and node management tasks. Through the use of separate applications or plugins loaded into the node software, users can interact with the network in other ways, such as forums similar to web forums or Usenet or interfaces more similar to traditional P2P "filesharing" interfaces.

While Freenet provides an HTTP interface for browsing freesites, it is not a proxy for the World Wide Web; Freenet can be used to access only the content that has been previously inserted into the

Freenet network. In this way, it is more similar to Tor's onion services than to anonymous proxy software like Tor's proxy.

Freenet's focus lies on free speech and anonymity. Because of that, Freenet acts differently at certain points that are (directly or indirectly) related to the anonymity part. Freenet attempts to protect the anonymity of both people inserting data into the network (uploading) and those retrieving data from the network (downloading). Unlike file sharing systems, there is no need for the uploader to remain on the network after uploading a file or group of files. Instead, during the upload process, the files are broken into chunks and stored on a variety of other computers on the network. When downloading, those chunks are found and reassembled. Every node on the Freenet network contributes storage space to hold files and bandwidth that it uses to route requests from its peers.

As a direct result of the anonymity requirements, the node requesting content does not normally connect directly to the node that has it; instead, the request is routed across several intermediaries, none of which know which node made the request or which one had it. As a result, the total bandwidth required by the network to transfer a file is higher than in other systems, which can result in slower transfers, especially for infrequently accessed content.

Since version 0.7, Freenet offers two different levels of security: opennet and darknet. With opennet, users connect to arbitrary other users. With darknet, users connect only to "friends" with whom they previously exchanged public keys, named node-references. Both modes can be used together.

Content

Freenet's founders argue that true freedom of speech comes only with true anonymity and that the beneficial uses of Freenet outweigh its negative uses.[30] Their view is that free speech, in itself, is not in contradiction with any other consideration—the information is not the crime. Freenet attempts to remove the possibility of any group imposing its beliefs or values on any data. Although many states censor communications to different extents, they all share one commonality in that a body must decide what information to censor and what information to allow. What may be acceptable to one group of people may be considered offensive or even dangerous to another. In essence, the purpose of Freenet is to ensure that no one is allowed to decide what is acceptable.

Reports of Freenet's use in authoritarian nations is difficult to track due to the very nature of Freenet's goals. One group, *Freenet China*, used to introduce the Freenet software to Chinese users starting from 2001 and distribute it within China through e-mails and on disks after the group's website was blocked by the Chinese authorities on the mainland. It was reported that in 2002

Freenet China had several thousand dedicated users.[31]:70–71 However, Freenet opennet traffic was blocked in China around the 2010s.[32]

Technical design

The Freenet file sharing network stores documents and allows them to be retrieved later by an associated key, as is now possible with protocols such as HTTP. The network is designed to be highly survivable. The system has no central servers and is not subject to the control of any one individual or organization, including the designers of Freenet. The codebase size is over 192,000 lines of code.[33] Information stored on Freenet is distributed around the network and stored on several different nodes. Encryption of data and relaying of requests makes it difficult to determine who inserted content into Freenet, who requested that content, or where the content was stored. This protects the anonymity of participants, and also makes it very difficult to censor specific content. Content is stored encrypted, making it difficult for even the operator of a node to determine what is stored on that node. This provides plausible deniability; which, in combination with request relaying, means that safe harbor laws that protect service providers may also protect Freenet node operators. When asked about the topic, Freenet developers defer to the EFF discussion which says that not being able to filter anything is a safe choice.[34][35]

Distributed storage and caching of data

Like Winny, Share and Perfect Dark, Freenet not only transmits data between nodes but actually stores them, working as a huge distributed cache. To achieve this, each node allocates some amount of disk space to store data; this is configurable by the node operator, but is typically several GB (or more).

Files on Freenet are typically split into multiple small blocks, with duplicate blocks created to provide redundancy. Each block is handled independently, meaning that a single file may have parts stored on many different nodes.

Information flow in Freenet is different from networks like eMule or BitTorrent; in Freenet:

1. A user wishing to share a file or update a freesite "inserts" the file "to the network"
2. After "insertion" is finished, the publishing node is free to shut down, because the file is stored in the network. It will remain available for other users whether or not the original publishing node is online. No single node is responsible for the content; instead, it is replicated to many different nodes.

Two advantages of this design are high reliability and anonymity. Information remains available even if the publisher node goes offline, and is anonymously spread over many hosting nodes as encrypted blocks, not entire files.

The key disadvantage of the storage method is that no one node is responsible for any chunk of data. If a piece of data is not retrieved for some time and a node keeps getting new data, it will drop the old data sometime when its allocated disk space is fully used. In this way Freenet tends to 'forget' data which is not retrieved regularly (see also Effect).

While users can insert data into the network, there is no way to delete data. Due to Freenet's anonymous nature the original publishing node or owner of any piece of data is unknown. The only way data can be removed is if users don't request it.

Network

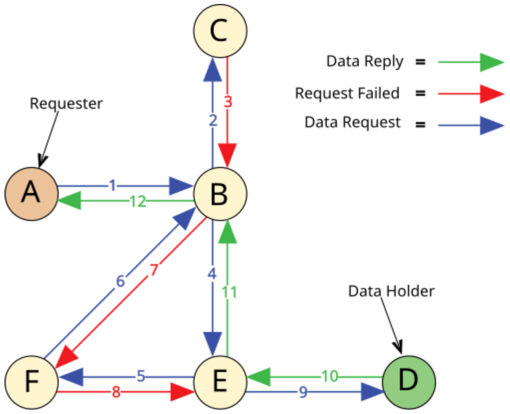
Typically, a host computer on the network runs the software that acts as a node, and it connects to other hosts running that same software to form a large distributed, variable-size network of peer nodes. Some nodes are end user nodes, from which documents are requested and presented to human users. Other nodes serve only to route data. All nodes communicate with each other identically – there are no dedicated "clients" or "servers". It is not possible for a node to rate another node except by its capacity to insert and fetch data associated with a key. This is unlike most other P2P networks where node administrators can employ a ratio system, where users have to share a certain amount of content before they can download.

Freenet may also be considered a small world network.

The Freenet protocol is intended to be used on a network of complex topology, such as the Internet (Internet Protocol). Each node knows only about some number of other nodes that it can reach directly (its conceptual "neighbors"), but any node can be a neighbor to any other; no hierarchy or other structure is intended. Each message is routed through the network by passing from neighbor to neighbor until it reaches its destination. As each node passes a message to a neighbor, it does not know whether the neighbor will forward the message to another node, or is the final destination or original source of the message. This is intended to protect the anonymity of users and publishers.

Each node maintains a data store containing documents associated with keys, and a routing table associating nodes with records of their performance in retrieving different keys.

Protocol



A typical request sequence. The request moves through the network from node to node, backing out of a dead-end (step 3) and a loop (step 7) before locating the desired file.

The Freenet protocol uses a key-based routing protocol, similar to distributed hash tables. The routing algorithm changed significantly in version 0.7. Prior to version 0.7, Freenet used a heuristic routing algorithm where each node had no fixed location, and routing was based on which node had served a key closest to the key being fetched (in version 0.3) or which is estimated to serve it faster (in version 0.5). In either case, new connections were sometimes added to downstream nodes (i.e. the node that answered the request) when requests succeeded, and old nodes were discarded in least recently used order (or something close to it). Oskar Sandberg's research (during the development of version 0.7) shows that this "path folding" is critical, and that a very simple routing algorithm will suffice provided there is path folding.

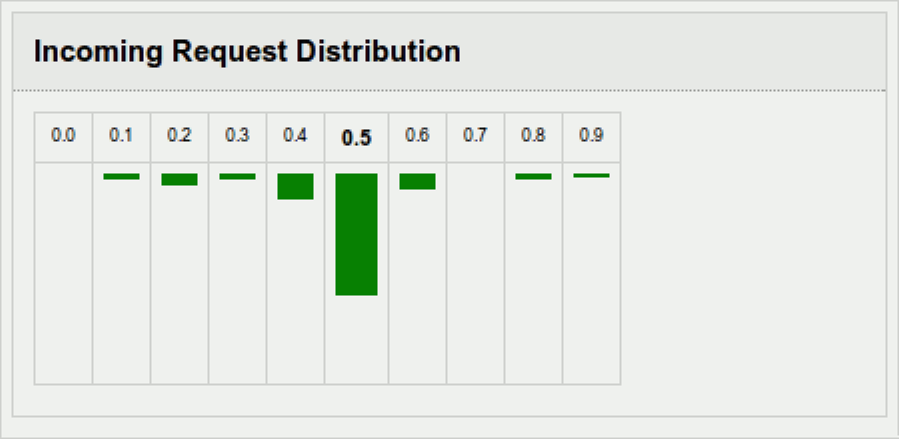
The disadvantage of this is that it is very easy for an attacker to find Freenet nodes, and connect to them, because every node is continually attempting to find new connections. In version 0.7, Freenet supports both "opennet" (similar to the old algorithms, but simpler), and "darknet" (all node connections are set up manually, so only your friends know your node's IP address). Darknet is less convenient, but much more secure against a distant attacker.

This change required major changes in the routing algorithm. Every node has a location, which is a number between 0 and 1. When a key is requested, first the node checks the local data store. If it's not found, the key's hash is turned into another number in the same range, and the request is routed to the node whose location is closest to the key. This goes on until some number of hops is exceeded, there are no more nodes to search, or the data is found. If the data is found, it is cached on each node along the path. So there is no one source node for a key, and attempting to find where it is currently stored will result in it being cached more widely. Essentially the same process is used to insert a document into the network: the data is routed according to the key until it runs out of hops, and if no existing document is found with the same key, it is stored on each node. If older data is found, the older data is propagated and returned to the originator, and the insert "collides".

But this works only if the locations are clustered in the right way. Freenet assumes that the darknet (a subset of the global social network) is a small-world network, and nodes constantly attempt to swap locations (using the Metropolis–Hastings algorithm) in order to minimize their distance to their neighbors. If the network actually is a small-world network, Freenet should find data reasonably quickly; ideally on the order of $O\left([\log(n)]^2\right)$ hops in big O notation. However, it does not guarantee that data will be found at all.[36]

Eventually, either the document is found or the hop limit is exceeded. The terminal node sends a reply that makes its way back to the originator along the route specified by the intermediate nodes' records of pending requests. The intermediate nodes may choose to cache the document along the way. Besides saving bandwidth, this also makes documents harder to censor as there is no one "source node".

Effect



The effect of the node specialising on the particular location.

Initially, the locations in darknet are distributed randomly. This means that routing of requests is essentially random. In opennet connections are established by a join request which provides an optimized network structure if the existing network is already optimized.[37] So the data in a newly started Freenet will be distributed somewhat randomly.[38]

As location swapping (on darknet) and path folding (on opennet) progress, nodes which are close to one another will increasingly have close locations, and nodes which are far away will have distant locations. Data with similar keys will be stored on the same node.[37]

The result is that the network will self-organize into a distributed, clustered structure where nodes tend to hold data items that are close together in key space. There will probably be multiple such clusters throughout the network, any given document being replicated numerous times, depending on how much it is used. This is a kind of "spontaneous symmetry breaking", in which an initially symmetric state (all nodes being the same, with random initial keys for each other) leads to a highly asymmetric situation, with nodes coming to specialize in data that has closely related keys.

There are forces which tend to cause clustering (shared closeness data spreads throughout the network), and forces that tend to break up clusters (local caching of commonly used data). These forces will be different depending on how often data is used, so that seldom-used data will tend to be on just a few nodes which specialize in providing that data, and frequently used items will be spread widely throughout the network. This automatic mirroring counteracts the times when web traffic becomes overloaded, and due to a mature network's intelligent routing, a network of size *n* should require only log(*n*) time to retrieve a document on average.[39]

Keys

Keys are hashes: there is no notion of semantic closeness when speaking of key closeness. Therefore, there will be no correlation between key closeness and similar popularity of data as there might be if keys did exhibit some semantic meaning, thus avoiding bottlenecks caused by popular subjects.

There are two main varieties of keys in use on Freenet, the Content Hash Key (CHK) and the Signed Subspace Key (SSK). A subtype of SSKs is the Updatable Subspace Key (USK) which adds versioning to allow secure updating of content.

A CHK is a SHA-256 hash of a document (after encryption, which itself depends on the hash of the plaintext) and thus a node can check that the document returned is correct by hashing it and checking the digest against the key. This key contains the meat of the data on Freenet. It carries all the binary data building blocks for the content to be delivered to the client for reassembly and decryption. The CHK is unique by nature and provides tamperproof content. A hostile node altering the data under a CHK will immediately be detected by the next node or the client. CHKs also reduce the redundancy of data since the same data will have the same CHK and when multiple sites reference the same large files, they can reference to the same CHK.[40]

SSKs are based on public-key cryptography. Currently Freenet uses the DSA algorithm. Documents inserted under SSKs are signed by the inserter, and this signature can be verified by every node to ensure that the data is not tampered with. SSKs can be used to establish a verifiable pseudonymous identity on Freenet, and allow for multiple documents to be inserted securely by a single person. Files inserted with an SSK are effectively immutable, since inserting a second file with the same name can cause collisions. USKs resolve this by adding a version number to the keys which is also used for providing update notification for keys registered as bookmarks in the web interface.[41] Another subtype of the SSK is the Keyword Signed Key, or KSK, in which the key pair is generated in a standard way from a simple human-readable string. Inserting a document using a KSK allows the document to be retrieved and decrypted if and only if the requester knows the human-readable string; this allows for more convenient (but less secure) URIs for users to refer to.[42]

Scalability

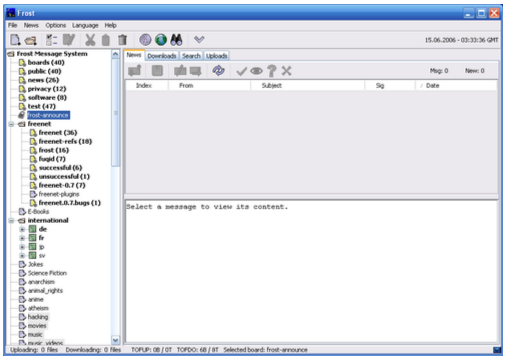
A network is said to be scalable if its performance does not deteriorate even if the network is very large. The scalability of Freenet is being evaluated, but similar architectures have been shown to scale logarithmically.[43] This work indicates that Freenet can find data in $O(\log^2 n)$ hops on a small-world network (which includes both opennet and darknet style Freenet networks), when ignoring the caching which could improve the scalability for popular content. However, this scalability is difficult to test without a very large network. Furthermore, the security features inherent to Freenet make detailed performance analysis (including things as simple as determining the size of the network) difficult to do accurately. As of now, the scalability of Freenet has yet to be tested.

Darknet versus opennet

As of version 0.7, Freenet supports both "darknet" and "opennet" connections. Opennet connections are made automatically by nodes with opennet enabled, while darknet connections are manually established between users that know and trust each other. Freenet developers describe the trust needed as "will not crack their Freenet node".[44] Opennet connections are easy to use, but darknet connections are more secure against attackers on the network, and can make it difficult for an attacker (such as an oppressive government) to even determine that a user is running Freenet in the first place.[45]

The core innovation in Freenet 0.7 is to allow a globally scalable darknet, capable (at least in theory) of supporting millions of users. Previous darknets, such as WASTE, have been limited to relatively small disconnected networks. The scalability of Freenet is made possible by the fact that human relationships tend to form small-world networks, a property that can be exploited to find short paths between any two people. The work is based on a speech given at DEF CON 13 by Ian Clarke and Swedish mathematician Oskar Sandberg. Furthermore, the routing algorithm is capable of routing over a mixture of opennet and darknet connections, allowing people who have only a few friends using the network to get the performance from having sufficient connections while still receiving some of the security benefits of darknet connections. This also means that small darknets where some users also have opennet connections are fully integrated into the whole Freenet network, allowing all users access to all content, whether they run opennet, darknet, or a hybrid of the two, except for darknet pockets connected only by a single hybrid node.[37]

Tools and applications



```
Select a message to view its content.
```

Uploading: 0 files Downloading: 0 files TOFUP: 0B / 0T TOFDO: 6B / 8T Selected board: frost-announce

Screenshot of Frost running on Microsoft Windows

Unlike many other P2P applications Freenet does not provide comprehensive functionality itself. Freenet is modular and features an API called Freenet Client Protocol (FCP) for other programs to use to implement services such as message boards, file sharing, or online chat.[46]

Communication

Freenet Messaging System (FMS)

FMS was designed to address problems with Frost such as denial of service attacks and spam. Users publish trust lists, and each user downloads messages only from identities they trust and identities trusted by identities they trust. FMS is developed anonymously and can be downloaded from *the FMS freesite* within Freenet. It does not have an official site on the normal Internet. It features random post delay, support for many identities, and a distinction between trusting a user's posts and trusting their trust list. It is written in C++ and is a separate application from Freenet which uses the Freenet Client Protocol (FCP) to interface with Freenet.

Frost

Frost includes support for convenient file sharing, but its design is inherently vulnerable to spam and denial of service attacks.[47] Frost can be downloaded from the Frost home page on

SourceForge, or from *the Frost freesite* within Freenet. It is not endorsed by the Freenet developers. Frost is written in Java and is a separate application from Freenet.

Sone

Sone provides a simpler interface inspired by Facebook[48] with public anonymous discussions and image galleries. It provides an API for control from other programs[49] is also used to implement a comment system for static websites in the regular internet.[50][51]

Utilities

jSite

jSite is a tool to upload websites. It handles keys and manages uploading files.

Infocalypse

Infocalypse is an extension for the distributed revision control system Mercurial. It uses an optimized structure to minimize the number of requests to retrieve new data, and allows supporting a repository by securely reuploading most parts of the data without requiring the owner's private keys.[52]

Libraries

FCPLib

FCPLib (Freenet Client Protocol Library) aims to be a cross-platform natively compiled set of C++-based functions for storing and retrieving information to and from Freenet. FCPLib supports Windows NT/2K/XP, Debian, BSD, Solaris, and macOS.

lib-pyFreenet

lib-pyFreenet exposes Freenet functionality to Python programs. Infocalypse uses it.

Vulnerabilities

Law enforcement agencies have claimed to have successfully infiltrated Freenet opennet in order to deanonymize users[53] but no technical details have been given to support these allegations. One report stated that, "A child-porn investigation focused on ... [the suspect] when the authorities were monitoring the online network, Freenet."[54] A different report indicated arrests may have been based on the BlackICE project leaks, that are debunked for using bad math[55] and for using an incorrectly calculated false positives rate and a false model.[56]

A court case in the Peel Region of Ontario, *Canada R. v. Owen*, 2017 ONCJ 729 (CanLII), illustrated that law enforcement do in fact have a presence, after Peel Regional Police located who had been downloading illegal material on the Freenet network.[57] The court decision indicates that a Canadian Law Enforcement agency operates nodes running modified Freenet software in the hope of determining who is requesting illegal material.

- **Routing Table Insertion** (RTI) Attack[58]

Notability

Freenet has had significant publicity in the mainstream press, including articles in *The New York Times*, and coverage on CNN, *60 Minutes II*, the BBC, *The Guardian*,[8] and elsewhere.

Freenet received the SUMA-Award 2014 for "protection against total surveillance".[27][28][29]

Freesite

A "freesite" is a site hosted on the Freenet network. Because it contains only static content, it cannot contain any active content like server-side scripts or databases. Freesites are coded in HTML and support as many features as the browser viewing the page allows; however, there are some exceptions where the Freenet software will remove parts of the code that may be used to reveal the identity of the person viewing the page (making a page access something on the internet, for example).

See also

- Peer-to-peer web hosting
- Rendezvous protocol
- Anonymous P2P
- Crypto-anarchism
- Cypherpunk
- Distributed file system
- Freedom of information
- Friend-to-friend

Free and open-source software portal

Comparable software

- GNUnet
- I2P
- InterPlanetary File System
- Java Anon Proxy (also known as JonDonym)
- Osiris
- Perfect Dark – also creates a distributed data store shared by anonymous nodes; the successor to Share, which itself is the successor of Winny
- Tahoe-LAFS
- ZeroNet

References

1. "People" (https://web.archive.org/web/20130921053414/https://freenetproject.org/people.html) . Freenet: The Free Network official website. 22 September 2008. Archived from the original (https://freenetproject.org/people.html) on 21 September 2013. Retrieved 31 May 2014.
2. "Release build01503: 2025-07-06 · hyphanet/fred · GitHub" (https://github.com/hyphanet/fred/releases/tag/build01503) .
3. Language specific versions of Freenet (https://github.com/freenet/fred/tree/master/src/freenet/l10n) Archived (https://web.archive.org/web/20180207061812/https://github.com/freenet/fred/tree/master/src/freenet/l10n) 7 February 2018 at the Wayback Machine, *GitHub: Freenet*.
4. "Freenet renamed to Hyphanet" (https://www.hyphanet.org/freenet-renamed-to-hyphanet.html) . *hyphanet.org*. 26 June 2023. Retrieved 8 May 2025.
5. What is Freenet? (https://freenetproject.org/whatis.html) Archived (https://web.archive.org/web/20110916012340/https://freenetproject.org/whatis.html) 16 September 2011 at the Wayback Machine, *Freenet: The Free network official website*.
6. Taylor, Ian J. *From P2P to Web Services and Grids: Peers in a Client/Server World*. London: Springer, 2005.

7. Cohen, Adam (26 June 2000). "The Infoanarchist" (https://web.archive.org/web/20080708213917/http://www.time.com/time/magazine/article/0,9171,997286,00.html) . *Time*. Archived from the original (http://www.time.com/time/magazine/article/0,9171,997286,00.html) on 8 July 2008. Retrieved 18 December 2011.

8. Beckett, Andy (26 November 2009). "The dark side of the internet" (https://www.theguardian.com/technology/2009/nov/26/dark-side-internet-freenet) . *The Guardian*. Archived (https://web.archive.org/web/20130908073158/http://www.theguardian.com/technology/2009/nov/26/dark-side-internet-freenet) from the original on 8 September 2013. Retrieved 26 November 2009.

9. "The Guardian writes about Freenet (Ian Clarke's response)" (https://web.archive.org/web/20140519101142/http://blog.locut.us/2009/11/26/the-guardian-writes-about-freenet/) . Archived from the original (http://blog.locut.us/2009/11/26/the-guardian-writes-about-freenet/) on 19 May 2014.

10. "Sone: Pseudonymes Microblogging über Freenet" (http://draketo.de/licht/freie-software/freenet/sone-pseudonymes-microblogging) . Archived (https://web.archive.org/web/20151005053905/http://draketo.de/licht/freie-software/freenet/sone-pseudonymes-microblogging) from the original on 5 October 2015. Retrieved 15 September 2015., German article, 2010

11. "Infoclypse" (https://www.mercurial-scm.org/wiki/Infocalypse) . Wiki. *Mercurial*. Archived (https://web.archive.org/web/20211103010527/https://www.mercurial-scm.org/wiki/Infocalypse) from the original on 3 November 2021. Retrieved 2 December 2021.

12. "Flog Helper: Easy Blogging over Freenet" (https://github.com/freenet/plugin-FlogHelper-staging) . *GitHub*. 7 February 2019. Archived (https://web.archive.org/web/20220205041917/https://github.com/freenet/plugin-FlogHelper) from the original on 5 February 2022. Retrieved 16 December 2011.

13. "Web of Trust" (https://wiki.freenetproject.org/WoT) . 7 February 2019. Archived (https://web.archive.org/web/20151208180619/https://wiki.freenetproject.org/WoT) from the original on 8 December 2015. Retrieved 15 September 2015.

14. "Web Of Trust" (https://github.com/hyphanet/wiki/wiki/Web-Of-Trust) . *GitHub*. Retrieved 13 October 2024.

15. Freenet over Sneakernet. Freenet Key: USK@MYLAnId-ZEyXhDGGbYOa1gOtkZZrFNTXjFl1dibLj9E,Xpu27DoAKKc8b0718E-ZteFrGqCYROe7XBBJI57pB4M,AQACAAE/Shoeshop/2/

16. Markoff, John (10 May 2000). "Cyberspace Programmers Confront Copyright Laws" (https://www.nytimes.com/2000/05/10/business/cyberspace-programmers-confront-copyright-laws.html) . *The New York Times*. Archived (https://web.archive.org/web/20170217084607/http://www.nytimes.com/2000/05/10/business/cyberspace-programmers-confront-copyright-laws.html) from the original on 17 February 2017. Retrieved 19 February 2017.

17. "Coders prepare son of Napster" (https://news.bbc.co.uk/2/hi/science/nature/1216486.stm) . *BBC News*. 12 March 2001. Archived (https://web.archive.org/web/20140104024058/http://news.bbc.co.uk/2/hi/science/nature/1216486.stm) from the original on 4 January 2014. Retrieved 1 June 2014.

18. "Fighting for free speech on the Net" (http://www.cnn.com/2005/TECH/12/19/internet.freedom/index.html?iref=allsearch) . CNN. 19 December 2005. Archived (https://web.archive.org/web/20140602200717/http://www.cnn.com/2005/TECH/12/19/internet.freedom/index.html?iref=allsearch) from the original on 2 June 2014. Retrieved 1 June 2014.

19. Ian Clarke. A distributed decentralised information storage and retrieval system (https://freenetproject.org/papers/ddisrs.pdf) Archived (https://web.archive.org/web/20120316102156/https://freenetproject.org/papers/ddisrs.pdf) 16 March 2012 at the Wayback Machine. Unpublished report, Division of Informatics, University of Edinburgh, 1999.

20. Ian Clarke, Oskar Sandberg, Brandon Wiley, and Theodore W. Hong. Freenet: A Distributed Anonymous Information Storage and Retrieval System (https://www.cs.cornell.edu/People/egs/615/freenet.pdf) Archived (https://web.archive.org/web/20150404062238/http://www.cs.cornell.edu/people/egs/615/freenet.pdf) 4 April 2015 at the Wayback Machine. In: Proceedings of the International Workshop on Designing Privacy Enhancing Technologies: Design Issues in Anonymity and Unobservability. New York, NY: Springer-Verlag, 2001, p. 46-66.

21. Clarke, Ian; Sandberg, Oskar; Wiley, Brandon; Hong, Theodore W. (28 February 2001). "Freenet: A Distributed Anonymous Information Storage and Retrieval System" (https://web.archive.org/web/20230603205950/http://www.facweb.iitkgp.ac.in/~niloy/COURSE/Autumn2010/UC/Resource/freenet1-big.pdf) (PDF). *Designing Privacy Enhancing Technologies*. International Workshop on Design Issues in Anonymity and Unobservability. Springer-Verlag. pp. 46–66. doi:10.1007/3-540-44702-4_4 (https://doi.org/10.1007%2F3-540-44702-4_4) . ISBN 978-3-540-41724-8. Archived from the original on 3 June 2023.

22. Singh, Munindar P. The Practical Handbook of Internet Computing. Boca Raton, Fl.: Chapman & Hall, 2005.

23. Ihlenfeld, Jens (4 April 2006). "Freenet 0.7 soll globales Darknet schaffen" (http://www.golem.de/0604/44448.html) . Golem. Archived (https://web.archive.org/web/20151005170034/http://www.golem.de/0604/44448.html) from the original on 5 October 2015. Retrieved 17 September 2015.

24. release information for Freenet 0.7.5 (https://freenetproject.org/news.html#freenet-0-7-5-released) Archived (https://web.archive.org/web/20141129011927/https://freenetproject.org/news.html#freenet-0-7-5-released) 29 November 2014 at the Wayback Machine, last accessed 17 September 2015

25. release information for Freenet build 1226 (https://freenetproject.org/news.html#build1226) Archived (https://web.archive.org/web/20141129011927/https://freenetproject.org/news.html#build1226) 29 November 2014 at the Wayback Machine, last accessed 17 September 2015

26. Freenet 1468 release notes (https://freenetproject.org/news.html#20150711-1468-release) Archived (https://web.archive.org/web/20141129011927/https://freenetproject.org/news.html#20150711-1468-release) 29 November 2014 at the Wayback Machine 2015

27. SUMA Award (http://suma-awards.de/en/index.html) Archived (https://web.archive.org/web/20150320201527/http://suma-awards.de/en/index.html) 20 March 2015 at the Wayback Machine, 11 February 2015.

28. recording of the SUMA Award Ceremony 2015 (https://www.youtube.com/watch?v=dZpsBSPsHDI) Archived (https://web.archive.org/web/20150905121823/https://www.youtube.com/watch?v=dZpsBSPsHDI&app=desktop) 5 September 2015 at the Wayback Machine, published on 14 April 2015.

29. SUMA Award für das Freenet Projekt (http://www.heise.de/newsticker/meldung/SUMA-Award-fuer-das-Freenet-Project-2548577.html) Archived (https://web.archive.org/web/20150924152732/http://www.heise.de/newsticker/meldung/SUMA-Award-fuer-das-Freenet-Project-2548577.html) 24 September 2015 at the Wayback Machine Jo Bager in Heise online, 2015

30. "The Philosophy behind Freenet" (https://web.archive.org/web/20110430201105/http://freenetproject.org/philosophy.html) . Archived from the original (https://freenetproject.org/philosophy.html) on 30 April 2011. Retrieved 20 December 2010.

31. Damm, Jens, and Simona Thomas. *Chinese Cyberspaces Technological Changes and Political Effects*. London: Routledge, 2006.

32. "Hyphanet" (https://www.hyphanet.org/) . *www.hyphanet.org*. Retrieved 3 July 2024.

33. Terry, Kyle. *The dark side of the web -- exploring darknets* (https://www.youtube.com/watch?v=HfuZJVpNWR4&feature=youtu.be&list=TLPQMjMwOTIwMjDcsXnGLhV7-Q&t=635) . Salem, Baden-Württemberg: TEDx Talks. Archived (https://ghostarchive.org/varchive/youtube/20211211/HfuZJVpNWR4) from the original on 11 December 2021.

34. Toseland, Matthew. "Does Freenet qualify for DMCA Safe Harbor?" (https://web.archive.org/web/20160303232303/https://emu.freenetproject.org/pipermail/chat/2009-February/001872.html) . Archived from the original (https://emu.freenetproject.org/pipermail/chat/2009-February/001872.html) on 3 March 2016. Retrieved 27 January 2013.

35. "IAAL*: What Peer-to-Peer Developers Need to Know about Copyright Law" (https://www.eff.org/wp/iaal-what-peer-peer-developers-need-know-about-copyright-law) . 10 January 2006. Archived (https://web.archive.org/web/20151130021911/https://www.eff.org/wp/iaal-what-peer-peer-developers-need-know-about-copyright-law) from the original on 30 November 2015. Retrieved 15 September 2015.

36. Clarke, Ian (2010). *Private Communication Through a Network of Trusted Connections: The Dark Freenet* (https://freenetproject.org/papers/freenet-0.7.5-paper.pdf) (PDF). Archived (https://web.archive.org/web/20171201033416/https://freenetproject.org/papers/freenet-0.7.5-paper.pdf) (PDF) from the original on 1 December 2017. Retrieved 15 September 2015.

37. Roos, Stefanie (2014). *Measuring Freenet in the Wild: Censorship-Resilience under Observation* (https://freenetproject.org/papers/roos-pets2014.pdf) (PDF). Springer International Publishing. pp. 263–282. ISBN 978-3-319-08505-0. Archived (https://web.archive.org/web/20141116144052/https://freenetproject.org/papers/roos-pets2014.pdf) (PDF) from the original on 16 November 2014. Retrieved 15 September 2015.

38. "Freenet Project Documentation" (https://freenetproject.org/) . *freenetproject.org*. Archived (https://web.archive.org/web/20110216062257/http://freenetproject.org/) from the original on 16 February 2011. Retrieved 20 April 2022.

39. "FreeNet" (https://www.networxsecurity.org/members-area/glossary/f/freenet.html) . *networxsecurity.org*. Archived (https://web.archive.org/web/20190126001007/https://www.networxsecurity.org/members-area/glossary/f/freenet.html) from the original on 26 January 2019. Retrieved 25 January 2019.

40. "freesitemgr, code for inserting files as CHK, fixed revision" (https://github.com/freenet/lib-pyFreenet/blob/b78aea05222c4afe5145d8b529d2a54d4b93887a/fcp/sitemgr.py#L976) . *GitHub*. Archived (https://web.archive.org/web/20220205041918/https://github.com/freenet/pyFreenet/blob/b78aea05222c4afe5145d8b529d2a54d4b93887a/fcp/sitemgr.py#L976) from the original on 5 February 2022. Retrieved 29 November 2017.

41. Babenhauserheide, Arne. "USK and Date-Hints: Finding the newest version of a site in Freenet's immutable datastore" (http://draketo.de/light/english/freenet/usk-and-date-hints). *draketo.de*. Archived (https://web.archive.org/web/20150208101405/http://draketo.de/light/english/freenet/usk-and-date-hints) from the original on 8 February 2015. Retrieved 29 November 2017.

42. Babenhauserheide, Arne. "Effortless password protected sharing of files via Freenet" (http://draketo.de/light/english/freenet/effortless-password-protected-sharing-files). *draketo.de*. Archived (https://web.archive.org/web/20150910030851/http://draketo.de/light/english/freenet/effortless-password-protected-sharing-files) from the original on 10 September 2015. Retrieved 29 November 2017.

43. Kleinberg, Jon (2000). "The Small-World Phenomenon: An Algorithmic Perspective" (https://www.cs.cornell.edu/home/kleinber/swn.pdf) (PDF). *Proceedings of the thirty-second annual ACM symposium on Theory of computing*. pp. 163–70. doi:10.1145/335305.335325 (https://doi.org/10.1145%2F335305.335325). ISBN 978-1-58113-184-0. S2CID 221559836 (https://api.semanticscholar.org/CorpusID:221559836). Archived (https://web.archive.org/web/20131112052807/http://www.cs.cornell.edu/home/kleinber/swn.pdf) (PDF) from the original on 12 November 2013. Retrieved 22 August 2013.

44. "Required trust for forming a darknet connection" (https://web.archive.org/web/20151007012112/https://d6.gnutella2.info/freenet/USK@sUm3oJISSEU4pl2Is9qa1eRoCLyz6r2LPkEqlXc3~oc,yBEbf-IJrcB8Pe~gAd53DEEHgbugUkFSHtzzLqnYlbs,AQACAAE/random_babcom/156/#Requiredtrustforformingadarknetconnection). *random_babcom*. Archived from the original (https://d6.gnutella2.info/freenet/USK@sUm3oJISSEU4pl2Is9qa1eRoCLyz6r2LPkEqlXc3~oc,yBEbf-IJrcB8Pe~gAd53DEEHgbugUkFSHtzzLqnYlbs,AQACAAE/random_babcom/156/#Requiredtrustforformingadarknetconnection) on 7 October 2015. Retrieved 29 November 2017.

45. "Darknet-Fähigkeiten sollen Softwarenutzung verbergen" (http://www.golem.de/0805/59592.html). Golem. 9 May 2008. Archived (https://web.archive.org/web/20151005070232/http://www.golem.de/0805/59592.html) from the original on 5 October 2015. Retrieved 29 November 2017.

46. Freenet Social Networking guide (http://freesocial.draketo.de/) Archived (https://web.archive.org/web/20150815123435/http://freesocial.draketo.de/) 15 August 2015 at the Wayback Machine Justus Ranvier, 2013

47. Developer discussion about fixing Frost shortcomings (https://www.mail-archive.com/devl@freenetproject.org/msg17363.html) Archived (https://web.archive.org/web/20171201033622/https://www.mail-archive.com/devl@freenetproject.org/msg17363.html) 1 December 2017 at the Wayback Machine Matthew Toseland, 2007

48. description of Sone by its developer (https://flattr.com/thing/81996/Sone-The-Freenet-Social-Network-Plugin) Archived (https://web.archive.org/web/20171201042007/https://flattr.com/thing/81996/Sone-The-Freenet-Social-Network-Plugin) 1 December 2017 at the Wayback Machine, "it's a Facebook clone on top of Freenet", retrieved 15 September 2015

49. Sone in Freenet Wiki (https://wiki.freenetproject.org/Sone) Archived (https://web.archive.org/web/20150812111038/https://wiki.freenetproject.org/Sone) 12 August 2015 at the Wayback Machine, with the description of the FCP API, retrieved 14 September 2015

50. babcom description (http://draketo.de/proj/freecom/) Archived (https://web.archive.org/web/20150511180725/http://draketo.de/proj/freecom/) 11 May 2015 at the Wayback Machine, "it submits a search request on your local Sone instance by creating an iframe with the right URL", 2014.

51. "Sone" (https://d6.gnutella2.info/freenet/USK@nwa8lHa271k2QvJ8aa0Ov7IHAV-DFOCFgmDt3X6BpCI,DuQSUZiI~agF8c-6tjsFFGuZ8eICrzWCILB60nT8KKo,AQACAAE/sone/71/) . Archived (https://web.archive.org/web/20151002144720/https://d6.gnutella2.info/freenet/USK@nwa8lHa271k2QvJ8aa0Ov7IHAV-DFOCFgmDt3X6BpCI,DuQSUZiI~agF8c-6tjsFFGuZ8eICrzWCILB60nT8KKo,AQACAAE/sone/71/) from the original on 2 October 2015. Retrieved 15 September 2015.

52. "Information about infocalypse. A mirror of the included documentation" (http://draketo.de/light/english/freenet/infocalypse-mercurial-survive-the-information-apocalypse#advocacy) . Archived (https://web.archive.org/web/20120127055008/http://draketo.de/light/english/freenet/infocalypse-mercurial-survive-the-information-apocalypse#advocacy) from the original on 27 January 2012. Retrieved 16 December 2011.

53. Volpenheim, Sarah (18 November 2015). "Predators, police in online struggle" (https://www.thedickinsonpress.com/news/predators-police-in-online-struggle) . *The Dickinson Press*. Archived (https://web.archive.org/web/20231230234948/https://www.thedickinsonpress.com/news/predators-police-in-online-struggle) from the original on 30 December 2023. Retrieved 30 December 2023.

54. "Man jailed indefinitely for refusing to decrypt hard drives loses appeal" (https://arstechnica.com/tech-policy/2017/03/man-jailed-indefinitely-for-refusing-to-decrypt-hard-drives-loses-appeal/) . *Ars Technica*. 20 March 2017. Archived (https://web.archive.org/web/20170321062227/https://arstechnica.com/tech-policy/2017/03/man-jailed-indefinitely-for-refusing-to-decrypt-hard-drives-loses-appeal/) from the original on 21 March 2017. Retrieved 21 March 2017.

55. "Police department's tracking efforts based on false statistics" (https://freenetproject.org/police-departments-tracking-efforts-based-on-false-statistics.html) . *freenetproject.org*. 26 May 2016. Archived (https://web.archive.org/web/20220205041920/https://freenetproject.org/police-departments-tracking-efforts-based-on-false-statistics.html) from the original on 5 February 2022. Retrieved 23 September 2017.

56. Arnebab. "Errors in the Levine 2017 paper on attacks against Freenet" (https://www.draketo.de/software/levine-2017-errors) . *draketo.de*. Archived (https://web.archive.org/web/20210414044800/https://www.draketo.de/software/levine-2017-errors) from the original on 14 April 2021. Retrieved 3 January 2021.

57. "CanLII - 2017 ONCJ 729 (CanLII)" (https://www.canlii.org/en/on/oncj/doc/2017/2017oncj729/2017oncj729.html) . 3 November 2017. Archived (https://web.archive.org/web/20210117201444/https://www.canlii.org/en/on/oncj/doc/2017/2017oncj729/2017oncj729.html) from the original on 17 January 2021. Retrieved 13 November 2017.

58. "A Routing Table Insertion (RTI) Attack on Freenet" (https://www.researchgate.net/publication/261061477) . Archived (https://web.archive.org/web/20220205041920/https://www.researchgate.net/publication/261061477_A_Routing_Table_Insertion_RTI_Attack_on_Freenet) from the original on 5 February 2022. Retrieved 12 February 2021.

Further reading

- Clarke, I.; Miller, S.G.; Hong, T.W.; Sandberg, O.; Wiley, B. (2002). "Protecting free expression online with Freenet" (http://www.doc.ic.ac.uk/~twh1/longitude/papers/ieee-final.pdf) (PDF). *IEEE Internet Computing*. **6** (1): 40–9. CiteSeerX 10.1.1.21.9143 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.21.9143) . doi:10.1109/4236.978368 (https://doi.org/10.1109%2F4236.978368) . Archived (https://web.archive.org/web/20040720044931/http://www.doc.ic.ac.uk/~twh1/longitude/papers/ieee-final.pdf) (PDF) from the original on 20 July 2004.
- Von Krogh, Georg; Spaeth, Sebastian; Lakhani, Karim R (2003). "Community, joining, and specialization in open source software innovation: A case study" (https://www.alexandria.unisg.ch/30623/1/Community%2C%20joining%2C%20and%20specialization%20in%20open%20source%20software%20innovation%20-%20a%20case%20study.pdf) (PDF). *Research Policy*. **32** (7):

1217–41. doi:10.1016/S0048-7333(03)00050-7 (https://doi.org/10.1016%2FS0048-7333%2803%2900050-7) . Archived (https://web.archive.org/web/20180720115900/https://www.alexandria.unisg.ch/30623/1/Community%2C%20joining%2C%20and%20specialization%20in%20open%20source%20software%20innovation%20-%20a%20case%20study.pdf) (PDF) from the original on 20 July 2018.

- Dingledine, Roger; Freedman, Michael J.; Molnar, David (2001). "The Free Haven Project: Distributed Anonymous Storage Service". *Designing Privacy Enhancing Technologies*. Lecture Notes in Computer Science. pp. 67–95. CiteSeerX 10.1.1.420.478 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.420.478) . doi:10.1007/3-540-44702-4_5 (https://doi.org/10.1007%2F3-540-44702-4_5) . ISBN 978-3-540-41724-8.
- Clarke, Ian; Sandberg, Oskar; Wiley, Brandon; Hong, Theodore W. (2001). "Freenet: A Distributed Anonymous Information Storage and Retrieval System". *Designing Privacy Enhancing Technologies*. Lecture Notes in Computer Science. pp. 46–66. CiteSeerX 10.1.1.26.4923 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.26.4923) . doi:10.1007/3-540-44702-4_4 (https://doi.org/10.1007%2F3-540-44702-4_4) . ISBN 978-3-540-41724-8.
- Riehl, Damien A. (2000). "Peer-to-Peer Distribution Systems: Will Napster, Gnutella, and Freenet Create a Copyright Nirvana or Gehenna?". *The William Mitchell Law Review*. **27** (3): 1761.
- Roemer, Ryan (Fall 2002). "The Digital Evolution: Freenet and the Future of Copyright on the Internet" (http://www.lawtechjournal.com/articles/2002/05_021229_roemer.php) . *UCLA Journal of Law and Technology*. **5**.
- Sun, Xiaoqing; Liu, Baoxu; Feng, Dengguo (2005). "Analysis of Next Generation Routing of Freenet". *Computer Engineering* (17): 126–8.
- Hui Zhang; Goel, Ashish; Govindan, Ramesh (2002). "Using the small-world model to improve Freenet performance". *INFOCOM 2002: Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies*. Vol. 3. pp. 1228–37. CiteSeerX 10.1.1.74.7011 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.74.7011) . doi:10.1109/INFCOM.2002.1019373 (https://doi.org/10.1109%2FINFCOM.2002.1019373) . ISBN 978-0-7803-7476-8. S2CID 13182323 (https://api.semanticscholar.org/CorpusID:13182323) .

External links

- Official website (https://www.hyphanet.org/)