Layer Minus Network Protocol

CONET Lab Oct/2023

ABSTRACT

The Internet has become an indispensable part of our lives. It has become the medium we communicate with, access digital media, shop and access our finances. A large amount of stable and reliable infrastructure has been created to support it, but at the same time is being leveraged by the companies that control it.

"Data is the new oil." - Clive Humby

The internet was not created with security or privacy in mind. Any attempt to add privacy or security has had to be "patched" in, not solving root issues the Internet creates due to its design. As tech companies grow, they look for ways of increasing their revenues by mining data from users to use themselves, or even sell to others, and it has become a digital gold mine. The majority of users are protected by government policy and regulation that mostly affect infrastructure providers, but it has been proven again and again that they can't be trusted. While anonymization tools exist, most users don't know or care about them and most are too technical to benefit the average user.

With the rise of cryptocurrencies such as Bitcoin and Ethereum in recent years, users have been shown the benefits of decentralized networks. These are systems where users have pseudo-anonymity and can interact with the networks in a trustless and permissionless way. These networks are impossible to take down, due to being decentralized, and no single entity has the power to censor interactions and track user data.

People have pinned their hopes of transforming the Internet using blockchain technology, and the concept of Web3 was born. When comparing blockchain technology with the Internet, the disadvantages are obvious. The amount of data stored on the internet is staggering and blockchain is a notoriously expensive way to store data. How can we take advantage of the privacy benefits of blockchain with the infinitely scalable data storage of the internet?

CONET intends to provide a privacy-first network infrastructure based on Internet and decentralized blockchain technology, achieve fast and high throughput of the Internet, and achieve the goal of getting rid of all the privacy constraints of the existing Internet on Web3.

INTRODUCTION

CONET created a physical virtual network infrastructure using the Layer Minus protocol on the Internet.

Layer Minus is a virtual private network infrastructure layer on the Internet. It uses wallet addresses as identifiers for private communication, in lieu of IP addresses, once inside the network, and is also the layer that provides anonymous routing of user communications.

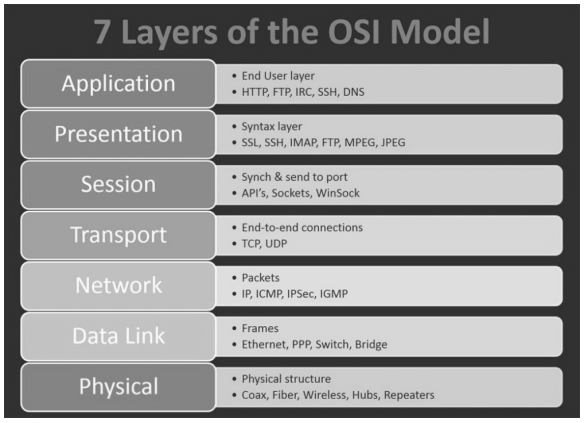
Whether it is ordinary Internet data, blockchain, or IoT, CONET can serve as the underlying infrastructure of the network, bringing them privacy, anonymity, and secure data communication.

LAYER MINUS PROTOCOL

The Internet is composed of hardware infrastructure and software infrastructure. The hardware infrastructure consists of client computers, routers, and critical Internet infrastructure[1] (routers, ISP access hubs, fiber optic cables, switches, satellites and submarine cables of the backbone network, etc.). Software infrastructure consists of communication protocols[2], domain name systems[3], login systems, data centers[4], etc.

OSI MODEL

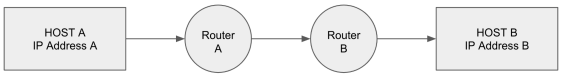
The model partitions the flow of data in a communication system into seven abstraction layers[5] to describe networked communication from the physical implementation of transmitting bits[6] across a communications medium[7] to the highest-level representation of data of a



distributed application[8][9]. Each intermediate layer serves a class of functionality to the layer above it and is served by the layer below it. Classes of functionality are realized in all software development through all standardized communication protocols[10].

The two major international organizations that play a major role in formulating computer network[11] standards are: International Telecommunication Union Telecommunication Standardization Sector [12] (ITU-T) and the International Standards Organization[13] (ISO). These standards allow computers of different types and operating systems around the world to communicate with each other.

TCP/IP PROTOCOL



TCP/IP provides a point-to-point connection mechanism that standardizes how data should be encapsulated, addressed, transmitted, routed, and received at the destination.

IP ADDRESS[14]

When a device is connected to the network, the device will be assigned an IP address, which is used as a unique identifier. Devices can communicate with each other through IP addresses on the Internet around the world. Without an IP address, we have no way of knowing which device is the sender and which is the receiver. An IP address has two main functions: identifying a device or network and addressing it.

In 1981, the IETF[15] defined IPv4 for 32-bit IP addresses. With the development of the Internet, IPv4 was gradually allocated and exhausted. Its upgraded version, IPv6[16], was officially announced by the Internet Engineering Task Force[17] in the form of Internet Standards Specification (RFC 2460) in December 1998.

IP ADDRESS SPACE ALLOCATION

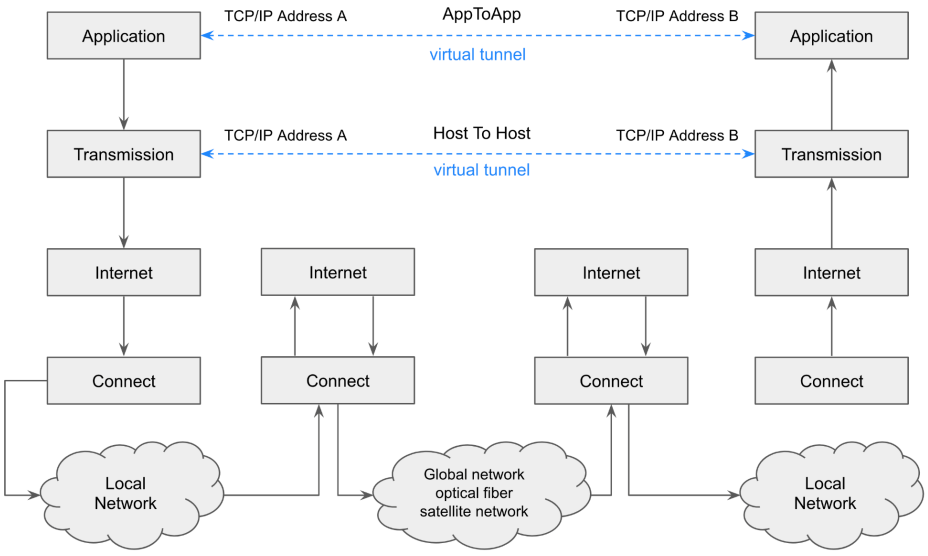
IP address space, whether IPv4 or IPv6, is allocated globally by the centralized Internet Assigned Numbers Authority (IANA[18]) and five other regional Regional Internet Registries (RIR) are assigned to the Internet within their designated area.

IP ADDRESS LEASING

When users use the Internet, they need to complete KYC[19] (Know Your Customer) procedures with the Internet service provider[20] before they can rent a globally unique IP address from an ISP.

ROUTING[21]

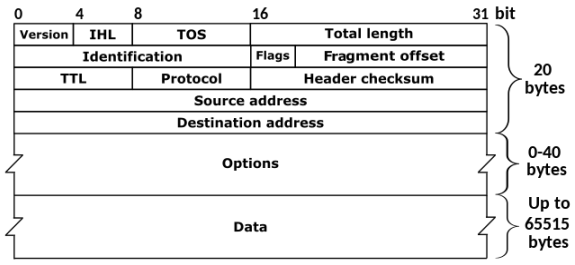
Due to the complex structure of the Internet, routing determines how two computers find each other and find a suitable best path. The router[22] is the key facility that determines how to forward an IP data packet and connect to each other on the Internet. IP packets[23] can pass through multiple routes, but there is no guarantee that they will arrive or that they will arrive in order.



VIRTUAL TUNNEL

Through the layering concept, Internet communication can be simplified into host-to-host network communication and application-to-application network communication.

INTERNET TCP/IP COMMUNICATION PRIVACY THREATS



IP Address Privacy Problems

The TCP/IP package of the Internet communication protocol consists of header metadata including the source address, destination address, and content (data). Due to the widespread use of SSL encrypted communication recommended by W3C[24], the threat of content (data) privacy leakage is greatly reduced.

Due to the header metadata being transmitted in clear text (unencrypted), personal information about users is leaked:

- Geographic location of communicating parties
- Software used to transmit the data
- Frequency of communication.

Due to ISPs requiring KYC, IANA can obtain a user's identity with just the IP address, including the registered owner, and possibly even the current tenant.

Having access to this information makes the internet less open and free.
Packet data can be blocked by IP addresses, on both the sending and the receiving end, preventing users from connecting or making outbound connections. This data leak can be abused by individual server hosts or even at the ISP level and it is all easily logged.

Web hosts can block users by ip address, preventing specific users or blocking whole regions of users from making connections. In the same way outgoing communications can be blocked as well.

Web hosts can deanonymize users that connect to their server.Web hosts can block certain types of applications.

- Internet traffic can be filtered based on origin or destination IP address or domain, banning specific users or large groups of users.
- Block network communication of certain types of applications, such as Bitcoin or torrents.

Technical measures that network monitors can take:

- Traffic filtering system based on destination IP address or domain name.
- Obtain the current real geographical location of the monitored object.
- Obtain the social network of the monitored object.
- Block network communication of a certain type of application software. Such as blocking the communication protocol of Bitcoin and Ethereum.

Internet application service providers exploit privacy:

- Obtain the visitor’s true identity.
- Tailor-made advertising.
- Identity-based denial of service.
- Record and collect visitor data, combined with big data models, to obtain an accurate personnel evaluation system. For example, a centralized artificial intelligence system can evaluate the user's cultural beliefs, knowledge reserves, living habits, IQ level, current happiness, anger, sorrow, and joy through big data analysis based on the accumulation of visitors' questions, and can predict the user's next step. hours, possible actions for the next week.

INTERNET PRIVACY COMMUNICATION SOLUTIONS

Almost all existing privacy enhancement tools are based on replacing the sender IP address with the service provider IP address to hide the metadata of the real sender IP address.

VIRTUAL PRIVATE NETWORK[25](VPN)

Sender first accesses the VPN provider, then replaces their source IP address with the VPN provider's IP address, and then visits the destination host IP address.
Advantages: Seamless integration with all Internet applications.The sender hides the real destination IP address, monitors can not know who the sender is communicating with and what application sender is using. Internet service providers also can not get the true location of the sender. A VPN only anonymizes the sender, not the Internet service provider host.
Disadvantages: Users cannot remain anonymous with a VPN provider, network access footprints can be recorded by the VPN provider, and VPN-specific communication protocols (fingerprint) can be intercepted by network surveillance (for example, the Great Firewall of China[26] blocks VPN protocols).

TOR ONION NETWORK[27]

Similar to VPN upgrades, the VPN that has mastered the secret is split into several parts, consisting of network entry nodes, intermediate springboards, and exit nodes. Increased difficulty in de-anonymization.

Advantages: Better privacy than VPN.

Disadvantages: Since it passes through more nodes than VPN, each node needs decryption and encryption operations, which results in lower communication efficiency than VPN. All Tor nodes are provided by volunteers, the network's quality cannot be guaranteed and can't be used by commercial applications. Special communication protocols can be intercepted by network monitoring. Provides limited anonymity host through augmentation technology.

DECENTRALIZED VPN (DVPN)

The decentralized VPN[28] service provision under the blockchain incentive mechanism inherits all the advantages and disadvantages of VPN. The workload proof mechanism promotes participants to provide high-quality services, but at the same time, allows users to be easier de-anonymized leaving hidden dangers. Blockchain-based payment systems could achieve better

anonymity.

NYM

Nym protects internet traffic by routing it through a decentralized mixnet[29] that can be accessed anonymously using zk-nyms.

Advantages: Better privacy than VPN and Tor, decentralization under the blockchain incentive mechanism, workload proof mechanism guarantees high quality of service.

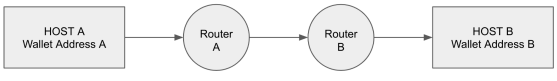
Disadvantages: Special communication protocols can be intercepted by network monitoring. The additional proof-of-work mechanism increases the cost of use and may cause the user to be de-anonymized. Provides limited anonymity host[30] through augmentation technology.

LAYER MINUS PROTOCOL

The Layer Minus Protocol is a network protocol that establishes a point-to-point communication used as a wallet address mechanism rather than an IP address, defining how data should be encapsulated, addressed, transmitted, routed, and received at the destination.

ASYMMETRIC CRYPTOGRAPHY

Cryptography contains the following elements:



- **Confidentiality**: ensuring that information can only be obtained by authorized persons.
- Integrity: Detects whether the message has been tampered with.
- **Authentication:** The sender and receiver need to be verifiable and identifiable.
- **Non-Reputation:** Provide transaction proof between the sender and receiver of the message.

Asymmetric encryption allows users to have a pair of keys: a public key and a private key. The "private key" is a random number randomly generated by the computer, including about fifty numbers and sizes. There is no fixed logic or rules for writing letters. The private key and the public key are generated in pairs by calculation and are unique and will not be repeated.

WALLET ADDRESS

The wallet address is calculated based on the asymmetric encryption "public key" through specific HASH calculation and encoding. Before using the Layer Minus network, users need to create a pair of "public/private keys" to distinguish their location on Layer Minus.

Wallet addresses are unlimited resources, created cryptographically by customers on demand, and there is no centralized distribution mechanism.

ENCRYPTED WITH PUBLIC KEY[31]

In a public key encryption system[32], anyone with a public key can encrypt a message and generate ciphertext, but only someone who knows the corresponding private key can decrypt the ciphertext to obtain the original message.

In a public key encryption system, anyone with a public key can encrypt a message

and generate ciphertext, but only someone who knows the corresponding private key can decrypt the ciphertext to obtain the original message.

DIGITAL SIGNATURE[33]

The sender can use the private key and the message to create a signature. Anyone with the corresponding public key can verify whether the signature matches the message, but a forger who does not know the private key cannot pretend to be the owner of the private key to sign the message. The signature is non-repudiation and plays a key role in Layer Minus P2P protocol.

LEAKAGE OF CIPHERTEXT SIDE CHANNEL INFORMATION

Anyone who obtains the ciphertext does not need to decrypt it, and can perform cryptographic calculations on the ciphertext to obtain the public key ID used to encrypt the ciphertext.

LAYER MINUS PACKET

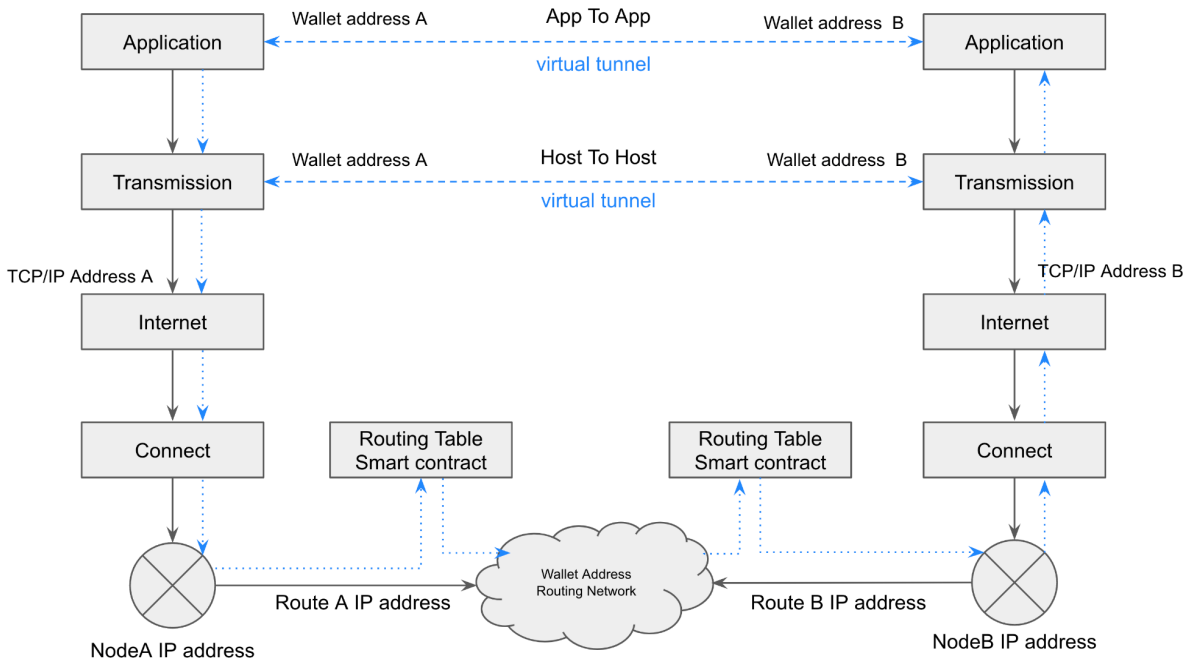
Layer Minus network data packets do not contain any metadata and are encrypted using the "public key" of the receiving party.


```
ZWN0MRcwFQYDVQQDDA5PcGVuUEdQLk9ubGluZTEiMCAGCSqGSIb3DQEJARYTaW5m
b0BPcGVuUEdQLk9ubGluZTCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIB
AOKXfU16GB1VOoEbUU60G0RpsScrM90lmzviioKXkpfnzOZK+fJO7dPjrNceC01A
CzmD/de5DzwqHKg5mAZ1oYjMThWAHKGyc8LjPTpH46OXvMd0VUjNRMCr9MwOv0wC
AjgBuIJZdEuIx3TiBf4LVXol2KVS4OaGBMn2peyhKt5rmmBYvENsLVGDYwx9D6g3
DIXpjuS5mffi1bjtoloQoeSPeSPmypedgVad24yH8Ps9HuHciAaCQmTPz0e/3IZm
SQCYk+TY+alKZgmo6wqEykcxDWFcydb+wM7CxadQJjulde4/AmjMQK2gz4xMSsNp
bTvkyNzlLvzULIX4UcZrHBl4XAL34t5nGzs+KZpG8uBi7H9bM79LpzVt0oLzBpEY
pQ1OUoQxVX1FU/2tRzp3axGchTetDo+gt8J9PU5Q/23jd/Rfa9HE3Y369KApvq7X
dLCNqRT4aslbagXJAOJQuPofrUJEAi79XqhtWeYN0aJKvpOu0pxh/w40FkKA9t4J
tIqimSJOKQwcGtT6FbcMployljiToltUMSIUnX3wp1fuiF7wBf1OWFF11cJvtSd3
8TDfXZbLXpbtmgEzj651YJj63Glks1w1z9M4YMad7Z3nMiH9LSj0Y4ZUplApuYzP
```


LAYER MINUS NODES

Layer Minus nodes are the key facilities that make up the Layer Minus wallet routing network. They perform the following tasks:

- **Relay node**: When a node obtains encrypted data that is not its own agent, node will forward it to the right node that is the agent for the delivery address. Obtain the corresponding traffic fee from the delivery node.
- **Agent receiving node**: Accept the customer's entrustment to receive the encrypted message of the customer's wallet address, and forward the encrypted message to the customer when the entrusted customer is online. Collect usage fees from customers in advance, pay for the data forwarding bandwidth fees forwarded by other nodes on behalf of customers, and deduct them from the prepayment.
- **Data caching in agent receiving node:** The inbound message was storage when the entrusted client is offline.All cached data will be sent to client when the client comes online, and the corresponding storage fee is calculated and deducted from the advance payment.
- **SSE in agent receiving node:** When the client connects to the agent receiving node of its own wallet through the network access node through the HTML protocol, the agent receiving node encrypted the incoming data with customer-specified temporary password, then pushes it to the client through W3C SSE[34] (Server-Sent Events) protocol. Pay the traffic fee to the relay node, charge traffic fee and relay traffic fee from the prepayment.



ROUTING

Routing is the process of selecting a path for traffic in a network or between or across multiple networks. In the Layer Minus network, each relay node represents one or a group of proxy wallet addresses. They are registered in the smart contract and are accessible to everyone. Therefore, the path discovery (routing) of Layer Minus is direct and Efficient.

TRAFFIC OBFUSCATION TECHNOLOGY

Layer Minus is a virtual network established using the W3C HTTP protocol at the application layer of OSI. The Layer Minus communication itself has no characteristics, which is a characteristic of the Layer Minus network.

LAYER MINUS NETWORK FEATURES

Today, the Internet is forced to enter Web3 because the Big-Tech that made a lot of money in Web2 no longer puts the interests of users first as their principle. They share customer privacy, deliver ads accurately, review and delete creative content stored by users, and end users' social lives at will.

The concept of online privacy protection has been discussed and implemented for more than 20 years, but not only has it not been improved, but with the development of big data, AI and censorship technology, it is facing even greater setbacks.

If Web3 relies too much on the critical infrastructure of Internet infrastructure, I'm afraid that Web3 will only be an empty slogan.

Rebuilding all Internet hardware and software infrastructure from scratch is

simply not possible. How to make limited use of infrastructure to meet the vision of Web3 to the greatest extent, CONET serves as a starting point for attracting new ideas.

A OPEN AND TRUSTLESS NETWORK PLATFORM

The Layer Minus assumes that all participants have the motivation to peek at the communication content and is designed under the premise of collusion. Combined with W3C Wasm[35] (WebAssembly) memory-safe sandbox execution environment, it provides an open zero-trust decentralized cloud computing platform.

LAYER MINUS NETWORK IS THE "SERVER" AND ALL USERS ARE CLIENTS

Layer Minus users, whether they are clients or servers, are all clients relative to the Layer Minus network. The client sends a request, and the Layer Minus network responds to the client's request. This structure gives Layer Minus users (including clients and servers) the greatest initiative and flexibility.

NATURALLY ANONYMOUS WALLET ADDRESS

Through cryptography, the wallet address is freely generated by the customer, allowing users to discard the de-anonymized wallet address at any time as needed. Also the wallet addresses are unlimited resources and no longer rely on a centralized issuing institution.

NATURALLY ANONYMOUS SERVER

Seamlessly connects to the traditional client-server (CS) model of the Internet. The server accepts data packets sent from the client through the wallet address, which can perfectly maintain anonymity. With the decentralized domain name interpretation system, it supports the transfer of readable domain names to wallet addresses.

CLIENT-SERVER MODE WITHOUT LOGIN

The client sends a digital signed request to the server. When the server receives the request, the cryptographic signature is undeniable and the sender ID can be determined. It is possible to build an authentication system via wallet address.

SENDER ADDRESS HIDDEN

The Layer Minus network uses encrypted data messages without metadata. The sender's address, one of the three major elements of communication, can only be obtained by the recipient who holds the key by decrypting the ciphertext. During the forwarding process, nodes do not need to perform encryption or decryption operations.

DECENTRALIZED ROUTING TABLE

The wallet address destination, through smart contracts, avoids the inefficient routing broadcast mechanism.

DATA CACHING MECHANISM IN P2P NETWORK

Clients can entrust Agent receiving nodes to store income data, which solves the pain point of data loss in point-to-point networks.

PROGRAMMABLE DECENTRALIZED CLOUD COMPUTING NETWORK

The node SaaS charging model mechanism can continuously provide novel functions through expanded plug-ins. The Web2 Bridge Service developed by Layer Minus network is a typical Layer Minus network SaaS case.

LAYER MINUS NETWORK RESOURCES ARE A DECENTRALIZED STABLE CURRENCY COLLATERALIZED

With the increase in Layer Minus participants, the settlement token has become a kind of service commitment IOU. Its actual value closely follows the cloud computing market price and has the attribute of relatively stable price.

All nodes of Layer Minus on IOUs to unconditionally fulfill the services promised by IOUs. Layer Minus's overall network bandwidth, computing resources and storage capacity form a powerful pledge for decentralized stable coins.

Avoiding the self-collateralized, death spiral of decentralized algorithmic stablecoins[36]. Layer Minus decentralized stablecoin is a huge contribution to the decentralization process of the encryption industry.

References

[1] Global Commission on the Stability of Cyberspace. November 20, 2017. p. 61.

[2] OECD (2014-11-06). "The Economics of Transition to Internet Protocol version 6 (IPv6)". OECD Digital Economy Papers.

[3] RFC 1034, Domain Names - Concepts and Facilities.
RFC 1035, Domain Names - Implementation and Specification.
RFC 1123, Requirements for Internet Hosts—Application and Support.

[4] "An Oregon Mill Town Learns to Love Facebook and Apple". The New York Times. March 6, 2018.

[5] Spinellis, Diomidis (2007). Beautiful Code: Leading Programmers Explain How They Think. Sebastopol, CA: O'Reilly and Associates. pp. 279–291.

[6] Mackenzie, Charles E. (1980). Coded Character Sets, History and Development. p. x. ISBN 978-0-201-14460-4. LCCN 77-90165. Archived from the original on 2016-11-18. Retrieved 2016-05-22.

[7] Agrawal, Manish (2010). Business Data Communications. John Wiley & Sons, Inc. p. 37. ISBN 978-0470483367.

[8] "Distributed Programs". Texts in Computer Science. London: Springer London. 2010. pp. 373–406.

[9] Tanenbaum, Andrew S.; Steen, Maarten van (2002). Distributed systems: principles and paradigms. Upper Saddle River, NJ: Pearson Prentice Hall. ISBN 0-13-088893-1. Archived from the original on 2020-08-12. Retrieved 2020-08-28.

[10] US 7529565, Hilpisch, Robert E.; Duchscher, Rob & Seel, Mark et al., "Wireless communication protocol", published 2009-05-05, assigned to Starkey Laboratories Inc. and Oticon AS.

[11] Sterling, Christopher H., ed. (2008). Military Communications: From Ancient Times to the 21st Century. ABC-Clio. p. 399. ISBN 978-1-85109-737-1.

[12] "TSB Director's Corner". ITU. Archived from the original on 2015-04-27.

[13] "How to use the ISO Catalog". ISO.org. Archived from the original on 4 October 2007.

[14] DOD Standard Internet Protocol. DARPA, Information Sciences Institute. January 1980. doi:10.17487/RFC0760. RFC 760.

[15] IETF standards documents.
RFC 2131, Dynamic Host Configuration Protocol.
RFC 2132, DHCP Options and BOOTP Vendor Extensions.
RFC 3046, DHCP Relay Agent Information Option.

[16] Deering; R. Hinden (December 1998), Internet Protocol, Version 6 (IPv6) Specification, Internet Engineering Task Force (IETF), RFC 2460 Obsoletes RFC 1883.

[17] "Internet Engineering Task Force" Archived December 28, 2014, at the Wayback Machine, Scott Bradner, Open Sources: Voices from the Open Source Revolution, O'Reilly, 1st Edition, January

1999, ISBN 1-56592-582-3. Retrieved 21 July 2014.

[18] "Internet Assigned Numbers Authority". Public Technical Identifiers. Archived from the original on 24 February 2011. Retrieved 17 December 2011.

[19] PYMNTS (2018-01-03). "Businesses Can't Just KYC, They Must Also KYCC". PYMNTS.com. Retrieved 2019-04-24.

[20] "What is an Internet Service Provider?". WhatIsMyIPAddress.com. Archived from the original on 2020-06-05. Retrieved 2020-05-30.

[21] Goścień, Róża; Walkowiak, Krzysztof; Klinkowski, Mirosław (2015-03-14). "Tabu search algorithm for routing, modulation and spectrum allocation in an elastic optical network with anycast and unicast traffic". Computer Networks. 79: 148–165. doi:10.1016/j.comnet.2014.12.004. ISSN 1389-1286.

[22] "Router". Oxford English Dictionary (Online ed.). Oxford University Press. (Subscription or participating institution membership required.) Medhi, Deepankar; Ramasamy, Karthik (2007). Network Routing: Algorithms, Protocols, and Architectures. Elsevier. p. 19. ISBN 9780120885886.

[23] Stallings, William (2001). "Glossary". Business Data Communication (4 ed.). Upper Saddle River, New Jersey, USA: Prentice-Hall, Inc. p. 632. ISBN 0-13-088263-1. Packet: A group of bits that includes data plus control information. Generally refers to a network layer (OSI layer 3) protocol data unit.

[24] Securing the Web W3C TAG Finding 22 January 2015 (http://www.w3.org/2001/tag/doc/web-https)

[25] "What is an Internet Service Provider?". WhatIsMyIPAddress.com. Archived from the original on 2020-06-05. Retrieved 2020-05-30.

[26] Clayton, Richard; Murdoch, Steven J.; Watson, Robert N. M. "Ignoring the great firewall of china". International Workshop on Privacy Enhancing Technologies.
Mozur, Paul (13 September 2015). "Baidu and CloudFlare Boost Users Over China's Great Firewall". The New York Times. Archived from the original on 24 January 2019. Retrieved 16 September 2017.
Clayton, Richard; Murdoch, Steven J.; Watson, Robert N. M. (2006). Danezis, George; Golle, Philippe (eds.). "Ignoring the Great Firewall of China". Privacy Enhancing Technologies. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer. 4258: 20–35.

[27] Dingledine, Roger (20 September 2002). "Pre-alpha: run an onion proxy now!". or-dev@freehaven.net (Mailing list). Archived from the original on 26 July 2011. Retrieved 17 July 2008.
Goulet, David (9 November 2023). "Stable release 0.4.8.9". Tor Project Forum. Retrieved 22 November 2023.
"Tor". Open HUB. Archived from the original on 3 September 2014. Retrieved 27 May 2021.

[28] dVPN vs VPN — What's The Difference? https://clearvpn.com/blog/dvpn-vs-vpn/

[29] Mixnet. https://nymtech.net/about/mixnet

[30] Nym Nodes
https://nymtech.net/build/nodes?name=service_providers

[31] Kessler, Gary (November 17, 2006). "An Overview of Cryptography". Princeton University.

[32] Handbook of Applied Cryptography 1997 by CRC Press, Inc
https://cacr.uwaterloo.ca/hac/about/chap8.pdf

[33] Bellare, Mihir; Goldwasser, Shafi (July 2008). "Chapter 10: Digital signatures". Lecture Notes on Cryptography (PDF). p. 168. Archived (PDF) from the original on 2022-04-20. Retrieved 2023-06-11.

[34] "HTML Living Standard: 9.2 Server-sent events". WHATWG. 31 March 2022.
https://html.spec.whatwg.org/multipage/server-sent-events.html

[35] "WebAssembly/design/Semantics.md". GitHub. Retrieved 23 February 2021.

WebAssembly code can be considered a structured stack machine; a machine where most computations use a stack of values, but control flow is expressed in structured constructs such as blocks, ifs, and loops. In practice, implementations need not maintain an actual value stack, nor actual data structures for control; they need only behave as if they did so.
Mozilla. "Understanding WebAssembly text format". MDN Web Docs. Retrieved 9 December 2019.

[36] “The ‘Death Spiral’ of a Stablecoin” WEDNESDAY, MAY 18, 2022 by WSJ’s Caitlin Ostroff
https://www.wsj.com/podcasts/the-journal/the-death-spiral-of-a-stablecoin/6c09080e-ee6e-4dd9-9a1d-78eb20034679