

COMPARISON BETWEEN TCP/IP AND LNP/BP

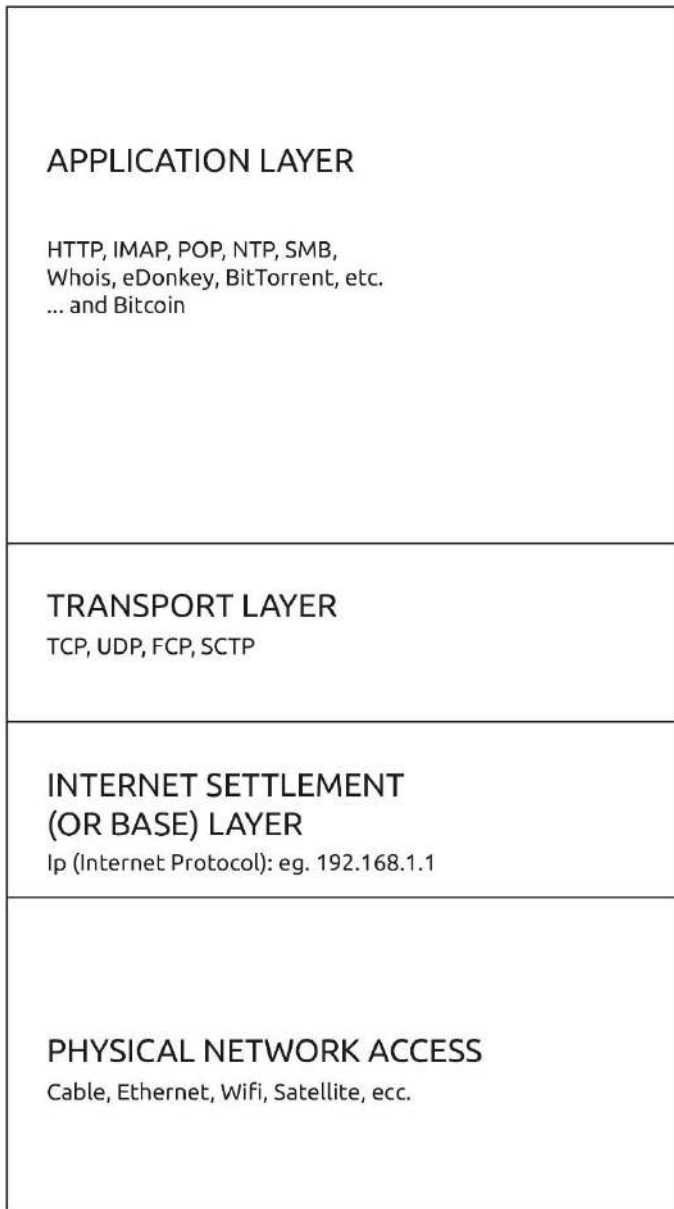
Before arriving at the definition of **LNP/BP** as a suite of protocols for the exchange of value among peers, let's see how the technology that instead allows us to exchange information (data) is composed and that is generically defined Internet.

The Internet is often displayed as a layered structure: it is customary to define this **TCP/IP** suite or stack.

The Internet Protocol suite was designed by Vinton G. Cerf and Robert E. Kahn [33] while working on a communication systems development project funded by the Defense Advanced Research Project Agency (DARPA).

The aim was to create a universal standard consisting of a series of communication protocols useful for the development of packet-switched networks. The TCP/IP suite was born, still used today.

Let's analyze it briefly.



PHYSICAL NETWORK ACCESS represents the set of physical connections (transmission media) between the nodes of the network, on which the sequences of bits physically travel, converted into electrical signals.

The physical layer provides an electrical, mechanical and procedural interface to the transmission medium. [37]

INTERNET SETTLEMENT (OR BASE) LAYER establishes the logical connections between the nodes of the network. The Internet Protocol identifies the nodes via IP addresses (eg 192.168.1.1) and sends data packets from the source to the recipient. The Internet level can be defined as agnostic, as it routes the packets through different physical structures (ethernet, coaxial cable, wifi, etc.) and makes no distinction with respect to the levels above it, directing and routing data for different transport and application protocols.

TRANSPORT LAYER establishes the data channels used by the applications. The transport protocol can deal with error control, packet segmentation, flow control with packet sorting, congestion control and application addressing via the port number. The most widely used transport protocol is TCP, connection-oriented (Byte flow). Thanks to the TCP protocol:

- data arrives in order
- data has a minimal error
- duplicate data is deleted
- packets lost or discarded are sent back

includes traffic congestion control. [38]

TCP does not receive information about IP addresses. TCP's task is to get application-level data from one application to another reliably. The Internet Protocol has the task of obtaining data from one computer to another. [39]

APPLICATION LAYER groups all the applications that use the protocols contained in the TCP/IP suite in addition to the protocols used by the same applications, which define the operation and the possible connection with other applications.

Examples of application-level protocols include Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Post Office Protocol (POP), Simple Mail Transfer Protocol (SMTP), but also BitTorrent (BT) and Bitcoin (BP).

We can now analyze how Bitcoin has evolved from an Application Layer software based on a P2P client/server sharing protocol to form itself a real Settlement Layer that presents characteristics of decentralization and "agnosticism" similar to those of the Internet Protocol.

We can have Bitcoin in a stack (or layer) structure similar to that of the TCP/IP suite, leaving out for the moment the PHYSICAL NETWORK ACCESS LAYER.



BITCOIN SETTLEMENT (OR BASE) LAYER establishes the logical connections between the nodes of the network as well as the basic rules of the network and monetary policy. The Bitcoin Protocol identifies the nodes through public addresses (eg 36R4qFsySb73YnRWcAUj3vjfsR5Z34mgPj)

calculated by cryptographic hash functions starting from public keys, in turn calculated by means of an elliptic curve multiplication (ECDSA), and preserves the transactions occurring between source and recipient through a chain of transaction blocks that adopts the UTXO model.

The Bitcoin Layer can be defined as agnostic, as it routes transactions through different software implementations and makes no distinction with respect to the levels above it, directing and routing transactions for different transport and application protocols.

TRANSPORT LAYER establishes the payment channels used by the applications. The Lightning Network transport protocol deals, among other things, with the creation of bidirectional peer payment channels, creation of Hashed Timelock Contracts, Decrementing Timelocks, Payment Routing and maintenance of Channel States. [40]

APPLICATION LAYER includes all the applications that use the protocols contained in the LNP/BP suite in addition to the protocols used by the same applications, which define the operation and the possible connection with other applications.

Examples of application-level protocols include RGB, Discreet Log Contracts [41] and Storm. [42]

To sum up, **just as our data packets travel on second layers of the IP protocol, above all the TCP protocol, we can use second layers for the "transport" of our value:** LNP (Lightning Network Protocol) and others.

Viewing Bitcoin as a structured network in the form of a LNP/BP suite is useful for understanding the features of the various protocols and above all for developing solutions “on top of Bitcoin (Protocol)” without the need to constantly redefine the basic protocols or create new ones for exchanges of value without reliable third party.

It follows the uselessness of creating new blockchains in competition with Bitcoin Protocol unless we only want to redefine economic policy.

In this case, good luck and Consensus decides.

If we do not constantly redefine the basic protocols, since we already have decentralization and the (tendency to) immutability we need, and we focus on creating different applications and transaction layers, we can even realize the Austrian libertarian dream: to have private coins to be used in the free market, usable as cash, without a reliable third party. They are the so-called tokens, usable on top of the Base Layer, therefore not using the blockchain, as instead happens for example with Ethereum.

Not only coins: we can have simple coupons (utility tokens) but also security (with automatic management of dividends) without touching the Base Layer, relying exclusively on Application Layer solutions.