

Deposit to earn rewards

Sign up and deposit to receive up to **10,055 USDT** in bonuses.
Exclusive for new users only.

Get it now

[PDF Database Document] - BTCC Cryptocurrency Exchange

Original:

<https://www.btcc.com/en-US/academy/crypto-basics/what-is-a-blockchain-protocol-and-what-is-a-blockchain-platform>

What is a blockchain protocol and what is a blockchain platform?

The blockchain protocol is a protocol similar to DNS, HTTP, or TCP/IP, but its role is to standardize the blockchain-related processes, which is equivalent to a standard. The blockchain platform is a trading platform, which usually represents a public website of the blockchain company or a trading platform.

What is a protocol?

As all of us already know, a protocol, in computer science, is a set of rules or procedures that govern the transfer of data between two or more electronic devices. This protocol helps in establishing how, in order for computers to exchange information, the information must be structured and how each party will send and receive it.

Some examples of familiar internet protocols are TCP/IP, HTTPS, and DNS.

Protocol in Blockchain

A blockchain is a network of multiple devices (nodes) — all equally important — connected to each other through the internet. Essentially, a blockchain is a ledger which stores the record of what has come in and gone out in a distributed p2p manner after the transaction has been verified by all participating nodes.

This distributed ledger works on pre-defined rules which are agreed upon by all the participating nodes (the peers) in the network. These rules include:

1. a how-to for governing and validating transactions,
2. an algorithm that defines the mechanism for all participating nodes to interact with each other, and,
3. (in some cases), application programming interface.

These rules that govern a blockchain network are referred to as a protocol. It is essentially the common communication rules that the network plays by.

Must-know terms for blockchain protocol

Distributed Ledgers: Distributed ledgers are a type of database that are spread across the multiple peers and the records are stored one after the other in a continuous ledger.

Smart Contracts: a set of logic rules in the form of a coded script which can be embedded into the blockchain to govern a transaction.

Consensus algorithm: an algorithm that defines the way consensus will be reached on the network to verify the transactions.

Coins and Tokens: Every blockchain protocol needs a digital asset to keep the network running. These are also used as incentives for the peers who participate in the network. This entails the presence of digital assets such as coins and tokens. The two terms are often used interchangeably in the realm of blockchain but there is a subtle difference between the two.

Essentially, coins and tokens are the digital assets used to power a blockchain network. Their functions are, more or less, same too. It is only the level in the protocol where they are defined that differentiates them.

Coins are defined at the lowest level by the protocol itself. Coins are the *native* digital asset of a blockchain network. For instance, bitcoin protocol's native currency is Bitcoin.

Tokens are the digital assets that are defined at a higher level not by the protocol but by smart contracts. For instance, the Ethereum protocol has a native coin Ether. Ethereum allows developers to build, among other things, dApps on its protocol. The node-communication rules for one dApp can be different from another dApp which are defined by smart contracts. Tokens are, therefore, the native digital asset of dApps.

51% Attack: the ability of someone controlling more than 50% of network nodes to revise transaction history and indulge in double spending.

Example: *The nodes on a blockchain network are supposed to broadcast the blocks they form to the entire network. If a node, or a group of nodes, begin to control more than 50% of the network, it can indulge in forming blocks privately and not broadcast those to the network. The network would still follow the public version of the blockchain and the node can indulge in double-spending by first spending their money on the public blockchain and then on the private one.*

After that, since they control 51% of the network, they can broadcast their private version of the blockchain and form longer chains. Because of the longest chain rule (which regards the longest chain to be the most legitimate chain to mine on), the other participants will consider this to be the correct chain. The previous transactions that were not included in this chain (because it was private) will be reversed giving the malicious nodes access to other people's money.

Examples of Blockchain Protocols

The world got introduced to the blockchain with the Bitcoin network. Following different objectives and use cases that were envisioned, different protocols were designed. We will look at the key features of three major blockchain protocols.

Bitcoin Protocol

Design objective: allowing crypto payment transactions over a decentralised network.

- Public, permissionless blockchain which anyone can join.
- Underlying technology components: cryptographic hash function, digital signature, p2p network, private-and-public key encryption, and proof-of-work (PoW) consensus algorithm.
- Every node has access to complete information on the blockchain. Therefore, Decentralised.
- Users can conduct non-reversible transactions without the need to explicitly trust a third-party.
- Native cryptocurrency *Bitcoin*

Ethereum Protocol

Design Objective: a blockchain platform for developers to launch their own blockchain projects and decentralised applications.

- Public, permissionless blockchain
- Underlying technology components: cryptographic hash function, digital signature, p2p network, private-and-public key encryption,
- and proof-of-work consensus algorithm.
- Every node has access to complete information on the blockchain. Therefore, Decentralised.
- Users can conduct non-reversible transactions without the need to explicitly trust a third-party.
- Native cryptocurrency *Ether*.

The Ethereum blockchain gave a larger, wider horizon to the objectives that blockchain could serve. Multiple cryptocurrency projects such as VeChain and OmiseGo were launched using the Ethereum platform. It also became a platform for dApp development and dApps such as Cryptokitties, Brave, and PundiX were developed on it.

Following this innovation, multiple protocols were launched with one or the other innovation. For instance, the every-node-verification feature of the blockchain rendered it slow thus leading to scalability issues. Zilliqa, EOS, and Cardano are some examples of blockchains that attempted to build solutions for scalability issues.

Another innovation in blockchain protocol was different models of consensus algorithms. With Bitcoin, the PoW algorithm was introduced. But later developments gave birth to algorithms such as proof-of-stake(PoS), delegated proof-of-stake (dPoS) etc.

Hyperledger is a blockchain that tried to solve the problem of enterprise adoption of blockchain via a permissioned protocol wherein only trusted entities could join the network and verify the transactions.

Blockchains are essentially ledgers and record transactions. A transaction with respect to blockchain refers to an exchange of assets manages under the rules (smart contracts) of the blockchain.

Consensus and Trustlessness

All peers on a blockchain network reach a consensus to verify transactions. This consensus is governed by an algorithm fed into the protocol layer of the blockchain. The blockchain gives all

peers an identical copy of each transaction which eliminates trust thus making a trustless, distributed network.

The essential features of a blockchain protocol can then be summarized as:

- Decentralised: a blockchain must be stored in a way that it can be accessed and copied and any node on the network.
- Immutable: blockchain records all transactions permanently. Once a record is added, it cannot be changed.
- Consensus Driven: transactions on blockchain are verified only after all the participating nodes have reached a consensus.