**Blockchain**

* Blockchain is a type of shared database that differs from a typical database in the way that it stores information; blockchains store data in blocks that are then linked together via cryptography.
* As new data comes in, it is entered into a fresh block. Once the block is filled with data, it is chained onto the previous block, which makes the data chained together in chronological order.
* Different types of information can be stored on a blockchain, but the most common use so far has been as a ledger for transactions.
* In Bitcoin’s case, blockchain is used in a decentralized way so that no single person or group has control—rather, all users collectively retain control.
* Decentralized blockchains are immutable, which means that the data entered is irreversible. For Bitcoin, this means that transactions are permanently recorded and viewable to anyone.

**Distributed systems**

A distributed system is a computing environment in which various components are spread across multiple computers (or other computing devices) on a [network](https://www.splunk.com/en_us/data-insider/network-operations-center.html). These devices split up the work, coordinating their efforts to complete the job more efficiently than if a single device had been responsible for the task

Distributed systems are an important development for IT and computer science as an increasing number of related jobs are so massive and complex that it would be impossible for a single computer to handle them alone. But distributed computing offers additional advantages over traditional computing environments. Distributed systems reduce the risks involved with having a single point of failure, bolstering reliability and fault tolerance. Modern distributed systems are generally designed to be scalable in near real-time; also, you can spin up additional computing resources on the fly, increasing performance and further reducing time to completion.

**History of blockchain and bitcoin**

The blockchain technology was described in **1991** by the research scientist **Stuart Haber** and **W. Scott Stornetta**. They wanted to introduce a computationally practical solution for time-stamping digital documents so that they could not be backdated or tampered. They develop a system using the concept of **cryptographically** secured chain of blocks to store the time-stamped documents

**Satoshi Nakamoto** introduced the bitcoin in the year 2008. Bitcoin is a cryptocurrency(virtual currency), or a **digital currency** that uses rules of cryptography for regulation and generation of units of currency. A Bitcoin fell under the scope of [cryptocurrency](https://www.javatpoint.com/blockchain-cryptocurrency) and became the first and most valuable among them. It is commonly called **decentralized digital currency**.

A bitcoin is a type of digital assets which can be bought, sold, and transfer between the two parties securely over the internet. Bitcoin can be used to store values much like fine gold, silver, and some other type of investments. We can also use bitcoin to buy products and services as well as make payments and exchange values electronically.

**Consensus**

Blockchain is a distributed decentralized network that provides immutability, privacy, security, and transparency. There is no central authority present to validate and verify the transactions, yet every transaction in the Blockchain is considered to be completely **secured** and **verified**. This is possible only because of the presence of the **consensus protocol** which is a core part of any Blockchain network. A consensus algorithm is a procedure through which all the peers of the Blockchain network reach a **common agreement** about the present state of the distributed ledger. In this way, consensus algorithms achieve reliability in the Blockchain network and establish trust between unknown peers in a distributed computing environment. Essentially, the consensus protocol makes sure that every new block that is added to the Blockchain is the one and only version of the truth that is agreed upon by all the nodes in the Blockchain. The Blockchain consensus protocol consists of some specific objectives such as coming to an agreement, collaboration, co-operation, equal rights to every node, and mandatory participation of each node in the consensus process. Thus, a consensus algorithm aims at finding a common agreement that is a win for the entire network. Now, we will discuss various consensus algorithms and how they work.

1. **Proof of Work (PoW):** This consensus algorithm is used to select a miner for the next block generation. Bitcoin uses this PoW consensus algorithm. The central idea behind this algorithm is to solve a complex mathematical puzzle and easily give out a solution. This mathematical puzzle requires a lot of computational power and thus, the node who solves the puzzle as soon as possible gets to mine the next block. For more details on PoW, please read [Proof of Work (PoW) Consensus](https://www.geeksforgeeks.org/proof-of-work-pow-consensus/)
2. **Proof of Stake (PoS):** This is the most common alternative to PoW. Ethereum has shifted from PoW to PoS consensus. In this type of consensus algorithm, instead of investing in expensive hardware to solve a complex puzzle, validators invest in the coins of the system by locking up some of their coins as stake. After that, all the validators will start validating the blocks. Validators will validate blocks by placing a bet on it if they discover a block which they think can be added to the chain. Based on the actual blocks added in the Blockchain, all the validators get a reward proportionate to their bets and their stake increase accordingly. In the end, a validator is chosen to generate a new block based on their economic stake in the network. Thus, PoS encourages validators through an incentive mechanism to reach to an agreement.

**Transactions in blockchain**

[Blockchain](https://www.geeksforgeeks.org/blockchain-technology-introduction/) technology is mostly about the transactions that we make digitally for ourselves. Eventually, these transactions make their way to the various blocks that become part of the Blockchain later on. So, it is important to understand the **transaction life cycle in Blockchain technology**.

This lifecycle follows the journey of a single transaction as it makes its way through each stage in the process of joining the blockchain. Transaction in simple words is the process of sending money by the sender and the receiver receiving it. The Blockchain transaction is also quite similar, but it is made digitally.

**Blockchain mining**

**What is mining ?**

Mining is the process that Bitcoin and several other cryptocurrencies use to generate new coins and verify new transactions. It involves vast, decentralized networks of computers around the world that verify and secure blockchains – the virtual ledgers that document cryptocurrency transactions. In return for contributing their processing power, computers on the network are rewarded with new coins. It’s a virtuous circle: the miners maintain and secure the blockchain, the blockchain awards the coins, the coins provide an incentive for the miners to maintain the blockchain.

**Bitcoin network**

The bitcoin network is **a peer-to-peer payment network that operates on a cryptographic protocol**. Users send and receive bitcoins, the units of currency, by broadcasting digitally signed messages to the network using bitcoin cryptocurrency wallet software

**Wallets**

Crypto wallets keep your private keys – the passwords that give you access to your cryptocurrencies – safe and accessible, allowing you to send and receive cryptocurrencies like Bitcoin and Ethereum. They come in many forms, from hardware wallets like Ledger (which looks like a USB stick) to mobile apps like [Coinbase Wallet](https://wallet.coinbase.com/), which makes using crypto as easy as shopping with a credit card online.

**Cryptocurrency payments**

Payment gateways are companies taking on the perceived risk of cryptocurrency payments by using their wallet(s) to facilitate transactions between merchants and their customers.

Payment Flow

In terms of steps, the following workflow gets executed:

1. Your customer opts to make payment in cryptocurrency at checkout (in-store, on the web, or in-app).
2. They pay you an amount equal to the digital currency's fair market value at the time of the transaction.
3. The cryptocurrency payment service instantly converts the payment into the currency you choose.
4. The money is added to your account with the provider; it is deposited to your designated bank account in intervals decided on in your service contract.