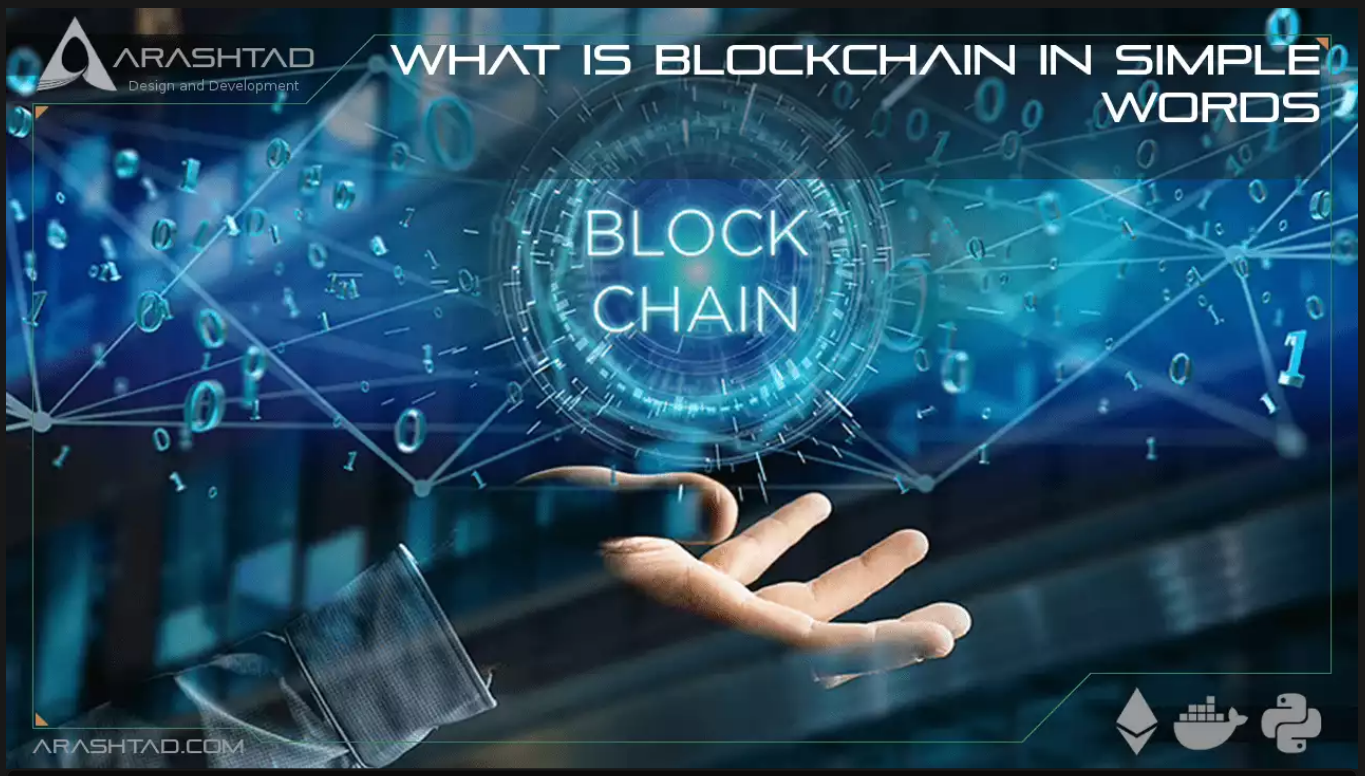
What is blockchain in simple words

No comments



Contrary to the popular fallacy, the Blockchain is not a new concept that has become the hot passion of the day in the form of cryptocurrency. The very first time blockchain was used, dates back to 1982 when a cryptographer (David Chaum), first proposed a blockchain-like protocol in his dissertation "Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups". More works on blockchain were described in 1991 by Stuart Haber and W. Scott Stornetta. However, none of these efforts were related to monetary or financial systems, rather, they were the kinds of efforts that would not allow the document timestamps to be manipulated or damaged by a third party and this was made possible by the means of Blockchain protocols. In 2008, for the first time, an anonymous group or a person called Satoshi Nakamoto proposed a hash-cash-like method to timestamp blocks without requiring a third party to sign them and introduced a new parameter called difficulty which is the rate at which the blocks are added to the chain and is good for the stability of the system. If you haven't understood many of the terms and expressions up to now, don't worry

cause in this article, we will explain everything from scratch.

Explaining blockchain to a 6-year-old kid:

You might read the above title and smile or think that we are writing this article for dummies or some kindergarten kid who wants to learn about the Blockchain while he or she doesn't even know the basics of computer science. But in fact, if you google about the blockchain throughout the internet, you will face many hard and mind-bending expressions that you wonder for example what is the meaning of hash or block or chain in the first place?!
Even if you read the definition, you will still have difficulty linking all the dots together.

In this first part we are going to explain Blockchain with a simple and real-world example so that the main concept and the expressions totally sink in for you.
Suppose we want to store the receipts of all the transactions inside a shopping center. And (although it may sound stupid ,) we have hired some people to hold the boxes containing the receipt papers. Once a box overflows, a new person is hired with a new box who will hold the rest of the receipts until this box also gets overflown and the same story goes on for other boxes and people who get hired along the way, as we go on in time. Also consider that all these people know only the person who had got hired just before them (the previous one) and they know all the information about the box of the previous person. In addition to that, each one of them has a number related to the sequence of getting hired.

If we want to translate this analogy into the Blockchain, the people and their boxes are the "blocks" containing the data of the transactions, the information about the previous box is encrypted into a format called "hash", and the number that each employee (box) gets according to the sequence of getting hired is called "nonce". In this system, no one from outside can cheat and enter the line of employees with boxes. Because each employee knows the previous one who got hired before them. So the recorded data is unalterable by a malicious third party and nobody can modify the receipts either intentionally or unintentionally. Also everyone from the outside can have access to the recorded data whenever they want if this publicizing authority is given by the shopping center (the Blockchain). You might wonder what the "chains" are. These are in fact the hashes that every block keeps about the previous one. Furthermore, the very first block has obviously no data of the previous block as there is no other block before the first one. This block is called the "Genesis Block".

What is blockchain?

In general, a Blockchain is a growing set of records that are called blocks. These blocks are securely linked together using cryptographic algorithms. Each block contains 4 key elements: Arashtad.com Design and development solutions arashtad 1. A cryptographic hash of the previous element: First of all, the hash is the output of a function that transforms the input data of any length into the string data of a fixed size. This kind of referring to the previous block by the current block, makes blocks be secured by the chains called hashes. And the primary block that all the blocks refer back to, is called the Genesis Block. Also notice that no one can change the state of any block because they are designed to be immutable and unalterable. And this hash of the previous element does this for the blockchain. 2. A

timestamp: The data relating to the time of the occurrences of every detail in a Blockchain that cannot be modified. 3. The transaction data: The data relating to the transactions including the sender and the receiver represented as the leaves of a Merkle tree which contains the transactions. 4. And finally a nonce: The number that each block gets, is usually in a sequence of creation.

Bitcoin Vs Blockchain:

Another question that newbies keep asking you is whether Blockchain is Bitcoin or not. The true answer is a bit different from the question which means that the answer is NO. In fact, Bitcoin is a kind of Blockchain but that doesn't mean that Blockchain is the same as Bitcoin. In other words, Blockchain is a wider concept than Bitcoin and it is a protocol for storing data in such a way that is not modifiable by anyone, even the creator of the Blockchain. In contrast, Bitcoin is one of the many Blockchains that uses this protocol to store the transactions and gives rewards to the ones who solve the mathematical problems related to encrypting data. But wait a minute! Why should mathematical problems be solved and data be encrypted? To answer this we will need to redefine the Blockchain, this time from the Bitcoin point of view: "Blockchain is a decentralized ledger of all transactions across a peer-to-peer network". In other words, in Bitcoin's Blockchain, there is no centralized authority or organization for monitoring and controlling the transactions. Rather there is a decentralized system in which we have 2 groups of people:
1. The ones who execute the peer-to-peer transactions. Like the normal people who send and receive Bitcoin. They pay gas fees for every transaction.
2. The miners or the ones who secure the network and process every transaction so that they can chain together the blocks of the transactions by solving the mathematical problems and get rewards in return for the computational power they consume and the problem they solve. The reward is retrieved from the gas fees that the Bitcoin senders pay for executing the transaction.
Blockchain decentralization emerged with the system that Satoshi Nakamoto proposed for signing the transactions without the need for a trusted centralized authority.

In this system the creation of the blocks was stabilized at a rate called "difficulty", The design of this kind of Blockchain helped the creation of the first cryptocurrency called "Bitcoin". The mentioned decentralized Blockchain served as the public ledger for all transactions on the network.

Blockchain, wallets, and exchanges:

The next thing that comes to mind after understanding the basics of Blockchain, is the mechanism of the wallets and exchanges. The very first and true question that challenges the so-called "Bitcoiners" is why should we even need an exchange when the transactions inside the Bitcoin Blockchain or other Blockchains are executed in a decentralized manner? The challenging part is that Bitcoin and other cryptocurrencies are not that widely adopted yet that you can for example buy a bottle of soda with the bitcoin you own from the nearest market of your residence.

The challenge itself answers the question. We still need the common currency of our region and that currency is not Bitcoin yet. This fact by itself leads us to the necessity of exchanges.
On the other hand, the blockchain wallets act more in a decentralized way considering that each of these computer,

web, or smart phone based applications create a full node in different Blockchains (such as that of Bitcoin) and directly connect to any one of them. This process makes them somewhat decentralized. However, some of these wallets have their Own IP tracking algorithms and imitate the governmental regulations to control the users and even in some cases retrieve their identity such as their location.

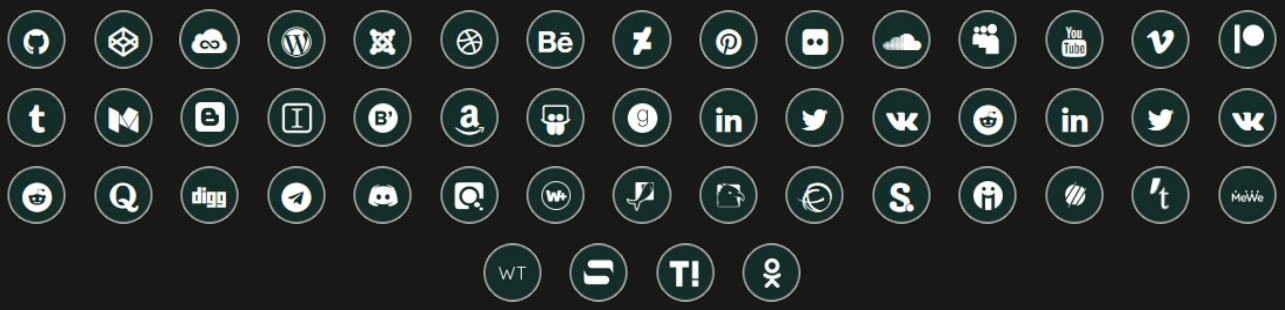
Wrapping up:

In this article, we briefly talked about the background of the Blockchain technology and then explained the Blockchain in simple words so that even a 6 the year-old kid can understand the concepts and expressions related to this technology. Afterward, we went deeper into the mechanism and the building blocks of all the Blockchains and after understanding the common features of them, we began exploring Bitcoin's Blockchain in particular. Then we introduced the necessity of exchanges in spite of the fact that the existence of the cryptocurrency exchanges contradicts the main purpose of their blockchain, which is decentralization. We also introduced the Blockchain wallets and explained their mechanism and why they cannot be considered as fully decentralized as they are told to be.

Join Arashtad Community

Follow Arashtad on Social Media

We provide variety of content, products, services, tools, tutorials, etc. Each social profile according to its features and purpose can cover only one or few parts of our updates. We can not upload our videos on SoundCloud or provide our eBooks on Youtube. So, for not missing any high quality original content that we provide on various social networks, make sure you follow us on as many social networks as you're active in. You can find out Arashtad's profiles on different social media services.



Get Even Closer!

Did you know that only one universal Arashtad account makes you able to log into all Arashtad network at once? Creating an Arashtad account is free. Why not to try it? Also, we have regular updates on our newsletter and feed entries. Use all these benefitial free features to get more involved with the community and enjoy the many products, services, tools, tutorials, etc. that we provide frequently.

SIGN UP | NEWSLETTER | RSS FEED