# BITCOIN: AN EMERGING TREND IN CRYPTOCURRENCY

[1]Devapriya E D, [2]Arjun M P
[1]Assistant Professor, [2]MCA Scholar
[1]Department of computer science
[2]School of Information Science and Technology
[1]Jamia Hamdard Kannur Campus, Kannur, India
[2]Kannur University, Kannur, India

---

**Abstract:** A crypto currency is a digital resource which act as a medium of exchange that uses cryptography to make its transactions secure. Cryptocurrencies are subset of digital currencies. In this economic world, different number of virtual currencies available over the internet. A new digital currency may create at any time. By market capitalization, Bitcoin is the largest blockchain network followed by many other cryptocurrencies like Ripple,Ethereum,Cardano and Litecoin.

Bitcoin, was created in 2009, first decentralised crypto currency, since then only the numerous other crypto currencies have been created. These are frequently called altcoins. Bitcoin and its products use distributed financial control as opposite to centralised electronic money/central banking systems. The distributed system uses the blockchain transaction using distributed ledger. Today cryptocurrencies have become a globally trending economic phenomenon known to most people, banks, governments and many companies are aware of the importance. Bitcoins were in the news recently after a massive global ransomware attack "WannaCry'' which hit systems in over 100 countries. To unlock the affected devices cybercriminals demanded a fee of about $300 in cryptocurrencies like bitcoin.

**Keywords:** Cryptocurrency, Bitcoin, Blockchain, Ledger, Miner

---

## I. INTRODUCTION

A cryptocurrency is a big menace to the existing currencies. The algorithms help to maintain the security of these systems and it is close to impossible to steal currency from these systems.

Bitcoin offers alternative to the conventional state banking system. Bitcoin is a cryptocurrency and worldwide monetary system. It is the first decentralized digital currency as the system works without a central bank or single administrator. Bitcoin network is a peer to peer network and transactions take place between users directly without an intermediary resource. These transactions are verified through the use of cryptography and recorded the information about the transaction in a public distributed ledger called a blockchain. Bitcoin was invented by an unidentified person or group of people under the tag 'Santoshi Nakamoto 'and released as open source software in 2009. Bitcoins are populated because of a process is known as mining. They can be exchanged for other currencies, products, and services. Cryptocurrencies not subjected to hacking and inflation in a decentralized system known as block chain.

There are many benefits of using a decentralized cryptocurrency.

**1. Highly Secure**
A decentralized cryptocurrency is immune to hacking or tampering. This is because cryptocurrency is not stored only in one location .it is existing on hundreds of thousands of servers across the world.

**2. Highly Transparent**
All cryptocurrencies are open source, as the source code is available for everyone to view.

**3. Too Fast and expensive**
The speed and cost of cryptocurrency transactions are the same in the world for everyone using the network.

The development of Bitcoin and Blockchain technology has been so quick. Bitcoin is a digital currency which was invented by an unknown programmer, or a group of programmers, under the name Satoshi Nakamoto. Bitcoin can be used as a normal currency, but it does not exist physically like dollar bills. These can be used as an online currency which can be used to buy things, similar to "digital cash" as bits on clients' computers. Bitcoin exists only in the cloud, like Paypal, Citrus or Paytm. In the web space, they are virtual, not physical, they are used like cash when transferred between people. The Bitcoin system is peer-to-peer network based and transactions take place between users directly, without an intermediary resource.

These transactions are verified and the transactions are recorded in a public distributed ledger called a Blockchain. Since the system works without a central server or single administrator, Bitcoin is called the first decentralized digital currency
Unlike normal currencies, Bitcoins cannot be created whenever the user demands. Only 21 Million Bitcoins can be created, of with 17 million have already been created. Bitcoin will get created only whenever a block containing valid transactions is added to the Blockchain. This is the only means for creating Bitcoins through numerous mathematical logic and encryption algorithms, no fake Bitcoins are created or circulated .The blockchain is the technology behind the bitcoin.

## II. Blockchain Technology

Blockchain technology and the cryptocurrencies have become a parallel platform for doing standard transactions and is replacing the issues with the existing systems. Some of the most commonly faced issues with the Banking system are:

**a. Transaction Fee is high**
Let's look at an example to understand this issue better:

Here, Anil is sending $100 to John but it must pass through a trusted third party like a Bank or financial service company before John can receive it. A transaction fee of 2% is deducted from this amount and John only receives $98 at the end of the transaction. This may not be a big amount, but imagine if it is $100,000 instead of $100, then the transaction fees also increases to $2,000 which is a big amount.

b. **Double Spending**
Double-spending is an error in digital cash system in which the same single digital token is spent twice or more.

**c. Transaction delay**
The existing monetary system requires a lot of time to be verified and completed causing huge delays.

d. **Net Frauds and Account Hacking**
Bank transactions due to fake currencies and digital frauds are one of the major concern in the existing system.

**e. Financial Crisis and Crashes**
In this, the financial asset suddenly loses a large part of their nominal values.Banks have become synonymous with crisis and crashes. This is happening when we are giving complete trust to third-party financial companies.
The blockchain is a system that overcame these problems and provided us with a decentralized monetary system.

## III. How Does Blockchain Solve These Issues?

Below are some of the methods through which the Blockchain technology tackles the above-mentioned issues:

a. **Decentralized Monetary System**
The Blockchain system follows a decentralized approach when compared to banks and other financial companies, where, everyone who is associated with the system becomes equally responsible for the ups and downs of the system. Using blockchain everyone who is involved with the system holds some power than in a single administrative system.

**b. Have Public Ledgers**
The Bitcoin blockchain has a distributed public ledger. It includes the details of transactions of everyone who is associated with the system. The ledger can be accessed by everyone who is part of the system. Once you are in the Blockchain network, then you can access the list of the transaction from the beginning. Only the transactional details are visible but the details of the people involved in the transactions remain completely anonymous.

**c. Verify Every Individual Transaction**
Each and every transaction in this system is crosschecked and a validation signal is sent after few minutes using several complex encryption and hashing algorithm, and also the double spending is eliminated.

**d. Transaction Fee is low**
Transactions fees are not applicable. But in certain cases Blockchain implement minimal transaction fees compared to the transaction fees implies by banks and other financial enterprise

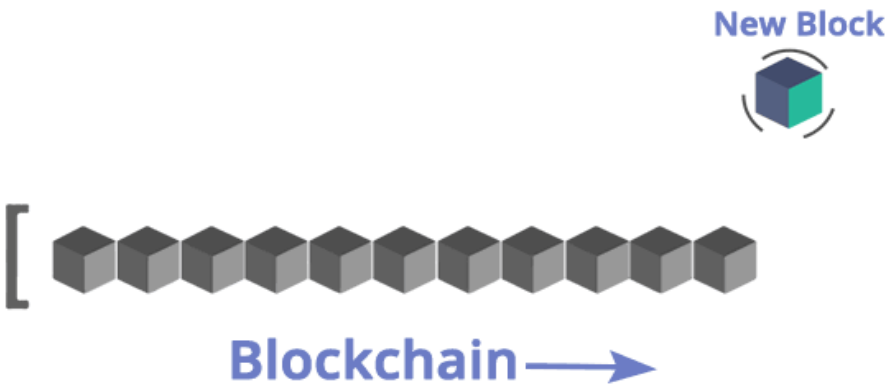


Figure 1: blockchain https://www.edureka.co/blockchain-training

The blockchain is the backbone of the entire cryptocurrency system. Blockchain performs transactions in the ledger but keeps security and anonymity of the users who are in the system.it contains a public distributed database holding encrypted distributed ledgers. A block stands for the present part of the block chain which records entire latest transaction and once finished goes into the blockchain as the stable database. Each time a block is get completed a new block is created.it is a continuously growing list of records.it is secured using cryptographic techniques. Because of the sharing behavior of the ledger brings transparency to the system and trustful. The blockchan is managed by a peer to peer network. The data in the block cannot be changed without alteration of all subsequent blocks. The transaction which are stored in the blockchain are permanent which cannot be hacked.

## IV. Features of Blockchain

Below are the most important features of Blockchain technology

### a. SHA256 Hash Function

The hashed algorithm used in blockchain technology is the SHA256.

Unlike encryption algorithm hash functions cannot be decrypted. It is highly secure as minute changes to input give completely different output. Someone tries using brute force attacks fail as there can be completely different input values giving the same output. It is a one-way cryptographic function and is a stable size for any size of the source text.


Figure 2: encryption of inputs https://www.edureka.co/blockchain-training

If you look at the first example, the input as “Hello World” and getting an output as “a591a6d40bf420404a011733cfb7b190d62c65bf0bcda32b57b277d9ad9f146e”. However, by just adding an “!” at the end, the output completely changes to “7f83b1657ff1fc53b92dc18148a1d65dfc2d4b1fa3d677284addd200126d9069”. If we change “H” to “h” and “W” to “w”, then the output value changes to “7509e5bda0c762d2bac7f90d758b5b2263fa01ccbc542ab5e3df163be08e6ca9”.

### b. Public Key Cryptography

This cryptographic technique uses a set of keys referred as Public key and Private Key. Here the Public key is shared with others whereas the Private Key is kept as a secret by the user. This uses asymmetric key encryption.

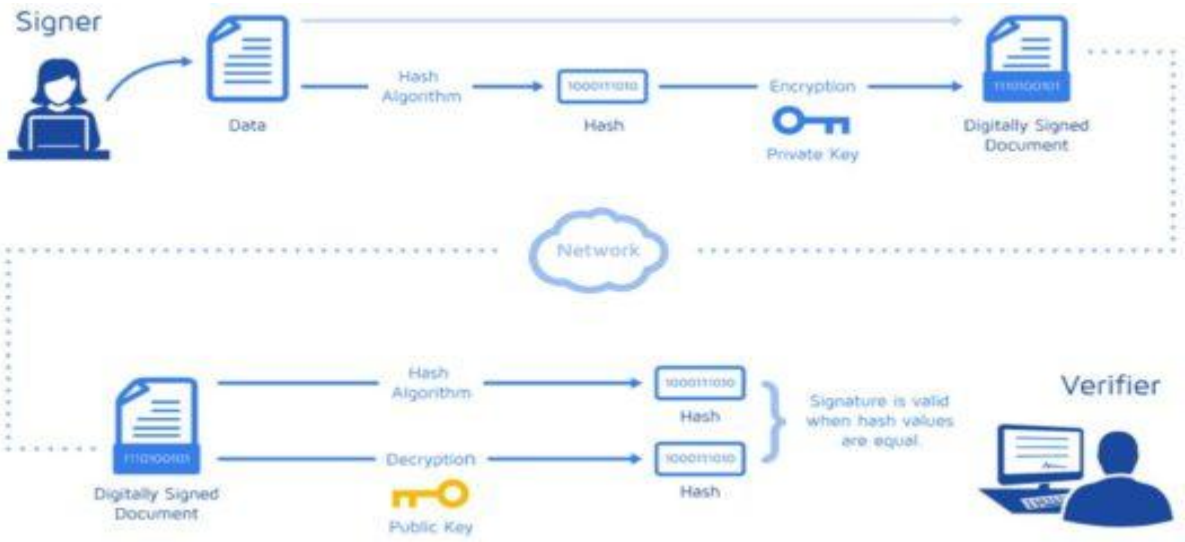


Figure 3: public key cryptography https://www.edureka.co/blog/blockchain-tutorial/

All data along with an encrypted digital signature is sent through the network for verification. This digital signature is encrypted by the private key. Once this data is received by a miner who has to verify this transaction, there is 2 process he does simultaneously.

1. He takes all the un-encrypted data like transaction amount and public keys and feeds it to a hash algorithm to get a hash value which we shall call Hash1
2. He takes the digital signature and decrypts it using public key to get a hash value which we will call as Hash2
3.

If both Hash1 and Hash2 are the same then it means that this a valid transaction.

**c. Distributed Ledger and P2P Network**

The blockchain is the core technology behind the popular cryptocurrency system Bitcoin. It is popularly growing technology because of the public distributed ledger. Every person on the network has a copy of the ledger. There is no single centralized copy. Even if you try to manipulate your ledger it only reflects in your ledger, the original will not get changed. This is what the peer to peer network comes in hand. No fake transaction or invalid transaction is part of the blockchain system as well. Since it's spread across everyone in the distributed system, If you lose your ledger you can download it from one of the other people holding on to the ledger. The ledger contains only the details of a transaction, amount of transaction being happening and the timestamp when the transaction was initiated. The transaction id is completely encrypted and encrypted value is hashed output value. Every transaction from the first one is stored in a continuously growing database called Blockchain. This ledger is distributed to all users of Bitcoin Blockchain, i.e., the ledger has no central location where it is stored. Everyone on the network owns a copy of the ledger and the true copy is the collection of all the distributed ledgers.

**d. Proof of Work**

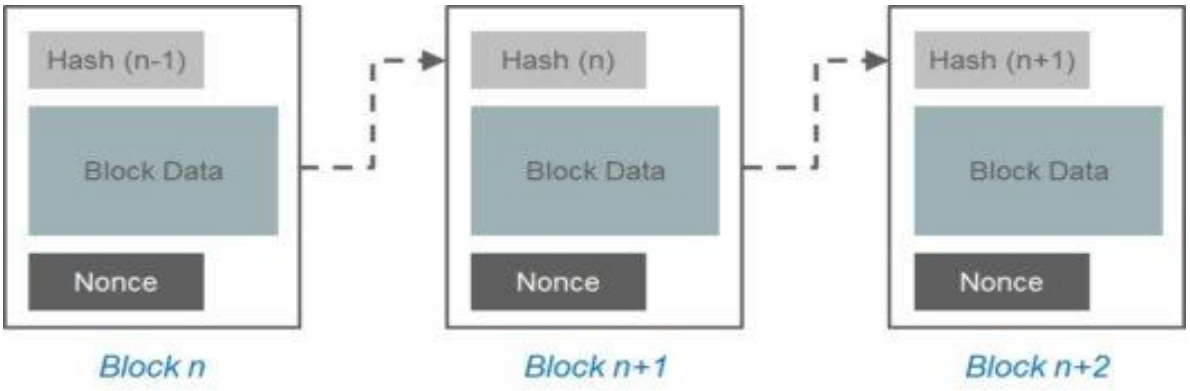


Figure 4: https://www.edureka.co/blockchain-training

Proof of work requires lots of computational effort. It involves solving the computationally expensive puzzle which is tough but easy to verify. This work is done by miners in the Bitcoin network. Bitcoin has miners who validate to solve a complex

mathematical puzzle to add a block to the blockchain. The miners verify all transactions. Miners search for a specific nonce which gives the desired hash which is predetermined. The miner will solve the complex mathematical puzzle associated with the block being created. In the present scenario, the miner needs to try 20.6 quadrillion nonce to get the correct hash.
Each block contains a hash value with the previous block's final hash, transaction data block, and the nonce. The final hash for the block must start with a specified number of trailing zeroes. So the person who finds this nonce is the successful miner. A miner can add their block to the blockchain. Then everyone in the P2P network verifies their hash match, updates the blockchain and moves to next block.

**e. Incentives for Validation**

The last step of a Bitcoin transaction is to giving a reward to the miner who has created the latest block. Every miner who successfully validates a block is paid an incentive. Bitcoin incentives are the only way to generate new currency into the system.

## V. Conclusions

Now a day's people start using cryptocurrency because it is a peer to peer network and it does not require any transaction charge and also no transaction delay for the cryptocurrency. The transaction is highly secure. In this new era of economic freedom, Bitcoin is considered to be the gold of blockchain. It is thought to be extremely gainful storing of value. The main problem of cryptocurrency can be overwhelmed by enlightening codebase and legalization. Cryptocurrency is not tied to any rules or regulations of any specific government exchange rates, interest rates and country to the country transaction fee. The international transaction will move faster. The future application of cryptocurrency deceits in letting your final control over your money with a fast secure global transaction and lower transaction fees when compared to all existing currencies. When used properly and fully understood it would be the initiator of many emerging systems that will fundamentally change our global economic system.

**REFERENCES**

[1] Satoshi Nakamoto "BITCOIN: a peer to peer electronic cash system"//www.bitcoin.org/

[2] Nakamoto, Satoshi (3 January 2009). "Bitcoin" //https://en.wikipedia.org/wiki/Bitcoin

[3] **Neel** "Blockchain Certification Training ".//www.edureka.co/blockchain-training

[4] Neel "Blockchain Tutorial A beginners guide to Blockchain Technology"://www.edureka.co/blog/blockchain- tutorial/

[5] Sandeep Dayananda"What is blockchain,Demystifying blockchain and Bitcoin technology"//www.edureka.co/blog/what-is-blockchain/

[6]Sandeep Dayananada "Blockchain Everything you need to know about Blockchain"
https://www.edureka.co/blog/blockchain- technology/

[7] M Andreessen "what is blockchain technology" // www.coindesk.com /information /what-is-blockchain-technology/

[8] M Andreessen "what is blockchain technology" // www.coindesk.com /information /what-is-blockchain-technology/

[9] Patrick "what is the difference between bitcoin forex and gold 'a tripod theory' "//www.newsbtc.com/2015/09/09/

[10] Brad Mills "CRYPTOGRAPHY: dawn of anew economy"//blockgeeks.com/guide/what-is-cryptography/

[11] Oliver Dale "what are cryptocurrencies"//blockonomi.com/what-are-crypto-currencies/

[12] Danton Bryans "bitcoin and money laundering mining for an effective solution", Indiana law journal,vol.89,//ilj.law.indiana.edu/articles/19-bryans.pdf on19-06-2014