Emperor Journal of Applied Scientific Research

www.mayas.info **© Mayas Publication** **ISSN No: 2581-964X**

Volume-VI **Issue-3** **March-2024**

Block Chain Techonology

Sathyajothi R
Lakshmi Bangaru Arts And Science College
Karunguzhi, Chengalpattu District-603303
sathyajothirajasekaran@gmail.com
720581009

I. INTRODUCTION

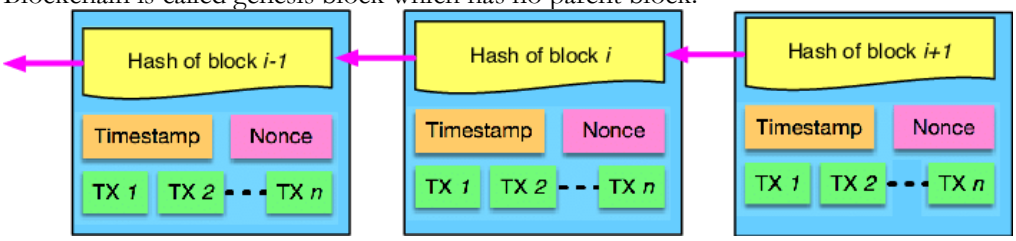
Blockchain can be defined as a digital record of all the transactions that take place in a computer network. The name comes from two words, one is block which means that there are blocks of individual data which has all the information about the transaction and the second is a chain which means that all this data is arranged in a single list which is here referred as a chain.

Block chain is a system of storing and transferring information in a distributed and decentralized way. You can think of it as a ledger or a record book that is shared and updated by many participants, instead of being controlled by a single authority. Each entry or transaction in the ledger is verified and encrypted by a network of computers, called nodes, using cryptography. These transactions are grouped into blocks, and each block is linked to the previous one by a unique code, called a hash. This creates a chain of blocks, or a block chain, that is secure, transparent, and immutable

One of the major tasks performed by Blockchain is to store the transaction data of Cryptocurrencies. The network required for Blockchain is a peer-to-peer network in which every user of the network has the information of all the transactions made in that specific network. Transactions are made using Cryptocurrency wallets. All the transactions that are made are encrypted. Some of the common examples of Cryptocurrency are Bitcoin (BTC), Litecoin (LTC), Ethereum (ETH), Ripple (XRP) etc.

Architecture of blockchain:

Blockchain is a sequence of blocks, which holds a complete list of transaction records like conventional public ledger. With a previous block hash contained in the block header, a block has only one parent block. It is worth noting that uncle blocks (children of the block's ancestors) hashes would also be stored in Ethereum Blockchain. The first block of a Blockchain is called genesis block which has no parent block.



A block it has information related to the transaction, such as when the transaction between two parties was made, what was the date and time and what amount was transferred between the two dealing parties. A block consists of the block header and the block body

Block Header

The block header consists of:

• **Block version:** Indicates which set of block validation rules to follow.

• **Merkle tree root hash:** Every transaction has its own unique code that differentiates it from other transactions. It basically separates all the transactions from others so that at the time of inquiry it would be easy to identify that specific transaction. The unique code is known as 'Hash'**.**

• **Timestamp:** Current time as seconds in universal time since January 1, 1970.

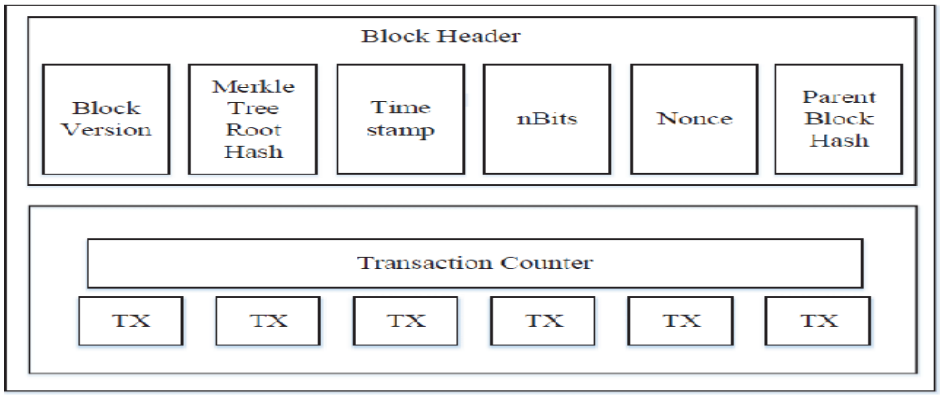
• **nBits:** Target threshold of a valid block hash.

• **Nonce:** An 4-byte field, which usually starts with 0 and increases for every hash calculation.

• **Parent block hash:** A 256-bit hash value that point to the previous block.

Block Body:

The block body is composed of a transaction counter and transactions. The maximum number of transactions that a block can contain depends on the block size and the size of each transaction. Blockchain uses an asymmetric cryptography mechanism to validate the authentication of transactions [9]. Digital signature based on asymmetric cryptography is used in an untrustworthy environment.



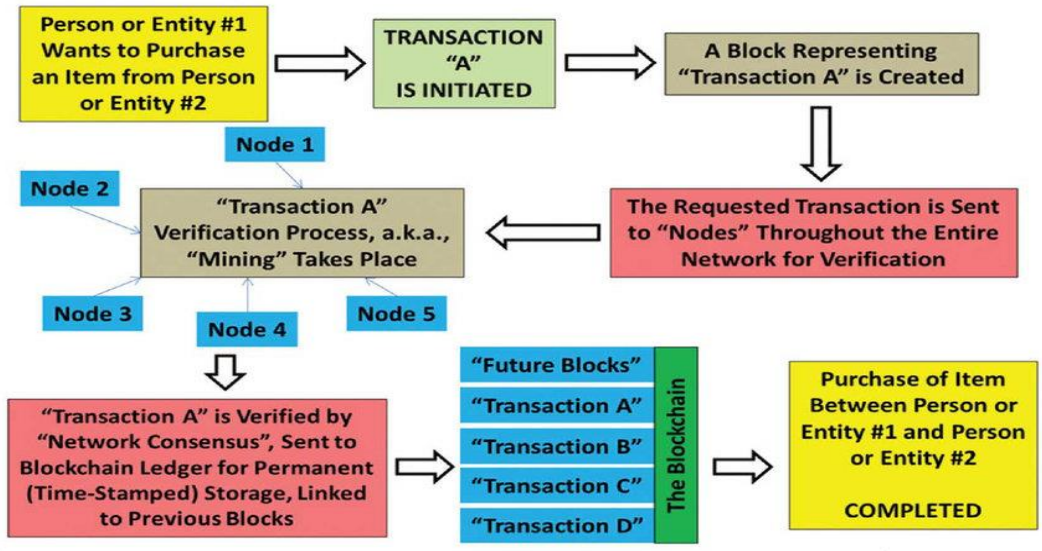
How the Blockchain works

In order to add a block into the Blockchain the block should fulfill the following criteria.

1. A transaction has to be made. An agreement between the users must take place in order to initiate the addition of a new block into the Blockchain.

2. The transaction that is made must be verified. In the case of Blockchain this verification is done by a computer network that is comprised of more than 5 million computers spread across the globe. This network make sure that the details of this transaction are right and they cross check thing like the time of the transaction, the amount of the transaction, the users involved, digital signatures etc.

3. The transaction is to be stored in the block. That means that once the transaction is verified and is accurate the information such as the users digital signatures, transaction time and the transaction amount is stored in the block having its unique hash. This block is then stored in the Blockchain along with thousands of other blocks. 4. The last step includes the assignment of Hash. The Hash given to this transaction is of the most recent block that is added in the Blockchain. As soon as the block is hashed, it can be added into the Blockchain . Once the block is a part of the Blockchain it can be publicly seen by everyone that is the part of that network. Every user has a copy of the Blockchain and they have access to the information related to the transactions along with the information about the time, date and amount added this block to the Blockchain.



Key characteristics of blockchain

Blockchain has following key characteristics:

• **Decentralization:** In conventional centralized transaction systems, each transaction needs to be validated through the central trusted agency (e.g., the central bank), inevitably resulting in the cost and the performance bottlenecks at the central servers. Contrast to the centralized mode, third party is no longer needed in Blockchain. Consensus algorithms in Blockchain are used to maintain data consistency in distributed networks.

• **Persistenc:** Transactions can be validated quickly and invalid transactions would not be admitted by honest miners. It is nearly impossible to delete or rollback transactions once they are included in the Blockchain . Blocks that contain invalid transactions could be discovered immediately.

• **Anonymity:** Each user can interact with the Blockchain with a generated address, which does not reveal the real identity of the user. Note that Blockchain cannot guarantee the perfect privacy preservation due to the intrinsic constraint.

• **Auditabilit:** Blockchain stores data about user balances. Any transaction has to refer to some previous unspent transactions. Once the current transaction is recorded in the Blockchain, the state of those referred unspent 357 transactions switch from unspent to spent. So transactions could be easily verified and tracked.

An Introduction to Cryptocurrency:

A cryptocurrency, crypto-currency, or crypto is a digital currency designed to work as a medium of exchange through a computer network that is not reliant on any central authority, such as a government or bank, to uphold or maintain it.

Cryptocurrency does not exist in physical form (like paper money) and is typically not issued by a central authority. Cryptocurrencies typically use decentralized control as opposed to a central bank digital currency (CBDC). When a cryptocurrency is minted, created prior to issuance, or issued by a single issuer, it is generally considered centralized. When implemented with decentralized control, each cryptocurrency works through distributed ledger technology, typically a blockchain that serves as a public financial transaction database.

Blockchain in Cryptocurrency:

These transactions are recorded on Blockchain which is a decentralized system and is hosted on computers across the world. Cryptocurrency is traded on Cryptocurrency exchanges just like money is traded in stock exchanges. A Cryptocurrency wallet is a digital wallet which is used to receive, store and send Cryptocurrency. Its security is ensured with the help of encryption algorithms that make sure that the Cryptocurrency is safe from any external threats. Transactions are made with the help of this Cryptocurrency wallet. There are two types of keys namely Public Key and Private Key. In order to transfer Cryptocurrency from an account to a specific account, we must know the Private Key of the account in which we have to transfer the amount. Cryptocurrency network gets encrypted transactions and it broadcasts these requests which are queued and are then later added in the Blockchain which in this case is a Public ledger. These transactions will then be saved on the Public ledger with the help of a technique called mining. When transactions are made and are added onto the Public ledger then which is the Blockchain then new coins or Cryptocurrency is created. This is known as mining. It is explained in the later part of the paper under the heading .Mining. All users have access to the Blockchain and every user has a copy of the Blockchain in their computer. The Blockchain available to the users tells the users about the time of transaction, the date of transaction and the amount of transaction but it never tells us about the identity of the user. This is a major trait of Cryptocurrency that it does not reveal the identity of the user. Just as in banks there are bank accounts similarly in the case of Cryptocurrency there are keys. Whoever owns the keys owns the amount of Cryptocurrency present in the accounts of the keys. All these transactions are added onto the Blockchain and they form up queues and then are added block by block forming a chain of blocks.

Cryptocurrency Mining

It can be defined as process in which different users compete with one and other to find new Cryptocurrency and also help in adding new Cryptocurrency transaction in the Blockchain. The users that compete with each other are known as Miners. When a transaction is made meaning either Cryptocurrency is spent or received a broadcast is made to the whole network about that transaction. In order to make this transaction permanent it has to be stored on the Blockchain. With the help of mining this process of adding the transaction in the Blockchain is carried out and this transaction is then stored in the Blockchain present on every computer.

Now we will discuss how mining works. All the miners in the Blockchain collect the broadcasted transactions which are being broadcasted by other users and then they verify if these transactions are valid or not according to the current Blockchain. After that they form a transaction block which is a compilation of all the transaction details. This task is performed as a whole by all the miners so that the confidentiality of the data is not compromised and no individual can create a fake transaction block and then add it on to the Blockchain.

In order to maintain the confidentiality, integrity and authenticity of the transition block each miner has to solve a difficult puzzle or in other words has to crack the bit coin algorithm. The miners have to crack a complicated computational puzzle known as the proof-of-work scheme and once they find the solution they broadcast it all over the channels on which other miners are also present. After that other miners will verify the solution and if it is the solution then this is added into the Blockchain and is considered to be successfully mined. The benefit that the miner gets is that he will be awarded with 25 bit coins for his efforts. This acts as an incentive for other miners to keep mining and win free bit coins. The newly created bit coins also add overall bit coin money supply.

Cryptocurrency Security.

The factor that makes Blockchain strong is its Distributed ledger technology (DLT). This means that the redundancy in its block makes it difficult for black hats to hack it. In order to hack a transaction a black hat has to hack every mining node till the start of the Blockchain till the block that has the hacked transaction. This is an impossible task as there are no processors that offer such great processing powers to simultaneously hack so many blocks and create a fake bitcoin.

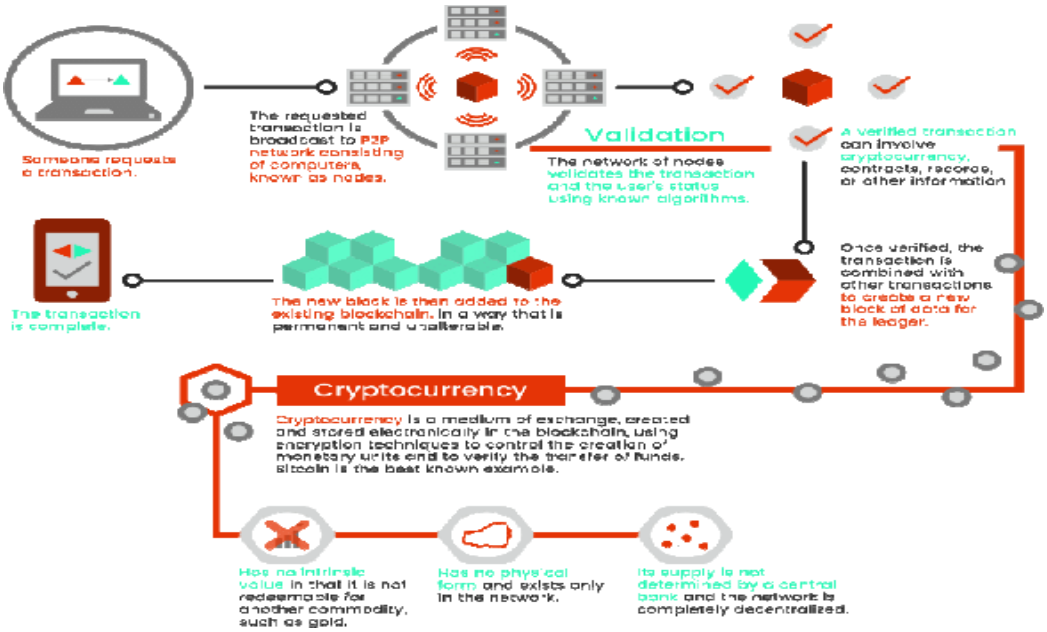
As the Blockchain is publicly shared so every user has access. To the data in it and if the data is altered at one place it can be easily detected as it will differ from the data of all other users. The block is firstly distributed in all the mining nodes of the network and this is done so that every miner knows that the transaction made is valid and can save its copy. This step helps in times when there is a need to trace a certain transaction. As the details of this transaction are a part of every single user in that network it makes the network safe and in case of any modification of data the network knows that this is invalid. Every single node or miner of thenetwork acts as an auditor and if they reject any transaction then it is invalidated.

How the Cryptocurrency Transaction Work?

In a Blockchain network, everyone has a public address on the network. This works just like an email address: if you know someone's address, you can send them something. Also like an email address, you can't determine someone's identity just from knowing their address. You can make up an email address and send mail to it but you can't tell from it the person's name (unless it's included in the address). The same is true for the addresses used in Blockchain, you can send money to an address but you can't tell from it who the money was sent to unless they tell you.

For a Cryptocurrency transaction to work, the person sending the money needs to know the recipient's public address. Many Cryptocurrency wallets make this easy by encoding it into a QR code that the buyer can easily scan into their own wallet application to make a transfer. Otherwise, the address is encoded as a string of letters and digits that the sender can type into their wallet to perform the transfer. This is all that the sender or recipient have to do to make a transaction. For some Blockchain s (like Bitcoin), the sender may be required to include a little bit of extra Cryptocurrency as a transaction fee used to pay the miners (more on this later). Behind the scenes, the sender's wallet digitally signs the transaction with their private key. This means that anyone knowing their public address (also called their public key) can verify that they authorized the transaction. Since the public address is included in the transaction, this is very easy to do.

Next, the wallet sends the transaction to one of the mining nodes on the Blockchain network. This node sends it to all of the other nodes that it knows about, they do the same, and so on until every node in the network has a copy of the transaction. At regular intervals, a block is created on the Blockchain. If a transaction is included in the block, the details of the transaction including at a minimum the sender and recipient's addresses, the amount of the transaction, and the sender's signature are written into the data section of the block. Through some process someone is selected to create the block and they sign it with their private key (just like the sender signed the transaction) to protect it from modification. Then, they send it to every node that they know and so on until everyone in the Blockchain network has a copy of the block. Figure 4, show how a Cryptocurrency transaction works in the Blockchain networks.



Blockchain and Cryptocurrency An Inspirable Relevance:

The Blockchain of a Cryptocurrency is the master ledger that generally records all prior transactions and activities, validating the ownerships of all units of the currency at any given point of time. The Blockchain contains the entire transaction history of a Cryptocurrency as a record. It has a finite length containing a finite number of transactions that eventually surges in due course of time. Identical copies of the Blockchain are stored in every node of the Cryptocurrency's software network. This network of decentralized server farms is managed by tech-savvy individuals or groups of individuals known as miners. Miners continually record and authenticate Cryptocurrency transactions.

A Blockchain currency transaction technically isn't necessarily finalized until it has been added to the Blockchain. Once the transaction is finalized, it is usually irreversible. Unlike traditional payment processors, such as PayPal and credit cards modes of transactions, most Cryptocurrencies have no built-in refund or chargeback functions. During the lag time between the transaction's initiation and finalization, Cryptocurrency units cannot be used by either party. They are held in a state of freeze down for all intents and purposes. Blockchain thus prevents double spending or the manipulation of Cryptocurrency code to allow the same currency units to be duplicated and sent to multiple recipients.

While Cryptocurrency transactions depict security, there are certain aspects that question the authenticity of their existence. To mitigate these allegations on authenticity, there was a need to develop a fool proof technology that would not only make online Cryptocurrency transactions safe but also construct an impregnable firewall through which hackers can't penetrate. This is where the Blockchain took the center stage. Apart from providing a secure platform, Blockchain s also ensured that transparency is the key to all Cryptocurrency transactions. With Blockchain s, any person on the Internet can have a sneak through at transactions that have happened on a Cryptocurrency unit since its inception.

This allows users to transparently traverse through transactions. Also, the ledger can be copied onto every computer in the world. This means that there exists no centralized place which a hacker can leverage to tamper with transactional data.

Assume that hackers became successful doing that. Still, they won't be able to change any of the previous blocks of transactions as all these blocks are knitted with each other in a

chain in a perfect order of cryptography. Any bitcoin transaction that ever happens is walled off and grouped together into blocks within 10 minutes of its successful completion. Each block contains a hash code which links it with its previous block, thereby making the whole Blockchain system tamper proof. If any information is tried to be changed within a block, the block will generate a new hash code, signifying what is the original data in the block and what is no

Blockchain and cryptocurrency Applications

There are numerous applications of Blockchain and Cryptocurrency. Some of these applications are stated as:

1. Travel industry is probably the industry that is most effected with the introduction of Bitcoin. As bitcoins are considered to be a universal currency so where ever you go you can use them without paying any extra banking or conversion fees. Cheapair.com is a website that has been accepting bitcoins for the booking of hotels, flights, rental cars and cruises.
2. Schools, colleges and universities now a day are also accepting payments in the form of Bitcoins. University of Nicosia is accepting payment of fees through Bitpay that is a platform that allows to pay academic fees through bitcoins. Some universities in Germany, Switzerland and United States are also accepting bitcoins as academic fees.
3. Blockchain and Cryptocurrency also help environmentalists. Surprisingly enough it can help the world be more green. It would eliminate the cost of making notes which is done at the expense of trees. As this is a digital form of currency so the need of hardcore currency would be eliminated hence saving the cost of the paper and production costs. Also there are some organizations such as Brooklyn Microgrid who allows the users that have solar panels to sell their environmental credits to people having no direct acess reducing carbon emissions and promoting green energy.
4. Another use of Blockchain and Cryptocurrency is in the field of charities and donations. It is often seen that the donations and charities never make it to the people that they are actually meant for resulting in corruption and mismanagement. By using Blockchain and Cryptocurrency it can be made sure that the amount meant for someone reaches that specific individual or organization. The World Food Program (WFP) is using Cryptocurrency for transferring its funds as it is safe and easily manageable with almost no chance of corruption.
5. Blockchain and Cryptocurrency can also be used in the field of advertisement and digital publishing. A common complication that every user using internet faces is irrelevant ads popping up on article. To eliminate this problem some organizations and companies such as SolidOpinion have introduced the option of pay-per-article advertising meaning that each 360 article will have its own set of ads related to the article and these sets are selected by the user itself so that it can make sure that the target beneficiaries get the benefits of the article. This technology utilizes a proprietary form of Cryptocurrency, Engagement Token, to fuel engagement; both publishers and audience members can earn tokens by commenting and publishing original content, and advertisers buy tokens to select their ad placements among relevant articles.

Comparison between Blockchain and Cryptocurrency:

Basis of Comparison	Blockchain	Cryptocurrency
NATURE	A technology that records transactions	Tools used in virtual exchanges
USE	Record transactions	Make payments, investments, and storage of wealth
VALUE	Have monetary value	Have no monetary value
MOBILITY	Can be transferred	Can't be transferred

III. CONCLUSION

As fundamental technologies with transformative potentials, Blockchain and Cryptocurrencies have found a wide spectrum of application scenarios in various types of industries, ranging from the underlying techniques of data storage, encryption, and verification, to the middle level of finance and asset management, and to a variety of high-level business models. The property of its security, privacy, traceability, inherent data provenance and time-stamping has seen its adoption beyond its initial application areas. Its decentralized application across the already established global Internet is also very appealing in terms of ensuring data redundancy and hence survivability. Thus the invention of the Blockchain and Cryptocurrencies can be seen to be a vital and much needed additional component of the Internet that was lacking in security and trust before. Blockchain and Cryptocurrencies technology still has not reached its maturity with a prediction of five years as novel applications continue to be implemented globally.