International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 10 | Oct 2020 www.irjet.net p-ISSN: 2395-0072

Blockchain Technology: History, Concepts, and Applications

Roopika J

Student, Dept of EEE, Kumaraguru College of Technology, Tamil Nadu, India

---

Abstract - *In technology, the most popular buzzword right now is Blockchain second to Artificial Intelligence and Machine Learning. Decentralized Ledger Technology(DLT) is the underlying concept behind blockchain. Bitcoin which is a cryptocurrency has been all over the news in recent years for both good and bad reasons but bitcoin is just an application built based on blockchain technology. Blockchain is extremely good at solving specific problems only. This paper elucidates the history, concepts, and various applications of blockchain with examples. A systematic explanation of blockchain's architecture and the working of blockchain is described in this paper. A few use cases from Ethereum are also mentioned in a few places to understand the concept better. Finally, this paper explains when and why one should opt blockchain technology and how blockchain is already ruling various businesses is discussed.*

Key Words: *Blockchain, Distributed Ledger Technology, Consensus, Bitcoin, Ethereum.*

1. INTRODUCTION

To begin with, blockchain in simple terms can be defined as a digital record of transactions. As the name implies, 'block' has the individual record of transactions and these are linked in a single list called 'chain'. Blockchain is a technology that enables digital exchanges of transactions similar to how the Internet which is also technology that enables the digital sharing of information. Before proceeding further it is necessary to know the general meaning of a few terms that are used throughout this paper. The term 'digital ledger' refers to a computer file that is used for recording and tracking of transactions. These transactions may not be monetary in nature but can be addition, interchange, and modification of data in the computer file. The term cryptocurrency refers to digital or virtual assets stored in digital ledgers and is secured by cryptography which makes it almost impossible for any counterfeit or double-spend. The consensus mechanism is a process of validating a transaction in Blockchain without the necessity to trust the centralized authority. Bitcoin and Ethereum are few cryptocurrency applications of blockchain technology. With this knowledge, let's dive deeper into how blockchain came into existence and how this technology has changed the world.

2. THE EPOCH OF BLOCKCHAIN

The historical background of blockchain doesn't go back far. However, it returns to the mid-1990s when a couple of scientists, Stuart Haber and W Scott Stornetta, were attempting to tackle a major issue, how to keep the past safe, and keep digital information secure and impervious to altering? It additionally tackled the Byzantine Generals Problem.

In 1991-The two scientists published their first paper to layout the utilization of a chain of cryptographically secured blocks to save the integrity of past data and ensure it.

In 1993 In light of the expansion of spam and other organization mishandles, the idea of proof-of-work was set up, which looked to give countermeasures to those.

In 2008-It was in 2008, a shadowy central figure in the tale of Bitcoin named Satoshi Nakamoto delivered a fundamental whitepaper that introduced the period of blockchain. The paper was known as Bitcoin: A Peer-to-Peer E-Cash System.

The actual characteristics of the central parts of the most usually known blockchain of today, Bitcoin, was published in this paper, This paper depicted a method of trading cash, Bitcoin, that consolidates cryptography, computer engineering, and game theory in its plan and usage. This information is regular to such an extent that a few people think Bitcoin is the blockchain, and that the terms are compatible. In any case, they aren't.

In 2014-Ethereum entered. Ethereum's key development is that it is considerably more than only money or a record of exchanges. Its specification can really run the computation. The Ethereum Virtual Machine, or the world computer, takes into account what is called smart contracts, or programs that can be deployed onto the blockchain, letting developers make dApps(decentralized applications) that are placed, distributed on the chain itself.

In 2015- The Bitcoin had started to quit fooling around the consideration.

In 2016, Blockchain had started to get serious attention and it truly hit its sweet spot in the financial industry.

In 2017- Blockchain was proposed as a basic technology by the Harvard Business Review.

Today, there is a vigorous and quickly developing environment encompassing blockchain, and the energy is just developing towards a decentralized future.

Despite the fact that the idea of a blockchain was first completely realized in Satoshi Nakamoto's Bitcoin

Whitepaper, the basic concept advances draw from long periods of examination across cryptography, computing, and financial aspects.

3.1DECENTRALIZATION

Centralization, or management by one authority or entity, could be a common and pervasive sort of governance. Governance indicates the principles of power and organization.

We tend to trust centralized authorities, like banks, governments, and alternative establishments to take care of the order and law among the house they operate. This trust is broken once the central authorities can't maintain that order and structure. For instance, if your MasterCard info is taken from the database of a bank you interact with, the centralization of your info in this bank has been used against you. Centralized technology and data permits for both the monopolization of power and creates a security risk.

The issues with centralization reached a critical stage during the worldwide financial crisis of 2007-2008. On October 31, 2008, amidst the financial crisis, Satoshi Nakamoto published the Bitcoin Whitepaper, named Bitcoin: Satoshi's creation empowered a member to carefully execute legitimately with another member without depending on a solitary, centralized intermediary, for example, a bank, to approve the payments. At the point when we express peer-to-peer, we are depicting a transaction starting with one entity to another, straightforwardly. There is no intermediary the transaction needs to go through.

For instance, in the event that you plan payment through a banking application on your phone to a companion of yours, the actual cash flow of money goes from an account controlled by your bank to an account controlled by your companion's bank. In the event that your companion doesn't have a bank account, you could send the cash from your bank to a third party, similar to a money transfer company, where your companion could get the installment. Regardless of whether you pulled back the cash from the bank and sent it to your companion, you would need to have a location to send it to and depend on the security of your postal help to get the cash there securely.

3.2 THE MOVE TO DECENTRALIZATION

In this part, we will review the different meanings of decentralization, and how individuals from the blockchain network have applied those definitions to the advancement of the technology. A decent method to consider decentralization is to connect the word with an exchange of authority.

There are three primary types of decentralization, or how authority is transferred. In a post on Medium.com, Vitalik Buterin, one of the originators of Ethereum, itemized the accompanying three types of decentralization:

Architectural (de)centralization — what number of physical PCs is a framework comprised of? What number of those PCs would it be able to endure breaking down at any single time?

Political (de)centralization — what number of people or associations ultimately control the PCs that the framework is comprised of?

Logical (de)centralization — do the interface and data structures that the framework presents and keeps up look more like a solitary solid item, or an indistinct multitude? One basic heuristic is: if you cut the system in half, including both providers and users, will the two parts keep on working as autonomous units?

Let's take a look at an example. The PC or tablet on which you are perusing this was likely made by an organization with a CEO and a leading body of heads. This organization is likely organized to have specialty units that deal with different parts of the building, showcasing, and selling the gadget you are utilizing. The CEO and the leading group of chiefs give guidance to the distinctive specialty units so they can cooperate to assemble PCs. On the off chance that the organization was to be separated, the CEO and leading body of chiefs would need to choose to separate the organization. The individual pieces of the organization couldn't choose to do that all alone. If the part of the company that assembles the mouse pronounced they no longer wanted to be part of the larger company, they really do not have the choice to break off into another company. As indicated by Vitalik, this implies the organization is logically centralized.

Another model that Vitalik utilizes is language. The speakers of any language adhere to syntactic guidelines and best practices regardless of the way that there is no unified authority driving individuals to talk in a specific way. Associations that distribute word references don't have direct authority over the language. Individuals who communicate in the language are the ones with authority over it. This is the reason dialects develop after some time, with structure and character contingent upon the spot and time in which it is communicated. An example is by which Latin developed after some time into the advanced sentiment dialects of Spanish, French, Italian, Portuguese, Romanian, and Catalan. No central authority concluded that Latin ought to develop into these dialects. For this situation, language is something that is logically decentralized.

On account of blockchains, they are politically decentralized since no individual has solitary power over them. They are additionally architecturally decentralized due to their infrastructure which has no central point of failure, as every node keeps a duplicate of the blockchain. However, blockchains are logically centralized since the framework behaves like one PC in spite of being spread apart on all the participating nodes in the network.

3.3 DECENTRALIZATION BENEFITS

Decentralization (politically and architecturally)) permits blockchains to be:

- Less liable to fail since they depend on many separate segments.

• Harder to attack since the nodes are spread across numerous PCs.

• Harder for clients with malicious intent to exploit clients who are utilizing the platform for its proposed purpose.

If one node quits working, or even 100 nodes, the blockchain survives assuming there is at the minimum one node fully operational. This makes the blockchain exceptionally impervious to attacks. The blockchain doesn't quit working regardless of whether the power is lost in a whole nation. This makes the blockchain very resilient, which can't be said of a considerable lot of the current frameworks we use on the Internet. Presently, organizations like Facebook, Amazon, and Google rule the Internet. They offer many free or modest administrations since they can gather important information on their clients, and discover approaches to adapt that information. As a client of the modern internet, one is never too sure where their data and individual information is being utilized. Through the execution of decentralization, also called Web 3, the information doesn't need to be put away in centralized systems.

Data can be validated independently and people can transact directly with one another, rather than requiring a centralized entity to check these transactions. Micropayments become an achievable technique for being compensated for value created. Clients control how their information is utilized and accessed over the Internet, and can be paid for the utilization of their information. Decentralization dis-intermediates the central control of systems. Rather than a solitary organization being liable for composing data to a unified database, the obligation of recording transactions falls to any individual who needs to take an interest in a blockchain. This is a remarkable shift-in-thinking, yet significant in seeing how blockchains could be progressive—they are diverse both logically and actually—and are explicitly designed to be an option in contrast to the centralized systems we know about.

4. DISTRIBUTED LEDGERS

Distributed ledgers can include many types of a shared database, of which blockchain implementations are just one. Blockchains generally do have distributed ledgers, but if you were to start your own blockchain on your computer, and that computer is the only node, then that blockchain wouldn't be distributed. You could also have a blockchain running on one computer, undistributed, for some other purpose that makes use of the other features of a blockchain.

Blockchain developers often use personal, single-machine blockchains to test software. You could say those blockchains don't technically have distributed ledgers, but the ledgers could be distributed if more computer nodes joined their system.

Blockchains also have other components; the ledger itself is just one part of the system overall. So, a blockchain need not have a ledger that is distributed, but the true power of blockchains is best unleashed when there are multiple distributed nodes working together.

5. THE PAPER BLOCKCHAIN

A blockchain is really a very basic concept. It's only a set of linearly connected information containing blocks secured with cryptography. Presently, there is plenty of details behind current executions, yet, we can take a look at what a basic blockchain is with a real-world example. Envision a little community called a little blockchain. This community has a little dynamic economy with individuals purchasing and selling merchandise with one another and at whatever point somebody makes a transaction, it's accounted for to the town accountant, who logs the exchange on a bit of paper. By the day's end, the accountant goes to the town square and openly staples the page to the earlier day's transactions. Let's assume that the accountant utilizes a fingerprinted wax seal to cover each staple so nobody can remove earlier pages or tamper with them, without it being exceptionally self-evident. That is an essential paper blockchain. This example of a paper blockchain is illustrated in figure 1.

Figure 1

Each bit of paper represents a block that is put in a linear arrangement containing exchanges. Anybody can proceed to take a look at exchanges previously, even a very long time back, back to at whatever point the system started and since each staple is wax fixed and fingerprinted, everybody can undoubtedly affirm that no one has tampered with any of the pages, each one of which was included publicly. By representing the consolidation of verified consensus over time, this chain would adequately be a record of verifiable, undeniable, and honest truth for the town.

Obviously, in a genuine blockchain, we'd need to expand this similarity. There are actually many accountants making records of exchanges and everyone is contending to be the person who gets the opportunity to add their record to the chain, what's more, obviously, there are additionally numerous town squares, each with its own nearby duplicate of the blockchain and all communicating with each other. However, in spite of all the town squares, only a solitary winning accountant's page will be the one duplicated and added to every one of the distributed chains and each secured with a fingerprinted seal.

At its simplest, this is pretty much what computerized blockchains do today. Nodes are the accountants attempting to put transactions broadcast to the organization into blocks also, being the victors in a competition that leaves them be the ones to add their block to the distributed chains.

6. THE ANATOMY OF A BLOCK

Blocks are the literal building blocks of the blockchain. The fundamental purpose of a block is to record the transactions. In this simplified example block given in figure 2, we can see the list of transactions that are included.

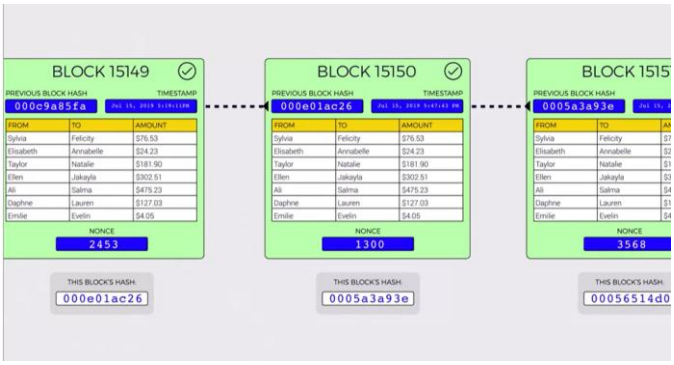

Figure 2

In the example of paper blockchain, a block was a solitary piece of paper listing a day's transactions in a ledger format. The example given here has only seven transactions. However bitcoin block consists somewhere up to 2,000 transactions per block, but this number differs between different blockchains and depends on block size limits.

Block sizes are basically limited to prevent network congestion. Bitcoin presently has a block size restriction of one megabyte. Every block has a unique number, also considered its height. These numbers again or heights increment because the blockchain is linear. At a given height there can only be one block. Similarly blocks also contain a timestamp, a weird number called a nonce, some other data not listed here, and fundamentally a hash of the previous block in the chain,

Validity is one of the most significant concepts in the blockchain. Not all blocks are built equal, the dominant part of blocks are invalid. This process is done by miners. Miners are nodes who also do what's called mining. They try to find a valid block by hashing and rehashing them while changing the nonces. When they find a valid block they add it to their blockchain and send it to the other nodes.

Blockchains have what's known as difficulty, which is basically an arbitrary setting that decides how hard it is to create blocks. From this only we are getting the value. If all the persons could just create blocks and throw them on the chain, then there would be no value there, and networks would never concede on which blocks must go on to the chain. Having created a block means you probably must have done a whole lot of work. This is known as proof-of-work means. When a person has found a block that is valid, one has proven that work has been done. For public blockchains like Bitcoin and Ethereum, the difficulty level can change in order to make sure that blocks are created regularly at specified intervals.

Let's take a look at how this works. A block is only considered as a valid block when the hash value of the whole block, the hash value being a number, is lower than another threshold number. That threshold number is set by the difficulty. If we take our block, and we hash the whole thing, we get a unique signature for all the information it contains. On the event that there is an alteration in any of the information, it necessarily changes the hash,

The way to determine if this particular block is valid is by checking whether this block's hash is lower than the difficulty threshold. The higher the difficulty, the lower the hash output number should have to be for the block to be valid. Since hashes are effectively random, lower values are difficult to find.

It resembles rolling a die. It's harder to roll a two or below than it is to roll a three or below you can think of each hash digit resembling rolling a 16-sided die. To get three zeros as we need, there is a need to roll three 16-sided dice and get three once, since there are no zeros on a die. As you can think you'd need to roll the dice many times around 4,000 times for that to occur. However to do that with our block, we need not roll dice, we can possibly alter the data and see if we happen to get a valid hash, and do it repeatedly. But what data can be changed in a block?

It consists of important transaction data that you can't alter. This is where the nonce comes in. The nonce is there just so that miners have a piece of information that they can really play with. They can alter it casually to change the block's output hash till they discover one that is lower than the required difficulty threshold. When they have discovered a nonce that results in their block's hash being lower than the difficulty threshold, the block is ultimately considered valid and it can be transmitted to the network with that miner taking a reward for their work. This process is completely based on chance. Miners simply attempt again and again changing the nonce and rehashing the block and trusting that they will find a hash below the threshold number.

Presently on the Bitcoin blockchain, miners need to find hashes beginning with 19 zeroes. That's hard as rolling 36-sided dice and getting all sixes. So, finding a block is truly difficult and a big deal.

It's hard to such an extent that with a best in class mining PC of today running 24/7, a valid block is expected to be mined about once every 40 years.

Note that if you attempt to change any of the information in a block once it has been mined and discovered a working nonce, you ruin the block once again, and need to start from the very beginning finding another nonce that goes with the new information. This is the reason blocks are so hard to alter after they've been mined.

As a note, the compensation for mining can be substantial, the current prize for finding a block in the Bitcoin network is 12.5 Bitcoin, or right now around $80,000. At the point when other nodes on the network got a valid block, they can effortlessly check its validity by just hashing the block by themselves, and making sure that it's lower than the target difficulty. If it is, it's added to their blockchain and work begins on the next block, and that the succeeding block will

include that previous block's hash in its own data which ensures the continuity of the blockchain.

7. THE CHAIN OF A BLOCK

The crucial part of including a block into a blockchain is the incorporation of a cryptographic hash of the previous block. In this way, blocks are connected all the way back to the very first genesis block and are checked by hashes. Since each block contains the previous hash and that gets hashed within the following block, it might be said, all the previous hashes are baked into all future block hashes. Here comes the real immutability. All the blocks are associated through the interrelationships of every one of their hashes.

The picture given below is a sequence of blocks each with their related data, hashes, and nonces. In the event that anything is changed anyplace in the chain, there's a ripple effect invalidating all the blocks that come thereafter. Assume a malicious person, Calvin, was trying to alter our transaction on the chain. As we are aware, data can't just be altered because that would create an invalid block, so you'd have to re-mine that block and find a nonce that gives a hash value lower than the target difficulty. Since all the succeeding blocks must contain the hash of the previous block, all the succeeding blocks would be invalidated as well. Only if Calvin had an incredible near-impossible amount of computing power, he would be able to rebuild the whole chain to incorporate his fraudulent transaction, and Calvin doesn't have nearly that much computing power. That robustness is the power of the distributed blockchain, and why it's thought of as being incorruptible.

8. NODES AND NETWORKS

Nodes are the PCs that make up a blockchain network. Generally, the Internet has been server-based with a server in the center and users all associated with it, something like what is given in figure 3.

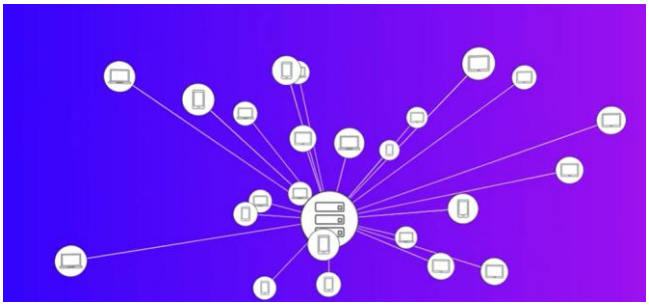

Figure 3

In this design, any individual who needs to associate with online assistance connects with the same server. There are several major disadvantages here. To begin with, the bandwidth demands on that server are very high because all traffic goes to and from it. The entirety of the pathways that exist for information between the organization's members goes unused here. Second, there is a solitary point of failure. On the off chance that the server crashes or gets hacked, the system will stop to work and there's surely a concentration of power here. Whoever controls the server controls the system which isn't essentially a terrible thing however it is a component in this model to observe. An option in contrast to the server-based model is the peer-to-peer model which is shown in figure 4.

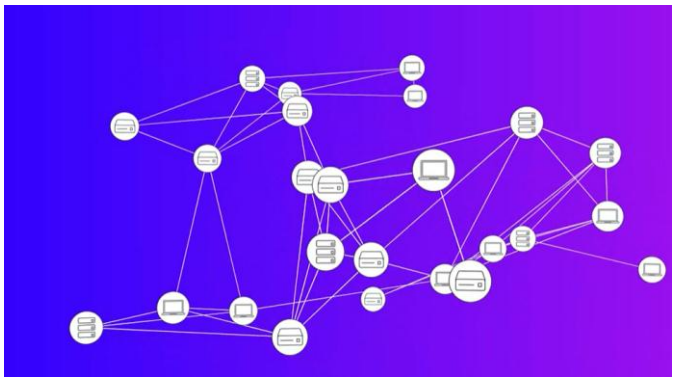

Figure 4

Here peers all interface with each other and are for the most part equivalent. Instances of these incorporate the Ethereum organization, Bitcoin, and BitTorrent. Here data can stream openly between nodes upgrading the utilization of available bandwidth. These systems are additionally resistant to failures in singular peers and stronger to network attacks. One of the most alluring highlights of decentralized blockchain networks is that anybody can go along with them and a network of individuals can share authority.

There is no need for consent to go along with them. The gateway of blockchain is the nodes. They are the frameworks that communicate with each other, guarantee the legitimacy of the blockchain, also, store nearby duplicates of it. There are various types of nodes. Full nodes store the whole blockchain and check everything, each and every exchange. Other nodes named light nodes store only a segment of the blockchain. Miners are independent of nodes. They don't store the blockchain, they are network members who create blocks and send them to nodes who verify and incorporate them or reject them. A node could likewise be a miner however it need not mine. At the point when a full node gets a legitimate block from a miner, it includes it for its nearby duplicate of the blockchain and broadcasts that block out to a couple of other associated nodes who additionally look at the square and broadcast it, etc.

Thus, the block spreads over the whole network and the cycle begins again on the following block.

9. CONSENSUS MECHANISMS AND TRUST FRAMEWORKS

In proof-of-stake, block validators stake their own cryptocurrency for the possibility to forge a replacement block. These validators are chosen to forge a replacement block algorithmically. If a fraudulent transaction is included within the new block, the validator loses their stake, strongly disincentivizing the inclusion of fraudulent transactions. for his or her efforts, the validators are rewarded with the transaction fees for the transactions they include in their block.

Consensus, as an idea, is prime to any system where over one entity is participating. As the Ethereum blockchain aims to

incorporate any participant that runs a node, there's a necessity to quickly reach an agreement on whether to simply accept a brand new block as a part of the chain when it's mined. Without the flexibility to succeed in this agreement, the blockchain cannot create new blocks. Consensus mechanisms are a set of rules that enables multiple machines that are connected together to work together while tolerating some machines providing incorrect data or failing completely. These properties are called fault-tolerance and resilience. A blockchain needs a consensus mechanism to make sure there is a group of rules for creating and accepting each newly created block.

10. PUBLIC KEY CRYPTOGRAPHY

Cryptography is fundamental to all aspects of cybersecurity we have. The Greek word Cryptography, the prefix "crypt" meaning "hidden" or "vault" and the suffix "graphy" meaning "writing", translates to hidden writing. This was originally utilized by Julius Caesar to keep military talks private. His cipher included moving each letter left by three in the alphabet. The fundamental thought here is that we utilize some sort of algorithm to scramble our messages before sending them, so they simply look meaningless to any individual who may peruse them. The persons who can really understand the message are those we share the algorithm with or the individuals who can make sense of the algorithm. The Cesar cipher is, by present-day norms, simple to break.

In today's world, we send messages digitally via the Internet. The issue is we live in a universe of unencrypted networks. On the Internet, there's consistently an outsider dealing with our communications. Communicating over a public unencrypted network implies that anybody along the way of the Internet traffic from point A toward point B can capture and read the messages in the event that they need to. Let's consider them public key A and private key A since they're a coordinating pair, similar to a lock and key.

Public key A is utilized to encrypt or maybe lock messages and private key A decodes messages however just in the event that they were encoded with the coordinating public key A.The public key is called that since it may be shared openly. It can't open anything by itself. Public key A can encrypt a message yet not decrypt a message that it encrypted. That is it can't open a message that it locked. So it doesn't make a difference who else on the organization may have it. Private key A, again, must be kept private because it can decode, or decrypt messages encoded with public key A.This ciphertext can be sent openly on the open network. Consider it a numerical one-way process, where, when a message is encoded with somebody's public key, the best way to read it is with that individual's private key. And it's difficult to decode or hack the message without it.

Public key cryptography is fundamental to making blockchain secure. It's the establishment for how advanced wallets work, and how tokens are exchanged, and how identity is confirmed. Public key cryptography is what is utilized to make verifiable records of the value-based transaction. It's the very thing that makes it workable for us to construct networks that are controlled by the worldwide network, networks that can be really decentralized. A knowingly shared encryption key is utilized to encrypt information that must be decoded by whoever holds its relating private key.

To conclude, a public key is coordinated with a private key. The public key encrypts information and is shared freely; the private key—which is kept secure by an individual or group—is the main thing that can decode messages encoded with its relating public key. Encryption is the way of encoding a message or data so that only approved or authorized groups can have access to it and the individuals who are not approved can't.

11. CRYPTOGRAPHIC HASH FUNCTIONS

A blockchain utilizes hash functions so as to make a record of the information recorded to the blockchain so any change to a solitary bit of information is effortlessly identified. A hash function is an advanced digital mechanism that is utilized to compress information into a particular format of a particular length. The hashing algorithm utilized by the Bitcoin blockchain is SHA-256, which represents the Secure Hashing Algorithm, with a hash length of 256 bits. In this hash, the hashed information is consistently 256 bits in length. The Ethereum blockchain utilizes a hashing calculation called Ethash. A hash made utilizing Ethash will resemble:

0xb846300e188829d1b819389b31cef3b9cfaf335082ee66f830a875f1c1beb396

The hash given above is from block 5000171 mined on Jan-30-2018 at 02:20:28 PM +UTC on the Ethereum blockchain. More information on this block can be found at Etherscan.

In the event that just one bit was changed in the input to the above hash, a totally unique sequence of numbers and letters would be made. At the point when data is incorporated into a block, it is hashed. Accordingly, if a single bit of information inside a block were to be changed on some other occasion, the hash would totally change. This rule permits the nodes taking part in the blockchain to find out alterations in the information or data.

This hashed information is utilized to make a connection between every specific block. This is done by imposing the hash of each prior block into the following block in the chain. At the point when a block is made, a hash of the information inside it is made, and that hash that is made incorporates the earlier block's hash. If even a bit of information is changed in any earlier block that is essential for the chain, each following hash could change. The change falls, permitting the identification of a change to any bit of information inside the chain by comparing hashes with one another over the nodes in the network. This obstructs changes to the blockchain after blocks are made and acquired by the network. Blockchain could be attacked so as to change the record, however making this attack is incredibly difficult. Hence, data written to the blockchain is viewed as lasting. The permanence of information written to the blockchain is the reason why blockchain is referred to as being immutable.

Besides hashing, the blockchain depends on public-key cryptography to acknowledge the concept of ownership on the blockchain. In particular, members on the blockchain have a private key that permits them to get to their data which is encoded with their public key. The public key and private key are connected, however, a malicious person can't get the private key from the obvious public key. Private keys are not intended to be shared since a private key is utilized to open its related public key. These keys sign transactions that are being made on the blockchain

Hashing and public-key cryptography work inseparably to keep up consensus in the system. Through consensus, the whole system has a general knowledge of the happenings on the platform and any activity is recorded and made accessible for the platform to see. This fathoms the issue of trustless systems with mediators because now, members on the blockchain have steady verification on the platform. The procedure of miners verifying activities on the blockchain is known as proof of work. Mining guarantees that the steady condition of the ledger has transactions that are on the whole truth. This keeps attacks and false data from sustaining inside the system, making sure of enduring validity.

12. PUBLIC AND PRIVATE CONSORTIUMS

The vast majority of the blockchains which have been recorded so far were public blockchains. Bitcoin and Ethereum are open public organizations that anybody can join. However, all organizations aren't like this, blockchains come in numerous varieties. When it comes to who is permitted to access them, there are three sorts. The public, consortium, or shared permission and private.

Technically, both consortium and private blockchains are known as permission since they require authorization to access them. Thus, where public blockchains permit anybody to download the software and make a node, consortium blockchains just permit certain individuals to be nodes i.e, nodes are allowed authorization to join, which is the reason for another name of the consortium blockchain is shared permission. For instance, there might be a consortium blockchain in which three organizations and the government regulator operate nodes. You could set up your blockchain so each of the four organizations needs to sign transactions and all would be able to access and review this ledger without requiring access to the constituent organization's internal ledgers. This can be viewed as a condition of low trust. Organizations might have some trust in one another yet not complete trust. Power isn't centralized with any one of the organizations and yet the general population cannot see the transactions.

Private blockchains make this one stride further. In a private blockchain, there is commonly a serious extent of trust. This is significantly more like a centralized system however gives a high degree of audibility since exchanges are distinguishable yet just to those with access. In numerous ways, private blockchains are basically just databases. However, blockchains have underlying advantages of cryptographic auditability, more immutability, and identity as it relates to transactions. Any transactions and changes can be and to be explicitly tracked after some time and to particular parties. It isn't really the situation with databases, in which information can be added, removed, and altered and isn't really traceable.

Private blockchains are of specific use to developers who can set up and control their own blockchain for example to test their software and trial with prototypes. Note that the working of private and consortium blockchains are usually much better since they don't depend on proof-of-work to build up consensus, their condition is more trusted.

Consortium blockchains are some of the time called shared permission blockchains and privately called permission blockchains. The key thing to know is that one is totally open and public. One limits to a couple of potentially competing entities and the last, to a couple or one trusted entity.

12.1 Blockchain interoperability.

Interoperability refers to the possibility of blockchains that can cooperate with each other. Throughout this paper, it has been that discussed each different blockchain as an ecosystem unto itself separated from all the others. However, efforts are taken to interweave blockchains with each other to offer services that work more transparently from one to the next.

For instance, there could be an application on the Ethereum blockchain that works with Bitcoins and does so transparently for a client. The main thing to tolerate as a primary concern here is that blockchains need not be Islands detached from one another, there are numerous projects in progress that integrate distinctive blockchains in novel and ground-breaking ways.

13. WHY BLOCKCHAIN

Blockchains offer humanity, essentially the next generation of the database. This is a period where customers of businesses or citizens of governments essentially allocate their digital assets and their personal information to either those businesses or those governments.

We create an adversarial environment whereby if I am a client in the business, I have to log into their turf and house all of our transactional and personal data on their environment. In the future, we're essentially creating a mesh network of having the database and the Internet be one such thing. We will be able to have multi-sided marketplaces, where instead of having to pay an intermediary to provide trust we are now evolving to trusting the software. There are two major distinguishing pieces of a technology upgrade that we're dealing with. One is the ability to digitize assets. In the future, there will be natively digital representations of assets. That means that there will be tokens that could signify fee out, stocks, bonds, derivatives, insurance policies, software licenses, credit card points, concert tickets.

The other technology upgrades that we're going to have due to blockchains is the ability to have Smart Contracts, which are neither smart nor contracts but basically, they are software objects that ease the ability for humans, and earth

and businesses to essentially agree much easier. This will lead us to re-structure the way our legal, financial, and social operating systems work.

14. WHEN TO USE A BLOCKCHAIN

In this section, the kinds of business problems that are best solved with blockchain are discussed. For all the hype around blockchain technology, it cannot do everything and it must not do everything. However for the things it can do well, it's unprecedented.

A decision tree is given in figure 5 includes the kinds of questions to ask when trying to determine whether we should be using a blockchain at all. If we should, what kind of blockchain we should be using, whether that's public, shared or consortium, or private.

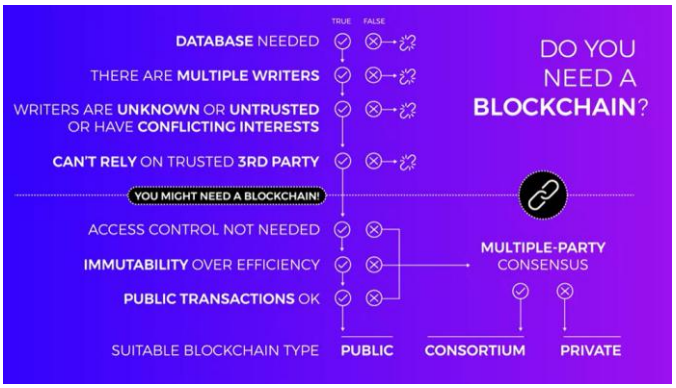

Figure 5

Let's consider an example, you're an executive and you're trying to determine if a blockchain is a right solution for a project that you have.

1. Database

The first question to ask about the project is, Is there a need for a database?BitTorrent, for instance, is a peer-to-peer document sharing network that doesn't have a database, so it wouldn't require a blockchain.

2. Multiple authors

Next, ask, does it require shared right access? The function of blockchain is to spread the power to write among a group with no one group controlling access. In the event that there is no compelling reason to impart shared right access to numerous individuals or groups, there is no requirement for a blockchain. For example, if an organization wants to collect traffic information and sell it, There is no need to have multiple groups that write to the database, so it doesn't need a blockchain.

3. Absence of trust

Until now, we have separate parties and we need to write to a database. So the question, "Are any of the parties unknown or untrusted? Or even if they're trusted, are there any chances for them to have clashing interests?"On the Bitcoin blockchain, people have clashing interests since they remain to pick up from an invalid exchange that works in their favor. So, in the event that you know and trust all the parties and you realize that everybody's advantages are bound together, at that point you needn't bother with a blockchain. For instance, assume three water organizations need to keep up a shared database of contamination levels across different sources. They all trust one another and every one of their interests is unified, they likely needn't require a blockchain. Incase if all parties aren't known or trusted, or they yet have potentially clashing interests, consider whether you could depend on an intermediary to control the database, or review it. If that is achievable, you needn't require a blockchain.

For instance, three successful furniture resellers give consent to a shared database of providers. But they are they are altogether ready to trust an intermediary to deal with the database. This intermediary is a third party yet they all trust it, so they needn't bother with a blockchain. However, in the event that you can't trust a third party, after all of that, you're at last ready to begin talking about blockchains. To recap, we have a business issue or task that needs a database, requires shared access among parties that may not be known or trusted or may have contending interests, furthermore, it's not pragmatic or workable for an intermediary to be trusted to deal with the database.

4.Few more questions to ask

Is there a need to control access and usefulness and will only one gathering confirm data without agreement inside in a high trust environment? If in this way, a private consent blockchain will work. That is a blockchain worked by you and your association. This is truly only a circulated record and it's not very blockchainy.

In the event that you need to control usefulness, however, the agreement must be reached by various gatherings, that is different substances will be confirming, writing, and examining information on the blockchain alongside you, then a mutual or consortium, or on the other hand shared authorization blockchain is the thing that you need to use. In this case, a gathering of perhaps contending elements share access and utilization of a blockchain database. If you don't need exchanges to be openly perceptible, you'll need a non-private blockchain of some kind, whether that is private or consortium.

To wrap things up, the public blockchain. In this one, you don't control functionality, and all exchanges are public. Anyone can go along with it and use it. But being public, you're managing unknown and untrusted substances writing to the blockchain, so incredible consideration must be taken to make sure a strong system of consensus mechanism is set up to keep the blockchain secure. By contemplating issues in this way and pondering the choices here, we can begin to discover whether a blockchain makes sense as well as provide the answer for a business issue.

15. IMPLICATIONS OF BLOCKCHAIN IN BUSINESS

As mentioned earlier, blockchain cannot solve every problem and it mustn't. With all the hype around blockchain and its application in cryptocurrency, it should be noted that blockchain can do much more than cryptocurrencies. This

section deals with the applications of blockchain in businesses. In figure 6 the various categories in which blockchain yields potential benefits are given.

Figure 6

15.1 SMART CONTRACTS:

The term 'smart contracts' was first termed in 1993, however, it's as of late become a buzzworthy term after the arrival of the Ethereum Project in 2013. The Project is a decentralized platform that is able to run smart contracts: applications that are capable of running precisely as programmed with no chance of fraud, downtime, censorship, or intermediary interference. Businesses will have the option to utilize 'smart contracts' to bypass regulations and lower the expenses for a subset of our most common financial exchanges. Also, the best of everything is these contracts are unbreakable. Organizations like Slock, which is an Ethereum-empowered web of-things stage, utilize this application to permit the client to lease bikes where they can open a smart lock after the two groups accepted on the terms of the contract.

15.2 CLOUD STORAGE

Cloud storage is another application that businesses can gain an advantage of. Storj is one such organization that is providing secure cloud storage while reducing dependency.

15.3 SUPPLY CHAIN MANAGEMENT

The immutable ledger of blockchain has made it well suited to services such as real-time monitoring of goods as they move and change hands throughout the supply chain. With the use of blockchain, several options are made available for companies in transporting these goods. For instance, the entries on a blockchain can be used to line up events with a supply chain-assigning goods newly arrived at a port to various shipping containers. A new and dynamic means of organizing tracking data and putting it to use is provided by blockchain

15.4 HEALTHCARE

Basic medical history like immunization history or vital signs and general information like age, gender can be stored in shared blockchains because none of this information would be able to particularly identify any specific patient and could be accessed by numerous individuals without any privacy concerns.

15.5 ENERGY

Energy supply transactions can also be executed by blockchain technology. Document ownership, asset management, origin guarantees, emission allowances, and renewable energy certificates are the other potential applications of blockchain technology in energy.

16. CONCLUSION

In this paper, we have seen the history of blockchain, its fundamental concepts with examples, and the applications of blockchain in various business applications. To recap, a blockchain is based on Distributed Ledger Technology (DLT) that is secured with the use of cryptography, by utilizing trusted, public, and private key signature technology. The alternative way to store data on a centralized database is blockchain technology. Blockchain technology is transparent and verifiable and it allows everyone who is signed into it to view a unified source of present and past data. DLT also increases the efficiency, speed, and accuracy of transactions, reducing disputes, and the need for third parties. Finally, the blockchain's distributed architecture is more resilient, and since there is no point of failure it also reduces the ability for hacks to happen. Blockchain is at the most hyped stage right now, it is our responsibility to people about blockchain technology and make them truly understand it.

REFERENCES

[1] Michael Crosby and Nachiappan, "Blockchain Technology: Beyond Bitcoin" AIR, issue 2, June 2016.

[2] Andreas M.Antonopoulos, Mastering Bitcoin, O'Reilly media.

[3] Advait Deshpande and Katherine Stewart, "Distributed ledger technologies/blockchain" BSI, May 2017.