International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Blockchain Technology: An Overview

Murlidhar[1] , Dr. Vishal Srivastav[2], Dr. Akhil Pandey[3]

[1]B.TECH. Scholar, [2]Assistant Professor,[3]Professor
Artificial Intelligence & Data Science
Arya College of Engineering & I.T. India, Jaipur
[1]murlidharverma2005@gmail.com, [2]vishalshrivastava.cs@aryacollege.in, [3]akhil@aryacollege.in

1. ABSTRACT:

Blockchain technology is a way to securely and transparently record transactions across a network of computers. It functions as a distributed, decentralized ledger that uses cryptographic security, a consensus protocol, and immutability to ensure that new data can be added without the risk of deletion or alteration. Initially created for Bitcoin, blockchain technology has broadened its applications beyond cryptocurrencies to fields like finance, supply chain management, healthcare, and smart contracts. Some of the main benefits include improved security, a reduced need for intermediaries, greater transparency, and quicker execution of electronic transactions.

Keywords: Blockchain, Bitcoin, Tiers of Blockchain, Public, Private

2. Introduction

A blockchain is basically a digital ledger where various block pieces of transactional information are connected in a secure chronological and immutable manner. A ledger is like a single continuous file that contains current transactions. Once transactions are put into a blockchain, they become part of this ledger column. Those transactions stay safely inside the blockchain. Its cryptographic setting seems so highly locked away that the content therein is kept safe from any external interferences. By chronological transactions, we mean that one transaction cannot go without a transaction happening before it. Another is that once you build a ledger, you can't change it again, once a transaction is added to it. A blockchain is a chain connecting all the blocks containing information, namely any recent transactions. Once this is completed, the block goes onto the blockchain as a permanent database. Each time a block is completed, it generates a new one.

Not only money transfer, lease of properties, and contracts, etc., can be carried out through the blockchain and the digital currency; it happens nit that mediation authority in between is of banks or governments. A protocol of blockchain is software whereby the working of it cannot be efficiently changed without the Internet, for example, SMTP for emails. The application of blockchain technique spans diverse fields. The central use of the blockchain is as the shared ledger for cryptocurrencies, but much more potentials could span banking and investment, governmental transactions, public health and social security, and supply management.

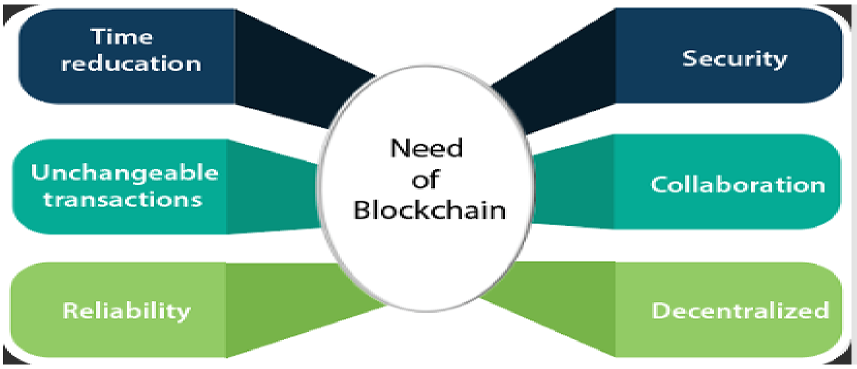
3. Literature Review

Need of Blockchain:

The key features lately that stimulate blockchain technology by time reduction, immutable transactions, reliability, security, collaboration, and decentralization.

Time Reduction: it was responsible for achieving a substantial reduction in settlement time of the trades involving boring levels of verification, settlement, or clearance in financial systems. Every interested party gets to share with each other one version of the agreed-upon data.

Immutable Transactions: Transactions that enter the blockchain are chronologically added to the ledger in a way that allows for no possibility of altering it. Once a new block is inserted into the chain of ledgers, it neither gets modified nor deleted.



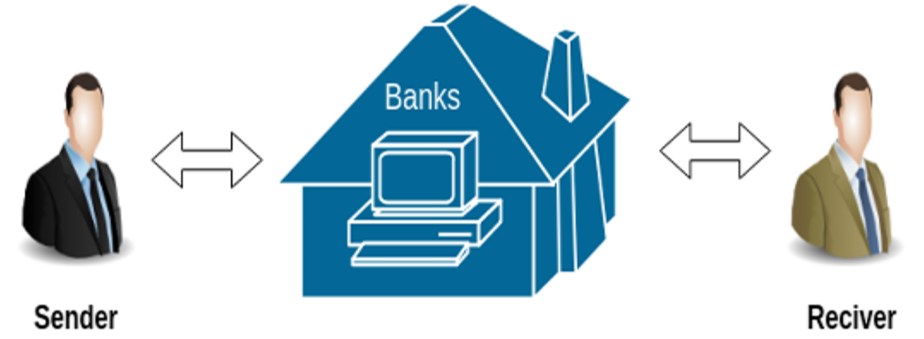
Reliability: The identity of the party of interest in a transaction is checked by blockchain. This removes duplicate from the registry and allows to lower transaction costs while effecting the deal in less time. Security: Blockchain uses strong encryption practices to ensure that information within the blockchain...It uses Distributed Ledger Technology, which allows for one copy: each party has a copy of the original chain, so it does not stop working even if many other nodes go down.

Collaboration: It allows for direct transactions and interactions between all parties without intermediaries. **Decentralized:** The other name for this is decentralized because this cannot be supervised by any central authority under this system, and all will comply with the general rules on how each node exchanges blockchain data. This guarantees that all the transactions are verified, hence ensuring valid transactions are sequentially appended to one another.

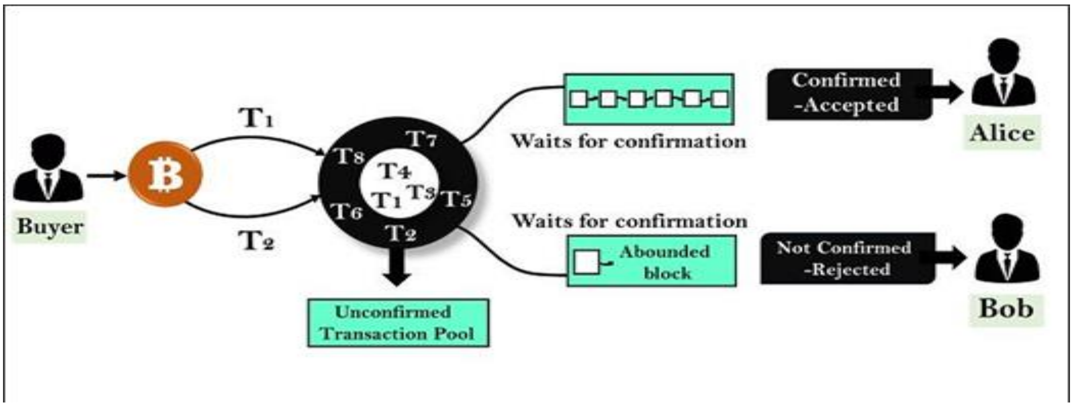
Bitcoin in Blockchain:

Bitcoin was introduced by the media in a presentation by Satoshi Nakamoto in 2008. It is called a cryptocurrency, a virtual currency, or digital currency governed by rules and procedures based on cryptographic findings that allow for the issuance and regulation of currency." It set the stage for entry into their system for the cryptocurrency camp. This is why Bitcoin is referred to as the first and foremost and is still the most valuable as of today. Bitcoin has also been defined as a decentralized digital currency that allows for the transfer of those digital assets between two parties for buying, selling, and transferring. Bitcoin is also used to store values like fine gold, silver, and other investments. It is used to purchase goods and services, make payments, and exchange values over the internet. This bitcoin is not to be confused with the dollar, pound, or euro; these traditional currencies also play an important role when it comes to the exchange of goods and services into digital value electrons. There are no coins that one can hold on to, nor do we have paper bills. There is no requirement for you to go through a bank, a credit card, or any third party if you want to send someone bitcoins or buy something using bitcoins. You can send them directly over the internet to the desired party securely and almost instantly." Bitcoin Works: Just like sending an email or an instant message. It's person-to-person communication. This interference is called pressure for a peer-to-peer. Whenever we send money over the internet, we relay on third-party services, such as banks, credit cards, PayPal, and money transfer services. You need a third party trusting in the transaction to make sure you really sent the money.

In other words, at each transaction-done-spent, the two parties need to check and verify that they fulfilled their part in an actual exchange. For instance, let us say that I want to send a capture image to someone. The easiest way for me to do so is to attach it to an email, type the recipient's email address, and send it. The other person receives that image, and I thought that ended it, but no. That is to say that we now have two copies of that image-an email picture and an original one in my computer. That being said, we have sent you the copy of the file-Picture, with the original still remaining in my computer. This problem is popularly known as the double spending problem. Double spending refers to the problem of human gullibility in telling whether the transaction was real or not, and this is exactly how you send a bitcoin to somebody through the internet without a central bank or other institution verifying that the transfer took place. This solution is developed in a global network of thousands of computers called a Bitcoin Network and another special one called Blockchain: a decentralized counting base.



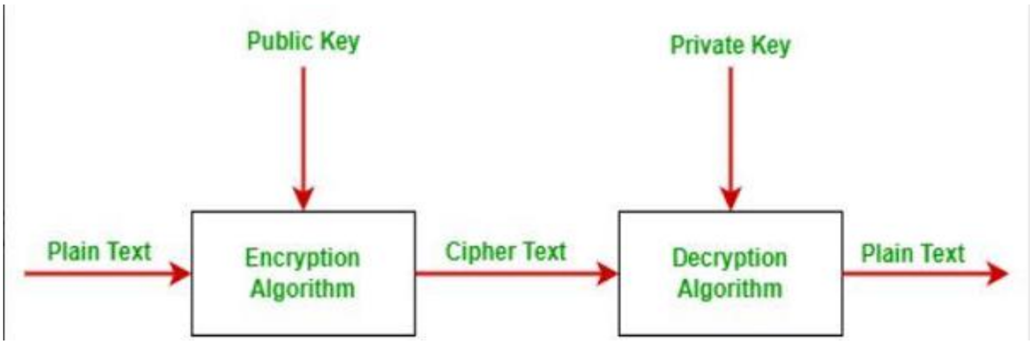
All the information concerning transactions is captured mathematically through a secure cryptographic process, further stored on all computers within the entire network for validation. Simply put, Bitcoin employs Blockchain technology across a decentralized network of computers able to safely verify and confirm each transaction, rather than relying on a centralized third-party database, like banks, to substantiate the existence of a transaction. It cannot be hacked or tampered with, and the moment it is hacked or tampered with, the blockchain becomes insecure and difficult to alter. **Double spend Problem in Blockchain:** The distributed decentralized network is solely responsible for data control-without control by any other authority. Thus, blockchain becomes safer, less prone to fraud, tampering, and systemic failures compared to centralized storage of data. In short, it has an inherent double-spending problem. To solve the double-spending problem, Bitcoin implements a confirmation mechanism built into the universal ledger called the blockchain. When you try to use your 1 BTC twice, you would first send this 1 BTC to Alice.



you also signed and sent the same 1 BTC to Bob. Both transactions would then land in the pool of hanging transactions, which is the repository for unconfirmed transactions. Those are transactions not yet approved by anyone. Thus, whichever transaction gets enough confirmations and is verified by miners first will always turn out to be valid. The other transaction having not enough confirmations is discarded from the network. In this case, transaction T1 was valid, and Alice received the Bitcoin.

Public-Key Cryptography:

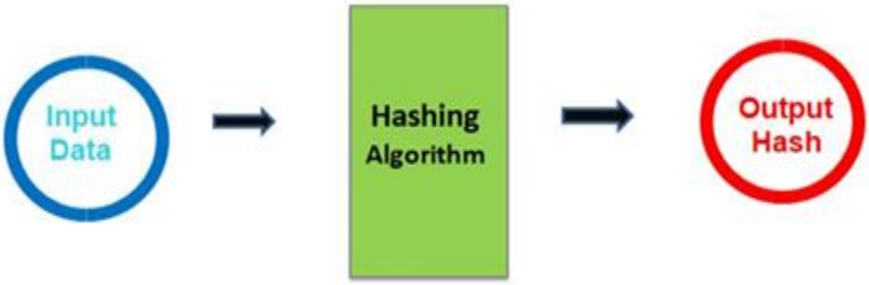
There is a vast approach called public-key Cryptography, which is using mainly in the blockchains. This cryptographic way is also known as asymmetric-key cryptography, based on the use of public and private keys for encoding messages, decoding messages, and signing data. Its common attributes of public key and private key create a mechanism with two sides in relations to the public. Basically, a public key is provided in the public domain while nobody can notice the private key. It mostly acts a lot like a tortuously encrypted tunnel of communication between two parties wherein both can be users or servers connected usually on the web with relatively delicate matters to handle when it comes to security.



Public Key: Public keys are meant to be shared widely and openly over the internet. It is used to allow encrypting a plaintext into ciphertext. It can be taken to authenticate the sender, in a way signalling that it can validate the opening of a lock on a door.
Private Key: Private key is indeed totally against the layer behind public key. It is a prime distinct of putative use in delete presentations. This key applies a conversion of the cleverly written code into simple plain text.
In simple terms, it could be said that the private key is used like the lock to open. Symmetric is, instead, used for both the high and the lower ends in encrypting or decrypting messages. This very point presents a whole scheme for data loss or unauthorized access to data. Any unauthorized access by public key cryptography is switched on using this schema for secure data transmission without the fundamental issue of data loss. It's just much superior to symmetric key cryptography, where two sets of encryption and decryption keys are needed to make the communication. Public key cryptography allows users to exchange data that do not want to be intercepted. The sender encrypts the message, and once it reaches the other end, the recipient decrypts it through some secret knowledge. The unauthorized user would therefore be able to give no meaning to the encrypted message. Suppose the sender wants to send some important messages to the receiver. Thus the first thing he needs to do is to write a plain text of the message.
Because the private key is kept secret by Anurag, the sender only knows Anurag's public key and not the private key. The sender forms the cipher text or encrypted message by using Anurag's public key along with his own private key. Cipher text exists in a form not suitable for comprehension. It occurs now that cipher text reaches the receiver end. The receiver uses her private key to revert the cipher text into an understandable or plain text. In order to have a better idea of the operations of public-key cryptography, here is an example. So in this exercise, you also get to see an example of public-key cryptography. Suppose Sachin is a sender of a message and Anurag is the receiver. Sachin uses Anurag's public key to encrypt the message, and Anurag uses his own private key to decrypt it. Anurag has Sachin's cipher text, and thus only Sachin could have encoded plain text onto that cipher text. The plain text undergoes encryption to finalize cipher text. Currently, Anurag obtains a cipher text. First, in deciphering the cipher text message, he would give it a readable format. Anurag will use the private key to decode. The cipher text would assemble to a plain text form that the intended receiver can read. Anurag knows that this message couldn't have come from anybody else since Sachin is the sole possessor of the private key. Thus, it is, hence, also known as a digital signature.

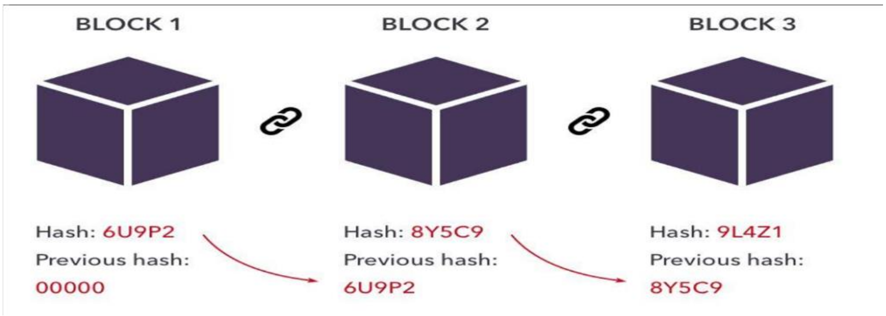
Hashing:

To ensure the block message security, the blockchain uses a cryptographic hash algorithm to connect each block into the chain, thus making an unbreakable chain. In a blockchain, each block holds the hash, combined with the hash from the previous block, making a linear chain of blocks that is cryptographically secure. Hashing is the function of taking any input string, no matter what length, and producing a cryptographic output of fixed length. Hashing is definitely not encryption, as there is no “reversing” or “decrypting” the hash; it cannot be undone, rather it is a one-way function in cryptography. Did you know that Hashing Algorithm can help to keep all the data available on the internet in fixed string length? The algorithm used is SHA-256 (Secure Hashing Algorithm- 256 bits). SHA 256 is the successor of SHA-1, a secret algorithm working on 160-bit data.



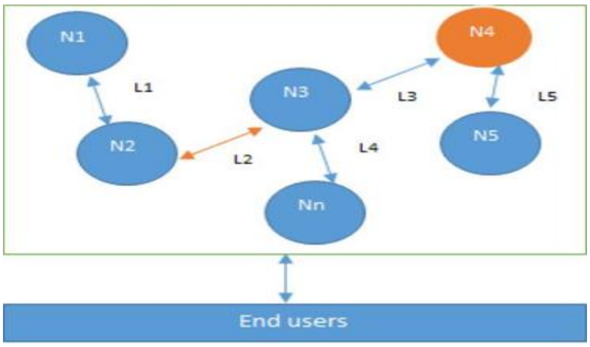
Blockchain hashing is what seems to be a predetermined process of making an input of any given length turn into an output of a defined character length. If blockchain technology is being used, transactions of various lengths are processed using a method of hashing so that the outcome of each hashing is put in a defined character length. This, on the other hand, particularly applies to all transactions, irrespective of transaction length, data size, and complexity level. It is indeed true how very long the input transaction becomes. The output has been described as the hash. SHA-256 has been a famous example for Bitcoin. When it comes to hashing using SHA-256, regardless of what the data in the transaction is; the output is always 256 bits or 32 bytes. Regardless of whether the data in that transaction consists of some words or is huge, the output length will always be 256 bits when hashing using SHA-256. This means that whenever you can remember a hash, keeping track of a transaction becomes easier.

It is not the same for each hashing function. Hence, each hashing function will always produce a hash value having fixed lengths: one such hash value is a data part, while others are hash values of the previous blocks. These include data, hash, and a hash value of the previous block.



Distributed System in Blockchain:

With DLT systems such as a blockchain, great opportunities arise for instituting and reliably maintaining trust-based relationships among many stakeholders. These distributed systems, forming part of the digital technologies stack, would facilitate the creation of shared data sets and coherence between industries that eliminate the choke points that partners would otherwise attempt to block. Essentially, the blockchain is a distributed framework. They usually have problems in gaining a sense of mutual confidence and assurance, and often finding it takes quite a long time for certain transactions to get authorized. We [gemtech] want to continue to evaluate the business value of distributed systems such as DLT to our target sectors and the factors/conditions that will favor such technology adoption beyond just early-phase projects. Documents such as the contract and accompanying papers for cooperative negotiating between parties can be turned into a digital format. Thus, there would be far less time required for building trust in inter-organizational agreements. This means that at its heart, blockchain is a distributed environment. Distributed Systems are computing paradigms in which two or many nodes work in coordination to achieve a common objective, while by choice, an eager user sees the whole network as a single logical entity. A node is defined as an individual or device expected to run that distributed system. Individual nodes communicate with each other by sending and receiving messages. Nodes may be honest, faulty, or outright malicious, and they can have their computing and storage devices. A node, William. A Byzantine node refers to such nodes that may exhibit arbitrary behavior in that distributed system.

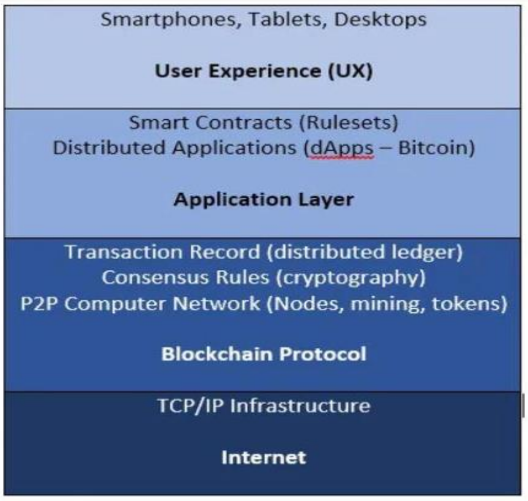


In colloquial terms, Byzantine essentially refers to the behavior of nodes that can be treated as arbitrary in this context. By definition, this is generally any behavior that raises suspicions: actions against the operating principles and practices of the network. The area is full of research that extends for several years, with numerous mechanisms and algorithms proposed to tackle these issues. Coordination between nodes and toleration of faults amounts to being the challenges in this context while designing the distributed system. For example, among these failures are Byzantine nodes; nodes having some failures or changes in performance; faults in links; or in some circumstances slow communicating links. Hence distributed systems must be able to withstand failures and operate correctly under conditions such as Byzantine node failures and link failures. Such an extensively researched area, therefore, indeed led to many algorithms and solutions to tackle these problems. Also, due to organizational orders, it has become impossible to have a theorem basically called the CAP theorem that says "You may not have all properties anymore."

Technology Stack of Blockchain:

Each technology stack represents a set of computer programs and developer tools used for designing and implementing software application projects. These constitute the basic platforms and protocols, that is, the tech stack employed by the applications forming the basis of a reasonably defined blockchain enterprise. The Web 3.0 tech stack is eclectic, widely different from Web 1.0 and Web 2.0 stacks. Distributed ledger technology forms one of three basic technologies at the backbone of blockchain. In simple words, the distributed ledger is a type of centralized database spread out on many computers in a form of a chain with a certain measure of decentralization and transparency involved. DLT is the foundation of blockchain technology, which is used for data storage and transaction recording across the network nodes. Cryptography is a method used to protect information and secure data. The primary purpose of cryptography in the blockchain is for securing payment transactions against fraud. A smart contract is self-executable when the terms and conditions behind it are met. This helps boost the working performance by enabling the two parties to settle directly without requiring intervention from a third party. They are sealed contracts immune to falsification.

User Experience: One of the top layers of the blockchain technology stack is responsible for the integration of all underlying technology development into various user applications that people see and use in their daily lives. Most Dapps are developed for less technical purposes and need special Dapp browsers visible on the users' devices. Potential Usage of Blockchain Applications is boundless; they will remain numerous yet in the process of development until you find the right one for your users to operate.
Layer of Application: In recent years, many blockchain applications have emerged; however, Bitcoin was, and is, the original and preeminent application intended to solve the problem of a protocol for blockchain technology. The Bitcoin network has largely been utilized in the centralized financial sector, with banks, resolution agencies, and other types of financial intermediaries acting primarily in this space. The DAO was invented in response to the idea of transferring value more impartially..


Smartphones, Tablets, Desktops
User Experience (UX)
Smart Contracts (Rulesets)
Distributed Applications (dApps – Bitcoin)
Application Layer
Transaction Record (distributed ledger)
Consensus Rules (cryptography)
P2P Computer Network (Nodes, mining, tokens)
Blockchain Protocol
TCP/IP Infrastructure
Internet

Blockchain Technology Stack

4. Tiers of Blockchain:

The final description of the evolution of blockchain technology and its versions from 1.0 to 3.0 is given below.

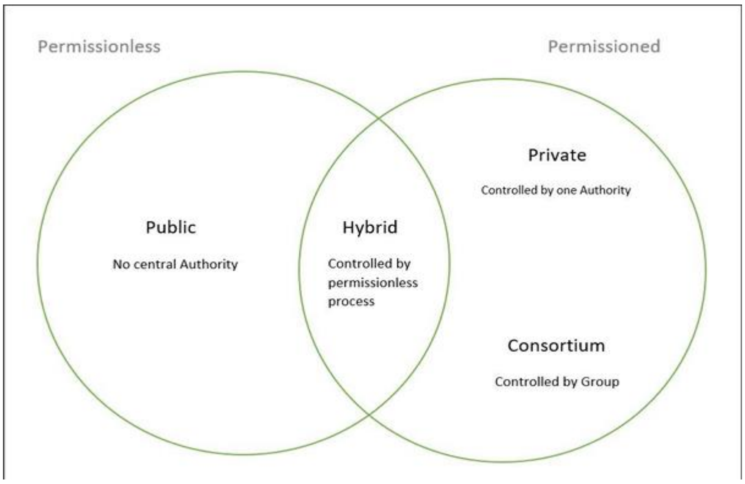
Blockchain 1.0: Currency : The first blockchain Bitcoin is always associated with Blockchain 1.0. Bitcoin is a digital currency for transferring values, peer-to-peer electronic payments. It introduced the decentralized and trustless model of making transactions without any third party mediators such as banks. Blockchain 1.0 aims at facilitating security and transparency in financial transactions, thereby enhancing its applications for store of value. Immutability, proof of work consensus mechanism and basic programmabilitits are its key features. Money created came from solving the computational puzzles, a concept first introduced in 2005 by Hal Finney, and then came up with the first conception for crypto currency (Implementation of distributed ledger technology). Distributed ledger technology executes transactions regarding the blockchain in Bitcoin. Within this season bitcoin.; the creation of Bit-Coin is taken as one of the examples in the protest or Internet cash in enabling the Internet of Money service.

Blockchain 2.0 and Smart Contracts: Mining in Bitcoin has become wasteful and cannot scale. It is really an attempt to go beyond Bitcoin and currency and propose Smart Contracts as the new building block. They are programs that are "living" in the Blockchain. They are free computer programs that self-execute and verify the conditions set forth previously to enable, confirm, or enforce them. However, this technology comes with great promise because the Smart Contracts cannot be tampered with or hacked, which is what blockchain will guarantee. BlockChain 2.0 has replaced BitCoin so highly that it has successfully absorbed a high number of transactions in a faster way on the public network. Ethereum blockchain is one of the best examples. It provides a platform to the developer community to build distributed applications for the Blockchain network.

Blockchain 3.0: DApps: DApps is also known as a decentralized application. It relies on decentralized storage and decentralized communication. The backend code is executed in a decentralized peer-to-peer network. A DApp may have front-end code residing in a decentralized storage system such as Ethereum Swarm, which uses any user interface language capable of connecting to its backend, much in the same way as an ordinary app.

5. Types of Blockchain:

Blockchain can also be categorized into different classes based on their evolution over the years and how each one is characterized-different from and in some cases overlapping with others.



Public blockchains: As indicated by the name, these refer to an open blockchain that allows anyone to take part as a node in decision-making. The user might or might not be rewarded for the participation. These ledgers are not owned by anyone, and everyone has access to them. At present, for a permission-less ledger, each of the users closely monitors a copy of the ledger on their respective nodes and uses a distributed consensus mechanism to decide on the final state of the ledger. Otherwise, they are often referred to as permissive ledgers.

Private blockchains: These kinds of blockchains are private and accessible only to members of a consortium or group of individuals or organizations that set out agreements to share the ledger amongst themselves.

Semi-private blockchains: In such blockchains, part of it will be private and part of it will be open to the public. The private part will be governed by a certain group of individuals while the public part is accessible for any individual to participate in. A semi-private blockchain, or consortium blockchain, basically combines the best of both public and private: it is shared between a group of known and trusted entities, e.g., companies in a specific industry or partners in a consortium.

6.Conclusion

The user-friendly definitions of what to perceive Blockchain technology as would portray: Blockchain is some revolutionary technology with enormous possibilities beyond their thrust into the world of crypto-currency; its features-decidedly decentralized, absolutely transparent, and thereby safe-seem most credible in transforming industries such as finance, supply-chain management, healthcare, and governance. The immutable character of record keeping coupled with the removal of intermediaries has ensured a great sense of security and efficiency for blockchain in the current digital ecosystem.

Mass adoption faces challenges such as scalability, energy consumption, regulatory concerns, and interoperability. On the other hand, recent pursuits and technological advancements, which include the integration of AI in conjunction with much more efficient consensus protocols, are bound to spur the growth of the technology.

In conclusion, the struggles of blockchain-a disputed issue; some people have said this to be the rebirth of many traditional systems-are sometimes worthy mentions in the context. The nimble technologies captured the attention of the various industries to be explored, analyzed, and solutions sought.

7. REFERENCES

1. Beal, V. (n.d.). Public-key encryption. *Webopedia*.
2. Cipher. (2014, May 25). The current state of coin-mixing services. *Depp.Dot.Web*.
3. Dawson, R. (2014, September 16). The new layer of the economy enabled by M2M payments in the Internet of Things. *Trends in the Living Networks*.
4. Gartner. (2013, December 12). Gartner says the Internet of Things installed base will grow to 26 billion units by 2020. *Gartner Press Release*.
5. Hajdarbegovic, N. (2014, June 30). Deloitte: Media 'distracting' from Bitcoin's disruptive potential. *CoinDesk*.
6. Hof, R. (2014, June 20). Seven months after FDA slapdown, 23andMe returns with new health report submission. *Forbes*.
7. Nakamoto, S. (2009, January 9). Bitcoin v0.1 released. *The Mail Archive*.
8. Omohundro, S. (2014, October 22). Cryptocurrencies, smart contracts, and artificial intelligence. *AI Matters* (Association for Computing Machinery).
9. Rizzo, P. (2014, September 26). Coinify raises millions to build Europe's complete Bitcoin solution. *CoinDesk*.
10. The Economist. (2012, May 19). Remittances: Over the sea and far away. *The Economist*.