International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 5 Issue 4, May-June 2021 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Blockchain and Beyond

Nandan Chitale[1], Yogeshchandra Puranik[2]

[1]PG Student, [2]Assistant Professor,
[1,2]Affiliated to Department of (MCA), P.E.S. Modern College of Engineering, Pune, Maharashtra, India

ABSTRACT

A blockchain is essentially a distributed database of records or public ledger of all transactions or digital events that have been executed and shared among participating parties. Each transaction in the public ledger is verified by consensus of a majority of the participants in the system. And, once entered, information can never be erased. The blockchain contains a certain and verifiable record of every single transaction ever made. Bitcoin, the decentralized peer to peer digital currency, is the most popular example that uses blockchain technology. The digital currency bitcoin itself is highly controversial but the underlying blockchain technology has worked flawlessly and found a wide range of applications in both the financial and nonfinancial-world.

The main hypothesis is that the blockchain establishes a system of creating a distributed consensus in the digital online world. This allows participating entities to know for certain that a digital event happened by creating an irrefutable record in a public ledger. It opens the door for developing a democratic open and scalable digital economy from a centralized one. There are tremendous opportunities in this disruptive technology and revolution in this space has just begun. This white paper describes blockchain technology and some compelling specific applications in both the financial and nonfinancial- sector.

KEYWORDS: *Blockchain Cryptocurrency crypto currencies bitcoin etherium proof-of-work mining bitcoin-mining proof-of-steak revolution Hashcash Smart Contract encryption hash security transaction digital*

How to cite this paper: Nandan Chitale | Yogeshchandra Puranik "Blockchain and Beyond" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-5 | Issue-4, June 2021, pp.874-878, URL: www.ijtsrd.com/papers/ijtsrd42425.pdf

IJTSRD42425

INTRODUCTION

A blockchain is certainly a ledger of transaction where each transaction recorded is validated by the majority of the consensus and is stored permanently over a digital network. Bitcoin and Etherium are some of the most popular implementations of blockchain technology.

Some innovations, technologies are disruptive, meaning that they change the traditional way that an industry operates, especially in a new and effective way. Some of the popular examples are Internet, Cars, Computers etc.

The current banking system is centralized; meaning that we need to trust the central authority (Bank) to perform all of our transactions. If we want to transfer the specific amount to another account, the bank keeps all the records and is known as the Ledger. Whenever a transaction happens, the bank records that transaction in the ledger with details associated with it like the amount to be transferred, the mode of transaction, who is sender and who is receiver etc. But what if someone hacks into this central system and alters some of the transactions. Let's say A sends an amount of INR 10 to B, the bank records the transaction saying that A is sending money to B. Now the banks for their convenience, reduce that amount from A's account (, and add the same amount to B's account saying that the transaction is now complete. The bank keeps this transaction's records in A's and B's individuals ledger entries. But let's say that C hacks this central banking system and modifies the transaction like instead of adding an amount to B's account, he adds the amount into some other account which is beneficial to him. Now from A's perspective, his part in the transaction is complete as he trusts the bank to transfer the amount to B's account. But B blames the bank for not getting his money. From the hacker's perspective, it is easy to alter such transactions. But what if there is another way to secure such transactions without trusting any central authority to do the work. What is there is a way to secure the transaction so that to modify the transaction, it will take billions of years to modify it. What if there is a way that instead of trusting the bank (The central authority) to verify the transaction, there are a bunch of people say thousands of people participate in verifying the transaction. Blockchain offers answers to all of these questions.

History of Blockchain:

Milton Friedman was one of the most renowned economists of the 20th century and his ideas radically changed the way that policymakers made their decisions.

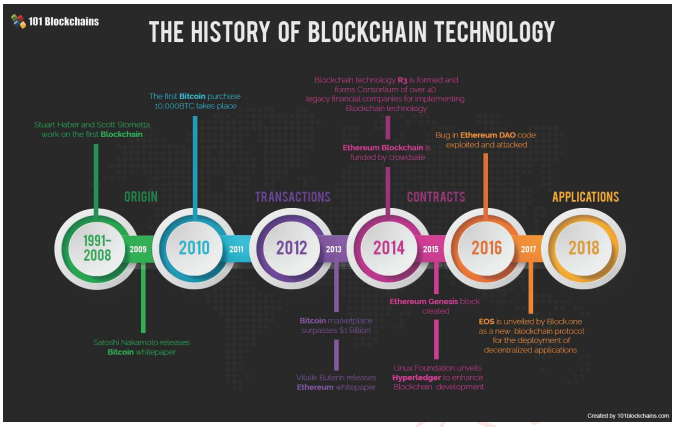
Friedman foresaw that bitcoin, or something like it, could have great advantages and would inevitably be developed – much to the animosity of incumbent institutions in the financial world.

What Friedman had in mind when he proposed the idea of digital cash, however, was reducing the need for a third party in transactions. He said that "The one thing that's missing, but that will soon be developed, is a reliable e-cash,

a method whereby on the Internet you can transfer funds from A to B, without A knowing B or B knowing A."

It seems that Friedman knew the decentralization of money would arrive one day. But it's not so certain that he willed it to happen.

Cryptographer David Chaum first proposed a blockchain-like protocol in his 1982 dissertation "Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups." Further work on a cryptographically secured chain of blocks was described in 1991 by Stuart Haber and W. Scott Stornetta. They wanted to implement a system where document timestamps could not be tampered with. In 1992, Haber, Stornetta, and Dave Bayer incorporated Merkle trees to the design, which improved its efficiency by allowing several document certificates to be collected into one block.



The first blockchain was conceptualized by a person (or group of people) known as Satoshi Nakamoto in 2008. Nakamoto improved the design in an important way using a Hashcash-like method to timestamp blocks without requiring them to be signed by a trusted party and introducing a difficulty parameter to stabilize the rate with which blocks are added to the chain. The design was implemented the following year by Nakamoto as a core component of the Cryptocurrency bitcoin, where it serves as the public ledger for all transactions on the network.

In 2008, an individual or group writing under the name of Satoshi Nakamoto published a paper entitled "Bitcoin: A Peer-To-Peer Electronic Cash System". This paper described a peer-to-peer version of the electronic cash that would allow online payments to be sent directly from one party to another without going through a financial institution. Bitcoin was the first realization of this concept. Now word crypto currencies is the label that is used to describe all networks and mediums of exchange that uses cryptography to secure transactions-as against those systems where the transactions are channeled through a centralized trusted entity.

The words block and chain were used separately in Satoshi Nakamoto's original paper, but were eventually popularized as a single word, blockchain, by 2016.

Structure of Blockchain:

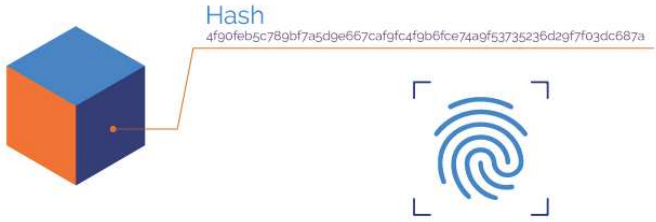
Blockchain is a decentralized, distributed and oftentimes public, digital ledger consisting of records called blocks that is used to record transactions across many computers so that any involved block cannot be altered retroactively, without the alteration of all subsequent blocks. This allows the participants to verify and audit transactions independently and relatively inexpensively.

Block in Blockchain:

A block can be said as a piece of data which contains a batch of transaction details. These transaction details are hashed and are encoded into a merkle tree.

Each block includes a cryptographic hash of the prior block which defines the linking between two blocks. This linking of the block forms a chain, thus Block - Chain.

A unit of data stored inside a block may be represented by any value depending on the type of blockchain. A block can store an amount of money, a share in a company, a digital certificate of ownership, a vote during an election, or any other value. A block stores encrypted details about the parties whose interaction resulted in the data stored in the block. A cryptocurrency block also contains the sender's and receiver's encrypted identifiers. A block for an ecommerce transaction will contain the identifiers of the retailer and consumer, for example.



Each block also has a hash. This hash is a value generated from a string of text using a mathematical function. A hash can be compared to a fingerprint, as each hash is unique. Its role is to identify a block and the block's contents. Once a block is created, its hash is calculated using hashing algorithms. The hash generated is depending upon the data inside the block. Meaning that if data inside a block changes, the hash value generated for that block will also change accordingly. So change in hash indicates that someone is trying to change the data inside the block. Hence proving the security of that block.

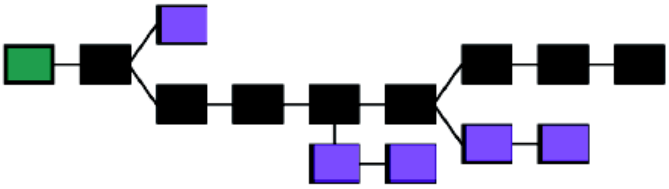
If anyone changes the data in a single block, the hash of that particular block changes, but it also makes the whole chain invalid.

A hash is a great tool for identifying attempts to change data in blocks. However, a hash algorithm alone is not enough to ensure the security of a blockchain.

It is the method through which a transaction is validated. Each blockchain can have a different consensus method attached to it. For example, Bitcoin utilizes Proof-of-Work (PoW), whereas Ethereum uses the Proof-of-Stake (PoS).

Consensus algorithms offer a set of rules. It needs to be followed by everyone in the network. Also, to impose a consensus method, nodes should participate. Without any node participation, the consensus method cannot be implemented. This also means that the more nodes join to participate in the consensus method, the stronger the network begins.

The Longest chain rule



Sometimes separate blocks can be produced concurrently, creating a temporary fork. In addition to a secure hash-based history, any blockchain has a specified algorithm for scoring different versions of the history so that one with a higher score can be selected over others. Blocks not selected for inclusion in the chain are called orphan blocks. Peers supporting the database have different versions of the history from time to time. They keep only the highest-scoring version of the database known to them. Whenever a peer receives a higher-scoring version (usually the old version with a single new block added) they extend or overwrite their own database and retransmit the improvement to their peers. There is never an absolute guarantee that any particular entry will remain in the best version of history forever. Blockchains are typically built to add the score of new blocks onto old blocks and are given incentives to extend with new blocks rather than overwrite old blocks. Therefore, the probability of an entry

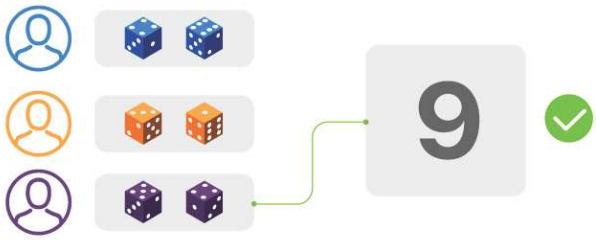
becoming superseded decreases exponentially as more blocks are built on top of it, eventually becoming very low. For example, bitcoin uses a proof-of-work system, where the chain with the most cumulative proof-of-work is considered the valid one by the network. There are a number of methods that can be used to demonstrate a sufficient level of computation. Within a blockchain the computation is carried out redundantly rather than in the traditional segregated and parallel manner.

Who validates the blocks?

A transaction in blockchain is said to be completed when a valid/ verified block is appended to the chain. An unconfirmed transaction means the block is not yet appended to the existing chain.

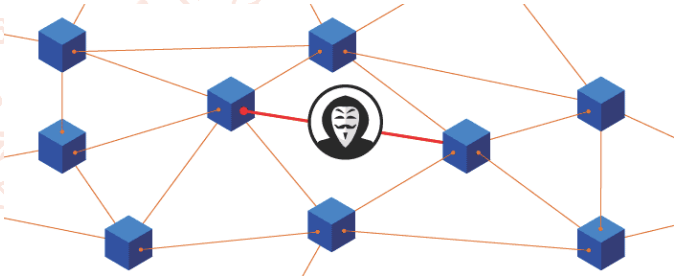
Any node in the network can collect unconfirmed transactions and create a block and then broadcast it to the rest of the network as a suggestion as to which block should be the next one in the blockchain. How does the network decide which block should be next in the blockchain? There can be multiple blocks created by different nodes at the same time. One can't rely on the order since blocks can arrive at different orders at different points in the network.

Each block generated is secured by cryptographic hash and is appended to another block forming a chain. But who appends a block to another block in the chain? Who validates the block? Answer is Minors. Nodes who validate the transaction are known as mining nodes or simply miners. They validates the block by solving a puzzle for e.g. A number guessing game. Whoever guesses the number first wins and gets the chance to validate the transaction. What's in it for the minors ? They are rewarded by the network in the form of cryptocurrency.



Let's take Bitcoin for example. To validate each bitcoin transaction, bitcoin uses the Proof of Work method. Proof of work is used to decide which block should be next in the blockchain. A node generating a block needs to prove that it has put enough computing resources to solve a mathematical puzzle. The miner tries to find a number known as nonce. This number will be combined with the data in the block. It will then be passed through the hash function. If it produces a result that should fall within a certain range. It is much difficult to guess the number. The value of nonce ranges from 0 to 4,294,967,296. The real question is how do miners find the nonce? It is almost impossible to forecast the output. The resulting hash should begin with a fixed number of zeros, currently it is eighteen. There is no way to guess the number which gives a hash beginning with a predefined number of zeroes. Moreover, the two consecutive numbers can have entirely different hash values. The only way to find the correct nonce is to keep trying until we get the desired output. The miner once finds the desired output; the miner communicates it to all other nodes in the network. The rest of the miners stop working on that block. The miner who finds the desired output gets the reward in terms of certain Bitcoin. The Bitcoins awarded for mining a block was initially 50 Bitcoins. Currently, the reward is 12.5 bitcoins, which is worth almost $125,000 which is nearly equal to 9263035 Indian Rupee.

SECURITY FEATURES OF BLOCKCHAIN



- Use a ledger. Ledger should record each and every transaction in a blockchain. This ledger is immutable. Existing data cannot be edited or deleted. In blockchain technology these ledgers are decentralized applications. So, no one can access the transaction or even any sensitive data from this ledger. People can only read the information from a ledger.
- Another type of security feature is the block chain. In blockchain each block should contain a hash value. These blocks are connected by its previous hash. Suppose an attacker came to correct the data, then its hash will be changed. It will affect the overall chain. So, it will increase the protection of sensitive data or information.
- Blockchain technology is a decentralized application. Mainly it will support peer to peer communication. So, a network node is considered a computer. These thousands of nodes should have the copy of the distributed ledger. This should be authenticating the

transaction. If any of the nodes does not agree to a transaction, then it cannot proceed. So, it will be cancelled. This will protect from a fraudulent transaction.

Applications of Technology:- Compelling Use Cases in both Financial and NonFinancial- Areas

1. Financial Applications:

➢ Cryptocurrency:

Cryptocurrency or now what is called "Crypto" is the most popular blockchain use case ever. A cryptocurrency is a form of digital asset based on a network that is distributed across a large number of computers. This decentralized structure allows them to exist outside the control of governments and central authorities.

➢ Insurance

Insurance is another financial sector where blockchain can play an important role. Assets which can be uniquely identified by one or more identifiers which are difficult to destroy or replicate can be registered in blockchain. This can be used to verify ownership of an asset and also trace the transaction history. Any property (physical or digital such as real estate, automobiles, physical assets, laptops, other valuables) can potentially be registered in blockchain and the ownership, transaction history can be validated by anyone, especially insurers.

➢ Banking

The potential for added efficiency in secure ledger storage makes a strong use case for blockchains in Banking. When executed peer-to-peer, transaction confirmations become almost instantaneous (as opposed to taking hours and days for clearance). Potentially, this means intermediaries — such as the clearing house, auditors and custodians — get removed from the process.

2. Non - Financial Applications:

➢ Smart contracts

Distributed ledger technology enables the coding of simple contracts that will execute when specified conditions are met. Ethereum is an open-source blockchain project that was built specifically to realize this possibility. Still, in its early stages, Ethereum has the potential to leverage the usefulness of blockchains on a truly world-changing scale. A smart contract as the name suggests, is a contract which is smart enough to trigger and execute automatically after some event happens. For instance, a derivative could be paid out when a financial instrument meets a certain benchmark, with the use of blockchain technology and cryptocurrency enabling the payout to be automated.

➢ IoT (Internet of Things with Blockchain)

What is the IoT? The network-controlled management of certain types of electronic devices — for instance, the monitoring of air temperature in a storage facility. Smart contracts make the automation of remote systems management possible. A combination of software, sensors, and the network facilitates an exchange of data between objects and mechanisms. The result increases system efficiency and improves cost monitoring. Blockchain capabilities like immutability, transparency, auditability, data encryption and operational resilience can help solve most architectural shortcomings of IoT. As the size of IOT network information sharing is increasing, thus the fundamental storage cost will also increase. So information sets are kept in distant origins and a centralized server is preserved which will lonelily keep the references to these origins. Moreover Blockchain is used to keep RIM (Reference Integrity Matrix) of information set. As the Blockchains have Immutability feature, and accessibility of the RIM with all IoT network devices in Blockchain, ensured the Integrity of RIM. Every time an obligatory Information Set is taken from the origin, its Integrity can be confirmed by comparing its RIM being maintained on Blockchain.

➢ Decentralized Storage System As blockchain itself is secure and uses decentralized system approach, it can remove the drawbacks of the central storage systems like

➢ Prone to failures

➢ Higher security and privacy risks for users

➢ Longer access times to data for users

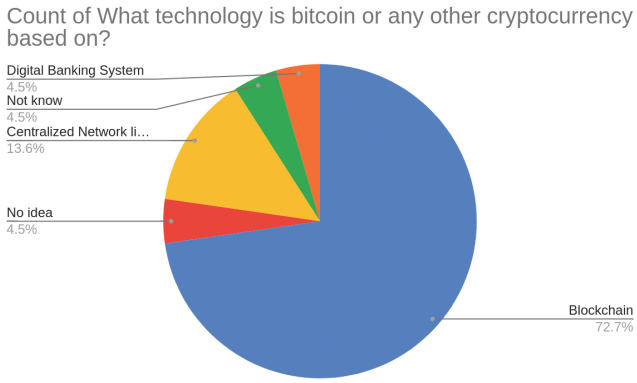
who are far from the server. Furthermore, Blockchain can be used as a peer to peer file storage system which can enable users to upload and retrieve the files securely. Users won't need to be dependent upon the central server to be up running all the time.

➢ Land Title Registration

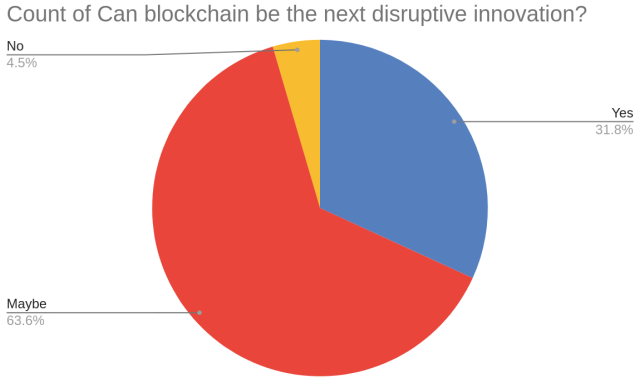
As Publicly-accessible ledgers, blockchains can make all kinds of record-keeping more efficient. Property titles are a case in point. They tend to be susceptible to fraud, as well as costly and labor-intensive to administer.

Awareness about the Blockchain:

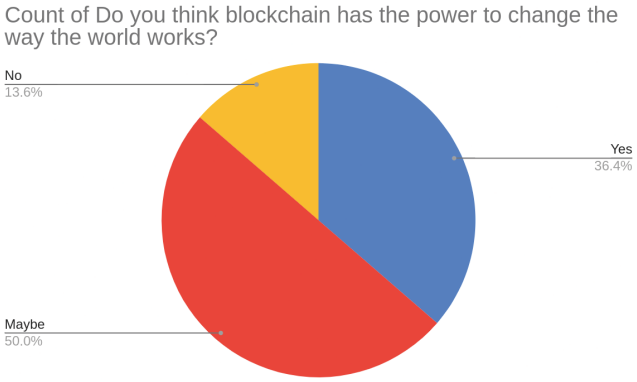
As per the survey conducted for this paper, 72% people said that they know about blockchain and the cryptocurrencies like bitcoin use it.



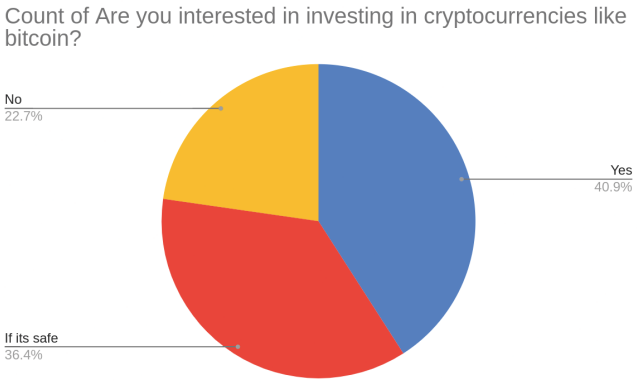
But some people are still scared about blockchain and think that it can be the next disruptive innovation.



Whereas, 36% people think that blockchain has the power to change the world, 13% of people don't think the same and 50% people are not sure about it.



Apparently, people are interested in investing in the cryptocurrencies like bitcoin as I believe that it is due to the big hype going on about Cryptocurrencies like Bitcoin, Dogecoin etc.



References:

[1] esakal | बलॉक चेन (अचयतु गोडबोले): https://www.esakal.com/saptarang/saptarang-achyut-godbole-write-disruptive-technology-article-202709

[2] BlockChain Technology Beyond Bitcoin (Sutardja Center for Entrepreneurship & Technology Technical Report): https://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf

[3] How Economist Milton Friedman Predicted Bitcoin: https://web.archive.org/web/20210127223050if_/https://www.coindesk.com/economist-milton-friedman-predicted-bitcoin

[4] A Survey on the Security of Blockchain Systems By Xiaoqi Li, The Hong Kong Polytechnic University, Peng Jiang, Ting Chen, Xiapu Luo : https://www.researchgate.net/publication/319249505_A_Survey_on_the_Security_of_Blockchain_Systems

[5] An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends By Thomas Kitsantas , Athanasios Vazakidis, Evangelos Chytis : https://www.researchgate.net/publication/318131748_An_Overview_of_Blockchain_Technology_Architecture_Consensus_and_Future_Trends

[6] IOT Security Issues Via Blockchain: A Review Paper By Abid Sultan, Muhammad Azhar Mushtaq, Muhammad Abubakar: https://www.researchgate.net/publication/333255641_IOT_Security_Issues_Via_Blockchain_A_Review_Paper

[7] An Introduction to the Blockchain and Its Implications for Libraries and Medicine By MatthewB Hoy : https://www.researchgate.net/publication/318473082_An_Introduction_to_the_Blockchain_and_Its_Implications_for_Libraries_and_Medicine

[8] Blockchain and IoT Integration: A Systematic Survey By Alfonso Panarello, Nachiket Tapas, Giovanni Merlino, Francesco Longo and Antonio Puliafito: https://pdfs.semanticscholar.org/3830/57f972b11b99cbc8c0d3e6c47170e9d95c1c.pdf

[9] Wikipedia:- Blockchain: https://en.wikipedia.org/wiki/Blockchain