International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.089|

||Volume 9, Issue 4, April 2020||

An Introduction to Blockchain Technology: Characteristics, Application and Future Aspects

Sabhya Saini[1], Shubh Dhawan[1], Dr. Deepak Chahal[2]

MCA Student, Department of IT, Jagan Institute of Management Studies, Sector -05, Rohini, New Delhi, India[1]

Professor , Department of IT, Jagan Institute of Management Studies, Sector -05, Rohini, New Delhi, India[2]

ABSTRACT: Technological innovations such as robotics, machine learning, cloud technology etc have established themselves very fast over the last few years and have now become a key element of the commercial and social economy [1]. Blockchain is a term that emerged in the year 2008, by a person or a group of people named Satoshi Nakamoto. The term has been in the limelight in the technology industry for a while now because of its contribution to the development of Bitcoin and the enhanced security features for data transactions. Blockchain has opened doors for enormous innovations one of which is the possibility of total exclusion of third parties which were earlier involved in a transaction. Specifically for digital transactions involving farm goods, Independent artists' works and capital.

KEYWORDS: Blockchain, Public Ledger, Secured Digital Transactions, Decentralized

I. INTRODUCTION

One of the initial works on chained blocks was discovered in 1991 which was carried out by Stuart Haber and W. Scott Stornetta. Their intention was to prevent the tampering of the document timestamp. Bayer, Haber and Stornetta in the year 1992 brought Merkle Trees into the design, thus improving the efficiency by collecting several document certificates into one block.
Satoshi Nakamoto introduced the Hashcash like method for adding the blocks of data into the existing chain without the requirement of them being signed by a trusted party.
The outcome of the development process resulted in a ledger for all the transactions on the network. Which further turned out as the core component of the crypto currency bitcoin where the ledger is public.

A cascading list of records which are interlinked through cryptography is called a Blockchain. The records are a block of data which possess a hash function of cryptography of the previous block of data, a timestamp, and a transaction data. Blockchain is a Distributed Ledger Technology (DLT) and an open public ledger.Every action performed on the Blockchain is a function of the network as a whole. Blockchain can only be updated by consensus between participants in the system, and once new data is entered it can never be erased. It is a write-once, append-many technology, making it a verifiable and auditable record of each and every transaction. One can think about the blockchain as a ledger of transactions [2].

II. WORKING

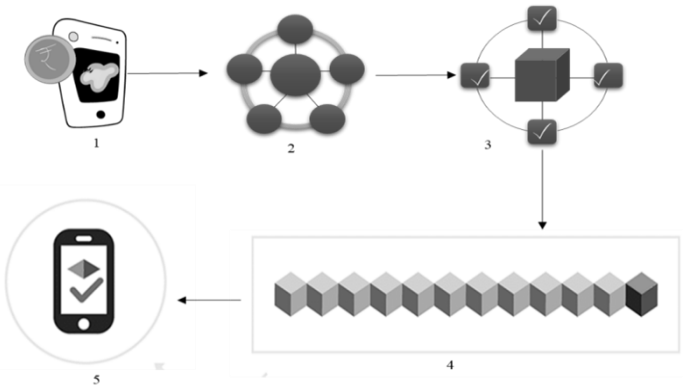

Fig. 1: Working of a Blockchain.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.089|

||Volume 9, Issue 4, April 2020||

Steps involved in the creation of the Blockchain are presented in Fig. 1 and are described below:

1. A transaction request is made.
2. The requested transaction is broadcast to a P2P Network, consisting of computers, known as nodes.
3. The network of nodes validates the transaction and the user's status using known algorithms.
4. Once verified, the transaction is combined with other previously made transactions, to create a new block of data for the ledger. The new blockchain is then added to the existing blockchain, in a way that is permanent and unalterable.
5. The transaction then is finally complete.

Blocks which are not selected for inclusion in the chain are called orphan blocks. Temporary fork is created where separate blocks can be produced concurrently. To deliver a secure hash-based history, a specified algorithm is associated with a blockchain for labelling rank for different versions of the history. With this, the one with a higher score can be selected over others.Peers supporting the database have different versions of the history from time to time. They preserve only the highest-ranked version of the database. Whenever a peer receives a higher-ranked version, 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 the history forever. Blockchains are typically built to add the rank of new blocks onto old blocks and are given incentives to extend with new blocks rather than overwrite old blocks. Within a blockchain the computation is carried out redundantly rather than in the traditional segregated and parallel manner.

The block time is the average time it takes for the network to generate one extra block in the blockchain. Some Blockchains create a new block as frequently as every five seconds. By the time of block completion, the included data becomes verifiable. In cryptocurrency, this is practically when the transaction takes place, so a shorter block time means faster transactions. The block time for bitcoin is set on an average of 10 minutes.

III. PEER – TO – PEER NETWORK

Blockchain uses the peer –to – peer Network for processing a transaction on its network. A distributed application architecture over a network that separates work between peers is Peer – to – Peer Network. Peers are equally privileged, equal participants in the application. They together form a peer-to-peer network of nodes. Peers, without the need for central coordination by servers or stable hosts create a secure space of their resources, such as processing power, disk storage or network bandwidth, which is directly available to the other participants on the designated network.Peers are both consumers and suppliers of resources, in contrast to the traditional client-server model in which the consumption and supply of resources is divided. Emerging collaborative P2P systems can bring in unique resources and capabilities to a virtual environment consisting of various communities which look out for accomplishing tasks that are beyond the reach of an individual alone and are of service to the entire peer community.

IV. DECENTRALIZATION

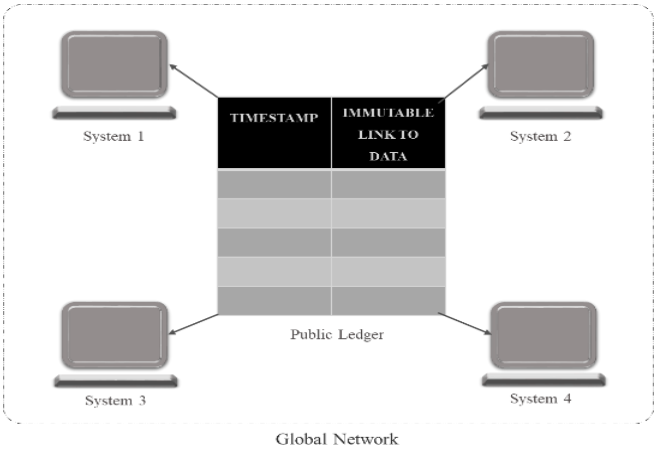

Fig. 2: Decentralization of Blockchain Network

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.089|

||Volume 9, Issue 4, April 2020||

Decentralization of the network enables a global network of systems encompassing Blockchain technology to collectively maintain the database that stores the transactions made through Bitcoin or any transaction using Blockchain technology. In this manner, the Block chained transactionsare managed by several distributed global network and not one central network or authority which surpass the security of the transaction and prevents data loss threats and corruption of any form.

IV. IMMUTABLE

Once the data has been registered as a record in a ledger for a Blockchain, then it is permanently registered, no alterations and modifications can be done on that ledger. It is possible due to the cryptographic hash function.

To take an input of any variable length and result in an output of fixed length is what closely defines hashing. In the case of cryptocurrencies like Bitcoin, the transactions are taken as input and passed through a hashing algorithm, which in return produces an output of fixed length.

Hashing's special class has a cryptographic hash function. For this function to be secure it has to have certain properties, one of which is the "Avalanche Effect". This particular property in cryptographic hash function results in a drastically overwhelming huge change in the output even if a very minute change has been made in the input. Table 1. Describes the mentioned property.

INPUT	HASH GENERATED OUTPUT
Hello	D89RG84ASW236FVB48D
hello	64GLSFIU127FRGKJH5

Table 1. Avalanche Effect Property in Cryptographic hash function

A list containing data and a hash pointer, pointing to its previous block, thus linked and forming a chain is the structure of the Blockchain. A blockchain is resistant to tampering of data. It is "a diffusion ledger that can record the transactions between two-person efficiently and in a permanent. way" [3].
A hash pointer contains the address of the previous block, and in addition, it also contains the hash of the data inside the previous block, which makes the Blockchain reliable.

V. TRANSPARENT AND PRIVATE

User's identity in a Blockchain environment is hidden via complex cryptography and represented only by their public address.
For example, a public ledger search for a transaction history will result in something like this "zz9vpFYEmvwT2TbyCt7NZJ transferred 1 Bitcoin" and not "XYZ transferred 1 Bitcoin". In this format, a user's real identity is secured as their transactions are visible in the public ledger through a public address which is cryptographically secured.
This representation of information of transactions not only enhances the transparency of the transactions being made but also increases security of the personal identity of the transactions and thereby increasing the accountability of the transaction makers.

VI. SECURITY

Encryption is being used to maintain the security of the Blockchain Network. The network due to decentralization does not possess a centralized area of vulnerability that hackers may tend to exploit. There are public and private keys. A "public key" (a long, randomly-generated string of numbers) is a users' address on the blockchain. Bitcoins sent across the network gets recorded as belonging to that address. The "private key" is like a password that gives its owner access to their Bitcoin or other digital assets. The data stored on the Blockchain is incorruptible as Interplanetary File System (IPFS) with respect to Blockchain enables the user manage data of great amounts and place the immutable, permanent links of it into Blockchain transactions. In this manner, the transaction of the data is also being time stamped and made secure without putting the data itself on the chain.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.089|

||Volume 9, Issue 4, April 2020||

VII. A REAL WORLD APPLICATION OF BLOCKCHAIN

- A farmer gets insurance for his apples that are to be exported to Singapore for `10000/-
- The apples are loaded in a fridge that has an IoT sensor, which continuously keeps checking the temperature inside the fridge and reports it to the ledger until the transaction is complete.
- In the mid-way to the airport, the truck carrying the fridge full of apples to be transported to Singapore meets with an accident and the fridge breaks. The temperature of the fridge reaches the degree which is no longer favorable for the apples to be exported with 100% quality.
- The insurance company gets the information about the poor transportation of the apples through the open ledger and thus reduces the premium amount for the transaction.
- Every minute information of the process is recorded here, and every person associated with the transaction has access to the open ledger.

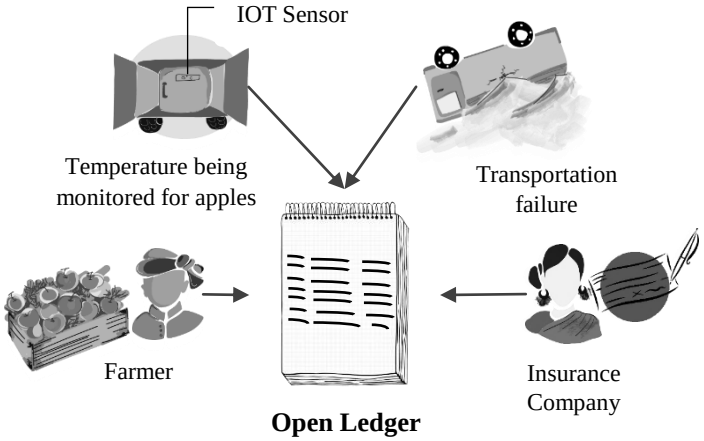

Fig 3 . Blockchain real world application

VIII. BUSINESS APPLICATIONS

Due to the growing Blockchain technology, Businesses are extensively looking out for opportunities in this field. Some of the future developments in the application of Blockchain are:

- Bitcoin
- Etherium
- Smart contracts
- The sharing economy
- Crowd funding
- Governance
- Supply chain auditing
- File storage
- Prediction markets
- Protection of intellectual property
- Internet of Things (IoT)
- Neighbourhood Microgrids
- Identity management
- AML and KYC
- Data management
- Land title registration
- Stock trading

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.089|

||Volume 9, Issue 4, April 2020||

IX. FUTURE ASPECTS

The music industry and the artists were escalating at the time when physical records of songs were being sold directly from the production houses. With the rise of the internet, the piracy and the third party distributors just levelled down the due credit of the artists performing those songs, and also reduced the earning value of the actual production houses. Not only just the music industry but also the farmers from time immemorial have been exploited by the intermediaries or the middle men who purchase their hard earned produce at a price that is not justifiable or fair.
Blockchain if implemented successfully and brought into the market can really benefit the farmers and the independent creators at a very large scale. As Blockchain is a peer – to – peer transaction, no middlemen will be a part of the transaction other than the actual entities involved. In this manner, the farmers will be directly able to sell their produce to the buyer in the city and will get actual capital for their produce. Similar with the artists, whatever they'll be creating will be sold directly to the buyer with no third party involved. The other advantage from this will be that not just the buyer will be paying directly to the producer, in contrast, they will also be aware of each and every step of the process of their product from the very beginning of creation, to the transportation and the final product delivery. All this data available to them without any alterations, thus making the creator being accountable for their product and it's quality from the very beginning.

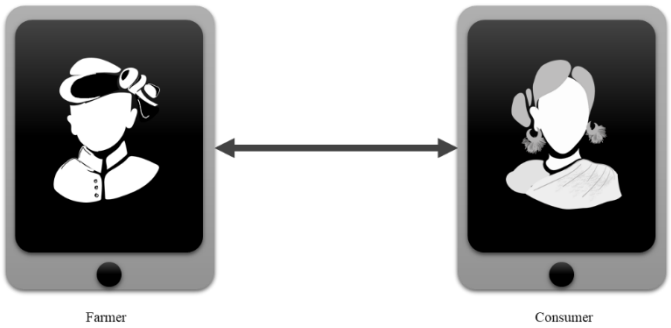

Fig 4. Direct network between the producer and the consumer

X. CONCLUSION

In this digital era when online transactions of information and money are happening at such a fast pace that is truly unprecedented, the need of the hour has become to secure the platforms through which these transactions happen. Not only will this enable the participants involved in the transactions, to feel secure but will also hold them accountable for each transaction. Block chain will be the key factor in making this possible as it ensures that the transactions of all forms be accounted for and interlinked. Blockchain's advance applications will create businesses and their CEOs the respectable and trusted individuals who care for the legitimate share of every individual who works for them or even collaborate. Because of the rise of Blockchain, the information sources will be held accountable as the interlinked blocks will together easily reveal the perpetrator when it comes to hate speech, crime and fake news. Blockchain can become the baton of hope and positivity in terms of cyber security, increased individual business growth online, due copyright credits for artists and safe digital financial transactions.

REFERENCES

1. Chahal D. et al. The Developing Role Of Block Chain(R)Evolution, EPRA International Journal of Multidisciplinary Research (IJMR), Volume: 4 | Issue: 11 | November 2018.
2. Kharb L et al, International Journal of Computer Science and Mobile Applications, Vol.5 Issue. 11, November- 2017, pg. 1-8].
3. Singhal A. et al. Blockchain: An Innovative Technology, International Journal of Scientific Research and Engineering Development, Volume 2 Issue 6, Nov- Dec 2019