International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 5 | Issue 4 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT195415

# An Exploration of Block-chain in the Financial World

Varanasi Deepthi
Department of Information Technology, Sreenidhi Institute of Science and Technology, Hyderabad, Telangana, India

## ABSTRACT

Blockchain is a non-centralized, conveyed record of considerable number of transactions which happens simply subsequent to different multiple parties. It guarantees a state of security as the exchanges or the transactions which happen are altogether mysterious. Every exchange or the transaction occurring in a Blockchain network is confirmed by people called miners, only if the event is settled upon by the agreement of the larger part gathering of these miners taking an interest in this procedure. Blockchain is one of the rising innovations in these days and a great deal of transformation and research has recently started with respect to this wide spread innovation. Bitcoin can be considered as the most well known cryptographic money since it has started and it is the best model that utilizes the Blockchain innovation.

**Keywords:** Block, Bitcoin, Blockchain, Cryptocurrency

## I. INTRODUCTION

The digital currency which had been released in 2009 as open source [1] software is called as a Bitcoin. Bitcoin is basically a Cryptocurrency that is decentralised and is made with the help of all the present nodes existing within the system at a particular rate. Bitcoins which are generated are linked with one another to produce a Blockchain. This Blockchain could be used in the exploration of any transaction that has occurred in the past over the network in between the Bitcoin addresses. Whenever a new transaction is occurred, a new block will be created and will be linked to the existing Blockchain. The newly created transactions are continually added to the open record of Bitcoin and the corresponding procedure is called as mining of Bitcoin.

Blockchain is a database repository that is decentralised, authentic and something which is difficult to use for the purpose of fraud or any mischief. On the other side, Bitcoin is a digital currency that utilises the public ledger of Blockchain to create transactions across the network. Bitcoin is one of the finance related applications that uses Blockchain technology. Apart from Bitcoin, there are other applications that use Blockchain technology namely, Smart contracts and Hyper ledger. Hence, Blockchain technology can be utilised to create a number of applications.

Blockchain being a database is used for the purpose of storage in a non-centralised network. Blockchain isn't meant only for the finance related applications, we can also make transactions to meet our application requirements. In the coming section we shall discuss more about the Blockchain technology.

In the olden days, before Google docs was invented, we would create a document and send it to the other person if we need any changes in the document or if we want the person to review our document. With this method, we will have to wait until the other person edits the document and gives us back.[2]This a time taking procedure. But with the invention of Google docs we are able to share the same document by two people at the same time and giving both the access to edit it simultaneously.

In the same way, all the transactions in the Blockchain are viewed by everyone and the transactions can be mined by anyone who are present in the same Blockchain network.

Blockchain is an exchange database which contains data which pretty much has every transaction at any point executed previously and takes a shot at Bitcoin convention [3]. It makes a computerised record of exchanges and enables every one of the members on system to alter the record in a verified manner which is shared over conveyed system of the PCs.

For rolling out any improvements to the present information, every one of the nodes that are in the network runs the algorithms to assess, confirm and coordinate information of transactions with the Blockchain history. If the major number of nodes concurs for the exchange, then the transaction is accepted and another block gets linked to the current Blockchain.

We can envision Blockchain as a stack of blocks kept over one another and the block which is at the bottom is the block that acts as an establishment of the same stack. Individual blocks are connected to one another and points out to the previous block present in the chain.

Every block on the Blockchain is recognised by hash value which is produced by utilising Secure Hash Algorithm (SHA-256)[4] which is a cryptographic hash algorithm present on the starting of each block. Block can have a single parent however it could have numerous children each alluding to the same parent block therefore it has the same hash in the past block hash field. Each block has hash of parent block in the starting of the block and the succession of hashes connecting each and every individual block with their respective parent blocks makes a major chain indicating the principal block called as Genesis block.

## II. BLOCKCHAIN AND IT'S WORKING

**A)** Let us first go through the working of the Bitcoin transactions first for the purpose of easily understanding the Blockchain mechanism and it's working.[5]Bitcoin, instead of having some trust on the third party, uses work of proof that operates under the primitives of cryptography. Therefore, the idea called digital signatures has started.

**B)** If a sender wants to send something then he can send utilizing his private key and the recipient utilizing his public key and the individual has to know the private key and the digital signature, on the off chance that he wishes to spend the cash. The companion nodes present in the Bitcoin network is totally mindful of the exchanges being occurring. The transactions must be "supported" and "approved" so as to be reflected in an open record. Initially, the validator must realise that the sender has the authority to spend it. Furthermore, the validators must know that the sender has enough cash in his record to make a "genuine" transaction.

**C)** The transactions that are occurring in the network are not requested. Thus, there is an opportunity of twofold spending and it could be expelled by the presentation of Blockchain Technology. In Blockchain, the transactions are requested in form of blocks which are presented in a linear chain, that are connected to one another. Each and every block will hold the previous block's hash. We have presented an idea called "Proof of Work". In this, the errand of the node is to locate a random string and this string will be linked with the transaction that has happened and with the hash representations of the previous blocks afterwards, it delivers a hash which has a number of zeroes in the beginning of a hash.

## III. BITCOIN AS AN APPLICATION OF BLOCK CHAIN

A) New possessor's ECDSA key is attached to the transaction message whenever the Bitcoin is to be sent and the current possessor's public ECDSA key is attached to each Bitcoin [6]. The machines which are associated with the web and permit to deposit money in return of Bitcoin's which are given as a receipt or by simply moving the cash to an open key on the Blockchain [7] are called as Bitcoin kiosks. At whatever point a Bitcoin is sent, it joins the new proprietor's open key and signs it using the sender's Private Key. The sender's mark upon the message checks that the message is real and transaction's history is available with everybody in order to make the verification easy.

B) It utilizes public key cryptography asymmetric encryption algorithm and idea of public and private keys to encode and decode information. In the event that message is encoded utilizing public key (Pk), at that point private or secret key (SK) is important to decode. Although, when message is encrypted utilizing private or mystery key (SK) at that point open key (Pk) is important to decrypt.

C) Generally public key can be given to anybody yet private key should be kept as a secret. Single participant can make different open key and mystery key pair.

D) Bitcoin doesn't need an outsider as it openly verifies the record named Blockchain. The intrigued with regards to giving CPU capacity to run a unique bit of some particular software are called as miners and all of them together form a network to keep up the Blockchain. In the Bitcoin mining process, users make new Bitcoin money and transaction is communicated over the system.

E) The network has computers running the software which solves the puzzles of cryptography that has information from the transactions that are made. The principal mineworker who quickly solves each puzzle first gets fifty Bitcoins and the related block of transaction will be linked to the current Blockchain.

F) The grade of difficulty of each and every puzzle is relative to the quantity of miners that are present. As the quantity of the miners increases, the toughness of the puzzle is further additionally incremented in order to guarantee the generation of one block of transaction for each and every ten minutes of time.

G) Bitcoin operates on the concept decreasing supply calculation which implies that reward for mining the Bitcoin block is decreased to exactly half after each two lakh ten thousand [8], [9]. The number of blocks that are created are balanced where each 2016 blocks guarantees the production of around six blocks for each hour. The number of Bitcoins produced per block is set to diminish and it will decrease by half every two lakh ten thousand blocks which is around 04 years' of time [10]. The point is to guarantee that the number of Bitcoins in never surpasses twenty one million

## IV. MERITS OF USING A BLOCK CHAIN

1) Blockchain is very difficult to tamper, it is highly impossible to alter a block present in the Blockchain.
2) Another interesting advantage of Blockchain technology is that, it's irreversible. It helps in the prevention of double spending.

3) Blockchain is a system which is distributed meaning that all the members present in the network has a copy of the ledger.
4) Blockchain is a decentralized system which does not depend up on a centralized authority to take over. It's more like a person to person system
5) Blockchain is a decentralized system which does not depend up on a centralized authority to take over.
6) It's more like a person to person system
7) Blockchain is flexible and is not prone to any kind of malicious attacks.

## V. BLOCK CHAIN AND ITS OTHER NON-FINANCE RELATED APPLICATIONS

### A) POLLING

Casting a ballot is a significant instrument for any equitable government. It is the most vital factor that makes a legislature "for the general population and by the general population". Truth be told, if not for casting a ballot than the idea of a "free nation" may not by any means exist. Having said that, it is truly entrancing and stunning that we have still not proceeded onward from the customary paper poll arrangement of casting a ballot.

The paper ballot framework has for quite some time been utilized by nations around the globe. The idea is straight forward; you put your vote on a bit of paper and place it in a tallying station. Toward the finish of the decision, the votes are tallied and whoever gets the most votes is the victor. Notwithstanding, as basic as it might sound, there are a great deal of issues that can happen on account of conventional paper balloting framework.

The main concerns of the basic ballot system:

1) The measure of time taken to check the votes is excessively high.
2) The decision can be seized by means of the inclusion of counterfeit vote papers.
3) The measure of paper wastage.
4) There is no chronicled record conceivable to monitor every single vote made.
5) The expense of use on paper ballots is extremely high.
6) It is difficult to monitor your vote.
7) When you have made a choice you can't transform it.

### B) REGISTRATION OF LAND

India has investigated the Blockchain innovation as a conceivable answer for their property registry issues. Property misrepresentation is one of the greatest issues in India.

$“Thinkaboutthisforasecond”.$

a) In 2013, New Delhi alone had 181 announced instances of property misrepresentation while Mumbai came a nearby second at 173 cases. In this way, to counter this issue, the administrations of Andhra Pradesh and Telangana have banded together up with Swedish startup to put their land registry on the Blockchain.
b) The execution will be incredibly clear. The framework will have a Blockchain back-end and a web application front-end. The front-end will help in the general framework reflection. ChromaWay will utilize their own database stage called "Postchain."
c) According to International Business Times: "Postchain is developed from the beginning work with most broadly utilized stages, and incorporating it into the administration's frameworks is done consistently."

### C) IN THE FIELD OF CRYPTOCURRENCY

a) One of the many fascinating advancements that they could be doing is the presentation of cryptographically secure, computerized fingerprints.

b) This is the way it can work: A hash is taken of the Geo-coordinates alongside a polygonal depiction of the land. This hash is fixing to the proprietor's ID and the outcome is hashed again and added to the Blockchain. Since the hash is dependably an exceptional esteem, everybody will have a remarkable ID. In addition, in view of the Block chain's changeless, nobody can mess with the records.

c) There are for the most part 3 includes that a Blockchain has that can help forestall Cybersecurity assaults.

- Trust-less System
- Changeless
- Decentralization and Consensus

### D) FOOD BUSINESS

a) All in all, what occurs if the Blockchain gets actualised here to keep up all the food records? Keep in mind that the Blockchain is an open record and the information in it is available to everybody and there is no focal expert assuming responsibility of the records. This enormously lessens the time that might be wasted experiencing interminable formality and pecking order. Indeed, having this information on the Blockchain will decrease the holding up time from weeks to negligible seconds.

b) Walmart has officially completed two trials with IBM, one with Chinese pork and the other with Mexican mangoes. Walmart and IBM utilized the "Hyperledger Fabric"[11], a Blockchain initially worked by IBM and now housed under the Linux Foundation's Hyperledger bunch for these tests. Blunt Yiannas, VP of sustenance well being at Wall-Mart had this to state about the aftereffects of the preliminaries (As advised to Fortune):

c) "We were encouraged to the point that we extremely immediately begun connecting with different providers and retailers also"

d) As the Blockchain gets increasingly more coordinated into the sustenance business it will make the entire procedure progressively straightforward and more secure. The benefits of a straightforward nourishment framework are complex (Taken from Frank Yiannas' discourse):

- Significantly improves food security.
- Guarantees fresher food since nobody will hazard sending "non-crisp" food in an open framework.
- There is less wastage of food in light of the fact that each and every bit of food is represented.
- Stops food extortion in light of the fact that the framework is open for anyone passing by to view.

## VI. ALGORITHMS USED

### A) SECURE HASH ALGORITHM

This is a cryptographic hash function (as in Fig. 1) that is primarily utilized by a Bitcoin. The integrity of the data which is given can be determined by the comparison of the output which is given by the execution of the algorithm called SHA-2 algorithm [12] with the help of a hash value which is already familiar and the hash value that we are expecting. The algorithm hash will convert a huge quantity of data in to a hash which is of a fixed length size. Production of the hash will be dependent on the data, similar data will always result in the production of similar hash and any small change in the data results in the complete change of hash.

### B) PKCAE Algorithm

It utilizes public key cryptography asymmetric encryption algorithm (as in Fig.2) and idea of public and private keys to encode and decode information [13]. In the event that message is encoded utilizing public key (PK), at that point private or secret key (SK) is important to decode. Although, whenever the message has to be encrypted utilizing the private or mystery key (Sk) at that point open key (Pk) is important to decrypt.

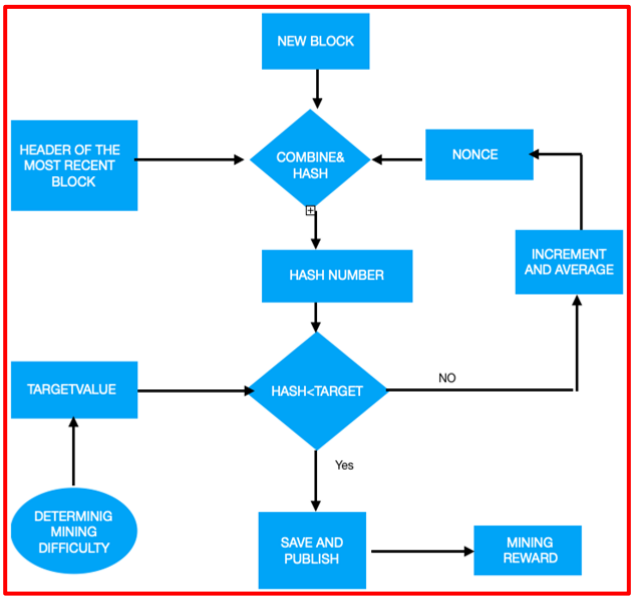

**Fig.1.** Hashing of Block

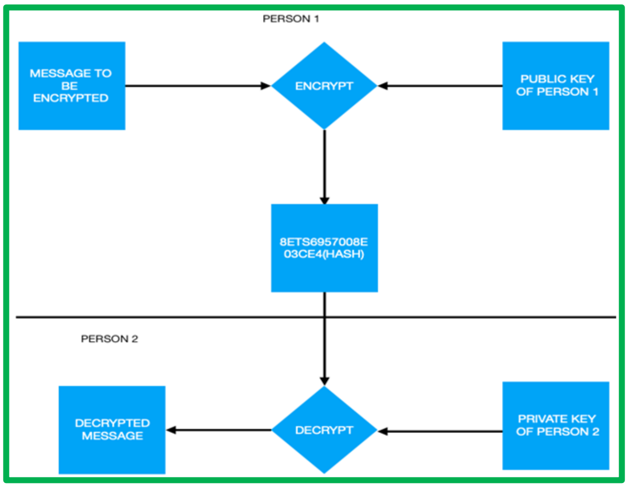

**Fig. 2.** Encryption and Decryption of a message

## VII. CHALLENGES AND LIMITATIONS

### A) ADAPTION TO A NEW LANGUAGE

Blockchain involves a complete new set of vocabulary, but thankfully there are people who started putting efforts at providing the glossaries that are germane and easy to understand.

### B) NEED OF MASS USERS

For user to experience the full benefit, it requires mass users in the network, which can be sometimes a challenge because gathering a mass in a network is a really hard aspect.

In order to experience the full benefit, it requires mass users in the network, which can be sometimes a challenge because gathering a mass in a network is a really hard aspect.

### C) COST PER TRANSACTION

The other major disadvantage is the transaction costs and the network speed. Bitcoin has started costing per transaction after a few years of nearly free transaction costs

There's not only cost for the transaction but there is an introduction of cost even for the storage of transactions which is definitely a major disadvantage [14].

### D) COMMITMENT OF ERRORS

Because the Blockchain is used like a database, the data which is going to be stored in it must be of high quality. There is a high chance of mistakes happening because of any kind of carelessness that we humans tend to commit.

## VIII. CONCLUSIONS

Blockchain in the area of research and development is still at its early stage. The researchers in the cryptography and security domain have come forward in order to take it to different heights. This technology is useful for both finance related and non-finance related areas. This technology will be of a great help in terms of trust, security and also mutually known knowledge. This can be considered as an amazing technology till date. The whole paper is trying to say that there are still a number of opportunities in the field of research and there is a great need for us to seek and explore the other aspects by decreasing the number of faults and simultaneously increasing the efficiency of the technology.

## IX. REFERENCES

[1]. Singh, S., & Singh, N. (2016). Blockchain: Future of financial and cyber security. 2016 2nd International Conference on Contemporary Computing and Informatics (IC3I). doi:10.1109/ic3i.2016.7918009

[2]. https://blockgeeks.com/guides/what-is-blockchain-technology/

[3]. Tasatanattakool, P., & Techapanupreeda, C. (2018). Blockchain: Challenges and applications. 2018 International Conference on Information Networking (ICOIN). doi:10.1109/icoin.2018.8343163.

[4]. Chapter 7. The Blockchain, http://chimera.labs.oreilly.com/books/1234000001802/ch07.html/

[5]. Chatterjee, R., & Chatterjee, R. (2017). An Overview of the Emerging Technology: Blockchain. 2017 3rd International Conference on Computational Intelligence and Networks (CINE).doi:10.1109/cine.2017.33

[6]. Elliptic-curve digital signatures, http://davidederosa.com/basic- blockchain-programming/elliptic-curve-digital-signatures/

[7]. How to sell bitcoins using Bitcoin ATM, https://coinatmradar.com/blog/how-to-sell-bitcoins-using-bitcoin-atm/

[8]. The Rise and Fall of Bitcoin, https://www.wired.com/2011/11/mf_bitcoin

[9]. State Of Bitcoin 2016 – A Summary For Bitcoin Investors, http://cryptorials.io/state-of-bitcoin-2016-investors-summary

[10]. CurrencywithFiniteSupply,https://en.bitcoin.it/wiki/Controlled_supply

[11]. https://blockgeeks.com/guides/blockchain-applications-real-world/

[12]. https://en.wikipedia.org/wiki/Secure_Hash_Algorithms

[13]. http://www.cs.miami.edu/home/burt/learning/Csc609.142/ecdsa-cert.pdf

**Cite this article as :**

Varanasi Deepthi, "An Exploration of Block-chain in the Financial World ", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 5 Issue 4, pp. 206-212, July-August 2019. Available at doi : https://doi.org/10.32628/CSEIT195415

Journal URL : http://ijsrcseit.com/CSEIT195415