IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-5, May 2019 E-ISSN: 2347-2693

Exploring the concept of Blockchain in Cryptocurrency and its uses in decentralizing banking system

Salil Abrol[1*], Ajay Dureja[2]

[1] Department of Computer Science & Engineering, PDM University, Haryana, India
[2] Department of Computer Science and Engineering, PDM University, Haryana, India

[*]*Corresponding Author: salilabrol@hotmail.com, Tel.: +91-7861900004*

DOI: https://doi.org/10.26438/ijcse/v7i5.263271 | Available online at: www.ijcseonline.org

11/May/2019, Published: 31/May/2019

***Abstract*—** The term blockchain emerged in trend with the popularity of the cryptocurrency called the Bitcoin, which also got the name tag "Digital Gold'. The idea of the cryptocurrency was to decentralize the currency system by establishing transactions over distributed peer to peer network. The technology of Blockchain was adopted to achieve this motive. The term blockchain comes from the idea of list of blocks, growing continuously over time wherein every block carries the data relating to the transactions and data regarding the cryptographical linkage using secure hash algorithms and the protocols. The idea was adopted from the paper that described about timestamping of digital document published by two people named S. Haber and W. S. Stornetta. The blockchain concept helped to revolutionize the system so as to prevent accidental leak and updation of confidential data, as there is no central authority or central server in this system that can be bribed to achieve the falsely motive. Through this paper, there is a lot to learn about the blockchain technology, its working and its applications.

***Keywords*—**Blockchain, Bitcoin, Distributed P2P network, Blocks, Transactions, Timestamping, Digital Document, Cryptographical linkage, Secure hash algorithms, Protocols.

I. INTRODUCTION

The term BLOCKCHAIN first existed in the year 2009. However, in 1981 two people named Stuart Haber and W. Scott. Stornetta published a paper on "How to timestamp a digital document" [1] which laid the initial basis of further research in the field of BLOCKCHAIN. The paper focused on how we can secure a digital document so as to prevent illegal and accidental updation of data and to prevent the chance of illegal forward dating and backward dating of the document by the means of digital signatures.

A person (or group of people) known as Satoshi Nakamoto in 2008 first implemented Blockchain. It was implemented in the later years by Nakamoto as a major part of the Bitcoin, which is a cryptocurrency implemented using Blockchain [2]. Blockchain is used as the public ledger for all transactions carried out on the peer to peer distributed network. Due to blockchain, was the first digitalized cryptocurrency to successfully solve the double spending problem without any employment of a server or a central trusted authority and has been the initial basis for many additional uses.

The technology of Blockchain was adopted to achieve this motive. The term blockchain comes from the idea of list of blocks, growing continuously over time wherein every block carries the data relating to the transactions and data regarding the cryptographical linkage using secure hash algorithms and the protocols. Each block carries a cryptographical hash of the previous block, a timestamp, nonce value, and the data [3]. The blockchain was invented so as to make it resistant to data modification such as an example where shopkeepers can modify their invoices later on, or the people may bribe the central authorities to make illegal modification of data. Block chain is a mechanism that stores and manages the data and the transactions over a decentralized network and is a public ledger. Due to the decentralization, the data is safe and permanent that is once written as there is no central server or authority that can be bribed. Data once written is permanent which cannot be altered or deleted at any point of time later on. BFT (Byzantine fault tolerance) is a parameter that is used to regard security of a Blockchain computing system [4]. Decentralization is therefore achieved using peer to peer networking. Thus, we may see the use of this technology in all the areas where we still rely on servers and central management authorities and revolutionize the era by implementing blockchains.

Blockchain was built for its use in crypto coin that is the bitcoin as its public ledger. This made it the first digital crypto currency to solve the problem of double spending (a

same digital coin/token/document/tender is used more than once) in a decentralized manner or we can say by without using centralized servers or authorities.

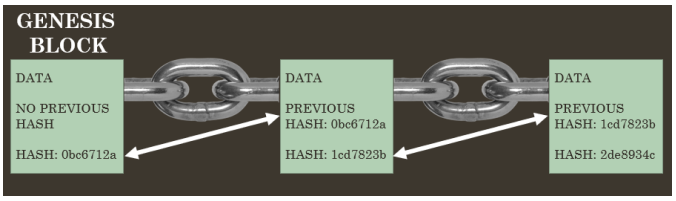

Figure 1 Typical structure of a BLOCKCAIN

Rest of the paper is organised as follows, Section I contains the introduction of Blockchain, Section II contains the description of main component of Blockchain that is the Blocks, Section III contains some relevant concepts about the Blockchain technology, Section IV contains the idea of Hash Cryptography adopted in the Blockchain technology, Section V contains the concept of Immutable Ledgers and Peer to Peer networks which is the backbone of blockchain, Section V discusses about the concept of mining, that is how the blocks are added to the chain, Section VI discusses about the protocol that is used while the chains get updated that is the Consensus protocol and Section VIII concludes the research work with future discussions.

II. BLOCKS

Blocks hold batches of valid transactions that are hashed and encoded into a Merkle root tree. Each block includes the cryptographic hash of the previous block in the blockchain, linking the two. The linked blocks form a chain. This iterative process confirms the integrity of the previous block, all the way back to the original genesis block [5].

Sometimes, there can be a possibility of temporary fork, which is due to the fact that blocks are mined one after another continuously. The algorithm that we use in Blockchain s SHA (Secure Hash Algorithm), but there may be some other mechanisms that can co-exist to choose which block have to be added to the blockchain, so the blocks are scored and the block with the highest score finds its place in the Blockchain. The low score blocks which are not added or are discarded are called orphaned blocks. Peers in the network keep only those blocks in database that have high score index. If by chance a block with more score index is encountered or is mined later on, peer will update its list by removing the block and replacing it with the more accurate block. So, this gives us a picture that there is no guarantee whether a particular entry will remain in the blockchain or it may get replaced. In the blockchain system, there are prizes for the miners who mines the block and if the block gets accepted they are paid more fees, but as the probability of remaining a block in the blockchain is decreased at stages, thus it is very competitive to mine a block with high score value and therefore the chain having with the most appealing proof-of-work is always regarded as the best chain and validates the network. [5].

Figure 2 Structure of a Block in Blockchain

III. UNDERSTANDING THE BLOCKCHAIN CONCEPT

The blockchain concept revolves around the following key entities −

- Hash cryptography.
- Immutable ledgers.
- Distributed peer-to-peer (P2P) networks.
- Mining.
- Consensus protocol

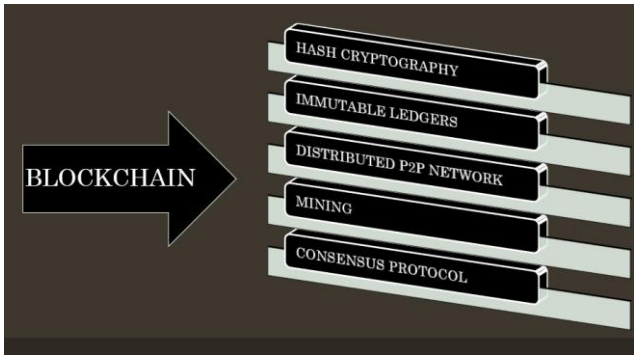

Figure 3 Blockchain Concept

- **Hash Cryptography**

The concept of hash cryptography is like a fingerprint to a document. Just as a fingerprint is an identity of human being, similarly hash is an identification number for a document.

- **Immutable Ledgers**

The term ‘immutable’ means non-changeable or something that cannot be tampered with and the terms ‘ledgers’ mean records. The concept of immutable ledgers together meaning non-changeable records apply in BLOCKCHAIN which implements the DATA-SECURITY.

- **Distributed peer-to-peer(P2P) networks**

A peer-to-peer (P2P) network in which interconnected nodes ("peers") share resources amongst each other without the use of a centralized administrative system.[2]

Figure 4 Distributed P2P Network

- **Mining**

Mining is the term that we use for the process that makes the blockchain to be a decentralized secure system. It secures the blockchain system and enable a system without any server or a central authority. Mining allows the user to create new blocks for the blockchain ensuring decentralization.

- **Consensus protocol**

Consensus protocol ensures two important security parameters:

1. Dealing with the Attackers that attack the blockchain system.
2. Dealing with the simultaneous updation of blockchain at two peers and resolving it.

IV. HASH CRYPTOGRAPHY

A hash is a function and cryptography is the way of encoding the data thereby implementing the data security. The data is applied with a hashing function, and the output of the hashing function is then encoded to get a number which is sequence of digits and can be understood only by a decoding mechanism [5].

- **USE OF HASH IN BLOCKCHAIN**

A hash defines the fingerprint for a document so that the document is uniquely identifiable with the corresponding hash value assigned by the hash function or hash algorithm. The blockchain implements the hash cryptography with the help of hash algorithms.

- **FIVE REQUIREMENTS OF A HASH ALGORITHM**

A hash algorithm must satisfy the following 5 requirements −

1. It should be one-way.
2. It should produce deterministic results.
3. It should have fast computation.
4. The avalanche effect.
5. It should withstand collisions.

- **UNDERSTANDING THE SHA256 HASH**

SHA stands for Secure Hash Algorithm and the value 256 represents the no. of bytes, meaning the SHA256 hash will be of 256 bytes. The SHA256 hash will be 64 characters long and is basically a number, more specifically a hexadecimal number. As it is hexadecimal number, it will comprise of digits from 0 to 9 and letters from A to F representing the numbers 10 to 15.

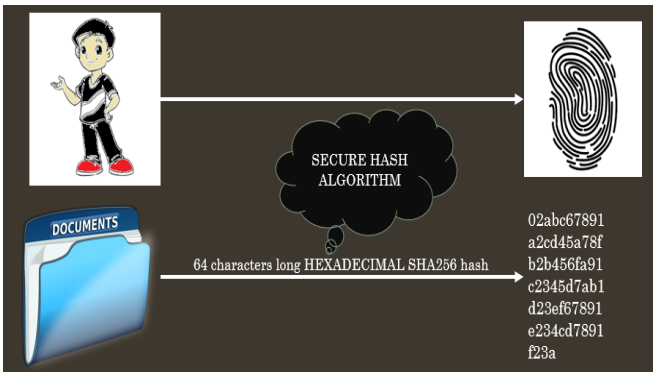

Figure 5 SHA256 ALGORITHM CONCEPT

- **WORKING OF SHA256 HASH ALGORITHM**

The SHA256 satisfies all the 5 requirements of the hash algorithm so, it is the most widely accepted hash algorithm that is used.

The SHA256 produces the 64 characters long sequence of digits for every change in the data.

For example, if there is no data written in the document then also the hash code will be generated as in below image:

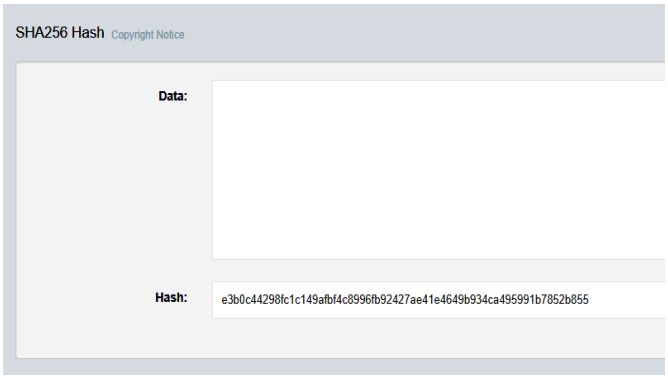

Figure 6 SHA256 hash without any data.

Now, suppose we write some data to the document, then the hash code completely changes.

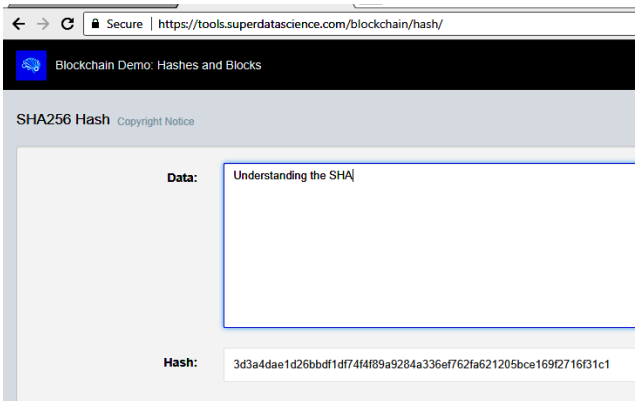

Figure 7 SHA256 hash with some data.

And now, if we change the data,

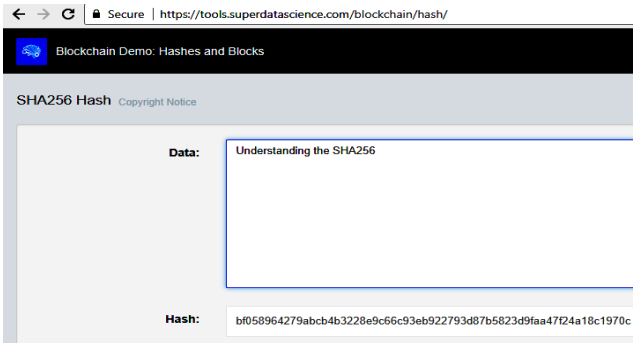

Figure 8 SHA256 hash with some changed data.

So, every time a new hash code is outputted by the algorithm, which signifies the Avalanche effect that upon a small change there will be complete change of the hash code. The hash code generated represents the fingerprint of the data that is unique for every data.

V. IMMUTABLE LEDGERS AND PEER TO PEER NETWORK

The concept of immutable ledger lies in its name only, where immutable means something that cannot be changed, and ledger means a record. So, an immutable ledger means a record that cannot be changed, which is the foremost requirement of a blockchain as by the definition of blockchain: Blockchain is list of records called the blocks that are related to each other. So, we need to maintain the immutable blocks in the blockchain so as to implement the data security.

Consider an example,

You have earned money through lots and lots of hard work and now it's the time to spend the money for your basic need that is owning your dream home. You contact the brokers or the owners of the house you dreamt about and finally you pay them the amount and get a deed stating that the previous owner has sold the property to you in specific amount and now the house is yours.

The next step is that both of you i.e. the previous owner and you have to go to a government registry office with the deed to get the property registered under your name by removing the name of previous owner and writing your name. For this, the government charges some registration fee and updates their records as per the deed made. The records of the government body may be in the computerized format or in the form of traditional ledgers where entry is marked with ink on paper. In both the cases, there is a possibility of tampering or forging the data.

Any hacker can creep into government intranet of the registry office and can do unauthorized updation of data by removing your name and writing someone else's name in the registry record or if it is pen-paper ledger, the task is much easier.

So, now the house for which you spent your hard-earned money is now not yours legally as you only have now the deed which you made with the previous owner which is not a legal document, the legal document is the registry of the house which is now changed by the hacker.

So, now there will be disputes and eventually the case would be one by the person whose name is written in the records of government.

Figure 9 Problems with traditional ledger system.

These kinds of problem are very common and thus there is need to implement the more secure means of record keeping, and that is done by blockchain.

Now in a blockchain, each block will represent the owner of the house, where first block is the first owner, second block is the second owner to which the first owner sold the property and so on, the blocks will be added to the chain. Now each block contains the previous hash value, i.e. the hash value of the previous block, so if a hacker hacks a block and changes the data in the block, then hash of the block will change as the SHA256 immediately changes the hash for a minute change in the data, then, the block next to it will be containing the old value of previous hash, which is also to be changed now by the hacker, and if the hacker

updates the value of previous hash in next block then now this block's hash will be changed thus again hacker will have to update the next upcoming block with a new 'previous hash' value. Thus, the hacker has to update all the blocks after the block in which it changes the data, which will be very tedious task as this has to be done while network is in operation and hacker can be caught at any time.

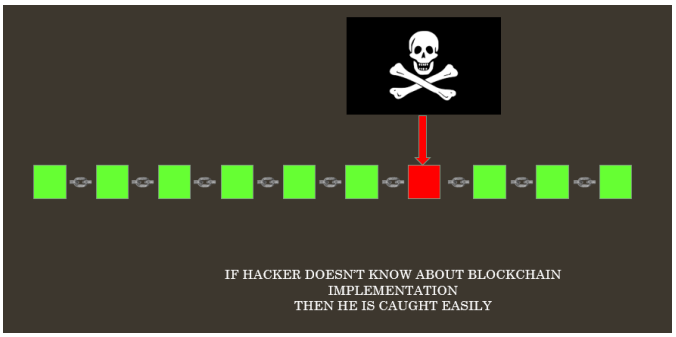

Figure 10 Hacker attacking the blockchain ledger system.

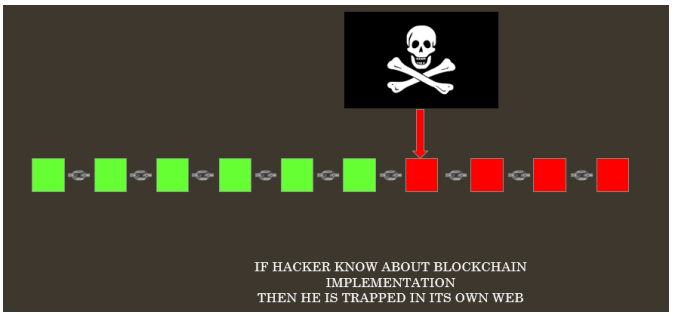

Figure 11 Hacker updates all later blocks.

Let's say, the hacker succeeds to update all the blocks, then there comes the role of P2P network, In the P2P network [2], the blockchain is present with every node and the neighbouring nodes in the network are mutually contacting with each other, so while communication they may detect that the blockchain with this particular node is not same as our blockchain, thus one of the neighbouring node will copy-paste its blockchain to the node which is not having valid blockchain, thereby maintaining the consistency of data. All the task, the hacker did by spending large amount of time, will be discarded in couple of seconds.

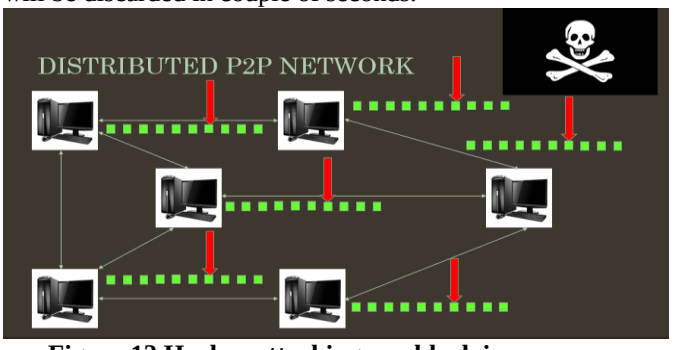

Figure 12 Hacker attacking one block in one peer.

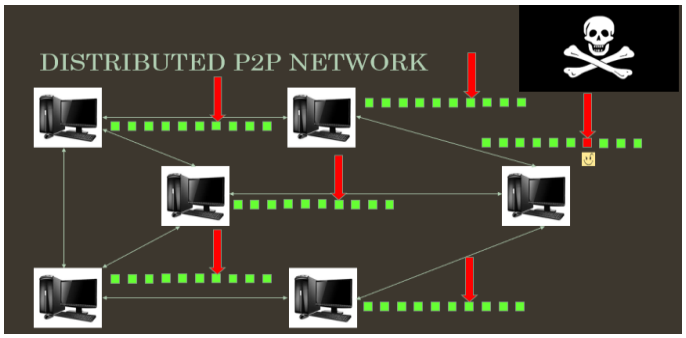

Figure 13 Hacker attacked block in one peer.

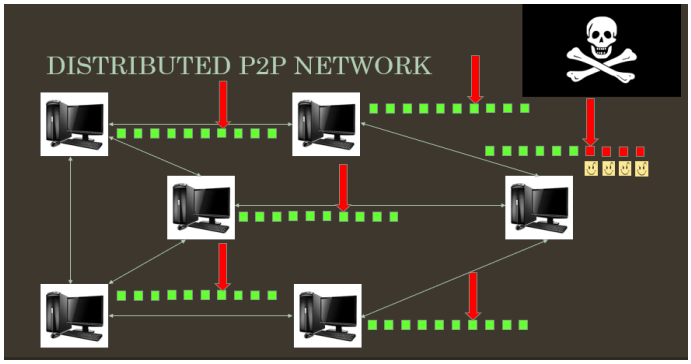

Figure 14 Hacker forced to attack all later blocks in one peer.

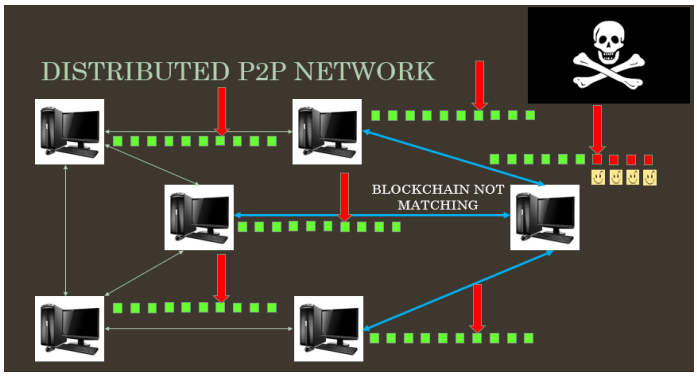

Figure 15 Neighbouring links passed message about invalid blockchain.

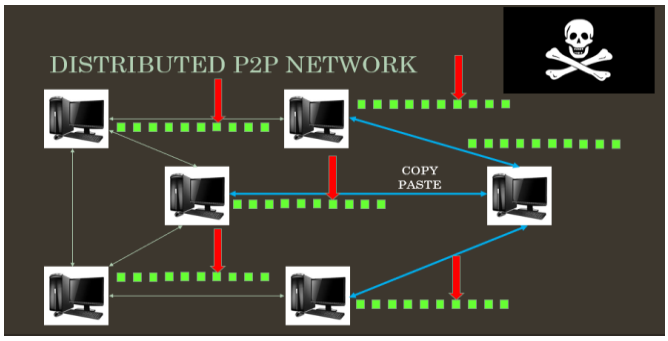

Figure 16 Neighbouring links replaced the invalid blockchain with valid one.

VI. MINING

Mining is the process of adding a valid block to the blockchain with added security features to be kept in mind. Mining is usually a hard process and the miner who successfully mines a block in blockchain is paid a reward in addition to a small fee for mining. The reward is usually in the modes of cryptocurrency [5].

Mining is accomplished by adding a valid block at the end of a blockchain. The block as you know till now contains a block number, data, previous hash and current hash.
For the process of mining, lets now get introduced to a new entity in the block, that is the 'Nonce'. Nonce means Number used only once.

As we know, we cannot change the block number, if want to add a block, the block number will be 1 plus in the previous block number always and we cannot change the data as well as the previous hash. So, the entity nonce is introduced so that we can change something in the block. Depending on the Nonce, previous hash, block number and the data the SHA256 will compute a hash for the current block. So, for different Nonce, there will be different hash codes produced due to the avalanche effect.

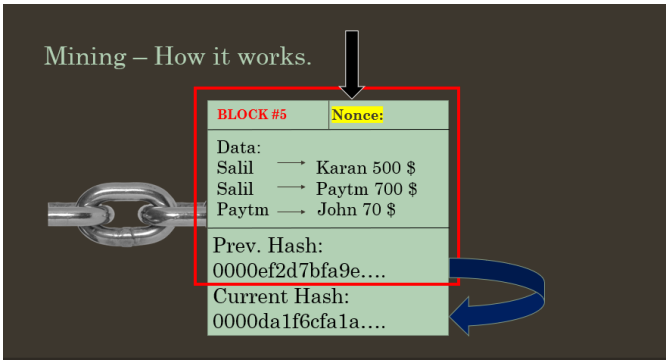

Figure 17 Calculation of hash for the block to be mined.

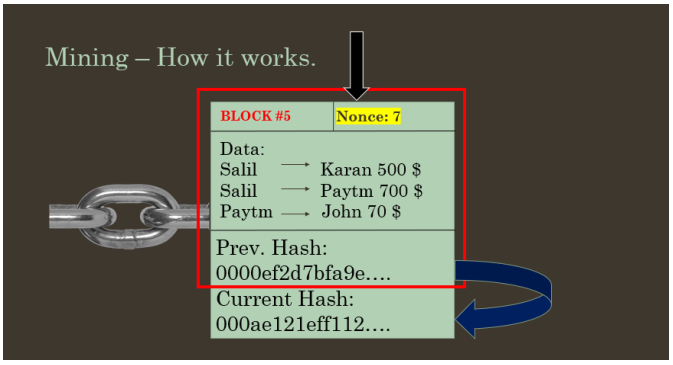

Figure 18 Variation of hash on changing nonce.

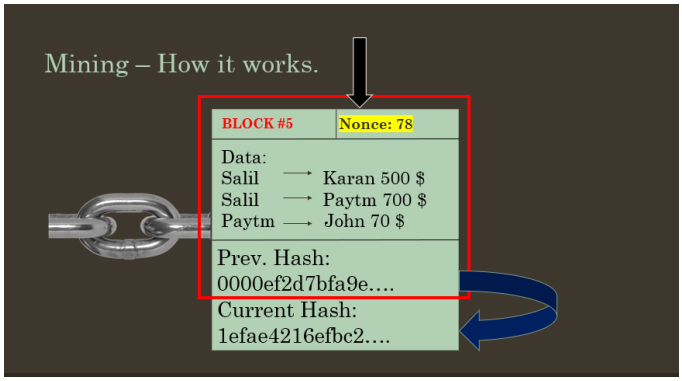

Figure 19 Variation of hash on changing nonce.

When a miner does mining of block, it is made available to a pool of hashes. And he/she has to mine the block which will have has one out of the available hashes.

Figure 20 Pool of hashes.

Now, the task is made bit difficult for the miner by the blockchain system. The blockchain system sets a target for the miner to have a hash within a target area.

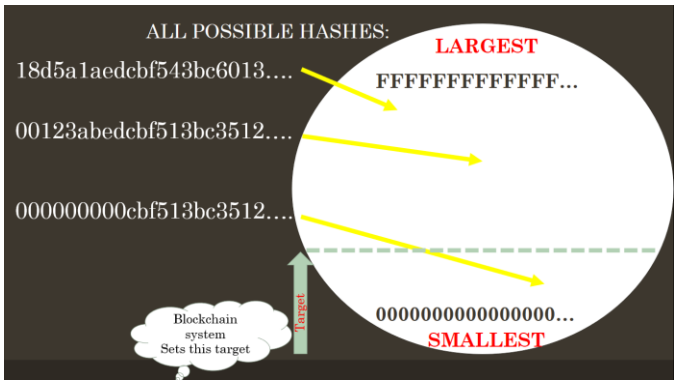

Figure 21 Target set by blockchain system.

This creates a lot of problems for the miner and is usually like a game. If the miner is successfully able to mine the block with hash within that area, the block will be added to the blockchain and the miner will be rewarded with some amount of money for doing this, which he actually deserves

for this whole process. Also, he is rewarded with a small mining fee for bringing the block in the blockchain system.
Now, the question is
How the miner will be able to get the hash within that target area?

The answer is through Nonce.
Nonce is varied in the block, and when the nonce is varied, the hash changes due to the avalanche effect of SHA256. Thus, whenever a block is mined such that it has a hash within the target value, the mine is now the king.

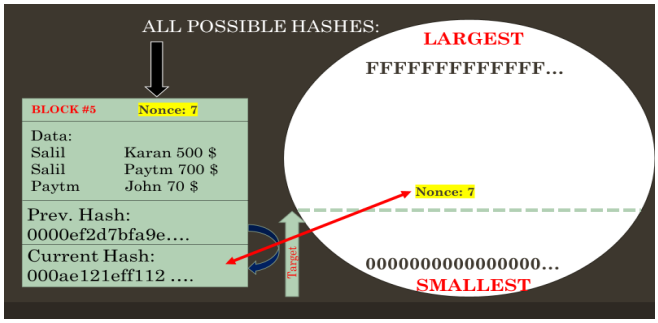

Figure 22 NONCE value 7 out of range.

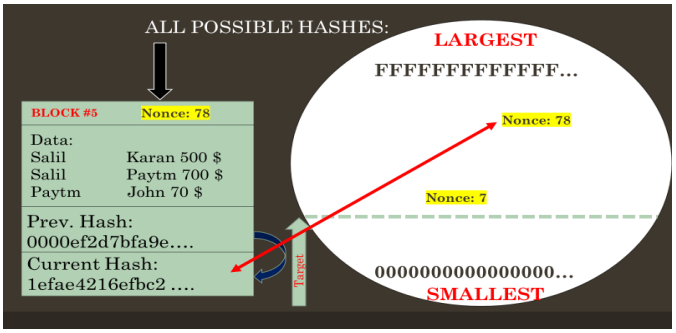

Figure 23 NONCE value 78 out of range.

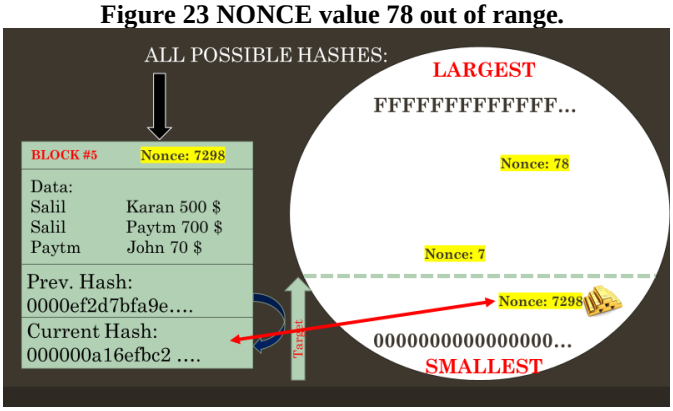

Figure 24 NONCE value 7298 in the range.

VII. CONSENSUS PROTOCOL

Consensus protocol is the protocol that governs the security features within a blockchain [5]. The consensus protocol is based on the byzantine fault tolerance principle and is used for 2 major tasks in the blockchain system:

- It deals with the attackers, attacking the blockchain.
- It deals with the problem of simultaneous addition of two blocks at a time, each a different peer in P2P network.

The byzantine fault tolerance principle helps to deal with the non-cooperating / not reliable / phishy node in a peer-to-peer distributed network.
Now suppose, while a block has to added to the blockchain, it is added at a peer and is propagated to all the chains over the network and this block is the block added at the end of the block.
Now the question is:
How the blockchain system comes to know that the block is a genuine block by some innocent miner or a block from a hacker?
The answer is the set of rules which are written for governing this task by the consensus protocol. The rules are 1000s in number and through various mechanisms they check the genuineness of the block.

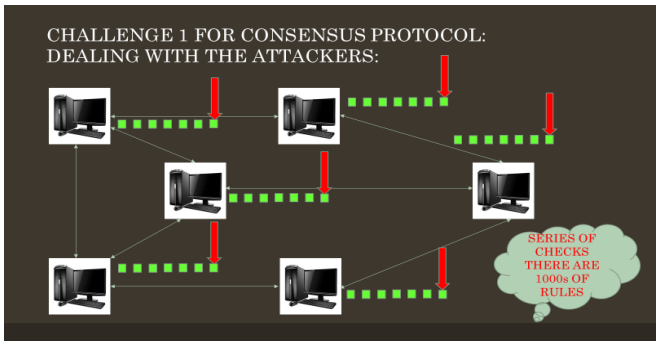

Figure 25 Series of checks for checking the genuine block.

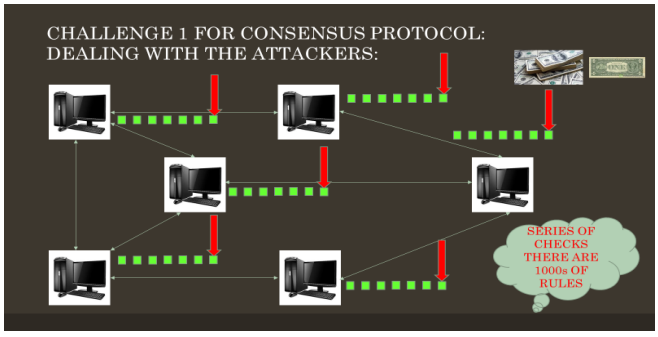

Figure 26 - The peer rewarded for genuine mining.

Now there may be a situation in the blockchain mining system that, a block is added at one peer and while the system was propagating the block to the other peers, at same time or some time in between another block is added to the blockchain in some other peer. This creates the situation of two competing chains.

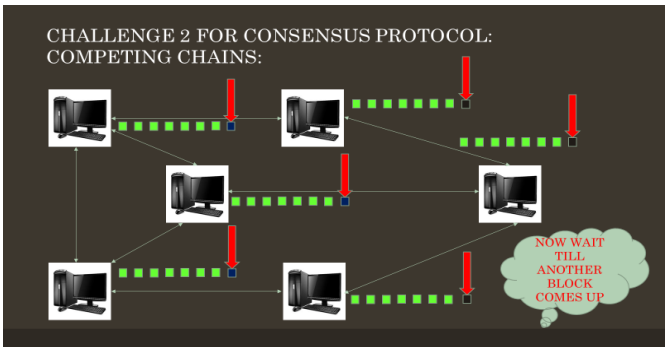

Figure 27 Competing chains.

The problem of competing chain arises because of the network delay or the power of hash function of various peers. The faster peers propagate the block fastly to other chains, but the peers with lower power propagate the block slowly.
So, to deal with this problem, the system will wait till the time some other block comes in the view of the blockchain system at some peer. Now that block if added to the peer which has the greater hash power, will make the block propagate to other peers in the network.

Now when this new node is propagating the blockchain system will check to which chains out of two competing chains the node is added at first. The chain which has the second new block at the first, will win and the same blockchain will be copied to all the peers in the network.

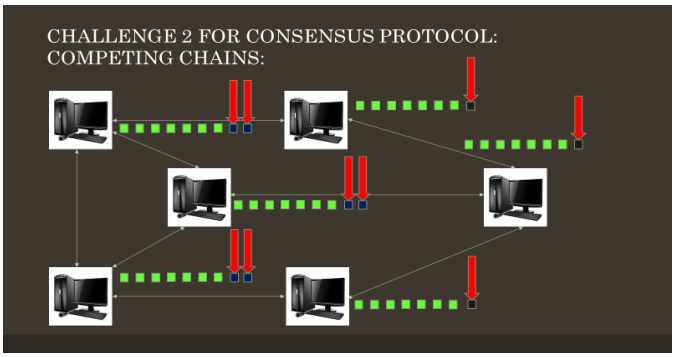

Figure 28 New node added to the blue chain.

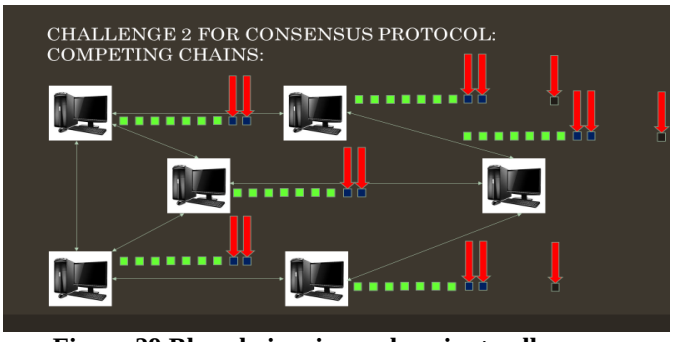

Figure 29 Blue chain wins and copies to all peers.

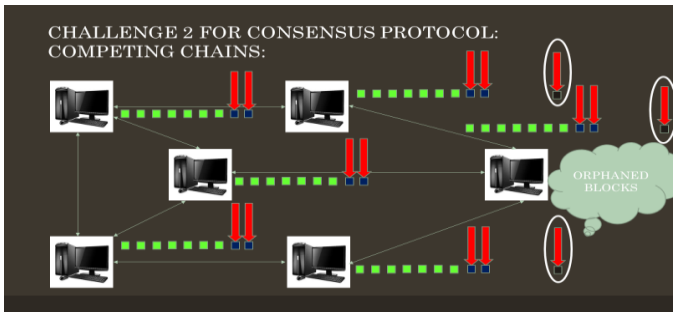

Figure 30 Orphaned blocks.

The loosing chain discard the blocks that were now invalid to the chain. These blocks are called the orphaned blocks and now are of no use. All the power, money and resources of the miner are now wasted that he spent on mining and will not get any reward till the time he again computes the hash for the blocks and again projects them to the system.

VIII. CONCLUSION

BLOCKCHAIN technology as we saw is a very intelligent method to solve the world's largest problem that is the data Security. The term blockchain was limited to originally for the cryptocurrencies but now it is a universal method that can be implemented to various projects and various sectors for implementing the security within the whole sector. Being an emerging technology, it will occupy our surroundings in every way and thereby providing us a secure digital world. This review paper carried only the understanding about the blockchain technology and concludes with the hope to show the practical implementation of this technology so as to build a new Cryptocurrency based on Blockchain, or can be adopted as a very efficient method to implement the Banking systems, ledger systems, accounting systems, payment wallets, credit and debit management in a totally decentralised manner without any central governing body.

REFERENCES

[1] S. Haber, W.S. Stornetta "How to timestamp a digital document", Journal of cryptology, Vol.**3,** no. 2, pp.**99-111**, **1991**.

[2] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.[Online]. Available: https://bitcoin.org/bitcoin.pdf

[3] L. Lamport, R. Shostak, and M. Pease, "The byzantine generals prob-lem," ACM Transactions on Programming Languages and Systems(TOPLAS), vol. 4, no. 3, pp. 382–401, 1982.

[4] C. Miguel and L. Barbara, "Practical byzantine fault tolerance," inProceedings of the Third Symposium on Operating Systems Design andImplementation, vol. 99, New Orleans, USA, 1999, pp. 173–186.

[5] Z. Zheng, S. Xie, H. Die, X. Chen, H. Wang, "*An Overview of Blockchain Technology:Architecture, Consensus, and Future Trends*", In the Proceedings of the 2017 IEEE 6th International Conference on Big Data, **Honolulu, HI, USA**.

Authors Profile

Salil Abrol pursed Bachelor of technology from PDM College of Engineering, MDU University in year 2017. He is currently pursuing Master of Technology from PDM University, Bahadurgarh, Haryana.

Ajay Dureja pursuing Ph.D. from DCRUST, Murthal, Sonepat. He pursed Master of Technology from PDM College of Engineering, MDU University in year 2010. He pursed Bachelor of Technology from Bhiwani Institute of Technology & Sciences, MDU in year 2007. He is currently working as Assistant Professor in Department of Computer Science & Engineering, PDM University since 2010. He has published more than 20 research papers in reputed international journals including Scopus Imdexed and conferences including IEEE and it's also available online. His main research work focused on Internet of Vehicles, MANET and Image Processing. He has 9 years of teaching experience and 4 years of Research Experience.

