IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.-7, Issue-6, June 2019 E-ISSN: 2347-2693

Bitcoin in Blockchain: A Survey

Syed Zishan Ali[1*], Dolly Sahu[2], Jatin Sahu[3]

[1,2,3]Dept. of Computer Science & Engineering, Bhilai Institute of Technology Raipur, CSVTU, Chhattisgarh, India

Corresponding Author: zishan786sl@gmail.com, Tel.: +919977701133

DOI: https://doi.org/10.26438/ijcse/v7i6.708712 | Available online at: www.ijcseonline.org

Accepted: 14/Jun/2019, Published: 30/Jun/2019

Abstract—The emerging technologies have highly incorporated with crypto-currencies and one of them is bitcoin which has a great effect on the digital marketing and day by day the amount of data associated with it is facing a steep growth and lots of security challenges are coming into play. In order to prevent the system from fraudulent transactions several methodologies have been used. In this study we have described how a digital currency can be maintained by the use of distributed decentralized ledger.

Keywords— Bitcoin, Blockchain, Mining, Proof-of-Work, minting, forging, proof-of-stake, Ledger Maintenance.

I. INTRODUCTION

With the expeditious development in the field of information technologies, the electronic currencies have escalated in recent years, which gave a new definition to the online trading system. Furthermore, in the meanwhile, the virtual (or digital) currency contemporary to the standard currency came into view the crypto-currencies were introduced one of them is ***Bitcoin***. The Bitcoin concept was first introduced by an unknown individual (or a group of people) named Satoshi Nakamoto. *Bitcoin* is a peer-to-peer crypto-currency and a decentralized worldwide payment system for digital currencies [1] here all the transaction takes place without intervention of any trusted third party authorities, it is performed entirely among the users in collaborative manner.

To verify their integrity, authenticity, and correctness of the transaction among the bitcoin we use group of network nodes (miners) and the then register the information regarding the transaction in the public ledger called as ***blockchain***. The rudimentary framework to perform all kinds of bitcoin related operations are provided by blockchain here each and every transaction is broadcasted to all peers into the network, instead of mining a single transaction, miners bundle a number of transactions that are waiting in the network to get processed in a single unit called a ***block***. A miner then advertises a block across the whole network as soon as it completes its processing (or validation) in order to claim a mining reward [1]. One of the node among the network can crash or behave abnormally such incident may lead to an interrupt during communication. Therefore, in order to guarantee an uninterrupted communication all nodes in the network need to run a fault-tolerant consensus protocol.

The implementations of digital currency have a way to secure its blockchain against attack, i.e., the security of the entire network relies on the ***Proof of Work (PoW)*** algorithm in the form of the block mining. ***Proof-of-Work (PoW)*** is one of the most widely-adopted consensus mechanisms. PoW requires a significant amount of computation effort to find a block that meets the consensus protocol [2]. The participating node in the mining process is required to solve computationally very difficult problem to ensure the authenticity and validity of newly mined block. PoW was considered to be resource intensive which resulted in high power consumption which leaded to find a similar bitcoin protocol which was not based on expensive computation rather it solely relied on an algorithm referred to as Proof-of-Stake. The idea behind proof of stake is simple. Instead of mining power, the probability to create a block and receive the associated reward is proportional to a user's ownership stake in the system [3].

1. BITCOIN

The era of cashless transactions began with a great impact on the society but all cashless transactions are done with the help of trusted third parties. While the system works well with good efficiency but still suffers from the primary weakness called as *trust based model* [4]. People have to rely upon the third party for making successful transactions which lowers the efficiency of the online transactions a little bit. These transactions are a little complex and costly mainly in case where transactions has to be reversed.

So, rather than going for third party a pure peer-to-peer version of electronic cash came into action by an unknown

person named *Satoshi Nakamoto* in 2009 called as *BITCOIN*. A bitcoin is considered to be a crypto-currency, but after the introduction of crypto-currencies in 1983, bitcoin was the very first distributed crypto-currency system to get introduced in 2009. "It's like paying cash to the shopkeeper and getting the change back" [4]. Reversibility of transactions is quiet easy. The transactions are publically known but are extremely secure due to the mechanism used behind making of the bitcoin called as *blockchain*.

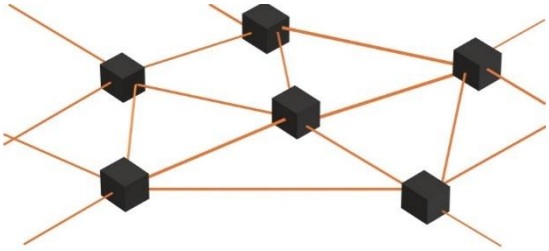

Fig 1. Distributed Ledger using Blockchain

The main idea behind the origination of such crypto-currency was to get a decentralized digital currency whose monetary power was not controlled by any party. Bitcoin is a distributed digital currency system based on a P2P networking system and a decentralized probabilistic consensus protocol where all payments and exchanges are accomplished electronically through the transaction between clients [4].

The blockchain technology had undergone a great hike and was in a dense media attention due to the uninterrupted growth in the value of bitcoin. So, a number of central banks started recently to explore the adoption of crypto-currency and blockchain technologies. For example, the People's Bank of China aims to develop a nationwide digital currency based on blockchain technology; the Bank of Canada and Monetary Authority of Singapore are studying its usage for interbank payment systems; the Deutsche Bundesbank has developed a preliminary prototype for blockchain-based settlement of financial assets. Many proponents believe that crypto-currency and blockchain technology will have a significant influence on the future development of payment and financial systems.

2. BLOCKCHAIN

Blockchain is a decentralized distributed ledger or data structure. It can be referred to as chain consisting of blocks where a particular block refer to a block prior to it. Once the information details related to the transaction performed are fed into the blockchain then, it is beyond the possibilities to tamper that details. Blockchain networks are completely acquainted with the transaction taking place in order to maintain the ledger in the form of blockchain each block present in the chain is built on the top of the previous block and it uses latter's nonce and signature as a key for moving to the next block. The process of building a new block and addition of it to the chain is done by the miners. It is not easy to add the blocks in blockchain and there is a reward of 12.5 bitcoin for that. Therefore we can define it as a consensus oriented secured distributed public ledger which allows to store the data over peer to peer network.

Advantages:

Few of the features of blockchain are listed below -

1) Immutable: it is nearly impossible to alter or tamper the block.

2) Irreversible: this feature helps to prevent from double spending.

3) Distributed System: it means that each and every transaction is broadcasted throughout the network.

4) Decentralized: It doesn't depends on a central server.

5) Resilient: with this feature we come to know that it is not prone to any sort of attack.

Evolution of Blockchain:

We are discussing about Bitcoin in Blockchain. Satoshi Nakamoto invented Bitcoin and since then, it is the most popular and used crypto-currency. He developed the Bitcoin concept as digital currency. This was consider to be resilient and trustworthy with some anomalies as listed:

1) It was essentially built as digital currency is not applicable for other modes.

2) The main was to achieve the maximum possible consensus in order to process the transaction it wasn't bother about the time taken to validate the same. [5]

3. ALGORITHMS USED

A. SHA 256

The Secured Hashing Algorithm, i.e., SHA-256 takes 512bit input and gives 256-bit unique hash as output. These hashes are generated from the content which each of the blocks contain in a blockchain. The hash generation does not depend on the size of the data, i.e. data of any size is converted into 256-bit hash.

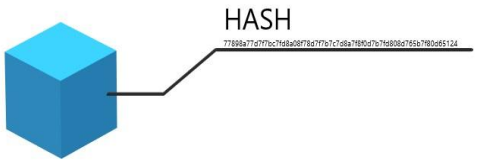

Fig 2. 256-bit hash code of single block

Algorithm:

Here 8 registers are used holding 32 bits each which when concatenated gives the 256-bits hash code. These registers predefined initially as per the requirement of the compression function. These values are the fractional part of the square roots of first 8 primes:

- Register Initialization :

a = 6A09E667
b = BB67AE85
c = 3C6EF372
d = A54FF53A
e = 510E527F
f = 9B05688C
g = 1F83D9AB
h = 5BE0CD19

- Now if the input string is not of 512 bits then padding is done by concatenating the original string with 1 and 0 until the count reaches 512 bits.

- The padded string is divided into N number of blocks which is then used for N times computation of compression function. Using this compression function we evaluate the hash code.[6]

II. METHODOLOGY

A. Proof-of-Work

The Proof-of-Work protocol is governed by the combination of cryptography and computational power which enable us to create consensus and also ensures the genuineness of data recorded over the blockchain network. To prove the validity of the block and the assurance of the viability, the nodes in the network (called miners) use their computational power endorse all the transactions(i.e. verify that a sender has enough funds and is not double-spending) and significantly compete with other peer nodes in a race to solve complex cryptographic problem obtrude by the corresponding protocol the first node (miner) who gave the solution is recompense with a defined endowment and accumulates all the transaction fees associated with the transactions[7]. An inevitable significant amount of computation effort is entail to find a block to meet the consensus protocol. Since it resemblances to the process of digging for gold in a mine, it is called as mining.[2]The process of mining necessitate computers to be capable of running with maximum capacity, which result in consuming a considerable amount of electric power which shows that PoW is a resource-intensive consensus protocol.

Bitcoin as an example of a crypto-currency system secured with a proof of work algorithm. Each block in Bitcoin consists of two parts:
• block header of key parameters, including block creation time, reference to the previous block and the Merkle tree root [4] of the block of transactions
• block list of transactions.[3]
To reference a specific block, its header is hashed twice with the SHA-256 function [8]; the resulting integer value belongs to the interval $[0, 2^{256} - 1]$. To account for different possible implementations, we will use a generic hashing function hash $(\cdot)$.

The proof work is performed in certain number of steps listed below:
Step I: One of the node in the blockchain network is willing to perform a specific transaction.
Step II: The transaction details are now broadcasted throughout the network and are waiting to be processed by the miners present in the network.
Step III: A Miner picks up the block which was broadcasted and try to add it as a new block in the distributed ledger.
Step IV: To add this block of transaction to the blockchain the block first needs a signature, for the same the miners need to solve very complex mathematical problem that is unique to each block.
Step V: The miner that finds an eligible signature (solution) for its block first, broadcasts this signature to all the other miners.
Step VI: The miner that finds a solution sends his 'proof of work' (or solution) to the other miners, and they in turn verify if the solution is legitimate. If it is then it gets is broadcasted to all other nodes on the network along with its signature.

With the reference to [9] because of the excessive electricity consumption and use of hardware resources to solve the complex problems. We have seen that the cost of Bitcoin mining on commodity hardware now exceeds the value of the rewards. To overcome this challenge a new consensus mechanism which is less resource intensive came into existence named Proof-of-Stake.

B. Proof-Of-Stake

It is considered to be one of the possible decentralized secure ledger implementation not based on expensive computations and completely relies on *proof of stake* (*PoS*) algorithm. Proof of stake, another consensus mechanism for digital currencies which is an alternative to proof of work used in Bitcoin. The proof of stake is consider to be a superior approach because of the absence of expensive computations. The simple idea behind PoS is, the probability to create a block and receive the associated reward is proportional to the user's ownership stake in the system not the mining power [3].

The logical basis behind proof of stake is the following: users having the highest stakes in the system is more willing to maintain a secure network, as they will be the one who will suffer the most if the reputation and price of the crypto-currency would depreciate because of the attacks.

The proof-of-Stake (PoS) consensus protocol go after a different approach, which gives the decision-making power of block inclusion to those possessing stakes in the system irrespective of the length of the blockchain or public ledger's history. Ability of a participant to add its block in the Blockchain is proportional to the amount of stake its own in the system, here stakes can be elucidated as the total digital currency a participant possess in the system.[10]

Proof-of-stake undeniably replace most the functions of proof-of-work's with careful redesigning of security model of bitcoin minting.

Benefits of proof of stake:

1) Doesn't require specialized and expensive hardware to run.
2) Anyone with enough coins to stake can validate transactions on the network
3) Proof of Stake is considered to be more energy efficient and environment friendly than Proof of Work.
4) Proof-of-stake cannot be easily forged.
5) Reduced threat of 51% attack (There is no chance that 51% stake of entire network will belong to an individual) [11]

Proof-of-stake undeniably replace most the functions of proof-of-work's with careful redesigning of security model of bitcoin minting.

C. LEDGER MAINTENANCE

When several bitcoin transactions are done then the record of such transactions are kept in *blocks.* The average block size of a single block is approximately 1MB. So each block has record of a number of transactions in it. Now for a large number of transaction records we have a large number of blocks. These blocks are linked together to form a chain called as *blockchain*. The blockchain acts as a distributed ledger for the bitcoin. The ledger maintenance process can be explained as follows:

- Storage of transactions records in blocks:

Let the blocks have two transactions each that are 'T1' and 'T2' (a block has more than two transactions in reality as it has a size of 1MB). Now from the content of each block we create a unique signature which is used to link one block with other. In fig 4, we can see the linkage of two blocks. The signature of the previous block is added to the content of the next block, hence we can also say that the next block is partially dependent upon the previous block for further linkages with other blocks. Along with the transaction records the *timestamp* of each transaction is added to the block. The timestamp consists of the instance of the transaction time.

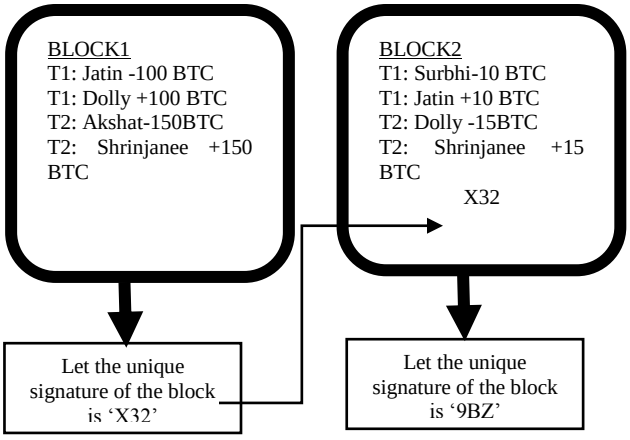

Fig 4.Linking of two blocks

- Generation of Hash Codes:

The unique signatures or hashes are generated from the content present inside the block. If any single character inside the block is tampered then the all the linked blocks which are connected with the tampered block will get disconnected from the chain.

How these unique signatures are generated? The answer is SHA-256 algorithm which is mentioned above. There are various hashing algorithms but in case of bitcoins in blockchain we use Secured Hashing Algorithm, i.e., SHA-256. This algorithm computes a 256-bit that is 64 hexadecimal characters of hash for each string input. For each and every string input we have a unique hash output.

For example, if we add a word 'T1: Jatin -100 BTC' then the output will be:

55703546FF83A76DAC14D48C0829C4832ED9213122BB5E0FFA5307076EA1E116

- Qualification Criteria for adding a block:

A block will *only* be accepted in a blockchain if its digital signature starts with a number of *zeroes*. For example, the hash of the block must contain first 30 bits as zeroes in its hash. Till now a block consists of the transaction records, hash of the previous block (excluding the *Genesis* block), and the Timestamp of each transaction. Since all the blocks have unique hashes depending upon their block content, so it is not possible that each hash will have first 30 bit as zeroes.

Well, in order to give the block a signature that meets the requirements, the string of data of a block needs to be changed *repeatedly* until a specific string of data is found that leads to a signature starting with thirty zeroes. Because the transaction data and m*e*tadata (block number, timestamp, etc.) need to stay the way they are a small piece of data is added to

every block that has no purpose except for being changed repeatedly in order to find an eligible signature. This piece of data is called as the *nonce* of a block. The *nonce* is completely random and could literally form any set of digits, ranging from spaces to question marks to numbers, periods, capital letters and other digits.
The nonce added to the block is hashed along with the content of the block together using the respective hashing function. If the resulting hash meets the requirements then the block is eligible to be accepted by the blockchain or else the nonce is changed repeatedly until the resulting hash meets the requirements. This process of repeatedly changing the nonce to find eligible signatures is called as *mining* and is what *miners* do.

Now a block contains 1) transaction data, 2) timestamp, 3) the signature of the previous block, 4) a nonce. Image 1 below represents the new block obtained:

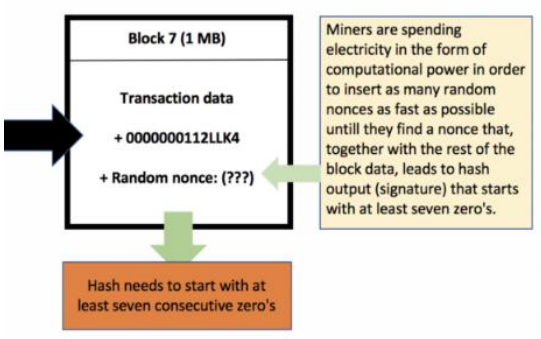

Fig.5 New Block

- Adding a block:

Miners spend electricity in the form of computational power in order to constantly try different nonces. The more computational power they have, the faster they can insert random nonces and the more likely they are to find an eligible signature faster. It is a form of *trial and error*.

Any user on a blockchain network can participate in this process by downloading and starting the according *mining software* for that specific blockchain. When a user does this, they will simply put their computational power to work in order to try to solve the nonce for a block.
The miner who gets the correct nonce first, that miner is eligible to add the block to the blockchain and hence a block is added.

III. CONCLUSION

The main objective of this paper is to make you understand the implementation of bitcoin using blockchain technology. To form this paper we have surveyed both the topics individually and represented the algorithms and methodologies which are used for implementation of bitcoin in the blockchain technology. The algorithm used in this paper is SHA-256 and the methodologies are proof of work & proof of stake. We also have concluded that why the proof of stake came into view by showing the several disadvantages and excessive use of electricity in proof of work.

REFERENCES

[1] Mohamed Rahouti, Kaiqi Xiong and Nasir Ghani,Bitcoin Concepts, Threats, andMachine-Learning Security Solutions, 10.1109/ACCESS.**2018.2874539**, IEEE Access.
[2] Hayungmin Cho, ASIC-Resistance of Multi-Hash Proof-of-Work Mechanisms forBlockchain Consensus Protocols, 10.1109/ACCESS.**2018.2878895**, IEEE Access
[3] www.bitfury.com/content/downloads/pos-vs-pow-1.0.2.pdf
[4] www.bitcoin.org/bitcoin.pdf
[5] Rishav Chatterjee and Rajdeep Chatterjee, An Overview of the Emerging Tchnology: Blockchain, 2017 International Conference on Computational Intelligence and Networks
[6] www.jwar.org.uk/comsec/resources/cipher/sha256-384-512.pdf
[7] www.gdre-scpo-aix.sciencesconf.org/195470/document
[8] Aradhana1, Dr. S. M. Ghosh International Journal of Technical Innovation in Modern Engineering & Science (IJTIMES) , e-ISSN: 2455-2584 Volume **3**, Issue **05**, May-**2017.**
[9]Karl J. O'Dwyer and David Malone, Bitcoin Mining and its Energy Footprint, ISSC 2014 / CIICT 2014, Limerick, June **26–27**
[10] Deepak K. Tosh, Sachin Shetty, Peter Foytik, Charles A. Kamhoua and Laurent Njilla, CloudPoS: A Proof-of-Stake Consensus Design forBlockchain Integrated Cloud, 2018 IEEE 11th International Conference on Cloud Computing.
[11] *Sunny King and Scott Nadal,* PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake, *August **19th, 2012***

Authors Profile

Mr.Syed Zishan Ali pursued Bachelor of Engineering from CSVTU, Bhilai in 2009 and Masters in Computer Science in 2014 from CSVTU.He is currently working as Assistant Professor in Department of computer Science & Engineering , BIT Raipur since 2012.He has published Research papers in IEEE which is availabe online and also presented paper on SPRINGER conferences.

Ms. Dolly Sahu is current a scholar under Mr.Syed Zishan Ali.

Mr.Jatin Sahu is current a scholar under Mr.Syed Zishan Ali

