International Journal of Management, IT & Engineering
Vol. 9 Issue 4, April 2019,
ISSN: 2249-0558 Impact Factor: 7.119
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

BLOCKCHAINS- AN ATTEMPT TO ARRIVE CONNOTATION THROUGH BITCOINS

Krishna Prasath S*

Abstract

We live in a World which is prone to innumerable changes. Rapid Urbanization, Technological Breakthroughs, Demographic and Socia Changes, Shift in Global Economic Power, Climate Change and Reso Scarcity are the five major shifts happening in the World at an extrav phase. The Global civilization is thriving to adopt itself to these megachanges. Adoptability always starts with acquaintance. Amidst Blockchain technology and Bitcoins have already become the buzzw the global economy. The latter, as most of us are aware, is a tool in th cryptocurrency world, whereas the former is the technique to ensure security and anonymity of the users involved with bitcoins. One shou that the bitcoin concept is one among the million entities based on th blockchain technology.This paper makes a humble attempt to illustra concept of blockchain technology through bitcoins.

Keywords:

Block Chain.
Bitcoin.
Disyributed ledger.
Cryptography.
Tranperency.

Author correspondence:

Krishna Prasath S

Assistant Professor, CHRIST (Deemed to be University), Bangalore – 29

krishna.prasath@christuniversity.in

* **Assistant Professor, CHRIST (Deemed to be University), Bangalore**

1. Introduction

Blockchain is an open, dynamic, distributed and transparent ledger, which records the transactions taking place between two parties in a confirmable and enduring way. The blockchain is indeed a list of blocks or popularly the records which grows proportionately to the transactions happening in the cryptocurrency world. This list is made available in the network for the netizens to view and ensure the security features of the cryptocurrency environment.

Now let us understand the working of theblockchains. The fundamental element of the blockchains is the blocks or the records. These blocks record the transactions happening at a given point of time. The blocks may record all the transactions or may skip a few. Once,the recording is done, the current block will get completed;later, it will get attached itself to the main stream of blocks i.e. blockchain. A new block will be generated by the blockchain for recording the forthcoming transactions. It is important to note that amending or altering the data stored in the blocks is impossible without disquieting the network majority and altering the adjacent blocks.

2. Research Method

Secondary data has been collected from various sources to comprehend the ideology of Block Chains. The methodology section of this paper is split into the following sections, which illustrate the ideology of blockchain in simple language.

a) SHA256 Hash Function
b) Public Key Cryptography
c) Distributed Ledger & Peer to Peer Network
d) Proof of Work
e) Incentives for Validation

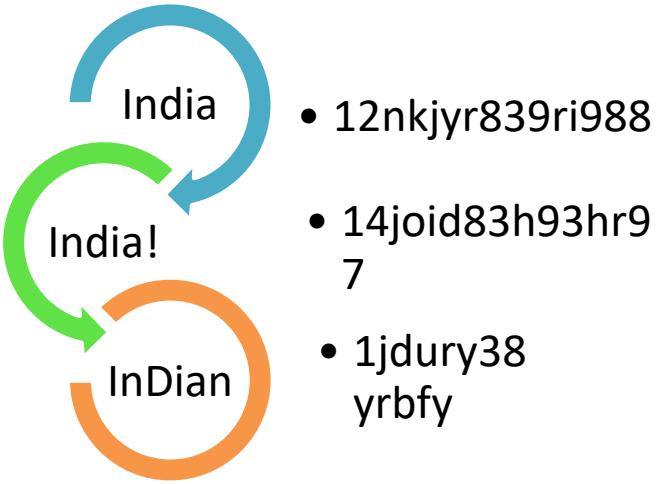
SHA256 Hash Function

In order to understand SHA256, one should know the working of a hash function. A hash function is a mathematical algorithm that converts the fed data into some output. For instance, suppose we have an algorithm to multiply all the numbers given in a string together, for an input of 12345 we would get an output of 120. Those hash functions featured with good properties are vital for the functioning of bit coins and blockchain technology.

One such hash function is the SHA256 hash function, which is also the core function of the blockchain technology. This function never allows a user to decrypt an encrypted code, thus

ensuring the security of the entire blockchain. Thus SHA256 is a one-way cryptographic function and also is of fixed size irrespective of the text kinds.

The SHA256 algorithm can be better understood with the following examples.



In this example, when the data 'India'is fed, the output will be generated as nkjyr839ri988. When an exclamatory mark is added to the data 'India', the output changes completely to14joid83h93hr97. If we change'd' to 'D' and add an 'n' at the end, the output gets changed again as 1jdury38yrbfy. Thus, for any given change in the input there will be an exorbitant change in the output generated by this **SHA256 Hash Function**.

Public Key Cryptography

It is a combination of public and private keys working together to ensure encryption all through the transaction. If Jai has to send some bitcoins to Krishna, the transaction will be having a three dimensional information viz.

(a) Jai's bitcoin address (Public Key)

(b) Krishna's bitcoin address (Public Key)

(c) The amount of bitcoins that is being sent to Krishna from Jai.

These three pieces of data will be accompanied by a digital signature, to the network for verification. The digital signature is a combination of the two public keys representing the bitcoin addresses of the receiver and the sender, which is further encrypted by a private key.

When the data miner receives such digital signature he will be engaged the following processes simultaneously.

(a) The un-encrypted data like the public key addresses of Jai and Krishna and the amount of bitcoins, found in the transaction will be taken. The collected data will be fed into a hash algorithm to fetch a hash value.

(b) By using the public key of Jai, the digital signature will be decrypted by the miner to create the second hash value.

If both the hash values are matching each other, then the miner will infer that the given

Distributed Ledger and P2P Network

Every individual associated with the bitcoin blockchain will be having a copy of the *ledger*. The *ledger* is a decentralized, distributed and anonymous entity found somewhere in this globe. This *ledger* does not look like a typical account enlisting the names of the participants or the traders with their bitcoin balances; rather, it is a dynamic database that will be having a perpetual record of all the transactions from the evolution of the ideology of bitcoin blockchain.As the sixth day of March 2018, there are about 512000 blocks generating $139595.8 USD per block.

B A N K L E D G E R	
0 6 M A R	Account 12345678 pays $1000 to Account 98765432
0 7 M A R	Account 98765432 pays $150 to Account 55566677
0 8 M A R	Account 55566677 pays to $2050 to Account 12345678
B I T C O I N L E D G E R	
0 9 M A R	Bitcoin Address xxx pays 0.6 BTC to Bitcoin Address yyy
1 0 M A R	Bitcoin Address yyy pays 2BTC to Bitcoin Address zzz
1 0 M A R	Bitcoin Address yyy pays 1 BTC to Bitcoin Address xxx

Proof of Work

Proof of Work (POW) is a mechanism to facilitate the transactions in a blockchain, by expensive computations or rigorous data mining.POW is always used along with cryptographic signatures, merkle chains and P2P networks, by the miners to solve the complex mathematical puzzles. The

miners will search for a specific *nonce* (Mathematical Value) which will fetch the desired hash that is a predetermined one.

Each block in the chain will be having a hash value. This hash value is in turn a combination of the final hash value of the previous block, the hash value of the transaction data and the mathematical value, the nonce. A specified number of trailing zeros should be preceding the hash, which is fetched as the last hash for a given block. This part of the computational process aimed at finding the nonce is really cumbersome, and that miner who discovers the nonce will be having sole rights to add their block to the blockchain. The newly added block will be appearing in the peer to peer network, so that everyone can verify if hashes match, can update their blockchain and move on to resolve the succeeding block.

Incentives for Validation

The miner who has created the latest block will be rewarded, by the blockchain system for enhancing the validity and scope of the chain. Currently, miners get 12.5 BTC (Rs.34,27,850 or $53,390). It is noteworthy that the new bitcoins can be generated only through these incentives.

BOONS OF BLOCKCHAIN SYSTEM

Decentralized System of Governance

For instance, the monetary system of the countries are supervised and regulated by the central bank or federal authorities. On the other hand, the cryptocurrency environment based on the block chain technology does not have an apex body and a regulatory authority to administer. Each stakeholder will be equally responsible for the rise and fall of the system. They hold a joint responsibility and pose a collective authority, thus making the entire system decentralized. So is the scenario in any given system, based on blockchains.

Transparent Ledgers Ensuring Transparency and Anonymity

Can a document be both transparent and confidential? Yes the blockchain ledger is one such. It documents each and every block/transaction happening in the system, for the purpose of broadcasting to the needy. One can have a complete track on all the blocks that has been placed

in the chain since its inception. However the blocks only reveal the amount dealt, the date and time in a given transaction. The identity of the miner is always concealed.

Verification of Each Swing and Shift

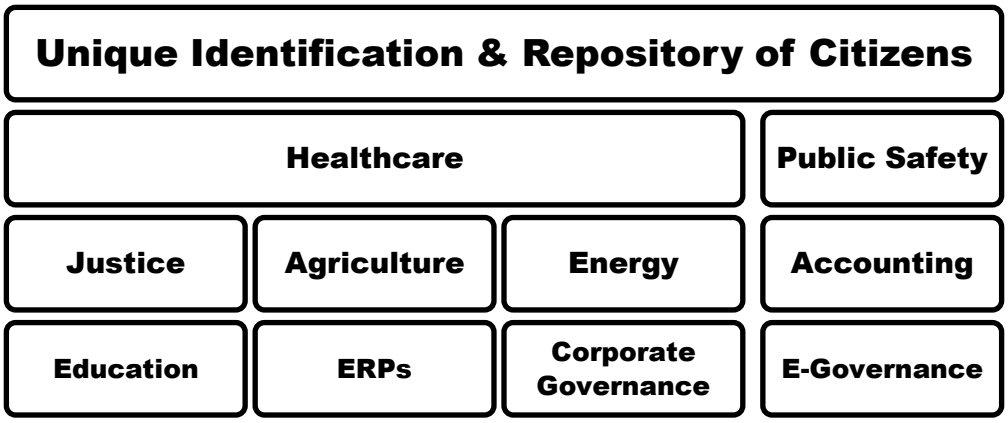
Double counting or duplication is a common threat found in the transactional World. For instance, the present monetary system is cursed with the feature of double spending. Double spending is an error occurring because of spending the same digital token more than once. Let us assume that Mr.Xavier has Rs.5000 in his bank account. He needs to pay Mr.Yasar with Rs.4500 and to Ms.Zulfia with Rs.5000, for which he is initiating two different transactions. As Mr.Xavier is not having the required balance in his account, these transactions will be never considered by the banking system. However, by creating a duplicate digital token, he will be able to pay both the parties even without having the sufficient balance. This duplication is denoted as double spending. Similarly, duplications in other fields can also be suppressed by implementing blockchain technology.

The blockchain technology, however feeds each and every transaction for ledger cross-checking. This validation facility is in turn, built on complex encryption codes and hashing algorithms, which will apparently alleviate the threat of double spending or duplication in the ledgers maintained.

Cut-rate Transactions

In the existing monetary system, one needs to incur additional charges for performing each and every monetary transaction, as these transactions are carried out by a common third party viz. the bank. Though the transaction charges for smaller value transactions are less, the monetary transactions for larger value transactions are always lavish. On the other hand, in the bitcoin technology or any other blockchain technology, the transaction charges are either levied at a minimal level or not at all levied.

OTHER APPLICATIONS OF BLOCKCHAIN TECHNOLOGY



3. Conclusion

The technological innovations have always attracted the enterprises and the economists tenanted in the World. This is largely due to, the promises they deliver in the arenas of service enhancement, deliverable assurance, quality improvement and thereby resulting in happiness, resonance, satisfaction in the minds of the stakeholders of the enterprise and the citizens of the economy. However the large scale implementation of newer technologies like blockchains always consumes time and undergoes a rigorous adoption process. The blockchain technology is also in such a phase of adoption. The technology of blockchains is still being tested in small scale cases and the results of which are satisfactory. Experts believe that a regulated, validated and a versatile blockchain technology by the enterprises and the federal governmental bodies will bring a tectonic shift in the way in which people lead their lives.

4. References

[1] Simon Barber, Xavier Boyen, Elaine Shi, and ErsinUzun. Bitter to better - how to make bitcoin a better currency. In Proc. Financial Cryptography and Data Security, 2012.

[2] Guido Bertoni, Joan Daemen, MichaëlPeeters, and Gilles Van Assche.The keccak sha-3 submission. Submission to NIST (Round 3) 6(7):16, 2011.

[3] Bitinfocharts. Website.https://bitinfocharts.com/namecoin/nodes-active/, 2016.

[4] Joseph Bonneau, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A. Kroll, andEdward W. Felten. SoK: Research perspectives and challenges for Bitcoin and cryptocurrencies.InIEEE Symposium on Security and Privacy(S&P), 2015.

[5] Christian Decker and Roger Wattenhofer.Information propagation in the Bitcoin network. In Proc. IEEE Conf. peer-to-peer networks (P2P), 2013.

[6] IttayEyal and EminGünSirer. Majority is not enough: Bitcoin mining is vulnerable. InProc. Financial Cryptography and Data Security, 2014.