RESEARCH ARTICLE OPEN ACCESS

Anticipation Algorithm Used in Block Chain Technology

Reeta Mishra
Assistant Professor in Information Technology Department,
K.J. Institute of Engineering & Technology, Savli, Dist.-Vadodara, Gujarat, India

Abstract:

Block chain (BC), the technology which behind the Bitcoin crypto-currency system, is both alluring and critical for ensuring enhanced security and privacy for diverse applications in many other domains - including in the Internet of Things (IoT) eco-system. Still research is currently being conducted in both academia and industry applying the Blockchain technology in multifarious applications. Proof-of-Work (PoW), a cryptographic puzzle, plays a important role in ensuring BC security by maintaining a digital ledger of transactions, which is considered to be incorruptible. Blockchain uses a changeable Public Key to record the users' identity, which provides an extra layer of privacy. Not only in crypto-currency has the successful adoption of BC been implemented but also in multifaceted non-monetary systems such as in: distributed storage systems, proof-of-location, healthcare, decentralized voting and so forth.

Keywords:**Blockchain (BC), Bitcoin,Crypto-currency; Proof of Work , Cryptography, Distributed Digital Ledger.**

Introduction:

"A block chain is a type of database that takes a number of records and puts them in a block . By using cryptographic signature , each block is then 'chained' to the next block. This allows block chains to be used like a ledger, which can be shared and verified by anyone with the appropriate permissions. There are many ways to corroborate the accuracy of a ledger, but they are broadly known as consensus"

Registration of cryptocurrencies in form of bitcoin transactions was the initiating of the blockchain technology (BL), a protocol where the related information is recorded in successive blocks on a ledger, shared by all the nodes of the network. Other cryptocurencies such as Litecoin, Feathercoin, Peercoin, Novacoin and others platforms such as Ethereum, based on Blockchain technology have been introduced and the potential of the technology began tounroll in areas other than cryptocurrencies.

A cryptocurrency like Bitcoin consists of a peer to peer network. Every peer has a information of the complete history of all transactions and thus of the balance of every account. A transaction is a file that says, "Mr. Ravi gives X Bitcoins to Amit" . It's basic private or public key cryptography. After signed, a transaction is broadcasted in the current network, sent from one peer to every other peer. The transaction is known almost promptly by the complete network. After a specific amount of time it gets confirmed. Confirmation is a critical concept in cryptocurrencies. As long as a transaction is not confirmed, it is pending and can be forged. When a transaction is confirmed, it is set in stone. It is no longer forgeable, it can‘t be contrary, it is part of an immutable record of historical transactions of the so-called blockchain. Only miners can confirm transactions. It is possible in a cryptocurrency-network. They take transactions, stamp them as confirmed and send them in the network. After a transaction is confirmed by a miner, every node has to append it to its database. It has become part of the blockchain.

For this job, the miners get rewarded with a token (Bitcoins) of the cryptocurrency, for example Since the miner‘s activity is the single most important part of cryptocurrency-system . Here is set of rule that the miners need to invest some work of their computers to qualify for this task. In fact, they have to find a hash – a product of a cryptographic function that connects the new block with its predecessor. This is called the Proof-of-Work.

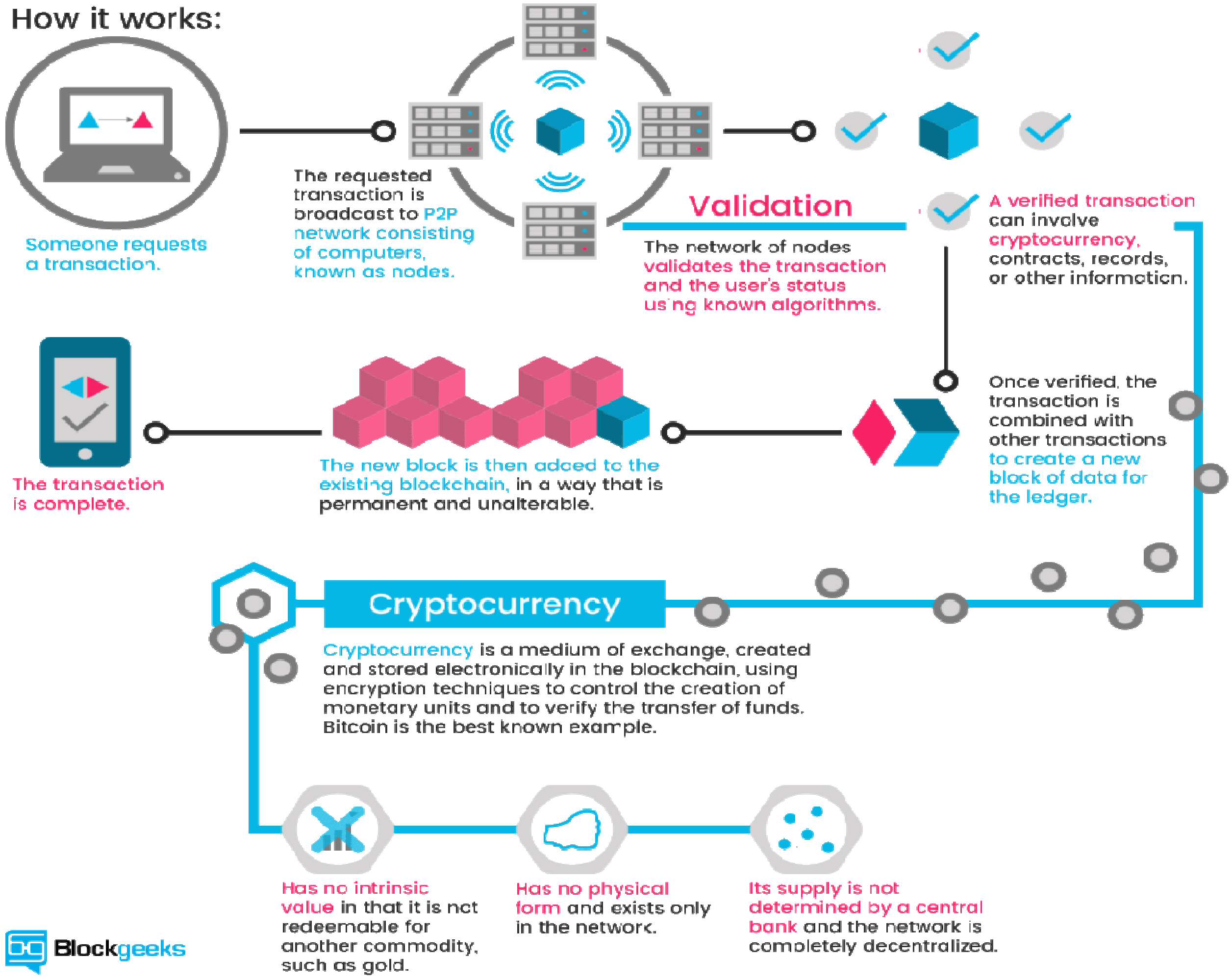

How it works:
Someone requests a transaction.
The requested transaction is broadcast to P2P network consisting of computers, known as nodes.
Validation
The network of nodes validates the transaction and the user's status using known algorithms.
A verified transaction can involve cryptocurrency, contracts, records, or other information.
Once verified, the transaction is combined with other transactions to create a new block of data for the ledger.
The new block is then added to the existing blockchain, in a way that is permanent and unalterable.
The transaction is complete.
Cryptocurrency
Cryptocurrency is a medium of exchange, created and stored electronically in the blockchain, using encryption techniques to control the creation of monetary units and to verify the transfer of funds. Bitcoin is the best known example.
Has no intrinsic value in that it is not redeemable for another commodity, such as gold.
Has no physical form and exists only in the network.
Its supply is not determined by a central bank and the network is completely decentralized.
Blockgeeks

Figure 1:-Block Chain working step

Block chain technology is based on the cryptographic principle of a private-public key approach.

"The block chain is an trustworthy digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value."

Don & Alex Tapscott, authors Blockchain Revolution (2016)

S.NO	Parameter	Value
1	Bitcoin market price per USD	13,915
2	Trade Volume last 24 hours	1.32 Billion
3	Trade Volume last 24 hours	94,018 BTC
4	Bitcoins in circulation	16.80 million
5	Bitcoin market capitalisation	233.74 billion
6	Size of the Bitcoin Block chain database	151.03 GB
7	Average transactions per block within 24 hours	1609
8	Hash Rate (Estimated number of tera hashes or trillion hashes per second) the Bit coin network is performing	18.53 million TH/s
9	Number of unique addresses used on the Bitcoin Blockchain	822,010
10	Blockchain Wallet user count	10 22.00 million

Figure2:-Blockchain.Technology related Analysis (Dated- 12 January 2018)

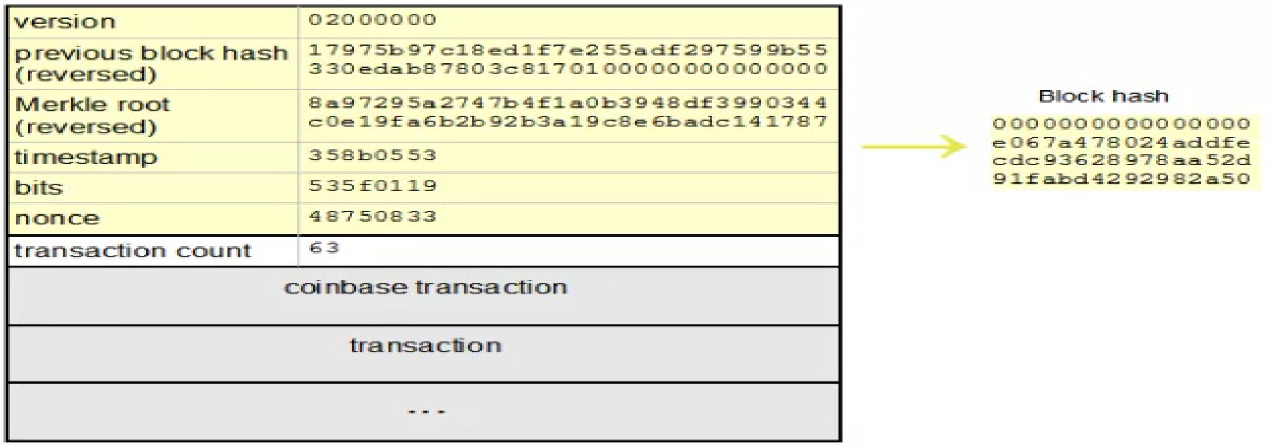
Bitcoin is based on blockchain technology which work with SHA 256 Hash algorithm.

SHA-256 is a cryptographic hash function (one-way) that takes an input of a random size and produces an output of a fixed size. Anyone to use a hash function to produce an output when given an input; it is impossible to use the output of the hash function to rebuild it's given input. This powerful feature of the SHA-256 hash function makes it ideal for application within the Bitcoin network.The SHA-256 hash function is employed within the Bitcoin network in two main ways:

- Mining
- Creation of Bitcoin addressess

1) Mining -

Mining is a process by which new coins are introduced into the existing course supply of the Bitcoin protocol and to secure the Bitcoin network.For an individual to be eligible to attach a block to the Bitcoin blockchain, they must first operate what is known as a *mining* node. An individual can begin constructing candidate blocks which are then relayed to the Bitcoin network to be checked for their validity. Inside a block is what is known as a *block header*.It consist of 6 parameters that must be filled in by the miner.



version	02000000
previous block hash (reversed)	17975b97c18ed1f7e255adf297599b55 330edab87803c81701000000000000000
Merkle root (reversed)	8a97295a2747b4f1a0b3948df3990344 c0e19fa6b2b92b3a19c8e6badc141787
timestamp	358b0553
bits	535f0119
nonce	48750833
transaction count	63
coinbase transaction	
transaction	
...	

Block hash

```
0000000000000000
e067a478024addfe
cdc93628978aa52d
91fabd4292982a50
```

Figure 3:- Block header parameter

In above figure a miner to produce the *previous block hash* parameter, the block header of the previous block must be put through SHA-256 algorithm **twice**, this also known as double-SHA-256. That is:

Previous Block Hash = SHA-256(SHA-256(Block Header))

SHA-256 algorithm is also used to produce the merkle root, which is then alternately inserted into the block header. Bitcoin protocol can be found here: .

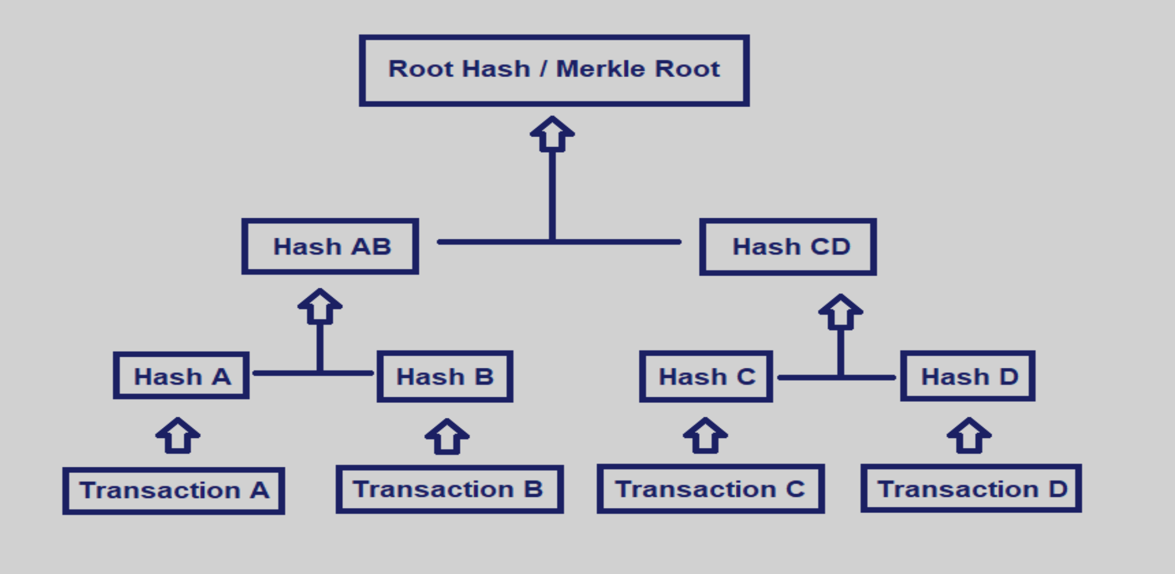


Figure 4:- Merkle Tree & Merkle Root

Upon successful building of a block, the miner can now begin the mining process, wherein another use case of the SHA-256 algorithm will present itself. In this instance, the *nonce* parameter of the block header, is a variable that is changed repeatedly, and upon hashing of the block header using the SHA-256 function, if the hash is below the target, the miner is observe to be successful.

2) Bitcoin addresses Creation-

Bitcoin address, a private key which is a randomly selected number, is multiplied using an elliptic curve to produce a public key. This public key is then put through both the SHA-256 & RIPEMD160 hashing algorithms.

“RIPEMD-160 is a cryptographic hash function is used in the Bitcoin standard,produces a 160-bit output. The compression function is made up of 80 stages made up of 5 blocks that run 16 times each. This pattern runs twice with the results being combined at the bottom using modulo 32 addition.”

Where K = the public key , A = Bitcoin address:

$$A = \text{RIPEMD160}(\text{SHA-256}(K))$$

The use of the SHA-256 and RIPEMD160 hashing algorithms for the creation of a Bitcoin address has one distinct advantage:

- Shorter addresses

Shorter addresses: A public key is 256 bits long the Bitcoin address, is 160 bits long. This makes it a lot more convenient for users to use due to the shorter character length.

Conclusion:

To conclude, the SHA-256 hashing algorithm is an integraland vital part of the Bitcoin protocol. It has seen implementation in different angle of the technology such as: bitcoin mining, merkle trees and the creation of Bitcoin addresses.SHA 256 can be the basis of a cryptologic puzzle the miners compete to solve. After finding a solution, a miner can build a block and attach it to the blockchain. As an incentive, he has the right to attach coinbase transaction that gives him a specific number of Bitcoins. This is one of best way to create valid Bitcoins.

Bitcoins can only be created if miners solve a cryptographic puzzle. Since the complexity of this puzzle enhanced the amount of computer power the whole miner’s invest, there is only a specific amount of cryptocurrency token that can be created in specific time period. This is part of the consensus no peer in the network can break.

Bitcoin, as a decentralized network of peers which keep a consensus about accounts and balances, is more a currency than the numbers you see in your bank account.

Reference

[1] Jesse Yli-Huumo1 , Deokyoon Ko2 , Sujin Choi4 *, Sooyong Park2 , Kari Smolander3 “Where Is Current Research on Blockchain Technology? - A Systematic Review.”, PLOS ONE, 10(11), [e0163477]. DOI: 10.1371,October 2016.

[2] Böhme R, Christin N., Edelman B., Moore T., Bitcoin: Economics, Technology, andGovernance, *Journal of Economic Perspectives*, 29, 213-238, (2015)

[3] Athey S., Parashkevov I., Sarukkai V., Xia J., Bitcoin Pricing, Adoption, and Usage: Theory and Evidence, *Stanford Business School Working Papers*, n° 3469, (2016)

[4] Chiu J., Koeppl T., The Economics of Cryptocurrencies. Bitcoin and Beyond, *Queen's University Working Paper*, Canada (2017)

[5] Dolev D., The Byzantine Generals Strike Again, *Journal of Algorithms*, 3, 14-30 (1982)

[6] D. Puthal, N. Malik, S. Mohanty, E. Kougianos, and C. Yang, "The Blockchain as A Decentralized Security Framework", *IEEE Consumer Electronics Magazine*, Vol. 7, No. 2, pp. 18--21, 2018.

[7] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A Survey on the Security of Blockchain Systems", *Future Generation Computer Systems*, 2017, doi = https://doi.org/10.1016/j.future.2017.08.020.

[8] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. Kroll, and E. Felten, "Sok: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies", in *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 104-121, 2015.

[9] https://www.epw.in/engage/article/block-chain-evolution-money-through-cryptocurrency

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