VOL 2 (2018) NO 3

e-ISSN : 2549-9904
ISSN : 2549-9610

INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION

Bitcoin Generation Using Blockchain Technology

Dr Balajee Maram#

Sr.Asst.Prof., Dept. of CSE, GMR Institute of Technology, Rajam, INDIA
E-mail: balajee.m@hotmail.com

***Abstract*— There are limitations in client-server model of communication. Distributed architecture provides good accessibility to all the nodes in the network. A blockchain technology is follows distributed model. In the digital era, all the transactions are available in the digital form is called a ledger. This ledger belongs to all the users in the network are shared by all the users in the network. Every transaction is monitored and verified by every user in the network. The blockchain is a chain of blocks that contains a collection of transactions. Bitcoin is a cryptocurrency, depends on blockchain technology. The Bitcoins are generated from the mining of a block for the miner. Every user knows about each and every Bitcoin transaction in the blockchain network. The block is immutable, because every block is verified by each customer in the blockchain network. This is the initiation for new trend for security to the digital transactions in the world. This paper presents the logic in the blockchain and Bitcoin generation process using blockchain technology.**

***Keywords*— Blockchain, SHA, public-key, Bitcoin, Mining, Peer-to-Peer.**

I. INTRODUCTION

At present, many issues have been binds with banking sector. There is a need to spend transaction fee for each and every transaction from customer-side. In double spending, the customer do not know about which transaction is successful when the customer transfers money to more than one customer with insufficient balance in his account. Because of net frauds, so much of money hacked by a hacker. The blockchain technology solves these issues.

A blockchain holds the details of all transactions of a group and is shared by everyone in that group. Once the customer joins in the group of blockchain, the entire blockchain can be accessible. It also provides privacy to each customer in the blockchain technology.

The blockchain technology has been initiated by Stuart Haber and W. Scott Stornetta in 1991. But the first blockchain is distributed by Satoshi Nakamoto in 2008, is called "Bitcoin". In 2014, "Blockchain 2.0" has been introduced, which is able to create new trends in economic and social systems.

II. LITERATURE SURVEY

The blockchain technology was first introduced in the year 2008 [3]. Some of the authors told that the blockchain technology is decentralized network [10,11] and it is a ledger of all transactions [12] and linked like a linked list [13]. The transactions are shared by all the participants in the network [14]. Every transaction is secured with public-key cryptography concept [15]. When the transaction is verified then new blocks are added to the existing blockchain and cannot be altered [16].

III. BLOCK-CHAIN TECHNOLGY

A. What is a 'Blockchain'?

A blockchain is a chain of blocks, which is decentralized public ledger of all transactions in digital form. A block is created with recent transactions and will be appended to the existing blockchain which is immutable and cannot be deleted. This blockchain is accessible to each participant who are included in the decentralized distributed network i.e. customers and miners.

B. Block in a Blockchain

Every minute, many transactions have been generated in the world. All the transactions will be available in single pool. Among them, 1000 to 2500 transactions are included into a single block. Each block is added to the existing blockchain in a chronological order after validation in a single list form. Genesis block is the first block in the blockchain. The data fields comprising a block typically consist of the following:

- The block number, also known as block height
- The hash value of the current block
- The hash value of the previous block
- The Merkle tree root hash
- A timestamp
- The size of the block

- The nonce value, which is a number manipulated by the mining node to solve the hash puzzle that gives them the right to publish the block
- A list of transactions included within the block

C. Functionality of the blockchain network

Different types of transactions are being generated from financial sector, banking sector, Government sector, real-estate sector etc. In banking sector, credit card the best example for blockchain technology. There are several communications are required to transfer money from one customer to another customer. For implementing all these steps, the banking sector collects the transaction fee from each customer. In this example, all the transactions are passing through the middle-man is bank. The direct communication is impossible in the current scenario. So each customer of the bank should trust and make a transaction.

In the research world, many researchers are trying to eliminate the concept of trusted third party for handling the transactions from different customers who belongs to different sectors. As a result, a new trend blockchain creates a platform for handling peer-to-peer transactions with minimal transaction fee with high privacy and efficiency.

Several transactions are generated from different sectors in the world. A block is created which contains several transactions. Each block is linked with previous block in a single linked-list form. Each block contains the hash value of the previous block. It is not possible to predict the data in the previous block using the hash value of the previous block. Because hash value is irreversible in cryptography. In this way, it provides the integrity in the blockchain technology. Here genesis block is the first block in the blockchain.

A block is the part of blockchain which contains 1000 to 2500 recent transactions. Once it is validated, this block is added to the existing blockchain.

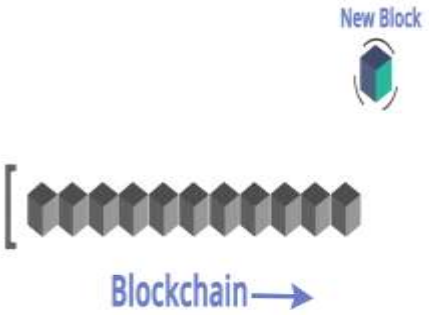

Fig. 1 Functionality of blockchain

Once the block is created, then it is validated by the miners. Because the blockchain technology has no centralized server for holding and validating the transactions. The linking of blocks isn't the only thing that keeps the chain secure, however. It's also decentralised, each computer with the software installed has a copy of the blockchain which is constantly updated with new blocks. When the miner validates the block, through our P2P distributed network, successful miner broadcasts their block and everyone verifies if hashes match, updates their blockchain and moves on to solving the next block immediately. The last step of a blockchain transaction is to giving a reward to the miner who has created the latest block. This rewards is provided by the Blockchain system for validating the transactions and maintaining the Blockchain. Currently the reward per block is 12.5 BTC. This is the most interesting part of Bitcoin Mining.

D. Cryptography for Blockchain Technology

A blockchain is a linked list of blocks. The blocks are added to the existing blockchain after validation only. Cryptography concepts plays an important role in creation of blocks for blockchain. The following are the useful security methods for blockchain technology:

- SHA256 Hash Function
- Public Key Cryptography

SHA-256 Hash Function

SHA stands for Secure Hashing Algorithm. The SHA transforms any size of data into a fixed size string is called "Hash" by applying bitwise operations, modular addition and compression functions. The SHA are designed to the given input into fixed string Hash and not vice-versa. It means that the hash value is impossible to transform back into the original data. There are several applications from SHA. It is very useful for servers, because the servers are responsible to store the passwords with high security. So all passwords are converted into hash and stored in the server database. If the hacker hacks and get the passwords, are not directly visible to the hacker and are not convertible back to the original passwords. Each SHA algorithm supports avalanche effect. A small change in the input reflects drastic change in the output is called avalanche effect. A single bit change in the input gives completely different hash value. So it is used to detect the tampering in the data, when data is in communication and attacked by the hackers.

In blockchain technology, the hash algorithm SHA-256 is used. Because it is a 'one-way' cryptographic function, and is a fixed size for any size of source text. Two different inputs gives entirely different outputs. Here is a simple example:

Public Key Cryptography

Public-key encryption (also called asymmetric encryption) involves a pair of keys, a public key and a private key, associated with an entity. Each public key is published, and the corresponding private key is kept secret. Data encrypted with a public key can be decrypted only with the corresponding private key.

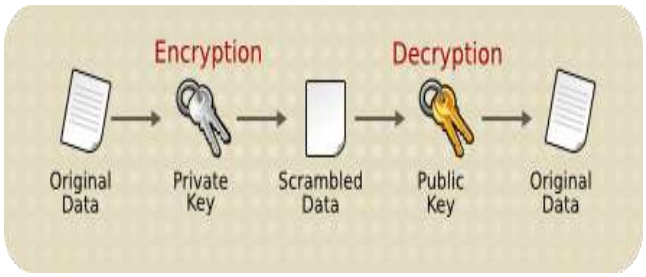

Fig. 2 Block-diagram of public-key cryptography

The most important properties of public key encryption scheme are −

- Each customer has to maintain two key i.e. private key and public key.
- Public key is for encrypting the data, but it should be available to the public
- Private key is for decrypting the data
- Though private and public keys are related mathematically, it is not be feasible to calculate the private key from the public key. In fact, intelligent part of any public-key cryptosystem is in designing a relationship between two keys.

This cryptographic technique helps the user by creating a set of keys referred as Public key and Private key. Here the Public key is shared with others whereas the Private key is kept as a secret by the user. To understand the roles of these keys, Let us look at the example below:

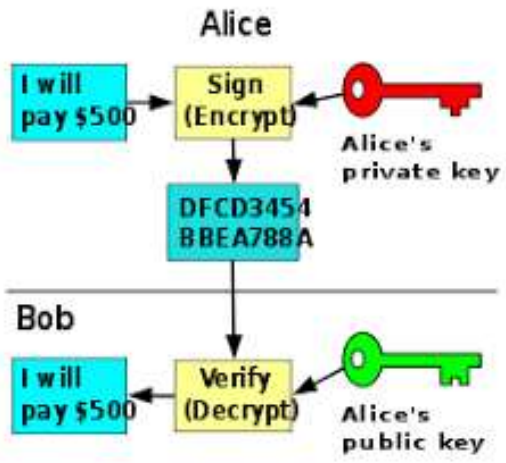

Fig. 3 Digital transaction between users

If the user A sends cryptocurrency to user B, that transaction will have three pieces of information:

- B's Public key
- The amount that A is sending to B.
- A's Public key

Now all this data along with an encrypted digital signature is sent through the network for verification. The Digital signature is again a hash value achieved by the combination of the A's address and the amount he is sending to user B. This digital signature is encrypted by the private key. Once this data is received by a miner who has to verify this transaction, there are 2 process he does simultaneously:

- He takes all the un-encrypted data like transaction amount and public keys of both B and A, and feeds it to a hash algorithm to get a hash value which we shall call Hash1
- He takes the digital signature and decrypts it using A's public key to get a hash value which we will call as Hash2

If both Hash1 and Hash2 are the same then it means that this a valid transaction.

E. Role of Miner in blockchain technology

Instead of relying on a third party, such as a financial institution, to mediate transactions, member nodes in a blockchain network use a consensus protocol to agree on ledger content, and cryptographic hashes and digital signatures to ensure the integrity of transactions. Consensus ensures that the shared ledgers are exact copies, and lowers the risk of fraudulent transactions, because tampering would have to occur across many places at exactly the same time. Cryptographic hashes, such as the SHA256 computational algorithm, ensure that any alteration to transaction input — even the most minuscule change — results in a different hash value being computed, which indicates potentially compromised transaction input. Digital signatures ensure that transactions originated from senders (signed with private keys) and not imposters.

The decentralized peer-to-peer blockchain network (as in Figure 4) prevents any single participant or group of participants from controlling the underlying infrastructure or undermining the entire system. Participants in the network are all equal, adhering to the same protocols. They can be individuals, state actors, organizations, or a combination of all these types of participants.

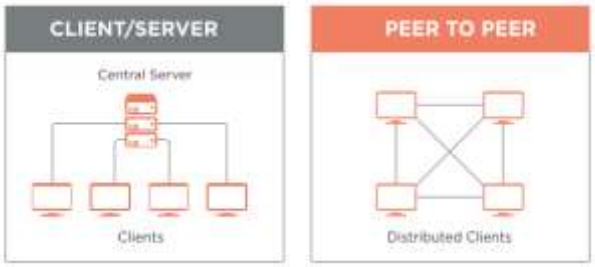

Fig. 4 Pictorial representation of Client/Server model and Peer-to-Peer model

At its core, the system records the chronological order of transactions with all nodes agreeing to the validity of transactions using the chosen consensus model. The result is transactions that are irreversible and agreed to by all members in the network. Before adding the block the existing chain, there is a need of "proof of work",

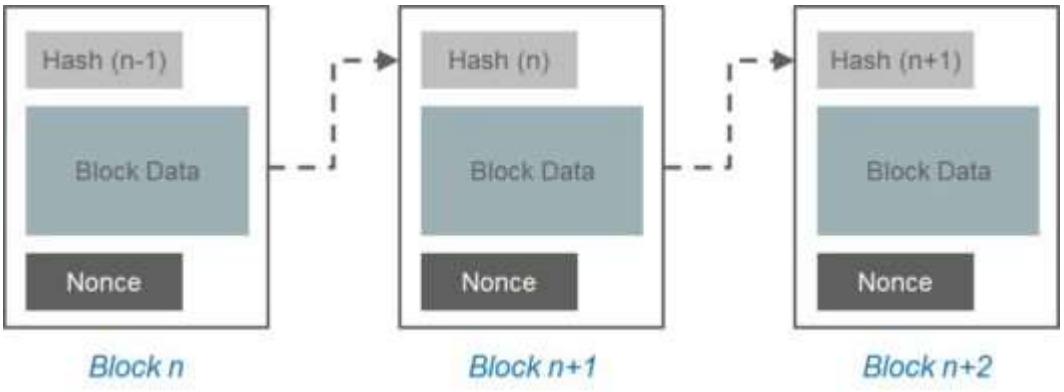

Fig. 5 Security of blocks in blockchain technology

F. Proof-of-work

In blockchain technology, everyone equally owns the ledger and also responsible to check whether the block is valid or not?

It requires lots of computational effort. This work is done by people in the Bitcoin network we call miners. The work of these miners is to verify the transactions and solve a complex mathematical puzzle associated with the block being created. The difficulty of the problem is adjusted so that on average a block is solved in 10 minutes. Miners search for a specific nonce(mathematical value) which gives the desired hash which is predetermined. The current difficulty level is such that you need to try about 20.6 quadrillion nonce to get the correct hash.

So the person who finds this nonce is the successful miner and he/she can add their block to the blockchain. Through our P2P distributed network, he/she broadcasts their block and everyone verifies if hashes match, updates their blockchain and moves on to solving the next block immediately.

G. How to generate Bitcoins from blockchain technology?

The Bitcoins are generated from the process of Bitcoin Mining. During mining, your Bitcoin mining hardware runs a cryptographic hashing function (two rounds of SHA256) on what is called a block header. For each new hash that is tried, the mining software will use a different number as the random element of the block header, this number is called the nonce. Depending on the nonce and what else is in the block the hashing function will yield a hash which looks something like this:
93ef6f358fbb998c60802496863052290d4c63735b7fe5bda ac821de96a53a9a

Here this hash as a really long number. To ensure that blocks are found roughly every ten minutes, there is what's called a difficulty target. To create a valid block your miner has to find a hash that is below the difficulty target. So if for example the difficulty target is
100000000000000000000000000000000000000000000000 00000000000000000

any number that starts with a zero would be below the target,e.g.:
0787a6fd6e0782f7f8058fbef45f5c17fe89086ad4e78a1520d 06505acb4522f

If we lower the target to
010000000000000000000000000000000000000000000000 00000000000000000

we now need two zeros in the beginning to be under it:
00db27957bd0ba06a5af9e6c81226d74312a7028cf9a08fa1 25e49f15cae4979

Because the target is such an unwieldy number with tons of digits, people generally use a simpler number to express the current target. This number is called the mining difficulty. The mining difficulty expresses how much harder the current block is to generate compared to the first block. So a difficulty of 70000 means to generate the current block you have to do 70000 times more work than Satoshi Nakamoto had to do generating the first block. To be fair, back then mining hardware and algorithms were a lot slower and less optimized.

To keep blocks coming roughly every 10 minutes, the difficulty is adjusted using a shared formula every 2016 blocks. The network tries to change it such that 2016 blocks at the current global network processing power take about 14 days. That's why, when the network power rises, the difficulty rises as well.

H. The Block Reward

Always the miners are trying to mine the blocks for blockchain parallelly. Among them, one of the miner announces his achievement. If it is valid and accepted by every node in the network , then the miner will get certain number of bitcoins and transaction fee from sender.

The process of globally distributed miners reaching consensus on the next block may result in some conflicts. In such cases, reconciliation or resolution of the conflicts is required. This requires consensus. The blockchain network for bitcoin uses the hash-cash proof-of-work (PoW) consensus algorithm to achieve distributed consensus.

I. CONSENSUS: How do you resolve conflicts?

The transaction pool contains transaction from different customers in the world. These transactions are to be converted into blocks. Then these blocks should be verified by the miners. During the block creation, a conflict may come when multiple miners create blocks at the same time. Assume the existing blockchain contains 50 blocks. Three miners ready to work on block number 51 simultaneously. Their block names are 51x, 51y, 51z. Again conflict will

come. It can be solved by "Longest chain rule". After completion of 51a, he has to check what is the progress of existing blockchain. When it is 50, 51y,52y etc. Then the first miner x, should follow from the block number 52. Because the block 51 is mined by y.

J. Benefits of blockchain technology

As a public ledger system, blockchain records and validate each and every transaction made, which makes it secure and reliable. All the transactions made are authorized by miners, which makes the transactions immutable and prevent it from the threat of hacking. Blockchain technology discards the need of any third-party or central authority for peer-to-peer transactions.

- Decentralization of the technology.
- Secure Digital Voting, a voter can check the casted vote was successfully recorded and transmitted.
- Decentralized Exchange, buying and selling the goods or properties without 3rd party arbiter.
- Safe and Secure Identity Verification, the owner of the transaction can be signed by the private key and secured by the blockchain security system.
- Limitations of Blockchain Technology
- Wastage of resources: Every node has to check the block is valid or not by consuming lot of electricity and other resources.
- Network speed: Every node should have some communication with its peers. When a node receives the valid block, then it has to send this information to its peers immediately.
- Size of the blockchain: Day-by-day, the transactions are being increased. So the size of the blockchain is also increasing by adding new blocks. Every node should maintain the entire chain of blocks in it memory.
- Redundancy: Every node in the network, has a copy of the entire blockchain. This is called redundancy, because remaining nodes also have the same copy where the first node contains.

K. The Blockchain & Enhanced security

By storing data across its network, the blockchain eliminates the risks that come with data being held centrally. Its network lacks centralized points of vulnerability that computer hackers can exploit. Today's internet has security problems that are familiar to everyone. We all rely on the "username/password" system to protect our identity and assets online. Blockchain security methods use encryption technology.

The basis for this are the so-called public and private "keys". A "public key" (a long, randomly-generated string of numbers) is a users' address on the blockchain. Bitcoins sent across the network gets recorded as belonging to that address. The "private key" is like a password that gives its owner access to their Bitcoin or other digital assets. Store your data on the blockchain and it is incorruptible. This is true, although protecting your digital assets will also require safeguarding of your private key by printing it out, creating what's referred to as a paper wallet.

IV. CONCLUSIONS

This paper provides the overview of blockchain technology. The issues in the existing technology have been discussed. The blockchain technology provides many benefits than the existing technology. The blockchain technology is based on the distributed systems. The blockchain technology does not create any monopoly in the public domain like banking sector, real estate sector etc. This technology eliminates the drawbacks in hard copy of the ledger, because manipulation may happen with hard copy of ledger. It is impossible in blockchain technology, when the ledger is developed with blockchain technology. This technology is also a base for cryptocurrency like Bitcoins. The generation of Bitcoins is based on blockchain technology. The Bitcoins are generated from the mining of the blocks in blockchain technology. The fundamental element of blockchain technology and Bitcoin is cryptography.

REFERENCES

[1] Clarke, A.C., "Hazards of Prophecy: The Failure of Imagination," from Profiles of the Future: An Inquiry into the Limits of the Possible, 1962.

[2] Narayanan, A., Bonneau, J., Felten, E., Miller, A., and Goldfede, S., Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction, Princeton University Press, 2016.

[3] Nakamoto, S., "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[4] Donnelly, J., "What is the 'Halving'? A Primer to Bitcoin's Big Mining Change," CoinDesk, June 12, 2016.

[5] Cachin, C., "Architecture of the Hyperledger blockchain fabric," in Workshop on Distributed Cryptocurrencies and Consensus Ledgers, July 2016.

[6] Scott Nadal Sunny King. (2012, August) PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake.

[7] Anish Dev J. Bitcoin mining acceleration and performance quantification. In: Electrical and Computer Engineering (CCECE), 2014 IEEE 27th Canadian Conference on; 2014. p. 1–6.

[8] Koshy P, Koshy D, McDaniel P. An Analysis of Anonymity in Bitcoin Using P2P Network Traffic. In: Christin N, Safavi-Naini R, editors. Financial Cryptography and Data Security. vol. 8437 of Lecture Notes in Computer Science. Springer Berlin Heidelberg; 2014. p. 469–485.

[9] Decker, Christian, Jochen Seidel, and Roger Wattenhofer., "Bitcoin Meets Strong Consistency."

[10] Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J.A., Felten, E.W.: Research perspectives and challenges for bitcoin and cryptocurrencies. In: 2015 IEEE Symposium on Security and Privacy, pp. 104–121 (2015)

[11] Kosba, A., Miller, A., Shi, E., Wen, Z., Papamanthou, C.: Hawk: the blockchain model of cryptography and privacy-preserving smart contracts. In: 2016 IEEE Symposium on Security and Privacy, pp. 839–858 (2016)

[12] Lewenberg, Y., Sompolinsky, Y., Zohar, A.: Inclusive block chain protocols. In: Böhme, R., Okamoto, T. (eds.) FC 2015. LNCS, vol. 8975, pp. 528–547. Springer, Heidelberg (2015).

[13] Sharples, M., Domingue, J.: The blockchain and kudos: a distributed system for educational record, reputation and reward. In: Verbert, K., Sharples, M., Klobučar, T. (eds.) Adaptive and Adaptable Learning: 11th European Conference on Technology Enhanced Learning, EC-TEL 2016, pp. 490–496. Springer International Publishing, Cham (2016)

[14] Garman, C., Green, M., Miers, I.: Decentralized anonymous credentials. In: Network and Distributed System Security (NDSS) Symposium 2014, pp. 23–26 (2014)

[15] Wang, H., Chen, K., Xu, D.: A maturity model for blockchain adoption. Financ. Innov. 2, 12 (2016)

[16] Beck, R., Stenum Czepluch, J., Lollike, N., Malone, S.: Blockchain - the gateway to trust-free cryptographic transactions. In: Twenty-Fourth European Conference on Information Systems (ECIS), pp. 1–14 (2016)
[17] https://www.weusecoins.com/en/mining-guide/
[18] https://bitsonblocks.net/2015/09/09/a-gentle-introduction-to-blockchain-technology/
[19] https://www.buybitcoinworldwide.com/mining/
[20] https://www.edureka.co/blog/blockchain-tutorial/