American Research Journal of Computer Science and Information Technology
ISSN: 2572-2921
Volume 3, Issue 1, pp: 1-8

AMERICAN RESEARCH JOURNALS
An Academic Publishing House

Research Article Open Access

Bitcoin Cryptocurrency: A Review

Anam Fatima[1], Dr. Vijay Kumar Tiwari[2]
M.Tech - Computer Science and Engineering
Centre for Advanced Studies, Dr. APJ Abdul Kalam Technical University, Lucknow, Uttar Pradesh
anamftm14@gmail.com[1], vktiwari@gmail.com[2]

Abstract: Bitcoin, the term coined by a person or group pseudonymously called Satoshi Nakamoto, is considered the world's first decentralized digital currency. Since its release in 2009, there has been tremendous growth in market value of Bitcoin, with anonymity and distributed nature removing the need for any central authority being the driving force for its popularity. The technology is relatively new and complex for a layman to understand. However, there has been enough hype about it which has drawn the attention of researchers and nemesis alike to expose vulnerabilities in the system as well as explore the future perspectives of this new concept.

This paper analyses major components of Bitcoin and related concepts of Blockchain, highlighting a few security concerns/ motivation to explore the future perspectives of this technology which is being considered analogous to the Internet revolution.

Keywords: Blockchain; Merkle Tree/Root; Bitcoin System; Bitcoin Mining; Proof-of-Work(PoW); Consensus; Security; Future perspectives

Introduction

The term Bitcoin was coined by a person or a group under the pseudoname of Satoshi Nakamoto. It is a decentralised digital payment system based on peer-to-peer network with no central authority to monitor transactions but between users directly without any intermediary. It is a type of cryptocurrency as the transactions are verified by network nodes through the use of cryptography and recorded in a public distributed ledger called a blockchain [1].

[2]. Blockchain was invented by Satoshi Nakamoto in 2008 for use in the cryptocurrency bitcoin, as its public transaction ledger It is the ingenious technology which serves as a platform for cryptocurrencies. It is based on the concept of distributed transaction ledger on a peer-to-peer network which is both public and anonymous and is not controlled by any single entity or centralized authority. It requires consensus of all the participating nodes with equal weightage in the distributed peer-to-peer network and removes the dependency on any trusted third party to verify the transactions. Rather it is based on self-regulation imposed by incentive driven Proof-of-Work and Consensus Protocol assuming that honest nodes in the peer-to-peer network always hold more than 50% of the computing resources such that any malicious node is always overpowered and placed in minority by its peers.

Technology Behind Bitcoin: Blockchain

Blockchain is a distributed ledger on a peer-to-peer network making use of cryptographic hash functions to prevent any alteration of data logged in the ledger. It is not controlled by a central authority but is based on replication of blocks (a record of transactions) across many computers such that each block contains cryptographic hash of previous block. Once recorded, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks, which requires collusion of the network majority [2].

Blockchain's ability to distribute processing while ensuring the veracity of transactions may allow companies to process data far more efficiently [20]. This has drawn the attention of many companies to put to affect this concept into many other applications requiring distributed secure database.

A. Block

A block is typically a collection of transactions stored in Merkle Tree Structure. It is used to maintain the integrity of the data in the block. The structure of the tree is such that if there is any single change in the transaction details or their order, the Merkle Root changes.

There are several transactions in a block. Every transaction in the block has a hash associated with it. The leaf-nodes contain these transaction hashes. All of the transaction hashes are further hashed repeatedly pair-wise in a bottom-up way to form a tree-like structure with its root containing hash of all the transactions in the block. The root of the tree called Merkle Root contains cryptographic hash calculated from the transactions included in the block serving as proof that the contents of the block have not been tampered with.

Figure 1 (Source: [3]) shows the Merkle Tree Structure where every leaf node contains hash of the transactions included in the block and every non-leaf node contains the hash of its child nodes.

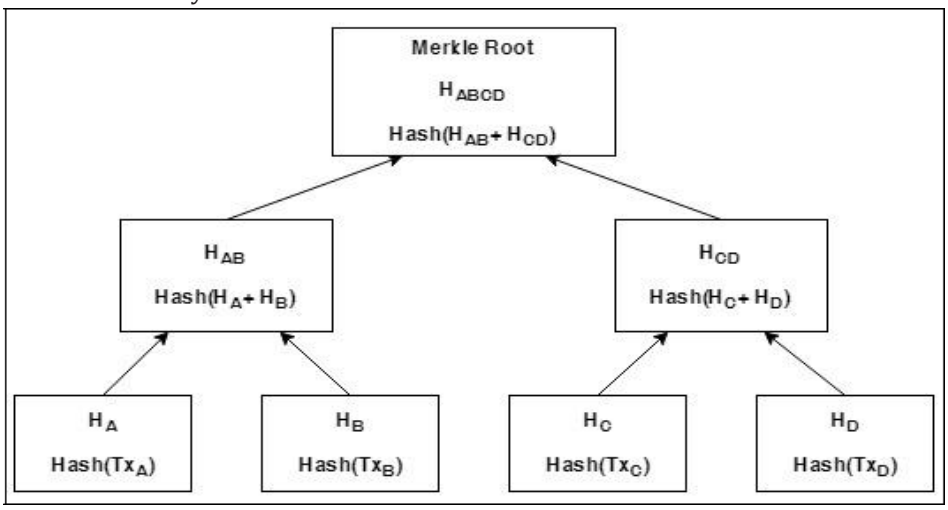

Fig1. *Merkle Tree Structure (Source: [3])*

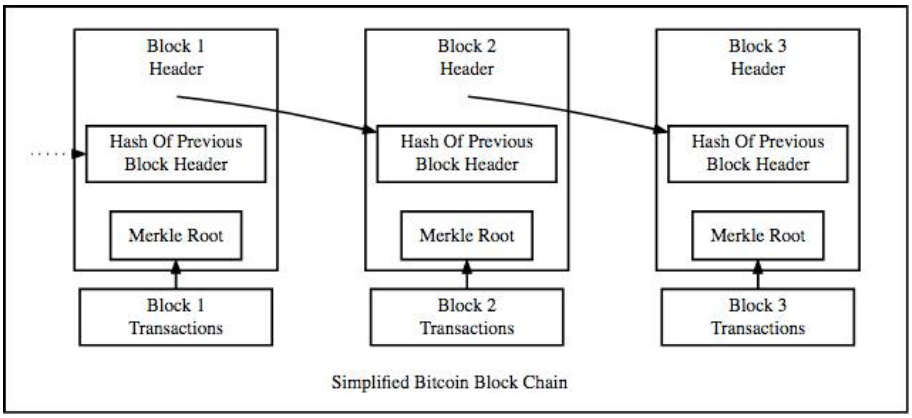

Fig.2. *Blockchain Structure (Source: [4])*

B. Blockchain

It is a linked-list type structure such that each block contains hash of the previous block intrinsic to prevent modification of data in a block once added to the distributed ledger, i.e., Blockchain. Build originally to support Bitcoin as its public distributed legder, it has tremendous scope to be used in several other applications such as those requiring permanent secure storage of data on a distributed network.

Typically, if a transaction in a block is tampered with, the hash value of the Merkle Root changes which in turn will change the subsequent blocks as each block contains hash of previous block. This makes the blockchain immutable as any slight change in any block will completely change the chain.

A block will have one parent but can have multiple child each referring to the same parent block hence contains same hash in the previous block hash field [16]. Every block contains hash of parent block in its own header and the sequence of hashes linking individual block with their parent block creates a big chain pointing to the first block called as Genesis block [16].

Figure 2 (Source: [4]) gives an overview of structure of Blockchain.

What is Bitcoin System

Bitcoin is the world's first decentralised cryptocurrency. It does not require a trusted third party such as a central bank or single entity to verify transactions. It is based on a peer-to-peer network where transactions take place directly between users and are verified by network nodes and recorded in public distributed ledger relying on the consensus of the nodes in the network.

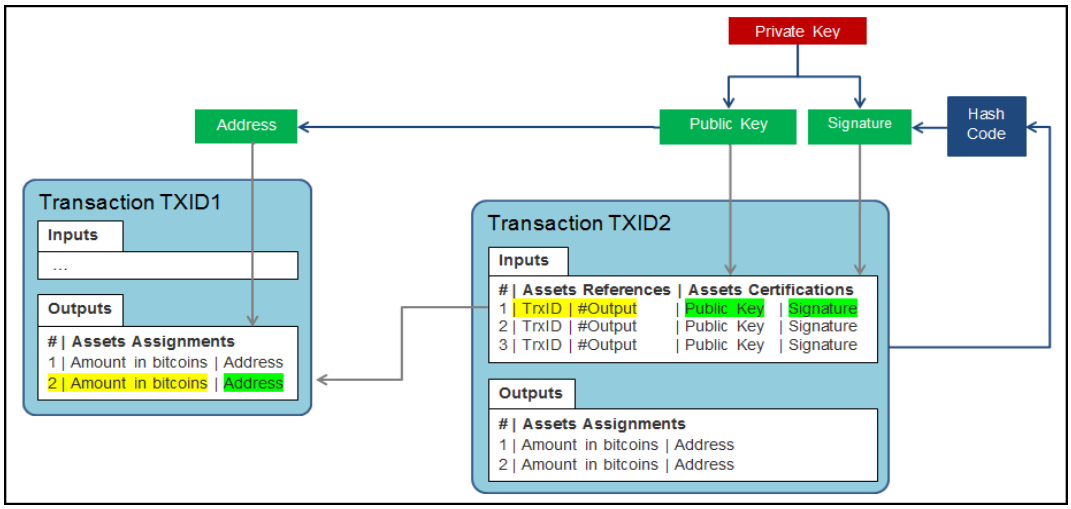

Fig3. *Bitcoin Transactions (Source: [8])*

When we are dealing in physical cash, there is no requirement of a third party to verify transactions as once the real money leaves our possession it completely belongs to the new person. But same thing cannot be said for digital money. One can simply copy that digital money and pay somewhere else (the double-spending problem). Bitcoin solves the problem of being copied and getting spent twice. Bitcoin users protect themselves from double spending fraud by waiting for confirmations when receiving payments on the blockchain, the transactions become more irreversible as the number of confirmations rises [5]. When miners pull the transactions simultaneously from the pool, then whichever transaction gets the maximum number of confirmations from the network will be included in the blockchain, and the other one will be discarded. That's why it is recommended for merchants to wait for a minimum of 6 confirmations [6].

A. Bitcoin Transaction

Transactions are a means to transfer coins from one wallet to another. Blockchain can be imagined as record of the transactions between various bitcoin addresses.

"We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin."

—Satoshi Nakamoto, Bitcoin Whitepaper [7]

Bitcoin Transactions consist of one or more inputs and one or more outputs. When a payer wants to send bitcoins to payee, a new transaction is created. It consists of an input table where each entry in the table is a reference to previous unspent output table entry of a previous transaction in the blockchain such that the current payer was the payee in the previous transaction. The output table consists of current payee address and the amount of bitcoin being sent to that address. The total amount being spent must be less than the total amount received in previous transaction and must be spent in entirety. If there is a difference, it will be automatically assigned to the miner who recorded the transaction as a transaction fee.

Figure 3 (Source: [8]) shows how the output of the previous transaction is used as input for the new transaction. The public key of current payer in input table is a reference to its address in the previous transaction where he received the amount. This unspent amount is being used as input for current transaction to transfer the money to the current payee whose address and amount being transferred is mentioned in output table.

B. Bitcoin Mining and Proof-of-Work

Bitcoin mining is the process of finding new valid blocks and adding it to public ledger. Whenever a transaction occurs, it is broadcasted in the peer-to-peer network. The miners try to bundle the unconfirmed transactions by firstly confirming every transaction being added in the block for correct digital signatures and checking that payer has enough bitcoins to spend. Then, the miner must solve the computationally complex cryptographic math puzzle as Proof-of-Work (PoW).

The problem of double spending is resolved by Proof-of-work and Consensus Protocol. A proof of work is a piece of data which is difficult (costly, time-consuming) to produce but easy for others to verify and which satisfies certain requirements [9]. They are like math puzzles which require some serious computational efforts for solving but are easy to verify. Originally, a proof-of-work (PoW) system (or protocol, or function) is an economic measure to deter denial of service attacks and other service abuses such as spam on a network by requiring some work from the service requester, usually meaning processing time by a computer [10]. A key feature of these schemes is their asymmetry: the work must be moderately hard (but feasible) on the requester side but easy to check for the service provider [10].

PoW involves searching for a value called nonce and calculating hash of the block with this varying nonce using some hash-function based algorithm such as SHA-256, such that the resulting hash begins with certain number of zeros. The average work required is exponential to the number of zeros in the correct hash however, the verification process consists of a single step, i.e., by executing a single hash [11].

As soon as the miner successfully finds this valid hash value for the block, he adds the block to his own local blockchain and broadcasts it immediately across the entire peer-to-peer network, so that it gets appended to the blockchain. The nodes on receiving this solution, first verify the block generated for correctness before adding to their local copy or else discard it. In practice, most Bitcoin clients require 6 "confirmation" blocks before accepting that a transaction is published.

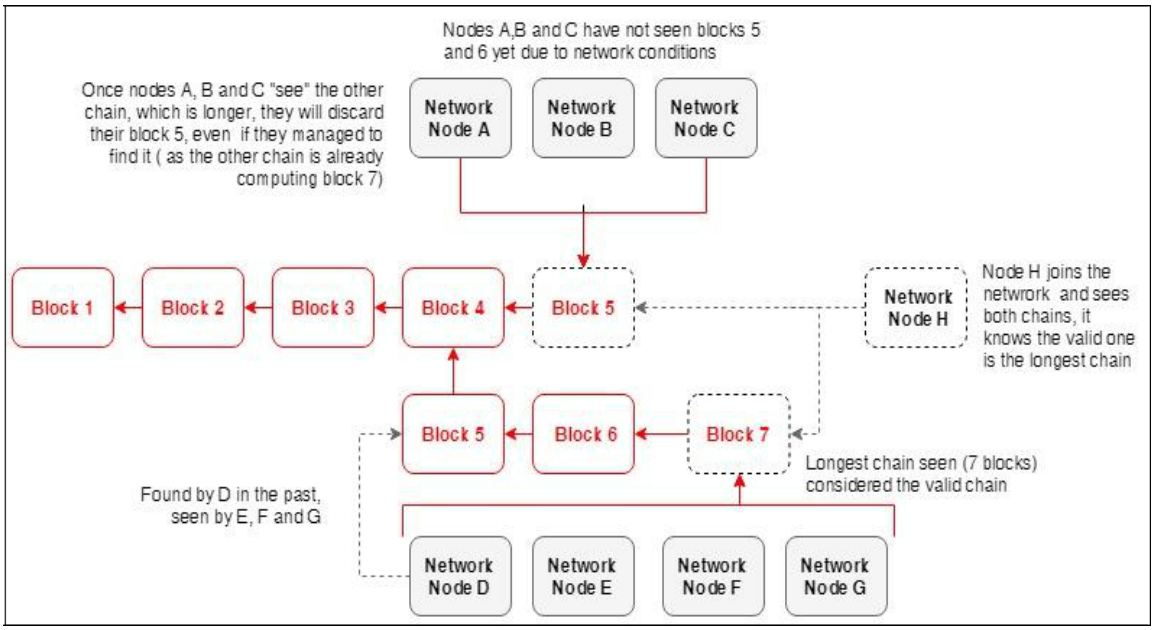

Fig 4. *Blockchain consensus model (Source: [12])*

The computational efforts involved with PoW computation make Bitcoin cryptosystem inherently resilient to Sybil attacks where a single adversary can control multiple nodes by creating several virtual machines or generating mulitple IP addresses. PoW computation is highly resource-exhaustive procedure thus making sure that the nodes are not mere virtual entities. Also, it is a means to make the blockchain tamper-proof as modifying a blockchain by a single entity would be practically impossible. In return, for the computational power put in to generate a new valid block, the miners are rewarded with incentives for generating this new block as well as with transactional fee associated with individual transactions in the block. The subsidy given for generating this new block is also a mechanism to introduce new Bitcoins in the system. At Bitcoin's launch, each new block awarded the miner with 50 bitcoins, and this amount halves every four years: Currently each block includes 12.5 new bitcoins [17].

Nowadays, miners join a mining pool instead of mining individually. In the context of cryptocurrency mining, a mining pool is the pooling of resources by miners, who share their processing power over a network, to split the reward equally, according to the amount of work they contributed to the probability of finding a block [19]. It is like a lottery system where if several friends come under a group to buy lottery tickets, it will increase the overall probability of winning and then the money won is shared among friends proportional to amount spend by them in buying the tickets.

C. Blockchain Forking and Consensus Protocol

Consensus is the mechanism for reaching agreement in a group by involving as many entities as possible and the vote of each and every entity has equal weightage.

Due to distributed nature of blockchain, it is possible that two valid blocks are arrived simultaneously, causing two valid separate paths called blockchain forks of equal lengths. The miners are free to choose either forks and continue mining on top of it. The time necessary for PoW calculation is random resulting in miners working on one fork to broadcast a valid block before the others. Whenever a longer instance of blockchain appears in the network, the principle of consensus protocol is to adopt the longest version as soon as it appears, and miners start adding their following blocks on top of this longer chain.
Figure 4 (Source: [12]) shows how nodes adopt the longest version as soon as it appears.

Potential Security Threats to Bitcoin System

Bitcoin is the most successful digital currency whose security heavily relies on cryptography and the distributed nature of the public ledger. However, the security of such a virtual currency has always been a debatable topic among researchers. Some of the potential threats on this cryptocurrency are discussed here.

A. Double Spending Attacks

Double-spending means spending same bitcoins more than once. This attack is most likely to occur with 'Fast payment' mode where the merchant does not wait to confirm transactions. To mitigate this attack, it is recommended for the merchant to wait for the minimum of 6 confirmations. However, this attack still has a chance to work if the attacker somehow captures 51% of network power (the 51% Attack).

The 51% attack, also known as majority attack is a potential threat where a single entity/group gets control over more than 50% of the network's computing power. The attacker having more than 50% network's computational power can intentionally introduce a blockchain fork by mining privately when paying a merchant for goods. After waiting for n confirmations, the merchant sends the product [18]. If the attacker happened to find more than n blocks at this point, he releases his fork and regains his coins; otherwise, he can try to continue extending his fork with the hope of being able to catch up with the network [18].

It is a debatable issue as practically speaking it is not possible for a single entity to gain more than 50% computational power as it will now act as central authority forfeiting the whole idea of Bitcoin. But it is theoretically possible especially with the rise of mining pools. One mining pool, Ghash.io, once reached roughly 50% of the total computational power. As the pool had no interest in attacking Bitcoin (this would devalue the currency), it took steps to bring the membership back down to below 40% [13].

.B. Selfish Mining

The idea behind Selfish mining attack is to withhold successfully generated block from publishing in the network immediately. Instead, the attacker continues to mine on top of this block secretly while rest of honest miners are wasting their computational power to create this block for the public chain. If this malicious miner is able to find a second block on this new secret chain, it will release its local chain in the network. Thereby forcing the honest miners to accept this chain as it is longer, wasting the efforts of honest miners.

C.Distributed Denial-of-Service Attack

Bitcoin Mining Pools are mostly targeted in Distributed Denial-of-Service (DDoS) Attacks. Malicious miners can perform a DDoS (by having access to a distributed Botnet) on competing miners, effectively taking the competing miners out of the network and increasing the malicious miners effective hashrate [11]. A simple example is sending more amount of junk data than can be handled by the targeted node, hindering its normal working to such as an extent that it starts rejecting requests from honest clients.

D. Attacks on Bitcoin wallets

The client-side applications known as 'wallets' are basically used to manage the Bitcoins owned by the client as well as the transaction of the Bitcoins from/to the client [14]. The wallet thefts are mainly performed using mechanisms that include system hacking, installation of buggy software, and incorrect usage of the wallet [11]. Researchers at the University of Edinburgh in the UK carried out an in-depth security analysis of the communications system used in popular models of Bitcoin wallet [15]. The team used their simple malware to intercept messages exchanged between hardware wallet and computers exposing the vulnerability which can put the users' privacy at stake.

Conclusion

Bitcoin is considered the world's first decentralized digital currency based strictly on peer-to-peer network without any central authority such as government or banks to monitor. Much like cash, the personal identity of the person is not needed. Due to increasing faith and recognition of the system, it has the potential to be future of currency as long as security concerns are taken into consideration. The privacy however, has raised certain concerns involving financing of criminal activities such as purchase of illegal goods, tax evasion, terrorist funding, ransom for hackers, etc.

Nonetheless, it gave an intriguing concept of Blockchain which is often considered the next revolution after the Internet, with big companies investing in it. Created as a technology to support cryptocurrency, it has immense potential to be used in Internet-of-Things (IoT), Smart Contracts, Digital Identities, Digital Voting, to name a few.

On the whole, the sole purpose of this paper is to present the basic concept of Bitcoin and the technology behind it, opening a few queries on security aspects so as to have a better understanding of the relatively new concept which has the tremendous potential to change the future of financial and many other services.

References

1. Bitcoin, From Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Bitcoin
2. Blockchain, From Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Blockchain
3. Why does each block store a Merkle root? https://bitcoin.stackexchange.com/questions/48928/why-does-each-block-store-a-merkle-root
4. What Is Hashing? Under The Hood Of Blockchain, By Ameer Rosic, https://blockgeeks.com/guides/what-is-hashing/
5. Irreversible Transactions, From bitcoinwiki, https://en.bitcoin.it/wiki/Irreversible_Transactions
6. What is Double Spending & How Does Bitcoin Handle It?, https://coinsutra.com/bitcoin-double-spending/
7. Satoshi Nakamoto, "Bitcoin: A peer-to-peer electronic cash system", 2008.
8. An Introduction to the Bitcoin System, Structure of a transaction, https://pascalpares.gitbooks.io/implementation-of-the-bitcoin-system/content/1-transaction-4-structure.html
9. Proof of work, bitcoinwiki, https://en.bitcoin.it/wiki/Proof_of_work
10. Proof-of-work system, From Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Proof-of-work_system
11. Mauro Conti, Senior Member, IEEE, Sandeep Kumar E, Member, IEEE, Chhagan Lal, Member, IEEE, Sushmita Ruj, Senior Member, IEEE, "A Survey on Security and Privacy Issues of Bitcoin", arXiv:1706.00916v3 [cs.CR] 25 Dec 2017
12. What is meant by forking in a Blockchain?, https://lightrains.com/blogs/what-is-meant-by-forking-blockchain
13. CS269I: Incentives in Computer Science, Lecture #9: Incentives in Bitcoin Mining∗, Tim Roughgarden†, October 24, 2016, http://theory.stanford.edu/~tim/f16/l/l9.pdf

14. Chinmay A. Vyas and Munindra Lunagaria, Department of Computer Engineering, Marwadi Education, Foundation's Group of Institutions, Rajkot, Gujarat, India, "Security Concerns and Issues for Bitcoin",International Journal of Computer Applications® (IJCA) (0975 – 8887), National Conference cum Workshop on Bioinformatics and Computational Biology, NCWBCB- 2014
15. Bitcoin wallet devices vulnerable to security hacks: Study, .https://telecom.economictimes.indiatimes.com/news/bitcoin-wallet-devices-vulnerable-to-security-hacks-study/6263284
16. Sachchidanand Singh, IBM Software Lab and Nirmala Singh, Tech Mahindra, "Blockchain: Future of Financial and Cyber Security", IEEE 2016
17. What is Bitcoin Mining?, https://bitcoinmagazine.com/guides/what-bitcoin-mining/
18. Majority attack, From bitcoinwiki, https://en.bitcoin.it/wiki/Majority_attack
19. Mining pool, From Wikipedia, https://en.wikipedia.org/wiki/Mining_pool
20. BLOCKCHAIN APPLICATIONS: BEYOND BITCOIN, https://www.itransition.com/blog/blockchain-applications-beyond-bitcoin

Citation: **Anam Fatima, Dr. Vijay Kumar Tiwari, "***Bitcoin Cryptocurrency: A Review". American Research Journal of Computer Science and Information Technology; vol 3, no. 1, 2018; pp: 1-8*

Copyright © 2018 **Anam Fatima, Dr. Vijay Kumar Tiwari.** *This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.*