IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 5, May 2020

The Bitcoin: An Unstable Boon

Surendhar.P[1], Subhashini.A[2]

UG Scholar, PERI Institute of Technology, Department of Computer Science, Chennai[1]

Assistant Professor, SMK Fomra Institute of Technology, Department of Computer Science, Chennai[2]

Abstract: This paper gives the complete overview of working of bitcoin and what are the problems will it face in the near future? It depicts the difference between the proposed theoretical architecture and current practical implementation of secure hash algorithm. The reason for proposing alternative secure hashing algorithm called SHA-512 replacing the most successful SHA-256 hashing algorithm is the evolution of quantum computers which has an ability to crack the hashing algorithm.

Keywords: Bit coin, Hashing Algorithms, Quantum Computers

I. INTRODUCTION

An unknown programmer under the name Satoshi Nakamoto published a paper **Bitcoin: A peer to peer electronic cash system**. That paper contains the first ever practical implementation of digital cryptocurrency. This cryptocurrency concept was already introduced by Wei Dai in 1998 in cryptographic mailing "Cypherpunks". Bitcoin eliminates the need of central authority for controlling the exchange of money t in the form of bitcoin. Hence it is decentralized and peer to peer system. Satoshi did not reveal his identity because to create the faith among the users that he did not get any profit from the bitcoin and additionally he made the coding of bitcoin as open source. Bitcoin can be earned by many ways. We can buy bitcoins by using our currency or we can sell the products and can get bitcoin instead of getting currency and . But to create new bitcoins we have to do mining. Speaking about mining I introduce u that the bitcoin runs under the most successful technology called Blockchain. Simply the process of adding the blocks in the blockchain is called mining and it involves some mathematical calculations. Bitcoin has a advantage over our current currency that it does not have any transaction fees. All the transactions are public and every one in the bitcoin network will have the copy of transaction records. Don't be panic because it does not have name of the person but it contains the wallet address of the persons involved in transaction and amount of bitcoin transferred from one to another. Bitcoin was launched soon after the financial crisis (2007-2008) that had demolished the faith of centralized banking system among the people.

II. WHY CAN'T WE MADE IT AS A GLOBAL CURRENCY?

The reason for this is the volatility and the degree of acceptance. Volatility can be reduced when number of people joins the bitcoin network but the degree of acceptance can only be increased when people and the government has an clear idea about this bitcoin technology. Another reason is, eventhough people lost a faith in centralized system they won't believe in the technology because of lack of awareness. In addition to this a criticism also is there on bitcoin that **IS IT REALLY A CURRENCY OR COMMODITY?** The reason for this confusion is that the value of bitcoin is not constant and it is varying like Gold or any other goods.

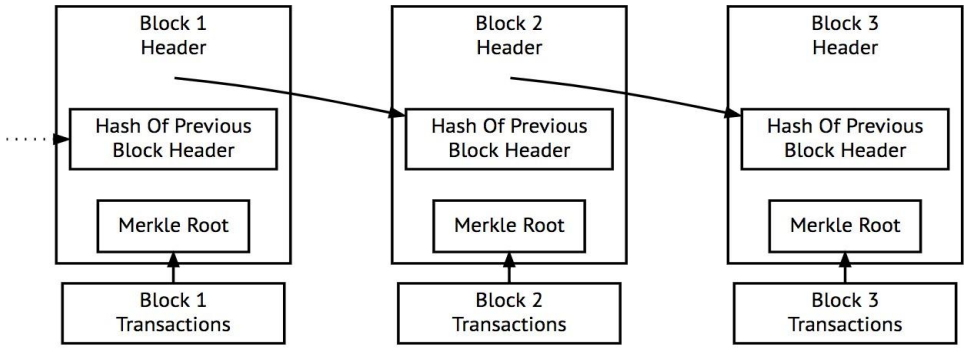
III. WHAT IS DECENTRALIZATION?

Decentralization is the term which says there is no authority or power controlling the transactions. Then the question arises how can the users believe that it is safe.Normally when a person wants to send money to another person the bank verifies that transaction and stores the amount of money transferred from that account and further decreases the money from sender and increases the money of receiver and stores all this information in a ledger(like a database) for future reference. In case of any problem with the transaction only the bank can deal with but not the persons. Additionally the person have to pay the transaction fee. In case of decentralization, transaction between the transactions between the two person will be maintained publicly by all the nodes(users) in the bitcoin network. Transaction occur after the nodes in the network validate the transaction. In technical terms transaction records are stored in a distributed ledger. This is the basic overview of decentralization. The more technical view will be discussed in the topic of mining.

1 AN OVERVIEW OF BLOCKCHAIN TECHNOLOGY.

As we seen in the previous topic all the transactions are stored in the public distributed ledger and that ledger is called block. Block is a collection of transactions and sequence of block in the chain format is called blockchain.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 9, Issue 5, May 2020



Simplified Bitcoin Block Chain

In bitcoin a block is added on the block chain in an average of 10 minutes. The block contains the reference to the previous block and the record of previous transaction. To add the block in blockchain the nodes in the network called miners will have to solve a mathematical problem(Hashing in technical term) and the first one who finds the correct answer publish his answer to all nodes and then block is added in the blockchain and the bitcoin will be rewarded to that person who found the correct answer and this is the basic of how new bitcoin is generated to reward the miner. This process is mining and we will see it in detail in the upcoming session.

IV. EXPLANATION ABOUTMINING.

As we have seen before the only way to generate the new bitcoin is through mining. What really this mining is. The bitcoin is programmed in this way that the bitcoin will be generated when the block is added successfully to the block chain. Therefore the process of adding the blocks in the blockchain is called mining. It is not that simple as explained in the theory. It needs huge computational power. Earlier when bitcoin was introduced mining can be done with a help of our normal CPU but now as the number are increased it becomes extremely difficult to mine as it needs a specific dedicated CPU and GPU. Why it needs so much computational power, let us discuss it below

STEP 1:If Bitcoin user A wants to send some bitcoins to user B from his bitcoin wallet(same as like paytm wallet and there is a specific software for it Eg.Bitcoin Core) , the transaction is picked up by a block chain network and it is inserted into the buffer of unconfirmed transactions still it is not confirmed yet.

STEP 2: Miners(nodes) on that blockchain network select that transaction from that buffer and add it to their block. Note that all the miners will have a individual block and add this transaction to their block and those who win in the process of mining will get their block added in the blockchain. Before that they check the balance in the user's wallet and gives priority to large transaction for their profit.

STEP 3:As soon as the miner has added the transaction in their block, mathematical problem arises for adding that block in the blockchain. The problem is unique for different miners but the difficulty of the problem is same. What is this problem? How to solve it?
Before we proceed we have to know what is called hash function? A hash function is one that takes any number of strings as input which can be infinite(Even a full book) and gives the 32-bit output in case of 32 bit or 64-bit or 256-bit or 512-bit in case of 32-bit 64-bit 256-bit 512-bit hash functions respectively. If we change even a single letter in that book hash output gets changed. So in case of bitcoin the hash function takes the meta data present in the transaction block and gives the hash output. The rule in the bitcoin mining says that the output hash will contain certain amount of zeros in the beginning. How it can be obtained with certain number of zeros? This is where the nonce field comes in. Nonce is the variable field present in the block.We have to achieve the hash output by changing this nonce field randomly.This takes more time to produce to calculate the output with preceding number of zeros so it needs more computational power. As the miner in the node decreases the difficulty of the problem is reduced.

STEP 4: The miner who finds the hash output with preceding number of zeros publish his answer and all other nodes verify this answer and finally the block is added. This is called proof of work as the miner shows the proof of his work to all the miners. Therefore consensus is reached (Consensus means agreement). Every time the another block added on to the blockchain it is called the confirmation of the block. The average time for a transaction in a block chain is 10 minutes.

This is how the mining works. The hashing algorithm used in this mining is SHA-256.We will see about this in detail in the next topic.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 5, May 2020

V. EXISTING SYSTEM USING SHA-256 ALGORITHM.

Before that we see some practical implementation of hash functions since they are used all throughout the Bitcoin protocol. If our input is 1234 we would get an output of 10.

1234==10(This is not the real calculation just for understanding)
It should be very easy to compute an output for any given input, but it should be impossible to compute the input for a given output even while knowing the mathematical algorithm. Consider, in the above example
we can easily compute an output of 10 given the input of 1234, however going in reverse is not easy because there are many possible inputs that can produce 10 (55, 136, 7111, etc). Unlike our example, each output should map to only one input. If a two different inputs can produce the same output this is called a hash collision. Good cryptographic hash algorithms are resistant to such collisions. A hash function should be able to take inputs of variable size and turn them into outputs of a fixed size. For example:

Hello==>**2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5 c1f45e73043362938b9824**
goodbye==> **82e35a63ceba37e9646434c5dd412ea577147f1e4a41cc de1614253187e3dbf9**

The output should be the same length whether the input has 10 characters or 10 thousand characters.
A tiny change in the input should produce an entirely different output. Example:
helloworld==> **98c615784ccb5fe5936fbc0cbe9dfdb408d92f0f** HelloWorld==>**a830d7beb04eb7549ce990fb7dc962e499 a27230**
HelloWorld!==> **8476ee4631b9b30ac2754b0ee0c47e161d3f724c** Hello, World==> **6782893f9a818abc3da35d745a803d72a660c9f**

From the above example we can see that even a comma exclamatory and case can entirely change the output. This is the common overview of practical implementation of hash algorithm.

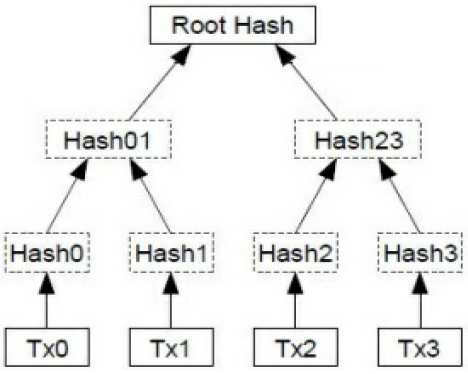
SECURE HASH ALGORITHM(SHA-256).
The existing system of bitcoin uses this cryptographic hash function developed by the National Security Agency. It is a hash function which takes any number of strings into input and hashes it into 256-bit(32 byte) output. The first step in the process is to hash each transaction in the memory pool using SHA256. The raw transaction data may look something like this

01000000017a06ea98cd40ba2e3288262b28638cec533
7c1456aaf5eedc8e9e5a20f062bdf000000008a4730440 22030e2d23be71a907a3ad7de846b3bbe8886c4a839e1
aa2cf0d314b1d327f12d2a022039718fc3886a171e4ec2 b138e6547b03dd326ef7f12295d06e351e7c020100680
14104e0ba531dc5d2ad13e2178196ade1a23989088cfb eddc7886528412087f4bff2ebc19ce739f25a63056b602
6a269987fcf5383131440501b583bab70a7254b09effffff ff01b02e052a010000001976a9142dbde30815faee5bf2
21d6688ebad7e12f7b2b1a88ac00000000

Once hashed it will look like this because SHA-256 converts any number of input into 256-bit string

2d94683fa2f8aaae4a6f377d93b875f680adf96b9c3e957 7554b742f412fa9ad

These hashes are then organized into something called a Merkle Tree or hash tree. The hashes of the transactions are organized into pairs and concatenated together then hashed again.



This diagram is called Merkle Tree diagram.

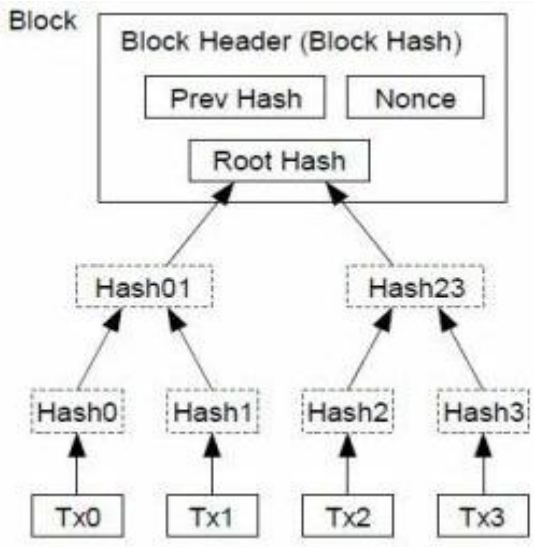
In the above example there are only four transactions (tx stands for transaction). A real block will contain hundreds of transactions so the bracket (tree) will be much larger. The hash at the very top of the tree is called the

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 9, Issue 5, May 2020

Merkle Root.The Merkle Root of this hash tree is placed into the block's header along with the hash of the previous block and a nonce.

The block's header is then hashed with SHA256 producing an output that will serve as the block's identifier. Now we have successfully hashed the data in the transaction block. Then as we had seen in the mining topic we have to make his hash output to start with leading number of zeros. To do that we have to change that nonce field and hash it again to produce a output with leading number of zeros. "Hello,world!0"=>**1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64**
"Hello,world!1"=>**e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d822f5928be8ca2a32aa475cf05fd4266b7**
"Hello,world!2"=>**ae37343a357a8297591625e7134cbea**
……. "Helloworld!4248=>**6e110d98b388e77e9c6f042ac6b497 cec46660deef75a55ebc7cfdf65cc0b965.**

From the example we can understand what is happening really. Helloworld is the data and the number near that is the nonce field we have to change it to attain our output. It takes 4000 attempts to produce a output with leading number of zeros. And this is how the block looks like



VI. SHA-256 IN PRIVATE KEY GENERATION.

Public and private key pairs are the essential first step in owning Bitcoin. A public key allows you to receive Bitcoin, and the corresponding private key keeps them safe. Knowing how these keys are created should be your first step in understanding Bitcoin.

A private key in Bitcoin is just a random number between
1 and 2^{256} as the algorithm used is SHA-256. All the private keys that protect all the bitcoins in the world are just different random numbers between 1 and 2^{256}. Theoretically anyone can attempt to guess your private key, but 2^{256} is such a large number that it would take an attacker billions of years to try all the possible private keys.

To create our private key we need a way to generate a random number. To do this we need to use a number generator that is cryptographically secure. A number generator is cryptographically secure when the number generated cannot be determined or known how it was chosen.

Step 1: Generate a random set of data

For our purposes of Bitcoin, we need a cryptographically secure number generator to generate our number. To satisfy this requirement we need to generate a random set of data, we will convert this data into a number later. This is the random data

AofidowXhk&)):@:@9727929Hcks&&&(nkhgiowiwj91928 3$'@bnwkiHhVjKihUNnkllswiwi9@/93938'bbndkk!?,(ikjql wlw188020$Hbnk

Step 2: Convert random data to 256-bit number

Now that we have a random set of data, we can use SHA256 to convert our random set of data into 256 bits. Here's the SHA256 hash of our random data.

**3133293B7827ED422EA95FF7E6B92145FAA6A22DE18
96043F457306AF4CF5B42**

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 9, Issue 5, May 2020

Now the question arises that there are only 64 bits and the reason is, it is denoted here in hexadecimal(64 characters x 4 bits = 256 bits)
In order for us to see our number we have to convert our hexadecimal into decimal.

22253723355774722335514752419334321201576740
24762163265803339289273407998240 2

22 quattuorvigintillion 253 trevigintillion 723 duovigintillion 355 unvigintillion 774 vigintillion 722 novemdecillion 335 octodecillion 514 septendecillion 752 sexdecillion 419 quindecillion 334 quattuordecillion
321 tredecillion 201 duodecillion 576 undecillion 740 decillion 247 nonillion 621 octillion 632 septillion 658 sextillion 33 quintillion 392 quadrillion 892 trillion 734 billion 79 million 982 thousand 402

Step 3: Verify Number
Now that we have generated a cryptographically secure 256-bit random number the final thing we need to do is verify if our number is between 1 and 2^{256}.
Our number, even though very large, is still much smaller than the Bitcoin limit of 2^{256}. This means our number qualifies and can now be used as a private key on Bitcoin.

Step 4: Add version number
In Bitcoin every private key on the main net begins with "5". This makes it easy to identify a private key. In order for us to have our private key start with "5" we need to add 80 to the beginning of our hexadecimal.

803133293B7827ED422EA95FF7E6B92145FAA6A22DE
1896043F457306AF4CF5B42

Step 5: Add 32 bit checksum
Typing our private key, because it's so large, can be prone to errors. Adding a checksum allows us to detect any typing errors when using our private key. To add a checksum to our private key we need to get the double SHA256 hash of our new hexadecimal number.
Here's the hash of our new hexadecimal.

F5A3CF1E170C27BEFA81A25E4ECA1B1E9BE1B822DFE 4095B82059B29A094784D
And here's the hash of the hash above, also known as a double hash.
58DAE61C47E89B61FFF699B413A8922AF5C6F1AB9FE
45ABBBBE6281547FC0904
Now take the first 8 characters, 32 bits, of the double hash and add it to end of our new hexadecimal above.
803133293B7827ED422EA95FF7E6B92145FAA6A22DE
1896043F457306AF4CF5B4258DAE61C

Step 6: Convert new hexadecimal to base58
To further prevent typing errors we need to convert our private key from hexadecimal to base58. Base58 removes easily mistakable alphanumeric characters o, O, L, and I. The result is 58 characters that can be used to represent our private key. Here's our converted base58 private key, which includes the "5" required for every private key on Bitcoin.

5JBxKqYKzzoHrzeqwp6zXk8wZU3Ah94ChWAinSj1fYmy JvJS5rT

This is our finalized private key.

VII. DISADVANTAGES OF EXISTING SYSTEM

An quantum computer said to be arrive in future can break the SHA-256 algorithm but many said that it cant happen as the normal computer may take trillion of years to break it.
We cant predict the future as anything can happen.
Still some security issues are there with bitcoin mining implemented using SHA-256 algorithm.

VIII. PROPOSEDSYSTEMUSINGSHA-512ALGORITHM

This is completely the theoretical approach. Moreover this is not criticization of the current implementation of SHA-256 algorithm. Just a suggesting way to escape the cryptographic algorithm from the attack of quantum computers.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 5, May 2020

SHA-512 is an advanced version of SHA-256 algorithm. Here there is no show off the implementation of this algorithm since it is same as that of SHA-256. But there is only one difference. The difference is that it produces 512 bit output but SHA-256 produces only output of 256 bits. It produces 2^{512} combinations.
As seen in the above figure the hash output will be of 512 bits. Then the question arises why it is preferred over SHA-256 algorithm.

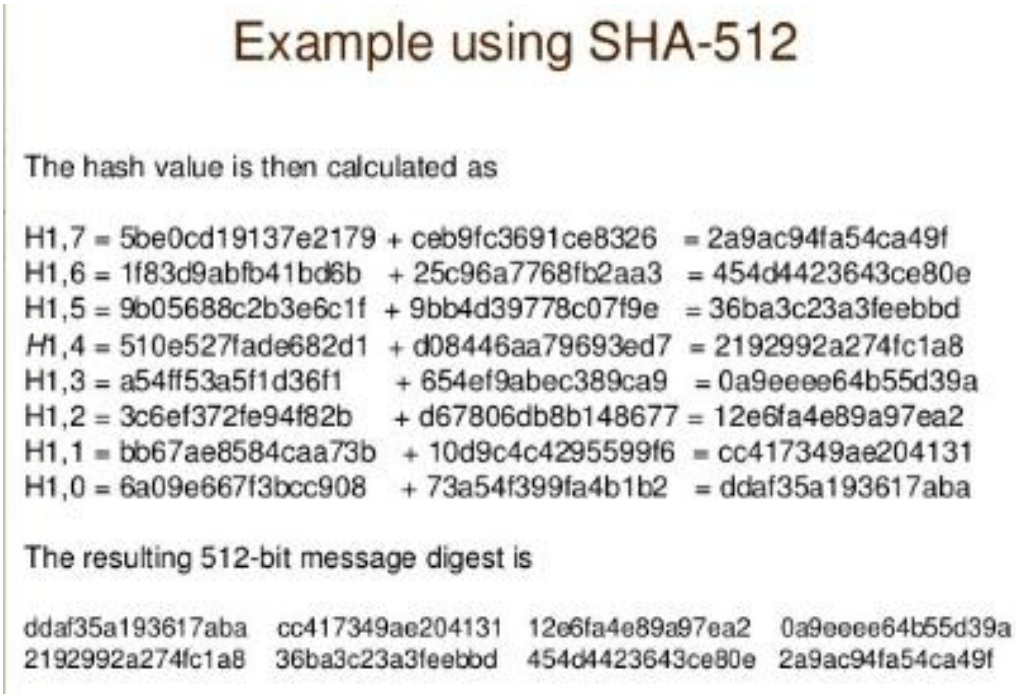
IX. SHA-512 IN MINING AND PRIVATE KEY GENERATION

If we implement SHA-512 in the process of mining, the miners have to generate 512 bit hash output. The advantage of it is that it increases the security of the block as many fraudsters are eager to attack the blockchain. There are many attacks like 51% attack occurred on the blockchain but it is impossible to attack the blockchain after implementing this algorithm because more than 50% of the miners cannot take over the blockchain network. The disadvantage is that it will increase the mining time as well as the transaction time.

If we implement this in the private key generation it will generate private key of 512 bits.
If any one wants to get a private key they have to check
2 power 512 combinations. For a super computer it takes billions of years to calculate. But quantum computers may have chance to crack it. Suppose if the quantum computer takes 1 year to crack the SHA-256 algorithm then it takes 2 years of time to crack the SHA-
512. To increase the security of bitcoin from the quantum computers I prefer SHA-512 over SHA-256.

X. CONCLUSION

It is impossible for fraudsters to take control over a blockchain network. It increases the security of bitcoin network 2 times more than that of existing system. It becomes difficult for a quantum computer to crack the private key. Moreover, it keeps the bitcoin network secure for more years.



REFERENCES

1. INVESTOPEDIA. www.investopedia.com
2. MYCRYPTOPEDIA www.mycryptopedia.com
3. Bitcoin: A peer-to-peer Electronic Cash System