A Bird's Eye View of Crypto Currency (Bitcoin)

B. Muni Lavanya
Lecturer, CSE Department, JNTUACEP, Pulivendala, India

Manoranjan G
Computer Science and Engineering, JNTU Ananthapuramu, Ananthapuramu, India

Pasula Madhu
School of Computer & Information Sciences, University of Hyderabad, Hyderabad, India

Abstract – Cryptocurrency has become the buzz word in today's digital currency. Bitcoin is popular among those cryptocurrency that records all the transactions in decentralized open ledger, the technology called Block chain. Though we have more than 100 cryptocurrency exist in digital world, bit coin hooked up the market most. Bit coin economic value has increased at the enormous rate and it is now worth of about $15629.6 U.S. In this paper we discussed the glimpse of bitcoin's past and present, and implementation of block chain and also addressed the risk of security issues and challenges.

Index Terms – Crypto currency, Bitcoin, Block chain.

1. INTRODUCTION

Bitcoin is a cryptocurrency and a worldwide payment system. It is the first decentralized digital currency. The system works without a central repository or single administrator. We come across with the lot of new technologies everyday which changes day to day life but once in a while we come across something that changes everything. It changes every fabric of society. Our paper is completely based on one such thing called bitcoin-a change in our money. To know about bitcoin first let us have brief look into the history [1] of change in evolution of money over the years. The firs pertinent thing to know in this transition process is why do we need money? In the past, the money was used for the exchange of commodities has some intrinsic value for money. Until several centuries ago, the concept of money was grown up with evolution of gift economy like exchanging cattle or grains or seashells. But there are extreme challenges while using gift economy like portability, divisibility of money and performing small transactions. A long time ago, the precious metal gold served as a form of money, which was easily movable and divisible. Gradually, the society started accepting it as global money. After a brief period, the paper currency as a legal tender evolved, replacing the existing system and emerged as an exigency. At this position, the concept of banking system has started with catching up the sources of technology. People were encouraged to reach banks to exchange the money and to deposit gold and metal with secure tracking records. Following this, the concept of payments system emerged with more effective use of advanced technology that accelerated whole system into a world of today. The concept of crypto currency is most advanced generation of exchange of money designed with particular software keys, which secures the identity details and transaction details. The differences are given with examples, on how are the transactions transacts over banking system and crypto currency, the need of third party intervention in the first case for authentication and none in second case. Until recent money was physical in nature if X wants to make a transaction he would physically exchange these paper but since few decades global unity started using the electronic network to transfer money where money is not physically moving between transactions but some other third party is needed to be trusted as gate keeper for example when same X wants to send money to Y over a network there would be five people performing a single transaction like in this transaction there are X, Y, X's bank, Y's bank and the other bank which confirms the transactions between X's bank and Y's bank as the most money is being transferred over the network the third party network has become more powerful sometimes they can even disallow any transaction over the network. It was like the only of using electronic money is as permissible. By the third party which was not in the case of physical money and the other case there are $6 trillion U.S. are being transferred among the globe which triggers an idea and a scope of global money that is what we call bitcoin. In 2009 January an unknown person called Satoshi Nakamoto [2] has invented bit coin which would give the benefits of both electronic and physical money as there is no involvement of third party permission to transfer money because of the brilliant back end technology of bitcoins. Bitcoin is the money which can be transferred over the network without giving data privacy and even without knowing anybody either the transaction happened or not. Bit coin is a decentralized currency [3] comprising computer codes that are signed each time; it travels from one owner to the next. The anonymous transactions are verified by miners, who perform complex calculations to maintain a secure network called 'block chain [2] [13]'. The miners receive bit coin for their services and the cycle continues to generate more of crypto currency [4]. The value of bit coin is precious because the designed algorithm by Satoshi could only generate 21 million

bit coins but till 09 Dec 2017 it has already generated 16.7 million bit coins. However, there is no official organization to decide and authenticate the procedural functioning of crypto currency, to determine the target figure to produce, and keep a track of crypto currency transactions details.

2. BLOCKCHAIN TECHNOLOGY

Block chain [2] [13] is a technology which enables the cryptocurrency or digital assets from one individual node to another. The basic ethic of block chain is to transfer the money. Before knowing about block chain let's look into the problems occur while transferring a money on electronic network now a days.

1. If A wants to send money to B when both are in different places globally they have to seek the help of trusted third party which charges for this transactions. And they maintain this transaction details in their log.

2. This trusted third party takes time to complete this transaction and the charges are more. By using the blog chain these problems are addressed without third authority and much faster and cheaper way. The major principle of block chain is maintaining the open ledgers.

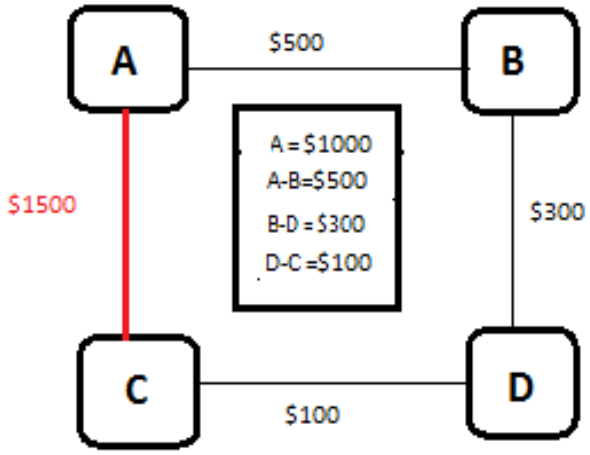


Figure 1: overview of block chain open ledger.

Example: [5] A has $1000. A, B, C, D is four nodes which are connected in chain if A sends $500 to B this transaction details written in ledger. In the same way B did transfer money of $300 to C, will also be written in the ledger. In case of D to C it is $100. In the same way A wants to send $1500 to C the transaction will not be valid as A doesn't have sufficient funds. This chain of transactions is open to public. The above transactions are look as they are being maintained in a centralized ledger but in block chains the ledgers are distributed in nature. They are being maintained by Voluntary nodes called Miners [5].

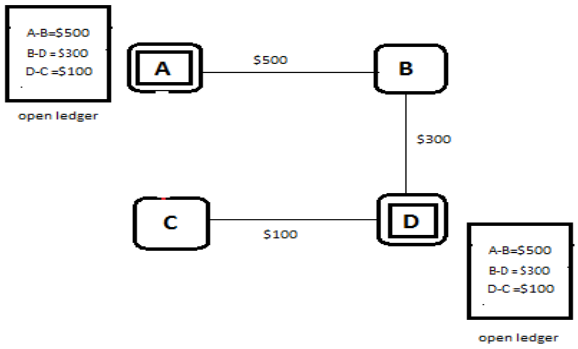


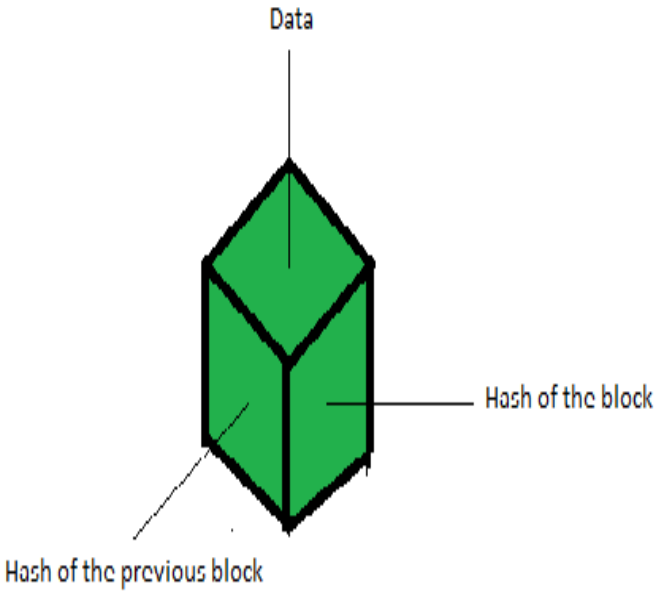
Figure 2: block chain open ledger.

HOW DO THEY EXACTLY MAINTAIN LEDGERS?

When the ledger books have been stored over a worldwide network managed by volunteers [6], as each node would have a copy of the ledger showing the copy of ownership. Which is visible and publically known? Every time nodes try to make a transaction it would just announce its intension to this computer network to send coins to someone else. Upon knowing this all other nodes will update their ledgers by deducting coins from sender and adding to the receiver in their own ledgers, to work out this in the real world without revealing the personal identity on this public ledgers the algorithm uses hash functions [7] and each node identity is summarized and recognized with a 20 bit code. Only owners know the inputs to generate this 20 bit code.

Note: Bit coin uses SHA-256 hash function [8] [13].

CLOSER LOOK AT BLOCK CHAIN:



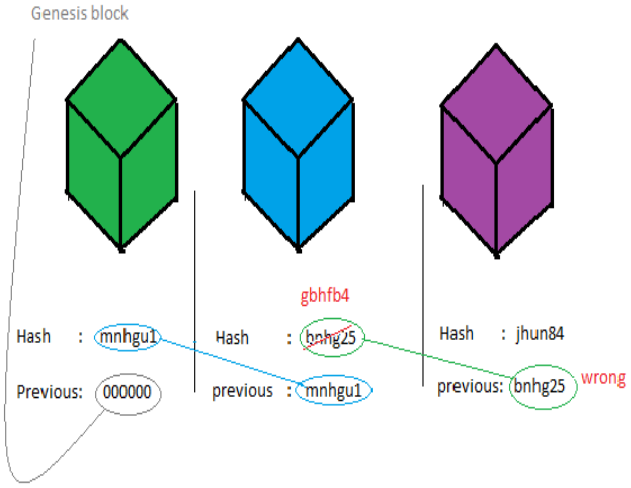
IN DETAILS OF BITCOIN BLOCK:

Data = Sender + Receiver + amount of coins

Hash = Unique identification for all the content of that block.

Hash of previous block = Unique identification code of previous block

The below fig shows how open ledgers are verifying the changes.



Note: In bitcoin case it takes 10 minutes to create every new block to the chain.

3. BIT MINING

Bit mining [6] is a process of generating bitcoins with the help of minors. Basically the mining is of two types they are Solo mining and pooled mining [9]. Solo mining can consist of single minor and it attempts to generate new blocks on its own by solving those blocks it can get block rewards and transaction fees [9] .In pooled mining, minor can pool the resources with other minors to find blocks. In generating bit coins miners are competing to perform two things.

- Validate
- Key

In validating process it just checks whether this transaction could happen or not (Eg: if sender has sufficient money or not). In order to find special key, that will enable to lock the new transaction with the old transaction. To do this, the miners has to invest their computational power, whichever the miner can do this would get a financial benefits. In this case its bit coins.

4. APPLICATIONS

- Security and control over the money
- Quick global transactions.
- Controlled brokerage.
- Disclosure of personal information.
- Digital transactions can be made effectively and uniform globally.

Present Circulation of bit coin in the world	16,728,663
Total amount of bitcoins can be produced by Algorithm	21,000,000
% of bitcoins mined till Dec 09	79.66%
Bitcoins are left to be mined in total	4,271,338
Bitcoin price (USD)	15629.16
Market capitalization (USD)	$257,454,115,875.00
Bitcoins generated per day:	1,800
Inflation rate of bitcoin per day	4.01%
Bitcoin inflation per day (USD)	$27,702,000
block generation time	10mins
blocks generated per day	144
Hash rate:	12.19 Exahashes/s

- New form of currency which is more secure and reliable.

5. TRENDING DATA OF BITCOIN (DEC 2017)

TABLE: [10] DATA BY BITCOINBLOCKHALF

6. SECURITY ISSUES AND CHALLENGES ON BITCOIN

- As we discussed in the section of block chaining all the transaction details are known to public, how do we achieve secrecy (personal identification). This will be addressed using the concept of hash function.
- The way to compare quickly the ledgers between the nodes to make sure that they are maintaining the correct version of transaction record. This also can be solved with the hash function. Like each node can transact to ledger, which hashes to 20 bit hash code and compare with hashes of other ledgers. If the hashes are same we know that the ledgers are same. If they are same it's likely that they represent an accurate

view of coin ownership. This clearly shows that it is almost impossible to tamper the ledgers. To do so, the intruder has to tamper all thousands of other copies which are independently stored at each nodes around the world.

- In cryptocurrency only the creator can crack the code. But if there is any intentional mollified behavior of the creator can harm the world's economy.
- Identity disclosure feature of cryptocurrency can be exploited by the black money holders in order to safeguard their illegal money.
- As per the article of fortune [11] says 4 million bitcoins are missing over the network which are worth of $8500 which means bit coins are more complex to understand than what people have assumed or these missing bitcoins might be already migrated into current currency value(it is an open question to be solved). Among these missing coins 2% of bitcoins are lost due to the death of bitcoin holders and loss of the private key due to carelessness.

7. FUTURE WORK AND CONCLUSION

There is a more scope to do research on bitcoins as there are many open questions to be answered like how are the bit coins missing from network? Why are they missing out? And is it possible to apply the Shamir secret sharing scheme as the bitcoin is decentralized to find out the missing bitcoins problem. Most importantly how this economic balance will be maintained if the bitcoin would be the global economy.

From the above knowledge we conclude that Bitcoin is an electronic simple of trade out the online world. For the past 50 years futurists have proclaimed the appearance of absence money society. A large number of their forecasts have been acknowledged, using crypto currency there would be no focal specialist in charge of the issuance of Bit coins, and there is no compelling reason to include a trusted outsider when making on the web exchanges. Dynamic investigations, where an invested individual can conceivably convey 'checked' Bitcoins and work together with different clients can find significantly more data. We additionally trust that huge unified administrations, for example, the trades and wallet administrations are equipped for distinguishing and following extensive bits of client action.

REFERENCES

[1] Sandeep Goenka, CO-founder of Zebpay, "Zebpay.com"
[2] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", *Jan 2009*.
[3] Puneet Kumar Kaushal, Dr. Amandeep Bagga, Dr. Rajeev Sobti,' Evolution of Bit coin and Security Risk in Bit coin Wallets", 2017 International Conference on Computer, Communications and Electronic (Comptelix).
[4] Rt.com*,"*Bitcoin mining uses more electric than 159 countries *", 09-Dec-2017*.
[5] Shai Rubin, CTO, "Citibank Innovation Lab, tlv"
[6] Matthew Vilim, Henry Duwe, Rakesh Kumar, "Approximate Bitcoin Mining", 2016 53nd ACM/EDAC/IEEE Design Automation Conference (DAC).
[7] Christofpaar." Understanding the Cryptography", *Spingers*,
[8] NSA, http://www.iwar.org.uk/comsec/resources/cipher/sha256-384 512.pdf
[9] Satoshi Nakamoto, https://bitcoin.org/en/, *Jan 2009.*
[10] Article, "http://www.bitcoinblockhalf.com/".
[11] Fortune, "Exclusive: Nearly 4 Million Bit coins lost Forever, New Study Says".
[12] Po-Wei Chen, Bo-Sian Jiang, Chia-Hui Wang," Block chain-base Payment Collection Super vision System using Pervasive Bit coin Digital Wallet", 2017 IEEE 13th ICW on Wireless and Mobile Computing, Networking and Communications (WiMob)
[13] Wikipedia,"https://en.wikipedia.org/wiki/Proof-of-work_system"