THE BITCOINS

Yashveer Yadav[1], Monika Gogna [2]
[1,2]Research Scholar,Dept. of CSE, NITTTR, Chandigarh, India.
Email: [1]yadav.yashveer@gmail.com

Abstract— The growth of the internet opens a new dimension of market where anyone can buy or sell anything at any time. Now there is no geographical boundary for the businesses. Internet put the whole world into a single platform where there is no concept of physical boundary. The business, take place over the internet is called at E-Commerce. E-Commerce supports all the functional area of buying sailing with payment methods. The payment needs to be transferred from buyer to seller. In the last few years E-Commerce required payment method that is secure and has very less overheads. Bitcoin is gaining popularity as the solution of funds transfer over the internet with very less overheads. Bitcoin is kind of payment method which is adopted in rapid pace in the last few years. In this paper, we discuss BitCoin with its pros and cons.

Index Terms— Bitcoin, Virtual Currency, E-Cash.

I. INTRODUCTION

Bitcoin is the first crypto-currency that has distributed in nature. Bitcoin is called as distributed currency because there is no central governing body for Bitcoin system. This is no central authority in Bitcoin that makes it peer to peer distributed digital currency. The concept of Bitcoin comes into the existence in mid-2008 when a young scientist Santoshi Nakamoto developed a digital network and describes the fundamental processing of the Bitcoin network in her research paper. In the original manifesto, Nakamoto described Bitcoin as providing "a system for electronic transactions without relying on trust" through the use of cryptographic proof [1].Bitcoins are gaining popularity day by day. The Bitcoin value is fluctuating from US $2.95 to approximately US $1200 per Bitcoin. The first Bitcoin was transacted in January 2009 and by April 2015 there are 14051350 Bitcoins are circulated in the Bitcoin network. The one Bitcoin can be divided into up to 8 precision. The smallest unit of a Bitcoin is 0.00000001 BTC and highest of a Bitcoin unit is 1 BTC equal to 1 Bitcoin. The smallest unit is also called as Santoshi to honor the original inventor of Bitcoin system.

To use the Bitcoin one need to create a Bitcoin wallet into his computer system. This wallet does not contain any money or anything but it contains only a regularly updated file that defines all the transaction ever made in the Bitcoin network. Every new user needs to validate all the transaction first to know about the current balance of other users. Sometimes this process takes more the 3 days, but it's necessary to perform the validity check at least once. Whenever a transaction is made between sender and receiver, the sender creates a transaction by using digital signature and a private key. The digital signature is a file that contains information about the sender which is unique over the internet. Private Key is a

mathematical function which is secreted from the outsiders, used for encrypting the message The message and digital signature are hashed together by using private key, then this transaction is broadcast into the Bitcoin network. All users in the Bitcoin network use the public key to validate the transaction and update their copy of the ledger the Wallet. One sender can make number of transactions, but every transaction has different digital signature and hash value.

Bitcoin is a digital currency so it can be easily transferred over the internet from one county to another county without interference of their party. There are only two entities in each transaction (Sender and Receiver) so overheads are almost nothing. There are many countries like Australia, Brazil, Canada, Denmark, France, Germany, Poland and USA who regulated the Bitcoin and consider Bitcoin as E-Cash or hard cash.

Bitcoin has many advantages, but on the other hand it also has many disadvantages or limitations. One needs to take a decision after considering both sides. In the II section we dicusssed the working model of Bitcoin system following by its advantages and disadtantages in sector III and IV. In the V section conclusion of the paper is discussed.

II. Working model of Bitcoin Network

As we have already described that BitCoin is a decentralized Peer to Peer digital currency over the internet. There is no central bank or fractional reserve system controlling the supply of BitCoins. Anonymous users do trading from different cities and countries. This makes security of every transaction, a prime concern of overall network. Every user also should know the changes taking place in each other's account. For the same BitCoin network, users use broadcasting method to update all copies of ledger in the network. We can also explain it with an example like if A wants to send 500 BTC to B so A broadcast a message in the network that A is sending 500 BTC to B. All of the nodes in the network update their copy of ledger with the transaction and forward this message to other nodes. To validate the authenticity of the received transaction BitCoin network uses digital signature.

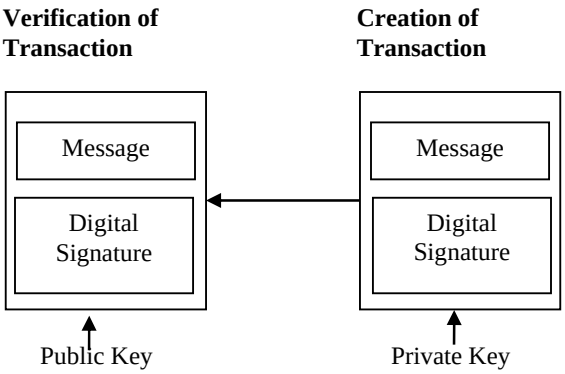


Fig.1. Creation and Verification of BitCoin Transaction.

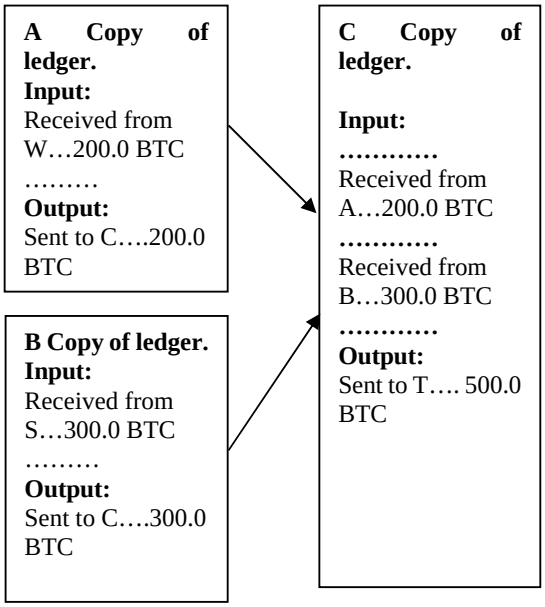
Digital signature is a unique mathematical algorithm for very user in the BitCoin network. Every transaction has its own digital signature and a time stamp that validate the authenticity of the sender. Every time different digital signature is used with different transactions by the same sender. A private key is used to create the digital signature and a public key is used to verify the signature as shown in fig. 1. When a receiver validates the transaction, transaction and its digital signature are checked together. Different transactions of same sender always have different digital signature. The mathematical function like elliptic curve digital signature algorithm is used for generation of digital signature that is totally dependent on the input message. Any change in the message occurs during the transmission makes the digital signature invalid.

To verify the funds that a person has is verified through the previous transaction. BitCoin network does not maintain the balance like banks does. To verify the balance a person has, is just through the links of the previous transactions. These previous transaction are called input transactions.

Fig. 2 states that C has received 200 and 300 BTC from A and B respectively. Every node in the BitCoin network has its entry in their ledger. Whenever C broadcast this message in the network that C wants to send 500.0 BTC to T, each node in the BitCoin network verify their copy that C has received BitCoin from A and B and their total is not more than the sending amount of BitCoin by C. Every node validates this transaction and updates their copy of ledger and pass it to other nodes. Through this process

the complete network update their copy of ledger automatically.

Fig. 2 Transaction Diagram in BitCoin Network.



Whenever a new client is added into the BitCoin network he/she has to validate all of the transactions before start with it. BitCoin validate software's are available to validate and verify the transaction. These software's validate and verify each transaction that have ever made in BitCoin network. Its important to validate all of the transactions because users of BitCoin network are strangers so to build the trust all transactions need to be verified at least once. This process may take more than more the a day but it's very important to know about the balance of the users in the network.

III. Advantages of using BitCoins

Bitcoin is decentralized crypto currency that has its own adtantages. Bitcoins are generated through the process of bit mining so its supply is always limited.Bitcoin system provides many other advantages. The following are the some of the main advantages of using the Bitcoins.

Low inflation risk

Inflation of currency is the biggest problem with all currency's used today in this world. Every year new notes and coins are released by the government to balance the economy or due to the expected physical loss of the currency. This process increases the supply of currency, due to that currency loses its purchasing power at the rate of few percentage every year. In Bitcoin we do not have this kind of problem. There is a finite number of Bitcoin that can be mined. The total number of Bitcoin that can be mine is about 21 million. Only 21 million bitcoins are there so with the time purchasing power of Bitcoin will be increased due to high demand and lack of supply. We cant speed up the mining of bitcoins. Bitcoins are mined with the predictable rate. We have a slowing population growth, which is projected to stop at around 10 billion by approximately 2050 which roughly coincides with the last Bitcoin to be mined. There will be roughly 1 Bitcoins for every 500 people. [2]

Freedom of payment

In Bitcoin we can send or receive money at anytime from anywhere in the world. We do not need to worry about the conversation of currency, without relay on third party, physical boundary, bank charges, secret codes, etc. Bitcoin is the distributed crypto currency which is widely accepted. Bitcoin has the unique value all over the world. Many countries consider Bitcoin as a digital currency. Countries have their own legal and regulatory framework for specially designed for trading in Bitcoins. Companies offer special discount to customers to acquire Bitcoin's. Dell a multinational computer based company offered up to 10% off on certain products for purchases made with Bitcoins. According to BitPay and BitcoinPlus, Bitcoin accepting merchants are increasing from 10k to 90k by the end of year 2015

Secure

In the traditional method of payment seller sales their item on credit and buyer can stop the payment from the bank at any time. Buyer need to use credit, debit or internet banking to transfer the amount which is risky. There are a number of internet frauds are reported in recent time. It has been reported that credit card, debit card even internet banking credentials have been stolen.
On the internet everyone has some kind of hesitation while inputting their card credential information. Above all payment is made using any traditional method sometimes takes up to a week long process to transfer the amount. In other hand Bitcoin is the peer-to-peer network

that gives it power to transfer the money instantly without the help of a third party. Once the transaction is executed no roll back of money is possible. That provides security to the seller as well as to the buyer. With Bitcoins once you have the money you have it and that's that. Buyers cannot in any way take the money back and the seller can safely ship the product or perform the service that the client purchased. From the buyer's perspective the infrastructure for payments and sending money between accounts is potentially going to be simpler and cheaper because it is peer-to-peer rather than done through some intermediary.[2]Buyer does not need to pay any extra charges for the transfer. Bitcoin is comparably simpler, less time consuming, and more secure than the traditional method.

Appreciating Value

Bitcoins are generated by a process is called as mining. The total number of Bitcoin that can be generated is also finite. Bitcoins were initially highly volatile during the first few years of its inception, however, during the last 6 months the currency has stabilized and has been steadily increasing in value on a daily basis[3].Total number of bitcoins that can be mined is 21 million. As Bitcoin's are gaining popularity day by day. So its demand is growing much faster rate than supply. That keeps the values of Bitcoin always high. As the time passes demands of Bitcoin increases and as supply is always constant, so the values of Bitcoin will increase. Investors also considering Bitcoin as a substitute of Gold for their investment need. Bitcoin shows higher return than gold in the last few years.

IV. Issues related to BitCoins

Bitcoin is a new concept to money transfer. it is undeniable that the digital currency also has some of the problem or disadvantages. Some of the biggest problems with the digital currency are described in the following sections.

Double spending

Double spending is the problem when the buyer uses the same Bitcoin for purchasing more than once. Double-spending is the result of successfully spending some money more than once. Bitcoin protects against double spending by verifying each transaction added to the block chain to ensure that the inputs for the transaction had not previously already been spent[4].Bitcoin is the decentralized peer to peer network. Whenever a transaction is created, it broadcast into the network. The members of the network update their copy of the ledger after verify the transaction using public key. Sometimes the transaction takes more time to get reflected to the ledger due to size of network and different topologies being used in the overall network. Due to this buyer gets the time to spend same Bitcoin again to make the payment. The transaction takes time to reflect, to the whole network. This time duration leads to the exposure of fraudulent of double spending.

Identification hiding

In Bitcoin network anonymous user's deals with other anonymous users. They create transactions and these transactions are created and verified by using private and public key concept. There is no physical interaction between the members of the network. Every transaction is publicly logged. In Bitcoin network every user has an internet address. Everyone has the right to check the transaction from address to address. These addresses are totally numbered and does not reveal any information about the sender and receiver. These addresses are normally changed every time whenever user logs in into the Bitcoin network. This provides additional security for the user that an attacker can't attack on the user address because it changes dynamically. In other hand it also hides the identity of the user and makes it difficult to trace a particular person.

Poor mobile platform support

The Bitcoin system works on transaction without the need of third party interference. In today's world most of the apps through which we can make payment charge some amount with each transaction. In Bitcoin network user do not need to pay for any transaction processing. The Sender sends the Bitcoin to receiver directly without additional charges. In this method there is no need to pay for anything to third party, makes it less popular among the banks and big mobile platform providers. The large technological companies do not support Bitcoin system. Apple the multinational mobile phone, computer and laptop manufacturer do not allow users to make payment using Bitcoin via wallet

in its app store. The Google also does not allow user to make payment in the form of Bitcoin for its app store. These larger technology companies do not want to compete with bitcoin. So they do the same thing as restrictive governments and use their power to regulate it out of existence – within their ecosystem, anyway [5]. Bitcoin is the simplest way to make payment. It can be used as an alternative of cards to make payment with the mobile phone and it more secure the card payment system.

Legal issues with Bitcoins

In most of the countries Bitcoin is considered as cash. On Bitcoin network one can receive or make payment in the form of Bitcoin without revealing it's identify. This feature attracts crime. Anyone can buy or sell illegal items and it's very difficult to trace the buyer and seller. Bitcoin network provides the complete protection for the buyer and seller. In Bitcoin network there is no central authority. Bit coin also can be used to save the tax. One can hide its money in the form of Bitcoin. It's very difficult to relate the IP address with the person. Black Money also can be received or send in the form of Bitcoin without any legal restriction. Bitcoin has proven to be a contentious issue for regulators and law enforcers, both of which have targeted the digital currency in an attempt to control its use. Many legal authorities are still struggling to understand the cryptocurrency. [6]

V. Conclusion

Bitcoin is the first decentralized crypto currency. It solves problem of transferring money from one country to another without the concern of third party. It has many advantages but like any other system it also has disadvantages associated with it. A lot of research is still need to be done in this field. We are expecting the regulatory framework in the future that governs the BitCoin system and increase the overall adaptation rate of Bitcoin system.

REFERENCES

[1] S. Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System", April 2015, available at https://bitcoin.org/bitcoin.pdf, 2008.

[2] Blog of Lvan Raszl, "Bitcoin: Benefits and Risks", April 2015 Available at:http://raszl.com /blog/bitcoin-benefits-and-risks.

[3]Bitcoin, "Benefits of Bitcoin", April 2015 Available at: https://bitcoin.co.th/benefits-of-bitcoin/

[4]Wikipedia, "Double-spending", April 2015 Available at https://en.bitcoin.it/wiki/Double-spending.

[5]CoinDesk, "The Five Biggest Threats Facing Bitcoin", April 2015, Available at: http://www.coindesk.com/five-biggest-threats-facing-bitcoin/

[6]CoinDesk, "Is Bitcoin Legal", April 2015, Available at: http://www.coindesk.com/five-biggest-threats-facing-bitcoin/