Bitcoin – A Bottom up Approach from a Common Man's Perspective

Ms. S. Arul Vallarasi,
Guest Faculty in Computer Science,
The Tamil Nadu Dr. Ambedkar Law University,
Chennai.

Abstract

Bitcoin is a digital currency, a form of electronic cash. It is a decentralized crypto currency without a central bank or single administrator that can be sent from person to person on the peer-to-peer Bitcoin network without the need for third parties. Digital transactions are verified by network nodes through cryptography and recorded in a public distributed ledger called a Blockchain. Bitcoin was invented by an unknown person or group of people using the name Satoshi Nakamoto and was released as open-source software in 2009. Business on internet depends almost solely on financial institutions serving as trusted third parties. Financial institutions like bank uses centralized sever which is used to keep all the transactions carried out through the bank. If a hacker outbreaks the transaction of a server, the transaction details could be changed. So is the emergence of the decentralised the electronic payment which is system based on histotrophic proof instead of the faith and allows any two interested parties to transact directly without the requirement of the trusted third party.

Keywords: Bitcoin, Blockchain, Digital Signature, Distributed ledger.

INTRODUCTION

Digital currency is used in video games and mobile apps that currency could be earned and spent with in the application or it could be converted into real money sometimes. Crypto currency is an entirely standalone currency changing the way we perceive real money. Bitcoin is the first digital currency moves world towards new virtual economy. The basic Idea for Bitcoin is formed based on novel paper written by Satoshi Nakamoto, which introduced the term to Bitcoin in 2009. Bitcoin is a peer-to-peer digital currency. It is decentralized, that means there is no central bank or hub. Bitcoins are fully digital, and so there is no physical representation of the money is required. The Bitcoin creation and transfer of money is completely based on cryptography and not trusting on a central authority. Many international companies started accepting Bitcoins.

BITCOIN WALLET

Bitcoin wallet is an installable app where you can store your Bitcoin addresses. One can install the app on their mobile device for everyday use or they can have a wallet only for online payments on their computer. The newly downloaded Bitcoin wallet has the block chain, and so it will have a copy of the entire network. Once the Bitcoin wallet is downloaded, the program generates an address by which it will receive Bitcoins. We can buy bit coins through Bit coin exchanges. The Bitcoin wallet will generate its first Bitcoin address after installation and new addresses can be generated whenever needed. The Bitcoin addresses will be informed to the other person whom we want to transfer Bitcoins. The process is similar to sending an email to a known email ID. Bitcoin address is made for single transaction and can be used only once.

Bitcoin

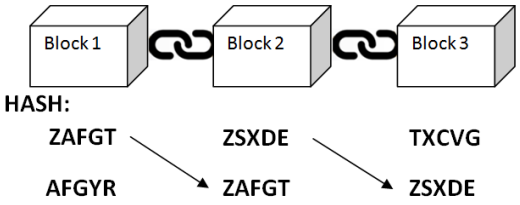
Bitcoin price had zero value at the time of its beginning stage in 2009. Initially there were no exchanges or market, users were mainly cryptography fans who were transferring Bitcoins for hobby. Over a period, market share was growing rapidly. Because of the increasing price of Bitcoin, there is an increasing interest among Bitcoin users, investors and economists. Bitcoins are dividable into smaller units called as satoshis — each satoshi value 0.00000001 Bitcoin.

Double spending

Digital transactions can be made more than one time with same wallet address. This leads the problem of "double spending" the digital currency. The timestamp server is small software that is used to digitally timestamp transactions. The server takes a small part of the transaction data (a hash) and timestamps it. Therefore, if a coin is spent two times, the transactions will have different time stamps and so the second transaction will be automatically discarded by the system. Time stamping also introduced to solve the problem a puzzle that a minor has to solve to validate the transaction. This time stamped hash is then made widely available for everyone in the network.

Block Chain

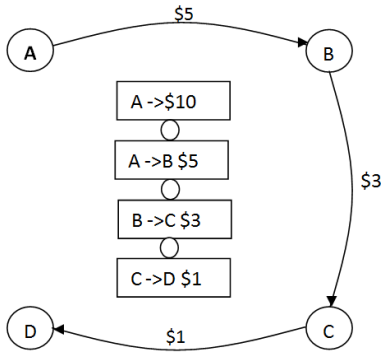
In Block chain each block hold one or more valid transactions that are hashed. Each block has the cryptographic hash of current block as well as the hash of prior block in the block chain, linking the two. The linked blocks form a chain. This iterative progression confirms the integrity of the prior block[5].



The block chain is an open ledger on which the complete Bitcoin network relies. All validated transactions are added into the block chain. The Bitcoin public ledger lets Bitcoin wallets to compute their remaining balance after a transaction. A transaction is a movement of Bitcoin value between two Bitcoin wallets which gets added in the block chain. Bitcoin wallets hold a secret section of data called a private key or seed, which is used to sign transactions, giving mathematical evidence that they have originated from the wallet. The signature also prevents the transaction from being modified by others once it has been validated. All transactions are broadcast to the entire network and typically be validated within 10-20 minutes, through a procedure called mining.

The open ledger

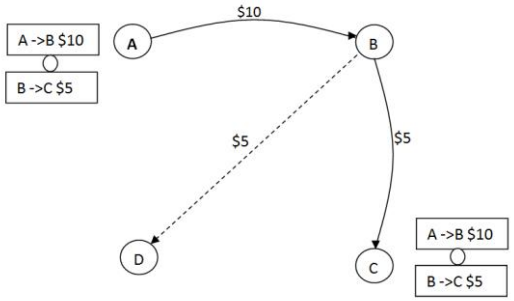
The concept of open ledger can be explained with the network of 4 people A, B, C and D.



Let's say at the starting A has $10. A wants to move $5 to B. So a transaction is added to the open ledger and it is linked to the previous or existing transactions. Now assume that B wants to move $3 to C. So the transaction is added to the open ledger and linked to the previous transaction. Finally C wants to move $1 to D. Again the transaction is added to open ledger with link to previous transaction. Everyone on the ledger can see where the money is transferred and how much money one has in his packet. Everyone can decide whether the transaction is valid or not valid. For example If A now attempts to move $15 to C everyone on the network can immediately find that it is not a valid transaction, as A don't have $15. In this example the ledger is centralized. But block chain ledger is not centralized, it is distributed which means multiple node takes the centralized ledger and distribute it across the network.

The Bitcoin transactions

Bitcoin uses distributed ledgers based on Block chain. A distributed ledger is a replicated, shared, and synchronized digital ledger geographically spread across multiple nodes. Various copies of the ledger are in the network. We need to make sure that all these copies are synchronized, and also the participants of the network see the same copy of the ledger. The block chain is an open ledger which is used in Bitcoin network.



Take the network of 4 people A, B, C and D. A transferred $10 to B, and B transferred $ 5 to C. Now B want to move $5 to D. B is going to publish and broadcast this intended transaction to the network. The timestamp server digitally timestamp the transactions. Everyone in the network will immediately see that B wants to move $5 to D. This is an invalidated transaction. It is not getting yet into the ledger. Miners play a vital role in adding this to a ledger.

The Mining Process

Miners are special nodes which can hold the distributed ledger. Mining is a distributed harmony process that is used to validate pending transactions and add them in the block chain, the distributed ledger. It follows a chronological order in the block chain. When validating transactions, the transactions will be

packed in a block and cryptographic rules will be verified by the network. These rules prevent preceding blocks from being altered. Mining prevents other individual from simply adding new blocks successively to the block chain. So, Individuals or intruders can't control or modify the block chain or roll back their own spends. In this example A&C are miners. Miners are going to compete among themselves who will be the first to take not validated transaction and be able to validate and put it into the ledger.

The first miner that will do that will get financial reward. In order to validate transactions a miner does two things. First one is validate a new transaction the second thing a miner is to do is find a special keyword that will enable this miner to takes the previous transaction and link the new transaction. In order to find these key miners needs to invest computational power and time because the search for the key is Random. The miner will repeatedly guess new keys until it finds the key that matches the random puzzle. The first one that will do that will get financial reward. Ledgers are synchronized across the network. If the miner C was able to solve the puzzle and to take the transaction then it will be added to its ledger. Now it's going to publish the solution to the entire network. Which means transaction is validated and key is added in the particular transaction and the transaction block is added to all the ledgers of the network.

Conclusion

One can have complete control over the value that is owned in Bitcoin transactions. There is no third party that has the value or can limit the access of Bitcoin transactions. The cost to carry out a transaction from and to everywhere on the globe is very little. Amount can be transferred in a few minutes, and the Bitcoin transaction are measured protected after a few hours, as the consecutive blocks are added. Transaction made by the Blockchain can be verified at anytime by anyone on the network, ensuing transparency. Although lots of exchange platforms are coming up, it's still not simple to do business on Bitcoins for goods and services. Bitcoin, similar to other crypto currencies, is extremely unstable: Bitcoins availability in the market is low and so the demand is varying rapidly. Bitcoin value is irregular, varying based on large proceedings or statement in the crypto currencies trade.

References:

1. Satoshi Nakamoto, satoshin@gmx.com, Bitcoin: A Peer-to-Peer Electronic Cash System, www.bitcoin.org

2. https://www.coinbase.com/price/Bitcoin

3. Dr Mark Abell, Simon Fielder and Mumuksha Singh, Bitcoin and International Franchising, in *International Journal of Franchising Law,* Volume 12 – Issue 4 – 2014, Bird & Bird LLP, London, UK.

4. Andreas M. Antonopoulos, *Mastering Bitcoin*, O'Reilly Media Inc., California, 2015

5. Michael Crosby, Nachiappan, Pradan Pattanayak, Sanjeev Verma and Vignesh Kalyanaraman, "Block Chain Technology: Beyond Bitcoin", in *Applied Innovation Review*, Issue No. 2, June 2016