Digital Transactions Through BTC

Rhytham Negi   Paramjeet Singh Prof. Latika Kharb
Jagan Institute of Management Studies
Delhi, India
latika.kharb@jimsindia.org

Abstract - Bitcoin is a digital currency like other digital currency, virtual currency, or electronic money which use to transact the amount (Digital currency) from one person to another. Bitcoin is a peer to peer payment system developed by "Satoshi Nakamoto" in the year 2009. Bitcoin is the decentralized currency, which means there is no middle organization or company keep the log of the transactions. According to the google.com, the current rate 1 BTC is 7,77,671.14 (INR) at time of (September,3,2019 08:27 PM). In the paper, before starting anything about the bitcoin, we need to know that "What the bitcoins are and how they come in existence?". Then we will study how digital transactions can be done through bitcoin.

Keywords- Bitcoin, transactions, digital currency, BTC, money.

I. INTRODUCTION

1.   Where the Bitcoins came from?

Bitcoin was developed by the group of developers called Satoshi Nakamoto. This group of developer also released the first Bitcoin software in which the first units of currency called bitcoins were essentially utilized. It is not commented that Satoshi Nakamoto was a group of people or one single genius.

2.   What are Bitcoin and Bitcoin Blockchain?

Bit coin is a virtual currency and therefore has no physical representation means, we can't feel Bitcoin. The Bit coin Block chain has a sequence of blocks where each block contains information about new Bitcoin transactions.The Bit coin Block chain has a public ledger, where it maintains all the ownership information for any point of time. To use the Bit coin system, we need to download the Bit coin wallet. The bit coin wallet is software that sends and receives the bit coin between two parties. The next step is to exchange of different currency into the Bitcoin unit. The easy and widely used way to exchange the Bitcoin unit with our physical currency, just make an account on one of the many Bit coin exchange and transfer fiat currency to Bit coin unit. Due to the widespread adoption of Bit coin, the pricing on large exchanges is very competitive with relatively small bid-ask spreads. Most exchanges provide order books and many other financial tools that make the trading process transparent.

II. WHAT IS BIT COIN MINING?

Bitcoin mining is one of the ways to earn bitcoins using our computational system power. Every bitcoin transaction consists of some mathematical calculations which need to solve using high computational system power. Those who mine the bitcoins are known as the Bitcoin Miners. The every bitcoin transactions are validated or verified by miners. A miner collects all the pending Bit coin transactions, verifies their legitimacy, and assembles them into what is known as a "block candidate."

Anyone can become a mine bit coin, means bit coin mining is a big task. He/she need a require a respected software which downloads the most recent copy of Bit coin Block chain. Generally, there are few large miners who accepted the new blocks and use highly specialized hardware and access to cheap electricity can still make a profit from mining. The fingerprint of block candidate is obtained by the computing the hash value of a block candidate, using the hashing function dSHA256.

For example, we will look at the hash value for the text, "jagan institute of management studies." The fingerprint text, which was calculated using the hash function dSHA256, is:

4896ffa3ead833b8c6a5b468dd679915bfb4125c5b6c5b969d6b5caf2b646ccb

Now notice the small change in the original text to "Jagan institute of management studies." It will cause an unpredictable change of the fingerprint, which can be seen from the corresponding new hash value:

a4a0f399b42b0dc27dc5f0cd2a0254d0800d15f78f82e6e65951b7cc23b9523d

According to the above example, the data file's hash value cannot be prognosticated. It means we can't able to determine the next hash value after the change fractions of things in data.

Every miner continuously tried out to find the hash value that satisfied the condition in block candidate, that the hashed value must be a certain threshold value means t must display several zeroes at the beginning of the finger print.

An example of a fingerprint of a block that was added to the Bitcoin Blockchain in 2010 is given in the following example:

Block #69785 (July 23rd, 2010, 12:09:36 CET)
0000000000
1djfhghkdhgkdhjlfj13235m65mk6555h78ffjfhnjaf6665656
gj

In the bit coin block chain, a data field contains an arbitrary value called nonce. The miner modifies this random value/data in order to get a new desire finger print. These modifications do not affect the set of included transactions. Just as with our example, every modification results in a new hash value.

III. HOW BIT COIN TRANSACTION WORKS?

The transaction system in the bit coin is similarly as the transaction through any payment app like Pay tm. Pay tm is the most popular and convenient payment system in India. The seller shows his/her payment link (QR Code) to the buyer, scan or accept the payment request and send the desired amount of BTC (Bit coin). A transaction in bit coin is a transfer of value between Bit coin wallets that gets included in the block chain. Each Bit coin wallets has a secret piece of data called a private key or seed, which is used to sign transactions, providing a mathematical proof of work (confirmation of transaction) that they have come from the owner of the wallet. The signature also prevents the transaction from being changed by anybody once it has been issued. All transactions are broadcast to the network and usually begin to be confirmed within 10-20 minutes, through a process called mining.

IV. ADVANTAGES OF BIT COIN

1. Decreases The Risks Of Fraud For Consumer
Buyers can complete their transaction without giving their sensitive and confidential information (like debit or credit card details) to the seller. Thus they provide an essential amount of invisibility that most of the credit card fails to deliver. Bit coin act as a digital currency that hackers cannot decrypt in any possible way because bitcoin makes use of cryptographic hash function known as SHA256 provides security by encrypting the data. At the same time, your identity was also obscured for safety. It helps a lot in preventing data breaches.

2. International Payment Becomes Easy For Small Business

Small online business sellers and retailers don't often sell their product or services internationally because of the high cross border transaction fees. , Bitcoins, being global, relives this pressure once and for all, thereby making payments cheaper, safer, faster, and more comfortable. Foreign currency exchange rates and cost will be minimized.

3. Decentralized Emission
The entire process of a bitcoin transaction is peer to peer. No one can freeze, tax, or claim your coins. They cannot be stolen and cannot be seized by the government in no possible circumstances.

4. No paperwork
Anyone, from any part of the globe, of any age can buy and receive bit coins within minutes. There is no ID card, pan card or passport or proof of bank is required to open an account. All you need to do is to make an account or sign up for a Bit coin Wallet and start purchasing and selling bit coins.

5. Lower transaction fees and Anonymity
Compared to other digital payment methods, such as credit cards and PayPal, Bitcoin comes with lower transaction fees. Though such fees are changeable, it's rare for a Bitcoin transaction to cost more than 1% of its value. Compare that to 2% to 3% for most other digital payments. Bitcoin has built-in privacy protections feature which allows users to completely separate their Bitcoin accounts from their public personas if they so choose. While it's possible to track Bitcoin flows between users, it's very difficult to figure out the user, who those users really are.

V. DISADVANTAGES OF BITCOIN

1. Bitcoins are not widely accepted
Like in India the "The Reserve Bank of India (RBI) "announces a ban on purchasing and sale of cryptocurrency like Bitcoins. Therefore bitcoins are still only be accepted by a small group of online merchants and vendors. To entirely rely on Bitcoins as a currency is quite tricky.

2. No Valuation Guarantee
Since there is no authority governing Bitcoins and suppose If a large group of merchants decides to "flood" Bitcoins and leave the system, its valuation will decrease significantly, no one can guarantee its minimum cost. So the users who have spent a large amount of wealth invested in Bitcoins would be in trouble. The decentralized nature of bitcoin has both merits and demerits.

3. Fluctuation in bitcoin value
Based on demand the value of the bitcoin fluctuates continuously. This constant fluctuation will cause Bitcoin-accepting sites to continually updating prices. Suppose when a user wants a refund for his product, causing a lot of confusion like should the new amount be sent?. There are still some essential scenarios that the Bitcoin community still has no consensus over.

4. Black Market Activity May Damage Reputation and Usefulness

Due to the security feature of the Bitcoin, it attracts the criminal and the Grey market participants. Obviously, dark web marketplaces like Silk Road and Sheep expose rank-and-file users to fraud and the threat of criminal prosecution. FBI's announcement that it would treat Bitcoin and other virtual currencies as "legitimate financial services," Bit coin's value spiked by a similar amount.

VI. CONCLUSION

In the paper, we discussed about all aspects of digital transaction of future i.e. Bitcoin. A number of people are not aware about the concepts and how it works. The paper is an initiative to enlighten young scholars towards basics of Bitcoin. In future, bitcoin will take over the digital transaction world and all of us will become habitual to it's benefits and cons.

REFERENCES

[1]. https://en.wikipedia.org/wiki/Bitcoin
[2]. Dr. Latika Kharb et al, International Journal of Computer Science and Mobile Applications, Vol.5 Issue. 11, November- 2017, pg. 1-8
[3]. Kharb L, Automated Deployment of Software Containers Using Dockers International Journal of Emerging Technologies in Engineering Research (IJETER) Volume 4, Issue 10, October (2016)
[4]. Michael PAETAU, Bitcoin: Network Based Currency and Its Self-Organizing Emergency, 823.2