Bit Coin: Future Currency

Vishal Batra
[1]M.Tech Student [2]Professor
[1,2]Department of Computer Science & Engineering
[1,2]GNIOT, Greater Noida (UP), India

Abstract— Now a days, online funds transfer becomes so common. Everyone is using this facility and Indian Economy is moving towards cashless economy. Even a street hawker is using online modes for accepting payments from his clients. But all these transactions are governed by Reserve Bank of India to avoid any kind of fraud. These online modes are feasible within a country. What happens, if client has to make payments outside the country? Then person has to go to bank and fill some forms and get the transaction done. These cross border transactions are governed by RBI and is not easy as normal transactions. Bit coins provide for making payments online and these payments are hassle free. Bit coins are facilitating peer to peer transactions without passing through a financial institution. Bit coins are not authorized by any financial institution in India as RBI does not hold any responsibility for Bit Coins as a legal tender for making payments. Bit coins are basically are the virtual currencies which are widely used over the internet for making payments.

Key words: Bit Coin, Crypto Currency

I. INTRODUCTION

Bit coins are the first crypto currency of the world which is used as electronic cash transferred peer to peer without intervention of a financial institution. It is a digital currency system works without single administrator. Bit coins are used as the latest mode of the payment over the internet to avoid hassle implicated by the central bank of any country to regulate the flow foreign currency in the country and avoid the money laundering.

Bit coin is open-source and its design is public so that no one can own or control. Bit coin are becoming so popular over the internet because it reduces the transaction cost across the border. Bit coins transactions are much faster as compared to normal cross border transactions. Normally, every country has its own currency and currency conversions are happened while in a cross border payments. Currency conversions incurs transaction cost and increases the overall cost for any project. Since bit coin are public and open source, number of bit coins are kept limited. The algorithm of bit coin is designed in such a manner so that number of bit coins are 21 million. This is the USP of the bit coins.

II. WORKING

Bit coins are transferred to the bit coin wallet. Each bit coin wallet have a unique address. Bit coins payments are simple as sending the email. As bit coins are not managed by any financial institution, all bit coins transactions database is maintained in block chain. In simple words, block chain is a public ledger that records all bit coin transactions. It is implemented as a chain of blocks, each block containing a hash of the previous block up of the genesis block of the chain. Since transferring of bit coins varies across platforms but common steps are described below:

1) Open bit coin wallet and select "Trade|Send Bitcoin".
2) Type the destination address for recipient's wallet.
3) Give a unique label to transaction for the tracking.
4) Type the value of transferring amount in "BTC" box.
5) Review the transaction and click "Send" to complete the transaction.
6) On completion, the transfer is irreversible.

III. TECHNICAL PROCESS

The technical process involves the following steps:

1) Someone request a transaction. Then this transaction is broadcasted over a P2P network of computers known as nodes.
2) The network of nodes validates this transaction and user's status using pre-defined algorithms.
3) After successful validation, this transaction involve bit coin, contracts and other records.
4) Once verified, the transaction can create a block of data for Block Chain.

Mining is a record keeping service carried out by using computer processing power. Miners keep the block chain consist, complete and unaltered by repeatedly grouping newly broadcast transactions into block. Each block uses SHA-256 cryptographic hash.

IV. BLOCK HASHING ALGORITHM

The service string in bit coin is encoded in following parts

- Block Header Data Structure.
- Version Field.
- Hash of the Previous Block.
- Root Hash of Merkle Tree.
- Current Time.

Nonce in extraNonce field is the leftmost leaf of the merkle tree. Bit coin uses this field as part of the coin base transaction. The counter part in the extraNonce field gets incremented after each transaction to avoid repeating work. During mining of bit coin, the hash code algorithm continuously hashing the block header while incrementing the counter and extraNonce fields.

Field	Size (in Bytes)
Version	4
hashPrevBlock	32
hashMerkleRoot	32
Time	4
Bits	4
Nonce	4

V. ADVANTAGES

A. Hassle Free

- No border limitations. Transfer bit coins as simple as sending an email.
- Decentralized authority.

B. Security

- All transactions are encrypted using SHA-256 cryptographic hash.
- No personal information is shared during transfer.
- Bit coins are virtual currency, so it can be easily backed up.

C. Transparency in Information

- All finalized transactions are available with the block chain but personal information is hidden.
- Although Bit Coin is virtual currency, it can't be tempered, reproduce or manipulated by anyone.

D. Very Low Fees

- Most of bit coins transactions are free.
- Conversion of across country currency is very costly as compared with bit coin conversion.
- Peer 2 Peer payments are very cost effective without intervention of a reputed financial institution.

VI. DISADVANTAGES

A. Fraud:

- Since it is a deregulated currency, in case of a fraud, culprit might be in another country. So, it is very difficult for local law agencies to deal with culprits due to some international issues.
- Terrorist can use bit coins for terror funding and do some anti-social activities.

B. Risk and legal issues

- Bit coins are neutral i.e. bit coins are not legal or illegal in some countries such as Switzerland, USA etc. But in some countries, bit coins are illegal in Vietnam.
- Since the bit coins are limited in number, but its demand in market is quite volatile.

VII. FUTURE WORK

The algorithm of the bit coins is designed in such a way that the number of bit coins will not go beyond 21 million. But according to unofficial sources, there are around 17 million bit coins are in circulation across the globe. If bit coins has to sustain in the future, the algorithm of bit coins should be changed and the number of bit coins should be increased. People are looking for some options of payment which can be accepted worldwide irrespective of the country.

Since bit coins are not managed any financial institution across the globe, it will be regulated by any reputed financial institution such as World Bank or IMF to avoid the misuse of the bit coins.

REFERENCES

[1] https://www.cryptoground.com/a/list-of-countries-where-bitcoin-is-legal
[2] https://coinreport.net/coin-101/advantages-and-disadvantages-of-bitcoin/
[3] https://en.wikipedia.org/wiki/Bitcoin
[4] https://bitcoin.org/en/
[5] https://bitcoin.org/bitcoin.pdf

