Bitcoin – A Cryptocurrency Protocol

Sloni
Assistant Professor,
Department Of Economics,
Gopichand Arya Mahila College, Abohar (Punjab)

Abstract-

Bitcoin is a currency among many cryptocurrencies. There are approximately 1324 crypto currencies registered under coinmarketcap.com. It is an electronic cash system that allow online payments to be sent directly from one party to another. Bitcoin is just like money in wallet. Bitcoins are stored in virtual wallets which keeps a record of every single transaction and allows to send and receive bitcoins and these all transaction are verified by members and the record is permanently stored by them that means it takes few minutes to verify the transaction. In easy words bitcoin is a virtual currency that can be mined with computers. There are 21.9 million bitcoins maximum of which already been found. All bitcoin transactions are publically and anonymously stored.

Introduction

Bitcoin is a peer-to-peer payments system introduced as open source software in 2009 by pseudonymous developer Santoshi Nakamoto. Bitcoin uses cryptography to control the creation and transfer of money. **Bitcoin can be divided upto 8 decimal places and 0.000000001 is the smallest denomination of bitcoin called 'santoshi'**

Symbol ₿

Ticker symbol - BTC, XBT
1 Bitcoin = 554858.87 Indian rupees approximately although it fluctuates timely.
The total market value of bitcoin is approximately 189 billion $. Its total market capitalization is increasing over time. Bitcoin is the most popular cryptocurrency through which we can exchange money without any bank or thirdparty or credit card issues. Money can be transferred from one country to another with very small amount of fees which is not possible in banks as E-commerce exclusively depends on financial institution to serve third parties for the process of electronic payments, but this system allow online payments to be sent directly from one party to another without going through a financial institution.

Bitcoin is like a computer code. Everytime when you pay money to someone, then in a very secured way the signature of that person are taken which no one can deny. It means the money that you have paid is recorded in a ledger in a legitimate way. Prices of bitcoins are rising now-a-days. This is because of the demand and supply situations. As more people are buying bitcoins, their demand is increasing and so is their value.

Bitcoins is like a virtual online wallet. This is a safe account set at third party website whose guarantee is not under any central bank and no interest payments are paid in bitcoin deals. Its only because of demand that its market value is increasing. Just like during diwali days gold prices like because of increase in its demand owing to limited supply.

Bitcoin is not to be compared with any currency as it is not registered under any state government Indian government doesnot consider Bitcoin as legal tender. It means it doesnot hold any value in RBI prospective. Though, Bitcoin is a legal exchange in trade in many currency but a demand based currency.

Methodology

The Methodology section of the paper is spilt into some sections that define the concept of Bitcoin in a very simple language. There are

(a) Transactions
(b) Timestamp server
(c) Proof-of-work
(d) Network
(e) Incentive
(f) Combining and splitting values
(g) Incentive
(h) Combining and splitting values
(i) Privacy

(a) Transaction- Bitcoin is a chain of digital signature which can be passed form one person to another using an electronic signature. This means you sign for the bitcoin package that you have received and then forward it. Each time the package is forwarded the history of past locations is mentioned on it. Bitcoin mining is the process by which the transactions are verified and added to the public ledger, known as block chain and also the means through which bitcoin are released. This history creates the 'Block Chain' which is a ledger of bitcoins transaction history and are processed in the sequence of their respective time stamp and so there will not be any problem of double spending.

Each and every transaction in Bitcoin system is publically announced and so thirdparty is not needed in this system and hence this system is decentralized. But to avoid the problem of double specding and multiple blockchains the computer nodes timeline and the transactions must be processed as per the timeline.

(b) Timestamp Server- This is a software which digitally timestamp the data and then it is made publically made available for everyone to see.

(c) Proof-of-work – Proof-of-work is to safeguard the Bitcoin system. Here, a mathematical problem is to be solved by the computer and its answer is presented to show that it has done the work. As a computer has to do work to solve a problem, people cannot spam the system with multiple requests. Blockchain increase in length with each correct answer generated. The transactions created through this cannot be reversed as it involves to do work on the whole chain to undo a single block.

(d) Network – New Transactions are publically announced to all nodes>> each node puts all new transactions into a block >> for its own block >> when a lucky node solves the puzzle for its block, it inform all other nodes>> nodes accept the solved block, if all the transactions are valid and there are no issues of double spending>> nodes move onto next block in chain>> This process them repeats in a loop. The longest chain is considered to be correct by nodes.

(e) Incentive- The first transaction in a block create a new coin which is owned by the person who created that particular block.

Old transactions can be discarded after some amount of time to save space in the disk but the trace of transactions will remain.

(f) **Combining and Splitting Value-** The value of Bitcoins can be split or recombined as per our needs. This means that large coins can be split into multiple parts before being passed on, or small coins to be combined to make larger amount.

(g) **Privacy-** Although transactions are publically declared but the identities of the sender and receiver can not be determined by the public. Its only like money is moving from point P to S and no Identifiable Information's is openly distributed

Conclusion

Bitcoin is an electronic payment system based on crypto currency introduced with each other without any intermediary party. And these cryptographic transactions will be computationally impossible to reverse, and hence users will be protected from fraud. A peer to peer electronic cash system will be created in which a set of interconnected computers will work together and no problem of double spending will be left. As a decentralized currency, bitcoin is not controlled by anyone. It is open so that anyone can benefit form it.

References

1. Bitcoin white Peper explained…
2. http://steemit.com
3. http://bitcoin.org
4. Bitcoin: A peer-to-peer Electronic Cash System.
5. https://www.investopedia.com
6. Investing in Bitcoin, ethereum and Altcoins could make you a millionaire.