International Journal of Latest Engineering and Management Research (IJLEMR)
ISSN: 2455-4847
www.ijlemr.com || Volume 04 - Issue 02 || February 2019 || PP. 79-82

Cryptocurrency: A Brief Discusion in Prospect to Bitcoin

Madhukar Goyal
PHD, FCA,CS (Professional Programme) M.COM, LLB, CCNPO (ICAI),UGC –NET(Commerce)
drmadhukargoyal@gmail.Com
"Sansmriti", 12-A/III, Shree Ganeshpuram,
P.O. - RKU, Bareilly, Uttar Pradesh

Abstract: Cryptocurrency use cryptographic protocols, or extremely complex code systems that encrypt sensitive data transfers, to secure their units of exchange. Cryptocurrency developers build these protocols on advanced mathematics and computer engineering principles that render them virtually impossible to break, and thus to duplicate or counterfeit the protected currencies. These protocols also mask the identities of cryptocurrency users, making transactions and fund flows difficult to attribute to specific individuals or groups.

Introduction

This currency is in a Digital form and in it, an encryption technique is used to regulate the generation of currency units & after generation verification of funds transfer, operating independently towards a lead bank. In simpler words, Crypto currencies are internet based currencies which have no physical existence and whose supply and exchange are not governed by any recognised authority. These crypto currencies are built on a set of cryptographic protocols based on advanced mathematical calculations and complex computer engineering principles which are completely encrypted and are transacted on peer to peer basis, which makes it more secure than any other currencies existing today. At present, there are about 667 crypto currencies being mined and exchanged all around the internet. History and Evolution of Crytocurrencies In late 1980's, a company named Digicash founded by Robert chaum, the first of kind to introduce cryptocurrency, unlike modern cryptcurrencies, Digicash was not decentralised as the company had the monopolistic control over the circulation and exchange of currency. Later in 1990's the company went bankrupt due to huge government intervention. Later in 1980's to 2000, E-gold were the most notable virtual currency based upon US. E-gold were the company who bought physical gold and added that to individual persons e-gold warehouse accounts. The users will also be able to trade their e-gold with other users. In mid 2000's e-gold had millions of active accounts and gradually the company vanished as it was found more vulnerable to hackers. The first successful crypto currencies originated in the year 2009 which was developed by a pseudonymous developer Satoshi Nakamoto, who developed the crypto currencies called 'Bit coins'. Bitcoins were designed as an open-source program to ensure transparency and create reliability among the users and hence it resulted in creation of further more crypto currencies or alt coins as otherwise called as they are altered form of bitcoins.

In the simplest terms, Bitcoin is a digital asset and a payment system which uses peer-to-peer technology to operate with no central authority or banks. Geographical boundaries don't limit it, and unlike paper currency, managing transactions and the issuing of Bitcoins is carried out collectively by the network, using complex and cryptographic code used in its design.

The most striking feature about Bitcoin is that it makes use of the Blockchain technology. A blockchain is an incorruptible digital ledger that can be programmed to record details of financial and non-financial transactions. The data is stored in a distributed database and is immutable and permanent. The whole ledger is entirely transparent, and anyone connected to the network can view the transactions.

Other Crypto Currencies:

1. Ethereum – Ethereum is the second most famous name in the virtual currency market. It somewhat similar to the concept of bitcoins however it possesses some additional attributes. It is purely a blockchain based platform. What makes it special is the Ethereum Virtual Machine. The blockcain in ethereum is used not to store the data of the transaction but to make sure smooth run of a decentralized application.
2. Ripple – Ripple is more in the nature of a payment protocol created and developed by a company named Ripple, which is based on the concept of Real time Gross Settlement. It was initially released in the year 2012.
3. NEM – Similar to bitcoin, NEM is also a peer-to-peer blockchain platform launched in the year 2015. It uses the unique Proof-of-Importance algorithm, a way to validate transactions and achieve the distributed concensus.

4. Litecoin – Initially introduced in the year 2011, litecoin is mostly identical to bitcoin. What makes it stand out is the use of Segregated Witness and the Lightning Network. Some other cryptocurrencies are bbqcoins and dogecoins which have not gained much significance due to their technical shortcomings and inability to stand out.

Blockchain Technology

Most cryptocurrencies are based on blockchain technology. In simple terms, it is a system to transfer and store data or information that is generated while transacting in a crypto currency.

ABlockchain may be described as a tamper-evident ledger shared within a network of entities, where the ledger holds a record of transactions between the entities. To achieve tamper-evidence in the ledger, Blockchain exploits cryptographic hash functions."

Blockchain technology is at the heart of how crypto currencies work. It helps to evade any possibility of fraud and makes any kind of tampering infeasible for the users. It is a support system for the encrypted currency, whereby the transactions are recorded and stored on the ledger. So even if the users are anonymous, it still becomes difficult for anyone to possibly change the data without involving other members on the network.

Each bitcoin consists of unique computer codes. Each coin can be split into fractions and those fractions are also each identified by unique codes. The smallest fraction is named the "Satoshi" in honour of the creator. Each coin and its owner can be identified by using a combination of private-public keys. The public key, which everybody knows, identifies the coin. But only the owners know the private key and can thus identify themselves. To put it another way, the owners are the owners because they have the private key. To use a physical analogy, think of a banknote inside a locked, transparent case. The number of the note can be read by all. But only the owner can unlock the case. If you can unlock the case, you own the money. Yes, this lays the crypto system open to hacks and if you forget the private key, the coin is lost, forever. Coins are held in digital wallets. Many programmers have created free digital wallets, which can just be downloaded by anybody, anonymously. Anyone can create their own digital wallet, or even just write down their private key on a piece of paper. Coins are generated by solving complicated mathematical problems that require vast amounts of computerised number-crunching. This is called mining. Anybody can use a personal computer to solve these problems in order to own the newly-minted coins. (Warning: This will take a lot of computer time and it's a very intensive process). "Mining" syndicates have been founded to pool computer resources dedicated to this task. The money supply is exactly regulated by that mathematical system of generation. It cannot be tampered with. Every transaction with every coin from the instant of generation is recorded in an open ledger called the blockchain. That ledger is constantly updated. It can be downloaded and checked by anybody. When a new transaction is made, the blockchain is used to check that:

1) The coin exists
   and
2) The coin is not being used for two transactions simultaneously.

The coin-owner transfers ownership to somebody who uses a different private key to "lock" it. A transaction is accepted as valid only when a large majority of people have checked the blockchain and agree that the transaction is valid. There is no RBI or Federal Reserve guaranteeing the validity of the coin; the bank is replaced by a peer-to-peer network. This verification can be interfered with only by collusion between a large number of network members. The network runs into millions of people but it has happened. The blockchain is an incredible concept and it's now being used for multiple other purposes. But the original blockchain led to slow verifications – transactions could take days. Some (actually the majority) of bitcoin users have agreed to replace the blockchain with a new blockchain which has more capacity and lends itself to faster verification. So there are now two types of bitcoin – bitcoin and bitcoin cash. A given coin can be traded/ transacted on either. Many other crypto-currencies have adopted various elements of bitcoin and tweaked those to try and create more secure and convenient protocols.

Bitcoin Exchanges in India and Services Provided By It

Amongst the plethora of services (including core and non-core services and including those driven by profit or not) provided by different exchanges in India, following are the services that are common in the market:

1. Storing bitcoin in a bitcoin wallet after deposit/receipt of the same in the wallet.
2. Exchange of bitcoin with other currency like a fiat currency.
3. A Merchant gateway service used to pay to merchants in bitcoins and acceptance by them thereon.
4. Mobile application providing ease of accessing bitcoin wallets.
5. Sending bitcoins stored in the wallet to another wallet/withdrawing.

Legal and Taxation Issues & Regulatory Status in India

The Reserve Bank of India has neither declared bitcoins as illegal in India nor has it accepted bitcoins as a currency. The RBI has only stated the risks that are associated with virtual currencies and cautioned that people dealing in it should do so at their own risk.

Legal Status of Bitcoins Currency

Currency is generally defined as tokens used as money in a country. In addition to metal coins and paper bank notes, money orders, traveller's checks, it also includes electronic money or digital cash.
To fit in this definition, which is not exhaustive,

- Either bitcoin has to be physical and movable, and fungible. It is movable and fungible but not physical.
- Electronic money or digital cash may include bitcoin but then it needs a legal backing from an authorized entity, which is not the case in India as of now.
  "Currency" includes all currency notes, postal notes, postal orders, money orders, cheques, drafts, travellers cheques, letters of credit, bills of exchange and promissory notes, credit cards or such other similar instruments, as may be notified by the Reserve Bank, refer to section 2(h) of FEMA Act, 1999 • As is evident from the above definition, bitcoin doesn't fit in any of the illustrative names, however if RBI wants, it can certainly notify it to be included in the above definition.
- RBI hasn't notified bitcoin as legal tender in India and therefore it couldn't be termed as real currency for the time being.

Bitcoin and Some Important Facts

Bypassing Currency Controls

Bitcoin is of course, the most well-known and oldest of these virtual currencies. And, bitcoin is extensively used to bypass currency controls, not just in China, but in Greece and other places as well. Bitcoin has become popular in India as well. Volumes of rupee trading in bitcoin have exploded this year – over 2,500 Indians trade bitcoins daily.

Government Recognition

Most governments don't recognise bitcoin as currency. In fact, most governments don't even classify these as anything at all. These can be passed off as computer code (which is the literal truth) or as digital curios(ities). Japan is one of the few exceptions – the Bank of Japan imposes stringent restrictions on use but Japan does recognise bitcoin as legal tender. South Korea also has rules for bitcoin-denominated payments and transfers.

Online Transactions in Bitcoin and Fema

If one transacts into export/import transactions in bitcoin, the provisions of FEMA will get attracted. Transactions in FEMA are categorized as 'Current account transaction' and 'Capital account transaction'. First we analyze current account transactions defined under FEMA (Section 2(j)). A "current account transaction" means "a transaction other than a capital account transaction and without prejudice to the generality of the foregoing such transaction includes,—

(i) payments related with foreign trade,services, other current business, credit facilities and short-term banking and in ordinary course of business,
(ii) Due payments as interest on loans and also net income from investments,
(iii) remittances for living expenses of parents, spouse and children residing abroad, and
(iv) expenses in connection with foreign travel, education and medical care of parents, spouse and children;"

Highlighting 'a transaction other than a capital account transaction' from the above definition, capital account transaction (Section 2(e)) means "a transaction which alters the assets or liabilities, including contingent liabilities, outside India of persons resident in India or assets or liabilities in India of persons resident outside India, and includes transactions referred to in sub-section (3) of section 6; Section 6(3) of FEMA lists out the following:

(a) transfer or issue of any foreign security by a person resident in India;
(b) transfer or issue of any security by a person resident outside India;
(c) transfer or issue of any security or foreign security by any branch, office or agency in India of a person resident outside India;
(d) any borrowing or lending in foreign exchange in whatever form or by whatever name called;
(e) any borrowing or lending in rupees in whatever form or by whatever name called between a person resident in India and a person resident outside India;

(f) deposits between persons resident in India and persons resident outside India;
(g) export, import or holding of currency or currency notes;
(h) transfer of immovable property outside India, other than a lease exceeding five years, by a person resident in India;

acquisition or transfer of immovable property in India, other than a lease not exceeding five years, by a person resident outside India;
(j) giving of a guarantee or surety in respect of any debt, obligation or other liability incurred—
(i) by a person resident in India and owed to a person resident outside India; or
(ii) by a person resident outside India."

Risks Associated with Bitcoins

- RBI through its press release dated 24th December, 2013 has warned the public about the negative attributes of bitcoins and its usage. It specifically pointed out, that since they are stored digitally, they are exposed to risks such as hacking, attacks, compromises etc.
- Bitcoins are not backed and/or regulated by a centralized agency till date, making them less reliable.
- There is no forum, where a user can possibly reach out for any help or grievance, as a result of which Indian consumers are being exposed to transactional and informative risks.
- Another issue pertains to awareness. Lot of consumers has little or no information regarding risks associated with bitcoins lending them into unwanted trouble under regulations such as anti-money laundering.
- One of the very important attributes of bitcoins is its volatility. Steep changes every second are expected, making investors prone to zero-worth risks.
- Several incidences have occurred stating that bitcoins have been used for illicit and illegal activities around the globe. Bitcoins have also been used in Ponzi schemes, resulting in huge loss of money for several investors.

Conclusion

Every new currency has to face an uphill battle legally and technically. The value of Bitcoins will depend upon the ever-fluctuating market value, if the system gets widely adopted. Bitcoins need to be accepted as a placeholder by the merchants for goods and services, just like any other currency. This has been a challenge to other digital cash options, so it is hard to say if Bitcoin will be ready to face these barriers. In views of many, there has always been a need of a decentralized currency system and Bitcoin surely is a huge step towards censorship-resistant digital currency.