

CRYPTOCURRENCY: BITCOINS AND ALTCOINS

Dr. Mamta Muthal

G. H. Rasoni Institute of Information Technology
Rasoni Group of Institutions, Nagpur, India.

Abstract : 21st century is the century of technological revolution. Technology is writing a new chapter in invention everyday. And its impact is felt in all areas of existence. One such invention of technology revolution is Cryptocurrency, a computer code that has taken the financial world by storm. Is it ‘ the future dawn of Trade & Finance’ or ‘Is it a cheap gamble’? The paper attempts to introduce the new technological phenomenon called Cryptocurrency—Bitcoins and Altcoins.

Keywords : Cryptocurrency, Bitcoins, Altcoins, Peer to Peer, Mining.

Cryptocurrency: Bitcoins and Altcoins

1.The Era of Digitization and Globalization:

Twenty first century is the century of digitization. Computer technology, internet, mobile computing have changed the means, speed and the manner in which we communicate. Digitization, an essential instrument of globalization, has made possible for people connect across the globe, rise over the physical, geographical and cultural barriers and act as consumers in one common market place.

Digitization quite simply means the transacting of information in an electronic format. The speed with which the information is transmitted, its dissemination and the transparency it entails make digitization a must way of communication today.

With digitization democratization of information has taken place. Digitization has in a sense empowered a digitally literate person irrespective of his socio-economic status or geographic location. Digitization has ushered in an easy gateway to articulate one’s opinion on the events happening around or to participate in commercial transaction. The freedom to express one’s views and the ease to connect with the world beyond, have changed the narrative and substance of public discourse.

Every business and personal information field is digitally touched today. The banking & financial sector is one of the areas where the power of digital impact is most visible. Today people are able to make payments virtually. One doesn’t need to go to a bank, stand in a queue to transact the business; one can transfer funds online. The use of plastic to make payments, digitized wallets is another game changer.

In a globalized world, no country can operate in isolation. Globalization and digitalization have converted the cyber space as one equitable platform where connecting for all areas of existence possible; monetary transaction and trade being the front -runner.

II. Cryptocurrency : Historical Perspective.

Buying and selling of commodities through physical tokens such as coins, gold, money has changed with digitization. The direct transaction between seller and buyer has given way to third party transaction in e-commerce where the seller and buyer are not present. Any financial transaction in digital mode necessitates an intermediary guarantor such as the bank or digital wallet like PayPal that assures payment for the commodity purchased. For overseas monetary transaction such as remittance, there is a necessity of a mediating bank that regulates the fiscal transactions between buyers or sellers from two different countries. Digital transaction, though fast paced does not give access to both parties to transact simultaneously; and there is a price to pay for every transaction made.

Enter Cryptocurrency, an electronic money, an entity created by computer programming. Cryptocurrency is a virtual system of payment where no third party is involved. Both seller and buyer trade directly on what is called the 'National Ledger' or 'Public Ledger' without having to go through a third party and the transaction takes place through 'Block Chain' technology.

Crypto-currency, the encrypted currency or token has a value of its own. Like Gold or Silver coins or shares it can be stored for the value. It could also become a medium for buying commodities. One such token, Bitcoins, the first crypto-currency, was came into existence the year 2008. A brainchild of an unknown person or group of people under the assumed name Satoshi Nakamoto, Bitcoins was released as open-source software, a computer programme in 2009. The currencies that followed Bitcoins are called Altcoins. There are as many as 1643 crypto coins enjoying substantial market share in the financial market. [1]

III. Understanding the Cryptocurrency Vocabulary : "Block Chain Technology", " National Ledger" and " Peer to Peer transaction", "Nodes" :

Let us understand the crypto-currency vocabulary:

- i) Block Chain Technology: It is an electronic spreadsheet that keeps getting modified with every virtual transaction. Block chain is known as the ' National or Distributed or Public ledger' which records the information on every transaction and stores it lastingly in blocks of information that can be accessed by miners simultaneously.
- ii) The information on block chain can be viewed by all who transact known as 'miners'. Sellers and buyers are the miners who participate in the trade.
- iii) Nodes are the servers on the network that log in to participate in the activity.
- iv) Peer to peer is the interested party's [seller and buyer] direct transaction without any third party's intervention.

IV. Step By Step Crypto-currency Transaction :

- i). The transaction begins with the change of ownership of currency from seller to buyer.
- ii). The Recording of the transactions is done by capturing digital signatures & the

timestamp, so that the transaction date is recorded generating a new code.

- iii). The Nodes (computers connected to and running the crypto-currency network software) receive the new code which is broadcasted subsequently.
- iv). The transaction is effected when the majority of nodes agree with the transaction. The consensual agreement solidifies the integrity of the system. It confirms the legitimacy of the transaction. A lack of consensus may mean double-spending and denial-of service (DoS) attack. Double spending means seller selling the coins to two different buyers in a short span of time before the first transaction is confirmed.
- v). The entire process at each node is called as mining. Each block that is verified, the node (now the miner) receives a payment for his service.
- vi). Miners make profits with each of the transactions.
 - a) Transaction fees and newly minted coins, called mined coins. Each block that gets verified under the Bitcoin protocol introduces new coins to the market, and is given to the miner as payment for the participation in the event. Payment is a reward for the time spent and effort made by the miner.
 - b) This number of coins minted decreases with time so that there will never be over 21 million BTC in existence under the Bitcoins protocol.

V. What is the secret of popularity of Cryptocurrency especially Bitcoins all over the world?

- 1) Bitcoins or Altcoins are virtual entities that are neither created by any mint press or central bank, nor regulated by any government. There is no third party surveillance or the bank to record transactions, or the income tax agencies that can trace or regulate monetary transaction.
- 2) Bitcoins or Altcoins, a personal transaction, make the entire Banking system seem irrelevant. There are no cumbersome procedures, permissions from authorities and the entire architecture of banking or other financial institutions .
- 3) Cryptocurrency wallets cannot be raided, seized, attached or audited by banks and law enforcement agencies. Bitcoin wallets do not have spending and withdrawal limits imposed on them. The owner of the Bitcoin wallet enjoys unregulated freedom to manage his money.
- 4) Cryptocurrency has transformed the way one stores [virtual space] and spends [virtual incident] one's personal wealth.
- 5) Bitcoins, being first of the crypto-currencies ,is popular because it hands in the control of personal wealth back into the hands of the individual. Instead of paper or virtual bank balances that promise to have value, Bitcoins are actual packages of complex data, that like gold coins, have value in themselves.
- 6) The success of Bitcoins or its popularity also lies in the complete anonymity it grants to its miners. Though the mode of transaction is peer to peer and direct, the miners do not know each other.

- 7) Although people cannot easily see the other miner's personal identity, they can see the history of the miners' Bitcoin wallet. The public history of the miner adds transparency and security, helps deter people from using Bitcoins for dubious or illegal purpose.
- 8) It is a self regulating currency the limit of which is 21 million. Beyond this limit Bitcoins can not be created or minted.

VI. Perils of Crypto-currency Transaction:

- i) Technical weakness – Time delay in confirmation: There is a possibility of double-spending in some instances during the confirmation interval. The interval lasts for several seconds for a transaction to be confirmed across the Peer2Peer swarm of computers. The intervening period can be spent by unscrupulous miner to make another transaction. Blockchain technology supposedly is designed to prevent any double-spending issues. However, the risk is always present.

While the system will eventually catch the double-spending and cancel the second dishonest transaction, if the second recipient transfers goods to the dishonest buyer before he receives confirmation, then that second recipient will lose both the payment and the goods. But for this kind of trickery one need superfast servers and hence the possibility of dishonest transaction though not ruled out is minimal and not significant.

- ii) Human Deceit – Integrity is a serious concern in any business transaction. Like any other cyber business, organized gangs of dishonest persons or cyber criminals can certainly work their way to beat the established system. Because Bitcoin mining is best achieved through pooling, [read brokers or agents or agencies] the organizers of each pool gets the privilege of choosing how to divide up any bitcoins that are available. There is always a possibility of unjust distribution or non-disclosure.
- iii) Human failure – Online exchanges like Mt. Gox[2] come as the biggest example of what can happen when unregulated online exchanges that trade cash for bitcoins are run by people that are dishonest or incompetent. Unlike conventional banking there is no compensation for partial or total losses in such exchanges. The currency is lost forever and cannot be recovered.
- iv) Bitcoin transactions are irreversible. Conventional payment methods, like a credit card charge, bank draft, personal checks, or wire transfer, there is a possibility of cancellation of transaction. The crypto-currency transaction is reversible. In the case of bitcoins, every time bitcoins change hands and change wallets, the result is final and irreversible. There is no insurance protection either. If the hard drive data or its password is lost, the money is lost and can not be recovered.
- v) Bitcoins have become an instrument for illicit trade and money laundering, precisely because of the lack of government supervision and control. The value of bitcoins scaled height in the recent past because cyber criminals entered the scene and were seen to be purchasing bitcoins in large volumes. As in the case of stock exchanges where there is no guarantee of the value an investment can fetch, the risk factor in investing in crypto currency is just as high or even higher as transaction is unregulated.

Bitcoin transactions are not absolutely free. There are small convenience charges that need to be paid to three groups: fees for the network of nodes, online conversion of bitcoins to dollars or euros and the mining pool or group the miner joins. However, these fees range from a few cents to 1 per cent of support fees in the form of one-time fees or a small donation. The costs are nominal as compared to banking transaction charges.

VII. Future of Crypto –currency:

For Warren Buffett Bitcoin is “The Real Bubble”.[2017] But for John McAfee - creator of the antivirus software, Bitcoin will hit \$500,000 within three years.[2014] And for Bill Gates Bitcoin is “Better Than Currency”[2014]. Some view crypto-currency as the dawn of new financial transactions.

Today, Microsoft, PayPal, Tesla, WordPress, Shopify, Virgin Galactic, Expedia, Whole Foods, Subway, PWC, EY, Bloomberg, and many more companies and merchants accept Bitcoin for payment, which displays the expanding nature of the currency.

A current status of the finance market shows that there are as many as 1643 cryptocurrencies worth \$ 378,356,324,778 with Market Cap of \$ 14,164,074,625 having 47.20 % market share.[Unconfirmed source]

So what is the future of Crypto currency? Will it replace and revolutionize the entire finance world or would it be only a temporary phenomena? Would it be regulated by nations?

Although Bitcoin is now nine years into existence, countries still do not have explicit systems that restrict, regulate, or ban the crypto-currency. The decentralized, distributed and anonymous nature of bitcoin has challenged many governments on creating safeguards to ward off criminal transactions. Most countries are still analyzing ways to properly regulate the crypto-currency. Overall, bitcoin remains in a grey area as the technological invention has left policymakers and lawmakers far behind.

As per Forbes, permissioned cryptocurrencies are preferred than permissionless cryptocurrencies. Thus it appears as if the world and countries would embrace crypto transactions in future, not as a matter of choice but as compulsion, but they would want regulatory safeguards to ensure that the cyber criminals do not hijack the system and investors are protected.

Notes:

1. Coincapmarket.com
2. Wiki Pedia :Mt. Gox was a [bitcoin exchange](#) based in [Shibuya, Tokyo, Japan](#).^[1] Launched in July 2010, by 2013 and into 2014 it was handling over 70% of all [bitcoin](#) ("BTC") transactions worldwide, as the largest bitcoin intermediary and the world's leading bitcoin exchange.^{[2][3][4][5]}

In February 2014, Mt. Gox suspended trading, closed its website and exchange service, and filed for [bankruptcy protection](#) from creditors.^{[6][7]} In April 2014, the company began [liquidation](#) proceedings.^[8]

Mt. Gox announced that approximately 850,000 bitcoins belonging to customers and the company were missing and likely stolen, an amount valued at more than \$450 million at the time.^[9]

3. ‘the future dawn of Trade & Finance’ or ‘Is it a cheap gamble’ quotes mine.

Sources :

1. Bloggeeks.com
2. Investopedia.com
3. Lifewire.com
4. The Economics of Cryptocurrencies – Bitcoin and Beyond
Jonathan Chiu Thorsten Koepl Bank of Canada Queen’s University Victoria University of Wellington April, 2017
5. https://repository.upenn.edu/cgi/viewcontent.cgi?article=1133&context=wharton_research_scholars&
6. Wikipedia

