



Knowledge Consortium of Gujarat
Department of Higher Education, Government of Gujarat
JOURNAL OF COMMERCE AND MANAGEMENT
ISSN : 2279-025X

Continuous Issue - 10 | July-October -2014

SOME REFLECTION ON BIT-COINS

Abstract :

Bitcoin is a peer-to-peer payment system and digital currency introduced as open source software in 2009 by pseudonymous developer Satoshi Nakamoto. It is a crypto currency, so-called because it uses cryptography to control the creation and transfer of money. Conventionally, "Bitcoin" capitalized refers to the technology and network whereas lowercase "bit coins" refers to the currency itself. Bit coins are created by a process called mining, in which participants verify and record payments in exchange for transaction fees and newly minted bit coins. Users send and receive bit coins using wallet software on a personal computer, mobile device, or a web application. Bit coins can be obtained by mining or in exchange for products, services, or other currencies.

Introduction:

First mentioned in a 2008 paper published under the pseudonym "Satoshi Nakamoto", Bitcoin became operational in early 2009 with the release of the first open source client or wallet, Bitcoin-Qt, and the issuance of the first bitcoins. The currency had early technical problems such as a 2009 exploit that allowed the creation of unlimited bitcoins. Historically, Bitcoin-Qt was the sole software that could facilitate bitcoins transactions, and it initially also supported mining. (This feature was later removed because specialized mining software is more efficient.) Since its 2009 release, it has been maintained and enhanced by a group of core developers and other contributors. It can be used as a desktop wallet for regular payments or as a server utility for merchants and other payment services. Sometimes referred to as the reference client because it serves to define the Bitcoin protocol and acts as a standard for other implementations, it is also called the Satoshi client. By May 2011 interest in Bitcoin was growing as were concerns.



Objectives:

1. To know about bit coins word and its inception in present E- commerce market.
2. To study the importance of bit- coins at global level.

Establishment:

A report by Jason Calacanis included statements such as "Bitcoin may be the most dangerous technological project since the internet itself. The price of bitcoins has fluctuated wildly since its inception, going through various cycles of appreciation, which have been referred to by some as bubbles. In 2011 the value of one bitcoin rapidly rose from about US\$0.30 to US\$32 before falling back down to US\$2.

Following increased media attention in the latter half of 2012 and the 2012-2013 Cypriot Financial Crisis, the bitcoin price began to rise again in early 2013 reaching a peak of US\$266 on April 10 before crashing to around US\$50. In March 2013 a technical glitch caused a fork in the block chain with one half of the network adding blocks to one version of the chain, and the other half adding to

another. For six hours there were effectively two Bitcoin networks operating at the same time, each with its own version of the transaction history. The core developers called for a temporary halt to transactions, sparking a sharp sell-off. Normality was restored when the majority of the network downgraded to version 0.7 of the Bitcoin software from the flawed version 0.8. In 2013, some mainstream services began accepting it as a form of payment. Certain non-profit or advocacy groups such as the Electronic Frontier Foundation also began accepting bitcoin donations. 2013 also saw the first interventions by law enforcement. Assets belonging to the Mt.Gox exchange were seized, and the Silk Road marketplace website was shut down. During November 2013, the China-based Bitcoin exchange BTC China overtook Japan-based Mt.Gox and Europe-based Bit stamp to become the largest Bitcoin trading exchange by trade volume. On 19 November 2013, the value of a bitcoin on the Mt.Gox exchange soared to a peak of US\$900 following a United States Senate committee hearing, at which the committee was informed that virtual currencies were a legitimate financial service. On the same day, one bitcoin traded for over RMB¥6780 (US\$1100) in China. With roughly 12 million bitcoins in existence as of November 2013, the new price increased the market cap for Bitcoin to at least US\$7.2 billion.

By November 23, 2013, the total market capitalization of all bitcoins in existence exceeded US\$10 billion for the first time. On December 5, 2013, the People's Bank of China announced it was prohibiting Chinese financial institutions from using bitcoins. Following the introduction of these new rules, the value of bitcoin dropped and Chinese internet giant Baidu reversed its policy of accepting bitcoins for certain services. Starting in October 2013, Baidu had been allowing clients of website security services to pay with bitcoins. Buying real-world goods with any virtual currency has been illegal in China since at least 2009. In January 2014, two were arrested in the US on charges of money-laundering using bitcoins. Charlie Shrem, the head of defunct Bitcoin exchange BitInstant and a vice chairman of the Bitcoin Foundation, allegedly allowed Robert Faiella, also arrested, to purchase large quantities of bitcoins that were subsequently used to buy illegal drugs on black market websites. In the US, Bitcoin exchanges are regulated as money services businesses and as such are obligated to report any activity symptomatic of money laundering.

Importance:

Following is discussed important points related to bit coins.

1) Transactions: Users send payments by broadcasting digitally signed messages to the network. Transactions do not explicitly identify the payer and payee by name. Instead, a transaction transfers ownership from one Bitcoin address to another. Approximately every ten minutes a bundle of transactions, called a "block", is confirmed to a public transaction record called the block chain. This confirmation process, known as "mining", carries a reward of 25 bit coins per block added to the block chain. Acting as an incentive for individuals and groups to maintain the integrity of the Bitcoin system by allowing their computers to be used to confirm transactions, the 25 bitcoins reward is also the way in which new bit coins enter circulation.

2) Software: Bitcoin wallet software, sometimes called a Bitcoin client, allows a user to transact bitcoins. At its most basic, a wallet program generates and stores private keys and communicates with peers on the Bitcoin network. The first was released in 2009 by Satoshi Nakamoto as open source code. When making a purchase with a mobile device, the use of QR codes to simplify transactions is ubiquitous. There are also now several server software implementations of the Bitcoin protocol. So-called "full" nodes on the network validate transactions and blocks they receive and relay them to connected peers. Bitcoin uses public-key cryptography, in which pairs of cryptographic keys, one public and one private, are generated. A collection of keys is called a wallet. Note that sometimes this term is used to mean the software itself in the sense of digital wallet. A Bitcoin transaction transfers ownership to a new address, an alphanumeric string of the form random letters and numbers derived from public keys by application of a hash function and encoding scheme. The corresponding private keys act as a safeguard; a valid payment message from an address must contain the associated public key and a digital signature proving possession of the associated private key.

3) Block chain: Integral to Bitcoin is a public database and sequential record of all transactions, known as the block chain that records current bitcoin ownership as well as at all points in the past. By keeping a record of all transactions, the block chain prevents a problem particular to digital money. Those who maintain the block chain are called miners and are rewarded with newly created bitcoins as

well as transaction fees.

4) Buying and selling bitcoins: Bitcoin can be bought and sold for many different currencies from individuals and from companies. The fastest way to obtain bitcoins is to purchase them in person for cash. Participants in online exchanges offer bitcoin buy and sell bids. Other companies buy or sell bitcoin in bulk on exchanges and offer their customers the option to buy or sell bitcoin at market price. Fees vary by transaction volume and services provided. Bitcoin ATMs allow cash-for-bitcoins transactions to be made. Using an online exchange to obtain bitcoins does entail some risk. These exchanges regularly fail, taking client bitcoins with them. In addition, since bitcoin transactions are irreversible, sellers of bitcoins must take extra measures to ensure receipt of traditional funds from the buyer.

5) Lack of Secrecy: The block chain provides a certain level of anonymity; it identifies receivers by Bitcoin addresses, not individuals' names. Tracking the flow of bitcoins can give clues as to who owns them, however. And while Bitcoin uses cryptography, it does not do so to protect the identities of its users. In addition, Bitcoin intermediaries, such as exchanges, are required by law in many jurisdictions to collect personal customer data.

6) Economics & Volatility: Bitcoin has garnered comments and attention from economists and journalists, as well as investors and speculators. Others who mistrust their national currency have seen Bitcoin as a safe haven from inflation and a way to circumvent capital controls. The Bitcoin market currently suffers from volatility, which limits the utility of bitcoins to act as a currency. This has not prevented their being used as a medium of exchange, however.

7) Alternative to national currencies: Bitcoin detractors as well as its supporters have suggested that Bitcoin is gaining popularity in countries with problem-plagued national currencies as it can be used to circumvent inflation, capital controls, and international sanctions. For example, Bitcoins are used by some Argentinians as an alternative to the official currency, at this time stymied by inflation and strict capital controls. In addition, some Iranians use bitcoins to evade currency sanctions. Financial journalists and analysts have suggested that there was a link between higher Bitcoin usage in Spain and the 2012-2013 Cypriot financial crisis. Others believe that mistrust in traditional financial institutions and central banks fostered by the Financial crisis of 2007-08 has helped bolster Bitcoin popularity.

8) Speculation and bubbles: Bitcoins are often traded as an investment by speculators who expect widening popularity along with increases in value. The European Banking Authority has warned that the risks of engaging in such speculation go beyond the possibility that the value of bitcoins drops. Vulnerability to hacking and theft makes their use as an investment questionable, especially for unsophisticated investors. Partially as a result of such speculation, the value of bitcoin has been volatile with repeated rapid rises and collapses. Many have named Bitcoin a speculative bubble including former Federal Reserve Chairman Alan Greenspan and Economist John Quiggin. Two lead software developers of Bitcoin, Gavin Andresen and Mike Hearn, have warned that bubbles may occur. Financial journalist Felix Salmon correctly predicted the bursting of one such Bitcoin bubble in April 2013. Nick Colas, a market strategist for ConvergEx Group, is among those who reject the existence of bubbles and see Bitcoin's quick rise in price as nothing more than normal economic forces at work.

9) Money supply: Growth of the Bitcoin money supply is predefined by the Bitcoin protocol, and in this way inflation is kept in check. Currently there are over twelve million bitcoins in circulation with an approximate creation rate of 25 bitcoins every ten minutes. The total supply is capped at 21 million and every few years or so the creation rate is halved. This means new bitcoins will continue to be released for more than a hundred years.

10) Bitcoin valuation: Bitcoin has been under scrutiny by financial journalists, notable economists, financial analysts, investors and researchers trying to determine its possible future value. Financial journalist Felix Salmon used the chart plotting bitcoin market capitalization as the primary reason (see also technical analysis) to forecast: "Rick Falvinge, then, the founder of the Swedish Pirate Party who has invested his entire net worth in bitcoins, might be a multi-millionaire right now, but he is doomed to end up a poor and disappointed man unless he changes his mind." Salmon also used a deeper reason to come to his conclusion, namely his opinion that: "bitcoins are an uncomfortable combination of commodity and currency.

11) Reception: Economists have had a mixed reaction to Bitcoin. Some have responded positively,

including François R. Velde, a senior economist at the Federal Reserve in Chicago, who described it as "an elegant solution to the problem of creating a digital currency." Others have been critical. Economists Paul Krugman and Brad DeLong have found fault with Bitcoin for numerous reasons including that bitcoins are not a reliable store of value and that there is no floor on their value. Economist and professor John Quiggin has called Bitcoin "the final refutation of the efficient market hypothesis". Bitcoin has been criticized for its proof of knowledge by the free software movement activists including Richard Stallman, who called for reformed development.

12) Acceptance by merchants: Large, established firms that accept bitcoins include Overstock.com, the Sacramento Kings, Tiger Direct, and Zynga. In November 2013, Richard Branson announced that Virgin Galactic would accept Bitcoin as a method of payment. In November 2013, the University of Nicosia became the first accredited university in the world to accept it as a method of payment for tuition and fees. Merchant processors such as Bitpay and Coinbase have had a huge influence over the acceptance of bitcoin. Overstock is working with Coinbase. The Sacramento Kings, Tiger Direct, Clearly Canadian and Zynga all work with Bitpay.

13) Legal issues and status: Criminal activity linked to Bitcoin has largely centered around theft of the currency, the use of botnets for mining, and the illicit use of bitcoins in exchange for illegal items or services. Certain nation states may feel that its use in circumventing capital controls is also undesirable. While some governments have taken a hands-off approach, others have moved to regulate Bitcoin and similar, private currencies. Critics have accused Bitcoin of being a Ponzi scheme. A case study report by the European Central Bank observes that the Bitcoin currency system shares some characteristics with Ponzi schemes, but also has characteristics that are distinct from the common aspects of such schemes.

14) Black markets: Several news outlets have asserted that the popularity of Bitcoin hinges on the ability to use them to purchase illegal substances. In 2013 The Guardian reported that the currency was primarily used to purchase illegal drugs and for online gambling, and The Huffington Post stated that "online gambling accounts for a huge portion of Bitcoin activity." C. 2013 legitimate transactions were thought to be far less than the number involved in the purchase of drugs, and roughly one half of all transactions made using Bitcoin were bets placed at a single online gaming website.

15) Criminal activity: Bitcoin's association with criminal activities has historically hindered the currency from attaining widespread, mainstream use and has attracted the attention of financial regulators, legislative bodies, and law enforcement.[108] The Washington Post had labeled it "the currency of choice for seedy online activities,"[109] and CNN has called Bitcoin a "shady online currency [that is] starting to gain legitimacy in certain parts of the world." Its links to criminal activities have prompted scrutiny from the FBI, US Senate, and the State of New York. The FBI stated in a 2012 report that "bitcoins will likely continue to attract cyber-criminals who view it as a means to move or steal funds". Steven Strauss, a Harvard public policy professor, has suggested that due to its close association with illegal purchases, governments could outlaw Bitcoin, which was also mentioned in 2013 SEC filing made by a Bitcoin investment vehicle. Bitcoins are not currently illegal in the US, however. FBI Special Agent Christopher Tarbell has stated that "bitcoins are not illegal in and of themselves and have known legitimate uses".

16) Legal status: Many governments have made announcements regarding Bitcoin, and these decisions also likely affect treatment of other crypto currencies as well. Some, including Australia, Canada, Finland, and Germany, have simply made it clear that normal earned income rules apply to Bitcoin. Other states reject the label of currency but will collect taxes on Bitcoin transactions, such as Norway. (Germany may technically fall into this latter category as it refers to Bitcoin as a unit of account, which is one of several roles fully fledged currencies play.) Still more have issued statements that assert Bitcoin is not regulated in their jurisdictions, such as Singapore and Poland.

17) Money laundering: Some regulatory and law enforcement authorities, including the European Banking Authority and the FBI, feel Bitcoin may be used for illicit money laundering purposes. In early 2014, an operator of a US Bitcoin exchange was arrested for money laundering. Some say one obstacle to bitcoins becoming widely used to launder money is that all transactions are public. During a US Senate hearing in 2013, Jennifer Shasky Calvery, director of the Treasury Department's Financial Crimes Enforcement Network stated, "cash is probably still the best medium for money laundering."

18) Unauthorized mining: In June 2011, Symantec warned about the possibility of botnets engaging in covert mining of bitcoins. Some malware used the parallel processing capabilities of GPUs

built into many modern video cards. In mid-August 2011, Bitcoin mining botnets were detected again, and less than three months later, Bitcoin mining trojans infecting Mac OS X were also discovered. In April 2013, electronic sports organization E-Sports Entertainment was accused of hijacking 14,000 computers to mine bitcoins; the case was settled in November with the organization fined US\$1 million if it breaks the law within the following ten years or \$325,000 if it does not.

19) Thefts: Theft of bitcoins means someone completed an unauthorized transfer of bitcoins out of the authorized user's wallet. Protection of the bitcoin wallet means protecting the private key used to unlock the wallet. Thefts happen when a thief gains access to the private keys in the bitcoin wallet. Most large-scale thefts occur at payment processors, exchanges, or online wallet services that store the private keys of many bitcoin users. The thief hacks an online wallet service by finding a bug in that website or spreading malware to computers holding the private keys. When they have control of the website or its database, they gain access to many users' private keys and can thereby steal those users' bitcoins.

20) Physical Bitcoins: The most notable physical bitcoins are the now-discontinued Casascius coins, which hide the private key behind a tamper-proof sticker. At the Defcon hacking convention, physical Casascius coins were found to be redeemable without significantly damaging the tamper-proof sticker, by chemically neutralizing the adhesive. New solutions include a 2-factor private key which requires a password to be redeemed. The creator of a physical bitcoin may retain private keys; therefore physical bitcoins created by third parties are not considered secure. Bitcoins have been stored physically on paper metal, wood and plastic. There are also specialized digital products known as "Hardware Wallets", designed to store bitcoins securely on a physical device.

Conclusion:

Bitcoin has been a subject of scrutiny due to ties with illicit activity. In 2013, the US FBI shut down the Silk Road online black market and seized 144,000 bit coins worth US\$28.5 million at the time. The US is considered Bitcoin-friendly compared to other governments, however. In China, new rules restrict bit coin exchange for local currency, and the European Banking Authority has warned that Bitcoin lacks consumer protections. Bit coins can be stolen, and charge backs are impossible. Commercial use of Bitcoin, illicit or otherwise, is currently small compared to its use by speculators, which has fueled price volatility. Bitcoin as a form of payment for products and services has seen growth, however, and merchants have an incentive to accept the currency because transaction fees are lower than the 2-3% typically imposed by credit card processors.

REFERENCES :

1. <http://www.forbes.com/sites/jonmatonis/2012/07/31/top-10-bitcoin-statistics/> Dated: 10/02/2014
2. http://bitcoincharts.com/markets/localbtcINR_trades.html. Dated 11/02/2014
3. <http://en.wikipedia.org/wiki/Bitcoin> 11/02/2014

DR. GAURANGKUMAR C. BAROT

GOVT. (AIDED) COLLEGE ARTS COMMERCE AND SCIENCE
SILVASSA, NAROLI