Volume 4, Issue 10, October 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Bitcoin: A Step Ahead in Technology

Garima Chaudhary
Assistant Prof.
Guru Gobind Singh College for women
Chandigarh, India

Abstract: Every now and then we come across one or the other technology, one surpassing the other. Bitcoin is a new revolution in the banking sector which has helped in creating an E wallet which will be carrying a currency that can be used worldwide. Though this has not been widely accepted everywhere but few European countries have started its applicability. There are numerous reasons behind being so reluctant in accepting this as a normal currency for any country which are further studied in this paper. Also the benefits attached with bitcoin can also not be ignored.

Keywords: Wallet, CPU, banks, network, privacy, password

I. INTRODUCTION

With the change in the current scenario, it is seen that the customer has become more demanding and the level of expectation has also increased many forth, which further has lead to the introduction of latest technology as a routine in the market. There was a time when internet and online banking bought revolution in the economy which gave a chance to the customer to use banking functions with just a click of mouse sitting anywhere. Then came the visa, debit and the credit card which further enhanced the level of banking sector so forth. And now to improve more and to remove the discrepancies and the left out demand by all these technologies, a new concept is there to bring a change in everyones' life, known as BITCOIN. It is though a new concept in India but it is frequently being used in the European and some American countries for the past few months. Talking about bitcoin, it is a peer-to-peer payment system and digital currency which was introduced as open source software in 2009. Bitcoin refers to the combination of technology with the network whereas lowercase "bitcoin" refers to the currency itself.

Basically, bitcoins are created when computer network participants or the users who provide their computing power, verify and record payments into a public ledger in exchange for transaction fees, this process is known as "Mining". Users send and receive bitcoins using wallet software on a personal computer, mobile device, or a web application. It is just a new revolution in the area of fast and easy payment because it is a form of payment for products and services used by the consumers. As the usage of this technology is not much so the crimes involved and the hacking part is very less as this is not a common process being used worldwide right now. But 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. The biggest transaction ever using Bitcoin was payment for buying a villa in Bali worth over $500,000.

When a Bitcoin user makes a purchase, the payment triggers a broadcast of the financial transaction to the Bitcoin network. The Bitcoin transaction is a digitally signed message to take effect it must be recorded in a public ledger or public transaction database called the block chain. Approximately every ten minutes a bundle of transactions, called a "block", is added to the block chain. The incentive for this accounting process, known as "mining", carries a reward of 25 bitcoins per block added to the block chain. This 25 bitcoins reward maintains the integrity of the Bitcoin system by allowing the computers that confirm transactions to also mint new bitcoins in the process. Bitcoin payment processing fees are optional, and generally substantially lower than those of credit cards or money transfers.

II. RESEARCH METHODOLOGY

Secondary data has been used. Data has been collected from various journals, websites and books.

Objectives:

1. To know the concept of bitcoin as a whole.
2. To study the working of bitcoin
3. To study the harmful effects of bitcoin on the economy.
4. To evaluate the performance of bitcoin.

Limitations of the study: Being a new concept, and as it is not being used too frequently worldwide, thus it was quite difficult to collect the data easily. Secondary data was also not readily available.

Block chain

Integral to Bitcoin is a public ledger, a database with a sequential record of all transactions, known as the block chain, that records bitcoin ownership at present and at all points in the past. By keeping a record of all transactions, the block chain prevents double-spending, a problem particular to digital money.[1] The block chain identifies receivers by Bitcoin addresses, not individuals' names, but the flow of bitcoins can give clues as to who owns them.[2] Bitcoin intermediaries, such as exchanges, are required by law in many jurisdictions to collect personal customer data.[3]

Buying and selling bitcoins

Bitcoin can be bought and sold for many different currencies from individuals and from companies or even from ATMs for cash. The procedure that is followed is that the companies buy or sell it in bulk on exchanges and then it is offered to the customers to buy it via ATMs at market price. Bitcoin ATMs allow bitcoins to be purchased for cash,[4] and some also allow cash withdrawals from Bitcoin wallets stored on smartphones.[5][6] Using an online exchange to obtain bitcoins entails some risk, since according to one study 45% of exchanges have failed and taken client bitcoins with them.[7]Unlike normal cash transactions, bitcoin transactions are irreversible,so it is advisable that the sellers must take extra measures to ensure they have received traditional funds from the buyer.

Wallets

Bitcoin uses public-key cryptography, in which a pair of a public and a private cryptographic key is generated.[8] A collection of keys is called a wallet. Note that sometimes the term is used to mean the software in the sense of digital wallet. A Bitcoin transaction transfers ownership to a new address, a string having the form of 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 for the owner; a valid payment message from an address must contain the associated public key and a digital signature proving possession of the associated private key. Because anyone with a private key can spend all of the bitcoins sent to the corresponding address, the essence of Bitcoin security is protection of private keys. Theft of bitcoins has occurred on numerous occasions,[9] and the practical day-to-day security of Bitcoin wallets is a concern like the security of other forms of payment.[10] Risk of theft can be reduced by generating keys offline on an uncompromised computer and saving them on external storage or paper printouts.[11] "Physical bitcoins", ubiquitous in media coverage of Bitcoin, are produced by various vendors. They store a private key on paper, metal,[12] wood,[13] or plastic. There are also digital products known as "Hardware Wallets" to store bitcoins securely on a physical device.[14] Bitcoins can be lost. In 2013 one user said he lost 7,500 bitcoins, worth $7.5m at the time, when he discarded a hard drive containing his private key.[15]

Price volatility

According to Mark T. Williams of Boston University, bitcoin is over 7 times as volatile as gold and over 8 times as volatile as the S&P 500.[16] The extremely volatile bitcoin exchange rate has led people to question its ability to function as a currency.[17] The Bitcoin Foundation contends that this is due to insufficient liquidity and claims volatility will lessen if its popularity continues to increase.[18] Volatility has little effect on the utility of Bitcoin as a payment processing system.[19] Volatility has damaged the ability of bitcoin to be a store of value; it has not hampered its function as a medium of exchange. Bitcoin volatility is linked to uncertainty about its long-term value per *Forbes* contributor Timothy B. Lee.[20]

III. FEATURES OF BITCOIN

a) **Bitcoin as investment:** One way of investing in Bitcoin is to buy bitcoins and hold them as a long-term, high-risk investment. The Winklevoss twins made a US$1.5 million personal investment and attempted to launch a bitcoin ETF.[16] Some investors, like Peter Thiel's Founders Fund, which invested US$3 million, don't purchase bitcoins instead funding Bitcoin infrastructure like bitcoin exchanges, companies that provide bitcoin payment systems to merchants, or bitcoin wallet services, etc. Investors also invest in bitcoin mining.

b) **Supply of money:** Growth of the Bitcoin money supply is predefined by the Bitcoin protocol,[15] 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 the arbitrary limit of 21 million,[7] and every four years the creation rate is halved. This means new bitcoins will continue to be released for more than a hundred years.

c) **Acceptance by merchants:** Large, established firms that accept bitcoins include Overstock.com, the Sacramento Kings, TigerDirect, Clearly Canadian and Zynga. In November 2013, Richard Branson announced that Virgin Galactic would accept bitcoin as a method of payment.[1]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.

Legal status and regulation

As far as the regulation is concerned, few governments have taken a hands off approach whereas others have moved to regulate bitcoin and similar private currencies. The main reason behind the free acceptance of bitcoin is that it does not involve traditional financial actors as both the issuers of bitcoin and software/hardware owners are non-financial private companies, thus the traditional financial sector regulation is not applicable. In the US the first step of regulation occurred in July 2011, when the US Department of Treasury's Financial Crimes Enforcement Network added "other value that substitutes for currency" to its definition of Money services businesses. In 2013 the Treasury issued an interpretive guidance regarding virtual currencies,[24] according to which, exchangers and administrators, but not users of convertible virtual currency are considered money transmitters, and must comply with rules to prevent money laundering/terrorist financing ("AML/CFT") and other forms of financial crime. There are no rules at the state level as of 3/2014. The U.S.Commodity Futures Trading Commission has stated in March 2014, that it has been considering regulation of digital currencies. Canadian government will be regulating Bitcoin under its anti-money laundering and counter-terrorist financing legislation, the Proceeds of Crime (Money Laundering) and Terrorist Financing Act.

IV. NEGATIVE ASPECT

a) **Increase in criminal activities:** Bitcoin has involved in criminal activities due to its ease in hacking which is further covered as cybercriminals. Bitcoins are seized when dark web black markets are shut by authorities. The association with criminal activities has stigmatized the currency and attracted the attention of financial regulators, legislative bodies, and law enforcementit has further increased cyber crimes in the world.

b) **Money laundering:** Criminal activity involving Bitcoin has largely centered around theft of the currency, money laundering, the use of botnets for mining, and the use of bitcoins in exchange for illegal items or services. " Despite the claims made by the non-profit Bitcoin Foundation that "cryptography is the reason no one can steal bitcoins," theft is widespread.

c) **Black markets:** The popularity and ease in using bitcoin has been one of the major motivating factor fro purchase of illegal goods. Some online gaming websites are also found to be usedas a platform for placing bets. Raher some illegal weapons and drugs are also sold by online drug and gun dealers.

d) **Money laundering:** The European Banking Authority and the FBI have both stated that Bitcoin may be used for money laundering. Rather in early 2014, an operator of a US bitcoin exchange was arrested for money laundering.

e) **Thefts:** 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 its 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.

f) **Malware:** Bitcoin-related malware includes software that steals bitcoins from users using a variety of techniques, software that uses infected computers to mine bitcoins, and different types of ransomware, which disable computers or prevent files from being accessed until some payment is made.

g) **Ransomware:** Another type of Bitcoin-related malware is a type of ransomware. A program called Cryptolocker, typically spread through legitimate-looking email attachments, encrypts the hard drive of an infected computer, then displays a countdown timer and demands a ransom, usually two bitcoins, to decrypt it.

h) **Bitcoin price is volatile:** The price of a bitcoin can unpredictably increase or decrease over a short period of time due to its young economy, novel nature, and sometimes illiquid markets. Consequently, keeping savings with Bitcoin is not recommended at this point. Bitcoin should be seen like a high risk asset, and one should never store money that they cannot afford to lose with Bitcoin. If the user receive payments with Bitcoin, many service providers can convert them to their local currency.

i) **Bitcoin payments are irreversible:** Any transaction issued with Bitcoin cannot be reversed, they can only be refunded by the person receiving the funds. That means the user should take care to do business with people and organizations they know and trust, or who have an established reputation. For their part, businesses need to keep control of the payment requests they are displaying to their customers. Bitcoin can detect typos and usually won't let the user send money to an invalid address by mistake. Additional services might exist in the future to provide more choice and protection for the consumer.

j) **Instant transactions are less secure:** A Bitcoin transaction is usually deployed within a few seconds and begins to be confirmed in the following 10 minutes. During that time, a transaction can be considered authentic but still reversible. Dishonest users could try to cheat. For larger amounts like 1000 US$, it makes sense to wait for 6 confirmations or more. Each confirmation *exponentially* decreases the risk of a reversed transaction.

k) **Bitcoin is still experimental:** Bitcoin is an experimental new currency that is in active development. Although it becomes less experimental as usage grows, the user should keep in mind that Bitcoin is a new invention that is exploring ideas that have never been attempted before. As such, its future cannot be predicted by anyone.

Procedure:

The steps to run the network are as follows:

1) New transactions are broadcast to all nodes.
2) Each node collects new transactions into a block.
3) Each node works on finding a difficult proof-of-work for its block.
4) When a node finds a proof-of-work, it broadcasts the block to all nodes.
5) Nodes accept the block only if all transactions in it are valid and not already spent.
6) Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Simplified Payment Verification

It is possible to verify payments without running a full network node. A user only needs to keep a copy of the block headers of the longest proof-of-work chain, which he can get by querying network nodes until he's convinced he has the longest chain, and obtain the Merkle branch linking the transaction to the block it's time stamped in. He can't check the transaction for himself, but by linking it to a place in the chain, he can see that a network node has accepted it, and blocks added after it further confirm the network has accepted it. As such, the verification is reliable as long as honest nodes control the network, but is more vulnerable if the network is overpowered by an attacker. While network nodes can verify transactions for themselves, the simplified method can be fooled by an attacker's fabricated transactions for as long as the attacker can continue to overpower the network. One strategy to protect against this would be to accept alerts from network nodes when they detect an invalid block, prompting the user's software to download the full block and alerted transactions to confirm the inconsistency. Businesses that receive frequent payments will probably still want to run their own nodes for more independent security and quicker verification.

Combining and Splitting Value

Although it would be possible to handle coins individually, it is not suggested to make separate transactions for every cent in a transfer. To allow value to be split and combined, transactions contain multiple inputs and outputs. There can be either a single input from a larger previous transaction or multiple inputs combining smaller amounts, and at most two outputs: one for the payment, and one returning the change, if any, back to the sender.

It should be noted that fan-out, where a transaction depends on several transactions, and those transactions depend on many more, is not a problem here. There is never the need to extract a complete standalone copy of a transaction's history.

Privacy

The biggest achievement of the traditional banking is that a level of privacy can be easily maintained even while using online banking transactions by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. As an additional firewall, a new key pair should be used for each transaction to keep them from being linked to a common owner. Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner. The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner.

V. PRECAUTIONS TO BE UNDERTAKEN

a) **Carefully using online services:** Many exchanges and online wallets suffered from security breaches in the past and such services generally still do not provide enough insurance and security to be used to store money like a bank.

b) **Small amounts should be transacted:** A Bitcoin wallet is like a wallet with cash. It is a good practice to keep only small amounts of bitcoins on your computer, mobile, or server for everyday uses and to keep the remaining part of your funds in a safer environment.

c) **Wallet backup:** Stored in a safe place, a backup of the wallet can protect the user against computer failures and many human mistakes. It can also allow the user to recover their wallet after their mobile or computer was stolen if they keep their wallet encrypted.

d) **Backup of entire wallet:** Some wallets use many hidden private keys internally. If the user has only a backup of the private keys for the visible Bitcoin addresses, they might not be able to recover a great part of their funds with their backup.

e) **Encrypt online backups:** Any backup that is stored online is highly vulnerable to theft. Even a computer that is connected to the Internet is vulnerable to malicious software. As such, encrypting any backup that is exposed to the network is a good security practice.

f) **Using many secure locations:** Single points of failure are bad for security. If the backup is not dependent of a single location, it is less likely that any bad event will prevent the user to recover their wallet. Different other locations like USBs, paper and CDs can be used to secure the

g) **Encrypt your wallet:** Encrypting wallet or smartphone allows to set a password for anyone trying to withdraw any funds. This helps protect against thieves, though it cannot protect against keylogging hardware or software.

h) **Use a strong password:** Any password that contains only letters or recognizable words can be considered very weak and easy to break. The most secure passwords are those generated by programs designed specifically for that purpose. Strong passwords are usually harder to remember, so you should take care in memorizing it.

i) **Offline wallet for savings:** An offline wallet, also known as cold storage, provides the highest level of security for savings. It involves storing a wallet in a secured place that is not connected to the network. When done properly, it can offer a very good protection against computer vulnerabilities. Using an offline wallet in conjunction with backups and encryption is also a good practice. Here is an overview of some approaches.

Offline transaction signing

This approach involves having two computers sharing some parts of the same wallet. The first one must be disconnected from any network. It is the only one that holds the entire wallet and is able to sign transactions. The second computer is connected to the network and only have a watching wallet that can only create unsigned transactions. This way, you can securely issue new transactions with the following steps.

1. Create a new transaction on the online computer and save it on an USB key.
2. Sign the transaction with the offline computer.
3. Send the signed transaction with the online computer.

Because the computer that is connected to the network cannot sign transactions, it cannot be used to withdraw any funds if it is compromised. Armory can be used to do offline transaction signature.

j) Multi-signature to protect against theft: Bitcoin includes a multi-signature feature that allows a transaction to require the signature of more than one private key to be spent. It is currently only usable for technical users but a greater availability for this feature can be expected in the future. Multi-signature can, for example, allow an organization to give access to its treasury to its members while only allowing a withdrawal if 3 of 5 members sign the transaction. It can also allow future online wallets to share a multi-signature address with their users, so that a thief would need to compromise both your computer and the online wallet servers in order to steal your funds.

VI. SOME IMPORTANT TERMINOLOGIES

MultiBit

MultiBit is a lightweight client that focuses on being fast and easy to use. It synchronizes with the network and is ready to use in minutes. MultiBit also supports many languages. It is a good choice for non-technical users. Hive is a fast, integrated, user-friendly Bitcoin wallet for Mac OS X. With a focus on usability, Hive is translated into many languages and has apps, making it easy to interact with your favorite Bitcoin services and merchants. Armory is an advanced Bitcoin client that expands its features for Bitcoin power users. It offers many backup and encryption features, and it allows secure cold-storage on offline computers. Electrum's focus is speed and simplicity, with low resource usage. It uses remote servers that handle the most complicated parts of the Bitcoin system, and it allows you to recover your wallet from a secret phrase. Web wallets allows the user to use Bitcoin on any browser or mobile and often offer additional services.

Third party

This wallet relies on a centralized service by default and requires a certain level of trust on a third party. This third party however does not control your wallet. Using backups and a strong password is always recommended when applicable. Web wallets host your bitcoins. That means it is possible for them to lose your bitcoins following any incident on their side. As of today, no web wallet services provide enough insurance to be used to store value like a bank.

Desktop wallets

Desktop wallets are installed on the computer of the user. They give them complete control over the user’s wallet. The user will be responsible for protecting your money and doing backups.

Mobile wallets

Mobile wallets allows to bring Bitcoin with in the pocket. The user can exchange bitcoins easily and pay in physical stores by scanning a QR code or using NFC "tap to pay".

Web wallets

Web wallet allows the user to use Bitcoin on any browser or mobile and often offer additional services. However, the user must choose the web wallet with care as they host your bitcoins.

VII. CONCLUSION

Though bitcoin is a new revolution in the hardware wallet system but every rose has thorns attached with it, anyone using this technology has to be very careful in actually practicing it. The reasons are far more than what one can imagine and the solution to all these problems have still not been reached as yet. Also it is a very important and potential tool for the banking sector in future which will help a consumer in availing services without any hassle of currency exchange. This is a technology beyond borders, beyond countries but with due care and diligence.

REFERENCES

[1] Wallace, Benjamin (23 November 2011). "The Rise and Fall of Bitcoin". *Wired*. Retrieved 4 November 2013.

[2] Ashlee Vance (14 November 2013). "2014 Outlook: Bitcoin Mining Chips, a High-Tech Arms Race". Businessweek. Retrieved 24 November 2013.

[3] "FIN-2013-G001: Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies". Financial Crimes Enforcement Network. 18 March 2013. p. 6. Retrieved 4 March 2014.

[4] Jervis, Rick (2014-02-20). "Bitcoin ATMs come to USA". *USA Today*.

[5] Lee, Timothy B. (19 November 2013). "12 questions about Bitcoin you were too embarrassed to ask". *The Washington Post*. Retrieved 12 December 2013.

[6] Steadman, Ian (2013-04-26). "Study: 45 percent of Bitcoin exchanges end up closing". *Wired*. Retrieved 2013-04-28.

[7] Bustillos, Maria. "The Future of Bitcoin". *The New Yorker*. Retrieved 3 December 2013.

[8] Danny Bradbury (2013-12-27). "5 things to do with those Christmas bitcoins". Coindesk.com. Retrieved 2014-01-14.

[9] Staff, Verge (2013-12-13). "Casascius, maker of shiny physical bitcoins, shut down by Treasury Department". The Verge. Retrieved 2014-01-10.

[10] Daniel Cawrey (@danielcawrey) (2013-12-20). "Canadian Man Builds World's First Wooden Bitcoin Wallet". Coindesk.com. Retrieved 2014-01-10.

[11] Joon Ian Wong (@joonian) (2013-12-04). "Trezor to Ship Physical Bitcoin Wallets in January". Coindesk.com. Retrieved 2014-01-10.

[12] "Man Throws Away 7,500 Bitcoins, Now Worth $7.5 Million". *CBS DC*. 29 November 2013. Retrieved 23 January 2014.

[13] Thompson, Jennifer (21 March 2014). "Mt Gox finds 200,000 ‘lost’ Bitcoins in old wallet". *Financial Times*. Retrieved 23 March 2014.

[14] Skudnov, Rostislav (2012). *Bitcoin Clients* (Bachelor's Thesis). Turku University of Applied Sciences. Retrieved 2014-01-16.

[15] http://www.coindesk.com/bitcoin-version-0-9-0-brings-transaction-malleability-fixes-branding-change/.\

[16] Gloria Goodale, Christian Science Monitor (17 September 2013). "The Rise Of Bitcoin: Is It A Solution Or Menace?". Business Insider. Retrieved 25 November 2013.

[17] Foxman, Simone (2 April 2013). "How to short bitcoins (if you really must)". Quartz. Archived from the original on 29 April 2013.

[18] "Warning to consumers on virtual currencies". European Banking Authority. 12 December 2013. Retrieved 23 December 2013.

[19] Kearns, Jeff (4 Dec 2013). "Greenspan Says Bitcoin a Bubble Without Intrinsic Currency Value". *bloomberg.com*. Bloomberg LP. Retrieved 23 December 2013.