ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 5, Issue 6, June 2016

Bitcoins,Its Advantages and Security Threats

Archana M. Naware

***Abstract*—Bitcoin is encrypted digital currency which can be bought, sold and exchanged from market places. Bitcoins are transfered like email. The Bitcoins are marked with identification key of the owner which does not include personal information of the user. So user remains anonymous. The value of Bitcoin continuously changes and is traded like stocks on various exchanges. Bitcoins are stored using Bitcoin wallets. Bitcoins have advantages such as freedom for payment, control and security, transparent information and disadvantages such as wallet can be lost, changing price of Bitcoins. The Bitcoins also have security threats such as attack to Bitcoin wallet, double spending, Pony Botnet, 51% attack.**

Bitcoins have emerging market in India. Unocoin, Coinsecure, BTCXIndia are companies which provide Bitcoin wallet, exchange services in India.

***Index Terms*—Bitcoin, Bitcoin wallet, Blockchain, mining**

I. INTRODUCTION

Bitcoin is a type of digital currency in which encryption techniques are used to regulate the generation of Bitcoins and verify the transfer of funds. It operates independently of a central bank and is described as "the first decentralized digital currency". Bitcoins are limited and their value depends on market forces. Bitcoins are traded like stocks on various exchanges [5].

Bitcoins can be broken into small units of up to eight decimal points like BTC, mBTC, uBTC and Satoshi and are sent like an email [24]. Bitcoins are marked out with the transaction details and the identification key of the new owner. Identification key includes no personal information. so buyers and sellers remain anonymous. All transactions are communicated to the public network and indexed for future verification [21]. Bitcoins can be bought and sold both online and offline. User can buy Bitcoins from either exchanges or directly from other people through market. Bitcoin buy and sell bids are available online for the users. Bitcoins may be purchased directly from an individual or at a Bitcoin ATM [16] and can be paid for them in a variety of ways using hard cash, credit and debit cards and other cryptocurrencies. Bitcoins are used to pay for goods and services on websites that accept them.

Bitcoins have advantages such as payment freedom, control and security, Information is transparent , very low fees and disadvantages such as unawareness of people about Bitcoins, wallet can be lost, changing price of Bitcoins and also have security threats such as attack to wallet , Pony Botnet, double spending, 51% attack. Bitcoins are stored using Bitcoins wallets. There are five main types of wallets such as desktop wallet, mobile wallet, web wallet, paper wallet and hardware wallets [6].

II. BITCOIN WALLETS

Bitcoins are stored using Bitcoin wallets. BTCXIndia, Coinsecure, Unocoin are the companies which provide Bitcoin wallets. The Bitcoin wallets are categorized in to five types as follow.

A. Desktop Wallet

The original Bitcoin client, Bitcoin Core, is Desktop wallet. This software relays transactions on the network, enables people to create a bitcoin address for sending and receiving the virtual money and to store the private key for it. There are different desktop wallets such as MultiBit which runs on Windows, Mac OSX, and Linux. Hive is an OS X-based wallet have some unique features and also have an app store that connects directly to bitcoin services.

B. Mobile Wallets

The mobile app for mobile wallet can store the private keys for your Bitcoin addresses, and enable people to pay for things directly with mobile phone. Android-based Bitcoin wallets, Mycelium, Xapo and Blockchain are examples of Mobile wallets which keeps bitcoin keys encrypted on phone and backed up on a web-based server.

C. Online Wallets

Online wallets store user's private keys online, on a computer controlled by someone else and connected to the Internet. Several such online services are available and some of them connect to mobile and desktop wallets replicating user's addresses between different devices that the user own. The user can access online wallets from anywhere regardless of which device the user has. Coinbase, Circle are examples of online wallets.

D. Hardware Wallets

Hardware wallets are dedicated devices that can hold private keys electronically and proceed the payments. The Trezor hardware wallet is an example of hardware wallets. The compact Ledger USB Bitcoin Wallet uses smartcard security.

E. Paper Wallets

Paper Wallets generate a Bitcoin address for user and create an image containing two QR codes. One is the public address that the user can use to receive Bitcoins. The other is the private key, which the user can use to spend bitcoins stored at that address. The private keys are not stored digitally anywhere. Thus it protects from standard cyber attacks or hardware failures.

III. WORKING OF BITCOINS

When Bitcoin wallet is installed, first Bitcoin address of user is generated **[7]**. This address can be given to other person to pay. User has many different Bitcoin addresses but a unique address should be used for each transaction. The unique address for each transaction of a user is generated by Bitcoin softwares and websites when the user creates an invoice or payment request each time. [8]

Bitcoins are generated after a block of data is processed. It creates a block of transactional data in the bitcoin network .Bitcoin network is a block chain which is a shared public ledger of bitcoins transactions. Bitcoin uses SHA-256 encryption for both its Proof of Work system and transaction verification. The security of the bitcoin protocol lies in the transaction blockchain [15]. All confirmed transactions are included in the block chain. Bitcoin wallets can calculate their counter balance. New transactions can be verified that are owned by the spender. Bitcoins are considered spent once a transaction has been verified. Cryptography is applied for integrity and the chronological order of the block chain.

A transaction between Bitcoin wallets is included in the block chain. Bitcoin wallets store the private keys that is needed to access a bitcoin address and spend the funds. This *private key* is to sign transactions which is a mathematical proof for they have come from the owner of the wallet. The *signature* also prevents the transaction from being changed by anyone once it has been executed. All transactions are broadcast between users and confirmed by the network within 10 minutes through a Bitcoin *mining process.*

*Bitcoin m*ining is defined in the protocol, implemented in software, and is an important function in managing the Bitcoin network. Mining verifies transactions, prevents double spending, collects transaction fees and creates the money supply [9]. Bitcoin mining is the process of adding transaction records to public ledger Bitcoins for past transactions. This ledger of past transactions is called the block chain as it is a chain of blocks. The block chain helps to confirm that transactions have taken place to the rest of the network[10].

IV. ADVANTAGES AND DISADVANTAGES OF BITCOINS

Bitcoins have advantages such as payment freedom, control and security, Information is transparent , Very low fees. They are as described below[11].

1. With Bitcoins, user has freedom for payment. The user can get and send money anywhere anytime. The user do not have limitations like bank holidays and the place where he has to transfer the money.
2. Merchants cannot charge extra fees on anything without talking with the consumer prior to adding any charges.
3. Payments in Bitcoin are done and confirmed without personal information of a user being tied to the transactions. Thus Bitcoin protects against identity theft.
4. Bitcoin can be backed up and encrypted to ensure the safety of a user's money.
5. Public ledger or block chain makes it hard for one to cheat anyone in Bitcoin. So with Bitcoins merchants are able to do business where fraud risk is high.

Along with advantages Bitcoins have disadvantages such as lack of awareness and understanding, risk and volatility, still developing. They are described below.

1.People are unfamiliar with digital currencies and Bitcoins. They should be educated about Bitcoins so that they will be able to use it to their lives. Introductory lectures, advertising can help to spread the knowledge about Bitcoin. Businesses are accepting bitcoins but the list is relatively small compared to physical currencies.
2. User can lost his Bitcoin wallet. Bitcoins can be lost and can not be recovered. If a hard drive crashes or a virus corrupts data, the wallet file is corrupted. These coins will be orphaned in the system. This can destitute a rich Bitcoin owner within seconds with no way to recovery.
3. The value of Bitcoin is constantly changing according to demand. This constant change in price will cause Bitcoin accepting sites to continually change prices. It causes a lot of confusion if a refund for a product is being made. For example, if an Item A is initially bought for 2.0 BTC, and returned a week later, should 2.0 BTC be returned, even though the price has gone up, or should the new calculated amount be sent? Which currency should BTC be tied to when comparing valuation? These are important questions that the Bitcoin community has not overcome yet.
4. When goods are bought using Bitcoins, and the seller doesn't send the promised items, the transaction can not be reversed. Third party escrow service like ClearCoin can solve this problem but escrow services considers the role of banks resulting Bitcoins to be similar to a traditional currency.
5. Bitcoins are virtual currency so cannot be used in physical stores. Cards with Bitcoin wallet information stored in them have been proposed, but because of multiple competing systems, merchants found it unfeasible to support all Bitcoin cards and therefore Bitcoins always have to be converted to other currencies.

V. SECURITY THREATS TO BITCOINS

There are security threats to Bitcoins as well as Bitcoin wallets as described below [15].

A. Attacks to Bitcoin Wallets

Bitcoins are stored in wallets. Wallets contain a public key that is used to receive bitcoins similar to a bank account number. It also contains a private key that is used to verify that you are indeed the owner of the bitcoins you are trying to spend.

Wallets are usually stored digitally either locally or online. Bitcoin wallets can be printed out and stored on paper on which user's private and public keys are printed. These are the paper wallets.

In hardware wallets the key data is stored in a protected area of a microcontroller. They are immune to software and viruses that can steal wallets stored on normal computers.

B. Double Spending

It is possible to spend the same bitcoins twice. The

action is known as double spending. This can be done by different ways. If a merchant doesn't wait for transaction confirmation, the attacker sends two conflicting transactions into the network and Bitcoins are spent two times by attacker. Another way is to premine one transaction into a block and then spend the same coins, before releasing the block into the blockchain.

C. Pony Botnet

Criminals used a botnet known as Pony to infect a large number of computers from Sept 2013 to Jan 2014 and stole up to $220,000 worth of bitcoins and other cryptocurrencies. It also have stolen more than two million passwords and stored them on a server owned by the hackers. The computers on which the wallets were stored locally were Internet connected devices.

D. 51% Attack

This is bitcoin network's most dangerous weaknesses. When an individual or a group of individuals owns more than 50% of the computing power within the bitcoin network, the network is opened up to the possibility of a 51% attack. The advantage in computing power can be used to fork the main transaction blockchain and do fraud, including the double spending attack.

VI. Bitcoins in India

Unocoin, Coinsecure, BTCXIndia are Bitcoin Wallet provider companies in India[18][19][20]. Unocoin provides a Bitcoin wallet by which a registered and verified user can trade, transact with, accept and store bitcoin. The user can send bitcoin to his friend's email address who may not have an Unocoin wallet, request bitcoin from a friend who may not have an Unocoin wallet. It also has address book option to store multiple wallet addresses and also can generate paper wallets. User can top-up mobile/DTH directly from Unocoin account by paying through bitcoin. Further, Coinsecure, BTCXIndia in India provides bitcoin exchange service that allows buyers and sellers to buy and sell bitcoins in exchange for Indian rupees. Zebpay bitcoin mobile wallet not only provides trading of the currency but also can be used for payments. Users can buy vouchers of Amazon, Flipkart, Freecharge, Bookmyshow and Makemytrip. Also, users can recharge their prepaid or pay for their postpaid plans with telecom operators such as Vodafone, Airtel, Uninor, Tata Docomo, Reliance, BSNL and MTNL using Zebpay Wallet. Bitcoins are used not only for online shopping, recharge and fund transfer but also used to pay school fees. Dharwad International School in Karnataka introduced bitcoins as an online payment facility for school fee this academic year. Bitcoins can be bought using Paytm and mobiKwik [22]. India is the fourth most likely nation in the world for mass adoption of Bitcoin, behind Argentina, Venezuela and Zimbabwe [23].

VI. Conclusion

Bitcoins are the cryptocurrencies in which bitcoins are transferred like an email from buyer to seller. The user can transfer bitcoins to his friend or family members. Bitcoins can be used to recharge mobile vouchers, to book tickets and even to pay school fees. There is no transaction fees and if it is applied only after talking to the buyer. These bitcoins are stored on mobile devices, desktop computers or taken as a hard copy on paper. Bitcoin wallets secures Bitcoins and transactions by using public key and private keys. The received Bitcoins can be converted into cash amount at market places or individuals or Bitcoin ATMs. In E-commerce and M-commerce money transfer is the instruction which is executed using credit or debit cards and bank. In Bitcoins no bank is involved in the process.

Its a peer to peer transaction system. Every spent Bitcoin with its transaction history is recorded in the blockchain. It takes 10 minutes for this mining process. After that the user get confirmation of payment. If these ten minutes confirmation period is reduced, the chances of attacks such as double spending attack can be reduced. The value of Bitcoin depends on market and traded like stocks. If values of Bitcoins is increased, a small invester can get good a profit. The user can enjoy the fact that his money is doubled in his pocket automatically. Thus Bitcoin is a virtual currency which allows the cashless transactions to the user like the transactions which are carried out using Internet banking on computers and mobile devices . But in Bitcoin wallets use of credit, debit cards and bank is excluded. Bitcoins are used in the transactions which the user has bought from market places and Bitcoin ATMs. Thus Bitcoin transactions can be developed further so that it can be used in E-commerce and M-commerce. Considering the all features, Bitcoins can be the alternate way for financial investment.

REFERENCES

[1] Lauren Gloudeman, "Bitcoin's Uncertain Future in China ", USCC Economic Issue Brief No. 4 , May 12, 2014.
[2] Vasudha Kapil,"BitCoin: A New Paradigm in E – Commerce", International Journal of Advanced Research in Computer and Communication Engineering , Vol. 3, Issue 9, September 2014.
[3] Philip Godsiff, "Bitcoin: Bubble or Blockchain?, Agent and Multi-Agent Systems: Technologies and Applications", pp 191-203, 10.1007/978-3-319-19728-9_16 ,Print ISBN 978-3-319-19727-2, Online ISBN 978-3-319-19728-9, Series ISSN 2190-3018 Publisher Springer International Publishing.
[4] Adrian Blundell-Wignall, "The Bitcoin Question: Currency versus Trust-less Transfer Technology",https://www.oecd.org/daf/fin/financial- markets/ The-Bitcoin-Question-2014.pdf
[5] "Defination of Bitcoin",https://www.Techopedia.Com/definition/ 27193/bitcoin
[6] http://www.coindesk.com/information/how-to-store-your-bitcoins, "How bitcoins are generated".
[7] "How bitcoins works", https://bitcoin.org/en/how-it-works#balances
[8] Bitcoin Address,https://en.bitcoin.it/wiki/Address#A_Bitcoin_address_ is_ a_single-use_token
[9] Bitcoin Mining, ""Introduction to Bitcoin Mining A Guide For Gamers, Geeks, and Everyone Else", http://euro.ecom.cmu.edu/ resources/elibrary/epay/ IntroductiontoBitcoinMiningSterry.pdf "
[10] "Bitcoin mining", *https://www.weusecoins.com/en/mining-guide*
[11] "Advantages and Disadvantages of Bitcoins", https:// coinreport.net /coin-101 advantages-and-disadvantages-of-bitcoin
[12] "Bitcoin Disadvantages", http://cs.stanford.edu /people/eroberts/ cs201/projects/2010-11/DigitalCurrencies/disadvantages/index.html
[13] "Security Concerns and Issues for Bitcoin", Chinmay A. Vyas, Munindra Lunagaria, International Journal of Computer Applications® (IJCA) (0975–8887) National Conference cum

Workshop on Bioinformatics and Computational Biology, NCWBCB-2014

[14] "Scope of Bitcoins in India", Pinank Shah, Neel Shah, Harsh Trivedi, International Journal of Engineering and Technical Research (IJETR)ISSN: 2321-0869, Volume-2, Issue-10, October2014

[15] "Security Threats to Bitcoins", http://www.hongkiat.com/blog/bitcoin-security/

[16] "Bitcoin Buying and Selling", https://en.wikipedia.org/wiki/Bitcoin# Economics

[17] "Bitcoin Users in India", http://www.indiabitcoin.com/the-rising-trend-of-bitcoin-in-2015-newsbtc

[18] "Unocoin", https://www.unocoin.com/how-it-works.

[19] "BTCXIndia",https://btcxindia.com/terms-conditions

[20] "Coinsecure", https://coinsecure.in

[21] "what-are-bitcoins",http://www.businesstoday.in/ moneytoday /stocks/what-are-bitcoins-their-use-function-and-more/story/194425.html

[22] "Buy bitcoins using Paytm and mobiKwik with Indian Rupee (INR) ", https:// localbitcoins.com /ad/157592/ purchase- bitcoin-paytm-and- mobiqwik-india.

[23] "India's Bitcoin use set to surge in 2016", http://www.redherring.com/finance/indias-bitcoin-use-set-surge-2016/

[24] "BasicBuildingBlocksofBTC",http:// bitcoinchaser. com /bitcoin-units-and-denominations