ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 9, September 2014

BitCoin: A New Paradigm in E - Commerce

Vasudha Kapil

UG Scholar, Department of CSE, UTU (Uttarakhand Technical University), Uttarakhand, India

Abstract: Electronic commerce (e- commerce) is generally known as doing business or trade using internet. It is a business model which facilitates the business or a firm to do business electronically. Bitcoin is a digital currency which allows transaction to be performed without banks or any other centralized system. Bitcoin enables person to transfer money without any transaction fee. Our paper is a study to analyse the advantage and disadvantage of bitcoin if it is being used in e-commerce in place of real money.

Keywords: E-commerce, bitcoin, digital currency, bitcoin mining

I. INTRODUCTION

E-commerce operates in all four of the major market segments: B to B (business to business), B to C (business to consumer), C to C (consumer to consumer), and C to B (consumer to business). Bitcoin is an electronic payment system, which is based on cryptographic proof this payment system need not any single administrator. Bitcoin is also referred as *virtual currency, crypto-currency or digital currency.*

Figure1 (physical) Bitcoin.

A bitcoin address is a single-use token like e-mail addresses you can send bitcoins to a person by sending one of their addresses, unlike e-mail addresses user have many different bitcoin addresses and a unique address should be used for each transaction to be made. When each time you create an invoice or payment request, bitcoin software and websites helps in generating a brand
new address. For example, using *Bitcoin-Qt,* user can click "New Address" and a new address will be assigned. It is also possible to get a Bitcoin address using an account at online wallet service.

An example of a Bitcoin address is *3J98t1WpEZ73CNmQviecrnyiWrnqRhWNLy*.

1.1 The block chain

As every bitcoin is spend, that bitcoin transaction is recorded permanently in a public distributed ledger, is called block chain. As a block is added to the block chain it is published or broadcasted to all network nodes. As every record of bitcoin is recorded it prevents double-spends in a peer to peer environment. The block chain is the only place where the bitcoins exist. To verify the ownership of chain bitcoin software stores its own copy of the block chain.

1.2 Mining

Maintain of the block chain is called *mining, miners are* rewarded with transaction fees and newly created bitcoins. Miners may be anywhere in the world, whose work is to verify each transaction as valid and adding it to the block chain. As of 2014, payment processing is rewarded with 25 newly created bitcoins per block added to the block chain. A special transaction known as *coinbase* is included with the processed payments, as a reward. Such *coinbase* transaction is traced back all bitcoins in circulation. The bitcoin protocol specifies the

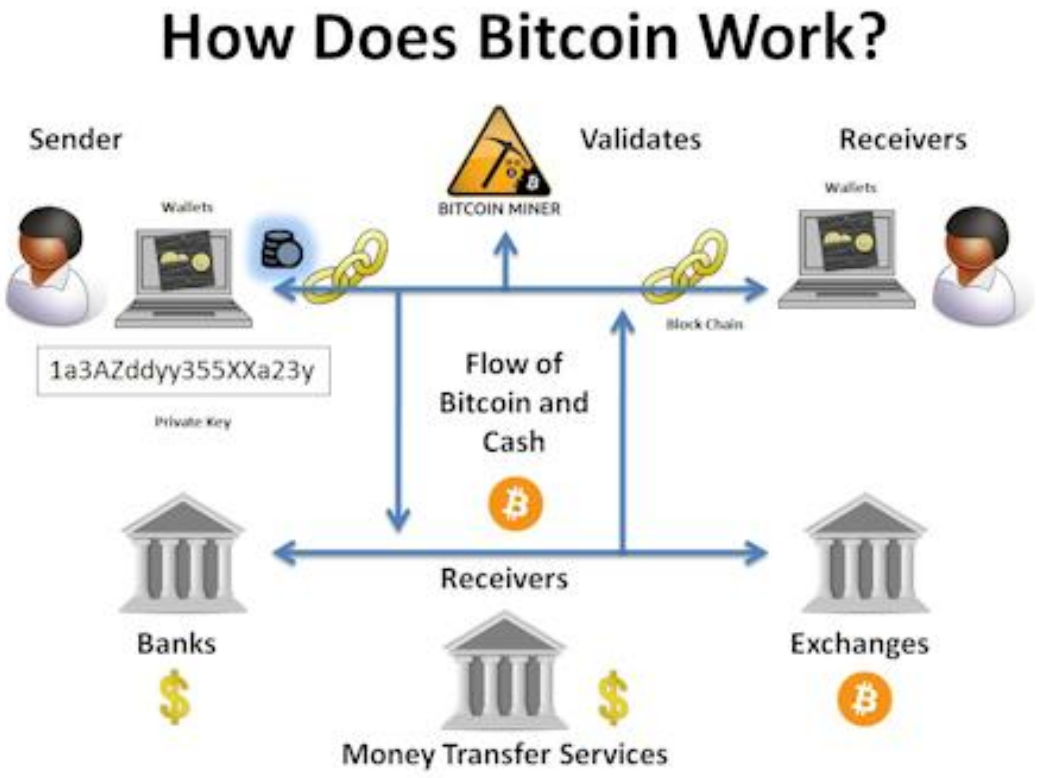
ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 9, September 2014

reward for adding a block in block chain will be halved approximately every four year. The reward will be removed entirely when an arbitrary limit of 21 million bitcoins is reached and transaction processing will then be rewarded by transaction fee only.

Figure 2 Bitcoin mining

2. WORKING OF BITCOIN



The working of bitcoin is similar to the email working. Once bitcoin wallet is installed on computer or mobile phone, first Bitcoin address is generated to the user and thus you can create more addresses when you need one. The address can be disclose to your partner to whom you want to pay or vice-versa.

BALANCE- *BLOCK CHAIN*

All valid transactions made by users are added in the block chain. The block chain is ledger which is publically shared. Bitcoin wallet can calculate user's spendable balance and new transactions are verified to the spender. The cryptography is used to enforce the integrity and the chronological order of the block chain.

TRANSACTION-*PRIVATE KEY*

To apply a security constraint bitcoin wallet keep *private key or signature*, which is use to provide proof to its user that the transaction has come from the owner of the wallet. A transaction is a transfer of value between bitcoin wallets that are the part of the bitcoin chain.

PROCESSING-*MINING*

To make money from bitcoin mining, hire a mining computer such as a server for website hosting.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 9, September 2014

Various bitcoin profit calculator are available online.
Profit is depend on –
1. Value of bitcoin.
2. Change in mining difficulty.
The work of miners is to collect the transaction on the network such as ”Ram pays Shyam 20 Bitcoins” and “Alisa pays Riya 8.9 bitcoins” into the bundles ,known as *blocks.* As there is no central authority the blocks are strung together into one continuous record known as *block chain.* Block chain restricts conflicts in transactions otherwise people would be able to sign the same bitcoin to two different receiver, it is like we are writing a cheque more than amount in current account.

The mining process includes following some tasks:
Bitcoin miners runs computer program on a specialised hardware that handles the process of securing the network.

The software does:
1. Collects transactions from the network made by users.
2. Provide validation to them and discard conflicting ones.
3. Transactions are put into bundles called blocks.
4. Computes cryptographic hashes again and again until which is good enough to count in block.
5. Then miner submit the block to the network add it to the block chain and earn a reward in return.

3. HOW TO MAKE MONEY USING BITCOINS

Bitcoin has the value at present each coin is worth $869.61 and the total dollar value of existing bitcoins is almost $11
Worldwide.
Unlike the traditional currency you cannot hold it your hand like precious metals, bitcoins are outside of national control.

->how to buy bitcoin
1. Bitcoins can be get by accepting them as payment as services or goods.
2. from a friend or someone near to you.
3. Directly from an exchange with your bank.
This is depend on where you are living.
Coinbase, Circle, Trucoin and coin.mx all offering purchase bitcoin through cards.

->Various sites are available to calculate profit:
http://blockchained.com/profit/.
http://www.bitcoinx.com/profit/

->First things first, before buying or selling you must know what the price is. There are many great indexes to see the price, here are some of them:
- http://www.coindesk.com/price/
- http://winkdex.com/#/

->After you know the price, you need a place to buy and sell your Bitcoins. There are some good and not so good options out there, here are a few:
- https://www.bitstamp.net/
- https://www.kraken.com/
- https://www.bitfinex.com/

Once you have created and funded an account in one or more of the exchanges, you need to learn when to buy and sell. To know when you need to buy or sell you have to have an idea of what is happening in the market. Whether the price is rising or falling, if we are in a bearish market (down trend) or a bullish market (up trend), etc. To find out this information you have to look at market data or charts as their called in the investment world. Here are a few:
- “https://bitcoinity.org/markets”.
- “http://bitcoincharts.com/markets/”.

4. Bitcoin in different countries:-few governments have move to regulate bitcoin. According to the European central bank, traditional financial sector regulation is not applicable on bitcoin payment system because bitcoin does not include traditional financial actors. Under other governments, existing rules have been extended to include bitcoin and bitcoin companies.

China	China restricted bitcoin exchange for local currency in December 2013. On 10 April 2014 the People’s Bank of China ordered banks and all third-party payment services to stop dealing with the bitcoin business.
Hong Kong	Pre-existing Hong Kong law covers acts of fraud and money laundering involving virtual commodities (digital coins or bitcoins).
India	After the Reserve Bank of India warning in December 2013, a number of bitcoin operators shut their shops, the legality of Bitcoin is in doubt in India. The Reserve

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 9, September 2014

	Bank of India has cautioned users of virtual currencies about various legal risks.
Jersey	After island leaders expressed a desire for Jersey to become a global center for digital currencies or bitcoin. The first regulated bitcoin fund was established in Jersey in July 2014, which is approved by the Jersey Financial Services Commission.

5. ADVANTAGES AND DISADVANTAGES OF BITCOIN

Advantages:

Transparent:
All information about bitcoin money supply itself is available on the block chain for anybody to verify and use. No individual or organization can control the Bitcoin protocol because it is cryptographically secure. This allows the bitcoin to be trusted as it is completely transparent and predictable.

Secure: Bitcoin payment bitcoin users are in full control of their transaction is made without personal information tied to the transaction. This offers strong protection against identity theft. It is impossible for merchants to force unwanted or unnoticed charges from merchants as can happen with other payment methods. Bitcoin users are in full control of their transactions. Bitcoin users can also protect their money with encryption and by keeping copy or backup.

Risks are few for users: Bitcoin transaction are irreversible, secure and do not contain customer's sensitive or personal information, thus protects users from losses caused by fraud. Merchants can easily expand to new markets where either credit cards are not available. Bitcoins results lower fees, larger market and fewer administrative costs.

Payment at any time: it is possible with bitcoin to send and receive any amount of money instantly anywhere in the world at any time. No bank holidays, no imposed limits. Bitcoin allow its user to be full control over their money. Low fees: bitcoin payments are currently processed with either small fees or no fees. Users may include fees with transaction to receive priority in processing, which results in faster transaction confirmation of transaction by the network. As the services based on Bitcoin, they can be offered for much lower fees than with PayPal or credit card networks.

Disadvantages:

Acceptance level: Many peoples are unaware of Bitcoin. Every day, more business accept bitcoins because they want to take the advantages of this, but this list bitcoin acceptance is small and need to grow in order to gain benefit from network effects.

Under development: Bitcoin software has incomplete features. New features and tools are being developed to make bitcoin more secure and accessible to the large users. Most bitcoin businesses are new and offers no insurance. In general, Bitcoins is in under the process of maturing.

Risk involved: Bitcoin has volatility mainly due to the fact that the demand for Bitcoin is increases by each passing day and there is limited amount of coins. Bitcoin price will goes on settle down as more trading centres, media, businesses begin to accept Bitcoin. Bitcoins price bounces every day.

Lack of awareness: peoples are unaware about bitcoins and need to be educated about bitcoin to apply it to their lives. Network of Bitcoin need to be spread around the world.

6. WHY USE BITCOIN?

Fast:
When we pay a check from one bank to another bank, the bank often taken that time to clear (If a cheque is in a foreign currency we have to pay charge for converting it into sterling. that cheque. Cheques in a foreign currency returned to the country where they were drawn in order to clear. Bitcoin transactions however are generally faster .transaction can be instantaneous if they are "no confirmation", means that merchant may take the risk of accepting a transaction that has not yet been confirmed by block chain. Or, they can take around few minutes if a merchant needs to confirm the transaction. Still it is faster than any bank transfer.

Cheap:
Credit card and debit card transaction are instantaneous but we have to pay for that

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 9, September 2014

privilege. Bitcoin transaction fees are free in some cases or it is minimal

No interference of central government:

No central authority has control on bitcoins so no bank take it away from you.

People can't steal your private information: nowadays online purchases are done using credit cards and online forms require you to enter all your secret information like expiry date, CSV (comma separated values) number, credit card number into a web form. This is not a secure way to do online business and chances that credit card number being stolen.

In bitcoin transaction there is no need to provide any secret information as it provides two keys: public key and a private key, public key can be seen by any one (as bitcoin address) and private key is secret. When we need to send a bitcoin we "sign" the transaction by combining both public and private keys together and apply some mathematical function to them which certifies that it came from you.

Not inflationary: The problem with regular currency is that government can print as much as they like and the do it when there are not enough US dollars to pay off the national debt, then simply Federal Reserve print more currency. Injection of such newly created money in market by government causes the value of currency to decrease.

Increase currency in market means inflation as if double the dollars in circulation in market then it means there are two dollars now while before there was only one dollar.

Example: - Person who is selling a product for one dollar will have to increase its price to two dollar to make worth as he has before thus the value of dollar become half. This is called inflation which results in increment in price of goods and services; inflation in very difficult problem to control which is still a big problem of various underdeveloping countries and also it decreases the purchasing power of ones. Bitcoin was designed to have a maximum number of coins. Under original specification this is define that 21 million will ever be created this means that after that the number of bitcoin cannot be produce so inflation is not a problem here. While deflation which causes when the price of goods or services falls, is exist in bitcoin world.

Bitcoin are private as anybody want:

Most of us do not want that anybody come to know that what we have purchased. Bitcoin is a private currency as well transparent to the block chain. But through the block chain everybody knows that where the transaction is being made and from where it come from. Unlike conventional bank accounts, no one knows who holds the particular address as private information is kept secret. It is similar to clear plastic wallet but no owner is visible; everyone can look inside but no one knows whose address it is. But this would be if we want to point out those people who use bitcoin unwisely such use same bitcoin address or combining coins from multiple addresses into a single address.

It is owned by itself:

It is not like other electronic cash system in which our account is owned by someone else.

With Bitcoin, user own the private key and the corresponding public key through which user get the address.

No one can take that away from user unless user loses itself.

Make money your own: As per the above mentioned procedure of "how to make money" anybody can make their own money.

REFERENCES

[1] Satoshi Nakamoto, "*Bitcoin: A Peer-to-Peer Electronic Cash System", satoshin@gmx.comwww.bitcoin.org*

[2] Luis Garicano and Steven N. Kaplan, "THE EFFECTS OF BUSINESS-TO-BUSINESS E-COMMERCE ON TRANSACTION COSTS", NATIONAL BUREAU OF ECONOMIC RESEARCH 1050 Massachusetts Avenue Cambridge, MA 02138 November2000.

[3] R.C. Merkle, "Protocols for public key cryptosystems," In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pages 122-133, April 1980.

[4] D. K. Gangeshwer, "E-Commerce or Internet Marketing: A Business Review from Indian Context", International Journal of u- and e-Service, Science and Technology Vol.6, No.6 (2013), pp.187-194http://dx.doi.org/10.14257/ijunesst.2013.6.6.17.

[5] M. Babaioff, S. Dobzinski, S. Oren, and A. Zohar. On bitcoin and red balloons. In The 13th ACM Conference on Electronic Commerce, pages 56–73. ACM, 2012.

[6] J.Bruce. Purely p2p crypto-currency with finite mini-blockchain (white paper) https://bitcointalk.org/index.php?topic=195275.0.

[7] E. Androulaki, G. Karame, M. Roeschlin, T. Scherer, and S. Capkun. Evaluating user privacy in bitcoin. IACR Cryptology ePrint Archive, 2012:596, 2012.

[8] F. Reid and M. Harrigan. An Analysis of Anonymity in the Bitcoin System. In Security and Privacy in Social Networks, pages 197–223. Springer New York, 2013.

[9] D. Ron and A. Shamir. Quantitative Analysis of the Full Bitcoin Transaction Graph. In Proceedings of Financials Cryptography 2013, 2013.

[10] B. P. Eha. Get ready for a Bitcoin debit card. CNNMoney, Apr. 2012. money.cnn.com/2012/08/22/technology/startups/bitcoin-debit-card/index.html.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 9, September 2014

[11] E. Androulaki, G. Karame, M. Roeschlin, T. Scherer, and S. Capkun. Evaluating User Privacy in Bitcoin. In Proceedings of Financial Cryptography 2013, 2013.
[12] T. Moore and N. Christin. Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk. In Proceedings of Financial Cryptography 2013, 2013.