International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 1 | Issue – 5

A Glimpse towards Bitcoin and its Reality Analysis on Mining and Protocol

K. Vinitha
Ph.D. research Scholar, School of Management Studies,Vels University, Chennai, India

Dr. S. Vasantha
Professor& Research Supervisor, School of Management Studies, Vels University, Chennai, India

ABSTRACT

Bitcoin has advanced as the most fruitful cryptographic currency in history. Since its launch in 2009.Bitcoingrewtocomprisebillionsofdollarsofeconomic value. Since then a lot of literature has been identified with concealed-but-vital properties of the system, exposed attacks, proposed promising alternatives, and singled out difficult future challenges. This paper threw light to many related cryptocurrencies or 'altcoins' and enables a more insightful analysis of Bitcoin's properties. The researcher maps the space for providing analyses for bitcoin mining, bitcoin protocol, and bitcoin value determinations.This paper surveys the anonymity in Bitcoins and provides an insight into the framework for analysing the mining hardware, the calculation of Bitcoin value by reviewing various literatures and websites related to Bitcoins.

Keywords: *Bitcoins, Cryptocurrency, mining.*

INTRODUCTION

Bitcoins was launched as an open source software in 2009. Its creator is identified by the name Satoshi Nakamoto. Nakamoto published a paper entitled "Bitcoin: A peer to peer Electronic cash system" in 2008. The pioneer exchange of Bitcoins the Bitcoins Market, open in February 2010 another exchange was also opened in July of the same year which is MtGox.The pioneer bitcoin exchange which was designed and built in India was BTCXIndia. The exchange followed KYC and AML guidelines, and it allowed instant INR (Indian rupee) deposits and withdrawals, BTCXIndia was forced to wind up by their bank, thus bringing a closure to longer services bitcoin businesses. The reason behind is anonymous whether the cause was because of perceived risk or it was a usual ban by the management[9]. A software developer called Satoshi Nakamoto proposed bitcoin. It is based on mathematical proof. He developed Bitcoin the focus behind it is to introduce a currency which works autonomous of any central authority, and is transferable electronically, and which gets transacted instantly, with an economical transaction charges. Bitcoin helps to secure a multibillion-dollar global market of anonymous transactions without any governmental control. As per Government of India incomes from investments are taxable. Hence it is obvious that Bitcoin investments are also taxable. The tax rate is 30% for short-term investments and around 20% for long-term (3 years) for the capital gains.So, it must deal with many regulatory issues involving national governments and financial institutions. Since its inception, bitcoin, a virtual currency, has grown in both its popularity and its use. Despite this, there still exists a relative scarcity of economic analysis in academia about this new economic phenomenon. Various topics have been researched regarding bitcoin, including its economic status as a currency [13], the incentives of bitcoin miners [10], the economics of bitcoin exchange prices[11], among others. Macroeconomist Paul Krugman weighed in strongly on the normative side of the economicdebate with his article "Bitcoin is Evil" published in late 2013.

Objectives

To explore the miningprocess of new bitcoins

To find the protocol behind mining of bitcoin

To study the calculation of bitcoin value

Methodology

The study is based on secondary sources of data/ information. Different books, journals, newspapers and relevant websites have been consulted to make the study an effective one. The study attempts to explore the protocol behind mining of bitcoin, and to study the calculation of bitcoin value. The paper also analyse the factors involved in mining of new bitcoins.

Mining of Bitcoins

Bitcoin mining serves for the addition of transactions to the block chain as well as to release new Bitcoin. The process of mining involves collecting recent transactions which must be converted into blocks and the miner should be able to solve the computational problematic puzzle. The one who solves the puzzle first can place the next block on the block chain and he can claim the rewards. The rewards includes the transaction fees paid to the miner which will be in the form of Bitcoin as well as the newly released Bitcoin.

Bitcoins can be obtained through three ways they can be bought from an exchange, accepting them for goods and services, or else mine new ones. For instance, A buys a TV from B with a bitcoin. Inorder to confirm his bitcoin is a genuine one miners will check the transaction. Numerous transactions the miners need to verify it is not just a single transaction. All the transactions are gathered into boxes with a virtual padlock on them which is called block chain. Inorder to search for the key the miners had to run a softwarethat will open that padlockOnce their system finds it, the box opens and the transactions are checked. Inorder to find that key the miners gets a reward of 25 newly generated bitcoins. The number of attempts taken to search for the apt key is around 1,789,546,951.05, according to Blockchain.info which is the topmost site for the newest bitcoin transactions. Even though this many attempts happens, the 25-bitcoin rewards is given out about every 10 minutes.

Private key is a confidential number that ensures the spending of bitcoins. Each Bitcoin wallet has one or more private keys and it is saved in the wallet file. It is mathematically related to all Bitcoin addresses generated for the wallet. A Bitcoin sent to anaddress can be spent by anyone who knows the private key. The private key is needed only to spend the bitcoins. If a private key of unspent bitcoin is compromised or stolen, the value can only be safeguarded if you are immediately spending it to a different output which is secure. You can spend bitcoins only once when it is spent using a private key. [8]

There is no single central authority to control the bitcoin network. Those machines which enter the mining work of the bitcoins forms a part of it and the machines need to work together and else the money keeps on flowing. Storage of each transaction happens in the network in enormous version of a general ledger which is known as the blockchain. Transfer can be done anywhere the time required is only a few minutes just to process the transaction.Once the bitcoins are sent there is no way of getting it back or else the recipient should return them to you. Bitcoins are not printed physically as in the case of physical money where it is printed with the authority by a central bank, and it is unaccountable to the population and creates its own rules[8]. Bitcoins are created using digital technologies by a group of people and in that group any one can join. This is mined using computing power in a distributed network. Base of Bitcoin is the mathematics formula is used for the production of bitcoins. Bitcoins are not under the control of any central Bank or Government which allows the owners to employ bitcoins anonymously. These are mined it does not have physical existence like coins or notes. These can also be subscribed from exchanges by converting US dollars and with other currencies.Anyone can become a Bitcoin miner if he is able to run a software with a specialized hardware. These mining software will listen for the transactions which are broadcasted through the peer to peer network and it will perform the accurate function in order to carry out the transactions. For any new transactions inorder to get it confirmed they have to be included in a block which has to be followed with a mathematical proof of work. The proof of work is not an easy task . Inorder to get that proof of work billions of calculations per second need to be tried. If the blocks are to be accepted by the network the miners must perform these calculations.When more number of people started to mine, the process to finding valid blocks automatically tend to increase by the network inorder to make sure that the average

time to find a block remained equal to 10 minutes. Inshort, we can say that mining is a very competitive business where no one can regulate what is included in the block chain. The proof of work is so designed as it should be subject to the preceding block inorder to maintain a chronological order in the block chain. This is actually a difficult task to reverse the preceding transactions because it requires to recalculate the proof of work of all the succeeding blocks. When simultaneously two blocks are created the miners will function on the first one and will in turn move to the longest chain of blocks as soon as the succeeding block is found. Thus, mining is protected and thereby maintains a global harmony. Cheating by the individuals included in the network by the way there as to increase their reward alone or if they are performing any fraudulent transactions thereby to corrupt the Bitcoin network is not at all possible as the Bitcoin nodes will reject the block which consists of invalid data according to the rules framed in the Bitcoin protocol.[9]Users can spend bitcoins anonymously. It is not tied to a bank or Government. Exchange of bitcoins are also possible with US dollars and other currencies. Bitcoins when they are transmitted from one user to the next user they are digitally signed each time they are just lines of compute code[1].

When the bitcoins are converted into currency the owner of the bitcoins can be traced. Until then the transactions and accounts can be traced. Now the ransomware attack accounts remains untouched as it is a hard task for the perpetrators to cash in.[2] The bitcoins work on the basis of lines of computer code that need to be signed digitally every time they need to be transmitted from one user to the other. As the transactions can be done anonymously libertarians as well as tech enthusiasts, speculators, perpetrators and criminals made the currency popular.Tom Bossert, President Donald Trump's adviser for homeland security and counterterrorism, said that less than $ 70,000 has been pooled in ransomware attacks, there are still more unidentified accounts other than the three known accounts.

Miners pour the transactions into a blockchain which runs the tally of each bitcoin transaction. Prevention of multiple spending of bitcoins are restricted by blockchains. Miners gets the reward of bitcoins for their effort. Bitcoin came into existence in 2009 by an individual or group of individuals operating under the name Satoshi Nakamoto. An internal logic existed behind the functioning of bitcoins. New blocks are added to the blockchain through mining thus it makes the history of transactions difficult to amend. There are two forms of mining.

Solo mining Here the miner makes an attempt to create new blocks of his own, for his job he will be rewarded with proceeds from the block reward and also the transaction fees also goes fully to him. This allows him to get large payments.

Pooled mining when the miner pools resources with others inorder to find blocks more often with the proceeds shared among the pool miners in rough correlation to the amount of hashing power they each contributed, here the miner receive only small payments.

Creation of newbitcoins

The process of mining paves the way for new bitcoins by the network. In this process the mining nodes on the network are awarded with bitcoins each time when they find the solution to a mathematical problem and as a result they can create a new block. Creating a block is thus a proof of work. The proceeds inorder to solve a block is automatically adjusted, so that every four years of operation of the network, half the amount of bitcoins created in the prior four years are created. An extreme of 10,499,889.80231183 bitcoins were formed in the first 4 (approx.) years from January 2009 to November 2012. Every four years thereafter this amount halves, so it should be 5,250,000 over years 4-8, 2,625,000 over years 8-12, and so on. So that the overall number of bitcoins in existence can never exceed 20,999,839.77085749 .

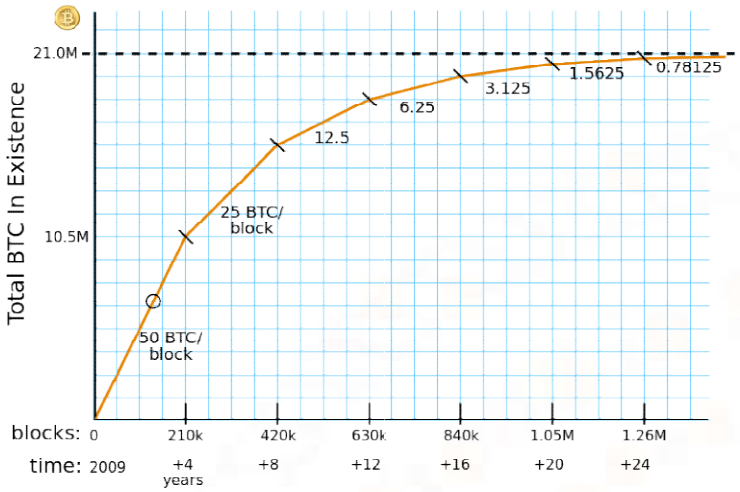
Government takes the decision to print and distribute the currencies in the case of physical cash where as Bitcoins doesn't have a central authority. A special type of software is used to solve the math problems and in return the miners get bitcoins. This really acts as an incentive for the miners and also an encouragement for more people to participate in mining . These Bitcoins are just ledger entries which are not backed by anything like any other currency. Even though they are not backed they are having value which is based on their utility and supply. Where as the inclusion of bitcoins into the money supply is regulated by the software for bitcoin and it is regulated to a predetermined amount and rate of distribution. The cause for the creation of new

bitcoins to be created is two-fold. It acts as a mechanism inorder to introduce bitcoins into the money supply whichis controllable and it happens random. And in other way it acts as an encouragement for people to run the software for mining which will be helpful to secure the entire system.[6]

Anyone can participate in mining for this one should have access to the internet and he should have the appropriate hardware for mining. At the beginning stage of Bitcoins, mining was carried out with CPUs from normal desktop computers. Graphics cards, or graphics processing units (GPUs), proved more efficient in mining when compared with CPUs and asBitcoin became popular, GPUs became dominant. Eventually, hardware known as an ASIC (which stands for Application-Specific Integrated Circuit) was designed specifically for mining Bitcoin. The initial one was released in 2013 . In today's scenario mining became so competitive, it can only be done profitably with the modern ASICs. When using CPUs, GPUs, or even the older ASICs, the cost of energy consumption is greater than the revenue generated. Due to speculation activities, the price may go up further. There are lot of companies which produce mining hardware. Some of the more prominent ones are Bitfury, Hashfast, KncMiner and Butterfly Labs. Companies such as MegaBigPower, CloudHashing, and CEX.io also give customers to lease minig hardware.

Bitcoin protocol

The fact is that you won't be able to mine unlimited bitcoins. There exists a bitcoin protocol which makes the bitcoin to work. In this rule it states that only 21 million bitcoins can be mined. Bitcoin works under a protocol which are the rules which makes the bitcoins to work. In the protocol, it is framed that only 21 million bitcoins can be framed by the miners. Likewise in rupee there are smaller divisions for bitcoins also and it is the one hundredth millionth of a bitcoin. when the algorithm was created under the pseudonym Satoshi Nakamoto – the individual created a finite limit on the number of bitcoins that will ever exist: 21 million. Currently more than 12 million are in circulation. This means that a little less than 9 million bitcoins are yet to be discovered. As per the current rate of creation, the final bitcoin will be mined in the year 2140.



Source: http://www.bitcoinnotbombs.com/bitcoin-mining

Blockreward is the amount of novel bitcoin released with every mined block. The Block reward is halved approximately each four year. The block reward was initiated at 50 bitcoins in 2009, and it is now 25 bitcoins in 2014. Thus, the reduction of block rewards will result in an aggregate release of bitcoin which approaches 21million. As per the existing Bitcoin protocol, 21 million is the cap and nor more will be mined after that number has been attained. According to the current scenario block rewards provides the majority of the incentives for the miners.

Calculation of Value of Bitcoin

Satoshi is currently the smallest unit of the bitcoin currency recorded on the blockchain. It is one hundred millionth of a single bitcoin (0.00000001 BTC). The name of the unit gives homage to the original creator of Bitcoin Satoshi Nakamoto. The amounts in blockchain are denominated in Satoshi before it is converted for display. Each bitcoin is divisible to the eighth decimal place so that each bitcoin can be split into 100,000,000 units. So, each unit of bitcoin is called satoshi. Hence a satoshi is the smallest unit of bitcoin[2].

The value of the Bitcoin is calculated using a formula PB=(SW + TX)/BC

SW=Storage of wealth

TX=Total amount of the Bitcoin used for concurrently transacting in it.

BC=Amount of Bitcoins in circulation

PB=Price of Bitcoin

Thus, we can say that we can calculate the value of Bitcoin which is derived from the total value of the Bitcoin used for storage of wealth(SW) added with the aggregate amount of the Bitcoin required for concurrently transacting in it (TX).The sum of these two numbers divided by the amount of Bitcoins in circulation (BC) (currently 12.2 million, ultimately 21 million), will give you the price of Bitcoin (PB).[7]

Conclusion

Cyber attackers' currency of choice are the bitcoins. Inorder to regain access to the system data the cyber attackers demand payments in bitcoins from the victims. Purchase of goods and services are possible without including the banks, credit card issuers or other third parties. It is not completely anonymous it can be traced when bitcoins are converted into regular currency. Due to bitcoin bandwagon and the outbreak of media coverage some businesses have plunged. For example Overstock.com payment is accepted only in bitcoins. Over 300,000 routine transactions occur through bitcoins thus making it prevalent according to bitcoin wallet site blockchain.info. But when comparison arises with physical money and cards many individuals business won't accept bitcoins for transactions. Anonymity of the users makes the bitcoin popular. Even though all the transactions are recorded in a ledger only the public address is related to the transaction one makes. As it does not contain any identifying information of itself. The users who are sake of this anonymity made the bitcoins popular. This anonymity was utilised by the "darknet" websites for trading illegal commodities such as drugs and weapons. One among the website was "Silk Road" in which the US Government shutdown it in October 2013.[9]

Future research

Other than bitcoins there are a lot of cryptocurrencies available in the market some of them are

- Ethereum
- Litecoin
- Ripple
- Peercoin
- Namecoin
- Quarkcoin
- Zetacoin

Thereby giving space for future research work which in turn can create opportunities to get the public acquainted with the new cryptocurrencies available in the global market.

References

1) http://economictimes.indiatimes.com/articleshow/58694578.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst
2) http://satoshitobitcoin.co/
3) http://www.bitcoinnotbombs.com/bitcoin-mining-101/10
4) http://www.coindesk.com/information/what-is-bitcoin
5) https://bitcoin.org/en/faq#what-is-bitcoin-mining
6) https://bitcoin.stackexchange.com/questions/182/where-do-bitcoins-come-from-and-what-gives-them-their-value
7) https://bitcoin.stackexchange.com/questions/182/where-do-bitcoins-come-from-and-what-gives-them-their-value
8) https://bitcoin.stackexchange.com/questions/29948/why-doc-says-importing-private-keys-is-so-dangerous4
9) https://www.cryptocoinsnews.com/top-10-countries-bitcoin-banned/
10) Kroll, J. A., Davey, I. C., & Felten, E. W. "The economics of Bitcoin mining, or Bitcoin in the presence of adversaries." In Proceedings of WEIS (2013).
11) Miroslava, Rajcaniova, Kancs d'Artis, and Ciaian Pavel. "The Economics of BitCoin Price Formation." EERI Research Paper Series (2014).
12) Power, Mike. "Life after Silk Road: How the Darknet Drugs Market Is Booming." The Guardian, May 30, 2014. Web(2015)
13) Yermack, David. "Is Bitcoin a real currency? An economic appraisal." No. w19747. National Bureau of Economic Research (2013).