Journal of Engineering and Applied Sciences 12 (Special Issue 2): 6215-6218, 2017
ISSN: 1816-949X

Bitcoin: The Future of Money

Shivam Bhatia and S. Chethan
Department of Information and Communication Technology,
Manipal Institute of Technology, Manipal, India

Abstract: We live in a civilized society that thrives on commerce; nothing can be bought for free. Hence, we all value money, some more than the other. Money creates a sense of security; it provides a medium to acquire resources that eventually help us to fulfill everything from our basic needs to our highest accomplishments. Crypto currency is a digital or virtual currency that incorporates cryptography for security. Bitcoin is a form of digital currency, created and held electronically. In this study, we will discuss in detail about the Bitcoins, its benefits and drawbacks and applications of Bitcoins.

Key words: Cryptocurrency, Bitcoin, SHA-256, Hash algorithm, currency, earth

INTRODUCTION

The earth is inhabited by 7.3 billion people of diverse origins. No matter which religion we follow what color our skin is what language, we speak our basic requirements are the same. We need water to quench our thirst, food to satiate our hunger, clothes to wear and a roof over our heads to call home. We live in a civilized society that thrives on commerce; nothing can be bought for free. Hence, we all value money, some more than the other. Money creates a sense of security; it provides a medium to acquire resources that eventually help us to fulfill everything from our basic needs to our highest accomplishments. We spend a major part of our lives trying to make money, some to earn a decent living and pay the bills and others out of this insatiable desire to accumulate wealth. This greed sometimes pushes human beings to a path of destruction, often culminating in criminal activities. The big corporate banks hold the reigns of present world. We have ourselves given money the importance for it to reach a status of omnipotent, omnipresent entity.

The world of banking came down crashing during the financial crisis of 2008. Despite, warnings by leading economists, the wall street and the banking moguls chose to ignore the inevitable. Billions of dollars vanished overnight and the world saw leading = investment bankers taking their own lives. Families were destroyed. Sometimes failure leads us to contemplate. A simple new idea can prevent this from happening again, that's how the concept of crypto currency was born.

"Crypto currency is a digital or virtual currency that incorporates cryptography for security". In 2008, on the day of Halloween, a programmer named Satoshi Nakamoto published his research on m etzdowd.com titled "A Peer-to-Peer Electronic Cash System". In January, 2009, the first Bitcoin Software was released by Nakamoto. This software launched the network and the first units of Bitcoin currency, called Bitcoins. Nakamoto released the Bitcoin Software on Sourceforge on 9th of January, 2009 whose 0.1 Version was compiled using Microsoft Visual Studio.

Nakamoto a 36 years old Japanese man claimed that he had spent more than 1 year of his life writing the software, driven over the anger over the financial crisis of 2008. He wanted to create a currency that was not controlled by banks, monetary policies and politicians. His invention only needed a software which governed it. The software was supposed to release 21 million coins over the span of next 20 years. The coins were distributed every 10 min through a process that resembled a lottery. The people seeking the coins, miners, would play the lottery repeatedly the fastest computer would win most of the money. Interest in Satoshi's investment grew and more and more people dedicated their laptops to the lottery and within no time 44 exchanges popped up which allowed anyone with Bitcoins to trade them for official currencies like dollars or Euros (Davis, 2011).

Despite, a lot of criticisms from various sections of society a tremendous increase in its value was observed between 2009 and 2013. The value of single coin appreciated from 0.1 USD to over 1100 USD. People who had invested in Bitcoin made huge profits in such a limited time period making it probably one of the most discussed economical successes ever in the financial history. This new technology allows everyone in the

Corresponding Author: Shivam Bhatia, Department of Information and Communication Technology,
Manipal Institute of Technology, Manipal, India

world to be their own bank, free from taxes and banking fee. Crypto currency is built on technological computer software with a shared code that connects a global network through the internet. Just like how the credit card companies keep track of money being transferred from one to the another account, crypto currency keeps record of every coin and every transaction made. Since, the number of coins is fixed, no coin ever leaves the system. When a transaction is made what is really being sent some where is the control of database with a code which is a unique key for every transaction. As transactions are made the public distributed database called the block chains/ledger are updated. Each and every user can access the database to keep track of Bitcoins and transactions (CPI, 2014).

MATERIALS AND METHODS

SHA-256 algorithm: SHA-256 is the most widely algorithm used for mining. SHA stands for secure hash algorithm. It is a method designed such that the information does not get altered from its original form. The algorithm is secure because it uses encryption and only the one who has access to the code can use it. The SHA-2 set of algorithm was developed and issued as a security standard by National Security Agency (NSA) of United States in 2001. SHA-256 is an extension to SHA-2 family. The algorithm generates bits that are 256 bits in size, hence the name SHA-256. The algorithm converts data into a 256-bit code. The resulted value obtained is referred to as hash. The processing time for each block varies from 6-10 min (BC, 2017).

To have a clear understanding of the algorithm, the reader must be familiar with a few terms. Firstly, what is a hash? A hash is a function that converts data into number with a specified range. Hash functions are such that predicting the output is unpredictable. The Hash function used in case of Bitcoin mining is SHA-26 applied twice.

Secondly, what do you mean by difficulty level and how does it works? The nature of hash function is quite unpredictable which means that if you put in some random data (the transaction+the random number), it will produce a random number within a certain range. If we further restrict the range of the desired output effect the probability of finding the solution in a single round decreases. As the number of hashes per second increases the difficulty level increases automatically.

Thirdly, what do you understand by the term that the block is mined? When a block has been mined, then the miner who has mined it sends the information and the block to all the miners on the network. The block is send as an evidence that he has found it. As the other miners receive the newly mined block, the miner removes all the transactions that are currently involved in mining the block and broadcasts the block to other miners and they follow the same procedure. The whole procedure happens really quickly. The miner of the block gets a "miner fee" which is a sum of unspent coins in the transaction and a "coin base" reward. The coin base reward halves after every 20 blocks mined and will be miniscule compared to miner's fees the algorithm is as follows:

Algorithm:

Step 1: Retrieve the hash value of the previous block from, the network
Step 2: Obtain a list of transactions known as "block". The transaction list can be obtained from peer to peer network
Step 3: A hash value is calculated for the potential transaction along with a random number
Step 4: If the hash value obtained is more than the current difficulty level, then you have mined the block. If the value obtained is not greater than the difficulty level obtained, you need to start over from Step 1

Let P be the hash of the previously mined block, B be the block of transactions, H be the has function and D be the difficulty level. The Pseudo code for the algorithm is as follows:

- Retreive P
- Construct/modify
- If H (P, B, some random number)>D end
- GOTO 1

RESULTS AND DISCUSSION

Advantages and disadvantages of cryptocurrency: There are different ways through which you can make money. You can work hard and earn it if you are lucky enough then you can find it, steal it if you don't want yourself stuck putting in a lot of efforts.

But if you are Santoshi Nakamoto, a naturally talented computer coder then you can invent it. This is exactly what happened on the eventful night of January 3, 2009 when he sat down in front of his computer and created a totally new currency called Bitcoin. The currency is all about bit, i.e., code and there is apparently no coin. The currency was basically 31 thousand lines of code and an announcement on internet. Bitcoin which was just 31 thousand lines of code in 2009 is now evaluated to be around $1170/coin (Davis, 2011).

Here are some of the advantages of Bitcoins: it's fast consider an example when you pay a cheque from another bank into your bank, it will take several days for money to reflect into our account. Similar is the case with the international wire transfer. These take more time as the banks can't assume that the funds are readily available and can make a transfer as such. Whereas transactions

that are made using Bitcoin are way faster. There are basically two types of transactions supported by Bitcoins, i.e., zero-confirmation and the one that require confirmation. In "zero-confirmation" transactions, the merchant takes the responsibility of the transaction before it is approved by the Bitcoin Block chain. Whereas the one that require confirmation can take around 10 min.

Secondly, Bitcoin security beats dollar security. How many times have you lost $20 note? Ok, now have you lost your computer or digital wallet? Immature people will say a lot of things but let's agree to the fact that this is very less likely to happen. It has been widely accepted fact that loosing paper money is relatively easy. Bitcoins are digital in nature hence can be saved on the server and computers protected by pass codes.

Thirdly, the rapid growth of Bitcoin suggests that it is something widely accepted and a powerful virtual currency. In spite of being open, it permits a degree of user anonymity. Moreover it's free of any transaction fee (SEI, 2017).

Fourthly, it is comes very handy for countries which do not have access to secure banking deposits or international trade. Fifthly, it is very useful in counties where there are issues of fraud counterfeit currency. For instance, after the Somalian State collapsed in 1992 the country was stuck in a state of financial unrest. It became so bad eventually that the world bank estimated that 80% of the currency circulated was forged, reprinted (Darlington, 2014).

There are different ways through which you can make money. You can work hard and earn it if you are lucky enough then you can find it, steal it if you don't want yourself stuck putting in a lot of efforts.

Bitcoin might seem very profitable overall but there are some major roadblocks in its adoption. The illicit activities associated with Bitcoin cover a wide range including sales of illegal drugs, assassinations, money laundering, Ponzi schemes, unlawful gambling, illegal mining and outright theft (SEI, 2017). Apart from all the cons listed above, one of the most important issues that could prevent the countries from adopting Bitcoin is lack of technology. Apart from reliable access to internet from personal computers and mobiles a proper financial technology that accepts Bitcoin as payment is required. Without the network the practicality of Bitcoin will be constrained. Bitcoins then would need to be converted to the local currency which is not conducive to frequent, casual spending. Another issue that is hindering the adoption of Bitcoin worldwide is the concerns raised over the actual infrastructure itself. In February, 2014, a flaw in the Bitcoin code was discovered which allowed people to report fraudulently that transactions had not been successful and led to hemorrhaging money from banks. The coding flaw was taken care immediately but led to loss of millions of coins that were fraudulently withdrawn from companies like Mt.Gox and Bit stamp (the economist) (Darlington, 2014).

Applications of cryptocurrency: Bitcoin which was just a 31 thousand line of code back in 2009 is now evaluated to be $1170/Bitcoin (ILLC, 2017). People who had invested in Bitcoins in the earlier stages turned into millionaires in a span of 23 years. With time, various companies have started accepting Bitcoin. Here are some of the applications of the Bitcoin.

Donations can be made through Bitcoin. It is highly debated topic that only 50% of the donations made reach the intended hands. But, with unique P2P sharing of cyrptocurrency, you can make sure that the money reache the hands of intended. A great example is WikiLeaks which has received around 3557.94535186 Bitcoins from anonymous donations.

There is one of the reknown coffee places in Downtown, Toronto called Snakes and Lattes. This place is a house of enthusiastic crypto fans with the owner accepting the payment in Bitcoin. Even the tourism industry is catching up. Cheapair.com on 22nd November, 2013, announced that they would be the first online travel agency accepting Bitcoin. You can book flights, hotels, car rentals and cruises there.

Even the education sector has started to accept Bticoin. The University of Nicosia based in Cyprus is the first university in the world to accept Bitcoin for tuition and other fees via Bitpay (Holmes, 2014). Even, the Notary service can benefit from the Bticoinblockchain. Bitcoin blockchain can be used as a notary service and data can be attached to transaction record which on a whole turns out to be inexpensive and easy. This can be done using websites like Proof-of-Existance. Com. Applications like uproov helps in notarizing smartphone multimedia immediately after creation.

Bitcoin Block chains store not only the transactions but also store the logic. This means the digital contracts can be written which will make transactions seamless and more or less self-executable if the conditions agreed are met (Gomeshttp, 2016).

CONCLUSION

It is widely accepted fact that "Every coin has two sides" but in case of cryptocurrency the positive side outweighs the negative. Bitcoin which was just 31 thousand lines of code back in 2009 now has market value of $1170/coin. People who had invested in Bitcoin made

huge profits in such a limited time period making it probably one of the most discussed economical successes ever in the financial history. After the financial crisis of 2008, Bitcoin gave people a sense of security. Those who invested in them had a complete control of their investment and the rate of appreciation was something unimaginable. Without fail, Bitcoin stands as one of the strongest contender as the future of money.

REFERENCES

BC., 2017. 7 reasons why bitcoins are better than fiat currencies. Bitconnect.Co., New York, USA.

CPI., 2014. An in-depth look at cryptocurrency mining algorithms. Coin Pursuit inc, Cedar Park, Texas.

Darlington, J.K., 2014. The future of bitcoin: Mapping the global adoption of world's largest cryptocurrency through benefit analysis. Master Thesis, University of Tennessee, Knoxville, Tennessee.

Davis, J., 2011. The Crypto-Currency: Bitcoin and its Mysterious Inventor. New Yorker Publisher, New York, USA.,.

Gomeshttp, P., 2016. Five interesting applications of block chain technology. Edelman, Chicago, Illinois. http://www.edelman.com/post/blockchain-technology/

Holmes, B., 2014. 10 awesome uses of cryptocurrency. Brave New Coin Company, New York, USA. https://bravenewcoin.com/news/10-awesome-uses-of-cryptocurrency/.

ILLC., 2017. Minimize your risk and maximize your profit in up and down markets. Investopedia LLC., New York, USA. http://www.investopedia. com/terms /c/cryptocurrency.asp.

SEI., 2017. The bitcoin mining algorithm from a programmer's viewpoint. Stack Exchange Inc, New York, USA. https://bitcoin. stackexchange. com/ questions/12603/the-bitcoin-mining-algorithm-from-a-programmers-viewpoint.