IJCSE International Journal of Computer Sciences and Engineering Open Access

Review Paper Volume-6, Issue-1 E-ISSN: 2347-2693

Bitcoin:Surveying First Revolutionary Cryptographic Virtual Currency

S.M. Nasti[1*], S.J.Nasti[2], R.Bashir[3], M.A. Butt[4]

[1*]Department of Computer Science and Information Technology, Central University of Jammu, Jammu, India
[2]Department of Computer Sciences, BGSB University, Rajouri, India
[3]Department of Computer Sciences, Islamic University of Science and Technology, Awantipora, India
[4]Department of Computer Sciences, University of Kashmir, Srinagar, India

**Corresponding Author: meshoaibnasti@gmail.com, Mob. +91-9622672022*

Available online at: www.ijcseonline.org

Received: 17/Dec/2018, Revised: 23/Dec/2018, Accepted: 11/Jan/2018, Published: 31/Jan/2018

***Abstract*—**Bitcoin - a new virtual currency may change the world as it is the first currency which is not tied to any bank or government agency. It is also the first global currency that uses cryptography allowing users to utilize money anonymously and having full control over its saving and expenditure. Since its inception in 2009, it is still in its infancy but is gaining popularity with each passing day and might replace existing currencies in near future. Bitcoin being open source acts as a revolutionary currency for e-procurement. The aim of this paper is to explore the concept behind exchanging and trading, introduces the concept of Bitcoin and illustrates the process of Bitcoin mining.

***Keywords*—**Bitcoin, Mining, Money, Virtual Currency

I. BACKGROUND

We as humans have some specific needs which cannot be fulfilled without money. Money is considered as a standard of exchange to solve the problem of barter. Thus money is nothing but a solution that has changed the very fabric of society. Today's money has become an outcome of long process and earlier when there was no money people were engaged in barter. When money was not in existence, the precious day to day utilities such as sea-shell, grain and cattle were used as a form of barter. But portability and divisibility were the two main problems with these commodities. After this era, as metal was discovered by men, people started exchanging valuable metals which solved the problem of portability and divisibility. Nearly thousand years ago the paper money came into existence. The idea behind this process was very unusual in which the people who had gold deposited their gold to goldsmith in order to avoid theft and receipts were given as a proof. Thus, goldsmith's acted as mini banks that could safeguard their gold. Over a period of time rather than exchanging gold, people exchanged these receipts. This is how paper money started being using in business transactions. Nearly hundred years ago, country after country, currency backed by the goldsmith's vanished in air and banknotes started replacing receipts. Thus banks became the evident payment system and fait money was born. Due to dramatic change in advancement of technology online transactions became popular, which involve trusted third party for non-repudiation. First time in the history of money: Bitcoin, an e-procurement system based on cryptography[10][13][14]was invented to transfer money between two communicating parties without involving third party. The Bitcoin is gathering lot of importance in the present virtual world. Hence this proposed survey paper discusses this digital currency used in a virtual world. This proposed survey paper is organised as follows, Section I contains the background which provides history of money, Section II introduces the concept of Bitcoin- a new virtual currency, Section III elaborates the Bitcoin mining and Section IV concludes the paper.

II. INTRODUCTION TO BITCOIN

Bitcoin is a first peer to peer and decentralized digital currency which is imminent just around the corner. This digital currency was invented by pseudonym personality under the name Satoshi Nakamoto. It is also presumed that a group of companies were involved in inventing it, Samsung and Toshiba as Satoshi and Nakamichi and Motorola as Nakamoto. Satoshi Nakamoto released the Bitcoin software as an open source code in January 2009. Bitcoin - a robust and global currency in which transaction takes place directly between users without a mediator is administrated by the Bitcoin network which is not owned and controlled by anyone like internet. Bitcoin has a brilliant technology at the backend so we don't need a trusted third party for transactions like in conventional online transactions third party is must to ensure transfer of money between sender and receiver. Even though it is digital and electronic, we can one-to-one transfer our money without giving our privacy and without seeking anyone's permission. We can own, buy or send Bitcoins at our own will like the cash we utilize from our pockets as this currency is detached from the government.

According to Satoshi Nakamoto, “Bitcoin is a purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution” [1]

According to Bill Gates, Microsoft Co-founder, “Bitcoin is exciting because it shows how cheap it can be. Bitcoin is better than currency in that you don’t have to be physically in the same place and of course for large transactions currency can get pretty inconvenient”[11]

According to Eric Schmidt, Former CEO of Google: "Bitcoin is a remarkable cryptographic achievement and the ability to create something that is not duplicable in the digital world has enormous value"[12]

According to Peter Thiel, Co-Founder of PayPal "Bitcoin is mineable like gold, it's hard to mine, it's actually harder to mine than gold. And so in that sense, it's more constrained"[2]

According to Ben Bernanke, Chairman of the Federal Reserve, USA “[Virtual currencies] may hold long-term promise, particularly if the innovations promote a faster, more secure and more efficient payment system.”[3]

Syed and Clake[6] discuss about Bitcoin that how it has become both a highly useful tool for online working criminals and a profitable target for crime, and claim that this arises from the same necessary, crucial, ideological and design choices that have driven Bitcoin's success. They have also surveyed the landscape of Bitcoin related crime, such as dark markets and Bitcoin theft. They have also proposed future crime possibilities using Bitcoins which include including tax evasion and money laundering. Nakamoto[1] also provides detailed presentation for the Bitcoin working mechanism.

Koshy, Diana[16] proposed a novel methodology of creating and evaluating such mappings solely using real-time transaction traffic collected over five months. They developed heuristics for identifying the ownership relationships between Bitcoin addresses and IP addresses of the systems. They discussed the major conditions under which these relationships become apparent and explain how nearly thousand Bitcoin addresses can be charted to their likely owner IPs by leveraging anomalous relaying performance.

III. BITCOIN MINING

Bitcoin is a first concept that implements cryptocurrency as it is based on cryptography [5][6][7][8][9] to secure transactions. It uses secure hash algorithm (SHA-256) to control the creation of coins and to verify transactions. It is the first cryptocurrency to rule-out the problem of double spending. That is why, it became most successful cryptocurrency. Bitcoin allow a user to spend money anonymously that means the identity of communicating parties’ remains hidden during the transaction. Bitcoin accounts are known as wallets. For every wallet that a person owns there is a key and within key there is a unique signature associated that is being transmitted and thus the receiver receives signature and Bitcoins. No doubt, the identity of parties is not revealed to anyone but the whole list of transactions is public and we have kind of distributed open ledger in which every transaction of the Bitcoin is recorded from the beginning of the Bitcoins creation. Bitcoin miners are some special nodes in the Bitcoin network which maintain this humongous public ledger. Bitcoin miners are those special nodes having high processing capabilities, willingly devoting their computational power to run a special piece of software and in-turn they get rewarded with some Bitcoins. Bitcoin mining is possible only as long as these nodes are honest. These miners take previous transactions, lock new transactions and compete among themselves to validate and add to ledger.

All users of Bitcoin network are not miners but every user has the same version of the public ledger. The transactions in the Bitcoin network are kept in the block chain which is a sequence of records known as blocks as shown below in Figure 1.1:

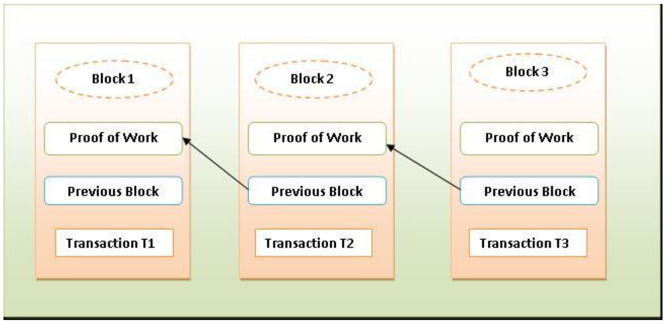

Figure 1.1: Block chain for three blocks

Block number is added to some arbitrary number known as Nonce which gives proof of work. Bitcoin miners create this proof of work that happens through block chain. Once the data is recorded inside the block chain, it is very difficult to change it. It takes about ten minutes to calculate the proof of work and add new block to chain. Proof of work slows the creation of new blocks. Thus it is very hard to tamper with the blocks, because tampering with one block means recalculating proof of work of all the following blocks. Apart from creative use of hashing and open distributed ledger, proof of work mechanism also adds security to Bitcoins. For every new block that is created, the miner gets some transaction fee and also earns some Bitcoins. After every\-=four years 2.1 lakh blocks are being created as every hour six blocks are made. Bitcoin is denoted by BTC, XBTC and ฿. The value of Bitcoin which is rewarded to miners is halved after every four years. In 2009 value earned by miners was 12.5 BTC, in 2013 the value was halved to 6.25 BTC, in 2017 it was 3.125 BTC and ultimately in coming years it will crash down to 0BTC.

Bitcoin software assures Bitcoin is rare in the sense that only 21 billion Bitcoins will be created ever by the Bitcoin network. One cannot end up by saying that bit coins will vanish soon, it is because Bitcoin is divisible up to the 8th decimal i.e. 1 BTC=100,000,000 Satoshi. That means if we have one BTC, we are having 100 million Satoshi. Supply and demand determines the price of Bitcoin which means Bitcoin is susceptible to inflation and hyper-inflation, the price increases as the demand increases and vice versa

IV. CONCLUSION

The proposed paper is purely a literature survey paper regarding the working concept behind Bitcoin. In this paper we have briefly reviewed money from its inception from barter system to the present Bitcoin transactions of the virtual world. Bitcoin also called as a common currency is a first peer-to-peer, faster, cheaper, transparent and secured payment method online. The specialty about this currency it that it is secured using cryptographic mechanisms also called as cryptocurrency. Bitcoins are not accepted yet by most of the countries because of no trusted third party, anonymity and due to lack of awareness.

REFERENCES

[1] Nakamoto.S ,*"Bitcoin: A peer-to-peer electronic cash system."* ,2008.

[2] https://www.coindesk.com/peter-thiel-bitcoin-like-reserve-form-money/

[3] https://www.forbes.com/sites/johnmauldin/2014/12/01/is-bitcoin-the-future/#2f38eb4b2ceb

[4] Ali.S,Clarke.D and McCorry. P,*"Bitcoin: Perils of an Unregulated Global P2P Currency"*,New Castle University Computer Sciences,No. CS-TR-1470,2005.

[5] Khan.QR, Butt. MA, Asger M, Zaman M, *"Integrity Model based Intrusion Detection System: A Practical Approach"* International Journal of Computer Applications.Vol. 115(10), 2015.

[6] Razeef.M, Butt. MA, and Zaman. M, *"Review of Predictive Analytic Modeling Techniques."*

[7] Mehraj.M, Butt.MA and Zaman.M, *"Automatic Speech Recognition Approach For Diverse Voice Commands"*, International Journal. Vol.8(9).2017.

[8] Firdous. A., Pawar.N., Butt. M.A. and Zaman.M., *"Character Recognition: A Signature Approach"* ,International Journal of Advanced Research in Computer Science,Vol. 8(5), 2017.

[9] Hassan .M., Butt. M.A. and Zaman.M "*Logistic Regression Versus Neural Networks: The Best Accuracy in Prediction of Diabetes Disease*."; Asian Journal of Computer Science and Technology, Vol.6(2), pp.33-42. 2017.

[10] Firdous, A., Pawar, N., Butt, M.A. and Zaman, M.*,"Character Recognition: A Signature Approach."*, International Journal of Advanced Research in Computer Science, 8(5). 2017.

[11] https://99bitcoins.com/bill-gates-bitcoin/

[12] https://bitcointrader.org.au/testimonial/eric-schmidt-ceo-of-google/

[13] Nayak, Deveeshree, and. Butt, M.A *"Empowering cloud security through sla."* International Journal of Global Research in Computer Science (UGC Approved Journal) ,pp.30-33, 2017.

[14] Butt. M.A et al. "*Threat Mitigation Strategy in Information System using Intrusion Detection System: A General Classification Reviews."* International Journal of Computer Applications,Vol. 115(10)2015.

[15] Diana.K *"An Analysis Of Anonymity In Bitcoin Using P2P Network Traffic."* 2013.