ZIBELINE INTERNATIONAL PUBLISHING

Information Management and Computer Science (IMCS)

DOI : *http://doi.org/10.26480/imcs.02.2019.01.03*

Online ISSN : 2616-5961
CODEN : IMCSBZ

RESEARCH ARTICLE

REVIEW PAPER ON BITCOIN TECHNOLOGY

Zoraiz Nawaz, Ahthasham Sajid, Summaya Anwar, Haroon Khalid

Department of Computer Science, Faculty of ICT, BUITEMS Quetta, Pakistan.
****Corresponding Author Email: gullje2008@hotmail.com, ahthasham.sajid@buitms.edu.pk***

ARTICLE DETAILS

Article History:

Received 26 August 2019
Accepted 29 September 2019
Available online 22 October 2019

ABSTRACT

Bitcoin is a cryptocurrency (digitized money) and is a worldwide decentralized payment system that is allowed and kept alive due to the technology called Block Chain. TheTnetworkTconsistsTofTpeer-to-peer transactions and these transactions are verified by using cryptography technology bank. Chain technology keeps the records of public distributed ledger. Bitcoins can be earned as a reward through mining. This currency can is convertible into other currencies, products and services. Bitcoin has been emerging as famous digital currency and getting popularity all over for quick transition. Moreover, bitcoin will be a financial asset because it has profitable results. The purpose of this research study is to explain complete working of bitcoins technology, highlights applications and research challenges to be address and current future international market scope of Bitcoin technology.

KEYWORDS

Block Chain, Cryptocurrency, Miners.

1. BACKGROUND

Bitcoin was proposed by Satoshi Nakamoto on Oct.31,2008 and First open source Bitcoin client was released and the Bitcoin network came into existence in January 2009.Satoshi Nakamoto is an inventor of bitcoin, as well the Block Chain technology. All through it's a false name; this is how he introduced himself to the internet. It is a men's name. However, it is possible the Satoshi Nakamoto might be a woman, man or a group of people. This is one of the biggest mysteries in the technology world. Unfortunately, many people think that because Satoshi Nakamoto has invented Bitcoin and the Block Chain technology, he is also the owner of those too. The reality is that Satoshi Nakamoto has no control over the Block Chain—neither bitcoin; therefore, it really doesn't matter who Satoshi Nakamoto [1].

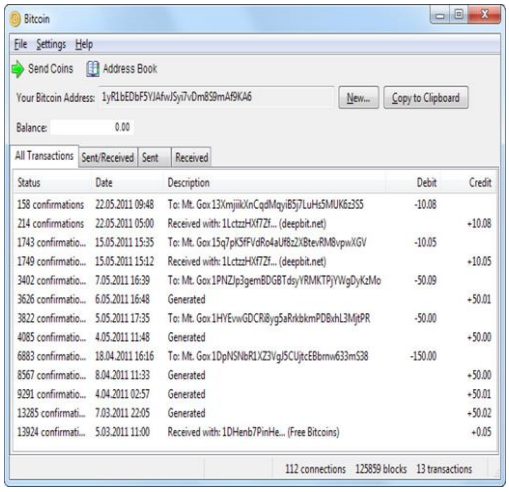

Figure 1: The first Bitcoin client version 0.1 [2]

2. INTRODUCTION

Block Chain is a technology, and its first application was on the platform named bitcoin. Bitcoin is Block Chain. However, Bitcoin itself is only a cryptocurrency that is capable of replacing fiat currencies. Nevertheless, not that many people will like the idea at first. The building block of bitcoin technology of the bitcoin is briefly explained in the following subsections.

2.1 Block Chain

When Block Chain technology began to exist, the first application that was tested on the platform was Bitcoin. Because Bitcoin was the first application on the Block Chain technology, one might say that Bitcoin is Block Chain. However, Block Chain is not Bitcoin. Block Chain is so complex that, still, there are very few human beings who understand each part of it. In fact, Block Chain is so complicated that we (humans) keep on finding more and more ideas that this technology can solve every day [3]. We could say that Block Chain is solving problems. However, for some large Financial Organizations, it's causing certain issues. Some of these matters, of course, are getting addressed and if you keep up with the news, you realize that more and more companies are beginning to use Block Chain Technology for many purposes [4].

Figure 2: The Bitcoin industry [5]

The Block Chain is truly revolutionary, as it's not for solving just one issue for some people, but can fix many problems for everyone. It has re-invented the financial institution, and the proof of that is simply because Block Chain is running and has existed for nine years already, beginning in 2008. The Block Chain is a globally distributed database that is completely decentralized, meaning it has no boss, or someone that we could blame or award. It is running on all computers, and it's unstoppable. Block Chain stands right now; I mean in 2019, is more like where the internet was in 1992-1993. What happened back then is most people said, "its nonsense," or "what's the point of it?" Granted, at the early age of the internet, there were only a few personal computers, very few websites, and the network was slow. In fact, it was so slow that if you wanted to download a one-page PDF document, you would probably go out for lunch, come back and you still had to wait another 30 minutes. The internet (Interconnected networks) seemed like a dumb idea to most people, even for those that had power in politics or others that already had existing large retail infrastructure. They believed that it was just background noise. Slowly, the internet grew and became bigger and faster. And once local support opened on the internet, everything changed. When you think about Block Chain, don't assume that it will not have the same power. Currently, we are innovating in large scale and technology grows with such a high speed that no human can keep up with it [6].

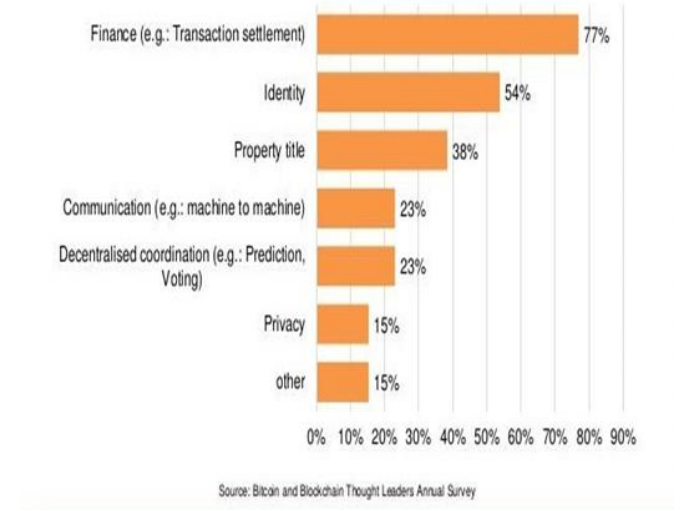

Figure 3: Areas that Block Chains has impact in [6]

2.2 Bitcoin

It is the first known digital currency that is running on a technology called Block Chain. It is entirely decentralized. Therefore, no one has control over it. It also is known as electronic money or digital currency. However, it is a peer-peer payment system. Therefore, it's software. It has no real presence whatsoever, as it's growing on your computer's hard drive. In fact, on every computer that exists in the world. This currency will never be touched by anyone as it only exists in a digital form. Regards to its value, it does seem to fluctuate. However, it has kept itself steady for a long period: moreover, continuously increasing. Back in 2008, it began to compete with the dollar—when one bitcoin was equal to 0.05 dollars. However, in June 2017, one bitcoin has reached $2,912.00; its highest value as of yet. Over the years, bitcoin not only proved that it could reach its highest over and over again, but it has increased its value higher than what we have ever experienced with any other currency Earth. As of June 2019, looking at the currency exchange, bitcoin against the dollar for the last ten years, I can tell that it will keep on growing [4,7].

2.3 Distributed Ledger System

Think of the ledger system as a family tree; but, instead of people's names, the huge ledger system holds information about payment value and addresses. In regard to the amount values, the ledger holds all the records of payments back to the first transaction that was ever made. In regard to the addresses, there are no URL's or location addresses. Instead, these are bitcoin, or any other cryptocurrency, addresses. The ledger holds a series of transactions of all cryptocurrencies [3]. Additionally, the current values are continually computed of the previous transfers. One part of the ledger is representing the value that has been assigned, some other parts of the ledger represent the date and time of each transaction. This is very similar to any of the current Banking systems.

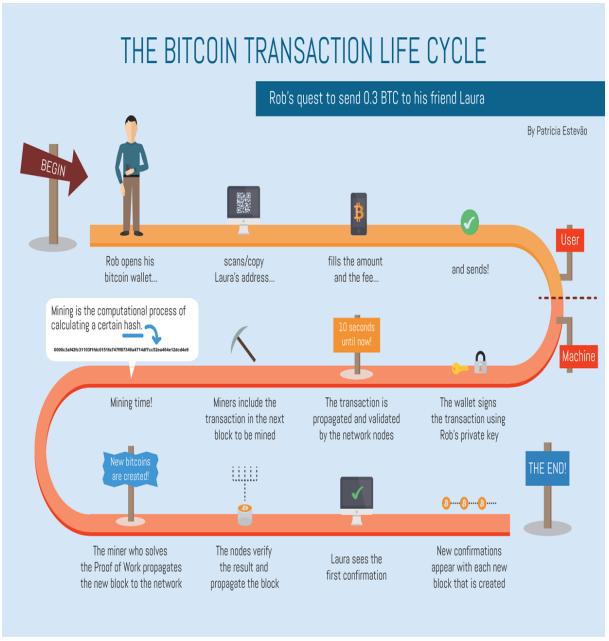

Figure 4: The Bitcoin Transaction Life cycle [8]

You can see who transferred to what account, what date and time, as well how much was each transaction; however, the ledger has no banker. Also, the addresses are not representing names of the individuals, neither who holds what amount; therefore, you can call this an anonymous ledger system. What you have to understand is that when it comes to an individual's bank account that has no relatives, the bank could seize that account. In addition to banks, even the Police, FBI, or any government official can take any bank account if they find a possible reason for it. When it comes to a bitcoin account within the great ledger, the only person who can access it is the person who has the password to that account. This process uses hashes for competition, to validate each block, and make sure that each citizen receives the same record [4].

2.4 Miners

Think about how new value enters the system. Back in 2008, Satoshi Nakamoto only created 50,000 bitcoins to start the process. If you think about it, had he built all 21 million in the first place, the bitcoin would be worthless, and the idea would have been dumb. Instead, Satoshi started with a moderate amount of bitcoin creation. Yet, as the bitcoin community grows, more and more value would be required for the system to be kept alive. There is a particular process that is needed for the system to be maintained; Satoshi has come up with the solution by creating a role. This solution is not only solving one, but two issues:

1. Permanently validating transactions
2. Adding new value into the existing system

The role is called miner. Miners can be individuals, or any bitcoin citizen. However, over time, many large companies have been formed, such as Genesis Mining, where you, as an individual, can join and rent their mining facilities. There are many other miners who over the years have created a pool, and many of them also offer to join these pools for certain reasons that I will discuss shortly [9]. The miners sealing, are sealing the blocks, which in itself can take an enormous amount of computing power, assuring that they cannot be easily replicated. There are multiple methods that each miner may use for the validating processes. Some of the miners may use different software, even creating their own in-house made software to speed up the authentication process [10,11]. However, it doesn't matter what software they use, as all of their work will be checked. It starts when a miner begins to gather transactions that have been broadcasted on the network, and then starts checking those transactions, and eventually sealing those collections of transfers and operations into a new block. A miner receives bitcoins as a reward for each sealed block that is added to the Block Chain [4].

3. LITERATURE REVIEW

Authors Abdirahman Gulled, "Bitcoins Challenge to the Financial Institutions "The purpose of this research is to remark the ways how Bitcoin challenge the traditional transaction system and to assess the future planning structure for traditional financial institutions T to T compete T with T digital T currency. A Survey on Security and Privacy Issues of Bitcoin by Mauro Conti, Sandeep Kumar E, Chhagan Lal, Sushmita

Ruj on a systematic survey that covers the security and privacy aspects of Bitcoin. They start by presenting an overview of the Bitcoin protocol and its major components along with their functionality and interactions within the system. They review the existing vulnerabilities in Bitcoin and its underlying major technologies such as Block Chain and PoW based consensus protocol. These vulnerabilities lead to the execution of various security threats to the normal functionality of Bitcoin. They then discuss the feasibility and robustness of the state-of-the art security solutions.

Additionally, they present current privacy and anonymity considerations in Bitcoin and discuss the privacy related threats to Bitcoin users along with the analysis of the existing privacy-preserving solutions. Finally, they summarize the critical open challenges and suggest directions for future research towards provisioning stringent security and privacy techniques for Bitcoin [12]. An Analysis of Cryptocurrency, Bitcoin, and the Future by Peter D. DeVries. Cryptocurrency, an encrypted, peer-to-peer network for facilitating digital barter, is a technology developed eight years ago. Bitcoin, the first and most popular cryptocurrency, is paving the way as a disruptive technology to long standing and unchanged financial payment systems that have been in place for many decades. While cryptocurrencies are not likely to replace traditional fiat currency, they could change the way Internet-connected global markets interact with each other, clearing away barriers surrounding normative national currencies and exchange rates. Technology advances at a rapid rate, and the success of a given technology is almost solely dictated by the market upon which it seeks to improve. Cryptocurrencies may revolutionize digital trade markets by creating a free-flowing trading system without fees [13].

4. APPLICATION & RESEARCH CHALLENGES

Bitcoin technology could have various applications such as assets managements, insurance, supply chains, smart appliances, block chain health care, Internet of Things [14,15,17]. Research on the Bitcoin technology has been dong from different domain; anonymity, security, platform, structure etc. other approaches perform research using the bitcoin system as a tool [16]. Examples of such approach are the design of secure multiparty computation or coin toss protocols. Furthermore, some structural parts of the bitcoin system, like the Bloch chain approach as an append-only ledger, may open interesting challenges for future developments on secure decentralized systems [14].

5. CONCLUSION

The aim of this paper is to give brief working on Bitcoin technology from all prospective; working, features, applications etc. Overall Block Chain has solved the problem that we have always faced, that is trust. Using Block Chain technology enables us to avoid trusting third party services. Therefore, any payment or exchange over the internet will be between 2 parties only. This is revolutionary as we can expand the trust gap, and the market of the future not only will be faster and cheaper, but will have no limitations, such as age, race, sex, occupation, nationality, or anything like that. This research paper would help young researchers of the next generation to understand Bitcoin technology working in general its importance with respect to its application along with research challenges to be handled. Of course, some people may have to learn the hard way, as many people have been hacked, and only after, begin to invest in learning and implementing security. Still, the time of Block Chain has begun, and it will change the world.

REFERENCES

[1] Bitcoin - Wikipedia. [Online]. 2019. Available: https://en.wikipedia.org/wiki/Bitcoin. [Accessed: 02-Jul].

[2] Coomans, J. 2019. The first Bitcoin client version 0.1 [ONLINE]. Available at: http://posta-magazine.ru/lifestyle/bitcoin?ver=1 [Accessed 31 July].

[3] (PDF) An Analysis of Cryptocurrency, Bitcoin, and the Future. 2019. [Online]. Available: https://www.researchgate.net/publication/316656878_An_Analysis_of_Cryptocurrency_Bitcoin_and_the_Future. [Accessed: 02-Jul]. (Book)

[4] Clark, C. 2013. Bitcoin Internals: A Technical Guide to Bitcoin (1 ed., Vol. 1). New York: Kindle. Retrieved from https://www.amazon.com/Bitcoin-Internals-Technical-Guide-ebook/dp/B00DG8EPT0 (book)

[5] Venture Scanner, 2019. Bitcoin Indusrty [ONLINE]. Availableat: https://venturescannerinsights.files.wordpress.com/2015/09/bitcoin1.jpeg [Accessed 31 July 2019].

[6] Sildeshare. 2019. Areas that block chain technology has impact in [ONLINE]. Available at: https://www.slideshare.net/CoinDesk/state-of-bitcoin-and-Block Chain-2016-

[7] Bitcoinwiki. 2019. Bitcoin price since 2009 to 2019. The historical chart shows the changes of price of Bitcoin (BTC). [ONLINE]. Available at: https://en.bitcoinwiki.org/wiki/Bitcoin_history#/media/File:Bitcoin_price.png [Accessed 31 July 2019]

[8] Bitcoinwiki. 2019. The bitcoin transaction life cycle [ONLINE]. Availableat: https://en.bitcoinwiki.org/wiki/Bitcoin_transaction [Accessed 31 July 2019].

[9] Tutorials Diary. 2019. Block in Bitcoin Block Chain [ONLINE]. Available at: http://tutorialsdiary.com/block-structure-in-bitcoin-Block Chain/ [Accessed 31 July2019].

[10] Prypto. (March 21, 2016). Bitcoin for Dummies. John Wiley & Sons. (Book).

[11] Bitcoins Challenge to the Financial Institutions A qualitative study of [Online]. Available: https://pdfs.semanticscholar.org/07fb/51cf2d8d180c7db4d4615821473e233d02e1.pdf. [Accessed: 30-June. -2019]. (Survey paper)

[12] (PDF) A Relative Study on Bitcoin Mining. [Online]. Available: https://www.researchgate.net/publication/318850089.A_Relative_Study_on_Bitcoin_Mining.[Accessed: 02-Jul.-2019]. (Survey paper)

[13] A Survey on Security and Privacy Issues of Bitcoin. [Online]. Available: https://arxiv.org/pdf/1706.00916. [Accessed: 02-Jul.-2019]. (Survey paper)

[14] Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J.A., Felten, E.W. 2015. SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies, IEEE Symposium on Security and Privacy.

[15] Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., Mccallum, P., Peacock, A. 2019. Blockchain technology in the energy sector: A systematic review of challenges and opportunities. Renewable and Sustainable Energy Reviews, 100, Pp. 143–174.

[16] Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., Mccallum, P., Peacock, A. 2019. Blockchain technology in the energy sector: A systematic review of challenges and opportunities. Renewable and Sustainable Energy Reviews, 100, Pp. 143–174.

[17] Hölbl, M., Kompara, M., Kamišalić, A., Zlatolas, L.N. 2018. A Systematic Review of the Use of Blockchain in Healthcare.