Afshan Zameer *et al*, International Journal of Computer Science and Mobile Applications,
Vol.6 Issue. 1, January- 2018, pg. 95-100 **ISSN: 2321-8363**
Impact Factor: 5.515

A REVIEW ON CRYPTO-CURRENCY

[1]Afshan Zameer, [2]Pawan Kumar Chaurasia
[1]Department of Information Technology, BBAU, Lucknow-226025, Uttar Pradesh, India
zameer.afsh@gmail.com
[2]Department of Information Technology, BBAU, Lucknow-226025, Uttar Pradesh, India
pkc.gkp@gmail.com

Abstract: ***Fortunately, we have entered in a world where most of the states of affairs are virtual. In this 21st century, the biggest mystery has solved. A big question about virtual currency got its answer. "A crypto-currency or a virtual currency is a decentralized currency based on cryptography for security purposes, works as a digital medium of exchange." Blockchain is the backbone of decentralized currency. The modernity of blockchain technology changes the payment system. Bitcoin as a crypto-currency become more famous in the past years. Satoshi Nakamoto introduced Bitcoin to the world in 2008. There are some countries where crypto-currency like Bitcoin is used for specific purposes. To make a complete and robust network, hardware wallets, mining network and microcomputers are required for infrastructure of crypto-currency. In this paper, we explained the working mechanism of crypto-currency. How it works when a transaction is requested by someone. Nodes of P2P network in which transaction is broadcasted, validates it and to fabricate a new block, the transaction is verified with another transaction. We will discuss the complete explanation of the working mechanism further. A probability is there to regulate the virtual currency in India so soon. The future of crypto-currency looks more promising due to increment in its users per year in India.***
Keywords: Cryptography, Blockchain Technology, Bitcoin

1. Introduction

In general terms, crypto-currency is a sort of a digital payment system through which we can transfer the money to one another. By solving mathematical problems, it can be digitally produced, unlike the fiat currency. Virtual currency is free from all government rules as it is decentralized. Therefore, no one can rule over it. Instead of the centralized banking system and economic system, decentralized crypto-currency does not have any control of governments or companies. It is an exoteric medium of exchange that recently emerged as a completely digital payment system [1]. It is the first crypto-currency which is decentralized. Therefore, we are taken Bitcoin into the account as a crypto-currency. It's a peer-to-peer system which is decentralized with no mediator or single authority. Bitcoin is based on SHA-256 hash algorithm [2]. A public distributed ledger is maintained to record all the Bitcoin transactions called blockchain. The current price (in September 2017) of Bitcoin is 1 BTC=265,442 INR and 1 BTC=3729.88 US Dollar. In 2017, worldwide there are 10 million users of Bitcoin. It uses the block-chain which is indeed a distributed database to record transactions or virtual workouts that have been shared among various participants. There are 3 elementary manners to get Bitcoin:

i) Mining
ii) Buying on an exchange
iii) Accepting them for goods and services

The whole world is now talking about the virtual currency or crypto-currency. It's a new era of the global digital organization in the economic system. In this article, we will get a quick overview of crypto-currency, its history, its status in India and the future of crypto-currency in India.

2. BACKGROUND OF CRYPTO-CURRENCY

The internet efficaciously makes crypto-currency usable for purchases as well as transactions which catch tremendous media attention. In the early 1980s, David Chaum who was an American cryptographer introduced about a Blinding algorithm to the universe [3]. The blinding algorithm is a technique in cryptography which is used for secure, inevitable information exchanges. It was called as "Blinded money". In the late 1980s, David Chaum founded DigiCash an electronic payment system whose transactions was anonymous [3]. In 1998, a software engineer, Wie Dai invented distributed electronic cash system named as "b-money" [3]. He published a white paper in which he described an anonymous e-cash system. After that BitGold came into the existence, developed by Nick Szabo [3]. In 2008, pseudonymous developer Satoshi Nakamoto published a white paper which describes bitcoin titled as Bitcoin: A Peer -To- Peer Electronic Cash System [4]. In 2009, this system has been started. Satoshi Nakamoto is an unknown person. A big controversy is there on this name. Some of the researcher or journalists found that he belongs to Japan. But in 2016, an Australian businessman Craig Wright claims that he is Satoshi Nakamoto but still this name is in controversy. And after Bitcoin, many more crypto-currencies come into the existence like Litecoin, Peercoin, Ether, Monero, Ripple, Dogecoin, Dash and much more.

3. USED BY COUNTRIES OF CRYPTO-CURRENCY

The world has some countries where crypto-currencies are not only tested or analyzed but also implemented. There are some countries where the use of crypto-currency like Bitcoin is legal but for specific purposes such as tax or others. These are the respected countries: United States of America, Australia, Denmark, Sweden, South Korea, Netherlands, Finland, Canada, France, Germany, Jordan, Lebanon, Spain, Luxembourg, Switzerland, United Kingdom. Some of the countries where virtual currency is illegal are: Bangladesh, Iceland, Kyrgyzstan, Thailand, China, Russia, Ecuador. In India Bitcoin is unregulated. Though various banks of India prohibited transactions related to them.

4. SECURITY FEATURES

Security features of the crypto-currency are the primary domain of research. Cryptography is the concept behind the crypto-currency to handle secure transactions and its creations. Cryptography is the study or a practice of hiding information. Basically, Cryptography is the ability to exchange the information over a secure communication system in the presence of adversaries [5]. This security feature makes virtual currency difficult to counterfeit. The security of virtual currency is the heart of the consideration from the scratch.
To make the mining of currency and transactions highly secure, all the possible efforts are made. Still there exist some threats against this crypto-currency because it may be permeable throughout the transactions or also attacked by the eavesdropper. A standard which provides the security to all the information system in crypto-currency is Crypto-Currency Security Standard (CCSS). CCSS steering committee maintains this standard.

5. INFRASTRUCTURE REQUIRED

Crypto-currency like Bitcoin infrastructure is expanding. The great thing is that infrastructure required for crypto-currency does not need to build new; heavy and big buildings and we do not need to build a new internet system because auspiciously we are in the world where internet is already present. Hardware wallets, mining hardware, and microcomputers are strongly required for crypto-currency infrastructure and all of these make the complete network more robust [6]. There are some companies which have shown the positive results and innovations to the world.

5.1 MINING HARDWARE

Bitcoin mining hardware mines Bitcoins. Mining Bitcoin is competitive. It is not easy for an average person to mine the Bitcoin in today's world. We'll need some specialized kind of hardware known as Application Specific Integrated circuits (ASICs). Radically, Satoshi proposed computer CPUs for Bitcoin mining. But

Bitcoin miners searched graphics cards for more hashing power. Bitmain, BitFury, Spondoolies Tech, KnCMiner are the well-known mining hardware companies [6].

5.2 HARDWARE WALLETS

The ascent of hardware wallets has shown a prominent degree of within the crypto-currency industry. Ledger, Trezor, KeepKey, Case is the startups coming into the virtual currency arena [6]. These hardware wallet start-ups have produced the modest device to secure individual's virtual currency.

5.3 MICRO COMPUTER

The small single-board computer named as Raspberry Pi invented by Raspberry Pi foundations in U.K. is used as a microcomputer [6]. This microcomputer has really made a huge splash in virtual currency atmosphere and the computing universe in general. Bitcoin computer can be made by anyone at very low cost. It processes micro-transactions and serves as a full node. This credit card sized computer has solidified the virtual industries.

If we take financial services infrastructure into the consideration then one of the innovations is the distributed ledger technology (DLT). DLT also called blockchain has captured the wallets of financial services environs [7]. Expeditiously consciousness of DLT has grown up. DLT is one of the technologies that will create the backbone of future generation financial services infrastructure. DLT will appreciably increase clarity between market shareholders. DLT will slowdown the need for brokers by implementing autonomous execution capabilities. DLT forms a solitary version of the truthfulness or legitimacy to provide pellucidity for an ancient & real-time transaction [7]. Bitcoin or any other virtual currency is the future of universe. It eliminates the limitations of having a bank account. Perhaps it's often free to exchange around the world.

6. MECHANISM OF CRYPTO-CURRENCY

Crypto-currency is consisting peer-to-peer network and each peer keeps the records of all transactions. Figure 1 shows the working mechanism of crypto-currency. A P2P network comprising computers called nodes in which requested transaction is broadcasted. Then these nodes of network validates of transaction. A verified transaction could involve crypto-currency, contracts, medical records, deeds, details of customer and other information that can be mentioned in digital way. Once verified, the transaction is concatenated with other transactions to construct a new block of data to be added. The new block is attached to the existing block-chain in an immutable and permanent manner. After that transaction is completed [8].

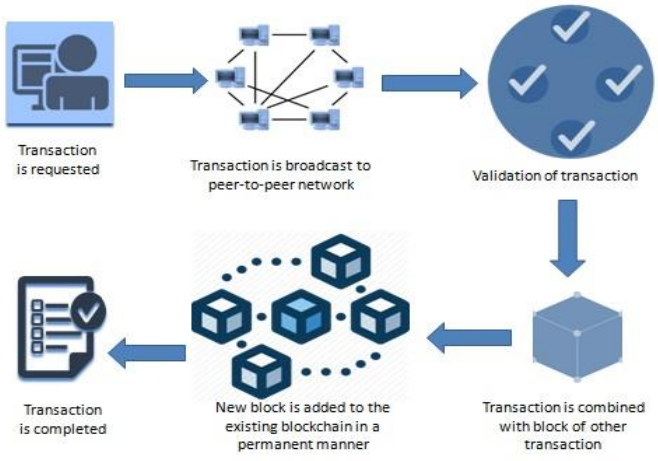

Figure 1: Mechanism of Crypto Currency

7. STATUS OF CRYPTO-CURRENCY IN INDIA

There is no regulation in India for virtual currency. Due to this, some Bitcoin exchanges such as Zebpay, Unocoin, and Coinsecure have initiated operating with trading platforms which are self-regulated along with Know Your Customer (KYC) system [9]. Coimama, LocalBitcoins, VirWox, Mycelium Local Trader, ShapeShift, Bitcoin-otc are some other India's popular Bitcoin exchanges.

Initially, in 2013, Reserve Bank of India gave warning against the usage of Bitcoin. But in 2014, RBI had shown its interest in blockchain technology to minimize the paper currency. The deputy governor H.R. Khan (2011-2016) also speaks up to study blockchain to reduce the paper currency usage. In 2015, a financial stability report was published by RBI to identify the importance of 'private blockchain'. In 2016, ICICI bank with Emirates NBD (in terms of assets, one of the largest banking groups in the Middle East) has executed transactions and remittance using blockchain technology. Then in 2017, a white paper has been issued by Institute for Development and Research in Banking Technology (IDRBT) of RBI and also a pilot test was taken [10].

According to media report Bitcoin is also illegally used in terror finance, drug transaction, and money laundering. Not only the Bitcoin some other virtual currency like Bbqcoins, Dogecoins, Litecoins having the same features and problems [13]. India's first Bitcoin exchange was Buysellbit.co.in founded by Mahim Gupta. He was arrested by Enforcement Directorate (ED) due to unauthorized dealer also he broke the Prevention of Money Laundering Act 2002 [11]. In India, Current status is no regulations for now.

8. PROPOSED MECHANISM FOR CRYPTO-CURRENCY

Due to the decentralized and distributed nature of crypto-currency like Bitcoin it has some issues in regulation in India. An increasing exigency for acceptance of a substantial regulatory policy pertaining to crypto-currency is there in India. The central bank or any other financial authority does not recognize the composition, trading or application of crypto-currency as a moderate for payout.

In India, Constitution is supreme. The Central Government has authority to legislate and regulate matters according to the Indian Constitution. An analysis of the Indian Constitution has been undertaken to recognize if crypto-currency is competent of government observation. For this concern, in Indian constitution there is an Article 246 read along with Seventh Schedule particularizes the activities that the Central Government and the State Government are permitted to legislate [12].

In Constitution, entry 36 of Seventh Schedule (List I) states that the Central Government is allowed to legislation pertaining to currency, coinage and legal tender; foreign exchanges and entry 46 is related to bills of exchange, cheques, and promissory notes and other like instruments [12]. Central Government would have peculiar authority to legislate if any crypto-currency or Bitcoin falls within any of the above categories of the modality. As discussed earlier Bitcoin's system practices the block chain technology to keep the records of transactions. Bringing crypto-currency underneath the present Indian laws could be complex as it is intangible. KYC norms could be capable of regulating the system of Bitcoin [12]. KYC stands for Know Your Customer. KYC is the procedure of identification and verification of customers, issued by RBI for prevention of money laundering. Crypto-currency should be legalized in India as government also focused on Digital India and promotes cashless transactions.

9. FUTURE OF CRYPTO-CURRENCY IN INDIA

Indian government is working towards making regulations and laws for the use of Bitcoin [13]. There are so many confusions in the market about its application, demand and supply in the consequences of demonetization. Though it is not issued by any bank or authority, therefore people do not know how investment can be taxed and due to the absence of a regulator there is no legal support. Because of these obligations, some crypto startups introduced Digital Asset and Blockchain Foundation of India (DABFI). They are Unocoin, Zebpay, Coinsecure and Searchtrade which have conjointly launched DABFI [13]. Like internet, crypto-currency has also exponential growth in India. With the help of internet and blockchain technology, in future there will be a probability to expect bank to be a virtual in India. Now crypto-currency is everywhere and it will develop over time. If due to some reasons, Bitcoin loses its prominence then to replace it a new virtual currency will come out. Therefore to plan something better RBI has hinted to make its own crypto-currency might be named as "Lakshmi". Also in India, there will be a prosperity reformation in the

crypto-world which is decentralized and it will lead to increased capacity in a sharing economy. Simultaneously it's a very difficult task to predict that where will the future of crypto-currency take to the Indian economy as it is still uncertain. Some experts predict that India will also regulate crypto-currency so soon. On the other hand some observers also indicate its drawbacks.

10. Conclusion

Crypto-currency is such an invention which has become a global phenomenon. Earlier RBI warned the Indians from using crypto-currency that to be associated with money laundering and terrorist financing. In September 2017, executive director Sudarshan Sen said that RBI is not comfortable with non-fiat crypto-currencies like Bitcoin. Sen said that there is a group of people who are studying and analyzing the fiat crypto-currencies that is a substitute to the Indian rupee.

Today, crypto-currency is a modern technology and a tool which needs to look after and further study. It still has no legislative response from the Indian government. In such currencies, the number of investors is increasing fastly over the last few years. Indian government should take responsible steps now to regulate such currency as its user in India is rapidly growing. In conclusion, we would like to say that the future of crypto-currency looks promising in India. There is a hope that Indian government will soon provide an admittable framework of crypto-currency to service providers.

References

[1] Chinmay A. Vyas, Munindra Lunagaria,"Security Concerns and Issues for Bitcoin", May 2014.

[2] Shaik Shakeel Ahamad, Madhusoodhnan Nair & Biju Varghese,"A Survey on Crypto Currencies," 2013.

[3] Brian Martucci, "What Is Cryptocurrency - How It Works, History & Bitcoin Alternatives", available at https://www.moneycrashers.com/cryptocurrency-history-bitcoin-alternatives/, accessed on August 14, 2017.

[4] Digital Currency Bitcoin, Innovation, Financial Instrument, and Big Data, David LEE Kuo Chuen, 1st ed., Singapore Management University, Singapore, 2015, pp. 11

[5] P. Garg, S Dilawari,"A Review Paper on Cryptography and Significance of Key Length", 2012.

[6] Jamie Redman. "These 8 Companies Strengthened Bitcoin's Infrastructure in 2015." Internet: https://news.bitcoin.com/8-companies-strengthened-bitcoin-infrastructure -2015/, December 31, 2015.

[7] R. Jesse McWaters, "The Future of Financial Infrastructure," World Economic Forum, 12 August 2016.

[9] S. Modgil, "Indian Government Mulling Legalizing Bitcoin Cryptocurrency In India", 26 June, 2017, available at https://inc42.com/buzz/bitcoin-cryptocurrency-india-government/, accessed on August 24, 2017.

[10] M. Patel, "Bitcoin Simplified, Blockchain Technology How Useful in Banking Transactions". Available at: https://www.youtube.com/watch?v=INxNZK8 Mw.J8.

[11] M. Patel, "Bitcoins- Mechanism, Money Laundering, RBI's Stand". 2015. Also Available: https:// www.youtube.com/watch?v=srbivXKX-vY.

[12] Nishith Desai Associates, "Bitcoins - A Global Perspective". 2015, pp.17.

[13]Vishal Gupta, "The Future of Bitcoin Industry in India", Available at http://bwdisrupt.businessworld.in/article/The-Future-of-Bitcoin-Industry-in-India/15-05-2017-118150.

Authors Profile

Afshan Zameer, B.Tech., is currently pursuing M.Tech (Software Engineering) in the Department of Information Technology from Babasaheb Bhimrao Ambedkar University, Lucknow, Uttar Pradesh, India. She received her Bachelor Degree in Computer Science Engineering from Uttar Pradesh Technical University, Lucknow (India) in 2014. Her research area includes Crypto-Currency like Bitcoin, Blockchain Technology.

Pawan Kumar Chaurasia is working as an assistant professor in the Department of Information Technology, Babasaheb Bhimrao Ambedkar University, (A Central University), Lucknow, India. His research area includes software reliability, software quality and software testing.

