International Journal of Trend in Research and Development, Volume 4(4), ISSN: 2394-9333
www.ijtrd.com

Cryptocurrency: Trends, Perspectives and Challenges

Er. Puneet Er. Deepika and Er. Rajdeep Kaur
Assistant Professor, Computer Science and Engineering Department, Chandigarh University, India

Abstract: There are many types of currency but the bitcoin is one of the most successful Cryptocurrencies due to its anonymity. Bitcoin has many names like it is known as cryptocurrency, cyber currency or alt coins. Bitcoin or BTC is known as a digital coin, issued for the first time in 2009 and based on a peer to peer system. Bitcoin is most widely used and emerging currency in today world. Bitcoin is valuable because of its various advantages. First of all it is decentralized money. Its two main strength are its anonymity and low transaction cost. So this paper discusses the bitcoin with its history and transaction procedure. Its trends and perspectives are also discussed in this paper. Block chain which seems to come from the concept of Bitcoin is also a part of this paper.

Keywords: *Bitcoin; BTC; Alternative private money; block chaining; cryptocurrency; Mining*

I. INTRODUCTION

The emergence of Internet and technology simplified all the area regarding the financial and economical area [4]. As the time changes, economic channels also undergoes many changes. Now people believe in online system such as online transactions. Earlier the paper currency was used to exchange goods etc Now, it's seems that paper money has become a traditional way of exchange, while the electronic currency became a much more attractive system [23]. Money is one of the most valuable for the transactions of goods and services. With increasing technology and innovations new types of money have been invented. Many types of money have come from older time till now. Every money has its advantages and limitations. This paper's main goal is to discuss the new innovation of currency known as cyptocurrency or digital currency or cyber currency. There are many types of cryptocurrency come in knowledge but studies shows that Bitcoin is the most successful cryptocurrency [12]. It is also considered to be the world's first decentralized currency .This currency is not issued by central bank and not protected by any government rules. It is launched in 2009. The inventor of Bitcoin is Satoshi Nakamoto [2]. The system is peer to peer, and transactions take place between users directly, as there is no intermediate. It is a combination of two words-Bit and Coin. Bitcoin is a remarkable cryptographic achievement and the ability to create something that is not duplicable in the digital world [15]. Cryptocurrency is a type of digital currency which is fully based on cryptographic methods. It also maintains the features of traditional currency but without the approval of any authority. Now a day's Bitcoins payments is acceptable form of payment due to its various characteristics.

The main characteristics of bitcoin payments are [3]:

- Transactions don`t require fees
- Payments get confirmed in short period of time
- There is a low risk of payment fraud, considering that the transactions are irreversible
- There is no need of identification

"Bitcoin is a remarkable cryptographic achievement and the ability to create something that is not duplicable in the digital world has enormous value."[19]
The subject matter of this paper is fully based on Bitcoin a type of cryptocurrency, its history, how its transaction takes place, what are the ways to get Bitcoins and so on.

The remaining structure of this paper is organized as follows. Section 2 gives the history and values of Bitcoin. Section 3 shows the Transactions of the Bitcoin with diagram. Applications of Cryptocurrency are discussed in Section 4. Section 5 discusses the concept of Block chaining. The paper is concluded in Section 6.

II. THE HISTORY AND VALUE OF BITCOIN

Bitcoin is an online payment system launched as on open source software in 2009 [5]. It is also known as BTC.Its creator known by the name Satoshi Nakamoto. Nakamoto published a paper describing his or her creation entitled "Bitcoin: A Peer-to-Peer Electronic Cash System" in 2008.

Bitcoin is generated though the sequence of mathematical formula runs on a system. There are many types of cryptocurrency like Bitcoin, PPcoin, Quark, Lit coin, Name coin, Nova coin and others [8]. Bitcoin is the most common and effective currency because of its easy transactions and simple algorithms which are built in and Bitcoins are built in protocols [14]. Some facts about Bitcoin history are as follow:

- On October 31st, 2008, "Bitcoin" was posted to a cryptography mailing list, published under the name "Satoshi Nakamoto" [11].
- On August 18, 2008, an unknown person registered the Bitcoin.org domain.
- On January 8th, 2009, the first version of Bitcoin is announced, and after that Bitcoin mining begins.

There are many factors due to which Bitcoin considered an ideal currency [2][9]:

1) Transaction speed: It means to transfer Bitcoins takes a very small time or we can say that this process is instantly.

2) Cost: This point means that transaction fee is very small for Bitcoin as compared to other currencies.

3) Exact cryptographically identification of each transaction for particular address.

4) Liquidity and convertionability: There are many electronic sites available for the reconvert able of Bitcoin into other currencies and also this process takes a very small time to execute.

5) Open source: It means the code has no copyright restrictions. Anyone can edit the code who wants.

People who want to invest their money in online black market uses the anonymity feature of bitcoin [13]. This feature made the bitcoin for the illegal website purposes which do the illegal selling of drugs and other weapons [13][15]. Many such websites has been come in notice and been closed by

government but with the time new and new websites emerged and the new emerging websites using the bitcoin as the medium between buyer and seller.

Figure 1: Prize chart of a Bitcoin

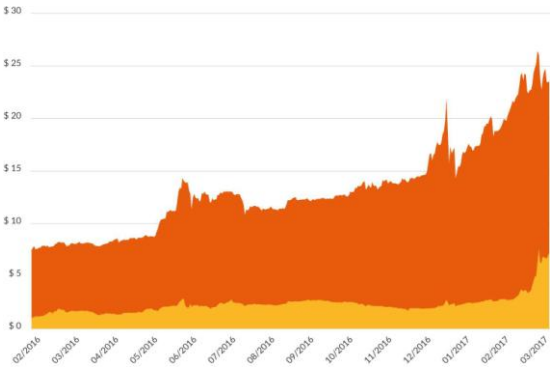

Fig 2: The total cryptocurrency market capitalization has increased more than 3x since early 2016, reaching nearly $25 billion in March 2017

III. TRANSACTIONS

We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the Next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin [8]. A payee can verify the signatures to verify the chain of Ownership. When one bitcoins moves from one address to another address it is known bitcoin transactions. The uniqueness of bitcoins depends on its unique address [5]. There exist a database with the bitcoins transactions and every transaction is recorded in this public database. For the transactions as shown in diagram below, the need is to broadcast the public key of the Payee and the amount of bitcoins transferred [15]. The diagram below show how the transfer of bitcoins takes place by using cryptographic methods [17].

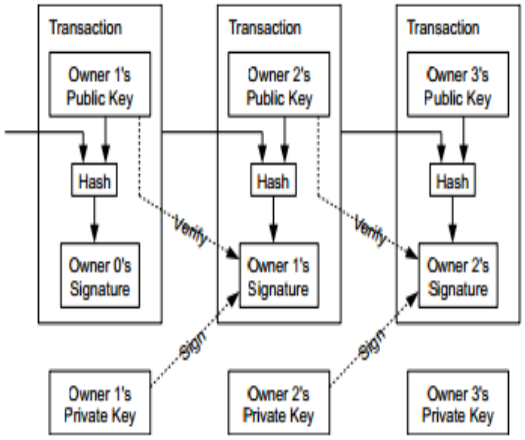

Figure 3: A Chain of Digital Signatures

Obtaining Bitcoins

There are three primary ways to obtain Bitcoin:

- Mining new ones.
- Buying on an exchange.
- Accepting them for goods and services.

'Mining' is discovering new Bitcoin. It is actually a verification of Bitcoin transactions. This process is done on the computer [11]. In order to make sure a Bitcoin is genuine,

Miners verify the transaction. There are many transactions that individuals are trying to verify and not just one [22]. These transactions are gathered into boxes with a virtual padlock on them which make up the 'block chains'. 'Miners' run software to find the key to open that padlock. Once the computer finds it, the box pops open and the transactions are verified [14]. Hence, it can be said that while Bitcoin are "mined" by individuals, they are "issued" by the software. During the mining process system adds new Bitcoin transactions to the block chain during this when a new block is discovered, miner will get a number of Bitcoin.

Mining is very expensive process for an individual [11]. So sometimes an individual miner joins a mining pool. By that there is no need to build your own mining farm as it is too expensive. Just we need to provide computing power to our pool [23]. Along with the expensive, mining process is also time consuming. So before mining we can calculate the mining cost on mining dashboard and by this we can decide whether we proceed further or not.

IV. APPLICATIONS OF CRYPTOCURRENCIES

Decentralized Cryptocurrencies like Bitcoin are more widely used than any previous e-cash. There are a growing number of businesses and individuals using Cryptocurrencies like Bitcoin. These include brick and mortar businesses like restaurants, apartments, law firms, and popular online services and games and many other many such types of business [10]. Bitcoin is growing fast in many areas due to its various advantages. It is widely used in USA Both in north USA as well as in south USA.Many firms and business accepted Bitcoin. Mostly merchants or individual working in technology field use Bitcoin [3]. It is now widely accepted as a mode of transfer for buying goods and services due to its various advantages.

Many vendors do not accept Bitcoin directly, they use an intermediary to accept Bitcoin payments and convert it into a standard currency. In short, Bitcoin has become a popular method of transacting with vendors of goods and providers of services. Bitcoin is also a popular currency with individuals who protest the U.S. monetary system or government. Bitcoin is used for illegal activities as well [20]. This includes donations to illegitimate organizations, such as the infamous site, Silk Road. In the area of online gambling, it is growing fast.

Many large companies are accepting bitcoins as a legitimate source of funds. They allow their online products to be bought with bitcoins [7]. With the extreme facilitation of transfer and earning of bitcoins, it would be a mistake not to accept online coins as cash. Many biggest companies accept Bitcoin as a mode of payment. Here are some examples [23]:

- **WordPress.com** – An online company that allows user to create free blogs
- **Subway** – Eat fresh
- **Microsoft** – Users can buy content with Bitcoin on Xbox and Windows store

- **Dell** – American privately owned multinational computer technology company
- **Steam** – Desktop gaming platform
- **The Internet Archive** – web documentation company

These are the examples of few companies which uses the advantages of Cryptocurrency. There are many such types of companies which use this. By Cryptocurrency concept a new concept comes into knowledge known as Block Chain. As a result a number of banks, including Deutsche Bank have started exploring block chain's potential to make payments faster, cheaper and transparent as well [16].

V. BLOCK CHAINING

When bitcoins are mined by the mining process immediately it will be added in the public database which is known as the Block Chain [20]. Every bitcoins record is in the database [19]. There is no bitcoin which is outside of the database [22]. The overall historical chain, containing every transaction ever created and verified in the system, has come to be known as Block chain. There are many different Block chains that can be constructed using the same, or similar, processes, and overall, a Block chain can be thought of as a chain where new transactions are inserted at the end of already existing chain [23].Block chain is a mechanism which provides the anonymity source which is very first advantage of Bitcoin.

In general, a Block chain process is comprised of the following steps: [23]

- Collect new transactions and organize them into blocks.
- Cryptographically verify each transaction in the block.
- Append the new block to the end of the existing Block chain.

The diagram below shows the Block chain process with the detailed cryptographic technique using blocks and hash function. How the new blocks are created using the previous hash is explained in Fig.4

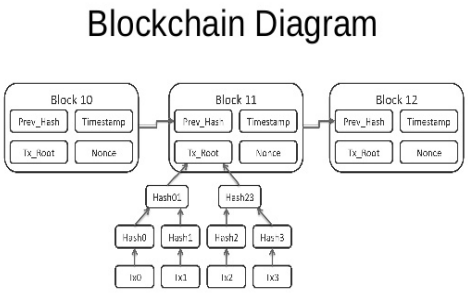

Figure 4: Block chain Diagram

CONCLUSIONS AND FUTURE SCOPE

Taking into consideration the new technology, the Internet applications and mobile phones, electronic currencies emerged and played a very important role. This paper discusses about the Bitcoin as an alternative currency with its value and methods to obtain Bitcoins is also discussed in this paper. Looking forward, virtual currencies are a part of an emerging market, which encourage both investment and risk. With proper regulatory policies, the world of digital currency can be considered a success also for governments and its users. By first introducing Bitcoin the work illustrates that the Bitcoin system implements the cryptographic mechanisms to allow transactions to be chained to one another and by this a concept known as Block chain comes into knowledge which stem from the Bitcoin system. This work provides technical clarity for the research on block chain.

References

[1] G. Andresen. March 2013 Chain Fork Post-Mortem. BIP 50.
[2] G. Andresen. Block size Economics. bitcoinfoundation.org, October 2014.
[3] M. Andrychowicz, S. Dziembowski, D. Malinowski, and L. Mazurek. Secure Multiparty On Bitcoin. In IEEE Symposium on Security and Privacy, 2014.
[4] M. Andrychowicz,S. Dziembowski, D. Malinowski, and Mazurek. On the Malleability Of Bitcoin Transactions.In Workshop on Bitcoin Research, 2015.
[5] A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, Miller, A. Poelstra, J. Timon,´ and P. Wuille. Enabling blockchain innovations with pegged sidechains, 2014.
[6] J. Herrera-Joancomart. Research and Challenges on Bitcoin Anonymity. Keynote Talk: 9th International Workshop on Data Privacy Management, 2014.
[7] T. Bamert, C. Decker, L. Elsen, R. Wattenhofer, and S. Welten. Have a snack, pay with Bitcoins. In IEEE P2P, 2013.
[8] E. Ben-Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, Tromer, and M. Virza. Zero cash: Decentralized anonymous payments from Bitcoin. In IEEE Symposium on Security and Privacy, 2014.
[9] S. Eskandari, D. Barrera, E. Stobert, and J. Clark. A first look at the usability of bitcoin key management. Workshop on Usable Security (USEC), 2015.
[10] Eyal. The Miner's Dilemma. In IEEE Symposium on Security and Privacy, 2015.
[11] I. Eyal and E. G. Sirer. Majority is not enough: Bitcoin mining is vulnerable. In Financial Cryptography, 2014.
[12] E. Ben-Sasson, A. Chiesa, M. Green, E. Tromer, and M. Virza. Secure Sampling of Public Parameters for Succinct Zero Knowledge Proofs. In IEEE Symposium on Security and Privacy, 2015.
[13] A. Biryukov and I. Pustogarov. Bitcoin over Tor isn't a good idea. In IEEE Symposium on Security and Privacy, 2015.
[14] G. Bissias, A. P. Ozisik, B. N. Levine, and M. Liberatore. Sybil-Resistant Mixing for Bitcoin. In WPES'14: Workshop on Privacy in the Electronic Society, 2014.
[15] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and W. Felten. Research Perspectives and Challenges for Bitcoin and Cryptocurrencies (Extended Version). Cryptology ePrint Archive, Report 2015/261, 2015.
[16] J. Bonneau, A. Narayanan, A. Miller, J. Clark, J. A. Kroll, and E. W. Felten. Mixcoin: Anonymity for Bitcoin with accountable mixes. In Financial Cryptography, 2014.
[17] J. A. D. Donet, C. Perez´-Sola, and J. Herrera-Joancomartı. The Bitcoin P2P network. In Workshop on Bitcoin Research, Jan. 2014.
[18] Schroeder, J.L, Bitcoin and the Uniform Commercial Code. University of Miami Business Law Review. 2016
[19] Sorrell, W.H, Block chain technology: opportunities and risks. Vermont Office of the Attorney General, 2016
[20] Zhu, H., & Zhou, Z. Z., Analysis and outlook of applications of block chain technology to Equity, 2016
[21] Prpić, J., Unpacking Block chains. Collective Intelligence, 2017.
[22] Glaser, F. Pervasive Decentralization of Digital Infrastructures: A Framework for Block chain enabled System and Use Case Analysis, 2017
[23] Bitcoin Wikipedia. Available:http://ru.wikipedia.org/wik