International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 04 Issue: 06 | June -2020 ISSN: 2582-3930

A Study on Bitcoin Technology

Bindu L[1], Dr.Manjunath M[2]

[1]*Bindu L , Master of Computer Application & R.V College of Engineering, Bengaluru, India*

[2]*Dr.Manjunath M, Master of Computer Application & R.V College of Engineering, Bengaluru, India*

Abstract - Bitcoin(BTC) is a virtual currency or digital cash and most successfull cryptocurrency, it is purely peer to peer version of digital cash launched in 2009 by the unknown group of individual with pseudo name called satoshi nakamoto, Bitcoin possess lots of features and is transparent in nature. The two main and important property which probably made bitcoin sucessfull is anonymity and decentralization. This paper, we provide a comphrensive description on the details of the crypto currencies and we provide the details on the bitcoin system. We explain the concept of bitcoin transactions and its implementation and also the first devised block chain database. This paper focus on the overview of the bitcoin structure and its system and bitcoin payments.

Key Words: Bitcoin, Cryptocurrency, Block chain.

1.INTRODUCTION

Bitcoin is the electronic money or cash implemented with digital signatures which depicts the gold coin picture and provide the security for the online transactions and the key producer of block chain development, Block Chain is the world wide public ledger yet complicated in nature, yet it has the capability of transferring the golden coin's via the email over the network, And these coins get transferred as analogy signal's in the network, Bitcoin is the smart invention in early 2009 by unknown individual's, these individual's has a pseudo name known as satoshi nakamoto. It is unanimity network model which is complicated yet provide the payment replacement system. Bitcoins can be duplicated or single coin can't be used double time , since it is revolutionary technology it won't support duplication of the particular coin. Bitcoin is the predominant implementation and prominent in triple-entry book-keeping system in existence. In current era, It has gained wide popularity and it been current trending topic of the payment system's, it is widely popular due to its strong features like private crypto-graphic key used in bitcoins to make the transactions payments, but still some countries not yet approved these coin's has legal.Some countries bitcoins regulations are considered as illegal, yet single bitcoin in india cost worth rupees 7,65,074.89 indian rupees. Since crypto currencies are inevitable because the coin's get transferred safe and securely in the online platform has it is encoded with cryptography concepts, these transactions are peer to peer without involving single or central authorities.This paper focus on the overview of the bitcoin's and characteristics of the bitcoin's and its structure and legal issues and challenges associated with bitcoin. Bitcoin has gained popularity and legal positions in some specific countries where the mining and regulation's of the bitcoin's are legally approved and after earning bitcoin's it can be converted to the money for the payment use. Bitcoin is an advance technology where it keep on updating the security system as the miners keep on digging the golden coins by solving the mathematical puzzles , these mathematical puzzles is not just a puzzle, it provide the security of each coins in the chain. Bitcoins has the bitcoin protocol, protocol is the certain terms and rules for the transaction of the coins over the network, each coin contains the blocks these blocks stores the information, but these information's are securely encoded so that no individual can hack others coins , block chain records the transactions accurately. In future it might become the first world currency.Since it is not legally approved in some countries but still peoples are digging the bitcoins like gold diggers, these diggers are know as miners, these earned bitcoins can be converted to the current paper currency in accord to use it.Using the appropriate and good nodes with high processor in the cpu can help digging these bitcoins over the network, without power of proceesor, mining of the coins is bit impossible and difficult, Bitcoins can be earned by investing on it or mining and trading.Bitcoins are inevitable and some websites and online shoppings accept the bitcoins for buying and selling the product's. So to earn a bitcoin first need to have the basic wallet which is the software where you can store the bitcoin's which are earned.The Bitcoins has the bitcoin protocol, protocol is the certain terms and rules for the transaction of the coins over the network, each coin contains the blocks these blocks stores the information, but these information's are securely encoded so that no individual

can hack others coins,Block chain records the transactions accurately.Bitcoin has strong featues like user anonymity and generation of the security key and transparency etc. Even it is a transparent in nature it provide anonymity that is individuals can't see the transaction but can see the bitcoins in there wallet and their transaction result. Bitcoin protocol is designed in such a way that each and every blocks in the chain takes around 10 minutes to mine the bitcoin's or golden coin's.

2. The Bitcoin System

In this section, we represent the main ideas that allow to know and understand the main and basic functionality of the bitcoin digital currency. Such background is needed to understand the meaning of the research performed so far. However, the complexity of bitcoins makes impossible to provide a fully description of the system in this review, so interested readers can refer to [12] for a detailed and more extended explanation on the bitcoin system.Bitcoin is an accounting-based, cryptocurrency. Because of that, looking at bitcoins as digital tokens is not right as bitcoins are interpreted as a balance in a bitcoin account. A bitcoin accounts are defined by a key pair of Elliptic Curve Cryptography. The Bitcoin account is publicly known by its bitcoin address, which is accessed using a unidirectional feature from its public key.Bitcoin is a consensus network that empower a new payment system and a fully digital money system.It is the first most decentralized peer-to -peer payment network to be powered by its consumers without any central authority or intermediary.From the user's point of view,bitcoin is relatively much like Internet cash.

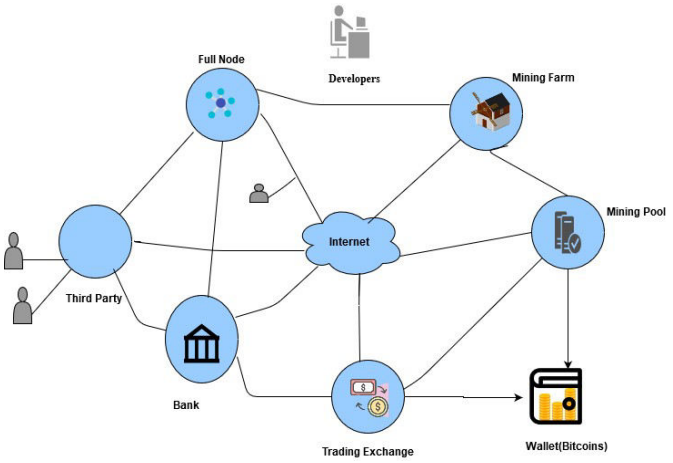

Fig -1: Bitcoin System

Above Figure illustrate the transaction's being processed across the wide range of the network. Above picture depicts the way of the transactions are injected over the network; And shows how the bank and trading exchange of the funds are being processed and how they are inter- connected with each other.Bitcoin transactions are done without central authority or middle man.During the transactions each and every transactions are encode with the private key's,so it can provide the security for the traders as well as for miners for exchanging and digging the golden coins.Each time the transactions are verified in every node's,And each and every blocks in the chain are verified so that miners can't know the new transactions for security purpose.Trades of these coins are commonly dealt with by a trusted in the central association, for instance, a bank and the trade is done. Every PC is related with a framework anyway travels through that association with a circled record. For this circumstance, it keeps an aggregate and open record of each trade that occurs over the framework. Since the structure is open and open, anyone with an Internet affiliation can use the framework to make trades in this record with some other individual on the planet. The daunting tasks in a distributed network system is the bitcoin transaction's need to develop a mechanism, so that entire bitcoin transactions network can order the transaction in manner. Bitcoin is extremely transparent in nature and is the predominant advantage for the ton's of people's because of the independence from the central government , banks and corporation's [11]. And no central or government authority can interfere the bitcoin transaction over the network. And as there is no fees for the transactions , each transactions get saved in the distributed public ledger called block chain. Block chain is the category blocks of the bitcoins. Moreover the bitcoins are not controlled as a network yet it provide the control over the user's finance.

2.1 The Bitcoin Payment

Payments to the Bitcoin system are made through transactions between the Bitcoin accounts. A bitcoin transaction indicates the movement of bitcoin from the source address to the destination address. Source addresses are referred to as input address in the transactions, and destination addresses are named output addresses.A single transaction can have one or more input addresses and one or more output addresses. The transaction specifies the exact sum of bitcoins to be transferred from each input address.The same applies to the output addresses, indicating the total amount of bitcoins that will be transferred to each account. For consistency, the total number of input addresses (source of money) must be greater or equal than the total amount of the output addresses.In addition, the bitcoin protocol enables the input addresses to invest the same sum of the previous transaction received and, for this purpose, each input address will explicitly show the indexof the transaction in which the bitcoins were obtained in the transactions. Suppose if the two input addresses that are precisely similar, indicating that bitcoins have arrived in this bitcoin account in two independent transactions. The transaction is recognized in the bitcoin system by its hash value. however this is the traditional approach of bitcoin verification for frequent bitcoin transfer transactions,the transaction verification can be more

complex and is based on a on a bitcoin transaction script language, and a stack-based execution language.At the end of the day, the owner of the input addresses will make a digital signature using his private keys, showing that he is the true owner of those accounts. Before receiving payment from a standard transaction, the recipient will verify that the input address bitcoins are not previously used Verify whether the digital signature is correct.The first validation prevents duplication (i.e., double-spending) in the bitcoin system and allows the system to be validated in such a way that it needs a ledger where all previous transactions are regularly updated.Before acknowledging the payment, the receiver must be sure that it is the only transaction in the ledger that has an input address with the same Previous Output (Index) of the input addresses of the transaction that must be validated.For this reason, the integrity of the system is based on the assumption that it is not modifiable, while it would be necessary to incorporate it.This append-only database is called blockchain in the bitcoin scheme. The second validation can be performed with the information included in the transaction itself together with the information of the transaction identified in the previous output (Index). Finally, it is worth to mention that the enforcement of spending the total amount of a previous transaction makes very difficult to perform exact payments in the bitcoin system (transactions with exactly a single input address and a single output address), and then users should collect the "change" of the payment in one of his addresses.The address that collects the change in a transaction is referred as a shadow address and it belongs to the same user that performs the payment.

2.2 Technical Significance

Bitcoin is the most mainstream model that is inherently attached to block chain innovation. It is likewise the most questionable one since it assists with empowering a multi billion-dollar worldwide market of mysterious exchanges with none legislative control. Subsequently, it needs to manage various administrative issues including national governments and money related establishments. Be that as it may, Block chain innovation is non-dubious and has worked completely throughout the years and effectively applied to both budgetary and non-monetary universe of utilizations. A year ago, Marc Andreessen, the doyen of Silicon Valley's business people, recorded the block chain dispersed accord model as the most significant innovation since the Internet itself.The current advanced economy is predicated on the dependence on a specific confided in power. Our every single online exchange think confiding in somebody to educate our reality—it is regularly an email specialist co-op revealing to us that our email has been conveyed; it very well may be an affirmation authority disclosing to us that a specific advanced endorsement is dependable, or it is frequently an informal community like Facebook revealing to us that our posts in regards to our life occasions are imparted distinctly to our companions or it is frequently a bank disclosing to us that our cash has been conveyed dependably to our darlings during a remote nation. Bitcoin gained wide popularity and success because of the strong feature it posses that is anonymity feature it has been the key property for the success of the currency deployment.

2.3 The BlockChain Analysis

The Block Chain is a general appended-only database of all bitcoin transactions completed since the network began running back in 2009. Such an approach signifies that the size of the blockchain is increasing exponentially and, for that reason, scalability is probably the biggest challenge the system faces.The blockchain is freely replicated and stored indifferent nodes of the bitcoin network , making the bitcoin a fully distributed system. Transactions are included in the blockchain at time intervals rather than in a flow mode, and this addition is carried out by collecting all new transactions of the system, compiling them together in a data structure called blocks. Like the block at the root of the ledger.Every time a block containing a specific transaction is included in the blockchain, such a transaction is said to be a confirmed transaction as it has already been included in the blockchain and can be checked for double-spending prevention.Blocks are data structures that mainly contain a set of transactions that have been carried out in the system.To obtain the append-only feature, adding a block to the blockchain is a hard problem, so adding blocks to the blockchain is time consuming and work consuming. In addition, every block indexed using its hash value and every new block uses the hash value of the previous block. This mechanism ensures that the change of a block from the middle of the chain would mean that all the remaining blocks of the chain would be changed from that point to the top in order to take all the hash values [11].

3. CONCLUSIONS

The Bitcoin in Current era gained the wide range of popularity and In future it might even replace the official currencies which every countries possess now. Since it is the world currencies, leads to hassle free work of converting currencies since it will be the world

currencies, So it can be used in any country without converting them. In some countries like US, Bitcoin usage are legally approved but still in some countries it is treated has illegal especially in growing countries like India. Bitcoins has tons of advantage's and support's which indeed attract the ton's of individual's. Block chain is the ledger where each and every bitcoins transactions get stored in minutes, Even it is secure and allows person to verify their money goes to/comes from authorized person, Even though having a lots of advantage's some peoples consider bitcoin as disadvantage in economy, because it's new thing , so as time goes on things get changed and they're going to be a least drag about it.

REFERENCES

[1] Sanjay Singh Rajpurohit, Talha Khan "Blockchain and Crypto-currency Based Transaction Systems"Department of Information Technology, SSIPMT,Raipur (C.G), India. 2018 march.

[2] Satoshi Nakamoto,"Bitcoin: A Peer-to-Peer Electronic Cash System".

[3] Michael Crosby, Nachiappan,Pradhan Pattanayak, Sanjeev Verma, AmericaVignesh"Blockchain Tenchology beyond bitcoin".

[4] Joseph Bonneau,Andrew Miller, Jeremy Clark, Arvind Narayanan,Joshua A. Kroll,Edward W. Felten "SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies".

[5]A.Back, "Hashcash - a denial of service counter-measure,"http://www.hashcash.org/papers/hashcash.pdf, 2002.

[6] Mauro Conti, Sandeep Kumar E, Chhagan Lal, Sushmita Ruj " A Survey on Security and Privacy Issues of Bitcoin".

[7]Reid, F., Harrigan, M.: An analysis of anonymity in the bitcoin system. In:Altshuler, Y., Elovici, Y., Cremers, A.B., Aharony, N., Pentland, A. (eds.) Securityand Privacy in Social Networks, pp. 197–273. Springer, New York (2013).

[8]S.Haber, W.S. Stornetta, "How to time-stamp a digital document," In Journal of Cryptology, vol 3, no2, pages 99-111, 1991.

[9]Androulaki, E., Karame, G.O., Roeschlin, M., Scherer, T., Capkun, S.: Evaluatinguser privacy in bitcoin. In: Sadeghi, A.-R. (ed.) FC 2013. LNCS, vol. 7859, pp.34–51. Springer, Heidelberg (2013).

[10] Ron, D., Shamir, A.: Quantitative analysis of the full bitcoin transaction graph.In: Sadeghi, A.-R. (ed.) FC 2013. LNCS, vol. 7859, pp. 6–24. Springer, Heidelberg(2013).

[11]Research and Challenges on Bitcoin Anonymity,Jordi Herrera-Joancomart ı(B)Dept. d'Enginyeria de la Informacio i les Comunicacions,Universitat Aut`onoma de Barcelona, 08193 Bellaterra, Catalonia, Spain.

[12]Maxwell, G.: Coinjoin: Bitcoin privacy for the real world. post on bitcoin forum.https://bitcointalk.org/index.php?topic=279249.