Understanding Bitcoin and Blockchain

Mohammed Danish Uddin

Suroju Samyuktha

Department of Computer Science and Engineering

Email:{danishdanish020@gmail.com}

{samyuktha.suroju@gmail.com}

Abstract **-2017 is the year when the cryptocurrencies came into limelight with the primary trading in bitcoin being featured on a mainstream market in Chicago, Since then many people started investing into bitcoins or at least wanting to know about bitcoin, mostly including the people from the software industry. In this article it is clearly defined in a stepwise order using meaningful pictures and figures, from the very beginning of cryptocurrencies to the technology behind bitcoin, that is the blockchain technology. Most people do not trust in the security of trading in cryptocurrencies, but after understanding the working of Blockchain one would definitely believe in the technical security of using a cryptocurrency but the financial reasoning to investment in cryptocurrencies is a whole another story.**

Index Terms**—Cryptocurrency(crypto currency), Bitcoin, Blockchain(Block chain),Consensus.**

I. INTRODUCTION

In the real world banks play an important role in each and every transaction of money from the sender's account to the receiver's account, the banks has all the possibilities to play with your money whether the transaction is online or offline. we have several rules and regulation on the real world currency that we use for exchanging of commodities, here the government or the bank acts as the third party imposing several control over the currency generated, used or destroyed but in case of cryptocurrency there is no centralized authority, all the transactions are done and verified in a very technical way without the utilization of any central governing authority, no rules and regulations can ever be forced by the government on the use, generation, or destruction of any cryptocurrency. Cryptocurrencies on one side being completely decentralized and on the other hand are vulnerable to be used for any illegal activities, during the transaction of money from the sender to the receiver the identity of both the sender and the receiver is kept encrypted(hidden) no one would ever know from where the money have been transmitted and to whom other than the sender and therefore the receiver themselves. Use of blockchain technology definitely guarantees safe and secure transactions but not genuine transactions.

II. CRYPTOCURRENCY

A. What is Cryptocurrency

In March 2018, the word "cryptocurrency" was added to the Merriam-Webster Dictionary and it

states that "Any form of currency that only exists digitally, which usually has no central issuing or regulating authority but instead uses a decentralized system to record transactions and manage the issuance of recent units, and which relies on cryptography(encryption) to stop counterfeiting and fraudulent transactions."

Cryptocurrencies use decentralized control as against to centralized electronic money and central banking systems. The decentralized control to each cryptocurrency works through distributed ledger technology, typically a blockchain, that assists as a public financial transaction database.

B. *Types of Cryptocurrencies*

Since May 2018, over 1,800 cryptocurrency specifications existed, Within a cryptocurrency system. The 5 most significant cryptocurrencies listed below with their respective logos in Fig.1.Logos of 5 most significant cryptocurrencies.

1) Bitcoin
2) Ethereum
3) Monero
4) Ripple
5) Litecoin

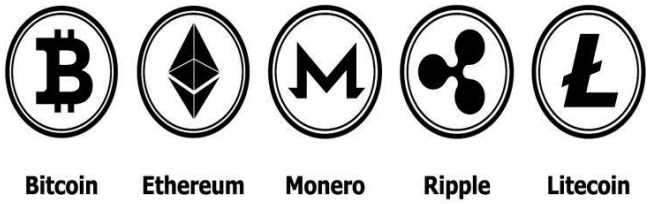

Fig. 1.Logos of 5 most significant cryptocurrencies.

III. BLOCKCHAIN

A. *Blockchain: The Technology Behind Cryptocurrency*

A blockchain is a growing list of records called blocks, which are linked using cryptography. Blockchains which are readable by the public are widely used by cryptocurrencies, So, the record can not be altered retroactively without the alteration of all subsequent blocks and also the consensus of the network. This let the participants to authenticate and audit transactions economically. Blockchain technology can be integrated into multiple areas. The first use of blockchain today is as a distributed ledger for cryptocurrencies, most notably bitcoin.

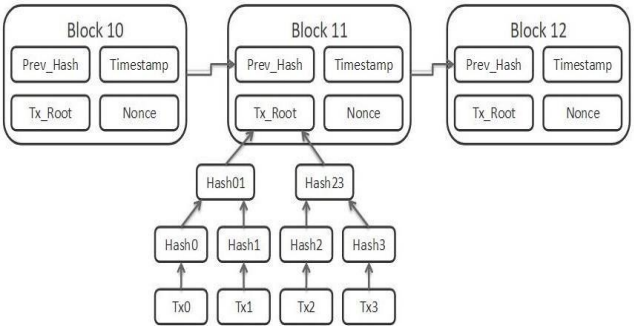

Fig. 2. Blockchain structure

B. *A Block in a Blockchain*

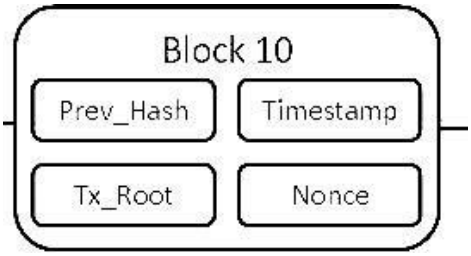

Fig. 3.A block

Blocks hold batches of valid transactions that are hashed and encoded into a Markle tree. Each block is said to comprise of the subsequent properties

- Prev_Hash
- Timestamp
- Tx_Root or Markle tree or Hash tree
- Nonce

C. *Peer to Peer Network in Blockchain*

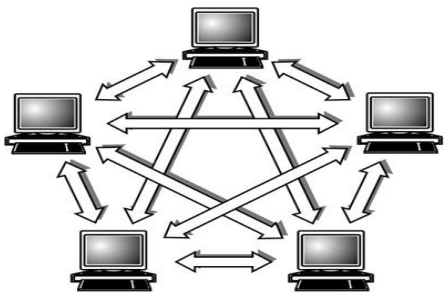

Fig. 4.A Peer to peer(P2P) network

Peer to peer network is said to make up the blockchain. In a P2P network, the "peers" are computer systems which are connected to each other via the Internet. Information are often shared directly between systems on the network without the requirement of a central server. In other words, each computer on a P2P network becomes a file server as well as a client, as illustrated in Fig. 4.

One way that blockchain secure itself is by being distributed, When someone joins the network he/she gets the complete copy of the blockchain that can be used to see if everything is in order when someone creates a new block(transaction) that block is send to everyone on the network, then each person(node) then verifies the block to make sure that it has not been tampered with and if everything is verified then, each person(node) adds this block to their chain and then all the nodes in this network are said to create consensus.

D. Functioning of a Blockchain

Step 1:

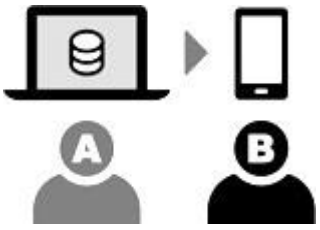

Fig. 5. A wants to send money to B

Step 2:

Fig. 6. The transaction is represented online as a block

Step 3:

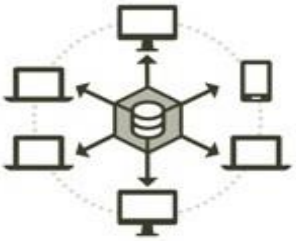

Fig. 7. The block is broadcasted to every party in the network

Step 4:

Fig. 8.The network approves the transaction

Step 5:

Fig. 9. The block is added to the existing blockchain
in a transparent and unaltered way

Step 6:

Fig. 10. The transaction is complete

IV. BITCOIN

A. What is Bitcoin

Bitcoin is a cryptocurrency created in 2009. It follows the concepts set out in a white paper by the mysterious Satoshi Nakamoto, whose real identity has yet to be confirmed. Bitcoin offers the promise of lower transaction fees than traditional online payment mechanisms and is operated by a decentralized authority, unlike government-issued currencies.Bitcoins can be sent from user to user on the peer-to-peer bitcoin network directly, without the necessity for intermediaries. Transactions are verified by network nodes through cryptography then recorded in a public distributed ledger termed as blockchain. In fact, there are only 21 million bitcoins which will be mined in total. Once miners have unlocked this number of bitcoins, the planet's supply will essentially be tapped out, unless bitcoin's protocol is modified to permit for a larger supply.

B. The World's Largest Cryptocurrency

A single bitcoin varies in value daily, As on 11th August 2018 the market values of 1 bitcoin when converted to Indian rupees is approximately equal to Rs. 4,00,000 (4 lakh rupees), While the other cryptocurrencies are long behind the worth of a bitcoin.

C. Acquiring or Buying a Bitcoin

Step 1 **:** Create a virtual wallet

Fig. 11. shows a screenshot of a virtual wallet which shows the balance and other necessary information about the person's virtual wallet.

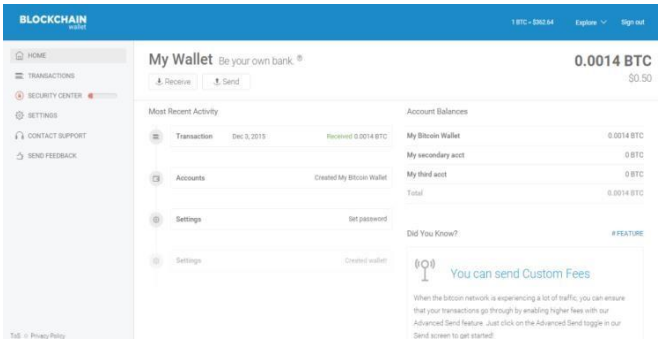

Fig. 11.A virtual wallet

Step 2 **:** Buy Bitcoins from wallet exchange

To buy a Bitcoin, real money should be deposited through an online payment company or transferred directly from a bank account into an account on a third-party website that connects Bitcoin buyers and sellers, one of those is Zebpay which is an Indian Wallet Exchange from where you will buy/sell bitcoins easily and quickly. The transactions are fast and quick.

Fig. 12.Zebpay logo

Step 3 **:** Buy Bitcoins from a Third party

Bitcoins can even be purchased from third parties such as a friend or a closeby trader, you can also buy from exchangers online via bank transfer or a host of other electronic payment methods, including PayPal, Moneygram and Western Union. The company charges a small fee per transaction.

Step 4 **:** Bitcoin mining

Mining bitcoins is incredibly complex and, honestly, probably is not something beginners should dabble in. The method involves using special software (and expensive mining

computers that suck up a lot of power) to resolve mathematical algorithms in exchange for bitcoins.

V. CONCLUSION

Cryptocurrency appears to have move past the early implementation stage that new technologies experience. Even motorized vehicles experienced this phenomenon. Bitcoin has begun to carve itself a distinct segment market, which could help advance cryptocurrencies further into becoming mainstream; or be the main cause of it failing. Cryptocurrencies are still in their infancy, and it is difficult to determine if they will ever find true mainstream presence in world markets. Also, the block chain technology that acts as Bitcoin's backbone has potential uses in other ways, like smart contracts (Hileman, 2016). These contracts are programmed payments that occur when a set condition occurs. Predetermined payment contracts are normally carried out by an entire accounting department of a company, making this an extremely interesting topic of further transformation. It possible that the future holds a place for cryptocurrency as a major currency solution, and Bitcoin will be instrumental in paving the way for those currencies to flourish. The European and Latin America markets are exploding with Bitcoin transactions, signifying real validity. Additional topics to explore regarding Bitcoin and cryptocurrencies are quite abundant. Extensive studies should be performed on the economic effects of Bitcoin's effect on long standing fiat currency performance, and compare the results to countries that are beginning to adopt state-sponsored cryptocurrencies.The Bitcoin can be useful to lot of people. Since they are an international currency. You can use them in any country without having to convert between currencies. The Block chain is really secure and it lets you make sure your money goes to or come from the right person.

REFERENCES

[1] N. T. Courtois, M. Grajek and R. Naik, "Optimizing sha256 in bitcoin mining", Cryptography and Security Systems, *2014*.

[2] A. Gervais, G. O. Karame, V. Capkun and S. Capkun, "Is bitcoin a decentralized currency?", IEEE Security & Privacy, vol. 12, no. 3, pp. 54-60, 2014.

[3] J. Garay, A. Kiayias and N. Leonardos, "The Bitcoin Backbone Protocol: Analysis and Applications", Cryptology ePrint Archive Report 2014/765, *2014*.

[4] https://bitcoin.org/bitcoin.pdf

[5] D. Chaum, A. Fiat and M. Naor, "Untraceable electronic cash", *CRYPTO*, 1990.

[6] S. Barber, X. Boyen, E. Shi and E. Uzun, "Bitter to Better-How to Make Bitcoin a Better Currency", *Financial Cryptography*, 2012.

[7] Bonneau J, Miller A, Clark J et al. (2015) Sok: research perspectives and challenges for bitcoin and cryptocurrencies. Secur Privacy IEEE, pp 104–121.