Blockchain and Cryptocurrency: The World of Blockchain and Cryptocurrency

Greeshma C Shekar[1]

[1]Department of Computer Science and Engineering, Dayananda Sagar University, Bangalore, Karnataka, India

Author's Mail Id: greeshma.shekar03@gmaill.com, Tel.: +91-9663762093

Abstract— The primary aim of Blockchain Technology is to maintain a wide variety of digital information that can be efficiently documented and distributed but, makes it difficult or impossible to edit, hack or cheat the system. In other words, the Blockchain Technology ensures security, transparency as well as decentralization of the digital asset. It can also be thought as a chain or interconnected records, that is stored in the form of blocks which is controlled by no single authority. Blockchain Technology forms the substratum for Bitcoin and other Cryptocurrencies. The Cryptocurrencies can operate without the need for central authority, with the help of Blockchain Technology. This research paper deals with how the World of Cryptocurrency is driven by the Blockchain Technology.

Keywords—Blockchain Technology, Bitcoin, Cryptocurrencies, and blocks.

I.   INTRODUCTION

The first embodiment of blockchain technology emerged back in 2009 with the bitcoin blockchain, a secure, transparent, peer to peer digital asset system. Since, bitcoin is obtainable by anyone, it is appropriate to call it an open, or even permissionless blockchain.

Today, blockchains have rapidly become the most popular and widely recognized form of distributed ledger Technology (DLT). DLT being the digital system is used for recording the transactions as well as their details in multiple places at the given same instance.

Fig.1. Cryptocurrencies

Overnight, one of the new currencies known as the bitcoin is being traded in the bitcoin exchanges or crypto exchanges. The dollar value has been emerging exponentially since 2012. Both, the bitcoin and the blockchain, the universal ledger where the bitcoin transactions are documented, are ruling the cryptocurrency insurgency.

The reason for blockchain being widely known and accepted is the digital financial transactions and cross-border payments.

This paper deals with the methodology in transaction of cryptocurrencies using blockchain, results and discussions, conclusion, and reference.

Fig.2. Binance 1

II.   RELATED WORK

Zibin Zheng, Shaoan Xie, Hong-Ning Dai Authors, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends."

III. METHODOLOGY

Before moving onto methodology concerned in transactions, one should know the different types of blockchains.

A. Public Blockchains
The public blockchains can be simply said as the open, and decentralized networks accessible to anyone participating, to solicit or certify a transaction. Those who certify are referred to as miners, who earn rewards for validating.
2 classic examples of public blockchains are Bitcoin as well as Ethereum (ETH) blockchains.

B. Private Blockchains
In comparison to public blockchains, private blockchains are not open, and possess access limit. Anyone who wishes to join, should need permission from the administrator of the system. In simpler words, private blockchains are ruled by an associate entity, that is they are centralized, such as Hyperledger.

C. Hybrid Blockchains or Consortiums
Consortiums are basically a combination of both, the public and the private blockchains. It contains the centralized as well as decentralized characteristics, such as Dragonchain and R3.

D. Sidechains
It is one of the blockchains, running in parallel to the main chain, allowing users to move digital assets between any two blockchains and improves both the scalability as well the efficiency. An example of which is Liquid Network.

Let's look into how a public blockchain work, since cryptocurrency exchanges occur globally using public blockchain at a larger scale.

In today's society, we have created ledgers in order to store information with the help of varies applications. Ledger in bookkeeping, records all the transactions that occur in the cryptocurrency exchanges. However, this lacks transparency as well as accountability, making it difficult for one participating party to verify the other party's records.

Records that are stored by using traditional ledgers are easily editable, removed, or even a new record can be added, making it less trustable with respect to the information being accurate.

These problems are solvable by the use of public blockchains, making it trustable by evolving traditional bookkeeping model to triple-entry bookkeeping, which means transactions on blockchains are basically cryptographically sealed by third entry. This generates a shielded record of stored transactions in blocks, which are then verified by a fault-tolerant mechanism (distributed census mechanism).

The fault-tolerant mechanisms allow contributions from over thousands of participants, who work on confirmation and authentication of transactions which are occurring on blockchains as well as block mining activities.

Mining is not ubiquitous to all blockchains, but a type of consensus mechanism being used in Bitcoin as well as Ethereum. Ethereum is on the verge to move to a different – proof-of-stake (PoS) by 2022.

When sending bitcoins, one pays a minimal fee in bitcoin for the computer network to validate his/her transaction, which is then clustered with various other transactions pending in queue in order to be added into a new block.

The nodes later operate to validate the list of transactions in the block, which is done by solving a mathematical problem that is complex to arise with a hash (64-digit hexadecimal number).

Fig.3

On solving this, the block is then added to the network. The fee paid, is combined with other transactions fees in the block, which is the miner's award.
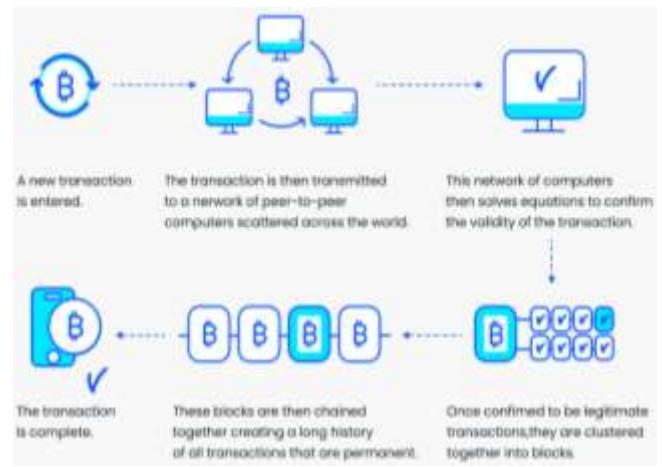

Fig.4

The Proof of work (POW) is a fault tolerant mechanism algorithm which is used by most of the well-known cryptocurrency networks, such as Bitcoin and Ethereum. It requires a active node to justify that the work has been done as and submitted by them to receive the authority to add new transactions to blockchain, requiring high energy and long processing time.

The Proof of Stake (POS) is an alternative to POW consensus algorithm that requires a low-cost and is low-energy consuming. It is an algorithm for attestation; however, transactions get validated by a validator on the basis of the coins they hold, also called as their stake. There is no technical mining as well as block reward involved for individuals.

IV.   RESULTS AND DISCUSSION

Blockchain Technology is a decentralized ledge of all the digital transactions across a network called peer-to-peer network. Participants have the freedom to confirm transactions without even the need for a central clearing authority.

Fig.5. Credits: pwc.com

Cryptocurrency is the medium of exchange which is created and stored digitally in blockchain, using encryption techniques for security in order to control creation of monetary units and also to certify the transfer of funds. Cryptocurrency has no intrinsic value, physical form, and its supply is not determined by any central authority such as central banks and the network is completely decentralised.

**How Blockchain works:**
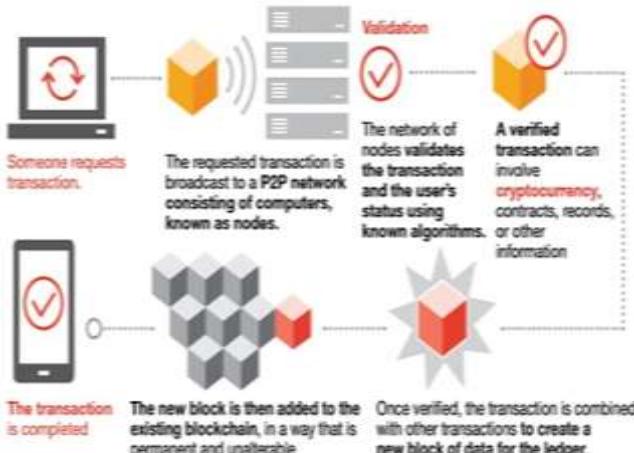
Fig.6. Credits: pwc.com

Blockchain has other significant applications other than cryptocurrencies as well, such as:

Automotive: Buyers can use blockchain to maintain ownership in autonomous cars.

Voting: Blockchain is used for coding, where voters can cast their votes in smartphones, computers or tablets leading to instant verifiable results.

Healthcare: Patients' health records is encrypted which may be shared with a couple of different producers without compromising the safety and threat of privacy breaches as well.

A. Title and Author Details
Blockchain and Cryptocurrency: The world of Blockchain and Cryptocurrency. Greeshma C Shekar, *Computer Science and Engineering, Dayananda Sagar University, Bangalore, Karnataka, India.*
greeshma.shekar03@gmail.com

Table. 1 The market trends

Name	Last Price in $	24h Change
BNB	305.10	- 4.34%
Bitcoin	31,360.43	-3.41%
Ethereum	1871.17	-4.72%
Chiliz	0.24300	-10.59%
Filecoin	46.74	-4.81%
Cardano	1.18	-5.23%

### B. Global Cryptocurrency charts
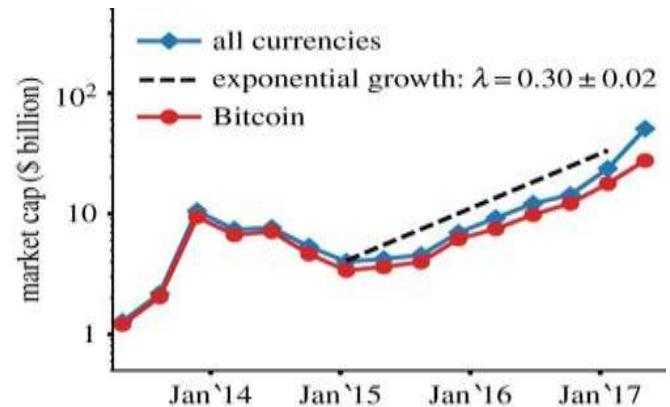
Fig.7. Credits: The Royal Society Publishing

Total Cryptocurrency market capitalization excluding Bitcoin
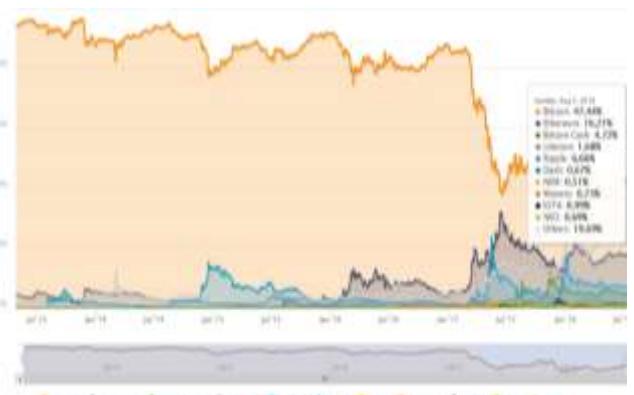
Fig.8. Major Crypto assets by percentage of total market capitalization

V.   CONCLUSION

Blockchain was first introduced by David Chaum, a cryptographer in the year 1982, following which Staurt Harber and W. Scott Stornetta in the year 1991 wrote consortiums. It was Satoshi Nakamoto who founded Bitcoin, he sent ten bitcoins to Hal Finney in 2004 which became first proof of work system.

Bitcoin is a combination of:
[1] Peer to peer payment system
[2] Digital gold which is, it is a store of gold like value
[3] Not controlled by any authority which is decentralised system.

Blockchain adoption is free of cost, however using the network will cost for performing transactions, incentives for transactions and a cost involved in deployment.

The primary purpose of Bitcoin, a cryptocurrency was to support digital payment systems based on cryptography which security instead of trust.

Public blockchain cannot be modified or edited after data has been permitted by the nodes which provides integrity and security mainly.

Thus, to summarize, blockchain, a distributed ledgers is behind the cryptocurrency. Today, no other applications of blockchain have had our attention, investment as well as development as cryptocurrency has.

Now is the time to think and invest, not fear and lose the opportunity because blockchains are designed in a way to protect the transaction integrity but not transaction privacy. Transactions can only be tracked from sender to receiver through their wallets, ensuring security and transparency to the participants.

VI.   RELATED WORK

[1] Zibin Zheng, Shaoan Xie, Hong-Ning Dai Authors, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends."
[2] Jianyu Niu, Ziyu Wang, Fangyu Gai, Chen Feng Authors, "Incentive analysis of Bitcoin-NG, revisited."

REFERENCES

[1] Zibin Zheng, Shaoan Xie, Hong-Ning Dai Authors, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends."
[2] https://www.investopedia.com/terms/c/consensus-mechanism-cryptocurrency.asp
[3] https://www.binance.com/en
[4] coinmarketcap.com
[5] Syed Zishan Ali, Dolly Sahu, Jatin Sahu Authors, "Bitcoin in Blockchain: A Survey", **Vol. 7, Issue 6, June 2019, IJCSE.**
[6] Mausumi Das Nath, Tapalina Bhattasali Authors, "Impact of Blockchain to Secure E-Banking Transaction", **Vol. 7, Issue 18, May 2019, IJCSE.**

AUTHORS PROFILE

Miss. Greeshma C Shekar is pursuing Bachelor of Technology degree in department of Computer Science and Engineering from Dayananda Sagar University, located in Bangalore, Karnataka, India. She is currenctly in her final year of Engineering and will be graduating from Dayananda Sagar University in the year 2022.