BLOCKCHAIN: - FUTURE OF THE WORLD

Shantanu Gade, Mayur Manwar, Sidhharth Rasal, Vishal Kotkar

Shobha Raskar

Jaya Mane

[#]*Modern Education Society's College of Engineering, 19, Late Principal V. K. Joag Path, Wadia College Campus Pune-411001 Computer Department Savitribai Phule Pune University*.

Abstract

Now a days,the internet is becoming more accessible and convenient, larger numbers of people and businesses are shifting towards digital transactions. Digital payment methods is an quicker, cheaper and much more efficient. Therefore, it is not surprising that the newer forms of digital payment systems are rapidly being developed. When we generastoredcompared no other method comes even close to the giant that is cryptocurrency. Cryptocurrencies like Bitcoin and Ethereum are among most popular forms of digital payments. Cryptocurrencies could be popularized in India as a viable option for digital currency, but it has both pros and cons which need to be acknowledged. Through the means of the literature review, this research paper will analyze the cryptocurrency, its working and perform a comparative study between China and India. Also, it considers the current status as well as the scope of cryptocurrency in India..

Keywords— Blockchain, Bitcoin, Consensus, Mining, Security, Internet of Things, Hyperledger.

I. INTRODUCTION

A Cryptocurrency is a peer-to-peer digital exchange system in which cryptography is used to generate and distribute currency units [1]. This process the requires distributed verification of transactions without a central authority. Transaction verification confirms transaction amounts, and whether the payer owns the currency they are trying to spend while ensuring that currency units are not spent twice. This verification process is called mining [2]. Cryptocurrencies use a variety of mining technologies, according to their particular requirements. For instance, certain Cryptocurrencies focus on restricting the number of transactions validated per unit time, while others concentrate on achieving fast, lightweight services [3]. Some
Of the mining algorithms are deliberately memory intensive; others are computationally expensive [4]. In this paper, we
have survey the Cryptocurrency mining systems and analyze their efficiency.

The remainder of this paper is organized as follows: Section II defines relevant terms. Section III provides historical perspective and background. Section IV provides the overview of Blockchains [16]. Section V overviews the mining, while Section VI provides further details. Section VII discusses relevant Hash algorithms. Section VIII addresses problems encountered with Cryptocurrencies. And Section IX offers conclusions. And the Proof construction requires intensive use of memory and/or computational power. The proof requirement also restricts the number of transactions that can be validated (and consequently the number of blocks added to the ledger) in a given time period. This restriction is necessary because, with

each block mined, new currency units—the total of which is finite—are produced.

- GENERAL WORKING PRINCIPLES OF CRYPTOCURRENCIES

The first fully implemented decentralized Cryptocurrency was Bitcoin, published by Nakamoto in 2008-09 [5]. Before this there were published articles about peer-to-peer currency systems but none were implemented. Following the success of Bitcoin, several others came into existence. Figure 1. A Bitcoin Blockchain (adopted from [5]) be linked with bank accounts and credit cards, and users can pay someone or receive payment through the PayPal accounts. PayPal does not have a its own currency. M-Pesa [22] was established by Vodafone initially in Africa, which later spread to other continents. M-Pesa is the mobile, online payment system in which the user can deposit money into an account stored in their cell phones and send PINsecured SMS texts to other users in order to send money [22]. All these online monetary systems were based on fiat currencies [23], whereas a Cryptocurrency has its own currency.

Cryptocurrencies work functionally as follows [19]:

• Ahe user has a wallet with a generated address. This address acts as a public key [24].

• The wallet also contains a generated private key, which is used to sign transactions, proving ownership [24].

• The payer sends money to the payee's address, and signs it using the payer's private key.

• The transaction is verified by mining [2].

- . BLOCKCHAIN OVERVIEW

1) A Blockchain is a distributed public ledger of Cryptocurrency transactions [17]. Each verified transaction is accumulated in a block [25]. Each block consists of a variable number of the verified transactions. The maximum size of a block is fixed in each Cryptocurrency system, providing an upper bound to the number of transactions included. For instance, the maximum size of a Bitcoin [5] block is 1MB. Figure 1 shows a simplified representation of a Bitcoin Blockchain.
2) *Private Blockchain:* Private exchange and data sharing between multiple organizations or between a single organization (or groups of people) is the private blockchain system whose mining is controlled by selected people or organizations. Private blockchains are also known as authorized blockchains. This is because unknown members cannot access it without special permission. And the person who controls the set of rules decides to join the node. This tends to centralize the network. When a node becomes part of the network of a private blockchain system, the node contributes to the execution of the distributed system, and each node imitates the law and works together to obtain upgrade approval. Unlike the public blockchain, it is reluctant to write operations. Compared to public blockchain, it is very cheap and fast because it does not require a huge amount of money, time and energy to get approval. Examples of private blockchains include Corda, Hyperledger, and Fabric. Corda allows businesses to build blockchain networks that can support inter-company contracts.

volatili

[5] FAIJAN AKHTAR, JIAN PING LI, MD BELAL BIN HEYAT, SYED LUQMAN QUADRI, SHAIK SOHAIL AHMED, XIAO YUN, AMIN UL HAQ.
"POTENTIAL OF BLOCKCHAIN TECHNOLOGY IN DIGITAL CURRENCY: A REVIEW." 978-1-7281-4242-5/19/$31.00 ©2019 IEEE.

[6] Suman Ghimire and Dr. Henry Selvaraj. "A Survey on Bitcoin Cryptocurrency and its Mining."
978-1-5386-7834-3/18/$31.00 ©2018 IEEE.

[7] Ujan Mukhopadhyay, Anthony Skjellum, Oluwakemi Hambolu, Jon Oakley, Lu Yu and Richard Brooks.
"A Brief Survey of Cryptocurrency Systems." white paper 2016.

[8] Jae Min Kim, Jae Won Lee, Kyungsoo Lee and Junho Huh. "Proof of Phone:A Low-cost Blockchain Platform"
Self-published.

[9] Yong Yuan and Fei-Yue Wang. "Blockchain and Cryptocurrencies: Model, Techniques, and Applications"
2168-2216-2018 IEEE.

[10] Wenzheng Li and Mingsheng He. "Comparative Analysis of Bitcoin, Ethereum, and Libra"
978-1-7281-6579-0/20/$31.00©2020 IEEE.

[11] Antea Knezevic, Zvonimir Musa and Tihana Babic. "Cryptocurrency as the currency of the future: a case study among ALgebra University College students."
MIPRO 2020, September 28 - October 02, 2020, Opatija, Croatia.

[12] Joseph Bonneau, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A. Kroll, Edward W. Felten.
"SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies"
2015 IEEE Symposium on Security and Privacy. DOI 10.1109/SP.2015.14.

[13] Dr. R. Raju, M. SaiVignesh and K. Infant Arun Prasad. "A Study of Current Cryptocurrency Systems"
In 2018 INTERNATIONAL CONFERENCE ON COMPUTATION OF POWER, ENERGY, INFORMATION AND COMMUNICATION (ICCPEIC).
978-1-5386-2447-0/18/$31.00 ©2018 IEEE.