Chapter 2
Blockchain Technology: Principles and Algorithms

Mohammad Khalid Imam Rahmani
https://orcid.org/0000-0002-1937-7145
Saudi Electronic University, Saudi Arabia

ABSTRACT

Blockchain is a distributed decentralized peer-to-peer network aiming to facilitate the immutability and security of data. Towards the service orientation, blockchain is a collection of distributed blocks having unique hash codes without any point of failure. Each block is stored on distributed ledgers, and transactions with them are secure, transparent, immutable, and traceable. To create a new block and allow a transaction to complete, an agreement between all parties is required. To reach an agreement in a blockchain network, consensus algorithms are used. In this chapter, fundamental principles and algorithms of blockchain networks have been discussed, and a detailed review of the blockchain consensus algorithms PoW, PoS, DPoS, PoET, PoWeight, PoB, PoA, and PoC have been provided including the merits and demerits of consensus algorithms with analysis to provide a deep understanding of the current research trends and future challenges.

INTRODUCTION

Blockchain is a distributed decentralized peer-to-peer network to facilitate transactions between participants that are not only secure but also transparent, immutable, and traceable (Ali et al., 2020). Blocks are stored on distributed ledgers having unique hash codes without any point of failure. The consensus algorithms and the underlying protocols are the backbones of Blockchain technology. The main objective of

DOI: 10.4018/978-1-7998-8382-1.ch002

blockchain technology is to make the concept of personal online valet a widespread reality in the entire world without fear of loss, cheat, or theft because there is no control of the government, banks, or any third party (Niranjanamurthy et al., 2019).

To create a new block and allow a transaction, a mutual agreement between all parties is required. Therefore, in a Blockchain network, various consensus algorithms are used for reaching that agreement. In the rapidly growing blockchain network initiatives in Government as well private departments, the security of the blockchain or cryptocurrencies is a major issue. The security assurance of the blocks and their transactions is a key to winning the trust of users for the safety and secrecy of the digital valet being spent by different parties over a network channel. The economical and widespread requirement of good quality consensus algorithms has created great opportunities for exploring more trustworthy and acceptable consensus techniques for first acquiring the blocks and then securing the transactions in a more efficient way (Jamil et al., 2021).

In this paper, first I have discussed some fundamental principles of Blockchain technology and then have given a detailed account of the Blockchain consensus algorithms as given by Alsunaidi et al. (2019), Gramoli (2020), Zheng et al. (2017), Pahlajani et al. (2019), and Bamakan et al. (2020) such as Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Proof of Elapsed Time (PoET), Practical Byzantine Fault Tolerance (PBFT), Delegated Byzantine Fault Tolerance (DBFT), Proof of Weight (PoWeight), Proof of Burn (PoB), Proof of Capacity (PoC), Proof of Importance (PoI), and Proof of Activity (PoA) including their merits and demerits to acquaint the researchers with the current research trends and future application challenges of Blockchain technology.

BACKGROUND

Blockchain can be dated back to 1982 when David Chaum proposed a similar protocol (Sherman et al., 2019; Chaum et al., 1998). Satoshi Nakamoto implemented the first digital currency Bitcoin using a Blockchain network and sent ten Bitcoins to Hal Finney (Buterin, 2014). Similar to the Internet there is no owner of the blockchain technology but people can have their blockchains.

WORKING PROCEDURE

Ledgers are used to record all transactions of a company through bookkeeping. There are two conventional bookkeeping methods: Single-entry and Double-entry methods. Single-entry ledgers are not transparent so their accountability