Chapter 2
A Brief Analysis of Blockchain Algorithms and Its Challenges

Rajalakshmi Krishnamurthi
Jaypee Institute of Information Technology, India

Tuhina Shree
Jaypee Institute of Information Technology, India

ABSTRACT

Blockchain is the world's most trusted service. It serves as a ledger that allows transaction to take place in a decentralized manner. There are so many applications based on blockchain technology, including those covering numerous fields like financial services, non-financial services, internet of things (IoT), and so on. Blockchain combines a distributed database and decentralized ledger without the need of verification by central authority. This chapter surveys the different consensus algorithms, blockchain challenges, and their scope. There are still many challenges of this technology, such as scalability and security problems, waiting to be overcome. The consensus algorithms of blockchain are proof of work (POW), proof of stake (POS), ripple protocol consensus algorithm (RPCA), delegated proof of stake (dPOS), stellar consensus protocol (SCP), and proof of importance (POI). This chapter discusses the core concept of blockchain and some mining techniques, consensus problems, and consensus algorithms and comparison algorithms on the basis of performance.

INTRODUCTION

Blockchain is one of the most important services. It is a database which contains information about all the transaction ever executed in the past and works on bitcoin protocol. It combines a distributed database and decentralized ledger and there is no need of verification by a central authority. In blockchain, the completed blocks are recorded and added to the blockchain in chronological order so that market participants can keep track of digital currency transaction without central record keeping. Each time the block is completed, the new block is generated and completed blocks goes into the blockchain as a permanent database. Each block contains a hash of the previous block. The blockchain has all the

DOI: 10.4018/978-1-7998-5351-0.ch002

information about user address and their balances from the genesis block to the most recent block. The first block is called as genesis block in blockchain. The blockchain was designed so that the transactions cannot be deleted. The blocks are added using cryptography so that data can be distributed but not copied. The continuous growth of blockchain can be considered as a problem to some, such as creating issue of storage and synchronization. Blockchain works on bitcoin protocol. *So now what is bitcoin?*

Bitcoin is digital currency released as open source software (Singh, 2016) and was first invented by a researcher 'Nakamoto' in 2008. It is a digital token that can be stored in a digital wallet and is designed to work as a currency. It is often called as a cryptocurrency because encryption techniques are used to secure transactions and controls the creation of additional units. It is a decentralized cryptocurrency produced by all the participating nodes in the system at a defined rate. The chain of bitcoin created over period and linked to each other called block chain. Bitcoin, which gave birth to the concept of blockchain and Ethereum. Ethereum, is an open source, public, blockchain based distributed computing platform and operating system featuring smart contract functioning. Through blockchain, bitcoin is solved the double-spending problem which is the risk, particularly when digital currency is exchanged, that a person could concurrently send a single unit of currency to 2 different sources. So, the bitcoin become unique because it solved the double-spending problem through blockchain.

The main objective of this work is overview and compares different consensus algorithms. There are so many algorithms which are currently using for blockchain technology. So, for the comparison, we have taken some commonly used algorithms like Proof of Work (POW), Proof of Stack (POS), Proof of Importance (POI), delegated Proof of Stake (dPOS), Practical byzantine fault tolerance and Ripple Transaction Protocol. Then we will compare those algorithms based on properties of blockchain and how they are fit for the blockchain technology. This work focuses on steps of the algorithm, scalability and method of algorithm and security risks present within the algorithm. We will discuss about consensus problem which includes The Byzantine Generals Problem, Byzantine Fault Tolerance (BFT) and Delegated Byzantine Fault Tolerance (dBFT).

Key contributions of this chapter are:

- First understand the core concept of blockchain.
- Secondly analyze the architecture of blockchain and some mining techniques.
- Then discuss about consensus problems and consensus algorithms including steps of algorithm and scalability of algorithm.
- Then analyze and compare the algorithms on the basis of performance and security risk present in algorithm.
- Finally conclude with limitations of blockchain.

THEORETICAL BACKGROUND

In this section, our focus is on core concept of blockchain, architecture of blockchain and some mining techniques used in blockchain.