Chapter 10
Blockchain and Its Integration as a Disruptive Technology

Dhanalakshmi Senthilkumar
https://orcid.org/0000-0003-0363-5370
Malla Reddy Engineering College (Autonomous), India

ABSTRACT

Blockchain is the process of development in bitcoin. It's a digitized, decentralized, distributed ledger of cryptocurrency transactions. The central authorities secure that transaction with other users to validate transactions and record data, data is encrypted and immutable format with secured manner. The cryptography systems make use for securing the process of recording transactions in private and public key pair with ensuring secrecy and authenticity. Ensuring bitcoin transaction, to be processed in network, and ensuring transaction used for elliptic curve digital signature algorithm, all transactions are valid and in chronological order. The blockchain systems potential to transform financial and model of governance. In Blockchain, databases hold their information in an encrypted state, that only the private keys must be kept, so these AI algorithms are expected to increasingly be used, whether financial transactions are fraudulent, and should be blocked or investigated.

INTRODUCTION

Blockchain is a decentralized, distributed database used to maintain a continuously growing list of records, called blocks. Each block contains a timestamp and a link to a previous block. Blockchain serves as an open distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way (Bruyn, 2017). Blockchain technology uses bitcoin; bitcoin is the first official cryptocurrency in the form of electronic cash. Bitcoin and its underlying Blockchain technology were first conceptualized by Nakamoto (2008) but implemented in 2009, as a core peer-to-peer version of an electronic cash system. These cash systems allow online payments to send directly from one party to another party without the central trusted authorities like bank systems or payment services (Nakamoto, 2008). Blockchain consists of a peer-to-peer network. It consists of a network of nodes that maintain a decentralized shared database of records. Records on the other hand, transfer the transactions of bitcoin

DOI: 10.4018/978-1-5225-9687-5.ch010

cryptocurrency between participating parties. Each party in the transaction has a public and private key pair of public key infrastructure (PKI). Transaction parties sign the transactions using their private key, verified by other parties using a public key. The transactions are broadcast to all the other nodes in the network (Shen & Pena-Mora, 2018). This permits bitcoin to be used like other assets in exchange for goods and services. Additionally, it is easily portable, divisible and irreversible. Bitcoin uses blockchain technology to maintain its public ledger of every single transaction ever made with Bitcoin.

In the understanding of blockchain technology, four kinds of keywords are essential. The four keywords are open, distributed or decentralized ledger, efficient, verifiable and permanent. The first keyword is open; whatever information you are putting inside the blockchain should be accessible to all; everyone will be able to observe and validate that information. The second keyword is a distributed ledger, where a copy of that public ledger to every individual party who is there in the platform as well as their communicating with each other is kept, so that the platform can be either distributed or decentralized based on a given application. The third keyword is efficiently. It is important to ensure the efficiency of the information and efficiency of the protocol. Furthermore, the protocol needs to be fast and scalable. The fourth keyword is verifiable. It is a crucial keyword that permits all on the network to check the validity of information. The final keyword is permanent, which indicates that all information registered in the blockchain remains persistent. It is sometimes referred to as tamper proof (Iansiti & Lakhani, 2017). Tamper proof signifies that once the information is registered into the blockchain, the information will not be able to be modified nor updated in future time. The blockchain technique thus ensures that all bitcoin transactions are recorded, organized and stored in cryptographically secured blocks, chained in a verifiable and persistent manner.

In the course of blockchain implementation, three basic capabilities are supported in the bitcoin network techniques; They are; a) hash chained storage where two fundamental building blocks can be used for hash chained storage capabilities, namely, hash pointer and merkle trees, b) digital signature: by using cryptographic algorithm, establishes the validity of data items, and c) commitment consensus: this technique secures the expansion of the global ledger and precludes malicious attacks (Zhang, Xue & Liu, 2019).

Blockchain can be classified into three categories: Public blockchain, Consortium blockchain, and Private blockchain.

1. A public blockchain enables anyone to read, send or receive transactions and allows any participant to join the consensus procedure of making the decision on which blocks contain correct transactions and get added to the blockchain.
2. A Consortium blockchain can read any participant in the network but write permissions only to a pre-selected set of participants in the network who control the consensus process, and the third blockchain type is,
3. In a private blockchain, write permissions are restricted strictly to a single participant, read permissions are open to the public or constrained to a subset of participants in the network, where only chosen players have the rights to join the network which then creates a closed loop environment (Zhang et al, 2019). Bitcoin is a public Blockchain, because it was designed completely open, decentralized, and permissionless, that means anyone can participate without establishing an identity and no central authority (Bojana, Elena & Anastas, 2017).