Blockchain Technology and Its Applications

7

Ting Wang
Indiana University South Bend, USA

Liguo Yu
Indiana University South Bend, USA

Yingmei Li
Harbin Normal University, China

INTRODUCTION

The most volatile currency on financial market in the past several years is bitcoin for sure (Grinberg, 2012). A unique property of bitcoin is that it has no backup from central banks of any country. In addition, bitcoin is a decentralized currency system, where the transactions and the creation of new coins are done automatically following computer algorithms (Nakamoto, 2008). Nobody is sure about the future of bitcoin, because this really depends on government regulations, customer preference, technology evolutions, and alternative financial solutions. However, one of the key technologies under bitcoin currency–blockchain, will definitely be utilized in many fields because of its revolutionary data design, data recording, transaction execution, and transaction validation.

This paper describes the fundamentals of blockchain technology, including its data structure and transaction rules. In addition, this paper describes representative blockchain development platforms, the current and potential applications of blockchain and its broader impact on business and industry. The objective of this paper is to help readers understand one of the disruptive technologies that are transforming the business practice and reshaping the IT industry's landscape.

BACKGROUND

In January 2009, the first bitcoin transaction was successfully completed. In 2010, the first commercial bitcoin transaction was recorded (Morse, 2017). These events marked the beginning of a revolutionary electronic currency. In less than ten years, bitcoin has become the most influential cryptocurrency on the planet. Currently, there are over 200 thousand bitcoin transactions per day. Although this number is much smaller than the number of traditional financial transactions (such as credit card transactions) per day, it is drawing more and more attentions. In addition, other cryptocurrencies were created in the past years following the success of bitcoin.

The major impact of bitcoin might not be limited to financial industries. What is more revolutionary is the fundamental technology used to implement bitcoin–blockchain (Hayen, 2016). Businesses, governments, and institutions have realized the importance and potential applications of blockchain. Intense research and developments are being carried out in various fields. However, as with any other

DOI: 10.4018/978-1-7998-3473-1.ch085

emerging technology, while blockchain has certain strengths and can bring certain benefits, it also has weakness and can bring certain risks. Therefore, it is worth of studying this technology in detail before adopting it in business and applications.

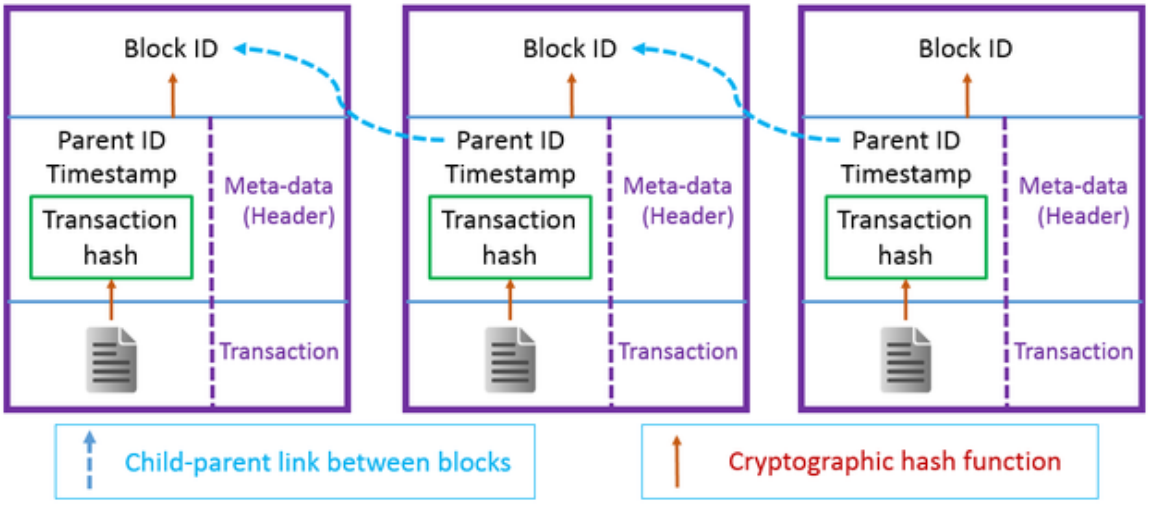
TECHNOLOGY DESCRIPTION

Data Structure

Blockchain is a back-linked list structure that consists of individual blocks. Like any list structure, Blockchain has a head-block and an end-block. If the blockchian size is 1, the head-block is just the end-block. Also like other list structures, the new block is added to the end of the chain and becomes the new end-block. The back-linked list means that newly-added block is pointed (linked) to the old end-block. In this paper, we call the relationship between the newly-added block and the block it points to a child®parent relationship. Clearly, every block except the head-block has a parent.

The data fields of each block basically include three parts: a block ID, transaction data, and meta-data (Eyal et al., 2016). The meta-data field is also called the header of the block. It includes timestamp the block is created, its parent block ID, and other data items. The main purpose of having a parent block ID in meta-data is not just to provide a physical link between the child and the parent. The physical link can be implemented in many different ways, such as pointers. Instead, having a parent block ID provides a mechanism to demonstrate or validate the legitimacy of a block. Using an analogy in biology, this is like to say that someone carries its own DNA together with its parent's DNA so that it can claim (prove) to be the biological child of its parent. Figure 1 shows a general block chain structure.

Figure 1. A general blockchain data structure.



In blockchain, the close relation between a child-block and its parent-block is achieved using the cryptographic hash function. Like a regular hash function, a cryptographic hash function can map arbitrary size data to a fixed value as shown in Figure 2. In addition, a cryptographic hash function has