Chapter 84
The Blockchain Technology:
Applications and Threats

Ahmed Ben Ayed
University of the Cumberlands, USA

Mohamed Amine Belhajji
University of Quebec at Rimouski, Canada

ABSTRACT

This article describes how Blockchain is a technology that has a great potential to change the way business is done in the future, exactly like the internet did in the early nineties. Blockchain offers new opportunities to develop new types of digital services to overcome business problems, and improve business practices by making transaction information a public resource. While research on the topic is still emerging, it has mostly focused on crypto-currencies instead of taking advantage of this novel concept to create new advanced services. This article discusses blockchain and the technology behind it, some of its possible applications, as well as threats targeting the new poorly understood technology.

INTRODUCTION

A Blockchain is essentially a dispersed data source of records, or public ledger, of all transactions or digital occasions that have actually been executed and also shared amongst participating parties. Each transaction in the public ledger is verified by the consensus of the majority of participants in the system. Once admitted, details can never, ever be removed. The Blockchain includes a particular and verifiable record of every single transaction ever made. Bitcoin, a decentralized peer-to-peer digital money platform, is one of the most popular examples that utilize the Blockchain innovation. The Bitcoin itself is very debatable; however, the underlying Blockchain innovation has worked perfectly to make it trustworthy and implemented in a vast array of applications in both the financial and non-financial worlds. The major hypothesis is that the Blockchain develops a system of distributed agreements in the virtual world. This allows participating entities to know for sure that an electronic event happened by creating an irrefutable record in a public ledger. It opens up the door for creating democratic open and scalable electronic

DOI: 10.4018/978-1-5225-9866-4.ch084

economies instead of centralized ones. There are tremendous chances in this disruptive technology, and the changes it is bringing to how business is being done have only just started.

SRUCTURE OF THE BLOCKCHAIN

The Blockchain is an arranged back-linked list of blocks that contain transactions.

The Blockchain can be stored as a flat file, or in a regular database. Blocks are linked back, where each block refers to the previous block in the chain. The Blockchain is often visualized as a vertical pile of transactions, and the first block ever created serves as the foundation of the stack (Figure 1).

Blockchain is the main technology behind the Bitcoin, which is considered the first decentralized crypto-electronic money. In Bitcoin, the transaction starts when the future owner of the Bitcoin sends out to the original own era request to receive money. If approved, the Bitcoin gets moved using a digital hash signature. Every coin is related to an address, and every transaction in the Blockchain is basically a trade in Bitcoin from one address to another. In Blockchain, the information utilized in transactions are saved in an unalterable public spreadsheet that is protected by users in a peer-to-peer network which acts as verification for the credibility of the transactions (Dorri et al., 2016). Blockchain technology allows "trustless" transactions without the need for entities to verify or check the amount exchanged by using a computer network. Simply speaking, Blockchain enables peers to perform transactions between one another without the need for a central bank or any other financial institution (Kiviat, 2015). A Blockchain transaction occurs between two parties and it begins when one of the involved parties sends a message to the network concerning the conditions governing the transaction. After that, the other party broadcasts their approval of the conditions to the network, which by default causes the network participants to authenticate and confirm the transaction (Kiviat, 2015). When the transaction becomes verified and validated, the public Blockchain record, as well as all users in the network, will be collectively updated with the status of the recently added blocks to the network. This decentralized system, along with the cryptography used, guarantees that no confirmed transaction can be altered or deleted, and helps in establishing trust between parties by using a decentralized public journal and cryptographic formulas that can ensure accepted purchases will not be changed after confirmation. Every block throughout the Blockchain is generally defined with a hash, created using the SHA256 cryptographic hash algorithm. Every block contains a reference to the previously created block, referred to as the 'parent'. Every block contains the hash information from the parent within its own header. This series of hashes makes it easy to connect each block to its parent, which helps create a chain that goes back to the first-ever created block, referred to as the 'genesis block'. Although a block has only one parent, it may momentarily obtain several children. Every child relates back to the exact same block as its parent, and has the exact same previous block hash. Several children blocks occur during a Blockchain "fork", which is a provisional circumstance that happens whenever various blocks are created at virtually the exact same time by different miners. Ultimately, just one child block will become part of the Blockchain, and the "fork" is fixed. Despite the fact that a block may have more than one child, each block can have only one parent due to the one single previous block hash located in every block header (see Figure 2).

A block is a container that aggregates different information that helps in identifying a transaction in the chain. The block header is 80 bytes, whereas the typical transaction is about 250 bytes. Every transaction is composed of the sender, the receiver, and any additional information about the transac-