Chapter 4
Evolution of Blockchain Technology:
Principles, Research Trends and Challenges, Applications, and Future Directions

Oluwaleke Umar Yusuf
The American University in Cairo, Egypt

Maki K. Habib
The American University in Cairo, Egypt

ABSTRACT

This chapter presents a detailed introduction to the decentralized data processing and storage paradigm called blockchain technology, delving into its fundamental concepts, foundational principles, and advantages. A literature review is conducted, detailing existing research areas, and enabling technologies driving further research and development into the technology. The two-way fusion of machine learning – another data-driven technology – is considered, wherein one technology addresses limitations and drawbacks within the other. The existing applications of blockchain technology within various domains are discussed, along with some identified research challenges and future trends. A case study is also provided to demonstrate the integration of blockchain technology into the internet of vehicles domain.

INTRODUCTION

The contemporary data processing and storage paradigm hinges upon centralized authorities for access, resolution, trust, and integrity. Blockchain Technology – also known as Decentralized Ledger Technology – aims to address the single-point-of-failure vulnerabilities introduced by such centralized authorities. A blockchain is a continuously growing data structure consisting of an immutable chain of blocks distributed among multiple authenticated nodes. Furthermore, no authoritative entity is required to validate

DOI: 10.4018/978-1-6684-7684-0.ch004

and ensure data authenticity, integrity, and security. Any form of digital (or digitalized) information can be stored on a blockchain to support various applications in different domains. Such digital information includes financial transactions, legal documentation, patient health records, supply chain, and logistical data, amongst others (Baiod et al., 2021; Casino et al., 2019; Hassan et al., 2020).

The origins of blockchain technology date back to 1991 when a paper (Haber & Stornetta, 1991) first appeared proposing the concept of attaching a time-stamp to a digital document. Building upon that paper and other related research work, a white paper (Nakamoto, 2009) was proposed in 2008, which established the utility of blockchain as a technology, popularizing the concept of secured peer-to-peer (P2P) transactions in the form of Bitcoin. Since then, blockchain technology has been implemented in capital markets, the Internet of Things, and supply chain management (Baiod et al., 2021; Casino et al., 2019; Zheng et al., 2019). In addition, blockchain technology has been proposed as a core component of smart cities (Salha et al., 2019), autonomous freight (Narbayeva et al., 2020), and the Internet of Vehicles (Mollah et al., 2021) in the near future.

Due to the relative immaturity and fast-paced innovation of blockchain technology, there is a lack of concise, up-to-date literature that provides an interested layperson with a detailed introduction to the technology and its potential to revolutionize diverse domains simultaneously. To this end, this chapter intends to provide a comprehensive overview of the evolution of blockchain technology underlying – from its fundamental concepts and foundational principles to its advantages for various applications. This is followed by a review of research areas and enabling technologies driving the continued development of blockchain technology. Next, we discuss some research challenges and detail the application of blockchain technology in various domains. We also examine a case study demonstrating the integration of blockchain technology into the Internet of Vehicles domain. Finally, we outline some future trends with blockchain technology.

FUNDAMENTAL CONCEPTS OF BLOCKCHAIN TECHNOLOGY

Blockchain Technology is built upon three fundamental concepts – blocks, nodes, and consensus protocols. The blockchain consists of *blocks* distributed across connected *nodes* governed by *consensus protocols* (Chandrayan, 2020; Malcom, 2021).

Blocks

The blockchain is a literal chain of blocks, each containing a block header and (transaction) data. The block header consists of metadata for identifying blocks in the chain and verifying the integrity of the blockchain using the hashes contained in each block. Depending on the application, the block data contains the actual system and user data. A block consists of three core elements, as demonstrated in Figure 1, as follows:

- **Data:** the data (or metadata) stored on the blockchain for a specific application.
- **Nonce:** a unique, randomly generated 32-bit number that contributes to the *hash* generation.
- **Hash:** a 256-bit number generated from the *nonce*, *data,* and the previous block's *hash* (denoted as *prev*). The blockchain is created and made immutable by including the *prev* value in the current hash.