Chapter 3
Blockchain Basics: A Deep Dive Into the Blocks, Chains, and Consensus

Muhammad Ahmed
Superior University, Lahore, Pakistan

Adnan Ahmad
COMSATS University Islamabad, Lahore, Pakistan

Furkh Zeshan
https://orcid.org/0000-0002-2960-9632
COMSATS University Islamabad, Lahore, Pakistan

Hamid Turab
https://orcid.org/0000-0002-2280-2704
COMSATS University Islamabad, Lahore, Pakistan

ABSTRACT

A blockchain functions as a decentralized network, serving both as a digital ledger and a mechanism for securely transferring assets without the need for a central authority. Much like the internet facilitates the digital flow of information, blockchain empowers the digital exchange of various value units. The tokenization of various assets, including currencies and real-world applications, is a feasible endeavor within the realm of blockchain networks. This technology not only facilitates secure value transfers but also maintains a persistent record of transactions, establishing a singular version of truth referred to as the network state. This chapter provides a succinct overview of blockchain, highlighting its defining characteristics that position it as a prominent and transformative technology.

DOI: 10.4018/979-8-3693-1532-3.ch003

INTRODUCTION

In recent years, there has been a significant surge in the application of Information and Communication Technologies (ICT) for swift, efficient, and secure data transfer among diverse devices globally. The rise of the internet has enabled a digital exchange of information between various parties, primarily conducted through online financial transactions where users send and receive payments. Traditionally, this system of communication and transaction relies on a centralized third-party verification entity, as depicted in Figure 1. Such an entity is responsible for ensuring the secure transfer and accurate recording of data across multiple accounts. Nonetheless, this method poses several challenges when dealing with the transmission of information through an open network (Sunyaev & Sunyaev, 2020). Therefore, the issues such as potential fraud by the trusted third party, vulnerability to cyber-attacks, which could lead to a single point of failure, delays introduced by third-party involvement, and the need for assured transaction validation arise. The exclusive reliance on a solitary third-party controller raises significant concerns regarding both trust and operational efficiency. Traditional methodologies are heavily contingent upon this third-party framework, introducing substantial apprehensions related to the potential compromise of privacy and anonymity. Consequently, there exists an urgent requirement for the establishment of a decentralized system capable of ensuring robust security for transaction management and contract execution, particularly within the realm of device communication. The implementation of a communication protocol that guarantees data protection, integrity, authenticity, irrefutability, and confidentiality becomes imperative, especially when dealing with the diverse range of data generated by smart devices (Ahmadi et al., 2014; Li et al., 2019). Hence, Distributed Ledger Technology (DLT), commonly recognized as blockchain, emerges as a plausible solution to address these challenges, as depicted in Figure 2. The genesis of this concept can be attributed to an individual or group operating under the pseudonym Satoshi Nakamoto, who introduced the groundbreaking Bitcoin, which is the pioneer in decentralized digital currency (Cosares et al., 2021; Gandal et al., 2021; Nakamoto, 2008). The widespread adoption of Bitcoin is reflected in its transaction volumes. This technology offers a decentralized network that is capable of generating and managing smart contracts within IoT-enabled smart applications, enhancing security and eliminating central points of vulnerability.