Chapter 11
Revolutionizing Industry and Business Processes With Smart Contracts in Blockchain

L. Mary Shamala
Vellore Institute of Technology, Chennai, India

V. R. Balasaraswathi
Vellore Institute of Technology, Chennai, India

R. Gayathri
Vellore Institute of Technology, Chennai, India

ABSTRACT

The evolution of blockchain technology, notably exemplified by Bitcoin, heralded a new era where smart contracts have taken center stage. Smart contracts are ingenious self-executing contracts that empower automatic enforcement of contractual terms, eliminating the need for intermediaries or trusted third parties. Consequently, smart contracts offer multifaceted benefits, including streamlined administrative procedures, cost savings, enhanced operational efficiency, and risk reduction. This chapter aims to provide the pivotal technical aspects of smart contracts and their significance within the blockchain technology landscape. The authors begin by elucidating fundamental concepts, structural intricacies, and the working principles of smart contracts. Subsequently, they delve into the technological platforms that support smart contracts. They then provide an overview of the application landscape, with a focus on Ethereum and hyperledger fabric platforms. Finally, they address the challenges associated with smart contract technology and offer insights into potential opportunities.

DOI: 10.4018/979-8-3693-1532-3.ch011

The worldwide web is continually evolving and is now on the third wave of web services called Web 3.0. Web 3.0 is an open-source internet where consumers control information while enjoying direct access to apps, eliminating the need for intermediaries. Web 3.0 focuses on decentralization, thus Blockchain has a crucial role in its evolution. Blockchain technology has recently sparked widespread attention in research and business. As the name suggests, Blockchain is a shared software platform that enables the execution of operations without an intermediary (Khan et al, 2021). Consequently, it is possible to accomplish commercial activities cheaply and quickly. Furthermore, blockchain ensures widespread confidence because it is tough to alter any activities contained in blockchains, and all past actions are transparent and provable. Smart contract technology, deeply integrated into blockchain ecosystems, is heralding a paradigm shift in traditional industries and business operations.

Nick Szabo, a cryptographer, and Computer Engineer first put forward the concept of smart contracts in the 1990s (Szabo, 1997). Smart contracts are codes that are independently grounded on blockchains or comparable networks and enable secure and transparent execution of predetermined procedures. Smart contracts currently manage billions of dollars in worth. These self-executing contracts have revolutionized the way agreements are made and enforced, eliminating the need for intermediaries and enhancing operational efficiency across various sectors. The primary distinction between smart contracts and ordinary contracts is that smart contracts record provisions in a programming language rather than a legal language (Khan et al, 2021). In decentralized blockchains, transaction-based smart contracts are fundamentally duplicated and maintained. On the other hand, traditional contracts would delivered in a centralized fashion by an established third party leading to lengthy processing periods and higher expenses.

Smart contracts, being autonomous and state-based, have transcended the realm of programmable currency and entered a domain characterized by decentralized, autonomous, observable, verifiable, and information-sharing capabilities. They facilitate the creation of customized programming logic across the blockchain, enabling the development of programmable finance and a programmable society. Smart contracts find extensive applications including electronic payments, controlling assets, multi-signature deals, the Internet of Things, cloud computing, and the economy of collaboration (Tern, 2021). Smart contracts thus represent an essential part of Web3 Technologies, allowing for a new paradigm of automated, trustless, decentralized, and ubiquitous services and applications.

BASIC CONCEPTS OF SMART CONTRACTS

A blockchain is a distributed information storage system that archives every activity in the blockchain network. The information within it is copied and distributed across members of the network. The key characteristic of this technology is the fact it enables unverified users to securely interact and transfer transactions to one another in the absence of an intermediator. The blockchain consists of a chronological collection of blocks. A cryptographic hash identifies each of these blocks. Every single block is linked to the previous forming a block chain. A block consists of a set of operations. After a block is generated and published to an existing blockchain, its actions are irreversible or incapable of being modified (Badri et al, 2022). This serves as the basis for avoiding the risk of double spending and preserving the integrity of information (Alharby et al, 2018). Blockchains are distributed, and extremely secure thanks to cryptographic functions and enforceable consensus procedures for fresh transactions, thereby eliminating the "middleman" to generate confidence. As a result, transaction fees are much lower (both in terms of money and time) than in the standard trade system.