Chapter 7
Design of Hash Algorithm for Blockchain Security

Yatri Davda
Marwadi University, India

ABSTRACT

Blockchain is the invention that permits digitally generated information to be allocated without being copied. Blockchain technology is the heart of the new internet (i.e., virtual currency). Emerging clever settlement structures over decentralized cryptocurrencies permit jointly suspicious events to transact competently without relying on third parties (i.e., the reason to provide wide security to blockchain technology). Cryptography has so many algorithms to provide security such as MD5, AES, RSA, SHA family, etc. Hash functions are extremely useful and appear in almost all information security applications, so hashing techniques are more secure among them. The authors are designing a new approach (i.e., SHA-512) in a local blockchain application. SHA-512 is a very secure algorithm that uses 64-bit words and operates on 1024-bit blocks. They are proving that SHA-512 is more collision-resistant than its predecessor with a few mathematical models.

INTRODUCTION

Today, some technologies are playing key role in the transformation of organizations like blockchain, IoT, AI and automation, to a cognitive enterprise. Interaction with its client's ecosystem which is used to find any enterprise as well as blockchain solutions to make these interactions efficient (Dhumwad et al., 2017; Nehe et al., 2019). Blockchains are additionally reliant on hashing. Hashing is a cryptographic strategy which is used to convert the data into a string of characters. Just as giving

DOI: 10.4018/978-1-6684-6247-8.ch007

security through encryption, hashing makes a more proficient stockpiling of information, as the hash is of a fixed size (Bauer er al., 2009). In view of providing better security, we are proposing a new idea based on the concept of Hashing in cryptography which aims at offering ownership protection in blockchain (Bhulania and Raj, 2018; Singh and Singh, 2016).

Blockchain refers to a technology that brings in the solution to the age-old human trust problem (Aswini and Kiruba, 2019). It emerged in the market with the renowned cryptocurrency Bitcoin. It provides an architecture that allows us to trust on a decentralized system (Internet or Web) rather than trusting any actor within it. It runs on top of a peer to peer network and holds the identical copies of the ledger of transactions. This helps to avoid any middleman and the entire process of transaction takes place through machine consensus (Alkandari etal., 2013; Lee et al., 2019).

It is a ledger that is shared between multiple entities that everyone can inspect but not any single user can control it. It is a distributed cryptographically secured database that keeps the record of every transaction from the very initial one (K.N. and Bhakthavatchalu, 2019; Taghipour and Frayret, 2010).

Blockchain mainly contains hash, hash of previous block and data, data can store an amount of money, a share in a company (Ferreira et al., 2019), a digital certificate of ownership, a vote during an election, or any other value (Figure 1).

Figure 1. Basic of blockchain