Chapter 12
Data Confidentiality, Integrity, and Authentication

Dhanalakshmi Senthilkumar
https://orcid.org/0000-0003-0363-5370
Malla Reddy Engineering College (Autonomous), India

ABSTRACT
Blockchain has been created in the process of development in bitcoin. It’s a singly linked list of block, with each block containing a number of transactions and each list in the blocks using with cryptographic functions. The cryptographic hash function contains the hash of the previous block, timestamp, and transaction ID. Blockchain services include the authentication, confidentiality, integrity, data and resource provenance, and privacy and access control lists technologies. The authentication provider authenticates decentralized database with transactions in private-public key pair. This key-pair is used in the transport layer security with the entire network. The network legitimizes the transaction after that and adds the transaction to the blockchain. A sequence of blocks in blockchain holds the complete record of transactions like a public ledger. The integrity data written in the blockchain cannot be altered subsequently. By limiting access to the information in confidentiality, only authorized users can access the information, so that information is also protected.

INTRODUCTION

Bitcoin and its underlying Blockchain technology were first conceptualized by Satoshi Nakamoto in 2008 but implemented in 2009, as a core of peer-to-peer version of electronic cash systems, these cash systems allows online payments to send directly from one party to another party without central trusted authorities like bank systems or payment services (Nakamoto, 2008). The digital currency i.e., Bitcoin components support for these transactions. Blockchain could be regarded as a public ledger for all committed transactions stored in list of blocks, are new blocks are appended to it continuously, and it resolved by double spend problem together with peer-to-peer technology with cryptographic tools. So that linking every transaction to the transaction preceding it in a tamper proof resistant manner. Blockchain is an open distributed ledger technology that can record the transactions between two par-
Data Confidentiality, Integrity, and Authentication

The evolution of Blockchain technology namely; Blockchain 1.0 – it’s the decentralization of money and payments, basically used for cryptocurrencies, Blockchain 2.0 used for digital finance and industries (In Blockchain 2.0 smart contract was first introduced the way to verify assets, properties, products and services), and Blockchain 3.0 is the decentralization of digital society and its used for applications of IoT, health and government, it offers more security as compared to Blockchain 1.0 and 2.0, and it’s used for various industries, arts health, media and many government institutions (Supriya and Kulkarani, 2017).

Blockchain technology is the sharing and storing of information in a single block, each block has many transactions, storing of information is permanent in the block; blocks are connected with each other. block chain has been created in the process of development is bit coin, is growing list of records with linked list manners, each list in the blocks using with cryptographic functions. Both users sharing the documents and also simultaneously edit the documents. One problem to be raised in centralized systems for single point of failure; to load the data in Google doc do not have enough bandwidth, not able to edit the documents. In centralized systems single point is not safe vs. decentralized systems can have multiple points of coordination’s vs. distributed systems can have each one executes the job. Blockchain is a type of database that is duplicated on many systems or nodes. Every node, the node maintains local copy of global data sheet. All the nodes have the same information’s for to access the transactions, the information is stored on blocks, but cannot change or delete a transaction from the Blockchain.

Each block has multiple transactions, with each transaction having a unique reference number, time stamp and points to previous transactions. Each node to access to all previous blocks. The last block in the Blockchain contains the latest executed transactions, so that the Blockchain is continuously growing. A decentralized database system ensures that strong consistency support with local copy of data; every node is identical based on the global information local copies of data always updated. The cryptographic
Related Content

Attacks on Implementation of Cryptographic Algorithms
www.igi-global.com/chapter/attacks-on-implementation-of-cryptographic-algorithms/188515?camid=4v1a

Addressing Security Issues of the Internet of Things Using Physically Unclonable Functions
www.igi-global.com/chapter/addressing-security-issues-of-the-internet-of-things-using-physically-unclonable-functions/222273?camid=4v1a

Secure Bootstrapping Using the Trusted Platform Module
www.igi-global.com/chapter/secure-bootstrapping-using-the-trusted-platform-module/188522?camid=4v1a

Secure Two Party Computation
www.igi-global.com/chapter/secure-two-party-computation/188520?camid=4v1a