Chapter 3
Introduction of Blockchain and Usage of Blockchain in Internet of Things

Chandrasekar Ravi
National Institute of Technology Puducherry, India

Praveensankar Manimaran
https://orcid.org/0000-0003-3614-5722
National Institute of Technology Puducherry, India

ABSTRACT

Since the advent of the web, the number of users who started using the internet for everyday purpose has increased tremendously. Most of the common purposes are to access their data whenever they want and wherever they want. So many companies have started providing these services to normal users. These companies store huge volume of data in the data centers. So protecting the integrity of the data is the main responsibility of these companies. Blockchain is one of the trending solutions that gives storage immutability to the users. This chapter starts with the working of blockchain and smart contracts and advantages and disadvantages of blockchain and smart contracts and then goes on to explain how blockchain can be integrated into the internet of things (IOT). This chapter ends with an architecture based on the proof-of-concept for access management, which is blockchain-based fully distributed architecture.

INTRODUCTION

Blockchain is a peer to peer network which is distributed among the untrustworthy peers and the untrustworthy peers can interact with each other. The interactions will be verified using some form of cryptographic mechanisms. Blockchain enables applications to run in a decentralized manner without any need for centralized authority. Blockchain makes it possible to do transactions between trustless parties without the need for centralized authorities (Christidis & Devetsikiotis, 2016). Blockchain uses cryptographic techniques to provide authentication functionality to peers. Smart contracts have been

DOI: 10.4018/978-1-6684-7132-6.ch003

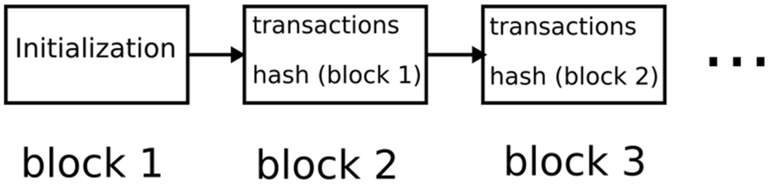
defined as "self-executing scripts" and usually smart contracts will be stored on the blockchain which can provide automated workflows in the network.

BLOCKCHAIN

Blockchain is similar to the database which is distributed among the peers participating in the network and the network structure it forms is peer to peer network so there is no need of centralized entity. Blockchain is a digital decentralized ledger (Novo, 2018). Blockchains are important because they provide a safe and secure way for people to make any type of transaction without having to trust anyone. Blocks in a blockchain can be thought of as a sheet of paper. Blocks, just like paper, can hold any type of data on them. The first block in the blockchain is called genesis block. The genesis block will be initialized when the blockchain network starts for the first time. The second block will have the transactions and the cryptographic hash value of the first block. Next blocks will follow the same.

Each block(other than genesis block) will include the hash value of the preceding blocks. This will form a linked list in which the node is a block. It is shown in Figure 1. Each block will have id associated with it. Each node will hold a copy of the blockchain. Each node can be used by a single user or more than one user. Bitcoin introduced blockchain architecture to solve the double-spending problem (Nakamoto, 2008).

Figure 1. Blockchain structure



Since different peers will have the same copy of the blockchain, each peer will try to create the next block for the blockchain. Once the peers created a new block, the new block will be broadcasted to all other peers in the network. If two peers have created two different blocks then the latest and the longest block will be chosen as the next block. This process is called forks. The discarded block is called orphan blocks. Based on the total difficulty of blockchain, the longest block is chosen.

Each user will have a pair of a private key and public key (Hellman, 2002). Using those keys the user can access the blockchain. Transactions will be signed by the peers using the peer's private key. Once the transaction is signed and verified it will be included in the block. Once a transaction is added to the block it will be broadcasted to the other peers or users in the blockchain. Peers can validate the transactions by using the creators public key. After the validation and verification of transactions, the transaction will be ordered based on consensus mechanism and the transactions will be packed into a block and it will be broadcasted to the other peers in the network.

Blocks contain a set of transactions. Each transaction transfers the values from one entity to another entity. Pool miners are solo miners who mine the blocks. Mining operation bundles the set of transactions