Chapter 51
Optimization of Consensus Mechanism for IoT Blockchain: A Survey

Shailesh Pancham Khapre
Amity University, Noida, India

Shraddha P. Satpathy
Amity University, Noida, India

Chandramohan D.
Madanapalle Institute of Technology and Science, India

ABSTRACT

The essence of blockchain is a decentralized distributed ledger system; the IoT is formed by accessing and interconnecting a large number of heterogeneous terminals and has a natural distributed feature. Therefore, the combination of the two IoT blockchains is widely optimistic. At the same time, due to the heterogeneity of IoT sensing terminals, limited computing storage, and data transmission capabilities, the IoT blockchain is facing greater challenges, among which cryptographic consensus technology has become a key issue. In this chapter, based on the summary of the current blockchain consensus algorithm, applicability to the IoT-blockchain has been analyzed, the application status of several major IoT-blockchain platforms and consensus mechanisms have been introduced, and also the IoT-blockchain research progress on optimization of consensus mechanism has been expounded. Looking forward to the optimization techniques of the IoT blockchain, potential research directions have been summarized.

DOI: 10.4018/978-1-6684-7132-6.ch051

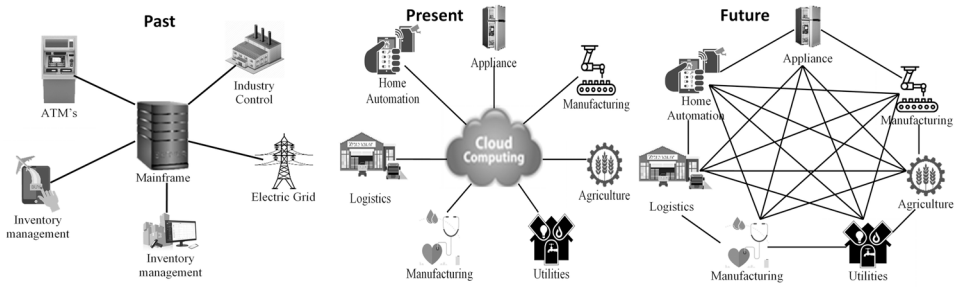
INTRODUCTION

With the advent of IoT (Khodadadi *et.al*, 2017), information sensing equipment is widely used in smart communities, smart agriculture, smart transportation, shared economy, and other fields to promote comprehensive interconnection and integration of man-machine-things. IoT research institutions predict that by the end of 2020 (Ashton, 2009), the number of IoT terminal devices will increase to 26 billion.

The main access control methods in the Internet of Things environment are: role-based access control RBAC, attribute-based access control ABAC, access control based on usage control model UCON, and capability-based access control CapABC. The aforementioned RBAC, ABAC and UCON IoT solutions rely on a centralized server-client architecture to connect to cloud servers via the Internet. In order to meet the growth, the decentralized architecture CapABC was proposed to create a large-scale P2P wireless sensor network. CapABC achieves lightweight distributed control, dynamics, and scalability, but CapABC cannot guarantee security or user privacy. Compared with the traditional Internet, IoT architecture expands network connections to a richer physical space. In view of its massive heterogeneous and resource-constrained IoT terminal, data sharing, privacy protection, intrusion detection, access control, and cross-domain authentication and other problems (Wang *et.al*, 2019, Kouicem *et.al*, 2018), traditional security technologies with large computing requirements and high deployment costs cannot be directly applicable to the IoT platform, we need to find new security solutions.

As shown in Figure 1, from the past closed centralized framework to the open cloud centralized architecture, and the next step is to distribute cloud functions to multiple nodes, blockchain technology can play a big role in the next trend effect.

Figure 1. The IoT architecture of the past, present and future



Blockchain is a decentralized distributed technology, a peer-to-peer distributed ledger based on cryptographic algorithms. The blockchain technology extracted from the underlying architecture of Bitcoin can be applied to the transfer of value between any media that does not require mutual trust, thereby spawning a general blockchain application platform such as Ethereum and hyperledger (Qi-feng *et.al*, 2017). Blockchain has the basic characteristics of decentralization, tamper-proof information, open and transparent data, and three guarantee mechanisms: consensus mechanism, smart contract, and asymmetric encryption. Blockchain technology can solve the following challenges in large-scale IoT systems: Most IOT solutions are still expensive because of the high cost of deploying and maintaining central clouds and servers. When the supplier does not provide the above facilities, these costs are transferred to the