Title: Principles of blockchain based secure and trusted IoT network

---

Keywords: blockchain, IoT, ODIN, PTTP

Abstract: This Recommendation defines principles of blockchain based secure and trusted IoT (BIOT)network architectures (which include BIOT functional architecture, BIOT information architecture and BIOT physical architecture) and their fundamental elements.

This Recommendation also describes the relationships among the three architectures.

1. Background

The networking of the IoT for carrying a single customer or a single service often leads to high cost of construction. Therefore, building a public IoT network to multiple customers and different services is inevitable. In this application scenario, the key problem is how to ensure the security of multisource data, the credibility of data access, and the isolation between different customers and services. Moreover, Snowden incident shows that all IOT participants including government, there may not be credible. To this end, decentralized trusted mechanism must be set up to ensure end-to-end data transmission security and privacy protection. Blockchain can provides decentralized trusted authenticate mechanism to satisfy IoT data security and trusted sharing requirements.

2. Secure and trusted IoT network application scenarios

Secure and trusted IoT network need to meet the requirements of the following application scenarios:

- Service data transferred transparently to the (IoT)network Operators. That is, although the data is transmitted through the network of the IoT operators, the IoT operators are unable to obtain data content (for example, the deep packet inspection(DPI) method).
- Data transfer reliability. Network interruption in part of the IoT link does not affect the sharing of data.
- Sliced Data transfer and shared by different services. Data can be shared across a specified number of services, and then a data sharing plane is formed. Data between different data sharing planes need to be isolated from each other.
- IoT terminals and the related data must be trusted.
- Decentralized trusted authenticate mechanism to IoT terminals and the related data.

3. Functional architecture blockchain based secure and trusted IoT network

Blockchain based secure and trusted IoT(BIoT) network functional architecture is shown in Figure 1.

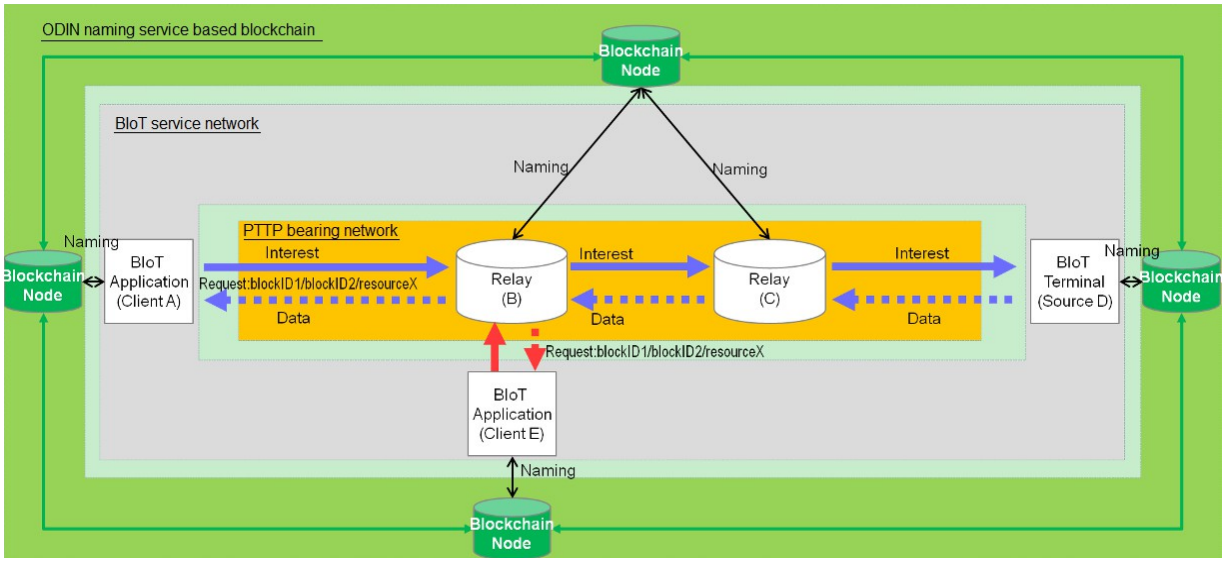

Figure 1 BIoT network functional architecture

BIoT network compose three domains including ODIN(Open Data Index Name) naming service, PTTP(Peer Truested Transfer Protocol) bearing network, and BIoT service network.

- In ODIN service domain, blockchain nodes in blockchain domain provides secure and trusted Naming service to the nodes in BIoT service network and PTTP bearing network domains. The blockchain stores the names of PTTP network nodes and the public key needed for data encryption, and provides naming and public key management services to the PTTP network nodes.
- In PTTP bearing network domain, IoT data is transferred by PTTP protocol. PTTP (related to Content-Centric Networking (CCN), content-based networking, data-oriented networking or information-centric networking) is a Future Internet architecture inspired by years of empirical research into network usage and a growing awareness of unsolved problems in contemporary internet architectures like IP. PTTP comes with potential for a wide range of benefits such as content caching to reduce congestion and improve delivery speed, simpler configuration of network devices, and building security into the network at the data level.
- In BIoT service network domain, **BIoT Applications** and **BIoT Terminal** share IoT data effetely, sliced, reliably and transparently. The **BIoT Terminal** uses its private key to sign the data to ensure the trustworthiness of the data source, and encrypts the data with the public key of the authorized **BIoT Application** party, so as to ensure that only the authorized **BIoT Application** party can get the data content, so as to ensure data safety. If the **BIoT Terminal** data is to be shared by multiple authorized **BIoT Applications,** it can be encrypted by the public keys of the authorized **BIoT Applications** separately, and the encrypted data is released to PTTP bearing network separately, so as to achieve data security sharing among multiple authorized services sharing.

4. Physical architecture for blockchain based secure and trusted IoT network

A typical general BIoT network physical architecture is shown in Figure 2.

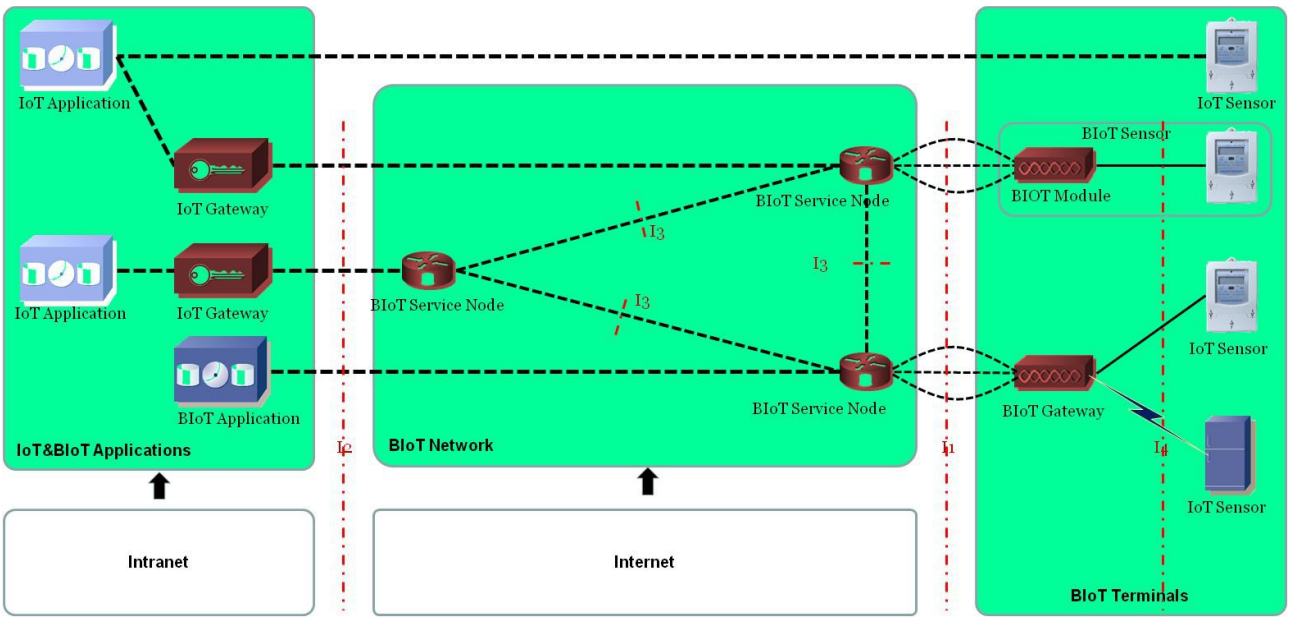

Figure 2 BIoT network physical architecture

BIoT physical architecture composed three domains including IoT&BIoT Applications, BIoT Service Network and BIoT Terminals.

- IoT&BIoT Applications domain: It includes traditional IoT applications and BIoT Applications which can share data released by BIoT Terminals. To traditional IoT applications, it needs a IoT Gateway to convert the BIoT protocol into the protocol accepted by the old applications.
- BIoT service network domain: It includes BIoT service nodes which form a network based on name addressing to provide a reliable and transparent network for the IoT.
- BIoT Terminals domain: There are two types of BIoT Terminals. One as an IoT communication terminal(BIoT Gateway), it supports data access of multiple IoT sensor service terminals, that is, BIOT ends in the IoT communication terminal, rather than the IoT service terminal. The other is an IoT communication module, which is integrated in the IoT sensor, that is, BIOT terminated in the IoT service terminal.
- Load-bearing network domain: It is composed of multiple PTTP service nodes, and uses PTTP network architecture and related protocols to provide data bearing network for IoT.

5. **BIoT service network and equipment interfaces**

Editor's note: Including the 4 types of interfaces(I1, I2, I3 and I4) shown in Figure 2. The interfaces definitions will be given latter.

6. **BIoT data naming service**

Editor's note: general data naming guidelines for PTTP which use blockchain will be given later.

7. **BIoT Data switching and share equipments**

Editor's note: BIoT Data switching and share equipments(which are listed in Figure 2) classification and related general technical requirements will be given later.