DINRG H.Ding
Internet Draft Z.Jiao
Intended status: Informational Chaincomp
Expires: March 13 2019 September 14, 2018

Blockchain-based IoT Infrastructure Functional Requirements
draft-ding-dinrg-biot-00.txt

Status of this Memo

Copyright Notice

Abstract

This document specifies the functional requirements for a Blockchain-based IoT infrastructure, including the IoT device identity management, service demand and supply matching, support of smart contract, etc.

Table of Contents

1. Introduction

With IoT devices proliferating in smart homes, smart cities, smart industries, smart transport, smart health, etc., these devices often lack security consideration due to constrained resources, hence vulnerable to hacking which may cause serious problems in businesses, environment and day-to-day lives. Besides, vendor specific IoT platforms hinder data exchange among devices, create isolated value island and hampers the growth of the ecosystem. The emerging Blockchain technologies, with a decentralized trustless architecture and incentives for sharing, may be able to resolve the trust, security and interoperability challenges for IoT.

IoT devices play an important part in businesses growth via digital transformation, while Blockchain technologies can be adopted to manage the identities of those devices as the very beginning to establish trust. Once registered in the immutable decentralized

ledger, admission control can be implemented, potential threats can be detected and mitigated.

Autonomous coordination among devices via transactions and smart contracts incentivize data and resource exchange across different vendor specific IoT devices, thus enables Device-to-Device economy.

2. Blockchain enabled IoT infrastructure requirements

The Blockchain-based IoT infrastructure should support identity management, service demand and supply matching, smart contract, etc. in a proper way to realize the value of Internet of Things. A possible large-scale Blockchain-based IoT infrastructure can be a hybrid of permission-less chain and permissioned chain, and applications can choose different deployment that suits its business requirements.

2.1. Identity Management

The life span of an IoT device can be several years to decades. The infrastructure should support identity management which is able able to register the device on the immutable ledger and authenticate its identity when necessary during its lifetime.

Once a device is produced, the manufacturer can register an identifiable ID along with its manufacturing information, such as warranty, to a permission-less chain so that it can provide maintenance to customers after products are sold. Besides, the registration on permission-less chain allows public access. If necessary, such identity information can also be used in shipping and inventory management at retailor sites.

After the device is purchased, the user obtains its full ownership including the data it collects and generates. The device should be able to generate a pair of public key and private key. The public key is used to identify a specific device among others, while the private key is used as proof of identity for future validation on real-time messaging and transaction.

The owner can register the device on a permissioned chain in order to perform admission control, so that only authorized devices and personnel can interact with the device and access its data. After the registration is completed, the device is able to submit transactions signed by its private key and the network of peer devices can verify them, so the history of all data/resource exchange will be recorded and kept safe for future reference and audition.

2.2. Service Demand and Supply Matching

To fully activate the capabilities of IoT ecosystem, the devices should have a way to demand and supply services to each other autonomously.

Each device will publish its specific functionalities to the peer-to-peer network, and other devices in the network can subscribe to the peers of interest by reading the published functionalities. As the subscription content grows, the possibility of one device finding a matching demand and supply service pair would be higher.

When a matching pair is found, the two devices will become two parties in a smart contract, trading service with associated fees without the need of a third party. The system can implement a number of service scheduling policies to optimize the matching process.

2.3. Decentralized Service Scheduling

There can be different service scheduling policies in the autonomous coordination among IoT devices, for example, service matching policies, and the consensus protocols.

2.3.1. Service Matching Policies

As introduced in Section 2.2. , peer nodes should coordinate autonomously in service exchange. Some service matching policies may be more suitable than others in different scenarios meaning that a certain policy would make a match sooner or more effective.

For example, a device adopting the latest publish first policy will choose the latest published services on Blockchain because the service will have higher availability given the dynamical change in Device-to-Device networks.

2.3.2. Consensus Protocols

Given the heterogeneous nature of IoT networks, each sub-network may employ different consensus protocols within its Autonomous Domain (AD).

The Blockchain-based IoT infrastructure should support coordination among different consensus protocols so that devices across ADs can exchange data and resources.

2.4. Smart Contract

Smart contract is an agreement between two or more parties that is defined and executed automatically, once certain pre-defined conditions are met. For a Blockchain-based IoT network, smart contract enables more complex device-to-device interaction than transaction.

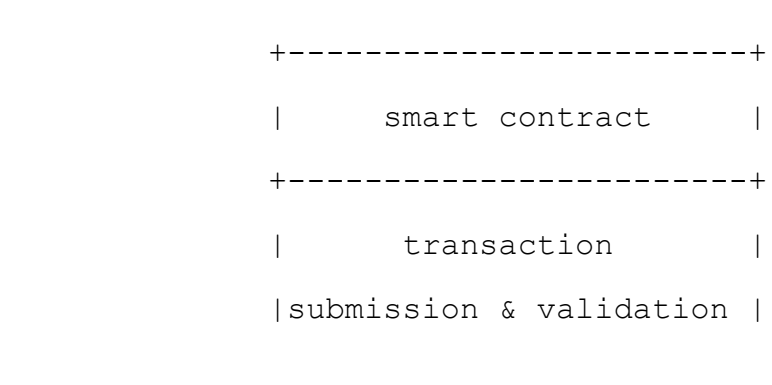
A crucial part in execution of a smart contract is to check and validate whether the pre-defined conditions are met. There can be two sources where such data come from, on-chain and off-chain. On-chain data are stored in the decentralized immutable ledger, which can be traced back to once it is packaged in the block. In some cases, the chain is designed to only carry important information under resource constraints, hence leave some information stored off-chain, which can be useful in the decision making process of smart contract. Special mechanism should be implemented to check and validate the correctness and truthfulness of off-chain data while still keep the decentralized nature of Blockchain system.

Once the condition for transactions are met, associated fees can be transferred from the service demander to the service supplier safely without a trusted third party. A smart contract can call a series of smart contracts, which makes it a powerful tool for automatic value exchange in IoT network.

3. Different Node Types and Functions

IoT devices have various computing power, storage space and networking capability. It is practically impossible to install a full stack of functions on every node.

The devices, given their varied capabilities, can be divided into light node and full node.



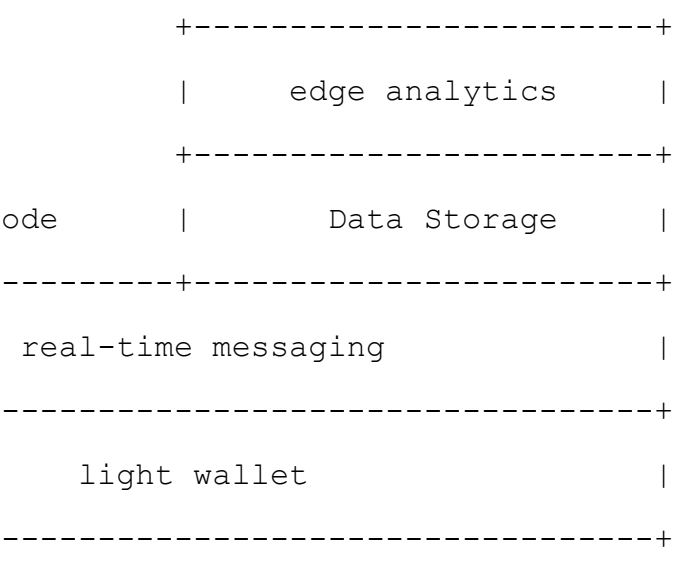


Figure 1 Function Stack of light node and full node

A light node often has low memory space, weak computing power and/or unstable connectivity to the network, such as sensors. This type of node only perform minimal message exchange with peer nodes, keeps a wallet with their address/name and a balance. Any heavier tasks, such as transaction validation will be off-loading to trusted full node. The trusted node can be one from the permissioned chain. A light node is a client of the blockchain, but not a blockchain node.

A full node will support all the functions a light node has with higher performance, including real-time messaging, transaction, block and file storage, local computing, etc. The full node is a complete blockchain node, which can submit and validate transactions, execute smart contract. It also helps trusted light nodes with heavy tasks when needed.

4. Security Considerations

The security of a Blockchain-based system relies on its consensus protocol.

For IoT, the possibility of being hacked poses security challenges to the system.

5. IANA Considerations

TBD

6. Acknowledgments

This document was prepared using 2-Word-v2.0.template.dot.

Authors' Addresses

Hui Ding
Chaincomp Technologies Co., Ltd.
Shixia New Times, Futian District,
Shenzhen, China, 518034

Email: hui.ding@chaincomp.net

Zhenzhen Jiao
Chaincomp Technologies Co., Ltd.
Shixia New Times, Futian District,
Shenzhen, China, 518034

Email: z.jiao@chaincomp.net