Abstract

The purpose of this document is to analyze several important use cases based on blockchain, including: blockchain based PKI for security device connection, blockchain as a service, interworking cross blockchain (exchange data and contracts across different chains). Through case analysis, important scenarios and specific requirements are listed. Related solutions are also provided for easy understanding.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 1, 2019.

Copyright Notice

Copyright (c) 2018 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of
1. Introduction

Blockchain helps to establish cross industry mutual trust and cooperation, and provides the transmission of value and trust on top of current information network (i.e., Internet). The following industries are studying the application of block chains: government, commerce, industry, finance, insurance, medical, education, communication, culture and art etc.

Blockchain can play the following role in a company:

- Promoting internal cooperation and optimizing the existing process, thus improves the production efficiency. Take an Internet service provider for example, the internal blockchain that involves product manager, develop team, QA team and service team, shall be able to trace each service features design, development and market feedback easily, thus accelerate the internal productivity.

- Improving the cooperation of eco-system players, to enlarge the overall benefit. Take Internet service provider for example, by using blockchain, a service provide shall be able to cooperate with other other service providers to expand the overall business based on trust, such as, a social network service provider can coopertate with content (music, video, online game) providers.

- Expanding business to the whole industry, the whole society and the world, to form new business models. For example, the social
network providers shall be able to provide the capability of user authentication to vertical service providers (such as freight, supply chain, finance, rental).

In this document, several important use cases based on blockchain are analyzed, including: blockchain based PKI system, blockchain as a service, interworking cross blockchain (exchange data and contracts across chains). For easy understanding, related solutions are also provided.

2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

3. Terminology and Abbreviations

The terminology and abbreviations used in this document are defined in this section.

- H(e)NB: Home (e)NodeB, An eNodeB is an end device of a Radio Access Network, it performs the same functionality of an eNodeB, but is deployed for indoor premises or public hotspots, using the local Internet connection to access operators’ network.

- MNO: Mobile Network Operator

- SeGW: Security Gateway, an edge device that is deployed on the boundary of an Operator’s network, to connect H(e)NB device remotely.

4. Use case 1: Secure connection management between devices using blockchain based PKI

Digital certificates are widely used to negotiate secure channels between devices and to establish secure connections as defined in RFC 5280 [RFC5280]. According to communication model, there are two typical scenarios: multiple devices are connected to the same centralized node (such as H(e)NBs connected to a MNO’s SeGW), peer to peer connection (such as IoT devices).

4.1. Centralized connected model

Take the H(e)NB scenario for example, H(e)NB is a device that is installed in the office/home where the radio signal is weak or not covered by MNOs, to provide mobile network services (such as voice call, messaging). H(e)NB access MNO’s network via local user’s
Internet access (LAN), thus, security solution is needed to authorize the H(e)NB device and to secure the connection between H(e)NB device and MNO network border (SeGW), as shown in Figure 1.

![Diagram showing secure connection via certificate]

Because SeGWs belongs to different operation domain, it is not possible to have them use certificates issued by the same CA, H(e)NB needs to configure the certificate of the SeGW that it is connected to accordingly. Two important functions is provided by certificate, authentication of H(e)NB devices to make sure that it is not a fake one, and the establishment of secure end to end communication channels between H(e)NB and SeGW under an unsafe Internet network. For this reason, the manufacture can not preinstall any certificate for H(e)NB, the installation of certificate is needed in the deploying stage. The workers manually install the certificate into the H(e)NB. In this way, the following problems occurs: first, the manually installation is low efficiency and error-prone; second, the certificate may be leaked out by the worker. Whats more, reconfiguration are needed each time when the certificate is expired or withdrawn.

The solution is:

- Establish a consortium blockchain, which SHALL be used to verify and store certificates. H(e)NB manufacturers and operator join the chain as nodes, which are responsible for certificate verification and storage.

- A self-signed certificate for each H(e)NB device is generated by the manufacture when it is produced.
o This certificate shall be sent to blockchain nodes to be verified.

o The certificate is verified by the verification node.

o The certificate is recorded into the blockchain if the consensus achieved.

o At the time H(e)NB is installed and powered on, it’s certificate will be used to establish connection to operator’s SeGW.

o The SeGW interacts with the operator’s blockchain node to verify the certification.

o If success, the secured connection between SeGW and H(e)NB shall be established automatically.

o The certificate is also used to identity and antenticate the H(e)NB itself.

Note: Although in this case we uses the operator’s H(e)NB scenario, this solution applies to other similar connection models, such as home gateway.

4.2. Peer-to-peer connection model

Take IoT scenario for example. Currently, IoT devices always talk to each other via the network server (such as IoT application server). For privacy and security consideration, we want IoT devices that produced by different venders to talk with each other directly in security. But we can not assume that all these devices be preinstalled with the certificates issued by the same CA. The regular solution is to introduce a centralized bridge-CA. The question is that, the bridge is lack efficiency and extensibility.

The blockchain provides a better solution:

o Establish a consortium blockchain, which SHALL be used to verify and store certificates. CAs join the chain as nodes, which are responsible for certificate verification and storage.

o When a CA issue certificate for a device, the certificate shall be sent to blockchain nodes to be verified.

o The certificate is verified by the verification node.

o The certificate is recorded into the blockchain if it achieves consensus.
o At the time devices need direct connection, they will lookup their CA’s node for certification verification.

o If success, the secured connection between devices directly and automatically.

4.3. Summary

The advantages of using blockchain based PKI includes:

o High reliability and performance: each node holds a copy of consistent certificate data, supports multiple duplicates and parallel queries, and better data consistency.

o Low cost: automatic operation of block chain system, low maintenance cost; no payment needed for self signed certificate.

5. Use case 2: Blockchain as a Service

The value of blockchain in building a system of trust and collaboration has been proved by the industry, enterprises and industries are applying the blockchain. However, not all enterprises are willing to establish and operate their own blockchain system because of costs. Therefore, providing blockchain-as-a-service solution contributes to the rapid popularization of blockchain.

The main requirements for blockchain-as-a-service may include:

o General proposed data format to support different applications, for storage/verification/resolution.

o Define flexible, extensible interfaces/APIs that is easy for programming.

o Enhanced performance for future proof.

6. Use case 3: Blockchain Interworking

According to the current situation of the vertical development of the blockchain infrastructures and applications, the cross-chain interworking shall be a very important demand in the future. Cross chain interoperability involves not only data, but also smart contracts, security and other aspects.

Two OPTIONAL solutions for blockchain interworking:

o API/Interface invocation based, using interworking gateway.
7. IANA Considerations

This memo includes no request to IANA.

8. Security Considerations

TBA

9. Normative References


Author’s Address

Yang Boyle
China Mobile
China

Email: boyxd@hotmail.com