INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION
STANDARDIZATION SECTOR

STUDY PERIOD 2017-2020

SG13-TD370/WP3

Study Group 13

Original: English

Question(s): 2/13 Geneva, 13 March 2020

TD

Source: Editors

Title: Draft new Recommendation ITU-T Y.DNI-fr: “Framework and Requirements of Decentralized Trustworthy Network Infrastructure”

Purpose: Discussion

Contact: Bo Lei
China Telecom
China
Tel: +861050902903
E-mail: leibo.bri@chinatelecom.cn

Contact: Miao Xue
China Unicom
China
Tel: +861068799999
E-mail: xuemiao9@chinaunicom.cn

Contact: Xinpeng Wei
Huawei Technologies Co., Ltd
China
E-mail: weixinpeng@huawei.com

Contact: David Dai
China Information Communication Technologies Group
China
E-mail: djy@fiberhome.com

Keywords: Decentralized Trustworthy Network Infrastructure, DNI, framework, requirements, use cases

Abstract: This document contains ITU-T Recommendation Y.DNI-fr: “Framework and Requirements of Decentralized Trustworthy Network infrastructure”, output of Q2/13 meeting, Geneva, 2-13 Mar 2020.

This output draft is based on TD332(WP3/13), output of Q2/13 meeting, Geneva, 14-25 Oct, 2019, and amendments according to 2-13 March Q2/13 Rapporteur meeting agreements based on meeting discussions and review of the following contribution:

No.	**Source**	**Title**	**Discussion and results**
17741-C5 (200302)	Huawei Technologies Co., Ltd	Proposed modifications on work item of ITU-T Y.DNI-fr	This contribution was accepted with some modifications.

Formatted Table

Table of Contents

Formatted: Centered

Formatted: Font: (Default) Times New Roman, 12 pt

Draft new Recommendation ITU-T Y.DNI-fr

Framework and Requirements of Decentralized Trustworthy Network Infrastructure

~~1.~~1 Scope

Formatted: Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0 cm + Indent at: 0,75 cm, Font Alignment: Baseline

This Recommendation aims to specify framework and requirements of decentralized trustworthy network infrastructure.

Formatted: Left

The scope of this Recommendation includes:

- ~~o~~ Framework of decentralized trustworthy network infrastructure;
- ~~o~~ Capability requirements of decentralized trustworthy network infrastructure;
- ~~o~~ Use cases and workflows of decentralized trustworthy network infrastructure.

Formatted: Normal, Left, No bullets or numbering

In terms of use cases, the Recommendation includes the application of this framework to NGN evolution.

Formatted: Normal, Left, Space Before: 0 pt

~~1.~~2 References

Formatted: Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0 cm + Indent at: 0,75 cm, Font Alignment: Baseline

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published.

Formatted: Left

The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

Editor's note: references to be completed as appropriate along the development of the draft Recommendation.

~~-~~[ITU-T Y.2012] Recommendation ITU-T Y.2012 (2010), *Functional requirements and architecture of the NGN*

[ITU-T Y.2001] Recommendation ITU-T Y.2001 (2004), *General overview of NGN*

~~2.~~3 ~~-~~Terms and definitions

Formatted: Heading 1, None, Space Before: 0 pt, Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0 cm + Indent at: 0,75 cm

Editor's note: terms to be completed as appropriate along the development of the draft Recommendation.

Formatted: Left

3.1 ~~3.1~~ Terms defined elsewhere

Formatted: Indent: Left: 0 cm, Outline numbered + Level: 2 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0,75 cm + Indent at: 1,75 cm, Font Alignment: Baseline, Tab stops: 1,4 cm, Left + Not at 0,77 cm

This Recommendation uses the following terms defined elsewhere:

Editor's note: the following is the current definition (under development) of "Blockchain" in ITU-T FG-DLT (DLT-O-047-DLT-1.1, Jan 2019)

Formatted: Normal, Space Before: 0 pt

3.1.1 Blockchain [ITU-T FG-DLT-1.1]: A type of distributed ledger which is comprised of unchangeable, digitally recorded data in packages called blocks, where each block is then 'chained' to the next block, using a cryptographic link.

NOTE – Consider the definition ‘blockchain’ as “A model that construct chained-block data structure which cannot be tampered with and can be traced in peer-to-peer networks through transparent and trustworthy rules.”

NOTE – Consider the definition ‘blockchain’ as “A ledger where data is recorded in blocks in such a way that each new block includes information about the previous block.”

NOTE – [b-X.sct-dlt] defines ‘Blockchain’ as “A peer to peer distributed ledger technology for a new generation of transactional applications which maintains a continuously growing list of cryptographically secured data records hardened against tampering and revision. NOTE 1 - Blockchain can help establish trust, accountability and transparency while streamlining business processes.

NOTE - Categorized by types of participants, blockchains can be divided as public blockchains, consortium (or permissioned) blockchains and private blockchains.”

NOTE – [b-X.strdlt] defines ‘Blockchain’ as “The technology underlying bitcoin and other cryptocurrencies—a shared digital ledger, or a continually updated list of all transactions. Blockchains are immutable digital ledger systems implemented in a distributed fashion (i.e, without a central repository) and usually without a central authority. [Draft NISTIR 8202]” referencing [b-DFS] and [b-NIST].

NOTE – [b-ISO/TC 307] defines ‘Blockchain(s)’ as “distributed ledger with confirmed and validated blocks organized in an append-only, sequential chain using cryptographic links” with a note, “blockchains are designed to be tamper resistant and to create final and definitive (immutable) records”

NOTE – [b-ISO/TC 307] defines ‘blockchain system(s)’ as “system that implements a blockchain.”

~~*Editor’s note: the following is the current definition (under development) of “Distributed Ledger” in ITU-T FG-DLT (DLT-O-047-DLT-1.1, Jan 2019)*~~

Formatted: Normal, Space Before: 0 pt

3.1.2 Distributed Ledger [ITU-T FG-DLT-1.1]: A type of ~~ledger, that~~ledger that is shared, replicated, and synchronized in a distributed manner.

NOTE – Consider the definition ‘distributed ledger’ as “An asset database that can be co-managed and shared across multiple sites, geographies, or networks of multiple agencies.”

Formatted: Normal

NOTE – [b-X.tfspd-dlt], [b-X.stov] and [b-X.sadlt] define ‘distributed ledger’ as “electronic data that has been replicated, shared, synchronized and stored by consensus in physically separate multiple places (e.g. states, organizations, etc.)”

NOTE – Consider the definition ‘distributed ledger technology’ as “A collection of technologies that enable distributed ledgers.”

NOTE – [b-X.srdrm-dlt], [b-X.sa-dlt] and [b-X.das-mgt] define ‘distributed ledger technology’ as “a shared digital ledger, or a continually updated list of all transactions” referencing ITU-T FG-DFS-Glossary. [b-X.sa-dlt] and [b-X.das-mgt] add a note “This is the technology underlying Bitcoin and other crypto currencies.”

NOTE – [b-X.ss-dlt] defines ‘DLT’ as “A peer to peer distributed ledger technology for a new generation of transactional applications which maintains a continuously growing list of cryptographically secured data records hardened against tampering and revision.

NOTE - [b-ISO/TC 307] defines ‘distributed ledger(s)’ as “ledger that is shared and synchronized in a distributed manner.” In addition of that, [b-ISO/TC 307] defines distributed ledger technology, distributed ledger network, distributed ledger system, distributed ledger technology platform, distributed system separately.

NOTE 1 - DLT can help establish trust, accountability and transparency while streamlining business processes.

NOTE 2 - DLTs can be classified three types (i.e. public, consortium and private) based on the relationship of the participants and the way to provide services.”

3.2 Terms defined in this Recommendation

Formatted: Indent: Left: 0 cm, Outline numbered + Level: 2 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0,75 cm + Indent at: 1,75 cm, Font Alignment: Baseline

This Recommendation defines the following terms:

Based on the definitions and concepts mentioned in 3.1, the DLT is seen as a general concept which contains public chain, consortium chain and private chain. The blockchain is seen as a specific implementation of DLT especially with public chain.

~~TBD~~

~~3.~~4 Abbreviations and acronyms

Formatted: Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0 cm + Indent at: 0,75 cm, Font Alignment: Baseline

Editor’s note: to be completed.

This Recommendation uses the following abbreviations and acronyms:

ASN	Autonomous System Number
BGP	Border Gateway Protocol
DDoS	Distributed Denial of Service
DLT	Distributed Ledge Technology
DNI	Decentralized Network Infrastructure
DNS	Domain Name System
IP	Internet Protocol
NGN	Next Generation Network
PKI	Public Key Infrastructure

Formatted: Left

~~4.~~5 Conventions

Formatted: Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0 cm + Indent at: 0,75 cm, Font Alignment: Baseline

In this Recommendation:

Formatted: Left

The keywords "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

The keywords "can optionally" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option, and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with this Recommendation.

~~5.~~6 Gap Analysis and Capability requirements

Formatted: Heading 1, None, Space Before: 0 pt, Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0 cm + Indent at: 0,75 cm

~~*Editor’s note: This clause will at first (in sub-clause 8.1) provide high level requirements of decentralized trustworthy network infrastructure based on the framework foundational elements*~~

~~*and their specific roles in the framework layering context. It will then provide (in sub-clause 8.2 and beyond) detailed requirements related to these various foundational elements.*~~

~~*More generally, this clause is expected to set the basic needs to promote the development of further specification works concerning the architecture and architectural components of a decentralized trustworthy network.*~~

~~*Editor's note: [20191022] It is suggested in SG-13 meeting that there should be a "Gap Analysis" before the framework. The chapter has been merged with the previous requirement chapter and the new Chapter is modified as "Gap Analysis and Capability requirements"*~~

6.1 Gap Analysis

~~6.1 Gap Analysis~~

~~6.2 High level requirements~~

Any services and applications must rely on the network infrastructure to support fundamental abilities such as admission, resolution and connectivity. Based on these abilities, the logic entities and functions can be executed. Furthermore, the core of this infrastructure is how to build up a trusted and robust system that provides universal and equal credibility. Most of the current network infrastructure systems tend to be centralized, which may have fundamental vulnerabilities:

- Entities rely on central authorities as trust anchors
- An authority has the privilege to unilaterally remove descendants' trust anchors
- A central authority can be hacked or compromised to perform malicious actions.
- A central authority may not be fully neutral.

Potential inequity caused by conflicts of interests, politics, or domestic laws, may lead to risks such as:

- A central authority can cause globally damaging impacts.
- Entities, relying on centralization, may become untrusted. Services may become unavailable, resulting in economic losses and even damaging impacts.
- An authority in one country can also damage the trust anchors of organizations in other countries, because trust chains are often across countries.

Thus, a decentralized architecture design of the trust infrastructure is able to consolidate the trust and equity of the network, and further facilitate the healthy and long-term sustainable growth of the network. An all-in-one design, which is expected to support various scenarios and act as a trustworthy framework for the future network infrastructure as mentioned above.

6.2 ~~6.3~~ Requirements of connectivity

~~*Editor's note:*~~ The connectivity of network is very important because it relates to the fundamental ability of the network. BGP is a typical case that provides connectivity in the network. It is taken as an example to show the potential requirements. The requirements of the BGP's trustworthiness are (but may not be limited to):

Formatted: Space Before: 6 pt

Formatted: Heading 2, Indent: Left: 0 cm, Outline numbered + Level: 2 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0,75 cm + Indent at: 1,75 cm

Formatted: Font: Not Bold, English (United Kingdom)

Formatted: Heading 2, None, Indent: Left: 0 cm, Outline numbered + Level: 2 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0,75 cm + Indent at: 1,75 cm

Formatted: English (United Kingdom)

Formatted: Heading 2, None

Formatted: Indent: Left 0 ch

Formatted: Indent: Left 0 ch

Formatted: English (United Kingdom)

Formatted: Heading 2, None, Indent: Left: 0 cm, Outline numbered + Level: 2 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0,75 cm + Indent at: 1,75 cm

Formatted: Font: Not Bold, English (United Kingdom)

Formatted: Font: Not Italic

- The novel proposed framework supports trustworthiness for the network connectivity so that any intentional attack or unintentional mis-operation can be avoided by using distributed ledger technology.
- Synchronization and update of route information is compatible with legacy approach. Even though some security schemes have been already developed, such as BGPSEC, the essential centralized authority architecture is still a potential problem. The novel framework is expected to solve the trusted connectivity essentially.

6.3 ~~6.4~~ Requirements of name and mapping management

~~*Editor's note:*~~ The name/identity resource in the network often needs to be mapped to other information, and the device participating in the communication obtains the mapping information from the mapping system. For example, in the DNS system, the domain name is mapped to an IP address, and the IP address is mapped to the ASN in the routing system.

- Avoid single point of failure problem, the mapping service runs normally even in case of the failure of one or several nodes that providing mapping service.
- The resource owner can manipulate mapping information related to the resource.
- The mapping information stored in the system should be trustable.
- The mapping information queried from the system is verifiable.
- Reducing the mapping query delay especially for the time-sensitive services.

A decentralized system is not similar to a distributed one. A distributed system can be centralized. The current DNS system is a typical case. A decentralized network infrastructure is expected to rebuild the trust logic so that a novel trusted system can be provided.

6.4 ~~6.5~~ Requirements of admission control and resource ownership management

~~*Editor's note:*~~ There are various resources in the network, for example, IP address, domain name, ENUM, autonomous number and various other forms of communication id. The trustworthiness of the network is established based on the trusted confirmation of the ownership of the resource. Taking IP address management as an example, the novel IP address management scheme is based on distributed ledger with admission control. The requirements of IP management are (but may not be limited to):

- The underlying distributed ledger runs in a permissioned mode and admission control for participants should be provided.
- The trustworthiness of resource ownership is confirmed by a group of parties instead of a single party.
- Trusted confirmation of network resource ownership. Providing support for IP address and domain name ownership confirmation, and exploring support for other resources ownership confirmation.
- Trusted recording of ownership information of resources, which is tamper-proof and others can verify ownership information for a particular resource based on recorded information.
- The validity of resource ownership and mapping only depends on the owner itself, instead of any third party.

Formatted: Indent: Left 0 ch

Formatted: English (United Kingdom)

Formatted: Font: Not Bold, English (United Kingdom)

Formatted: Heading 2, None, Indent: Left: 0 cm, Outline numbered + Level: 2 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0,75 cm + Indent at: 1,75 cm

Formatted: Font: Not Italic

Formatted: Indent: Left 0 ch

Formatted: English (United Kingdom)

Formatted: Heading 2, None, Indent: Left: 0 cm, Outline numbered + Level: 2 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0,75 cm + Indent at: 1,75 cm

Formatted: Font: Not Bold, English (United Kingdom)

Formatted: Font: Not Italic

Formatted: Indent: Left 0 ch

For other aspects, there are also potential benefits, such as preventing address exhaustion, enforcing prefix aggregation, and organization-level traceability and admission control. The new framework can support dealing with IPv6 address allocation, and IPv6/IPv4 address re-allocation. Introduction of Decentralized Trustworthy Network Infrastructure.

7 The introduction about Decentralized Trustworthy Network Infrastructure

The Decentralized Trustworthy Network Infrastructure (DNI) aims at building a fully decentralized and distributed network infrastructure which aims at improving the current centralized network infrastructure systems to avoid the above listed fundamental vulnerabilities of centralized network infrastructure.

The DNI is built based on distributed ledger technology which has intrinsic feature of decentralization, and also distributed ledger technology can provide other useful capabilities such as smart contract, verifiable translations, multiparty consensus, and immutable records.

The distributed ledger technology may be permissioned and permissionless, which determines if anyone or only approved people can participant in the ledger system. For DNI, the system needs to provide admission control and only the admitted participant can play the role of system node, so a permissioned distributed ledger is chosen. For other public participants without permission can retrieve information on DNI through admitted participants.

In order to consolidate the trust and equity of the network infrastructures, and further facilitate the healthy and long-term sustainable growth of the network, DNI define a new trust mode which removes the relay on central authorities as trust anchors. Based on the new trust mode, network resources management scheme is defined to certify resources ownership which is a basis for other functionalities.

The DNI system will act as a universal basic service for different kinds of high level network service and application service. A DNI framework is defined below that can adapt to different kinds of scenarios.

~~6.~~8 Framework of Decentralized Trustworthy Network Infrastructure

8.1 Framework overview

~~**Editor's note: This clause will at first (in sub-clause 7.1) provide an overview of the framework from an architectural perspective, with its foundational elements, and will then provide (in sub-clause 7.2 and beyond) a technical description of these elements and the specific roles played by such elements for the purpose of enabling a decentralized trustworthy network infrastructure.**~~

~~**8.1 Framework overview**~~

~~**Editor's note: further content concerning framework layering is for consideration (see C589 and C581R2 of March 2019 SG13 meeting).**~~

~~The~~ The framework of decentralized trustworthy network infrastructure consists from the architectural viewpoint of three layers, as shown in Figure 8-1.

Formatted: English (United Kingdom)

Formatted: Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0 cm + Indent at: 0,75 cm, Font Alignment: Baseline, Tab stops: Not at 0,76 cm

Formatted: English (United States)

Formatted: Font: Not Italic

Formatted: Font:

Formatted: Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0 cm + Indent at: 0,75 cm, Font Alignment: Baseline, Tab stops: Not at 0,76 cm

Formatted: Heading 2, Indent: Left: 0 cm, Outline numbered + Level: 2 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0,75 cm + Indent at: 1,75 cm

Formatted: Font: Not Italic

Formatted: Indent: Left: 0 cm, Outline numbered + Level: 2 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0,75 cm + Indent at: 1,75 cm, Tab stops: 1,4 cm, Left + Not at 0,56 cm

Formatted: Font: Bold

Formatted: Pattern: Clear

Formatted: Heading 2, Indent: Left: 0 cm, Outline numbered + Level: 2 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0,75 cm + Indent at: 1,75 cm

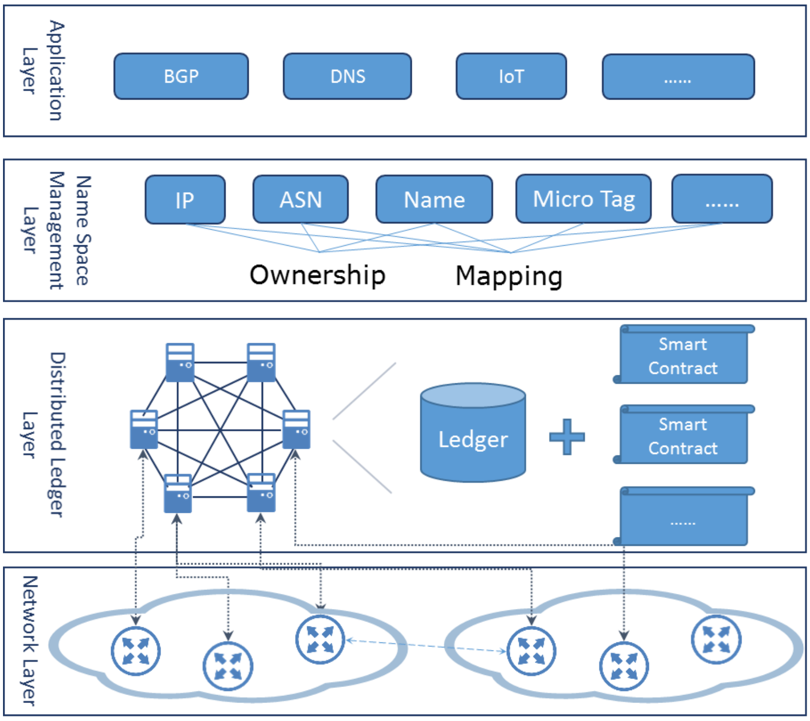


Figure 8-1 Framework of Decentralized Trustworthy Network Infrastructure

~~*Editor's note: contributions are invited to update the figure into more technical manner, especially concerning "network infrastructure" focus and the terminology of the layers.*~~

~~*Editor's note: brief description of the Network Layer to be added.*~~

a) Network Layer

This layer provides network connectivity for the nodes in Distributed Ledger Layer.

■ b) Distributed Ledger Layer

This layer uses distributed ledger technology to build the underlying decentralization capabilities.

■ c) Name Space Management Layer

This layer uses the basic capabilities provided by the distributed ledger to construct a decentralized trusted management mechanism for network namespaces such as IP addresses, domain names and others.

■ d) Application Layer

This layer is an open application layer that supports and promotes innovative, trusted, decentralized network applications.

Formatted: Normal, Space Before: 0 pt, No bullets or numbering

Formatted: Normal, Space Before: 0 pt, No bullets or numbering

Formatted: Normal, Space Before: 0 pt, No bullets or numbering

8.2 ~~8.2~~ Network Layer

Formatted: Indent: Left: 0 cm, Outline numbered + Level: 2 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0,75 cm + Indent at: 1,75 cm

The Network Layer provides basis network connectivity for the nodes in Distributed Ledger Layer. The security-related operations based on the information retrieved from Distributed Ledger Layer is also established in this layer. It is basically seen as the continuation of the network infrastructure.

Formatted: Normal

8.3 Distributed Ledger Layer

Formatted: Indent: Left: 0 cm, Outline numbered + Level: 2 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0,75 cm + Indent at: 1,75 cm

The Distributed Ledger Layer is the basis of decentralized network infrastructure. It is in charge of providing the following functions:

- Providing decentralized system structure
- Providing distributed consensus mechanism
- Providing smart contracts capability
- ~~-~~ Guarantee of trustable trade

Formatted: Normal, Space Before: 0 pt, No bullets or numbering

Formatted: (Asian) Chinese (China), Not Highlight

The Distributed Ledger Layer is in the form of a coalition, and each member in the coalition runs a server node to communicate with other members' server node and finally a distributed system is built up.

~~Underneath of the Distributed Ledger Layer is the global network system (Internet), the network system provides connectivity for the Distributed Ledger Layer, and at the same time the network system could do security-related operations based on the information retrieved from Distributed Ledger Layer.~~

The Distributed Ledger Layer participates are ISP users. They have the offline trusted business relationship. The security can be enhanced based on this feature. Some Distributed Ledger information (such as the account/node information) can be exchanged by BGP message in BGP peer establishment. The Distributed Ledger Layer can detect some attacks such as eclipse attack according to this information.

8.4 ~~8.3~~ Name Space Management Layer

Formatted: Indent: Left: 0 cm, Outline numbered + Level: 2 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0,75 cm + Indent at: 1,75 cm

Formatted: Font: Bold

Formatted: Space Before: 6 pt

The namespace is at the heart of the TCP/IP protocol and the core of the network infrastructure.

For example, BGP and DNS, as the core functions in the network, rely on namespaces. BGP maps the IP address prefix to the AS number and AS Path to calculate the inter-domain route in the IP address space. Trusted IP address prefix ownership and mapping are very important, otherwise there will be network attacks such as BGP prefix hijacking and path hijacking. DNS maps the namespace to the IP address space, allowing the service to be accessed at the network layer. Trusted domain name ownership and mapping are also critical, otherwise there will be loopholes such as domain name cache pollution, DDoS attack on DNS server and domain name hijacking. The Micro Tag indicate the identity for light-weight IoT devices or services, which can provide trusted verification function. These are huge number of light-weight devices connecting to the network in the future and their trusted identity could provide reliable condition.

Trusted and reliable name attribution and name mapping are the basis for a trusted and reliable infrastructure. For this reason, the name space management layer is used as the middle layer of the architecture to ensure the security and credibility of the infrastructure through decentralized trusted name attribution and mapping, and thus support of trusted upper-layer applications.

~~*Editor's note: this part needs to be reviewed in next meeting*~~

8.5 ~~8.4~~ Application Layer

Formatted: Indent: Left: 0 cm, Outline numbered + Level: 2 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0,75 cm + Indent at: 1,75 cm

Formatted: Font: Bold

The Application Layer provides support for secure and trusted decentralized network applications based on the services provided by the Distributed Ledger Layer and Name Space Management Layer.

Here are several typical applications that runs on DNI infrastructure:

1. BGP security-related application. Based on the IP address ownership information provided by Name Space Management Layer, the IP prefix hijacking prevention application can be implemented to provide security service for BGP system.

2. Trusted domain name application. The trustable binding information on domain name and IP address can be used to provide domain name verification service.

3. Identity-related application for Internet of Things. The IoT device’s trustable ID information could be maintained in Name Space Management Layer, and the trustable ID can be used for security communication between IoT devices.

8.6 ~~8.5~~ Components of Distributed Ledger Layer

Formatted: Font: Bold

Formatted: Indent: Left: 0 cm, Outline numbered + Level: 2 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0,75 cm + Indent at: 1,75 cm

The Distributed Ledger Layer builds up on several basic components, as illustrated in Figure 8-2, and these components provide required functionalities for Name Space Management Layer and Application Layer.

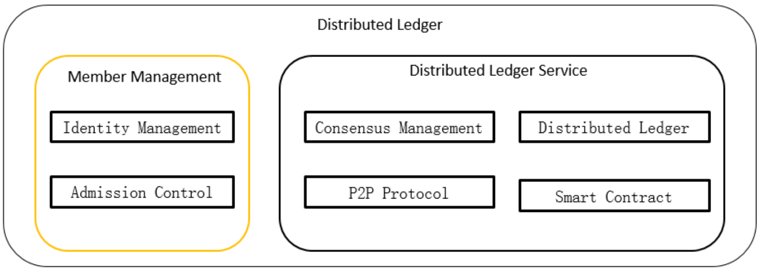


Figure 8-2 Components of Distributed Ledger Layer

Components for Member Management:

Identity Management

Each participant node is assigned an Identity for access to the system and the node will be uniquely identified by its Identity in the whole system.

The Identity Management component is in charge of managing the Identity of all participants node, including Identity assignment, Identity cancellation etc.

Admission Control

The Admission Control component is in charge of the admission control policy control, only the participant nodes permitted by the admission control police is allowed to access to the system.

Components for Distributed Ledger Service:

Consensus Management

The Consensus Management component is in charge of the running of consensus procedures to get consensus among Nodes.

Distributed Ledger

The Distributed Ledger is in charge of storage of data that passes through the consensus procedure, with the characteristic of irreversible and cannot be corrupted.

Smart Contract

The Smart Contract is charge of maintaining and running of smart contract.

P2P Protocol

P2P protocol component is in charge of communications among nodes.

8.7 ~~8.6~~ Roles of Nodes

Formatted: Indent: Left: 0 cm, Outline numbered + Level: 2 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0,75 cm + Indent at: 1,75 cm

The role of node in the system can be sorted into different types, and in actual deployment, some of these roles may implemented on the same node.

Peer Node

The Peer node is the fundamental element of the DNI system, and there will be many Peer nodes connecting to the DNI system. Each player participate in the DNI will run a Peer node and interact with DNI system through the Peer node.

Each Peer node has the following basic functionalities:

(1) Retrieves information from Distributed Ledger.

(2) Runs application layer functions.

(3) Invokes smart contracts in DNI system.

Endorser Node

The Endorser node is in charge of providing endorsement for requests from Peer node, and there will be different Endorser nodes connecting to the DNI system, each Endorser node can provide endorsing service for different Peer node.

Each Endorser node has the following basic functionalities:

(1) Validating the content of request from Peer node.

(2) Endorsing for the request by signing with Endorser’s private key.

Consensus Node

The Consensus node plays critical role in the DNI system. Consensus node runs consensus protocol between each other to reach consensus for each transaction.

The Consensus node collects a bunch of transactions and orders the transactions into block.

Committer Node

The Committer node is in charge of maintains the Distributed Ledger records.

The interaction process between different roles is illustrated in Figure 8-3.

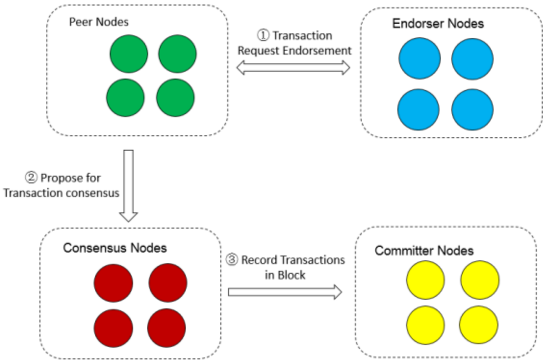

Peer Nodes
① Transaction Request Endorsement
Endorser Nodes
② Propose for Transaction consensus
Consensus Nodes
③ Record Transactions in Block
Committer Nodes

Figure 8-3 Interactions between Roles

In case a Peer node start out a Transaction, the Transaction needs to be first endorsed by one or more Endorser node, the Endorser node checks the validity of the Transaction and make endorsement for the Transaction.

After get the Transaction endorsed, the Peer node propose the Transaction to Consensus nodes for consensus, the Consensus node put a list of Transactions received into Block orderly, and the Block will be recorded by the Committer node.

~~7.~~9 Security considerations

~~*Editor's note: To be completed*~~

The goal of this work item aims to provide a new trust mode as basic service to other applications, therefore, the security of DNI system itself is critical. This section will provide an analysis of security issues that DNI system would encounter and also some considerations to mitigate these issues are also provided.

Two aspects have been considered. The network layer security and the distribute ledger layer security.

9.1 Network Layer security

Network layer is responsible for providing secure connection between different ledger nodes. One of the possible attack at network layer is Eclipse Attack, which is a well-known means of attacking a decentralized network. In eclipse attack, the attacker try to isolate specific ledger node from the other nodes to prevent the node to synchronize its state with other nodes. It could be possible for attackers to isolate one ledger node from the others, but it would be hard to isolate all ledger nodes from each other which requires the control of whole network, the level of difficulty would be similar to isolate hosts on the Internet from each other. Because the ledger layer could still work even when some of its nodes are isolated, so we think the eclipse attack is not a big issue here.

9.2 Ledger Layer Security

The ledger layer security will be guaranteed by specific ledger technology, because the distributed ledger technology itself is a Byzantine Fault Tolerance system, so it can cope with some amount of

Formatted: Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0 cm + Indent at: 0,75 cm, Font Alignment: Baseline, Tab stops: Not at 0,76 cm

Formatted: Heading 2, Indent: Left: 0 cm, Outline numbered + Level: 2 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0,75 cm + Indent at: 1,75 cm

Formatted: Heading 2, Indent: Left: 0 cm, Outline numbered + Level: 2 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0,75 cm + Indent at: 1,75 cm

Formatted: Left

byzantine fault node which could act arbitrarily. For DNI system, the security properties provided by ledger technology would be enough, such as Hyperledger Fabric.

One aspect needs to be considered is information privacy. Even though the DNI is based on permissioned ledger system, but the information recorded in the ledger will be open to public for different kinds of services, so the privacy considerations need to be taken.

Appendix I Use Cases and Workflows of Decentralized Trustworthy Network Infrastructure

Formatted: Tab stops: 1,4 cm, Left + Not at 0 cm

(This appendix does not form an integral part of this Recommendation)

Formatted: Left

~~*Editor's note: In terms of use cases, the study will include the application of the framework to NGN evolution.*~~

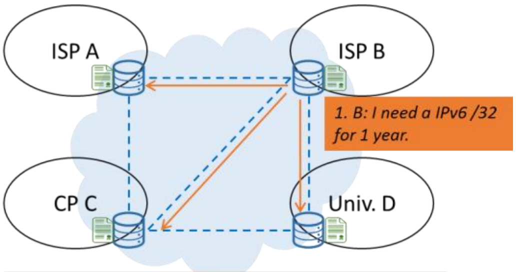
~~*Editor's note: The following content provides some examples of use cases. Further developments are invited.*~~

1. IP and ASN Ownership Management

Formatted: Font: (Default) Times New Roman, 12 pt, Bold, (Asian) Chinese (China)

Formatted: Space Before: 0 pt, Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0 cm + Indent at: 0,74 cm, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Font: (Default) Times New Roman, 12 pt



1. B: I need a IPv6 /32 for 1 year.

2. Other nodes: the best prefix for you is 2001:da8::/32, written into ledger.

Figure I-2 General Overview of IP and ASN ownership management

The distributed ledger is used to deal with IP and ASN ownership. Only eligible organizations (e.g., RIRs, NIRs, ISPs) can participate in the smart contract.

Formatted: Left

The process of address allocation is simple. Take ISP B as an example.

~~[1]~~ First, B sends a transaction to other ~~blockchain~~ DLT nodes requesting for an IPv6 /32 prefix and pays an annual fee in the transaction.

Formatted: Normal, Space Before: 0 pt, No bullets or numbering

~~[2]~~ Other nodes receive the transaction, and use smart contract to calculate a continuous prefix for B from available address pool and writes the results into the ledger.

~~[3]~~ B needs to renew the prefix before it expires. Otherwise, smart contract will be triggered and the prefix is recycled into the pool.

AS number ownership is managed in a similar way.

Formatted: Left

Formatted: Font: (Default) Times New Roman, 12 pt

Formatted: Space Before: 0 pt, Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0 cm + Indent at: 0,74 cm, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

2. Domain name management

Domain name management runs in a separate smart contract, because the requirement is different from that of IP&ASN.

- First, IP address space can be exhausted, while domain name space cannot.
- Second, IP address is allocated using sparse delegation algorithm, while domain name is allocated in a first-come first-serve manner.

Besides, the sub-spaces of domain name are managed differently.

For generic domains, like .com, .net etc., the focus is on SLD (e.g., example.com) allocation. Agencies (e.g., GoDaddy) participate the smart contract for name space operations. Users can apply or transfer names via agencies, while avoid agency lock-in or misbehaviors. For ccTLDs, only the national network information centers (NICs) are permitted to operate on ccTLDs.

3. Decentralized Root DNS

Building decentralized root DNS in NGN network based on the defined Decentralized Network Infrastructure is shown below.

The decentralized root DNS is to provide the DNS zone file locally and lower synchronization delay, while on other hand this increases the independence and autonomy of the participants (NGN operators) and reduces the domain name query delay especially for the time-sensitive services.

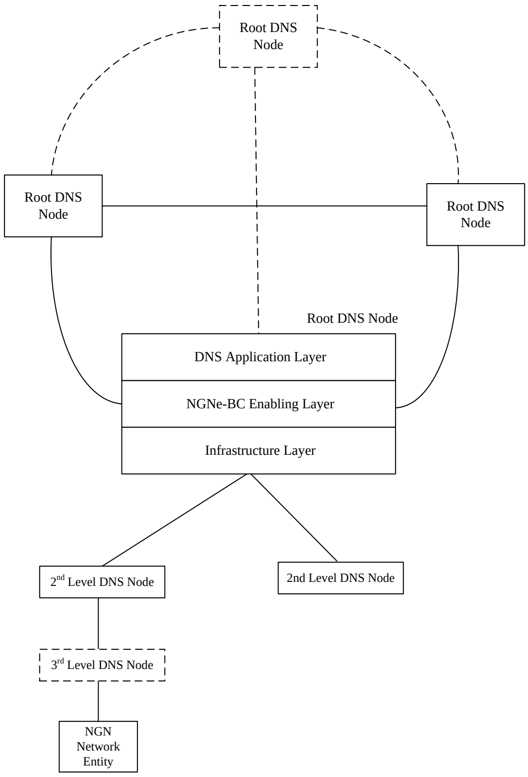


Figure I-2 High-Level Framework of Decentralized Root DNS

Formatted: Left

Formatted: Normal, Space Before: 0 pt, No bullets or numbering

Formatted: Left

Formatted: Font: (Default) Times New Roman, 12 pt

Formatted: Space Before: 0 pt, Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0 cm + Indent at: 0,74 cm, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Left

4. ~~Security~~ Secure Distributed Ledger

The Distributed Ledger Layer participates are ISP users. They have the offline trusted business relationship. The security can be enhanced based on this feature. Some Distributed Ledger information (such as the account/node information) can be exchanged by BGP message between BGP peers. The Distributed Ledger Layer can detect some attacks such as eclipse attack according to this information.

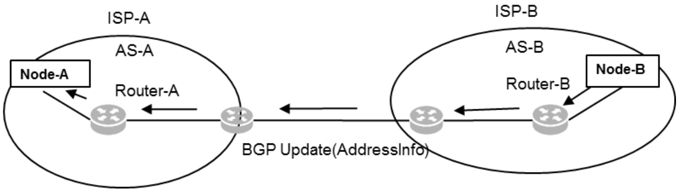


Figure I-3 Address Information Exchange between ASes

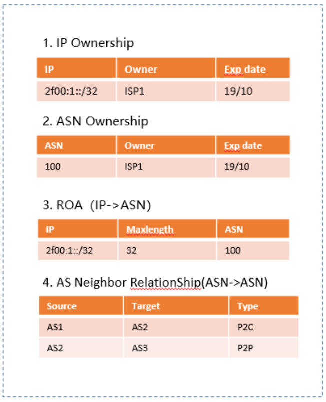
Autonomous System AS-A and AS-B are the neighbor. Node-A in AS-A can get the AddressInfo of Node-B in AS-B through the routers. Node-A can establish the connection with Node-B based on the AddressInfo of Node-B. This Distributed Ledger Layer connection can be trusted for the peers have the offline trusted relationship.

The interface between Node and Router can be BGP, RPKI-RTR or new-defined interface. The addressinfo can be the nodeID, IP address or MAC address of the Node.

5. BGP Security based on DNI

BGP (Border Gateway Protocol) is a standardized exterior gateway protocol designed to exchange routing and reachability information among autonomous systems (AS) on the Internet. The security of BGP protocol is critical for the running of Internet, and there are three well-known BGP security issues which are prefix hijack, route leak and path hijack. The BGP security issues can be solved based on the DNI architecture defined above.

Firstly, the information required to deal with BGP security issues needs to be recorded in the distributed ledger. The information to be recorded includes: IP ownership, ASN ownership, the mapping between IP prefix to ASN, and the AS neighbour relationship.



1. IP Ownership

IP	Owner	Exp date
2f00:1::/32	ISP1	19/10

2. ASN Ownership

ASN	Owner	Exp date
100	ISP1	19/10

3. ROA (IP->ASN)

IP	Maxlength	ASN
2f00:1::/32	32	100

4. AS Neighbor RelationShip(ASN->ASN)

Source	Target	Type
AS1	AS2	P2C
AS2	AS3	P2P

Formatted: Left

Formatted: Font: (Default) Times New Roman, 12 pt

Formatted: Space Before: 0 pt, Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0 cm + Indent at: 0,74 cm, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Space Before: 6 pt, Tab stops: Not at 1,62 cm + 3,23 cm + 4,85 cm + 6,46 cm + 8,08 cm + 9,69 cm + 11,31 cm + 12,92 cm + 14,54 cm + 16,16 cm + 17,77 cm + 19,39 cm + 21 cm + 22,62 cm + 24,23 cm + 25,85 cm

Formatted: English (United Kingdom)

Formatted: Space Before: 6 pt, Tab stops: Not at 1,62 cm + 3,23 cm + 4,85 cm + 6,46 cm + 8,08 cm + 9,69 cm + 11,31 cm + 12,92 cm + 14,54 cm + 16,16 cm + 17,77 cm + 19,39 cm + 21 cm + 22,62 cm + 24,23 cm + 25,85 cm

Formatted: Left

Formatted: Font: (Default) Times New Roman, 12 pt, Bold

Formatted: List Paragraph, Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0 cm + Indent at: 0,74 cm

Formatted: Font: Bold

Formatted: Centered

Figure I-4 Ownership and Relationship Storage

The routers running BGP protocol are connected to DNI system, and when a BGP Update message is received the router retrieve the recorded information from DNI system to verify the contents in BGP Update, if the verification result is valid the BGP Update message will be sent to the next hop router, otherwise the BGP Update message will be dropped.

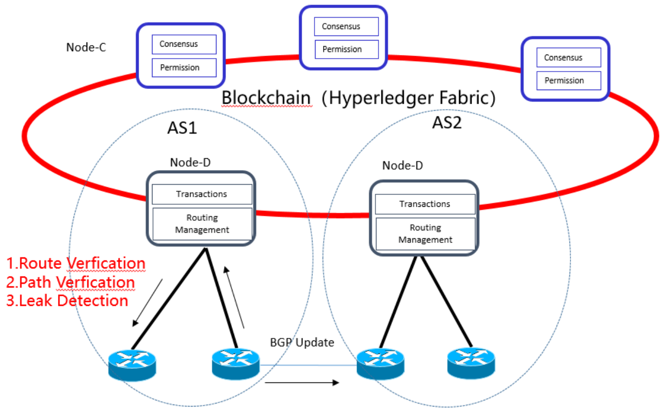


Figure I-5 A Hyperledger Fabric based Path Verification System Framework

Bibliography

To be completed.

Formatted: Centered

Formatted: Left

Formatted: Left, Indent: Left: 0 cm, Hanging: 1,4 cm