Draft new Recommendation ITU-T Y.2086 (formerly Y.DNI-fr)

Framework and Requirements of Decentralized Trustworthy Network Infrastructure

Summary

This Recommendation specifies the framework and requirements of Decentralized Network Infrastructure. The Decentralized Network Infrastructure is expected to enhance the trustworthiness of the network infrastructure via a universal basic framework for different kinds of high-level network services. This Recommendation includes the framework, requirements, and use cases of the Decentralized Network Infrastructure.

Keywords

Decentralized trustworthy network infrastructure, framework, requirements, use cases.

Table of Contents

Draft new Recommendation ITU-T Y.DNI-fr

Framework and Requirements of Decentralized Trustworthy Network Infrastructure

1 Scope

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

The Decentralized Network Infrastructure is expected to enhance the robustness of the Internet infrastructure via a universal basic service for different kinds of high-level network services.

The scope of this Recommendation includes:

- Framework of Decentralized Network Infrastructure;
- Capability requirements of Decentralized Network Infrastructure;
- Use cases and workflows of Decentralized Network Infrastructure.

As far as the use cases, they highlight the application of this framework applied to Next Generation Network (NGN) evolution and are aligned with [ITU-T Y.2342].

2 References

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.

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

[ITU-T Y.2342] Recommendation ITU-T Y.2342 (2019), *Scenarios and Capability Requirements of Blockchain in Next Generation Network Evolution.*

3 Terms and definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 Next Generation Network (NGN) [b-ITU-T Y.2001]: A packet-based network which is able to provide telecommunication services and able to make use of multiple broadband, Quality of Service (QoS)-enabled transport technologies and in which service-related functions are independent from underlying transport-related technologies. It enables unfettered access for users to networks and to competing service providers and/or services of their choice. It supports generalized mobility which will allow consistent and ubiquitous provision of services to users.

3.1.2 Block [b-ITU-T FG-DLT-D1.1]: Individual data unit of a Blockchain, composed of a collection of transactions and a block header. NOTE – A block may be immutable and considered as the digital entity described in clause 3.2.2 in [b-X.1255], however, it can be applied to other networks or other computational facilities.

3.1.3 Blockchain [b-ITU-T FG-DLT-D1.1]: A type of distributed ledger which is composed of digitally recorded data arranged as a successively growing chain of blocks with each block cryptographically linked and hardened against tampering and revision.

3.1.4 Distributed Ledger [b-ITU-T FG-DLT-D1.1]: A type of ledger that is shared, replicated, and synchronized in a distributed and decentralized manner.

3.1.5 Smart Contract [b-ITU-T FG-DLT-D1.1]: Program written on the distributed ledger system which encodes the rules for specific types of distributed ledger system transactions in a way that can be validated, and triggered by specific conditions.

3.1.6 Transaction [b-ITU-T FG-DLT-D1.1]: Whole of the exchange of information between nodes. A transaction is uniquely identified by a transaction identifier.

3.1.7 Participant [b-ITU-T FG-DLT-D1.1]: An actor who can access the ledger: read records or add records to.

3.1.8 Consensus [b-ITU-T FG-DLT-D1.1]: Agreement that a set of transactions is valid.

3.2 Terms defined in this Recommendation

None

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AS	Autonomous System
ASN	Autonomous System Number
BGP	Border Gateway Protocol
BGPsec	BGP Security Protocol
ccTLD	country code Top Level Domain
DNI	Decentralized Network Infrastructure
DDoS	Distributed Denial of Service
DLT	Distributed Ledge Technology
DNS	Domain Name System
IP	Internet Protocol
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IMSI	International Mobile Subscriber Identity
ID	Identifier
ISP	Internet Service Provider
IoT	Internet of Thing(s)
MAC	Media Access Control
NGN	Next Generation Network
NIR	National Internet Registry
NIC	Network Information Center

P2P	Peer to Peer
PUF	Physical Unclonable Function
PKI	Public Key Infrastructure
RIR	Regional Internet Registry
RPKI	Resource Public Key Infrastructure
RTR	RPKI to Router
ROA	Route Origin Authorization
RP	Relying Party
SLD	Second Level Domains
TLD	Top Level Domains
QoS	Quality of Service

5 Conventions

In this Recommendation:

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.

6 Introduction of the Decentralized Network Infrastructure Framework

6.1 Vulnerabilities of the current centralized network infrastructures

Any services and applications must rely on the network infrastructure to support fundamental network related abilities such as admission control, resource name resolution and network connectivity, while logic capabilities are executed based on these abilities only. Specifically, the credibility of a network infrastructure relies on its trustworthiness and robustness. According to the pioneer studies of a decentralized Internet infrastructure, most of the current network infrastructure systems built through a centralized structure, have the following vulnerabilities which are naturally embedded in a centralized structure is:

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

Further, 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, such that 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.

Alternatively, a decentralized architecture design of a network infrastructure is able to consolidate system trust and equity, and further facilitate the healthy and long-term sustainable growth of the entire ecosystem. Accordingly, a decentralized network infrastructure is expected to act as a trustworthy framework for the future network infrastructures.

6.2 Value of the decentralized network infrastructures

The Decentralized Network Infrastructure (DNI) framework aims at building a fully decentralized network infrastructure as improvement of the current centralized network infrastructure systems. Overall, DNI is designed to eliminate the fundamental vulnerabilities of a centralized network infrastructure as described in clause 6.

The DNI framework is built based on the distributed ledger technology which intrinsically enables decentralization. Besides, the distributed ledger technology can provide other useful capabilities for a decentralized network infrastructure, such as smart contract, verifiable translations, multiparty consensus, and immutable records.

The distributed ledger technology (DLT) may be permissioned and permissionless, which determines if anyone or only approved people can participate in the ledger system. For DNI, as it is needed to provide network admission control and only the admitted participants can play the role of node in the system, a permissioned distributed ledger is the choice. Other parties which do not have permission to participate, can retrieve information from DNI through the 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, in the DNI framework it is specified a new trust mode which removes the relay on central authorities as trust anchors. Based on this new trust mode, a network resources management scheme is specified to certify the resource ownership which is a basis for other capabilities.

The DNI framework is expected to act as a universal basic service for different kinds of high-level network services and application services without refactoring network entities. Theoretically, the DNI framework enhances the robustness of the Internet infrastructure by addressing the vulnerabilities described in clause 6.

No novel techniques related to Blockchain or DLT per se are required for the DNI framework: the DNI framework uses the capabilities and properties supported by the common Blockchain or DLT.

7 Capability requirements of a decentralized network infrastructure

7.1 Requirements of inter domain connectivity

The connectivity capability of a network is critical because it relates to a fundamental ability of a network. The following provides trustworthiness requirements for inter domain connectivity taking BGP as an example.

The requirements of BGP’s trustworthiness include (but may not be limited to):

- The decentralized network infrastructure framework should supports route validation for the network connectivity such that any intentional attack or unintentional mis-operation can be avoided via distributed trustworthiness.

- Given that the synchronization and update of route information should be compatible with the legacy approach, and that security schemes like BGPsec have been already developed and standardized, the decentralized network infrastructure framework should be compatible with both BGP and BGPsec.

7.2 **Requirements of name mapping management**

The network resource names often need to be mapped to other information, and the devices participating in the communication retrieve this information from the mapping service system. The following provides trustworthiness requirements for name mapping system taking DNS as an example.

A decentralized system is not similar to a distributed one. A distributed system can be centralized, the current DNS system being a typical case. A decentralized network infrastructure is expected to rebuild the trust logic.

The requirements of the DNS's trustworthiness include (but may not be limited to):

- It is required to avoid a single point of failure problem, i.e., the mapping service should run normally even in case of the failure of one or several nodes that providing the mapping service.
- It is required to the owner of a given resource to manipulate the mapping information related to the resource.
- The mapping information stored in the system should be trustable.
- The mapping information queried from the system should be verifiable.
- It should be minimized the mapping query delay, especially for the time-sensitive services.

7.3 **Requirements of admission control and resource ownership management**

There are various types of network resources, such as IP addresses, domain names, and various forms of communication identifiers. The trustworthiness of a network relies also on the trusted ownership of resources. The following provides trustworthiness requirements for resource ownership management taking IP addresses as an example.

The requirements of IP address management's trustworthiness include (but may not be limited to):

- The underlying distributed ledger capability should run in a permissioned mode (motivation for permissioned mode should be given inside these brackets) and admission control for participants should be provided.
- The trustworthiness of resource ownership should be confirmed by a group of parties instead of a single party.
- Trusted confirmation of network resource ownership should at least support IP address (automatic IPv6 address allocation, and IPv4/IPv6 address re-allocation), domain name ownership confirmation.
- It should be provided trusted, tamper-proof recording of network resources ownership information, and other parties should be able to verify the ownership information for a particular network resource based on the recorded information.
- The validity of network resource ownership and mapping should only depend on the network resource owner, instead of any third party.

Potential benefits include address exhaustion prevention, prefix aggregation enforcement, organization-level traceability, and admission control.

8 Framework of Decentralized Network Infrastructure

8.1 Framework overview

The framework of Decentralized Network Infrastructure, from the architectural viewpoint, is composed of four layers, as shown in Figure 8-1.

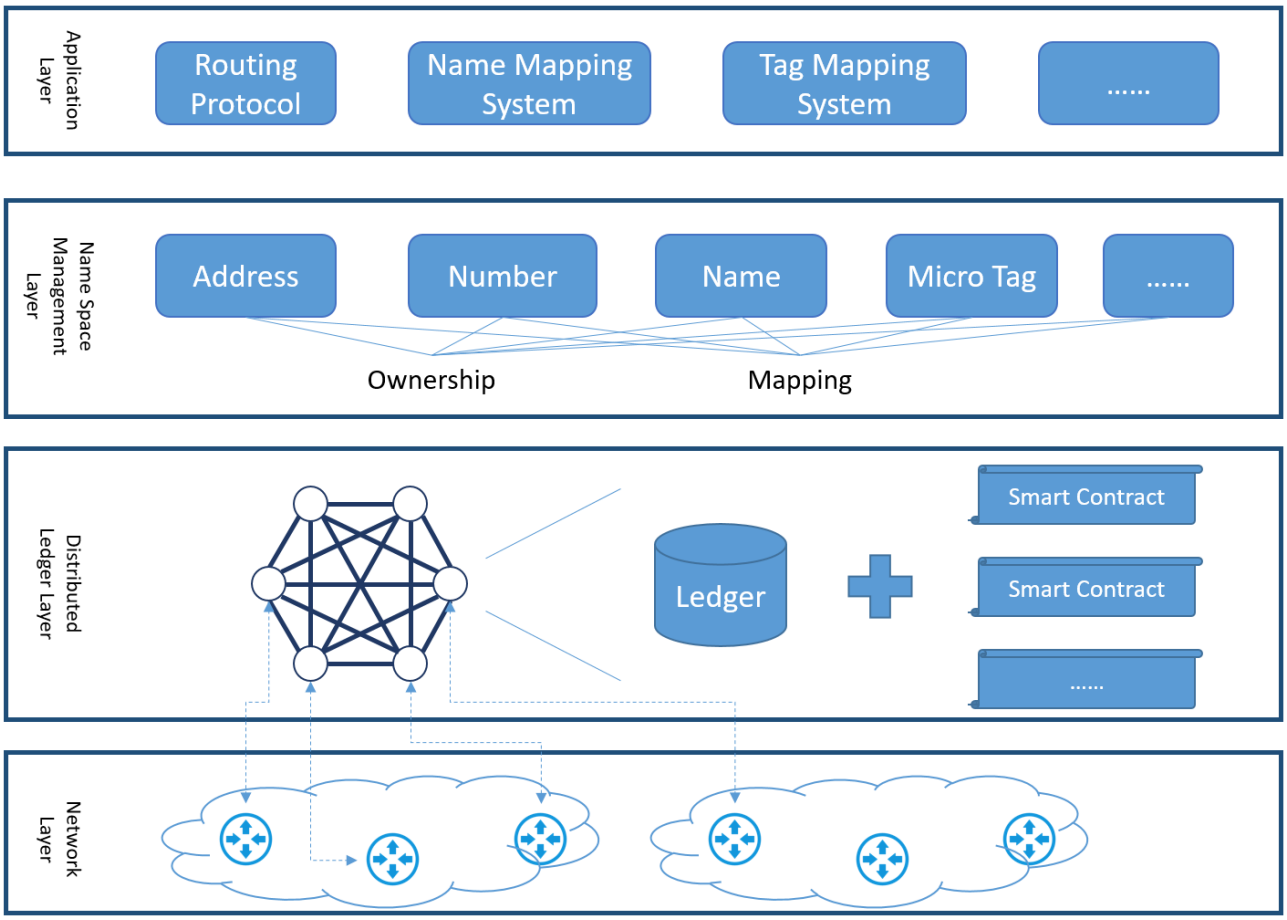

Figure 8-1 Framework of Decentralized Network Infrastructure

1. Network Layer

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

2. Distributed Ledger Layer

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

3. 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.

4. Application Layer

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

The following sub-clauses provide details about the four layers of the framework as well as components and nodes of the Distributed Ledger Layer

8.2 Network Layer

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

8.3 Distributed Ledger Layer

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

1. Providing decentralized system structure
2. Providing distributed consensus mechanism
3. Providing smart contracts capability
4. Guaranteeing trustable trade

The Distributed Ledger Layer operates in the form of a coalition, with each member in the coalition running a server node to communicate with other members' server nodes and finally build up a distributed system. The Distributed Ledger Layer participants are service providers with offline trusted business relationships.

8.4 Name Space Management Layer

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 capabilities in the network, rely on namespaces. BGP maps the IP address prefixes to the Autonomous Systems (AS) number and AS Path to calculate the inter-domain routes in the IP address space. Trusted IP address prefix ownership and mapping are significantly important against 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 identically critical, otherwise loopholes such as domain name cache pollution, DDoS attack on DNS server and domain name hijacking could survive. The Micro Tag indicates the identity for light-weight IoT devices or services, which can provide trusted verification capability. Given that there will be a huge number of light-weight devices connecting to the network in the future, trusted identity will provide a reliable precondition.

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

8.5 Application Layer

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

Below are typical examples of the application that can run on a DNI framework based infrastructure:

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

2. Trusted domain name applications. The trustable binding information on domain name and IP addresses can be used to provide domain name verification services.

3. Identity-related applications for Internet of Things (IoT). The IoT devices' trustable ID information could be maintained in the Name Space Management Layer, and the trustable IDs used for security communications among IoT devices.

8.6 Components of the Distributed Ledger Layer

The Distributed Ledger Layer builds up on various components, as illustrated in Figure 8-2, these components providing the required capabilities for the Name Space Management Layer and the Application Layer.

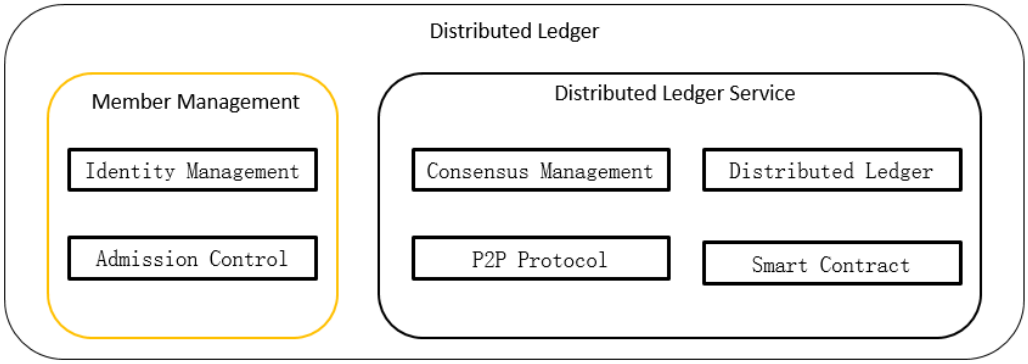

Figure 8-2 Components of the Distributed Ledger Layer

- **Components for Member Management:**
  - Identity Management: an identifier is assigned to each participant node for access to the system and the node is uniquely identified by its identifier in the whole system. The Identity Management component is in charge of managing the identifier of all participant nodes, including Identity assignment, Identity cancellation etc.
  - Admission Control: the Admission Control component is in charge of the admission policy. Only the participant nodes permitted by the admission control policy are 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 the nodes.
  - Distributed Ledger: the Distributed Ledger component is in charge of the storage of the data that passes through the consensus procedures, with the characteristic of irreversibility and incorruptibility.
  - Smart Contract: the Smart Contract component is charge of maintaining and running smart contracts.
  - Peer-to-Peer (P2P) Protocol: the P2P protocol component is in charge of the communications among nodes.

8.7 Nodes of the Distributed Ledger Layer

The roles of the nodes in the system can be sorted into different types. In actual deployments, some of these roles may be implemented in the same node.

Peer Node: The Peer node is the fundamental element of the DNI system. There are multiple Peer nodes connecting to the DNI system. Each player participating in the DNI will runs a Peer node and interacts with the DNI system through the Peer node.

Each Peer node contains the following basic capabilities:

1. Retrieval of information from the Distributed Ledger.
2. Running of Application Layer capabilities.
3. Invocation of smart contracts in the DNI system.

Endorser Node: The Endorser node is in charge of providing endorsement for requests from the Peer node. There are multiple Endorser nodes connecting to the DNI system, each Endorser node providing endorsing service for different Peer nodes.

Each Endorser node contains the following basic capabilities:

1. Validation of the content of requests from Peer nodes.
2. Endorsement for the requests by signing with the Endorser's private key.

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

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

Committer Node: The Committer node is in charge of maintaining the Distributed Ledger records. The interaction process between different roles is illustrated in Figure 8-3.

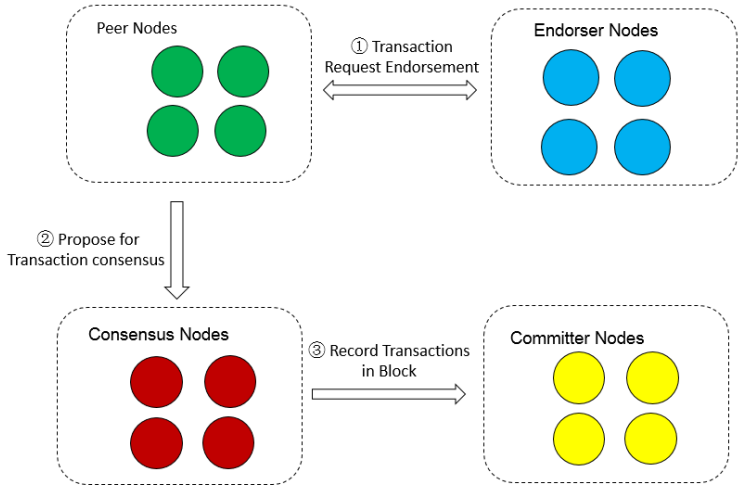

Figure 8-3 Interactions between Roles

In case a Peer node starts 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 performs a Transaction endorsement.

After getting the Transaction endorsement, the Peer node proposes the Transaction to Consensus nodes for consensus. Then the Consensus nodes put a list of Transactions received into a Block orderly, and the Block is recorded by the Committer node.

9 Security considerations

The Decentralized Network Infrastructure framework aims to provide a new trust mode as basic service to other applications, therefore, the security of the DNI framework based infrastructure itself

is critical. This clause provides an analysis of the security issues that a DNI framework based infrastructure can encounter.

Security has to be considered for both the Network Layer and the Distribute Ledger Layer.

9.1 Network Layer security

The Network Layer is responsible for providing secure connection between different ledger nodes. One of the possible attacks at the Network Layer is the Eclipse attack, which is a well-known means of attacking a decentralized network. In the Eclipse attack, the attacker tries to isolate a specific ledger node from other nodes to prevent the synchronization of the states among them. It is possible for attackers to isolate one ledger node from the others, but it is hard to isolate all ledger nodes from each other as this requires the control of the whole network. (In general, the level of difficulty is similar to that for isolating hosts on the Internet from each other.) However, because the Ledger Layer can still work even when some of its nodes are isolated, the Eclipse attack can be considered a non-serious issue in a DNI framework based infrastructure.

9.2 Distributed Ledger Layer Security

The Distributed Ledger Layer security can be guaranteed by the distributed ledger technology itself because this technology enables a Byzantine Fault Tolerance system, so it can cope with byzantine fault nodes which could act arbitrarily. For a DNI framework based infrastructure, the security properties provided by the distributed ledger technology are sufficient.

One essential aspect to be considered is the information privacy. Even though a DNI framework based infrastructure builds on a permissioned ledger system, the information recorded in the ledger is of open access for different kinds of services, so the information privacy needs to be addressed.

Appendix I. Use Cases and Workflows of Decentralized Network Infrastructure

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

1. IP and ASN Ownership Management

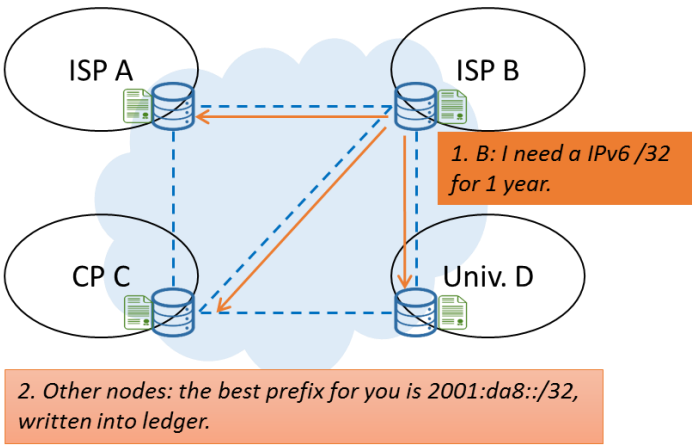

Figure I.1 - General Overview of IP and ASN ownership management

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.

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

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

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.

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.

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 Next Generation Network (NGN) 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.

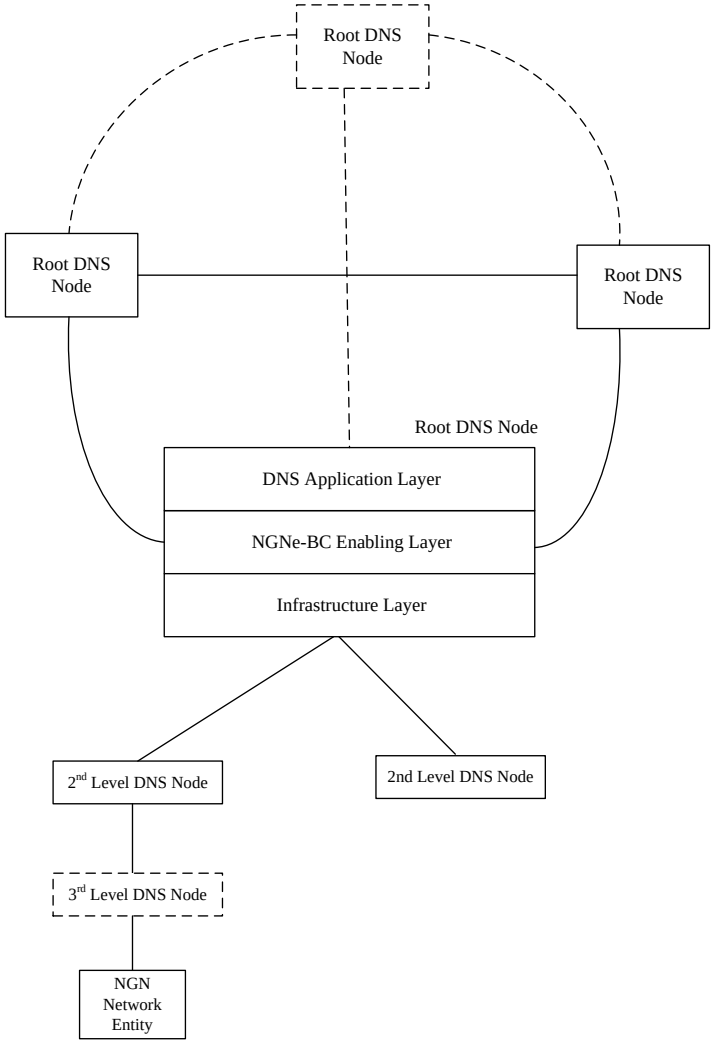

Figure I.2 - High-Level Framework of Decentralized Root DNS

4. 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.

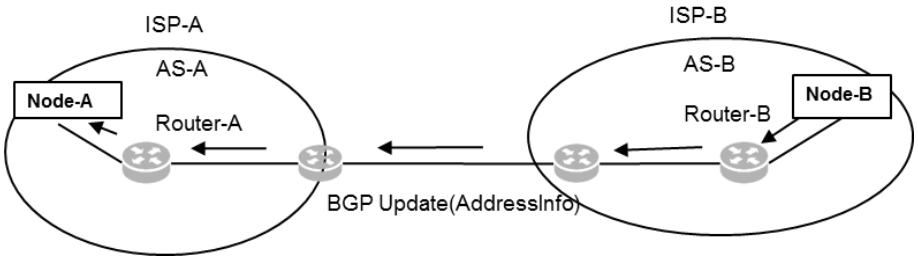

Figure I.3 - Address Information Exchange between ASes

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 (Resource Public Key Infrastructure to Router) or new-defined interface. The AddressInfo can be the nodeID, IP address or Media Access Control (MAC) address of the Node.

5. BGP Security based on DNI

BGP is a standardized exterior gateway protocol designed to exchange routing and reachability information among ASes 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
1.1.1.0/24	ISP1	19/10

3. ROA (IP->ASN)

IP	Maxlength	ASN
1.1.1.0/24	32	100

2. ASN Ownership

ASN	Owner	Exp date
100	ISP1	19/10

4. AS Neighbor Relationship (ASN->ASN)

Source	Target	Type
AS1	AS2	P2C
AS2	AS3	P2P

Figure I.4 - Ownership and Relationship Storage

The routers running BGP protocol are connected to DNI system and retrieve the recorded information from DNI system to verify the contents of consequential 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 is considered to be offensive and dropped instantly.

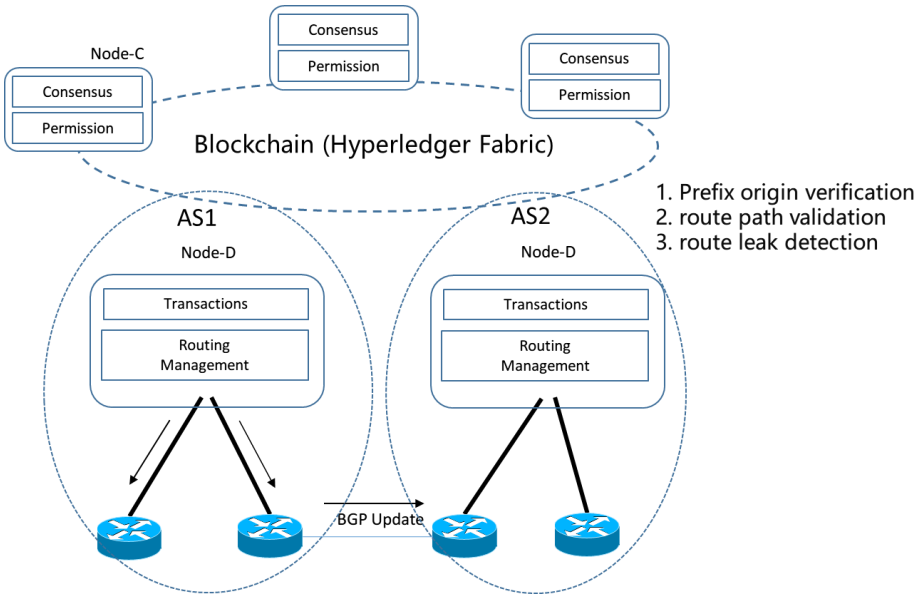

Figure I.5 - A Hyperledger Fabric based Path Verification System Framework

6. IoT Micro Tag Management

The IoT Micro Tag is used for the identification of objects at the network layer. By using a unique physical code, the digitization of objects and the communication and interaction between objects can be achieved. Malicious terminals can attack the network by forging object identifiers, so the

management of the identifiers is critical to the security of IoT. The Distributed Ledger Layer participators are ISPs and large-scale terminal suppliers. The verification of Micro Tag can be realized by running a smart contract, which can effectively intercept illegal terminals in non-administrative domains from entering the network. Security verification across management domains can be solved based on the DNI distributed architecture proposed above.

Specifically, the information required to deal with IoT security issues needs to be recorded in the distributed ledger. The information to be recorded includes: IPv6 Prefix, IMSI, Encrypted PUF Value, and the mapping between IPv6 prefix to PUF Value.

The terminals with Micro Tag are connected to DNI system, and DNI system retrieves the recorded information when receiving the terminal log in message to verify the credibility of the terminal. If the verification result is valid, the terminal is allowed to log into the network, otherwise the terminal's request for network access will be considered invalid and thus rejected.

Bibliography

[b-ITU-T FG-DLT-D1.1] Technical Specification FG DLT D1.1, *Distributed ledger technology terms and definitions.*

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

[b-ITU-T Y.2701] Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1.*

[b-ITU-T Y.2012] Recommendation ITU-T Y.2012 (2010), *Functional Requirements and Architecture of the NGN.*

[b-ITU-T Y.2340] Recommendation ITU-T Y.2340 (2016), *Next Generation Network Evolution Phase 1 – Overview.*

[b-X.1255] Recommendation ITU-T X.1255:2009, *Framework for discovery of identity management information.*

[b-Heilman] Heilman E, Cooper D, Reyzin L, et al. From the Consent of the Routed: Improving the Transparency of the RPKI//Proceedings of the 2014 ACM conference on SIGCOMM. 2014: 51-62.

[b-Saad] Saad M, Anwar A, Ahmad A, et al. *RouteChain: Towards blockchain-based secure and efficient BGP routing*//2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). IEEE, 2019: 210-218.

[b-Chen] Chen D, Ba Y, Qiu H, et al. ISRchain: Achieving efficient interdomain secure routing with blockchain. Computers & Electrical Engineering, 2020, 83: 106584.

[b-Xing] Xing Q, Wang B, Wang X. BGPcoin: Blockchain-Based Internet Number Resource Authority and BGP Security Solution. Symmetry. 2018, 10(9):408

[b-Sfirakis] Sfirakis I, Kotronis V. Validating IP prefixes and AS-paths with blockchains[J]. arXiv preprint arXiv:1906.03172, 2019.

[b-Eclipse] Heilman E, Kendler A, Zohar A, et al. Eclipse attacks on bitcoin's peer-to-peer network//24th USENIX Security Symposium. 2015: 129-144.

_____