ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

ITU-T Y.4492 (11/2023)

SERIES Y: Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities

Internet of things and smart cities and communities – Frameworks, architectures and protocols

Decentralized Internet of things communication architecture based on information-centric networking and blockchain

ITU-T Y-SERIES RECOMMENDATIONS

Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of things and smart cities

GLOBAL INFORMATION INFRASTRUCTURE	Y.100-Y.999
INTERNET PROTOCOL ASPECTS	Y.1000-Y.1999
NEXT GENERATION NETWORKS	Y.2000-Y.2999
FUTURE NETWORKS	Y.3000-Y.3499
CLOUD COMPUTING	Y.3500-Y.3599
BIG DATA	Y.3600-Y.3799
QUANTUM KEY DISTRIBUTION NETWORKS	Y.3800-Y.3999
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	Y.4000-Y.4999
General	Y.4000-Y.4049
Definitions and terminologies	Y.4050-Y.4099
Requirements and use cases	Y.4100-Y.4249
Infrastructure, connectivity and networks	Y.4250-Y.4399
Frameworks, architectures and protocols	**Y.4400-Y.4549**
Services, applications, computation and data processing	Y.4550-Y.4699
Management, control and performance	Y.4700-Y.4799
Identification and security	Y.4800-Y.4899
Evaluation and assessment	Y.4900-Y.4999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Y.4492

Decentralized Internet of things communication architecture based on information-centric networking and blockchain

Summary

Recommendation ITU-T Y.4492 gives an overview of decentralized Internet of things (IoT) communication and its requirements. Recommendation ITU-T Y.4492 also includes the functional architecture of decentralized IoT communication based on information-centric networking (ICN) and blockchain, and an implementation view of decentralized IoT communication architecture based on ICN and blockchain.

History *

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T Y.4492	2023-11-29	20	11.1002/1000/15686

Keywords

Blockchain, information-centric networking, Internet of things, named data object.

* To access the Recommendation, type the URL https://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Y.4492

Decentralized Internet of things communication architecture based on information-centric networking and blockchain

1 Scope

This Recommendation describes a decentralized, Internet of things (IoT) communication reference architecture based on information-centric networking (ICN) and blockchain.

This Recommendation includes:

– an overview of decentralized IoT communication;

– decentralized IoT communication requirements;

– a functional architecture of decentralized IoT communication based on ICN and blockchain;

– an implementation view of decentralized IoT communication architecture based on ICN and blockchain.

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.2760] Recommendation ITU-T Y.2760 (2011), *Mobility security framework in NGN*.

[ITU-T Y.3033] Recommendation ITU-T Y.3033 (2014), *Framework of data aware networking for future networks*.

[ITU-T Y.3071] Recommendation ITU-T Y.3071 (2017), *Data aware networking (information centric networking) – Requirements and capabilities*.

[ITU-T Y.4000] Recommendation ITU-T Y.4000/Y.2060 (2012), *Overview of the Internet of things*.

[ITU-T Y.4401] Recommendation ITU-T Y.4401/Y.2068 (2015), *Functional framework and capabilities of the Internet of things*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 blockchain [b-ITU-T Y.2342]: 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.

3.1.2 DAN element [ITU-T Y.3071]: A network component that forwards messages to producers, consumers, and other data aware networking (DAN) elements.

3.1.3 data name [ITU-T Y.3071]: A string of alpha-numeric characters that is used to identify the data object. A data name, which may have variable length, is usually configured in such a way that it would be easier to be read and remembered by humans.

NOTE – In this Recommendation, the terms "data name" and "NDO name" are used interchangeably.

3.1.4 device [b-ITU-T Y.4000]: With regard to the Internet of Things, this is a piece of equipment with the mandatory capabilities of communication and optional capabilities of sensing, actuation, data capture, data storage and data processing.

3.1.5 information-centric networking (ICN) [b-ITU-T Y.3075]: A new approach to networking where named objects (not only devices) are the principal components of the network. Named data objects can be stored in network nodes (with caching capability) distributed throughout the network. Data objects are transmitted by using names to requesting consumers from any network node that can provide requested data. Locations of the nodes that store data objects in their caches are irrelevant to consumers because they send their requests for data objects using names (not the data object locations).

3.1.6 Internet of things (IoT) [ITU-T Y.4000]: A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving, interoperable information and communication technologies.

3.1.7 named data object (NDO) [ITU-T Y.3071]: A data object that is identifiable by a name.

3.1.8 NDO consumer [ITU-T Y.3071]: A component that makes requests on named data objects (NDOs).

3.1.9 NDO producer [ITU-T Y.3071]: A component holding named data objects (NDOs) and make them reachable by corresponding requests. An NDO producer may be an actual owner of the NDO or a delegate of the actual owner.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

DAN Data Aware Networking

ICN Information-Centric Networking

IoT Internet of Things

NDO Named Data Object

5 Conventions

None.

6 Overview of the decentralized IoT communication

Decentralized IoT communication capabilities cover the whole network layer in the IoT reference model specified in [ITU-T Y.4000] (see the box with the dashed border in Figure 1). Such capabilities can enhance those of the current IoT network layer, based on ICN and blockchain functional architecture, including decentralized management capability, data communication security, and IoT device and application creditability.

To the upper layers, this service can provide all communication capabilities specified in [ITU-T Y.4401] in a decentralized, unsafe and untrusted network environment, and support on the

IoT direct communication between devices and applications that belong to different domains with sliced communication mode.

To the bottom layer, this service can support IoT device and gateway trusted access capabilities, although these terminal devices belong to different IoT domains.

The left management capabilities can manage all entities that make up this service.

IoT-specific data security capabilities are realized in this service, and network security still belongs to the right security capabilities.

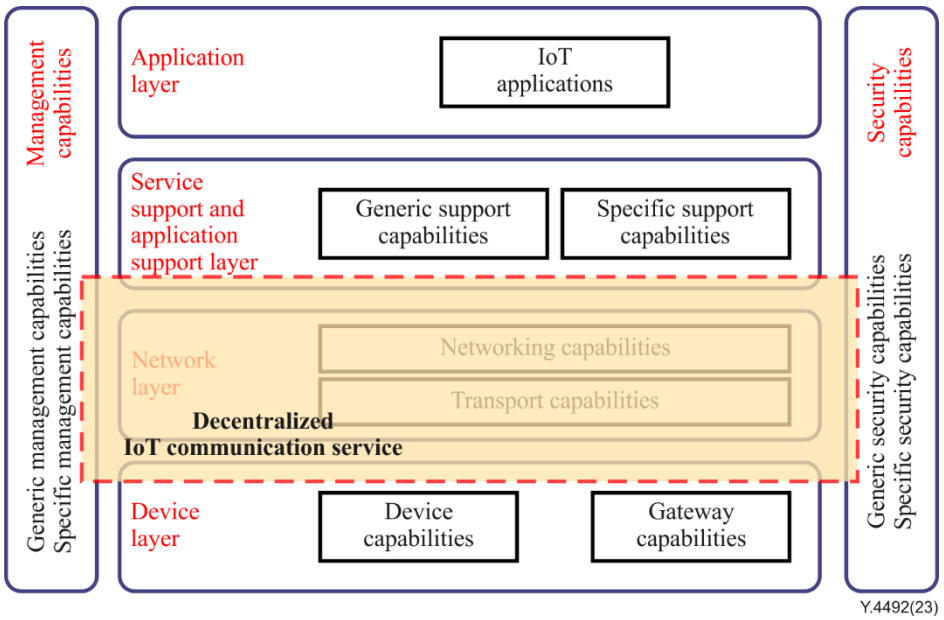

Figure 1 – Decentralized IoT communication capabilities mapping

7 Decentralized IoT communication requirements

Decentralized IoT communication needs to meet the following requirements.

– Establishment of communication access channels on the IoT between devices and applications to ensure data transfer capability. Support for IoT terminal access and collaboration, IoT application business packaging and interface provision.

– ICN technology is introduced to realize the subscription and distribution communication mode. Content and location separation, network cache, and other technologies improve the content distribution rate, data-sharing efficiency and better network traffic load balancing of large-scale mobile networks.

– Blockchain technology is introduced to provide a data naming and key distribution mechanism for IoT devices and applications. It provides trusted support for content-name-driven routing and forwarding.

8 Functional architecture of decentralized IoT communication based on ICN and blockchain

Decentralized IoT communication functional architecture describes communication capabilities at the functional level to guarantee that it can fulfil all communication requirements specified in clause 6. The functional architecture consists of groups of IoT communication capabilities and their relationships.

8.1 Functional architecture

This functional architecture comprises four layers: blockchain-based service; ICN; IoT device; and IoT application. See Figure 2.

– Blockchain-based service layer: This layer includes a naming and key distribution service. The naming service stores the global unique name in the blockchain based on the blockchain, and the key distribution service manages the public key in the system. Among them, the blockchain node publishes the NDO or public key as the "transaction" content to the blockchain network. The blockchain nodes store the identity and NDO name of the IoT data transmitted in the ICN layer and the registered IoT devices and application public keys. The blockchain nodes provide naming and key distribution services to the ICN, IoT device, and IoT application layers. The transaction stored on the blockchain layer is synchronized through a consensus mechanism between the blockchain nodes.

– ICN layer: This layer uses a data-naming addressing mode instead of IP addressing mode to provide real-time data transmission capability. The ICN layer provides IoT data packet addressing and forwarding capability between ICN nodes. The ICN nodes can also cache transmitted IoT data to improve the efficiency of nearby access.

– IoT device layer: IoT devices act as data providers. IoT devices can publish IoT data with a registered NDO name. IoT devices use the public key distribution service of the blockchain-based service layer to share data. The IoT device signs the data with its private key and encrypts it with the public key of the data requesters.

– IoT application layer: IoT applications act as data requesters. IoT applications can obtain IoT data with a registered NDO name. The IoT application verifies the data signature with the public key of data providers and uses the private key to decrypt the data.

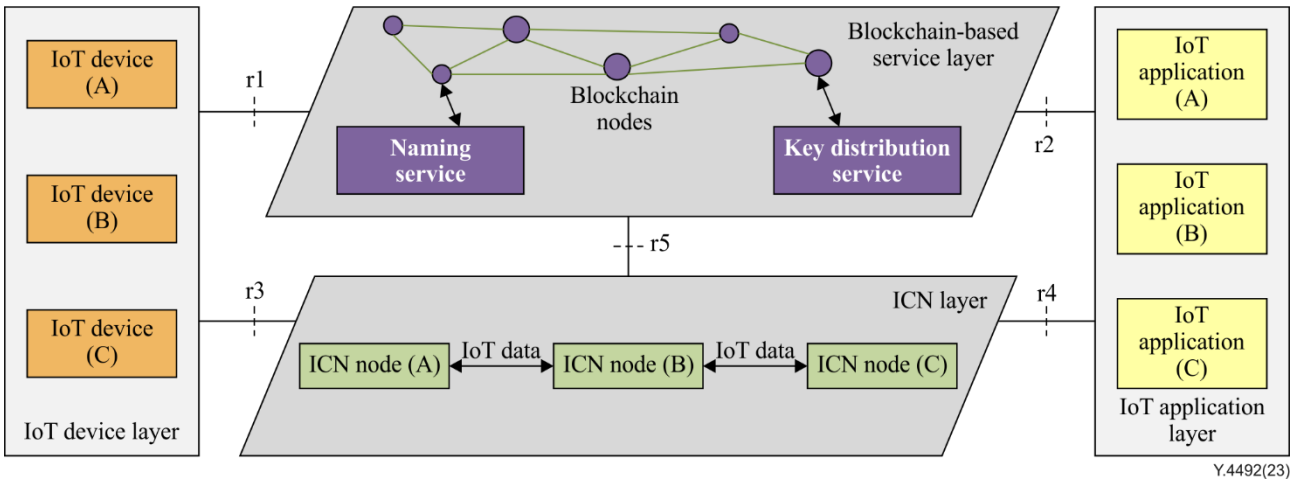

Figure 2 – Architecture in functional view

8.2 Blockchain-based service layer

– Naming service: A data provider registers a data name for the NDO to be shared through the naming service. The data name contains a prefix and a suffix. For unique identification, the prefix is used for the data provider and the suffix for the corresponding IoT data. The data name is bound to the IoT application resource, and the data user accesses shared data through the data name.

– Key distribution service: The data requester obtains the public key from the blockchain. The public key encrypts and verifies the data to make it tamper-proof when transmitted over the network. The data provider signs the IoT data using the private key and encrypts the packet with the public key of the ICN node or data requester. When acquiring the data, the ICN node

or data requester decrypts it with its private key and verifies it with the public key of the data provider.

8.3 ICN layer

– ICN layer functions are specified in [ITU-T Y.3033] and [ITU-T Y.3071]. The ICN layer consists of DAN elements that provide name-based communication capabilities.

8.4 IoT device layer

An IoT device layer consists of IoT devices. IoT devices act as data providers. Data providers share data resources through shared data publishing.

– The data provider obtains the data identification through the naming service.

– Sending data identification and address information to the naming service.

– Naming service binds the data identifier to the address information and forms a mapping relationship.

– When an interest packet arrives, it is forwarded to the corresponding resource access point for data access in accordance with the mapping relationship.

8.5 IoT application layer

An IoT application layer consists of IoT applications. IoT applications act as data requesters. Data requesters can access the data they need through a shared data subscription.

– When requesting data, a data requester subscribes to the data of interest based on the data identifier. The address of the corresponding resource access point can be obtained using identity resolution, and the data resource corresponding to the data identity can be obtained.

8.6 Reference points

Figure 2 shows reference points between entities in different layers. To distinguish these reference points in this Recommendation, which can establish the relationship among functional components, they are numbered as r1, r2, r3 r4 and r5 respectively.

– Reference point r1 is between IoT devices and blockchain nodes. Through this reference point, IoT devices can register their NDO name on blockchain nodes and obtain the public key from the blockchain layer to encrypt the data.

– Reference point r2 is between IoT applications and blockchain nodes. Through this reference point, IoT applications can obtain the NDO name of IoT devices and obtain the public key from the blockchain layer to verify the data packet.

– Reference point r3 is between IoT devices and ICN nodes. Through this reference point, IoT devices can publish IoT data with the registered the NDO name to ICN nodes.

– Reference point r4 is between IoT applications and ICN nodes. Through this reference point, IoT applications can request IoT data with the NDO name from ICN nodes.

– Reference point r5 is between blockchain nodes and ICN nodes. Through this reference point, ICN nodes can resolve the address of IoT data with the NDO name from the blockchain layer. Moreover, the ICN node can obtain the public key from the blockchain layer to verify the data packet.

Appendix I

Decentralized IoT communication architecture in implementation view

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

An implementation view of the decentralized IoT communication architecture consists of functional entities and their high-level relations. This communication architecture in the implementation view comprises three domains related to: blockchain-based service; ICN network; and IoT communication. The IoT communication domain includes IoT device domain and IoT application domain.

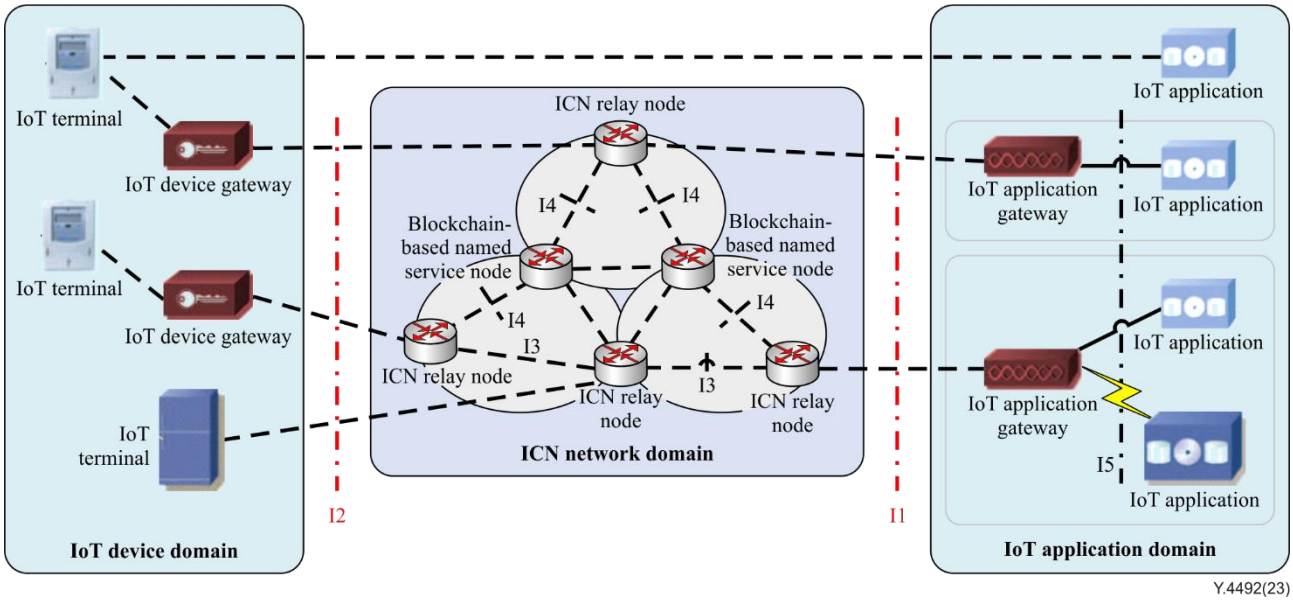

Figure I.1 – Architecture in implementation view

– Blockchain-based service domain: Blockchain nodes in this domain provide secure and trusted naming services and key management for nodes in the IoT communication domain and ICN network domain. Blockchain can provide name registration, publishing and management services for IoT devices, applications and ICN nodes.

– ICN network domain: IoT data is transferred by an ICN-bearing network in this domain. ICN aggregates interest packages through a pending interest table in a DAN element to save network traffic. The data package path is the opposite of the interest package path. The return path can be cached according to the caching policy so that other IoT applications can request consumption. ICN allows users to float a data request without knowledge about the hosting entity. ICN can handle user mobility and security issues more efficiently than the current Internet.

– IoT communication domain: In this domain, an IoT application and IoT device share IoT data sliced, reliably and transparently. The IoT device uses its private key to sign the data to ensure the trustworthiness of the data source. Then it encrypts the data with the public key of the authorized IoT application party. This guarantees that an authorized IoT application party can obtain data content, and also ensures data safety. If the IoT device data is to be shared by multiple authorized IoT applications, it can be encrypted by the public keys of the authorized IoT applications separately. The encrypted data is distributed to ICN network separately. This could achieve data security sharing among multiple authorized data-sharing applications.

Appendix II

Decentralized IoT communication architecture data transmission process

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

II.1 Name registration process

NOTE – There is no requirement for NDO nomenclature in this Recommendation, and the format can refer to post-processing kinematics.

A naming registration service can be secure and reliable for distributed IoT communication architecture. Names need to be registered before they can be used across the ICN network. An NDO registry implements a globally unique name so that NDO consumers can use the name or identity to access data resources corresponding to the NDO. The implementation process is shown in Figure II.1, including the following steps.

Step 1: Register the data resource name. The NDO producer sends the newly generated resource name to the name registration service of the blockchain-based service layer.

Step 2: New block is confirmed. The registration data is packaged as a blockchain transaction into a new block and accessed into the blockchain.

Step 3: Blockchain synchronization. Blockchain agrees on block registration information through a consensus protocol, which enables global uniformity in the NDO name. Registration information is synchronized in the blockchain ledger.

Step 4: Obtain relevant attributes. The name registration organization obtains registration information from the blockchain and constructs the corresponding NDO name for the NDO producer according to the NDO naming rules.

Step 5: Return successful registration. The NDO name is passed back to the NDO producer, who forms a named data resource based on the NDO name.

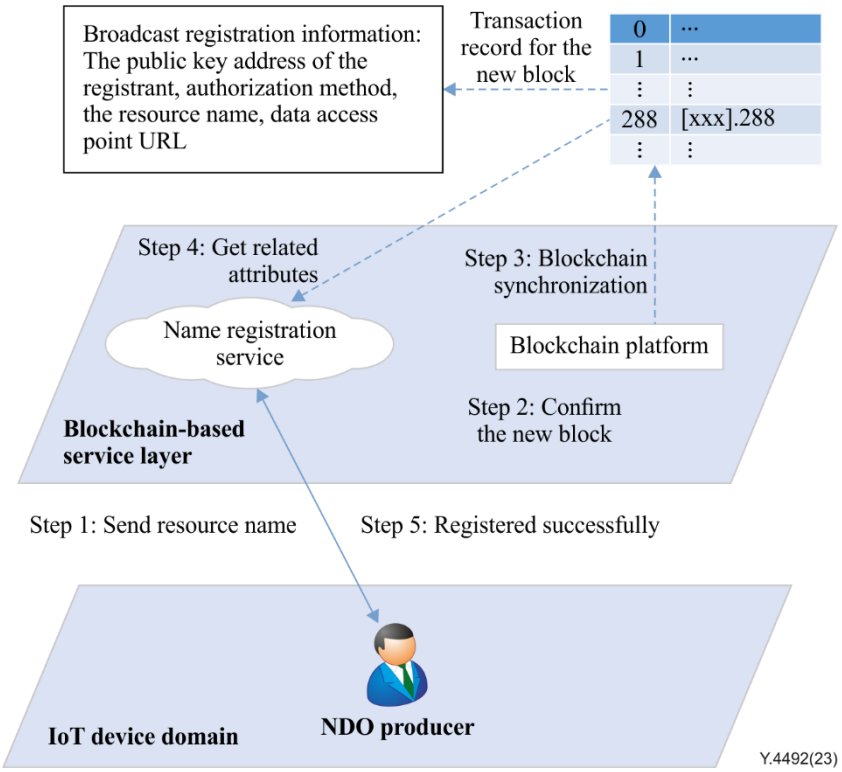

Figure II.1 – NDO name registration process

II.2 NDO name publishing process

The blockchain will publish the registered NDO, which will be run once during system initialization and when the NDO name is updated. The main process steps are as follows.

Step 1: NDO publishing service sends the NDO name registration information to the IoT device.

Step 2: The IoT device sends the NDO name registry information to the nearest ICN relay node, indicating that the corresponding NDO can be subscribed to through the name registry.

Step 3: The ICN relay node fills in the forwarding information base in the DAN element information according to the NDO name and floods the entry to the neighbour, so that when the interest package arrives, it can be forwarded to the corresponding resource access point according to the forwarding information base in the DAN element for data access.

II.3 Public key encryption process

[ITU-T Y.2760] describes the mobile security architecture of next-generation networks such as ICN, including authentication and key management. Data is transmitted at the ICN layer as encrypted data, which is encrypted and signed by the NDO producer before publication. After receiving the data, the NDO consumer must verify the data signature to ensure that the data is from a reliable source and has not been tampered with. The key distribution service generates the encryption and decryption process key during the generation of NDO.

II.4 NDO communication process

See Figure II.2.

II.4.1 Data request

Step 1: The NDO consumer requests the corresponding NDO through the NDO name. First, it looks for the local cache, and if there is one, it directly returns the content to the browser for display. Otherwise, it generates an interest package and sends it to the ICN relay node.

Step 2: After receiving the interest package, the ICN relay node parses the message according to the protocol requirements and looks for a content store in the DAN element named according to NDO. If the match is successful, the data return module is called for data return. If the match fails, match the pending interest table in the DAN element information.

Step 3: Determine whether the pending interest table in the DAN element has a matching NDO name. If the same interest packet is found to have been forwarded in ICN relay mode, the inbound interface of the interest packet is added to the existing pending interest table in the DAN element. If not, the entry is populated.

Step 4: Find the forwarding information base in the DAN element for the routing address. If there is a corresponding entry in the forwarding information base in the DAN element, forward it according to the corresponding interface, and create an information entry into the interface in the pending interest table in the DAN element for data transmission back. Discard the interest package if it is not found.

II.4.2 Data response

Step 1: Call the return module. When the interest package reaches the NDO producer or the ICN relay node that satisfies the content cache, the data content is found, or the matching content store in the DAN element is returned. When transmitting back, the encryption and decryption module of the system should be called for encryption and signature to ensure the confidentiality and integrity of the data. Then the data package return module of the system needs to be called to return the content according to the transmission path of the interest package.

Step 2: Find the content store in the DAN element information. In the return process, the data package is first matched with the longest prefix and the content store in DAN element entries is found. If there is the same cache data, the data package is repeated and discarded. If not, the pending interest table in the DAN element is queried.

Step 3: Find the pending interest table in the DAN element information and determine whether there is an interest package for this data. If there is, the data is cached locally, and the data validation module is called for the data package that needs to be cached. Considering the complexity of digital signature verification, packet validation in the relay node is optional. Most strategies should be sample validation. Then, data content is returned according to the interest package's source interface to realize efficient data distribution. If there is no matching entry in the pending interest table in the DAN element, the data package is discarded. The routing path of the data package is the opposite of that of the interest package. During this process, if one of the intermediate nodes has problems processing the packet, the abnormal interest feedback package is returned directly to report the error.

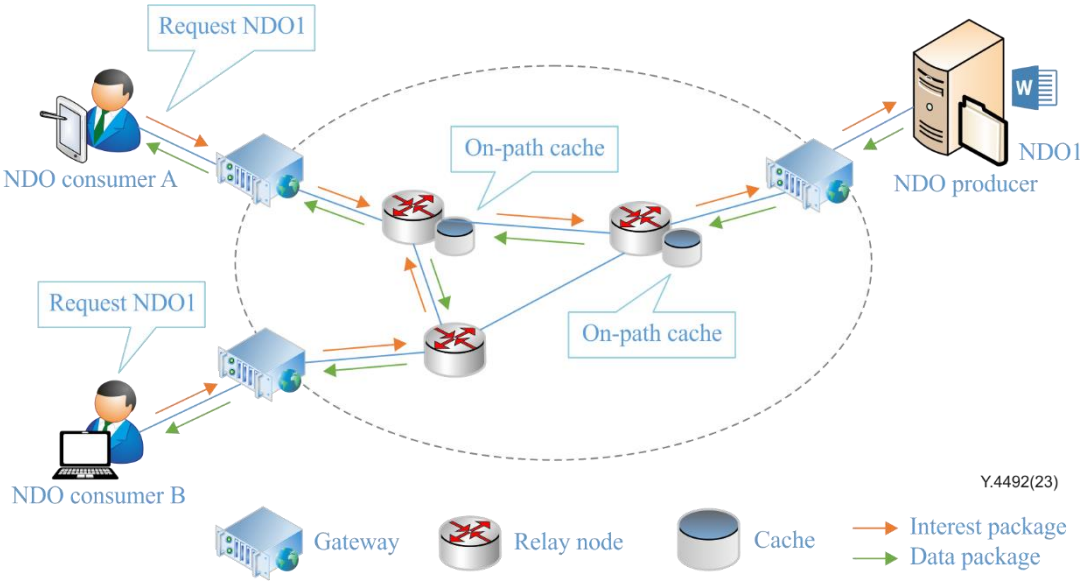

Figure II.2 – NDO communication process

Bibliography

[b-ITU-T Y.2342] Recommendation ITU-T Y.2342 (2019), *Scenarios and capability requirements of blockchain in next generation network evolution*.

[b-ITU-T Y.3075] Recommendation ITU-T Y.3075 (2020), *Requirements and capabilities of information-centric networking routing and forwarding based on control and user plane separation in IMT-2020*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities**
Series Z	Languages and general software aspects for telecommunication systems

Published in Switzerland
Geneva, 2024