ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

ITU-T Y.4491 (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

Framework of blockchain-based self-organization networking in Internet of things environments

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.4491

Framework of blockchain-based self-organization networking in Internet of things environments

Summary

Self-organization networking (SON) is responsible for automatically planning, configuring, managing, optimizing and remedying networking. When building SON in an Internet of things (IoT) environment, an IoT device moves frequently and IoT service requirements change from time to time. In such an environment, it is difficult to manage IoT services and devices in a centralized manner. Blockchain supports dynamic trusted SON management and secure network resource sharing by using smart contract and consensus protocols.

Recommendation ITU-T Y.4491 describes a framework for the support of SON in an IoT environment using blockchain.

History *

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T Y.4491	2023-11-29	20	11.1002/1000/15685

Keywords

Blockchain, blockchain-based self-organization networking, Internet of Things (IoT), self-organization networking.

* 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.4491

Framework of blockchain-based self-organization networking in Internet of things environments

1 Scope

This Recommendation describes a framework of blockchain-based self-organization networking (SON) in an IoT environment. In particular, the Recommendation includes:

– An introduction to blockchain-based SON;

– Requirements for SON using blockchain;

– Architecture of blockchain-based SON in an IoT environment.

Use cases of blockchain-based SON are provided in Appendix I.

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.3530] Recommendation ITU-T Y.3530 (2020), *Cloud computing – functional requirements for blockchain as a service*.

[ITU-T Y.4417] Recommendation ITU-T Y.4417 (2018), *Framework of self-organization network in Internet of things environments*.

[ITU-T Y.4560] Recommendation ITU-T Y.4560 (2023), *Blockchain-based data exchange and sharing for supporting Internet of things and smart cities and communities*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 blockchain [b-ITU-T Y.Suppl.62]: A peer to peer distributed ledger based on a group of technologies for a new generation of transactional applications which may maintain a continuously growing list of cryptographically secured data records hardened against tampering and revision.

NOTE 1 – Blockchains can help establish trust, accountability and transparency while streamlining business processes.

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

3.1.2 blockchain data [b-ITU-T Y.Suppl.62]: The data in a blockchain, such as distributed append-only ledgers, state information, permission policies etc.

NOTE – Blockchain data may be distributed and be stored in blockchain peers. A blockchain peer may store whole or part of the data in a blockchain.

3.1.3 blockchain network [ITU-T Y.3530]: A network to implement a blockchain platform among nodes.

3.1.4 blockchain platform [ITU-T Y.3530]: Implementation of blockchain to process data in a node.

3.1.5 consensus [b-ITU-T Y.Suppl.62]: Agreements to confirm the correctness of the blockchain transaction.

3.1.6 constrained device [b-ITU-T Y.4451]: A device that has constraints on characteristics such as limited processing capability, small memory capability, limited battery power, short range and low bit rate.

3.1.7 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 the optional capabilities of sensing, actuation, data capture, data storage and data processing.

3.1.8 distributed ledger [ITU-T Y.3530]: A type of ledger that is shared, replicated, and synchronized in a distributed and decentralized manner.

3.1.9 infrastructure [b-ITU-T Y.4407]: The basic facilities and systems comprised of network nodes (i.e., switches and/or routers) and the means to connect them (i.e., wired (cable or fibre) or wireless) for the purpose of communication between two end-points.

3.1.10 Internet of things (IoT) [b-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.

3.1.11 self-organization networking (SON) [ITU-T Y.4417]: Autonomous networking established by individual devices, where the device can effectively interact with its peers and perform self-control for network organization and for joining networks according to its own status, own services and dynamic network circumstances in a decentralized infrastructure or an "infrastructure-less" network.

3.1.12 smart contract [b-ITU-T Y.Suppl.62]: Embedded logic that encodes the rules for specific types of blockchain transactions. A smart contract can be stored in the blockchain and can be invoked by specific blockchain applications.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

B-SON Blockchain-based Self-Organization Networking

BLE Bluetooth Low Energy

ECDSA Elliptic Curve Digital Signature Algorithm

FE Functional Entity

IoT Internet of Things

IoT-CN Internet of Things Coordinator Node

IoT-DN Internet of Things Device Node

RAT Radio Access Technology

SON Self-Organization Networking

5 Conventions

The following conventions are used 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 document 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 keyword ""**may**" indicate an optional requirement which is permissible, without implying any sense of being recommended. These terms are 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 the specification.

6 Introduction

6.1 Self-organization networking in an IoT environment

[ITU-T Y.4417] describes a framework of self-organization networking (SON) in an IoT network without the help of infrastructure.

NOTE – An infrastructure-unsupported IoT network is independent on pre-existing infrastructure networks. [ITU-T Y.4417] [b-ITU-T Y.4407].

SON in IoT environment refers to autonomic networking functionalities among heterogeneous networked IoT devices [ITU-T Y.4417] [b-ITU-T Y.3680]. SON performs various operations such as neighbour node discovery and routing for network configuration and communication services without relying on infrastructure.

A SON network is intended to be a network that uses self-organization networking capabilities. A SON network supports four autonomic networking functionalities: self-configuration, self-healing, self-optimizing and self-protecting.

Figure 1 shows the basic configuration of a SON network in an IoT environment.

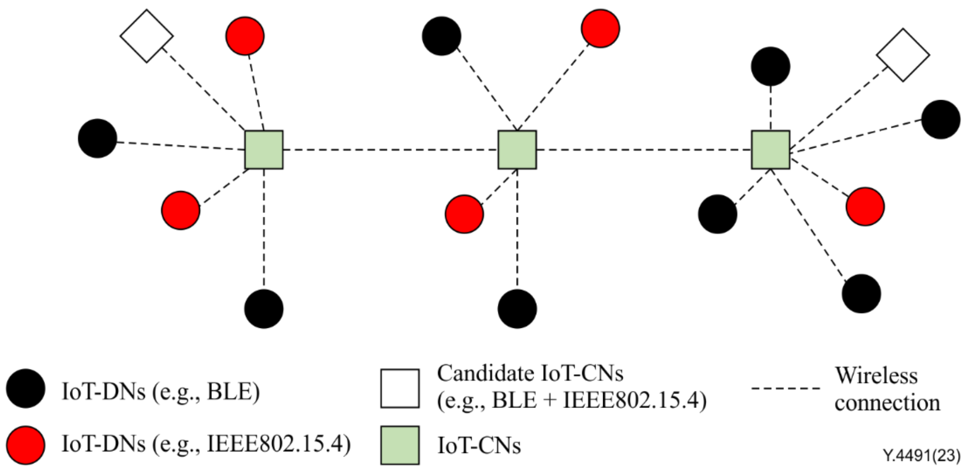

Figure 1 – Basic configuration of a SON network in an IoT environment

A SON network in an IoT environment consists of SON nodes, which are IoT devices with radio interfaces. The IoT devices may have diverse capabilities in terms of processing, memory, battery power, mobility and transmission ranges. An IoT device may use multiple radio access technologies. Some of the IoT devices that support multiple radio access technologies can act as IoT coordinator nodes (IoT-CN), while other IoT devices act as IoT device nodes (IoT-DN). Therefore, a SON network in an IoT environment is logically composed of two types of SON nodes: IoT-DN and IoT-CN.

Figure 2 shows the creation process of two examples of SON networks in an IoT environment according to the radio access technologies of the IoT-DNs participating in the SON network.

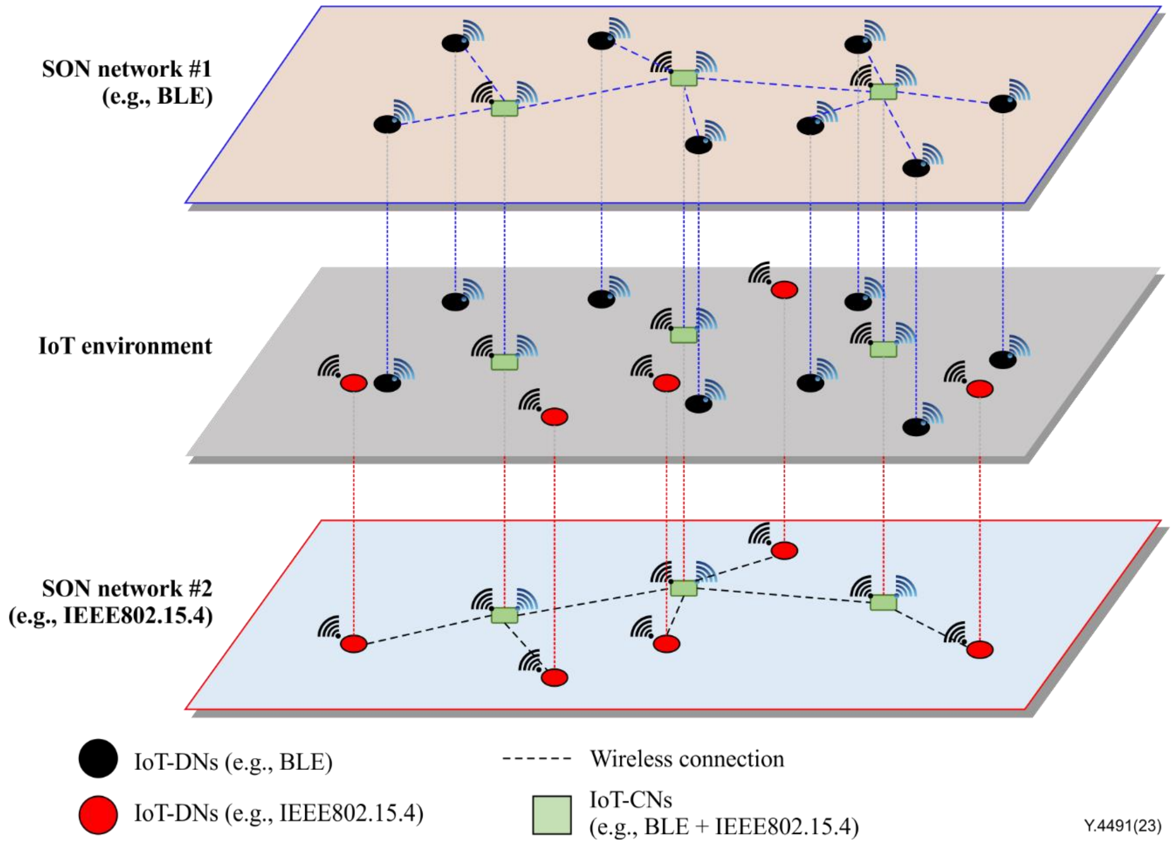

Figure 2 – Examples of SON networks in an IoT environment

In Figure 2, IoT-DNs and IoT-CNs are scattered in the IoT environment area. The IoT-DNs firstly connect to an IoT-CN and the IoT-CN also connects to other IoT-CNs. Then, every IoT-CN builds a routing table for supporting peer-to-peer communications with the other IoT-DNs and, according to the radio access technologies of the IoT-DNs, two SON networks are created simultaneously. The two SON networks use the same radio technology among all their corresponding nodes (i.e., BLE based SON network and IEEE 802.15.4 [b-IEEE 802.15.4-2020] based SON network). All IoT-CNs and IoT-DNs in the same SON network share the same predefined optimization policies to configure the SON network functionalities [ITU-T Y.4417].

6.2 Blockchain-based self-organization networking

Blockchain is a distributed ledger which is characterized by digitally recorded data arranged in a successively growing chain of blocks, with each block being cryptographically linked and hardened against tampering and revision. A blockchain-enabled node creates a block with final and definitive (immutable) records of transactions. The block is also shared, replicated and synchronized among nodes in a distributed and decentralized manner [ITU-T Y.3530].

The blockchain technology provides the following specific benefits: trustworthiness, transparency, highly resistance to outage, tamper-proofness, auditability and self-regulating ability. The blockchain technology can efficiently ensure the integrity, authenticity and auditability of all transactions [ITU-T Y.4560].

Given these abilities, the blockchain technology can hence help make SON configuration data trusted in order to support autonomous networking functions in a SON network. The functions of SON (i.e., self-configuration and self-healing) can operate to recover a connection failure in the SON network, but these functions cannot dynamically and autonomically create the new connections. For the dynamic and automatic recovery of the SON network, the policy information for these functions needs to be maintained. The usage of the blockchain technology [ITU-T Y.3530] is one possible option to maintain policy information.

This Recommendation describes a blockchain-based SON framework, which, among others, allows policy information to be maintained securely.

Figure 3 shows a blockchain-based SON (B-SON) in an IoT environment. B-SON is based on a blockchain network consisting of IoT-CNs and application servers.

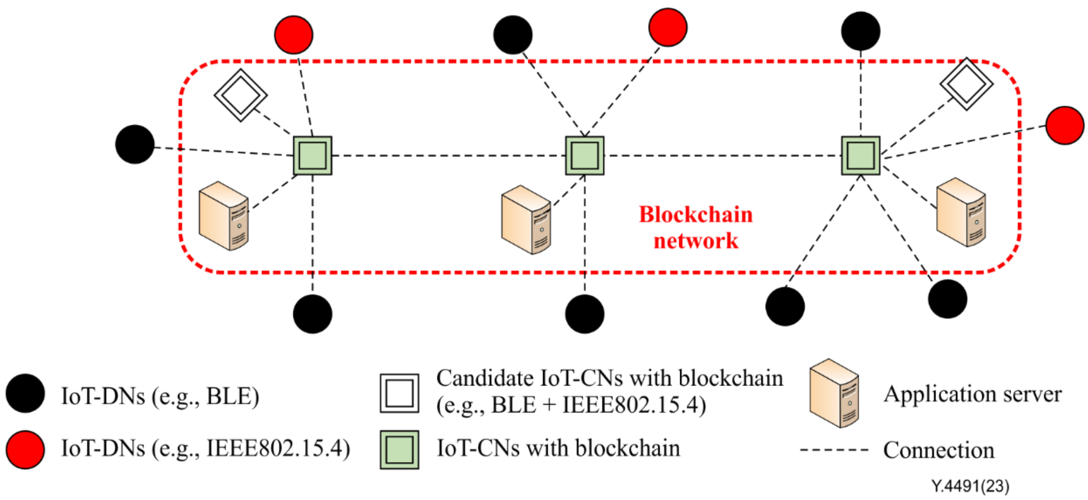

Figure 3 – Blockchain-based self-organization networking in an IoT environment

A B-SON network is intended to be a SON network that uses blockchain-based SON capabilities.

In Figure 3, all IoT-CNs of the B-SON network support blockchain capabilities [ITU-T Y.3530]. Each IoT-CN is usually directly connected to an associated application server. The IoT-CN plays a role in the blockchain network with the help of an application server as it supports part of the blockchain capabilities.

NOTE – The application servers work like a distributed database.

On the other hand, there might be the case that just one of the IoT-CNs is directly connected to an application server. In this case, the remaining IoT-CNs have indirect connection via this application server to the blockchain network.

The following four autonomous networking functions are supported by the B-SON network:

– Self-configuration function: IoT-CNs can configure the network dynamically using smart contracts on blockchain depending on the SON capability of IoT-DNs and IoT-CNs.

– Self-healing function: green-coloured IoT-CNs connect each other with the help of blockchain and an application server. As shown in Figure 2, IoT-DNs are connected to an IoT-CN in a star topology to configure a SON network. If an IoT-CN fails in the SON network, all IoT-DNs associated with the IoT-CN stop working. When an IoT-CNs failure occurs, the candidate IoT-CNs restore network configuration information (e.g., routing table) from an adjacent IoT-CN in order to maintain network connectivity. If all IoT-CNs and candidate IoT-CNs are included in a blockchain network, this configuration information is received via the blockchain network.

– Self-optimizing function: a blockchain network is maintained using consensus mechanisms. The B-SON network maintains the status of IoT-DNs and IoT-CNs, coordinator election rules and smart contracts in the blockchain network.

– Self-protecting function: the blockchain technology supports secure identification management. Authentication, digital signature and consensus mechanisms in blockchain network support non-repudiation and secure join/leave in/from a B-SON network.

Figure 4 shows two types of interworking between the internal blockchain network of a B-SON network and an external blockchain network composed of application servers. The left side of Figure 4 shows a case of IoT-CNs which cannot fully support the blockchain technology because of the lack of hardware capabilities: in this case, the blockchain functionalities are performed with the help of application servers in a separated external blockchain network. The right side of Figure 4 shows the case of IoT-CNs which can support blockchain technologies: in this case, just one of the IoT-CNs connects to an application server of an external blockchain network.

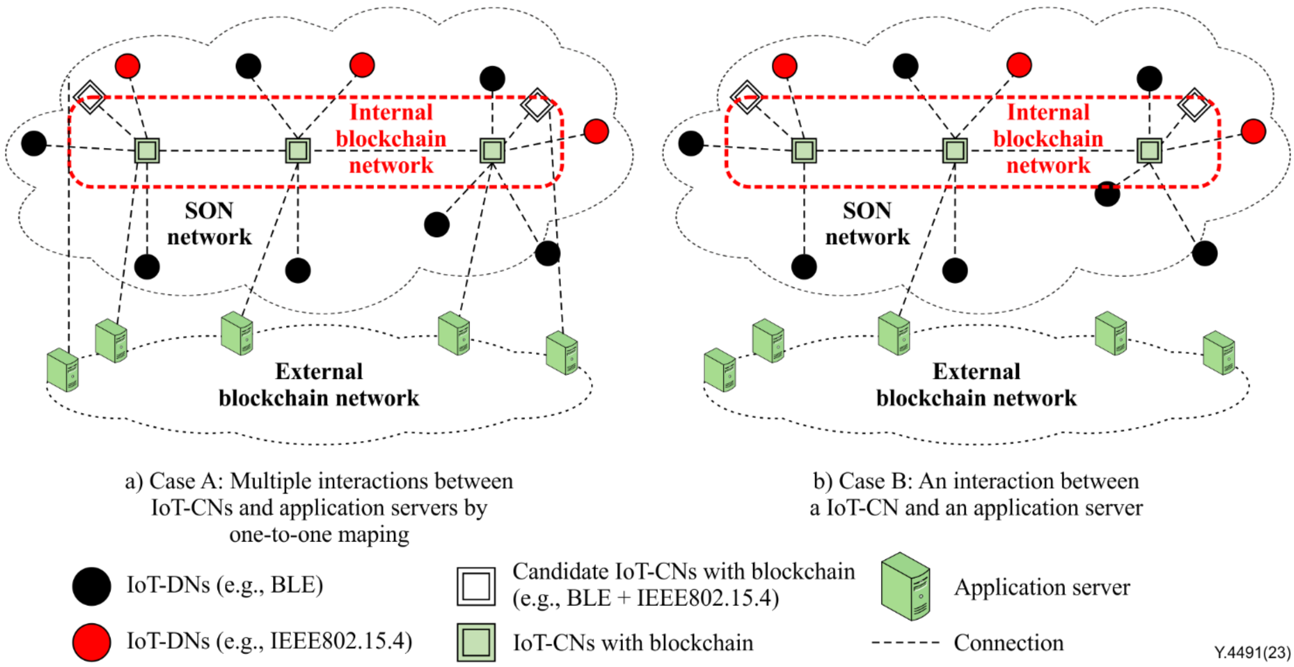

Figure 4 – Types of interworking between the B-SON network and blockchain network

7 Requirements for self-organization networking using blockchain

7.1 General requirements

7.1.1 Support for heterogeneous IoT networks

Heterogeneous IoT networks consist of heterogeneous IoT-CNs and IoT-DNs in terms of different radio access technology.

– B-SON is required to support heterogeneous IoT-CNs and IoT-DNs in an IoT environment.

– B-SON is recommended to build a B-SON network with homogeneous IoT-CNs and IoT-DNs in an IoT environment.

– B-SON is required to manage predefined policy information to operate IoT services [ITU-T Y.4417] in an IoT environment.

NOTE 1 – Policy information for the support of IoT services is usually predefined.

– An IoT-CN is recommended to have the ability to support blockchain capabilities with the help of one or more application servers in a separate blockchain network.

NOTE 2 – Heterogeneous IoT-CNs may support diverse radio access technologies.

7.1.2 Decentralization of blockchain-based self-organization networking

- B-SON functions are required to be distributed to IoT-CNs according to the predefined policies to operate IoT services [ITU-T Y.4417].
- The policy information for IoT services in B-SON network is recommended to be kept in the blockchain network with the help of application servers.
- Data sharing between the B-SON network and blockchain network (e.g., via mechanisms such as interledger protocol [b-Hyperledger Quit]) is recommended to be supported.

7.2 Functional requirements

7.2.1 Self-configuration functional requirements

- B-SON is required to support a self-configuration function for connectivity of IoT-DNs to IoT-CN.
- B-SON is required to support a self-configuration function among IoT-CNs.
- B-SON is recommended to support all procedures to initiate IoT-DN to IoT-CN networking (e.g., registration, authorization, access control, neighbour discovery) via the support of blockchain technology (e.g., smart contract).
- A blockchain network composed of application servers is recommended to manage the networking information of a B-SON network (e.g., routing tables, IoT-DN information, IoT-CN information and routing path information).

7.2.2 Self-healing functional requirements

- B-SON is required to have a self-healing function (e.g., neighbour IoT-CN discovery, network failure detection, election of new IoT-CN on behalf of failed IoT-CN) among IoT-CNs.
- IoT-CN is recommended to obtain the self-healing information from neighbouring IoT-CNs and application servers.
- A blockchain network composed of application servers is recommended to keep the information to support the recovery of a B-SON network.
- The blockchain network composed of application servers is recommended to keep the information to support the IoT-CN election.

7.2.3 Self-optimizing functional requirements

- B-SON is required to manage the performance information (e.g., delay, packet loss, throughput) for IoT services.
- B-SON is recommended to manage the performance information for IoT services with the help of application servers.

  NOTE – Performance information for IoT services is compared with the predefined policy information in the blockchain network for possible IoT environment performance adjustment.
- A blockchain network composed of application servers is recommended to use consensus mechanisms to support the self-optimizing function in a B-SON network.

7.2.4 Self-protecting functional requirements

- B-SON is recommended to use smart contracts to support the decentralization of B-SON functions.
- B-SON is recommended to use smart contracts to authenticate IoT-DNs and IoT-CNs to become members of a B-SON network.
- B-SON is recommended to maintain access information (e.g., join and leave in/from a B-SON network).

– B-SON is recommended to use smart contracts in IoT-CNs to support IoT services.

– A blockchain network composed of application servers is recommended to support smart contracts of IoT-CNs for IoT services support.

8 Architecture of blockchain-based self-organization networking

8.1 Functions of blockchain-based self-organization networking

B-SON provides autonomous functions through the cooperation of IoT-DNs and IoT-CNs as shown in Figure 3. The B-SON functional architecture shown in Figure 5 is an extension of the SON functional architecture described in [ITU-T Y.4417]. The B-SON functional architecture includes a blockchain function with four related functional entities. The three B-SON functions, i.e., coordination function [ITU-T Y.4417], networking function [ITU-T Y.4417] and blockchain function, support the requirements identified in clause 7 for the IoT environment.

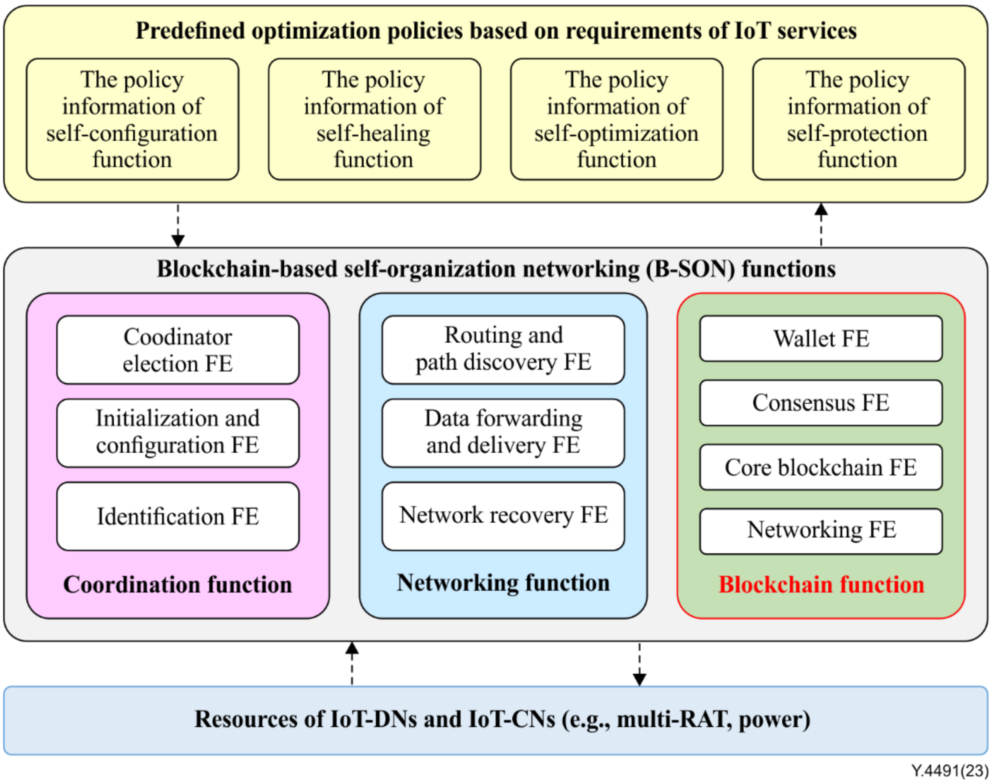

Figure 5 – B-SON functional architecture

The B-SON functional architecture is comprised of three functions:

– ***Coordination function***: this has the role of building network topologies with three functional entities (FEs), i.e., coordinator election, initialization and configuration, and identification.

– ***Network Function***: this enables data communication among IoT-DNs with three FEs: routing and path discovery, data forwarding and delivery, and network recovery.

– ***Blockchain Function***: this provides blockchain capabilities in support to the B-SON functions (i.e., coordination and network functions) with four FEs: wallet, consensus, core blockchain and networking.

Predefined optimization policies of autonomous functions are built in terms of the requirements of specific IoT services. With the coordination function, IoT-CNs collect resource information from neighbouring IoT-CNs, such as remaining energy or processing performance. The coordination function elects coordinators and builds initialization and configurations to control network topologies, while the networking function builds routing paths for packet forwarding in terms of the elected coordinators and the policies for optimization. Then, data delivery beings [ITU-T Y.4417].

The role of predefined optimization policies is to analyse the status and requirements for IoT services and decide an optimal policy based on the requirements. The determination of optimization policies is dependent on the requirements of IoT services. If IoT services require energy-efficient networking, all procedures are focused on energy saving. If the IoT services require high performance (e.g., high-speed or big-data processing), B-SON is configured for high-performance. Such policies can vary according to the characteristics of the IoT service requirements [ITU-T Y.4417].

In Figure 6, the B-SON functions shown in Figure 5 are allocated to each IoT-DN or IoT-CN. These functions exchange the necessary information for constructing and maintaining a network through the blockchain. There are two cases according to the hardware capabilities (e.g., storage capacity, CPU speed, etc.) of IoT-DNs/IoT-CNs. The left of Figure 6 shows non-constrained IoT-DN/IoT-CN with four blockchain FEs. The right of Figure 6 shows constrained IoT-DNs/IoT-CNs with the help of application servers to perform the blockchain function as described below.

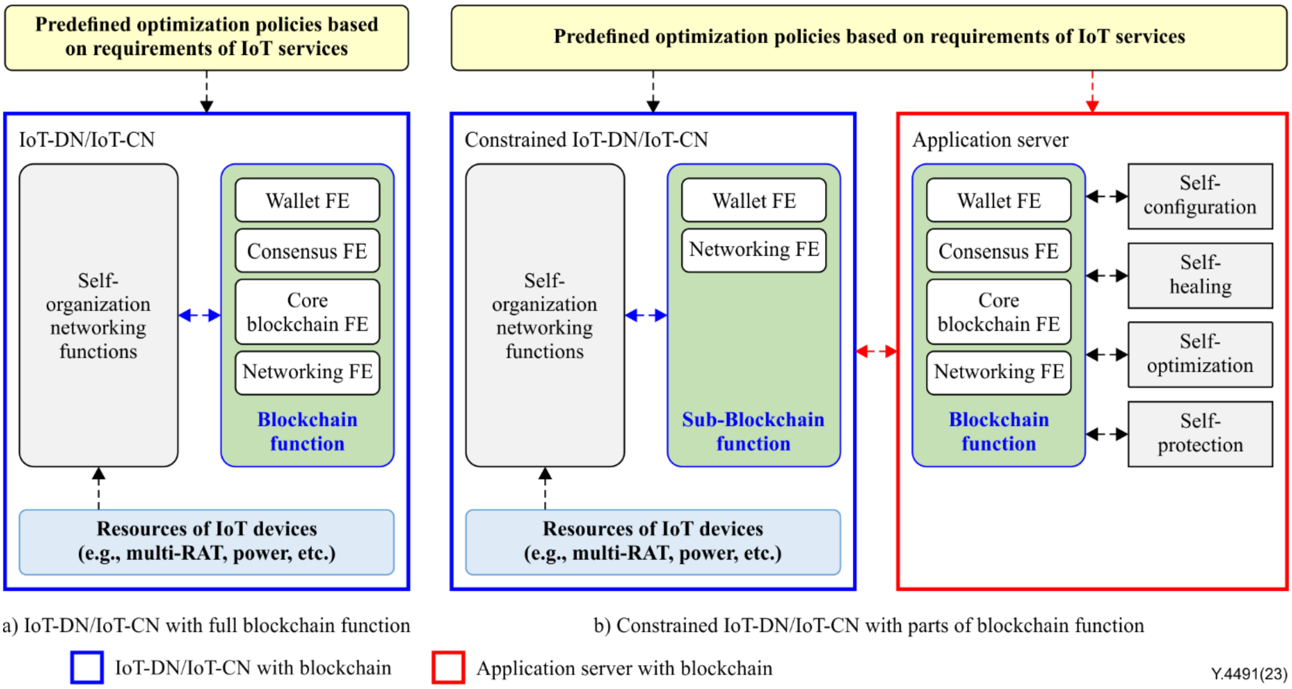

Figure 6 – Two cases of blockchain functional entity locations

8.2 Functional entities of blockchain-based self-organization networking

8.2.1 Coordination function

The coordination function has three FEs, i.e., coordinator election, initialization and configuration, and identification [ITU-T Y.4417]. The following describes how these FEs interact with the blockchain function.

– Coordinator election FE: IoT-CNs manage neighbouring IoT-CNs and forward the data to target IoT-DNs. IoT-CNs act as a gateway for the neighbouring IoT-DNs. In B-SON, there may be many candidate IoT-CNs with multiple radio access interfaces. Some of them become coordinators according to a predefined optimization policy for IoT services. The blockchain function, in particular the consensus FE, interacts with this FE for the self-optimizing function. The consensus mechanisms are used to elect IoT-CNs. Therefore, B-SON maintains the neighbouring and forwarding information (e.g., lists of IoT-CNs/IoT-DNs, election rules, revocation lists, multiple radio access interfaces and networking capabilities of IoT-CNs/IoT-DNs).

– Initialization and configuration FE: All IoT-DNs belong to one of the IoT-CNs for management. Hence, the IoT-DNs are connected to one of the IoT-CNs with star topology. Theses connections between sending and targeting IoT-DNs are exploited for data forwarding through the IoT-CNs. The blockchain function, in particular core blockchain FE and networking FE, interacts with the initialization and configuration FE for the self-configuration function. Smart contract is triggered to configure B-SON network according to the predefined optimization policy.

– Identification FE: The identification schemes in [ITU-T Y.4417] are not appropriate for IoT-CNs and IoT-DNs in a B-SON network. Therefore, new identification schemes are required. Even though these schemes are out of scope in this Recommendation, they support blockchain technologies to support secure identification management. The blockchain function, in particular wallet FE and core blockchain FE, interacts with the identification FE for self-protecting function. Authentication and digital signature mechanisms of blockchain [ITU-T Y.3530] may be used to support secure join and leave events in a B-SON network.

8.2.2 Networking function

The networking function has three FEs: routing and path discovery, data forwarding and delivery, and network recovery [ITU-T Y.4417]. The following describes how these FEs interact with the blockchain function.

– Routing and path discovery FE: network topology among IoT-CNs is created according to predefined optimization policies. The routing path is built in terms of the IoT-CNs between a source IoT-DN and a destination IoT-DN. The blockchain function interacts with this FE for self-optimizing and self-configuration functions. The consensus mechanisms select appropriate IoT-CNs to make routing path.

– Data forwarding and delivery FE: data forwarding can be conducted with various traffic patterns (e.g., unicasting, multicasting and broadcasting). Data forwarding is managed by IoT-CNs and data delivery to IoT-DNs is done through IoT-CNs. Blockchain function interacts with this FE for self-optimizing and self-configuration functions. The consensus mechanisms select appropriate IoT-CNs for data forwarding and then smart contracts are triggered to select proper target IoT-DNs.

– Network recovery FE: There are two types of network node failures. One is the failure of IoT-CNs and the other is the failure of IoT-DNs. If an IoT-CN fails, one of the candidate IoT-CNs is elected as new IoT-CN with the help of a blockchain network with application servers. Then, neighbouring IoT-DNs are recovered. The blockchain function interacts with this FE for self-healing service. All information for self-healing function is obtained from the B-SON network. Furthermore, if a connection between an IoT-CN and an IoT-DN fails, the IoT-CN tries to reconnect to the IoT-DN. When it finally turns out that the connection is closed, the IoT-CN does not manage information of the disconnected IoT-DN any longer. This information is kept in a revocation list on the blockchain network.

8.2.3 Blockchain function

The blockchain function has four FEs: wallet, consensus, core blockchain and network FEs. The following describes how these FEs interact with the coordination and networking functions.

– Wallet FE: the FE manages the identification information for IoT services (e.g., identification of IoT-CNs/IoT-DNs, IoT services and smart contracts, currency, coupon and so on). The FE is not limited to specific identification schemes because IoT services may support different identification schemes.

– Consensus FE: the FE selects IoT-CNs with predefined optimization polices to support authentication and authorization for join and/or leave of IoT-CNs. As shown in Figure 6, the FE is not located in IoT-CNs. Therefore, application servers may have this role on behalf of IoT-CNs.

– Core blockchain FE: the FE manages the distributed ledger. This FE is not supported in constrained IoT-DNs. In this case, application servers join the blockchain network.
– Networking FE: the FE manages the blockchain network. This network is composed of IoT-CNs, IoT-DNs and application servers.

Appendix I

Use cases of blockchain-based self-organization networking

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

I.1 Smart contract-based network autoconfiguration in an IoT environments

In a B-SON network, dynamic network configuration is possible between IoT-CNs (i.e., IoT coordinators). When constructing a SON network, the network configuration is initiated utilizing a smart contract. This configuration can be differentiated according to necessity of network resources in each IoT service. IoT-CN can configure the smart contract with network policy. When the network environment changes, it is possible to change the network configuration dynamically. And when a SON network failure occurs, the SON network can be restored or changed dynamically by network policy. This is because blocks in the blockchain store routing table, IoT device information, and routing path costs for network configuration. Smart contracts can be created for events such as addition, deletion and update of IoT-DNs and/or IoT-CNs.

B-SON supports a distributed environment. IoT-CNs construct a blockchain network. So, an identical routing table is stored in all IoT-CNs. When an IoT-CN fails, the routing is changed to another IoT-CN, and it can be restored from the neighbouring IoT-CN. In a B-SON environment, various application configurations are possible. The routing table is distributed and executed to recover from the application failure.

I.2 Distributed ledger based routing table management in an IoT environments

B-SON supports IoT device authentication and routing table validation. In an IoT environment, authentication of the IoT devices is important to construct a B-SON network. In fact, it is possible for a malicious IoT device to deliver incorrect routing tables, to set incorrect route paths or to communicate incorrect information of neighbour IoT devices during the process of constructing the B-SON network. This issue can be solved by the elliptic curve digital signature algorithm (ECDSA) [b-FIPS-186-3] using public and private keys in the B-SON network.

The validity of information delivered by the participating IoT devices is verified. This verification can be addressed by transactions containing information for routing table, storing it in a block and validating it with a consensus mechanism.

Bibliography

[b-ITU-T Y.3680] Recommendation ITU-T Y.3680 (2022), *Framework of human-like networking*.

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

[b-ITU-T Y.4407] Recommendation ITU-T Y.4407/Y.2281 (2011), *Framework of networked vehicle services and applications using NGN.*

[b-ITU-T Y.4451] Recommendation ITU-T Y.4451 (2016), *Framework of constrained device networking in the IoT environments*.

[b-ITU-T Y.Suppl.62] Recommendation ITU-T Y.Suppl.62 (2020), *Overview of blockchain for supporting Internet of things and smart cities and communities in data processing and management aspects.*

[b-FIPS-186-3] FIPS 186-3, National Institute of Standards and Technology (2009), *Digital Signature Standard*.

[b-Hyperledger Quit] Hyperledger Foundation (2019), *Hyperledger Quilt*. https://www.hyperledger.org/use/quilt.

[b-IEEE 802.15.4-2020] IEEE 802.15.4-2020, *IEEE Standard for Low-Rate Wireless Networks*.

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