ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

ITU-T Y.2345 (05/2023)

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

Next Generation Networks – Enhancements to NGN

Scenarios and requirements of network resource sharing based on distributed ledger technology

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
Frameworks and functional architecture models	Y.2000-Y.2099
Quality of Service and performance	Y.2100-Y.2199
Service aspects: Service capabilities and service architecture	Y.2200-Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250-Y.2299
Enhancements to NGN	**Y.2300-Y.2399**
Network management	Y.2400-Y.2499
Computing power networks	Y.2500-Y.2599
Packet-based Networks	Y.2600-Y.2699
Security	Y.2700-Y.2799
Generalized mobility	Y.2800-Y.2899
Carrier grade open environment	Y.2900-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

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

Recommendation ITU-T Y.2345

Scenarios and requirements of network resource sharing based on distributed ledger technology

Summary

Recommendation ITU-T Y.2345 aims to provide the overview and general framework of the network resource sharing based on distributed ledger technology and specifies scenarios and capability requirements which are derived from use cases.

History [1]

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T Y.2345	2023-05-14	13	11.1002/1000/15530

Keywords

Distributed ledger technology, network resource sharing, requirements, scenarios.

[1] 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.2345

Scenarios and requirements of network resource sharing based on distributed ledger technology

1 Scope

This Recommendation specifies the scenarios and capability requirements of network resource sharing based on distributed ledger technology.

The scope of this Recommendation includes:

1) Overview of network resource sharing.
2) General framework of network resource sharing based on distributed ledger technology.
3) Capability requirements of network resource sharing based on distributed ledger technology.
4) Scenarios and use cases of network resource sharing based on distributed ledger technology.

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 X.1400] Recommendation ITU-T X.1400 (2020), *Terms and definitions for distributed ledger technology.*

[ITU-T Y.2340] Recommendation ITU-T Y.2340 (2016), *Next generation network evolution phase 1 – Overview.*

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

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 distributed ledger [ITU-T X.1400]: A type of ledger that is shared, replicated, and synchronized in a distributed and decentralized manner.

3.1.2 smart contract [ITU-T X.1400]: Program written on a 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.

3.1.3 transaction [ITU-T X.1400]: Whole of the exchange of information between nodes. A transaction is uniquely identified by a transaction identifier.

3.1.4 entity [b-ITU-T F.751.4]: Anything that has a separately identifiable existence (e.g., organization, person, group or device). An entity uses distributed ledger technology to solve the problem of its business or information systems.

3.1.5 participant [b-ITU-T X.1405]: Entity who participates in the DLT system's decision making. For example, miners, validators, node owners, orders, voters, etc.

3.1.6 node [ITU-T X.1400]: Device or process that participates in a distributed ledger network.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API	Application Programming Interface
CCPE	Computing Capabilities Provider at the Edge
DLT	Distributed Ledger Technology
HPC	High Performance Computing
ICT	Information and Communication Technologies
IoT	Internet of Things
NRB	Network Resource Broker
NRC	Network Resource Customer
NRNSM	Network Resource Node Service Maintainer
NRNSP	Network Resource Node Service Provider
NRP	Network Resource Provider
NSP	Node Service Provider
ProSe	Proximity-based Service
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 Overview of network resource sharing

6.1 Background

Network resource sharing is the system that support the users of different networks to share the network resource among networks as business demands, including sharing computing, storage, connection and data resource.

With the rapid evolution of 5G networks and IoT technology in recent years, an increasing number of devices are connected to the network, producing complex and enormous business demands, which need more flexible and efficient network resource support. Therefore, how to effectively promote network resource sharing to meet the demands of diversified services is a critical issue in the next generation network [ITU-T Y.2340].

Distributed ledger is a type of ledger that is shared, replicated and synchronized in a distributed and decentralized manner [ITU-T X.1400].

Distributed ledger technology (DLT) can record each transaction through distributed ledgers that are secured from tampering and revision. In a distributed ledger, the records, that are called blocks, are chained one by one using the cryptographic signature. To ensure the authenticity and integrity of the ledger, every record is provided a unique cryptographic signature and is time and date stamped. Only when the participants reach a consensus over the validity of a block, can the block be added in the distributed ledger. Beyond that, DLT has a unique token incentive model, which can increase the motivation of the participants on the chain, promote participants to jointly govern the network environment to achieve network resource sharing regularly, and further, enable users, contributors and regulators to achieve ecological balance.

As one of the emerging technologies in recent years, DLT has core technical features such as smart contracts and distributed consensus, which can bring enhancement to network application scenarios in next generation networks as described in [ITU-T Y.2342].

NRS-DLT is distributed network resource sharing which supports traditional network system interaction and provides DLT related capabilities among various network entities by utilizing DLT as a data carrier for resource status, for allocating computing, storage and network resources of infrastructure layer and network layer to applications.

6.2 NRS-DLT ecosystem and roles

This clause describes a network environment, called a NRS-DLT ecosystem, with roles and sub-roles. It also defines necessary activities for roles sharing resource based on DLT, as well as relationships between roles.

The NRS-DLT ecosystem includes the following roles:

- network resource node service provider (NRNSP);
- network resource node service maintainer (NRNSM);
- network resource provider (NRP);
- network resource broker (NRB);
- network resource customer (NRC);
- network operator (NO).

The NRS-DLT ecosystem is shown in Figure 6-1.

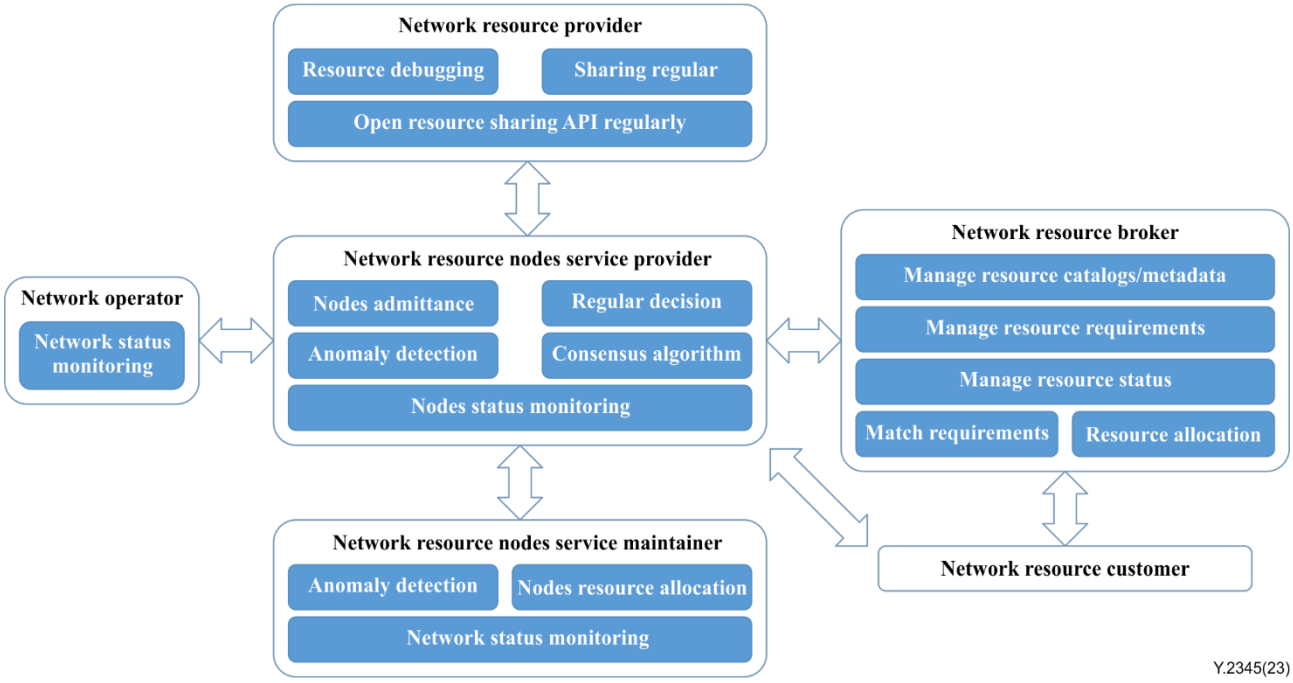


Figure 6-1 – The ecosystem of NRS-DLT

6.2.1 Network resource nodes service provider of NRS-DLT

The NRNSP role provides the DLT infrastructure, which is the core of this ecosystem. The NRNSP could receive the resource API from the NRP and share to the NRC regularly, and record all the operations in the chain for tracing. The NRNSP's activities include:

- DLT infrastructure construction, include consensus algorithm design, smart contract;
- Nodes admittance and nodes classification, such as consensus nodes, common nodes;
- Regular decision;
- Anomaly detection;
- Node status monitoring, such as computing resource status, node normal status, node activity.

6.2.2 Network resource node service maintainer of NRS-DLT

The network node service maintainer (NRNSM) role provides DLT network maintenance, which supports capabilities for breakdown maintenance, technical support, etc. The NRNSM's activities include:

- Anomaly detection;
- Network status monitoring, such as computing resource status, node normal status, node activity, etc.;
- Node resource allocation: Through the result of node status monitoring feedback itself or by NRNSP, the NRNSM allocates and balances the resource among nodes.

6.2.3 Network resource provider of NRS-DLT

The NRP provides network resources, such as computing resources, storage resources, data resources and connection resources to the NRC. The NRP's activities include:

- Resource debugging before sharing;
- Making the sharing strategy include sharing conditions, sharing ways, sharing time, etc.;
- Open resource sharing API, recorded by DLT, according to sharing strategy.

6.2.4 Network resource customer of NRS-DLT

The NRC is the end user or a system to use the results or services from the NRNSP to obtain the resource of the NRP.

the NRC's activities include:

- Requesting the network resource to the node service provider (NSP);
- Obtaining the network resource API from the NSP and using it regularly.

6.2.5 Network operator of NRS-DLT

The network operator (NO) is usually the telecom operator, whose function is providing the normal operation of the network. The NO's activities include:

- Monitoring network status.

6.2.6 Network resource broker of NRS-DLT

The network resource broker (NRB) serves to connect the NRC and network resource service provider. The NRB can act as an open network resource mart and aim to collect and manage resource information and requirements, to help achieve accurate resource matching between the NRP and NRC. The NRB could interact with the NRNSP and NRC, and its activities include:

- Providing a meta-information registry to the NRNSP for publishing network resources;
- Providing a service catalogue to the NRC for searching a usable network resource;
- Supporting requirements management for NRC;
- Interacting with the NRNSP to update network resource transaction and status information, such as the resource transaction amount, resource types involved in the transactions, etc.;
- Supporting interactive information security and credibility.

7 General framework of network resource sharing based on distributed ledger technology

7.1 Network resource sharing based on distributed ledger technology

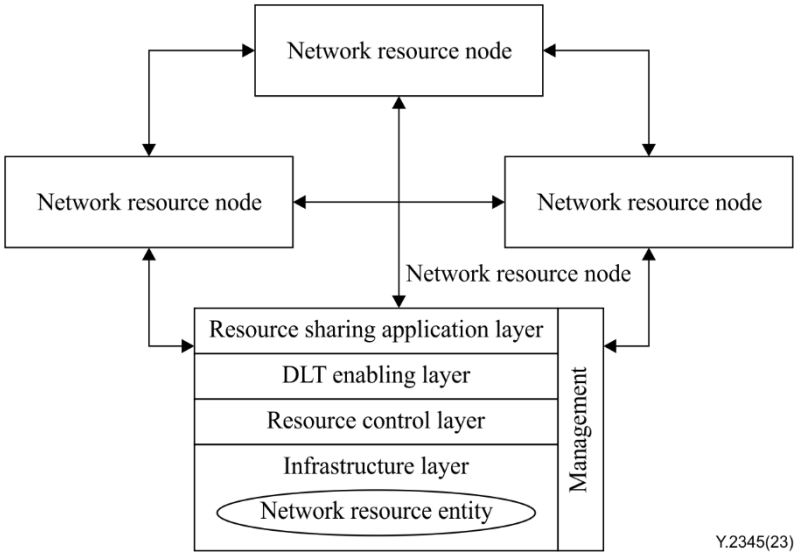


Figure 7-1 – General framework of network resource sharing based on distributed ledger technology

As shown in Figure 7-1, the framework of network resource sharing based on DLT involves multiple network resource nodes, which work together to promote network resource sharing. There are four layers in the framework of network resource sharing based on DLT:

- The resource sharing application layer provides specific decentralized network resource sharing application, such as computing resource sharing resolution, data resource sharing, based on the smart contracts.
- The DLT enabling layer provides core features to support network resource sharing application layer services, including providing decentralized ledger storage, consensus mechanism and smart contract execution environment.
- The resource control layer provides asset control, network resource management, network resource breakage capability, etc., to support network resource allocation.
- The infrastructure layer provides support for access of various network resource entities which belong to different physical nodes.

It is recommended to consider these four layers in network resource sharing based on DLT. For each layer, specific relevant use cases need to be devised to derive requirements for different aspects.

It is recommended that these requirements be classifiable into high level requirements and capability requirements.

7.2 High-level requirements of network resource sharing based on distributed ledger technology

7.2.1 Account management

It is required to provide valid account management mechanisms for NRS-DLT, including account generating, role assignment, identity authentication. Each participant, or user, of NRS-DLT will be provided an account with different authorities to act in different roles, e.g., resource provider, computing capability requester, system maintainer.

7.2.2 Asset and resource control

It is required to provide asset and resource control mechanisms for NRS-DLT. Asset control enables each participant to manage and maintain their resources and transaction related activities directly, and resource control provides necessary resource registration, validation, reservation and dispatchment functions for resource capacity sharing. Asset and resource control should also ensure asset safety and data protection for each provider or requester and should be hot-pluggable.

7.2.3 Scalability

It is required to support scalability, including:

– Supporting the consensus mechanism of high scalability and efficiency;

– Supporting availability management mechanisms for consensus nodes and network resource service nodes, such as heartbeat monitoring mechanisms;

– Supporting system expansion, cross-system interaction and multisystem access.

7.2.4 Intrusion prevention mechanism

It is required to provide intrusion prevention mechanisms such as network attack behaviour monitoring and malicious code detection, which should be set at key nodes (e.g., network resource service nodes and consensus nodes).

It is required to upgrade and update intrusion prevention mechanisms regularly.

7.2.5 Security mechanism

It is required to provide security protection for resource sharing, including data resource information protection, participants' identity information protection, sharing processes protection.

It is required to provide failure detection mechanisms to automatically identify failed nodes to ensure DLT network security.

7.2.6 Network management

It is required to provide network management mechanisms for NRS-DLT, including connection network management and blockchain network management, as follows:

– Connection network management should monitor and record the connection performance and status of each participant to ensure effective resource sharing;

– Blockchain network management should monitor the operation status of the consensus process and smart contract, provide timely feedback and deal with problems, and ensure the stable operation of the blockchain network.

8 Capability requirements of network resource sharing based on distributed ledger technology

8.1 Resource sharing application layer

8.1.1 Computing resource related capability requirements

It is required to provide a capability to record the attribute information of the computing resources on the distributed ledger.

It is required to provide a capability to receive and record the resource requests from the NRC.

It is required to provide a capability to record the computing resource sharing transaction on the distributed ledger.

It is required to provide a capability to manage computing resource nodes and schedule computing resources between computing nodes. For example, the management capability will schedule more computing resources to consensus nodes to achieve an efficient consensus process.

8.1.2 Billing related capability requirements

It is required to provide a capability to open/close payment channels. It will open payment channels after matching resources successfully, and close payment channels before allocating a token to guarantee mutual interest.

It is required to provide a capability to calculate the cost of the resource sharing based on the quality of service (QoS) of the resource service, service time, etc. This capability will trigger a smart contract to complete the resource sharing settlement, and record settlement transaction on the distributed ledger.

8.2 DLT enabling layer

8.2.1 Consensus mechanism capability requirements

It is required to provide the consensus mechanism for NRS-DLT. The consensus mechanism enables the guaranteeing of the consistent and authentic record of blockchain by consensus nodes.

8.2.2 Smart contract capability requirements

It is required to support smart contracts for NRS-DLT to execute resource sharing transaction and settlement automatically. Smart contracts should keep status update records to meet security audit requirements.

8.2.3 Incentive mechanism capability requirements

It is required to provide an incentive mechanism for NRS-DLT. An incentive mechanism, unique to the DLT, could stimulate more participants to join the NRS-DLT ecosystem, to promote network resource sharing.

8.2.4 Cross-chain interaction capability requirements

It is recommended to provide a cross-chain interaction capability for NRS-DLT, which could extend the ecosystem of NRS-DLT, not only limited to network resource sharing between nodes on this chain, but also extended to the heterogeneous chains.

8.2.5 DLT service support and management capability requirements

It is recommended to provide a capability to support more service nodes and support heterogeneous network resources.

It is required to provide a capability to monitor and alert node service performance.

8.3 Resource control layer

8.3.1 Resource control capability requirements

It is required to provide a capability to write/read data from NRS-DLT ledger rapidly and precisely to be used for resource registration and history traceability.

It is required to provide a capability to validate the authenticity and availability of resources.

It is required to provide a capability for invoke/query smart contracts for resource reserving, capability estimating, dispatching, plan generating, demand analysing etc.

It is required to provide a capability to read/write data from/to other layers to receive and return data stably. Resources control layer and other layers should have full mutual access.

It is required to provide a capability to the NRNSP for publishing network resources, including computing resources, edge resources, data resources, etc.

8.3.2 Resource allocation capability requirements

It is required to provide a capability to analyse the requests of the NRC.

It is required to provide a capability to recommend or match appropriate resources to the NRC. It will recommend or match network resources based on the analysis results of the NRC's requests to meet the service needs of multiple NRCs to the greatest extent possible.

8.4 Infrastructure layer

8.4.1 Asset control capability requirements

It is required to provide a capability to manage users' resource related assets, including resource management and resources overview.

NOTE – User resource related assets includes the resource providers' assets, such as the edge-computing resource or the storage resource, and the resource requesters' assets, such as the context data or the algorithm code.

8.4.2 Network resource brokerage capability requirements

It is required to provide a capability to set the NRB in the edge of NRS-DLT for network resource scheduling.

It is required to provide a capability to manage sharing resource information, including resource requirements, resource status and resource metadata.

It is required to provide a capability for the NRB to match the requirements of NRC with registered resources.

It is required to provide a capability to provide a network resource catalogue to the NRC.

It is required to provide a capability to interact between ecosystem roles. For example, the NRB interact with the NRNSP for notifying the corresponding NRP to share a network resource to specific NRC, such as the edge-computing resource or data resource; the NRB forwards resource requests to the nearest NRNSP; interacts with the NRC to feedback resource status after the ensuring edge-computing resource; and interacts with the NRP to inform it to share a resource to the NRC after verifying user signatures.

8.4.3 Network resource entity capability requirements

It is required to provide a capability to network a resource entity for sharing computing, storage, connection, data and other resources.

It is required to provide a capability to network a resource entity for invoking a smart contract to apply for computing, storage, connection, data and other resources.

8.5 Management-related capability requirements

In network resource sharing based on DLT, the system is required to provide management capabilities to ensure the normal operation of the sharing ecosystem, which includes node management, user identity management and sharing service management.

According to the definition of ecosystem roles in clause 6, the NRNSP provides the DLT infrastructure and receives the resource API, which is required to provide node management, user management and sharing service management; and the NRNSM provides DLT network maintenance, supports capability for breakdown maintenance and technical support, which is required to provide node management and user management; and the NRB serves to connect between the NRC and NRP for resource sharing, which is required to provide sharing service management.

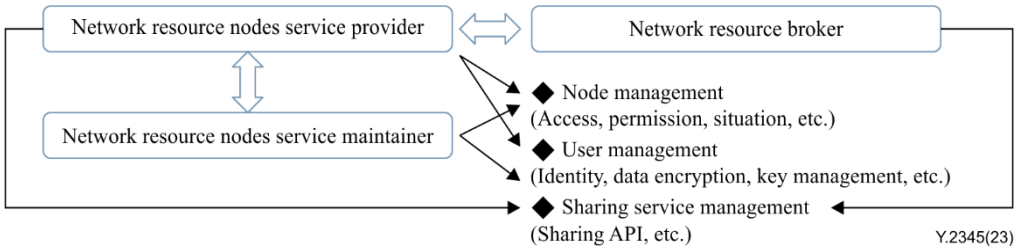


Figure 8-1 – Relationship between management requirements and roles

8.5.1 Node security management capability requirements

It is required to provide the node security management strategy to achieve security management and control for nodes access to ensure the normal operation of their NRS-DLT while users register to and join the sharing ecosystem.

It is required to provide a capability to respond to the node registration request and acquire the information to register, including: node identity, registered roles, credit rating information and node permission information, and record it on the distributed ledger by smart contract. Nodes' permission in NRS-DLT should be determined by roles in ecosystem and credit rating information. For example, registering the role of the NRC could be given the rights to query resource catalogue and obtain according to the strategy, which has no authority to participate in consensus. And if users apply to register the role of the NRNSP, the system will give different permission with different credit rating; low credit ratings do not authorize participation in the consensus.

It is required to provide a capability for dynamic evaluation and updating nodes' credit rating information by online duration, activity levels and historical action, ensuring the dynamic adjustment of permissions, which could be monitored by the NRNSP. If the nodes' credit rating information changes, the nodes permission information that control the nodes permission in NRS-DLT should be updated and recorded on the distributed ledger. For different business, the weight of these indicators could be adjusted by the NRNSP or node consensus.

It is required to provide a capability for repair faulty nodes to restore resource sharing services in a timely manner.

8.5.2 User management capability requirements

It is required to provide a capability for identity authentication and data encryption to ensure users' identity security.

It is required to provide a key management mechanism to ensure the security of key storage for completing the public and private key encryption and authentication during the sharing.

It is required to provide a capability of user access management to give users access to computing, storage, connection and data resources.

It is required to provide a capability of user information management to provide a basis for user identity authentication, transaction traceability, transaction settlement, etc.

8.5.3 Sharing service management capability requirements

It is required to provide a capability of network resource sharing API managements to ensure normal sharing in NRS-DLT.

It is required to provide a capability to manage the list of the sharing service resources to maintain and update NRP resource information in a timely manner.

Appendix I

Scenarios and use cases of network resource sharing based on distributed ledger technology

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

Table I.1 – Use case of edge-computing resource sharing based on NRS-DLT

Title	Use case of edge-computing resource sharing based on NRS-DLT
Description	With the development of 5G and edge computing, the need for computing capabilities of edge resources grows dramatically, as computing capabilities form the basis of ubiquitous computing. Hence, it is necessary to take good advantages of edge resources and share extra computing capabilities properly to help boost computing processes. However, centralized resource management systems fail to provide satisfying solutions: 1) Centralized management system may confront single point failure, which causes the computing resource sharing service to be unavailable. 2) The system operated by centralized mechanisms may have the risk of information leak. 3) Centralized architecture are insufficient for high performance computing (HPC) and distributed computing. A problem solver needs to use several centralized resource management systems to fulfil the computing capability requirements. This process can be error prone and costly – toward both money and energy. In this case, NRS-DLT could be a potential solution for sharing the edge-computing resources. Based on distributed ledger technology, the NRS-DLT system is inherently suitable for HPC and distributed computing, and could manage, dispatch and share these computing resources at the edge automatically, instantly, uninterruptedly, safely and readily. Moreover, distributed architecture could easily build up trust between providers and users.
Roles	Computing capabilities provider at the edge (resource provider): The owner of the edge resources. Except for computing capabilities, the resource provider needs to provide necessary techniques such as device registration, device dispatch, device maintenance and so on. Computing capabilities requester (resource requester): The purchaser of the computing capabilities at the edge. NRS-DLT maintainer: The provider of NRS-DLT. The NRS-DLT maintainer should provide necessary capabilities, techniques, maintenances and functions of NRS-DLT under computing capabilities sharing of edge resources scenario.

Table I.1 – Use case of edge-computing resource sharing based on NRS-DLT

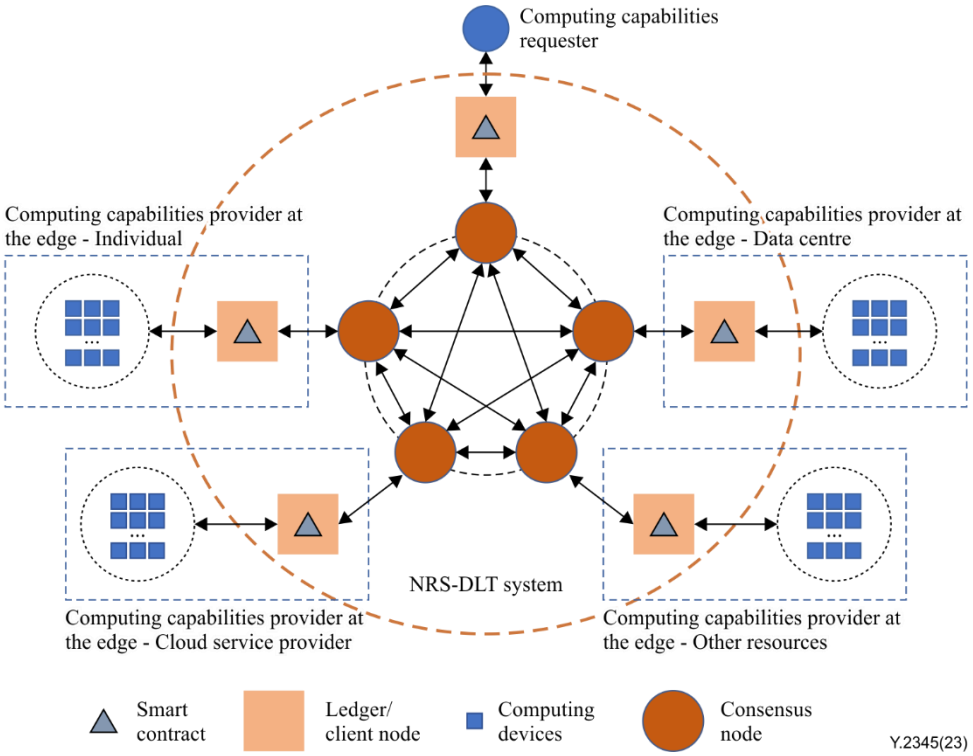
Title	Use case of edge-computing resource sharing based on NRS-DLT
Figure and operational flows	 **Figure I.1 – Edge-computing resources sharing based on NRS-DLT** 1) The resource provider should register all the edge resources with computing capabilities to the NRS-DLT system, and key configurations, including exact computing capabilities, network capabilities, identity information, should be clarified and their availability verified via smart contract. 2) The resource requester publicizes the demand of computing capabilities to the NRS-DLT system. The request should give an estimate of resources usage, algorithm, throughput, etc. 3) NRS-DLT uses a smart contract to analyse the exact demand of edge resources according to the request. The exact demand, or plan, should in detail include the requirement and framework of the algorithm, network usage, storage, the need of computing capabilities, and so on. Meanwhile, the estimate cost of the plan should be provided to the requester. 4) The resource requester chooses a plan to purchase, returns the decision back to NRS-DLT, and waits for the resources ready to use. 5) After receiving the decision from the requester, the NRS-DLT system uses a smart contract to complete the following steps: 1) The NRS-DLT system analyses the decision and prepares the resources, i.e., divides tasks into sub-tasks and assigns them to different providers. 2) Resource providers receive tasks/sub-tasks, then reserve and dispatch corresponding edge resources with computing capabilities. The NRS-DLT system will generate configurations of network, safety and resource, install requester's algorithms on these edge resources and give a link to access the resources. 3) The NRS-DLT system will send the link back to the requester. The requester uses the link to connect to and access purchased computing capabilities at the edge.

Table I.1 – Use case of edge-computing resource sharing based on NRS-DLT

Title	Use case of edge-computing resource sharing based on NRS-DLT
	It is necessary to clarify that step 5 described above is only an implementing option for sharing the edge-computing resource. Depending on the application features and computing provision methods, there are different implementing methods, e.g., transferring the context data to the execution environment base on the serverless service. 6) After computing is done, linkage between the requester and provider is cut off, and all the computing capabilities at the edge will be returned. The whole process is recorded in the distributed ledger for auditability and traceability.
Derived requirements	Requirements for computing capabilities provider at the edge (CCPE): It is required that the CCPE provide the capability to access resource control. It is required that the CCPE provide the capability to register all the edge resources with computing capabilities and record the required parameter to the NRS-DLT ledger. Requirements for the NRS-DLT: It is required that NRS-DLT provide the ledger to record the resources. It is required that NRS-DLT provide the consensus mechanism to guarantee the consistent record. It is required that NRS-DLT provide sufficient reading/writing performance from/to the ledger. It is required that NRS-DLT provide the smart contracts to implement date entries reading/writing. It is required that NRS-DLT provide nodes management and access control. It is required that NRS-DLT provide the scalability. It is required that NRS-DLT provide necessary protection for user identity and data information by user management. It is required that NRS-DLT provide asset control and resource control.

Table I.2 – Use case of cross-system network data resource sharing based on NRS-DLT

Title	Use case of cross-system network data resource sharing based on NRS-DLT
Description	With the development of a series of emerging technologies and significant growth of business demand, an increasing number of devices are connected to the future network, which produces an enormous amount of data. How to effectively promote the interconnection and comprehensive sharing of network data resources to meet the demands of diversified services is a critical issue in the future development of computer network technology. Centralized data resource sharing fails to provide satisfying solutions for the following reasons: 1) Centralized sharing solutions may confront single point failure which causes data resources to be unavailable. 2) Network data is stored on the centralized server side, which may have unauthorized behaviour, leading to problems of data security. 3) The centralized data management agency has a heavy responsibility, data rights are difficult to distinguish and meanwhile it also has the risk of information leak. 4) Data sharing in a centralized way has low efficiency, such as, "one situation, one discussion" and centralized approval, which will affect the sharing process. It is necessary to provide a suitable interconnection solution with high performance for ever-richer access and various networks to maximize the data value through efficient

Table I.2 – Use case of cross-system network data resource sharing based on NRS-DLT

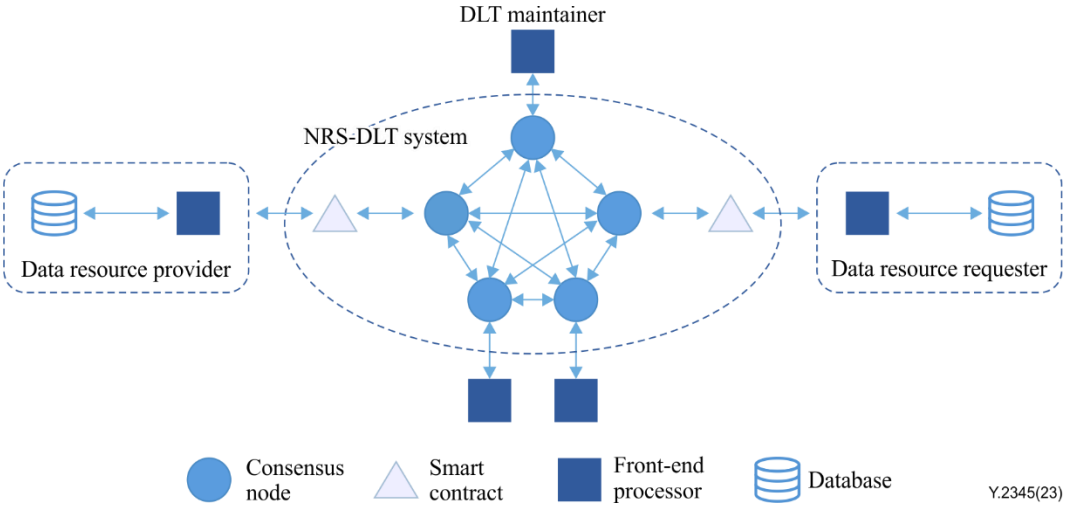
Title	Use case of cross-system network data resource sharing based on NRS-DLT
	sharing. Distributed network data resource sharing based on DLT provides a suitable management model to address single points of failure and trust problem among networks. The network data resource is the data resource that is transmitted and released by network; further, the network data resource includes non-sensitive data (public data) and semi-sensitive data (conditional sharing data) classified by sensitivity. Sensitive data involves a confidentiality clause and data protection, which is not circulated by the network generally, so it is not included in the network data resources.
Roles	Network data resource provider: the owner of the network data resources. Network data resource requester: the purchaser of the network data resources. NRS-DLT maintainer: the provider of NRS-DLT. The NRS-DLT maintainer should provide necessary capabilities, techniques, maintenances and functions of NRS-DLT under a scenario of network data sharing resources.
Figure and operational flows	 **Figure I.2 – Cross-system network data resources sharing based on NRS-DLT** 1) The network data resource provider should divide their own network data into two categories: public data and conditional sharing data, and clarify their sharing conditions, such as: the business relevance, business support of data resources and using time. 2) The metadata of network data resource is recorded by smart contract, then sharing conditions and resource locations are also recorded. 3) The resource requester publicizes the demand of network data resources, then query metadata of existing resources on the NRS-DLT, where metadata is a description of data resource items. 4) Apply for the data resources in NRS-DLT by smart contract, and provide key contents of using, include: purpose, time, etc. 5) NRS-DLT estimates the relevant usage condition automatically by smart contract, if the condition meets the requirements, NRS-DLT provides the data sharing interface (API) to the requester. 6) Within the allotted time, the resource requester uses data according to the sharing strategy. After using or after the allotted time, the sharing interface fails. The whole process is recorded in the distributed ledger for auditability and traceability.

Table I.2 – Use case of cross-system network data resource sharing based on NRS-DLT

Title	Use case of cross-system network data resource sharing based on NRS-DLT
Derived requirements	Requirements for network data resource provider: It is required that the provider ensures that metadata is consistent with the data in the database, so the requester could obtain the data according to the metadata. It is required that the provider have the capability to access resource control. Requirements for NRS-DLT: It is required that NRS-DLT provide computing nodes and adjust node computing resources, for example, to adjust more computing resources to consensus nodes or provider. It is required that NRS-DLT provide an alert service when nodes are short of computing resource. It is required that NRS-DLT automatically identify failed nodes by node management to ensure DLT network security. It is required that NRS-DLT provide sharing service management to manage the resource API from the NRP for resource sharing. It is required that NRS-DLT provide cross-system interaction for achieving resource sharing between different platform, which can be achieved by building cross-platform DLT network nodes.

Table I.3 – Use case of proximity-based service (ProSe) based on NRS-DLT

Title	Use case of proximity-based service (ProSe) based on DLT
Description	With the popularity of various intelligent terminals and 5G and 6G wireless connection access, network connection capacity is undergoing explosive growth, the original connection mode is facing challenges, and improving cellular frequency reuse has become a new solution. 3GPP proposes ProSe (proximity service), a new technology that allows LTE terminals to communicate directly from device to device (D2D) by sharing the network resources without infrastructure. In short, it is a new way of connection between two peer-to-peer user nodes under the network resource sharing mode. How to achieve secure and fair sharing of network resources between two untrusted nodes (under a weak trust environment) is an existing challenge. It is necessary to provide a suitable interconnection solution with high performance for ever-richer access and various networks to maximize network value through efficient sharing. Distributed ProSe based on DLT provides a suitable solution to address the trust and security problem in network resources sharing, to improve cellular frequency reuse.
Roles	Service node (ProSe provider): Contributor of the network resources. User node (ProSe requester): Demander of the network resources. Operator node (network resource administrator): Administrator of the network resource. NRS-DLT maintainer: The provider of NRS-DLT. The NRS-DLT maintainer should provide necessary capabilities, techniques, maintenances and functions of NRS-DLT under scenario of network sharing resources.

Table I.3 – Use case of proximity-based service (ProSe) based on NRS-DLT

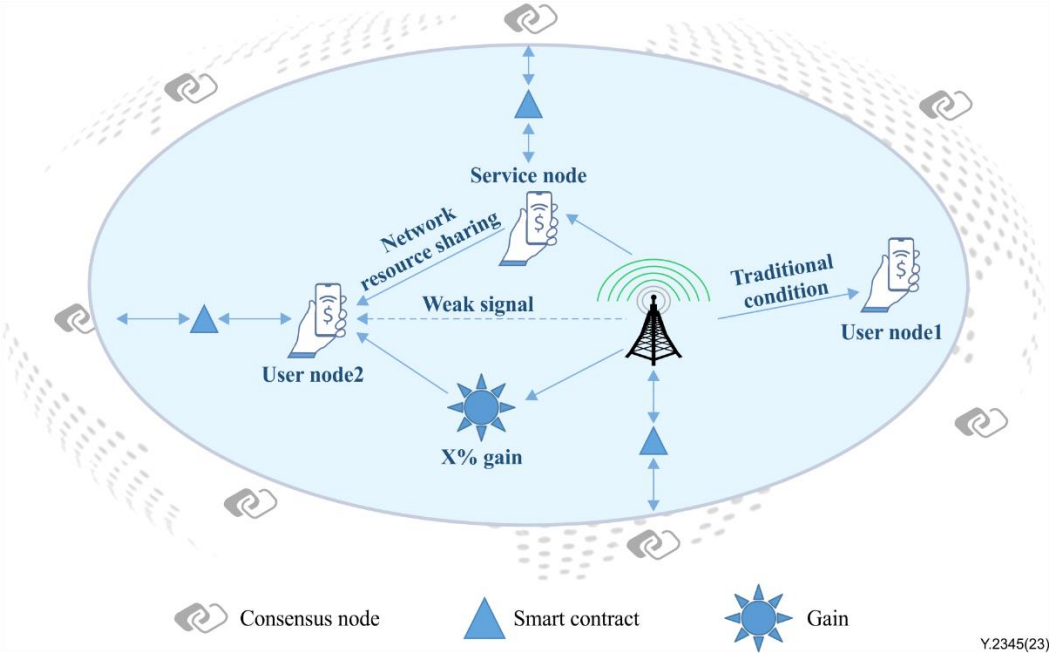
Title	Use case of proximity-based service (ProSe) based on DLT
Figure and operational flows	 **Figure I.3 – Proximity-based service (ProSe) based on NRS-DLT** Mobile users can register as a service node to share mobile network resources for other mobile terminals, so as to obtain the token. At the same time, it can also be used as a user node to obtain network services and pay for the token. 1) **Node registration**: Mobile phone users can apply for and register as hotspot service nodes, that is, network data resource providers, so as to directly share 5G network resources for other mobile terminals and provide near field network services. 2) **Identity authentication**: NRS-DLT records the registered nodes, and the smart contract transmits them to the operator for identity information comparison and authentication. 3) **Resource preparation**: The certified service nodes join the resource sharing pool through the app and open the hot spots. 4) **Recommendation of smart contract**: According to the current network quality, waiting time and historical evaluation, the smart contract recommends appropriate service nodes to network resource user nodes. 5) **Waiting for connection**: The user node makes its own choice according to the recommendation of the smart contract, and pays the token to the service node according to the rules of the smart contract to obtain the network service. 6) **Process record**: Until disconnection, the smart contract records the network resource sharing to the NRS-DLT, including: service node, user node, usage duration, network quality evaluation. 7) **Gain revenue**: For the completed services, according to the service duration and charging rules, the operator pays token to the service node to encourage more mobile users to participate in the ProSe, which can drive efficient and reliable frequency resource reuse, and improve the capacity of the 5G connection system.

Table I.3 – Use case of proximity-based service (ProSe) based on NRS-DLT

Title	Use case of proximity-based service (ProSe) based on DLT
Derived requirements	• Requirements for the ProSe provider: It is required that the ProSe provider ensure its identity is credible and verifiable. It is required that the ProSe provider provide stable services and not disconnect frequently. • Requirements for the ProSe user: It is required that the ProSe user provide enough tokens to pay for the service. • Requirements for the operator: It is required that the operator provide a database that contains identity information; in order to protect the data information, the database is stored locally and will be called by smart contract to comparison automatically. It is required that the operator provide the ability to monitor network resources. • Requirements for NRS-DLT: It is required that NRS-DLT provide the smart contract with recording, settlement, recommending, query functions. It is required that NRS-DLT provide identity protection for contributors. It is required that NRS-DLT provide a token-based incentives mechanism to stimulate increased node participation in ProSe based on NRS-DLT.

Bibliography

[b-ITU-T F.751.4] Recommendation ITU-T F.751.4 (2022), *General framework for distributed ledger technology (DLT)-based invoices*.

[b-ITU-T X.1405] Recommendation ITU-T X.1405 (2021), *Security threats and requirements for digital payment services based on distributed ledger technology*.

[3GPP WI #580059] 3GPP WI #580059[Rel 12], *Proximity-based service*.

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, 2023