

Recommendation

## **ITU-T Y.3082 (03/2023)**

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

Future networks

---

**Mobile network sharing based on distributed ledger technology for networks beyond IMT-2020 – Requirements and framework**



ITU-T Y-SERIES RECOMMENDATIONS

**GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES**

GLOBAL INFORMATION INFRASTRUCTURE

General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899

INTERNET PROTOCOL ASPECTS

General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999

NEXT GENERATION NETWORKS

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

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.3082

### Mobile network sharing based on distributed ledger technology for networks beyond IMT-2020 – Requirements and framework

#### Summary

Recommendation ITU-T Y.3082 specifies the requirements and framework of distributed ledger technology used in mobile network sharing for networks beyond IMT-2020. The detailed requirements of distributed ledger technology based mobile network sharing are put forward. The high-level framework, service procedures and security considerations are presented. The detailed use cases are described in the appendix.

#### History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.3082	2023-03-24	13	<a href="http://handle.itu.int/11.1002/1000/15246">11.1002/1000/15246</a>

#### Keywords

Distributed ledger technology, framework, mobile network sharing, requirements.

---

\* To access the Recommendation, type the URL <http://handle.itu.int/> in the address field of your web browser, followed by the Recommendation's unique ID. For example, <http://handle.itu.int/11.1002/1000/11830-en>.

## 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/>.

© ITU 2023

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

## Table of Contents

	<b>Page</b>
1 Scope .....	1
2 References.....	1
3 Definitions .....	1
3.1 Terms defined elsewhere .....	1
3.2 Terms defined in this Recommendation .....	2
4 Abbreviations and acronyms .....	2
5 Conventions .....	2
6 Introduction.....	3
7 Requirements of DLT based MNS.....	4
7.1 General high-level requirements of MNS-DLT .....	4
7.2 Capability requirements of MNS-DLT .....	5
8 High-level framework of DLT based MNS.....	6
8.1 Overview .....	6
8.2 DLT structure and properties.....	7
8.3 MNS-DLT enabling layer .....	7
8.4 MNS-DLT application layer .....	8
8.5 MNS-DLT management layer .....	8
9 Service procedures of DLT based MNS .....	9
9.1 Overview of service procedures .....	9
9.2 Service activation .....	10
9.3 Service deactivation .....	10
9.4 Service suspension .....	10
9.5 Service resumption.....	11
10 Security considerations .....	11
Appendix I – Use cases of DLT based MNS .....	12
I.1 Statistics of physical resource utilization acquirement .....	12
I.2 Fault reporting .....	12
I.3 Transport layer resource utilization acquirement.....	13
Bibliography .....	15



# Recommendation ITU-T Y.3082

## Mobile network sharing based on distributed ledger technology for networks beyond IMT-2020 – Requirements and framework

### 1 Scope

This Recommendation specifies the requirements and framework of credible mobile network sharing including site-sharing and radio access network (RAN) sharing, supported by distributed ledger technology for networks beyond IMT-2020.

The scope of this Recommendation includes:

- Requirements of distributed ledger technology based mobile network sharing
- High-level framework of distributed ledger technology based mobile network sharing
- Service procedures of distributed ledger technology based mobile network sharing
- Security considerations of distributed ledger technology based mobile network sharing
- Use cases of distributed ledger technology based mobile network sharing

### 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.1402] Recommendation ITU-T X.1402 (2020), *Security framework for distributed ledger technology*.

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

[ITU-T Y.4464] Recommendation ITU-T Y.4464 (2020), *Framework of blockchain of things as decentralized service platform*.

### 3 Definitions

#### 3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

**3.1.1 block** [b-ITU-T X.1400]: Individual data unit of a blockchain, composed of a collection of transactions and a block header.

NOTE – A block may be immutable and considered as the digital entity described in clause 3.2.2 of [b-ITU-T X.1255], however, it can be applied to other networks or other computational facilities.

**3.1.2 blockchain** [b-ITU-T X.1400]: 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.

**3.1.3 consensus** [b-ITU-T X.1400]: Agreement that a set of transactions is valid.

**3.1.4 consensus mechanism** [b-ITU-T X.1400]: Rules and procedures by which consensus is reached.

**3.1.5 distributed ledger** [b-ITU-T F.751.0]: A type of ledger that is shared, replicated, and synchronized in a distributed and decentralized manner.

NOTE – Originally published in [b-ITU-T TS FG DLT D1.1].

**3.1.6 identity** [b-ITU-T Y.2720]: Information about an entity that is sufficient to identify that entity in a particular context.

**3.1.7 IMT-2020** [b-ITU-T Y.3100]: Systems, system components, and related technologies that provide far more enhanced capabilities than those described in [b-ITU-R M.1645]

**3.1.8 participant** [b-ITU-T X.1400]: An actor who can access the ledger, read records or add records.

**3.1.9 service** [b-ITU-T Y.2091]: A set of functions and facilities offered to a user by a provider.

**3.1.10 smart contract** [b-ITU-T F.751.0]: Program written on the distributed ledger system which encodes the rules for specific types of distributed ledger system transactions in a way that can be validated, and triggered by specific conditions.

**3.1.11 transaction** [b-ITU-T L.1317]: Whole of the exchange of information between nodes. A transaction is uniquely identified by a transaction identifier.

## **3.2 Terms defined in this Recommendation**

None.

## **4 Abbreviations and acronyms**

This Recommendation uses the following abbreviations and acronyms:

AMF	Access and Mobility management Function
BS	Base Station
CAPEX	Capital Expenditure
DLT	Distributed Ledger Technology
EMS	Element Management System
IMT-2000	International Mobile Telecommunications-2000
MNS	Mobile Network Sharing
MOCN	Multi-Operator Core Network
NMS	Network Management System
OPEX	Operating Expense
OAM	Operation Administration and Maintenance
P2P	Peer to Peer
RAN	Radio Access Network

## **5 Conventions**

In this Recommendation:

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



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

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

## 6 Introduction

Networks beyond IMT-2020 are expected to achieve global telecommunication evolution and support a dramatic improvement in system capacities, performance and delays. Higher frequency spectrum will be utilized to meet the stringent application requirements. Thus, more base stations (BSs) should be deployed to cover the same area of IMT-2000, which leads to the high cost of infrastructure deployment for operators. Network sharing among the operators is the most feasible way to reduce the capital expenditure (CAPEX) and operating expense (OPEX).

Network sharing can be realized in several ways, such as sharing of site infrastructure and multi-operator core network (MOCN) mode. Sharing of site infrastructure is the most common form of network sharing, where multiple operators share site locations, equipment rooms, towers, etc., and each operator operates and maintains its network independently. MOCN mode means that a radio access network (RAN) can be connected to multiple operator core networks, and can be built by multiple operators in cooperation, or one of the operators can build the RAN alone, while other operators rent the operator's RAN.

The motivation for mobile network sharing (MNS) is to provide the enhanced capabilities to suit the new demands from the sharing mechanism. This is a good opportunity for MNS to evolve towards a distributed and trusted network with equal rights among each of the network sharing operators [ITU-T Y.2342]. MNS is expected to enhance the following three aspects:

- 1) Operation and maintenance processing of MNS,
- 2) data sharing among operators of MNS,
- 3) operation and maintenance management of MNS.

Distributed ledger technology (DLT) is considered as a promising technology to solve these problems in a secure, efficient and decentralized way. DLT enables distributed data storage in a chain of blocks with immutable features, thus it becomes easier for multiple operators to access data for different purposes. In addition, smart contracts, which contain the rules and agreements among operators, are employed in DLT to operate the stored data automatically, and the operation results are validated and agreed by all nodes. Therefore, it is feasible to deploy DLT in MNS.

In order to satisfy the specific requirements derived from the MNS scenarios, such as reliability, privacy protection and supervision. Considerations of DLT based MNS comprise the following three aspects.

- Operation and maintenance processing

In RAN sharing scenarios, the hosting operator is mainly responsible for the network performance and user experience. Hence, reliable and traceable information about network measurement, emergency reporting, fault localization and user priority configuration should be credible (tamper-proof and traceable) to avoid artificial modification. The advantages of DLT could solve the problem of information asymmetry, and provide a credible record and trust mechanism for the whole operation and maintenance process.

- Data sharing

The hosting operator is responsible for the construction and maintenance of the RAN network sharing, and provides the participating operators with operation and maintenance data query authority. There are a lot of data to be transmitted in the process of network sharing, including BS parameters (such as latitude, longitude, antenna height and direction), and measurement and inspection results. There are also a lot of data to be shared during the network operation, including the performance data, resource data, service statistics, tracking record data, etc. of the wireless network. Therefore, it is necessary to consider how to ensure the neutrality, trustworthiness, timeliness and accuracy of data transmission and sharing. DLT could be a potential solution to build the data sharing approach. The data sharing approach based DLT would be a decentralized, secure and multi-party participated data marketplace, where the data is aggregated, shared, exchanged and monetized in a distributed and credible manner.

- Operation and maintenance management

The network management capabilities for sending queries to obtain data about alarms, performance, configuration and user-level tracing are required to be exposed by the hosting operator. Although the participating operators could read these data, when a dispute arises there is no effective way to trace the data state at the problem causing moment. Based on the smart contracts and the consensus, operation and maintenance management capabilities of MNS are enhanced to achieve credibility by making the system tamper-proof and traceable to avoid intentional modification of data.

## 7 Requirements of DLT based MNS

### 7.1 General high-level requirements of MNS-DLT

The general high-level requirements of MNS-DLT are put forward to satisfy MNS basic service implementing, operation and maintenance.

#### 7.1.1 Roles and authority management

Table 7-1 provides requirements regarding roles and authority management.

**Table 7-1 – High-level requirements – Roles and authority management**

REQ-MNS-DLT-RAM	The MNS-DLT is required to support roles and authority management.
Description	In MNS scenarios, roles and authorities of multiple participants need to be defined. The roles management is responsible for assigning the actor roles of the participants. For example, hosting operator, participating operators and other participants. Authority management identifies applicable privileges for each role. The roles and authority management requirement is also responsible for revisiting and updating roles when changes are needed based on the negotiation among participants.

#### 7.1.2 Tamper-proof and traceable records

Table 7-2 provides requirements regarding tamper-proof and traceable records.

**Table 7-2 – High-level requirements – Tamper-proof and traceable records**

REQ-MNS-DLT-TTR	The MNS-DLT is required to support tamper-proof and traceable records for getting network information credibly.
Description	In MNS scenarios, it is necessary for MNS-DLT to avoid disputes among participants by providing tamper-proof and traceable records, such as network measurement, emergency report, fault localization and user priority

**Table 7-2 – High-level requirements – Tamper-proof and traceable records**

	configurations. Recorded network information cannot be modified artificially. In addition, all recorded information can be traced to its source and generation time.
--	--

### 7.1.3 Secure data sharing

Table 7-3 provides requirements regarding data sharing and security.

**Table 7-3 – High-level requirements – Secure data sharing**

REQ-MNS-DLT-DSS	The MNS-DLT is required to support a mechanism of secure data sharing.
Description	In the MNS process, network data (engineering parameters, performance data, resource data, service statistics, etc.) need to be transmitted, exchanged and aggregated. The secure data sharing mechanism should protect against loss, destruction or disclosure of the data in a distributed and credible manner, such as partition consensus and data encryption.

### 7.1.4 Action audit

Table 7-4 provides requirements regarding the action audit mechanism.

**Table 7-4 – High-level requirements – Action audit**

REQ-MNS-DLT-AA	The MNS-DLT is required to provide an action audit mechanism to ensure that each participant's operation is compliant with the MNS contract approved by other participants.
Description	In MNS scenarios, network parameters should be configured correctly by an action audit mechanism, in order to avoid network performance differences among operators and affecting the network experience of users. The audit mechanism is responsible for assuring that an action procedure is credible and transparent based on a consensus algorithm and smart contract.

## 7.2 Capability requirements of MNS-DLT

### 7.2.1 Interface capability

- It is required that the element management system (EMS) and sharable BS support MNS data collection interfaces.
- It is required to support interfaces between the EMS/sharable BS and DLT platforms.
- It is required to support interface adaptation capability, which provides both synchronous and asynchronous modes.

### 7.2.2 Distributed ledger capability

- It is required to support a decentralized and trustworthy system structure, in order to eliminate the fundamental vulnerabilities of a centralized system.
- It is required to support a distributed consensus mechanism for getting consensus among MNS nodes.
- It is required to support smart contracts capability to automatically perform agreements among participants, which promotes MNS application layer functions.

### 7.2.3 Detection and alarm capability

- It is required to support detection of MNS-related anomalies.

- It is required to support an alarm due to tampering with historical data, and support to automatically correct tampering.
- It is recommended to store MNS anomalies information on MNS-DLT nodes.

#### 7.2.4 Data collection and storage capability

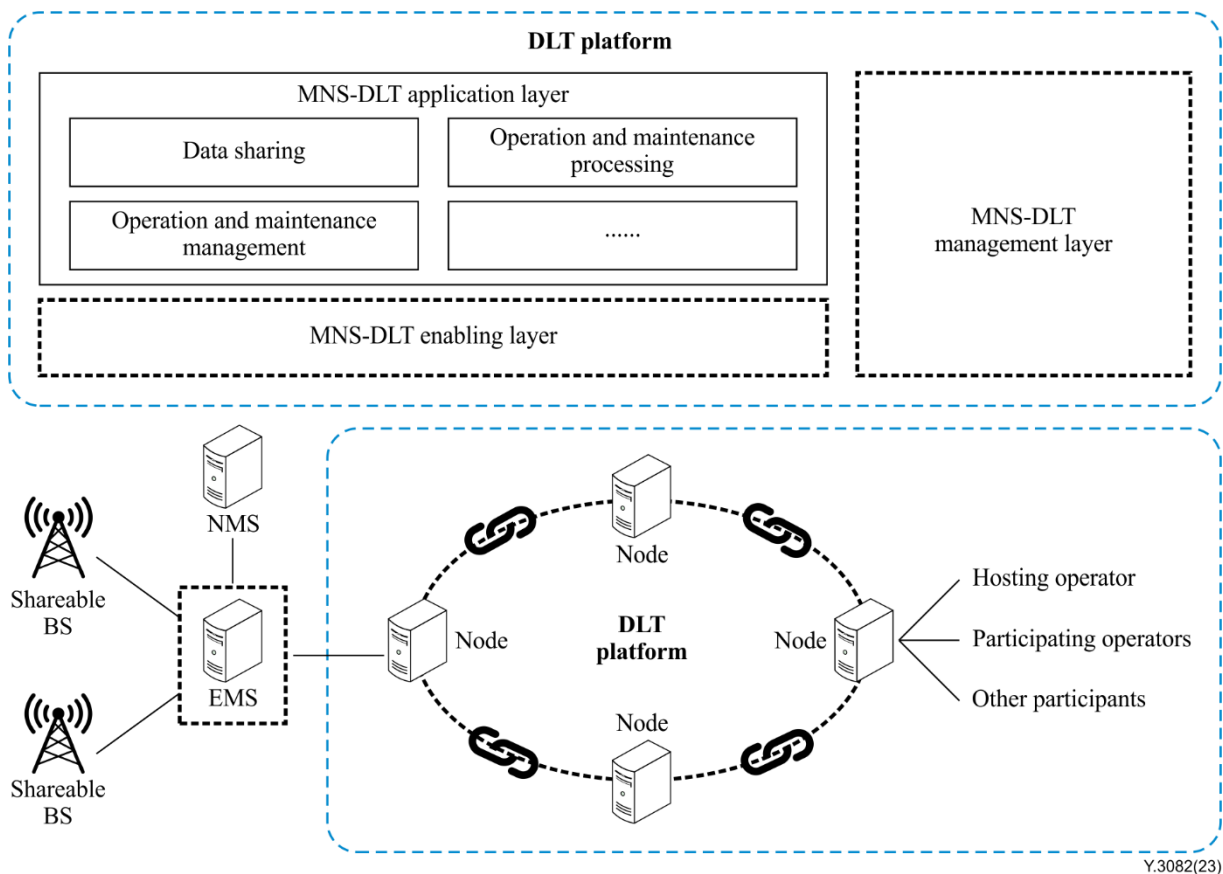
- It is required to collect shared data of the mobile network during the network operation and maintenance from the sharable BS/EMS, including the performance data, resource data, service statistics, engineering parameters, and tracking record data.
- It is required to store multi-source, heterogeneous MNS data. The storage adopts the structure of block chain. Additionally, the record storage supports various storage mediums, such as databases, file systems and cloud storage media.

#### 7.2.5 Data processing and backup capability

- It is required to support data encryption to protect the privacy of participants.
- It is required to support data backup to recover lost data of some nodes.

### 8 High-level framework of DLT based MNS

#### 8.1 Overview



**Figure 8-1 – Framework of DLT based MNS**

Figure 8-1 depicts the framework of DLT based MNS. Both the EMS and sharable BSs of the hosting operator can upload required information (such as cell load information, packet delay over air interface, and backhaul delay) to the DLT platform through the corresponding interfaces. Data with low latency requirements, such as real-time utilization of resources, is supposed to be uploaded via a sharable BS for rapid processing. Data without latency requirements or that needs to be further

processed by EMS, such as fault reporting, is preferably uploaded by EMS. The DLT platform is used to guarantee the trustworthiness and transparency, and avoid disputes among operators. Participating operators and non-operator participants can access to the DLT platform to get trusted data according to operators' policy and regulation needs. As shown in Figure 8-1, there are three functional layers in the MNS based DLT platform [ITU-T Y.4464], including the MNS-DLT enabling layer, MNS-DLT application layer, and MNS-DLT management layer.

## 8.2 DLT structure and properties

The structure of DLT is depicted in Figure 8-2. It enables distributed data storage in a chain of blocks. Each block is composed of a block header and a block body. The block header includes a hash value of the previous block, a Merkle root, timestamp and nonce value. The transaction records are stored in the block body. Each block is hashed and linked with other blocks, thus the content of each block is immutable. Another key property in DLT is the consensus mechanism. When a new block is appended to the chain of blocks, all the DLT nodes managed by participants must reach a consensus, which means that all the participants have equal rights to avoid security issues and maintain high immutability. In addition, smart contracts are used in DLT to operate the stored data automatically based on the predefined rules and agreements, which cannot be altered by any third party. This ensures high resistance to external attacks. DLT has the ability to achieve secure, immutable and decentralized data storage with low latency. It is also feasible to deploy DLT to provide a neutral platform for operators in MNS.

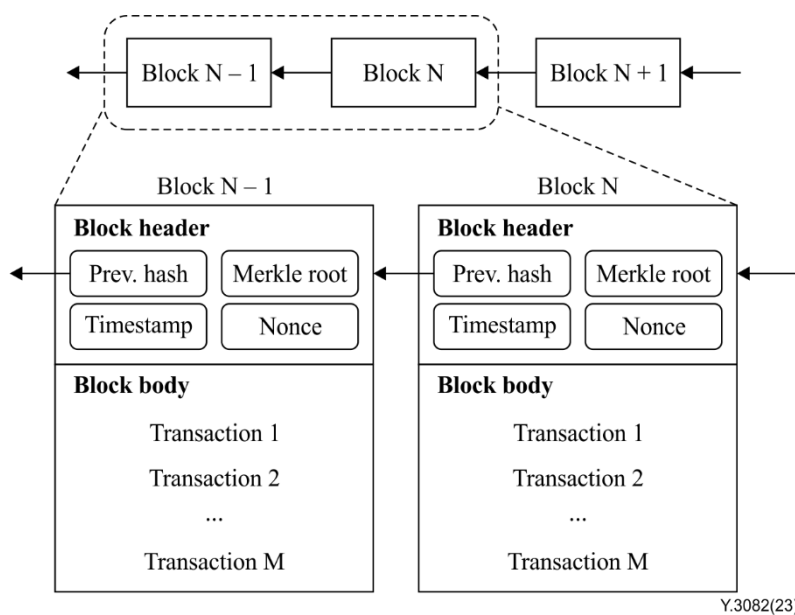


Figure 8-2 – DLT structure

## 8.3 MNS-DLT enabling layer

The MNS-DLT enabling layer is the most important part of the MNS based DLT framework since it provides the basic functions of DLT, which includes node connectivity, decentralized data collection, consensus mechanisms, smart contracts, and trustworthy data storage. Node connectivity ensures the connection and communication of network nodes. Each participant of the DLT based MNS is a node of the peer to peer (P2P) network, and can participate in activities such as network routing, DLT information verification, DLT information broadcasting and discovery of new nodes. In this distributed P2P network, each participating node can communicate with the other node to get the required information. The openness, decentralization and trustworthiness of the P2P network are guaranteed by the consensus mechanisms and smart contracts of DLT. This layer also provides the interface between the collected data and various MNS application services, so that the data can be further processed through consensus mechanisms and smart contracts to achieve trustworthy data

storage for the services. The data is synchronized and validated among the nodes to achieve consensus with the consensus mechanisms. The collected data privacy can be ensured by the encryption/decryption keys and algorithms.

#### **8.4 MNS-DLT application layer**

The MNS-DLT application layer provides support for specific decentralized MNS applications based on the service provided by the MNS-DLT enabling layer. Typical MNS applications include:

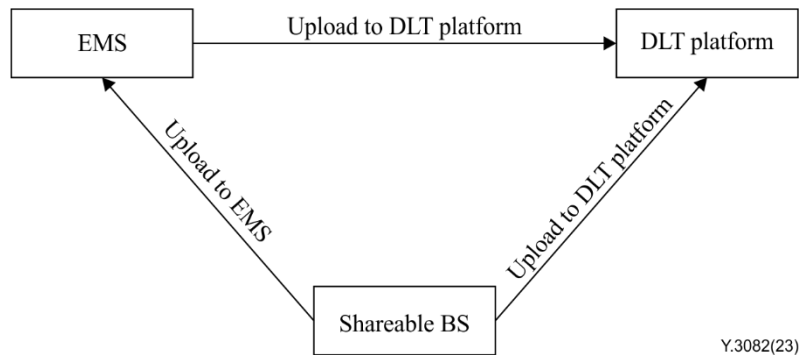
1. **Data sharing application:** In MNS, there are many data that need to be shared, such as resource data, performance index data, and tracking record data. Based on the trusted data provided by the MNS-DLT enabling layer, a data sharing application can be implemented.
2. **Operation and maintenance processing application:** In MNS, the hosting operator is responsible for maintenance and optimization of the sharing service, and takes the lead in fault handling. The participating operators are responsible for cooperating with fault handling and testing. Based on the smart contracts and traceable data provided by the MNS-DLT enabling layer, an operation and maintenance processing application with high-efficiency and high-transparency can be implemented.
3. **Operation and maintenance management application:** In MNS, the hosting operator is responsible for providing a query and export service, and the participating operators are allowed to access required data. Based on the smart contracts and traceable data provided by the MNS-DLT enabling layer, a credible operation and maintenance management application without manual intervention can be implemented.

#### **8.5 MNS-DLT management layer**

The MNS-DLT management layer includes management capabilities to operate the MNS-DLT and the applications established on the MNS-DLT, which provides the interface for the service subscribers of MNS-DLT to monitor the function status. This layer can provide management functions such as identity management, authorization management, access management, configuration management, and resource management. Through these functions, the service subscribers can view all the stored information for MNS, and search for desired records. The service subscribers can also view the node status of each participant, and provide the configuration information such as the selection of the consensus mechanism, network configuration, and authorization configuration. Each participant is assigned a unique identity to be monitored and can only access the whole system with access permission. When a fault occurs, the corresponding fault information is reported to the service subscribers. Resources such as computing resources and network resources are also allocated through this layer to meet the needs of each participant.

## 9 Service procedures of DLT based MNS

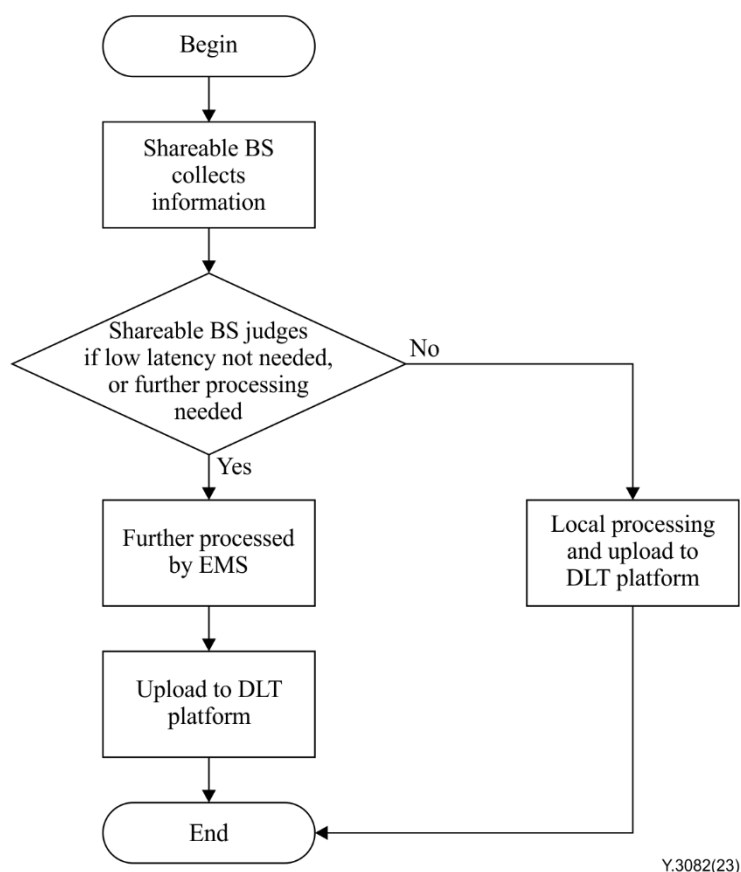
### 9.1 Overview of service procedures



**Figure 9-1 – Schematic diagram of service procedures**

A schematic diagram of the service procedure of the MNS based on DLT is shown in Figure 9-1. It includes EMS, sharable BS and DLT elements. Through the information interaction between EMS, DLT platform and sharable BS, both the EMS and sharable BS of the hosting operator can upload required information to the DLT platform according to service procedures. Service procedures of MNS based on DLT include service activation, service deactivation, service suspension and service resumption.

The flowchart of the sharing network data processing service is shown in Figure 9-2. Firstly, the sharable BS collects the required information (such as cell load information, packet delay over air interface, backhaul delay, etc.). Next, it needs to judge whether data with low latency requirements is supposed to be uploaded directly to the DLT platform for rapid processing and data without latency requirements, or if it needs to be further processed by EMS, which will be uploaded to EMS and then uploaded to the DLT platform.



**Figure 9-2 – Flowchart of data processing service**

## 9.2 Service activation

The DLT service activation procedure can be configured by the operation administration and maintenance (OAM) and triggered by the access and mobility management function (AMF), or configured and triggered by the OAM. The triggering node (AMF or OAM) then sends service activation information to the sharable BS through the interface between the BS and triggering node. The service activation information may include the DLT platform server address, uploaded data content, data format, service type, and the BS/UE ID. The delivery of service activation information to the BS can be achieved through interface messages. After receiving service activation information, the sharable BS will report this information to the DLT platform, or to the DLT platform via the EMS.

## 9.3 Service deactivation

The DLT service deactivation procedure can be configured by the OAM and triggered by the AMF, or configured and triggered by the OAM. The triggering node (AMF or OAM) then sends service deactivation information (server address, service type, BS/UE ID, etc.) to the sharable BS through the interface between the BS and triggering node. After the sharable BS receives the above service deactivation information, it terminates the DLT service and may report this information to the DLT platform.

## 9.4 Service suspension

When there are many requests and the available resources are not sufficient for the EMS/BS/DLT to deal with the requests in a short period of time, this situation causes suspension of the DLT service.

The DLT service suspension can be configured by the OAM and triggered by the AMF, or configured and triggered by the OAM. The triggering node (AMF or OAM) then sends the service suspension information (server address, service type, BS/UE ID, etc.) to the sharable BS. After the sharable BS



receives the above-mentioned DLT service suspension configuration information, it suspends the DLT service and may report this information to the DLT platform.

### **9.5 Service resumption**

Under suspension status, when enough resources become available to satisfy DLT service requests, the OAM or AMF can trigger the DLT service resumption process by sending the DLT service resumption information (server address, service type, BS/UE ID, etc.) to the sharable BS. After the sharable BS receives the above-mentioned DLT service resumption configuration information, it uploads the collected local measurement data and/or the measurement data collected from the UE to the DLT platform.

## **10 Security considerations**

This Recommendation specifies the requirements and framework for credible mobile network sharing including site-sharing and RAN-sharing, supported by distributed ledger technology for networks beyond IMT-2020. Therefore, it follows that the security considerations for distributed ledger technology identified in [ITU-T X.1402], which includes the security considerations on data security, network security, consensus security, and application security apply.

## Appendix I

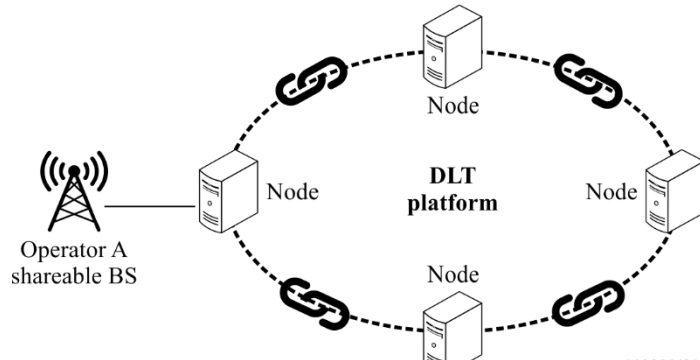
### Use cases of DLT based MNS

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

#### I.1 Statistics of physical resource utilization acquirement

Table I.1 describes the process for statistics of physical resource utilization acquirement.

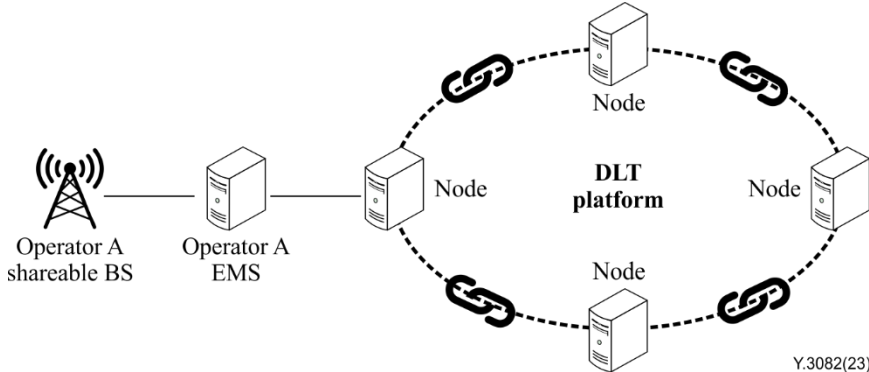
**Table I.1 – Statistics of physical resource utilization acquirement**

Title	Statistics of physical resource utilization acquirement
Description	The acquirement of statistics of physical resource utilization is essential for operators in MNS to get the utilization information of each operator. DLT is used to ensure the neutrality and trustworthiness of the statistics of physical resource utilization. Thus, participating operators and non-operator participants can acquire this information through the DLT platform. Furthermore, the hosting operator can optimize the allocation of system physical resources in a high-efficiency mode based on the operators' real resource occupancy from the DLT platform.
Pre-conditions (optional)	The sharable BS of hosting operator A is connected to the DLT platform.
Post-conditions (optional)	The statistics of physical resource utilization of each operator are stored in the DLT platform.
Figure and operational flows (optional)	<div style="text-align: center;">  <p style="text-align: right; font-size: small;">Y.3082(23)</p> </div> <p>BS: Base station DLT: Distributed ledger technology</p> <p>Operational flows:</p> <ol style="list-style-type: none"> <li>1. The sharable BS constructed by hosting operator A stores the statistics of physical resource utilization in the DLT platform.</li> <li>2. Participating operators and non-operator participants can acquire this information through the DLT platform.</li> </ol>
Derived requirements	Credible statistics of physical resource utilization should be acquired by the BS of hosting operator A.

#### I.2 Fault reporting

Table I.2 describes the fault reporting process.

**Table I.2 – Fault reporting**

Title	Fault reporting
Description	Trusted fault reporting can be achieved using DLT based MNS. The hosting operator is responsible for providing service to the customers of participating operators, and reporting the fault from those customers to the DLT platform to prove they are treated equally as the hosting operator's customers. Participating operators can acquire the fault reporting of their customers through the DLT platform.
Pre-conditions (optional)	The EMS of hosting operator A is connected to the DLT platform.
Post-conditions (optional)	The fault reporting is stored in the DLT platform.
Figure and operational flows (optional)	 <p>BS: Base station          EMS: Element management system          DLT: Distributed ledger technology</p> <p>Operational flows:          1. The sharable BS constructed by hosting operator A reports the fault to the EMS of hosting operator A.          2. The EMS of hosting operator A stores the fault reporting in the DLT platform.          3. Participating operators and non-operator participants can acquire the fault reporting through the DLT platform.</p>
Derived requirements	<ol style="list-style-type: none"> <li>1. Credible fault reporting should be acquired by the BS of hosting operator A.</li> <li>2. EMS could provide the fault reporting of BS.</li> </ol>

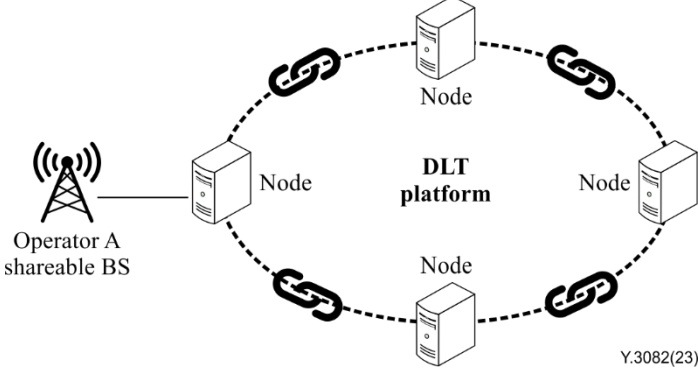
**I.3 Transport layer resource utilization acquirement**

Table I.3 describes the process for transport layer resource utilization acquirement.

**Table I.3 – Transport layer resource utilization acquirement**

Title	Transport layer resource utilization acquirement
Description	Participating operators and non-operator participants can acquire the transport layer resource utilization of each operator through the DLT platform. DLT is used to ensure the neutrality and trustworthiness of the transport layer resource utilization. Furthermore, the hosting operator can optimize the allocation of system transport layer resources in a high-efficiency mode based on the operators' real resource occupancy from the DLT platform.
Pre-conditions (optional)	The sharable BS of hosting operator A is connected to the DLT platform.
Post-conditions (optional)	The transport layer resource utilization is stored in the DLT platform.

**Table I.3 – Transport layer resource utilization acquirement**

Title	Transport layer resource utilization acquirement
Figure and operational flows (optional)	 <p>BS: Base station DLT: distributed ledger technology</p> <p>Operational flows:</p> <ol style="list-style-type: none"> <li>1. The shareable BS constructed by hosting operator A stores the transport layer resource utilization in the DLT platform.</li> <li>2. Participating operators and non-operator participants can acquire this information through the DLT platform.</li> </ol>
Derived requirements	Credible transport layer resource utilization should be acquired by the BS of hosting operator A.

## Bibliography

- [b-ITU-T F.751.0] Recommendation ITU-T F.751.0 (2020), *Requirements for distributed ledger systems.*
- [b-ITU-T L.1317] Recommendation ITU-T L.1317 (2021), *Guidelines on energy efficient blockchain systems.*
- [b-ITU-T X.1255] Recommendation ITU-T X.1255 (2013), *Framework for discovery of identity management information.*
- [b-ITU-T X.1400] Recommendation ITU-T X.1400 (2020), *Terms and definitions for distributed ledger technology.*
- [b-ITU-T Y.2091] Recommendation ITU-T Y.2091 (2011), *Terms and definitions for next generation networks.*
- [b-ITU-T Y.2720] Recommendation ITU-T Y.2720 (2009), *NGN identity management framework.*
- [b-ITU-T Y.3100] Recommendation ITU-T Y.3100 (2017), *Terms and definitions for IMT-2020 network.*
- [b-ITU-R M.1645] Recommendation ITU-R M.1645 (2005), *Framework and overall objectives of the future development of IMT-2000 and systems beyond IMT-2000.*
- [b-ITU-R M.2083] Recommendation ITU-R M.2083 (2015), *Framework and overall objectives of the future development of IMT for 2020 and beyond.*
- [b-ITU-T TS FG DLT D1.1] Technical Specification ITU-T FG DLT D1.1 (2019), *Distributed ledger technology terms and definitions.*





## 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
<b>Series Y</b>	<b>Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities</b>
Series Z	Languages and general software aspects for telecommunication systems