

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2342

(12/2019)

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 capability requirements of
blockchain in next generation network evolution**

Recommendation ITU-T Y.2342



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
Network control architectures and protocols	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.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.2342

Scenarios and capability requirements of blockchain in next generation network evolution

Summary

Recommendation ITU-T Y.2342 presents an analysis of the motivations and scenarios of blockchain used in the next generation network evolution (NGNe). The general high-level requirements of blockchain in NGNe are put forward. Detailed descriptions of the use cases are listed in the appendix. This Recommendation provides the framework of the blockchain for NGNe and specifies the capability requirements that meet the needs of next generation network (NGN) and the blockchain framework. The framework provided in this Recommendation is intended for NGNe as defined in Recommendation ITU-T Y.2340, however, it could be applied as appropriate to other types of telecom networks (e.g., IMT-2020 and Future Network).

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.2342	2019-12-14	13	11.1002/1000/14128

Keywords

Blockchain, consensus, decentralization, general framework, ledger, network evolution, next generation, smart contract.

* 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, 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 TSB patent database at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2020

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

	Page
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	3
6 Introduction of NGNe-BC	3
6.1 Background and motivations	3
6.2 NGNe-BC overview	4
7 Scenarios and requirements of NGNe-BC.....	5
7.1 Scenario description	5
7.2 General high-level requirements of NGNe-BC	6
7.3 General requirements of NGNe	8
8 General framework and capability requirements of NGNe-BC	8
8.1 General framework of NGNe-BC	8
8.2 NGNe-BC application layer capability requirements.....	9
8.3 NGNe-BC platform layer capability requirements.....	9
8.4 NGNe-BC network layer capability requirements	11
8.5 NGNe-BC infrastructure layer capability requirements	11
8.6 NGNe-BC management capability requirements	11
8.7 NGNe-BC Cross layer capability requirements	13
9 Security consideration	14
Appendix I – Use Cases of NGNe-BC.....	15
I.1 NGNe-BC use case of international roaming	15
I.2 NGNe-BC use case of mobile number portability	16
I.3 NGNe-BC use case of data sharing	18
I.4 NGNe-BC use case of network elements management.....	20
I.5 NGNe-BC use case of MSISDN as a service	22
Bibliography.....	24

Recommendation ITU-T Y.2342

Scenarios and capability requirements of blockchain in next generation network evolution

1 Scope

This Recommendation provides the framework of the blockchain for next generation network evolution (NGNe) and specifies the capability requirements that meet the needs of next generation network (NGN) and the blockchain framework. This Recommendation covers the following aspects:

- Motivations and scenarios of the blockchain in the next generation network evolution (NGNe).
- High-level requirements of the blockchain in the NGNe based on the scenarios.
- General framework and capability requirements of the blockchain in the NGNe.

This Recommendation also provides an appendix describing:

- Use cases of blockchain in the NGNe.

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

[ITU-T Y.2012] Recommendation ITU-T Y.2012 (2010), *Functional requirements and architecture of next generation networks*.

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

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

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

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

3.1.2 block [b-ITU-T FG-DLT-D1.1]: Individual data unit of a blockchain, composed of a collection of transactions and a block header.

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

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

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

3.1.5 consensus mechanism [b-ITU-T FG-DLT-D1.1]: Rules and procedures by which consensus is reached.

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

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

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

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

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API	Application Programming Interface
BC	Blockchain
CA	Certificate Authority
CDR	Call Detail Record
DCH	Data Clearing Houses
DDoS	Distributed Denial-of-Service
DLT	Distributed Ledger Technology
DNS	Domain Name System
HPMN	Home Public Mobile Network
KYC	Know Your Customer
MNO	Mobile Network Operator
MNP	Mobile Number Portability
MSISDN	Mobile Subscriber International ISDN Number
NGN	Next Generation Network
NGNe	Next Generation Network Evolution
NGNe-BC	NGNe-Blockchain
OTT	Over The Top
P2P	Peer to Peer

PBFT	Practical Byzantine Fault Tolerance
PoS	Proof of Stake
PoW	Proof of Work
SIM	Subscriber Identification Module
SMS	Short Message Service
TAP	Transferred Account Procedures
TEE	Trust Execution Environment
VPMN	Visited Public Mobile 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.

In the body of this document and its annexes, the words shall, shall not, should, and may sometimes appear, in which case they are to be interpreted respectively as, is required to, is prohibited from, is recommended, and can optionally. The appearance of such phrases or keywords in an appendix or in material explicitly marked as informative are to be interpreted as having no normative intent.

6 Introduction of NGNe-blockchain (NGNe-BC)

6.1 Background and motivations

Next generation network (NGN) [ITU-T Y.2012] is a packet-based network which is able to provide telecommunication services with decoupled service-related functions and underlying transport-related technologies. The NGN is naturally distributed both nationwide and worldwide. Equality and interconnection are the essential attributes between and even within the NGNs. However, due to the distrust between the NGN operators, centralized intermediary functions are deployed, such as the clearing houses for the international roaming mobile number portability database among the NGN operators and even the root domain name system (DNS) for interconnection and roaming. The centralized intermediary functions on one hand bring additional costs, and on the other hand lead to security issues for superimposing centralized functions over the distributed networks. In addition, the NGN has abundant network data resources which could be shared to improve and innovate the applications for the industry, however, it is hard to create the application ecosystem due to the distrust between the NGN operators and the application developers when making use of the network data.

NGN evolution (NGNe) [ITU-T Y.2340] is a non-stop long-term project. The motivation for NGN evolution is to provide the enhanced capabilities to suit the new demands from industry based on the NGN infrastructure. It is a good opportunity for NGN to evolve towards a distributed and trusted network with equal rights among each NGN operators. The NGNe is expected to be enhanced in the following three aspects: 1) collaborative relationship among the NGNeS;

2) collaborative relationship between the NGNs and the industry participants; 3) collaborative relationship between the NGN and the applications. Blockchain is considered as the candidate technology.

The blockchain leverages the block-chain structure to store transactions and data in a decentralized way, and uses cryptography to ensure the security of the transmission and access. The blockchain could achieve consistent data records, anti-tampering/non-repudiation and failure-resistance. With the blockchain, applications can operate in a decentralized manner, without the need for a central authority and a trusted intermediary. Moreover, smart contract, a piece of self-executing program which resides on the blockchain, could provide distributed and automated workflows. The blockchain is not a specific technology, but a collection of technologies, such as cryptography, peer to peer (P2P), distributed system, distributed storage, consensus mechanisms, and so on.

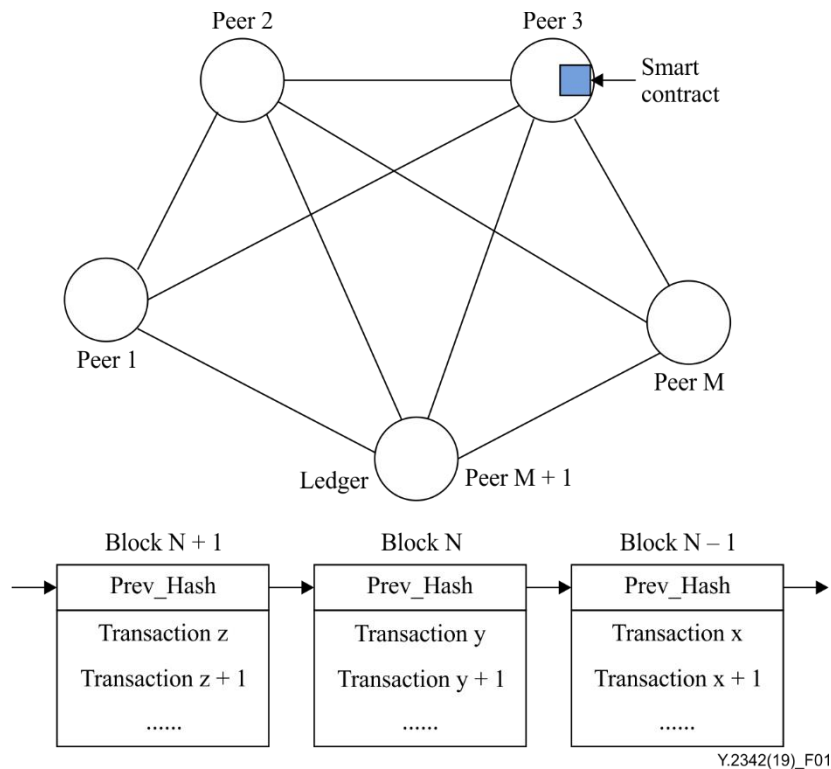


Figure 1 – Blockchain overview

As illustrated in Figure 1, the blockchain mainly comprises the blockchain ledger, the blockchain network and smart contract mechanism. The blockchain ledger is a chain of blocks which record the transactions (or data record entries). The block is the smallest storage unit, which is generated by the peer node after collecting and sequencing new transactions. To guarantee the immutability, usually the transactions are organized in the form of a Merkle hash tree and the root hash is included in each block head domain. Before adding a block to the blockchain ledger, a consensus process is needed among the peer nodes, such as proof of work (PoW), proof of stake (PoS) or practical byzantine fault tolerance (PBFT), etc. The blockchain network is a P2P network, which interconnects all peer nodes in a mesh network. The peer nodes broadcast and synchronize the transactions and blocks to achieve a consensus of the blockchain ledger. The smart contract mechanism provides the program to operate the data of the ledger and the execution environment for the program. The smart contracts can enable decentralized applications and services based on the data from the blockchain ledger.

6.2 NGNe-BC overview

NGNe-blockchain (NGNe-BC) is a specific blockchain which is utilized in NGNe, satisfying the specific requirements derived from the NGNe scenarios, such as reliability, privacy protection, supervision, etc. NGNe-BC supports the features of NGN/NGNe and has enhancements taking advantage of the blockchain concept and technologies. NGNe-BC comprises three types as follows:

- **Public NGNe-BC:** a NGNe-BC which allows any participants to access the ledger for reading/writing the data records, operating the smart contract and carrying out the consensus.
- **Consortium NGNe-BC:** a NGNe-BC which only allows the approved participants to access the ledger for reading/writing the data records, operating the smart contracts and carrying out the consensus.

NOTE 1 – The consortium NGNe-BC protects the data privacy of the participants depending on the policies.

NOTE 2 – The consortium NGNe-BC may restrict the privileges of the participants to read/write the ledger data, and operate the smart contracts.

- **Private NGNe-BC:** a NGNe-BC which only allows the approved participants in the same NGNe to access the ledger for reading/writing the data records, operating the smart contracts and optionally carrying out the consensus.

The NGNe-BC is complementary to NGNe by providing the decentralized application capability. Figure 2 shows the relationship between the NGN and the NGNe-BC. The applications and services based on NGNe-BC may have impacts on different function domains of NGN, as shown in Figure 2 the shading of the colour represents the degree of influence in general terms, e.g., the dark colour means deep influence. Appendix I provides typical use cases of NGNe-BC.

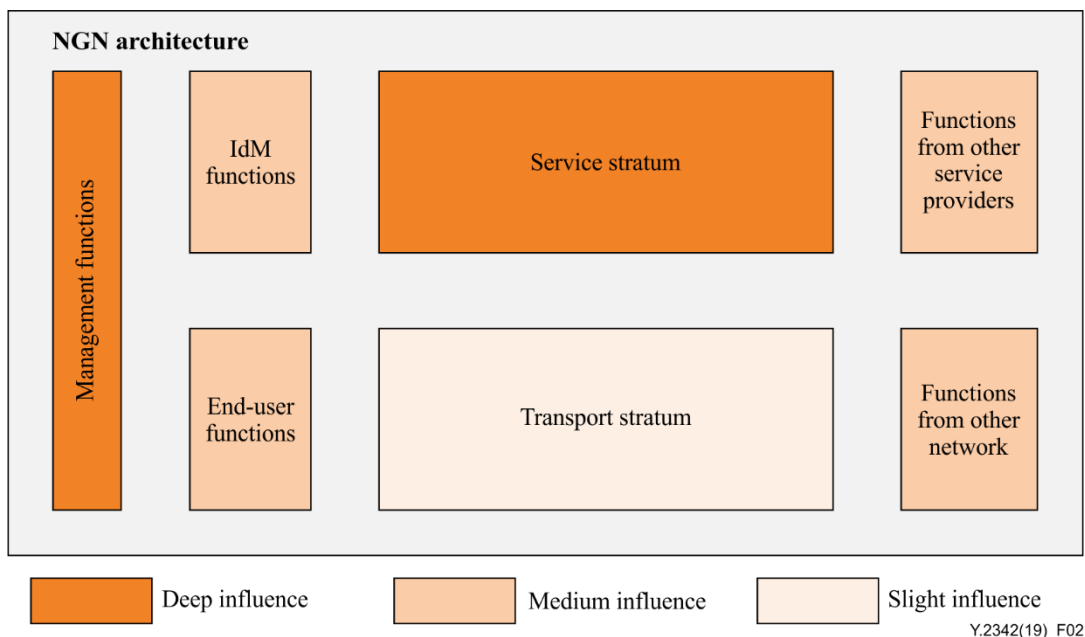


Figure 2 – Relationship of NGNe-BC with the NGN

7 Scenarios and requirements of NGNe-BC

7.1 Scenario description

The NGNe-BC could be adopted in coupled applications and services in NGNe. These applications and services could be assigned to different areas, thus it is necessary to categorize the scenarios to summarize the requirements. Considering the NGNe-BC feature of enabling trust in a trustless environment, the scenarios are divided into four categories, i.e., within the NGNe, between NGNe,

between NGNe and customers and between NGNe and other networks, based on the relationship between the NGNe-BC participants.

7.1.1 Within the NGNe

In this scenario, the applications and services based on the NGNe-BC are mainly used for self enhancement and optimization of NGNe. Hence, the participants of the NGNe-BC are the entities within the NGNe, e.g., network entities or administration entities. The NGNe-BC could be a consortium NGNe-BC or private NGNe-BC since the participants needed to be approved to access the ledger.

Appendix I.4 is an example of this type of scenario. Appendix I.3 also could be an example of this type of scenario if the participants are all entities in the NGNe.

7.1.2 Between NGNs

Currently there are interoperability requirements between multiple NGNs. Taking the roaming and interconnection as an example, usually it is time costly to negotiate and to archive an agreement between the NGNs, and financially costly to settle up through a clearing house. The NGNe-BC is promising to develop the decentralized applications and services between NGNs both nationwide and globally to enhance the current systems.

Furthermore, the NGNs naturally have the alliance attribute. This is because combined NGNs could serve more customers, which would generate new innovative services leveraging the NGNe-BC.

The NGNe-BC would be a consortium NGNe-BC in this scenario where all participants are equal and permissioned. For efficient coordination, there is optionally a management union coexisting with and independent of the consortium NGNe-BC.

Appendices I.1 and I.2 are examples of this type of scenario.

7.1.3 Between NGNe and customers

The NGNe-BC could serve as an application infrastructure between NGNe and customers for sharing data and resources. For example, the customers could share the storage, bandwidth and even computing resources, thus the NGNe could distribute the applications, such as the video content, to the edge of the network to reduce the burden on the backbone network and having to settle and clear in close to real-time. Moreover, the customers not only refer to the personal customers but also the enterprise customers. The enterprise customers could share data with NGNe, e.g., the status information of NB-IoT smart parking lot, on the NGNe-BC infrastructure to incubate new business.

In this scenario, the NGNe-BC could be a consortium NGNe-BC or a public NGNe-BC since the number of the participants joined in the NGNe-BC may be large.

7.1.4 Between NGNe and other networks

Usually there is a data sharing demand between an NGNe and other networks, e.g., regulator/government networks, service provider networks and enterprise networks, etc. However, the data sharing demand is hindered by the lack of trust between the NGNe and other networks.

The data could be shared unidirectionally by the NGNe, such as the data for lawful interception to the regulator or the authentication data to the service provider as described in Appendix I.5. The data such as the security vulnerability information could also be shared between the NGNe and other networks.

In addition, the NGNe-BC could be used for data and record traceability when the NGNe and the other networks do not trust each other.

In this scenario, the NGNe-BC would be mainly a consortium NGNe-BC.

7.2 General high-level requirements of NGNe-BC

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

7.2.1 Account and membership management

The NGNe-BC is required to support the account and membership management. The account management is responsible for recording the active status of the participants, and if applicable the ownership status. The membership management provides the functions of the member identification, access control, authorization and authentication management, etc.

The account and membership management requirement is not only applicable for the consortium and private NGNe-BC but also for the public NGNe-BC for the operation and maintenance.

7.2.2 Scalability

The NGNe-BC is required to provide sufficient scalability.

In NGNe-BC, the NGNe-BC node is an entity to execute all or part of the NGNe-BC function. However, the function granularity of the NGNe-BC node depends on the implementation. The NGNe-BC node can join in and quit the NGNe-BC without degrading the read-write throughput and impacting the other NGNe-BC nodes. Moreover, the consensus mechanism in the NGNe-BC is pluggable, and the NGNe-BC nodes can be separated into different clusters using different consensus mechanisms.

7.2.3 Maintenance management

The NGNe-BC is required to provide maintenance management capabilities to guarantee long-term stable operation of the services running over the NGNe-BC.

- **NGNe-BC node management**

The NGNe-BC node management is required to have a global view of the NGNe-BC, such as the node number, node type, block generation status of the nodes, active status, node topology, etc.

Optionally, the NGNe-BC node management could be a centralized system coexisting with the NGNe-BC in parallel.
- **Configuration management**

The configuration management is required to provide the initial default and updated configuration information and parameters to the NGNe-BC nodes, such as the software version, the ledger setting, consensus module selection, and so on.
- **Monitoring and alarm**

The NGNe-BC is required to provide monitoring and alarm capabilities. The NGNe-BC could keep monitoring the node status, the broadcasted messages status, the block generation status, the throughput performance and other parameters. When a predefined abnormal situation occurs, the NGNe-BC could receive the alarm information.
- **Block information query**

The NGNe-BC is required to have the capabilities to query the block and transaction information, and to generate statistical results which could be used for the system operation.

7.2.4 Auditability

The NGNe-BC is required to support data auditability to fulfil the regulation requirements. The NGNe-BC could provide the data operation record and log access in the condition of meeting the regulatory compliance.

7.2.5 Failure and disaster recovery

The NGNe-BC is required to have a failure and disaster recovery mechanism.

It is necessary for the NGNe-BC to provide the disaster recovery system to guarantee uninterrupted service, e.g., the automatic recovery of the smart contract and the redundant backup of the data stored locality.

It is also necessary for the NGNe-BC to resist risk caused by fault configuration and operation. The NGNe-BC is required to discover the abnormal behaviour node and recover in a timely fashion.

7.2.6 Data privacy

The NGNe-BC is required to provide a data privacy protection mechanism. The protection methods may be various and in different dimensions, e.g., isolating the NGNe-BC nodes and establishing multiple message broadcast channels for different services, data encryption between the participants.

7.2.7 NGNe-BC smart contract management

The NGNe-BC is required to provide smart contract management. In NGNe-BC, the NGNe-BC smart contract is a piece of program code which is recorded on NGNe-BC and can be self-executing based on the data of NGNe-BC ledger. The NGNe-BC applications are able to trigger the execution of NGNe-BC smart contracts. In this case, the NGNe-BC smart contract is a data reading/writing interface between the NGNe-BC applications and the ledger.

It is necessary for the NGNe-BC smart contract to be identified, which includes the owner, version, function, the updated history, etc. To recover the service quickly from a failure, the NGNe-BC could maintain a smart contract depository.

7.3 General requirements of NGNe

Since the applications and services based on the NGNe-BC are derived from NGNe scenarios, the NGNe is taken as part of applications.

The NGNe is required to provide a capability to read/write the application related data entries from/to the NGNe-BC ledger.

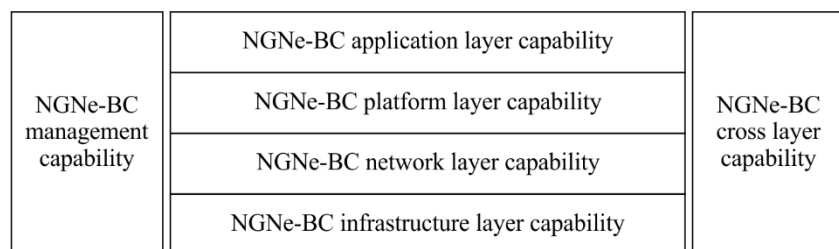
The NGNe is required to provide a capability to invoke/enable/update/disable the smart contracts according to the application function requirements.

The NGNe is required to provide a capability to integrate the NGNe-BC smart contracts to the workflow existed for backward compatibility.

The NGNe is required to provide normalized data format for the transactions recorded in the ledger.

8 General framework and capability requirements of NGNe-BC

8.1 General framework of NGNe-BC



Y.2342(19)_F03

Figure 3 – Framework of NGNe-BC

The general framework of NGNe-BC includes six capability sets, which are the infrastructure layer capability, network layer capability, platform layer capability, application layer capability, NGNe-BC management capability and cross layer capability as shown in Figure 3.

- NGNe-BC infrastructure layer capability: the NGNe-BC infrastructure layer capability provides the resource required to deploy the NGNe-BC nodes. The resource includes the computation, storage and network.
- NGNe-BC network layer capability: the NGNe-BC network layer capability is responsible for the peer to peer communication which is used for ledger synchronization. In addition, the interaction between the NGNe-BC nodes, e.g., the ledger node and the smart contract execution node, relies on the network layer function.
- NGNe-BC platform layer capability: the NGNe-BC platform layer capability provides the basic functions of blockchain including the ledger, consensus mechanism, membership and smart contract. Furthermore, the platform layer provides the uniform interface to the application layer by encapsulating the call of reading/writing the ledger and initializing/invoking the smart contract.
- NGNe-BC application layer capability: the NGNe-BC application layer capability provides the applications and services derived from the NGNe.
- NGNe-BC management capability: the NGNe-BC management capability includes the management capabilities to operate the NGNe-BC and the applications established on the NGNe-BC.
- NGNe-BC cross layer capability: the NGNe-BC cross layer capability aims to implement the functions that need the cooperation of multiple layers.

8.2 NGNe-BC application layer capability requirements

The NGNe-BC application layer capability provides specific services running over the NGNe-BC to the users, such as mobile number portability (MNP), the roaming settlement, etc. The services may make use of the NGNe-BC partially or adopt the NGNe-BC completely to establish the application architecture. The application layer is the source to read/write data from/to the NGNe-BC, and also the drive to carry out incentive if applicable. Generally, the application layer implements the service logic and completes the data processing.

It is required to provide a capability for defining the data format stored in the NGNe-BC.

It is required to provide a capability for coordinating the processing of the data stored in the NGNe-BC and other centralized database in the same service architecture.

It is required to provide a capability for managing the secret key and encryption algorithm to guarantee the data privacy.

It is required to provide the UI or wallet between the user and the NGNe-BC ledger, including account operation, authentication, asset operation and personal privacy data granted if applicable.

8.3 NGNe-BC platform layer capability requirements

The NGNe-BC platform layer capability is the core in the NGNe-BC framework as it provides the basic service features and execution environment. There are multi-dimensional capabilities the platform layer provides such as the application programming interface (API) capability, membership capability, ledger capability, consensus capability and smart contract capability, etc.

- API capability

The API capability is the interface between the service and the NGNe-BC, which is the only method for the application layer accessing and managing the data in the ledger and the smart contracts.

It is required to provide a capability for an encapsulated interface to the application layer for reading and writing the data from/to the ledger.

It is required to provide a capability for an encapsulated interface to the application layer for deploying, initializing, invoking and updating the smart contracts.

- Membership capability

The membership capability is responsible for the access control and authorization management of the NGNe-BC participants.

It is required to provide a capability to grant and examine the authorization of the participant to read and write the ledger and query the account information.

It is required to provide a capability to grant and examine the authorization of the participant to deploy, initialize, invoke and update the smart contracts.

It is recommended to provide a capability to store the encryption/decryption key and execute an encryption/decryption algorithm to protect the data privacy.

- Ledger capability

The ledger capability is mainly used for the data and transactions/records storage and validation.

It is required to provide a capability to store the data and transactions/records in a blockchain structure to guarantee the integrity and time sequence.

It is required to provide a capability to guarantee the data and transactions/records in a block are appropriately organized, e.g., the Merkle tree, to resist the tampering.

It is required to provide a capability to validate the data stored in the ledger rapidly.

It is required to provide a capability to query and locate a specific transaction/record from the ledger rapidly.

- Consensus capability

The consensus capability implements the consensus mechanisms to guarantee the consistency of the ledger data stored in different NGNe-BC nodes.

It is required to provide a consensus capability which is energy efficient to reduce the energy consumption.

It is required to provide a consensus capability which could synchronize and validate the data or transactions/records and reach the consensus status rapidly in order to obtain a high performance.

It is required to provide a consensus capability which is scalable for adding or reducing the consensus nodes without decreasing the system performance.

It is required to provide a consensus capability which could maintain the system stability and correctness when the number of the malfunctioning or malicious nodes is less than a predefined proportion value.

It is required to provide a consensus capability which could resist Sybil and distributed denial-of-service (DDoS) attack.

It is required to provide a consensus capability which implements pluggable consensus algorithms.

It is required to provide a consensus capability which could assign different consensus methods for different NGNe-BC network and NGNe-BC nodes.

- Smart contract capability

The smart contract capability implements the smart contract execution environment and smart contract management.

It is required to provide the execution environment which includes the computing resource, storage, I/O and network resource for the smart contracts. If applicable, the execution environment of the smart contracts is recommended to be the trust execution environment (TEE) to protect the sensitive data of the ledger.

It is required to provide a capability to manage the deployment, termination and update of the smart contracts.

It is required to provide a capability to check the execution status of the smart contracts.

It is required to provide a capability to allow the smart contracts accessing to the ledger to obtain the data or update the data in the ledger according to the execution results of the smart contracts.

It is required to provide a capability to deliver the event notification generated by the smart contracts to the application layer.

It is required to provide a capability to suspend the smart contracts execution to resist resource occupation attacks.

It is required to provide a capability to detect and find the vulnerabilities of the smart contracts.

- Interoperation capability

The interoperation capability allows the NGNe-BC to obtain the necessary data from the source out of the ledger, e.g., leveraging the second layer protocols or oracle.

It is required to provide a capability to interact with other blockchains and the off-chain data source.

8.4 NGNe-BC network layer capability requirements

The NGNe-BC network layer capability implements the communications between the NGNe-BC nodes, mainly focusing on the network reachability and the message broadcast.

It is required to provide a capability to build a P2P network for equal message dissemination among the NGNe-BC nodes.

It is required to provide a capability to discover the NGNe-BC nodes automatically in a neighbourhood without the pre-configuration.

It is required to provide a capability to maintain the system stability in case the NGNe-BC nodes are in and out frequently.

It is required to provide a capability to evaluate the feasibility of providing a NGNe-BC node based on the consideration of not impacting other NGNe-BC nodes.

8.5 NGNe-BC infrastructure layer capability requirements

The infrastructure layer capability is required to provide the computing/storage/networking resource for the NGNe-BC nodes. The computing/storage/networking resource could be physical or virtualized.

It is required to provide a capability to recover from disaster and hardware/software malfunctions rapidly by triggering automated healing.

It is required to provide a capability to be able to evaluate automated optimization results of the computing/storage/networking resource for the NGNe-BC nodes.

It is recommended to provide specific capabilities which could accelerate the services deployment, such as database and encryption/decryption.

8.6 NGNe-BC management capability requirements

The management capability in the NGNe-BC framework includes multiple capabilities which help to maintain and monitor the operation of the NGNe-BC. The management capabilities could be deployed centralized or together with the NGNe-BC nodes. The management capabilities include the blockchain information inquiry capability, the topology view capability, the configuration management capability, the monitoring and alarm capability, the account management capability, the CA management capability, the IaaS resource management capability, which are important for the applications based on the NGNe-BC to guarantee the steady running and timely troubleshooting.

- Blockchain information inquiry capability

The blockchain information inquiry capability is the interface for the operators of NGNe-BC services to view the status of the NGNe-BC.

It is required to provide a capability to view all of the blocks and transaction information.

It is required to provide a capability to search for and return the exact blocks and transactions based on keywords and the combination of the keywords.

It is required to provide a capability to present or deliver the inquiry results to the operators.

It is required to provide a capability to view all of the smart contract information.

- Topology view capability

The topology view capability provides the NGNe-BC nodes topology and status view.

It is required to provide a capability to collect the online/offline status of the NGNe-BC nodes and present the overall status view.

It is recommended to provide a capability to generate a topology view of the NGNe-BC nodes based on the NGNe-BC node identities.

- Configuration management capability

The configuration management capability provides the configuration function for the NGNe-BC node.

It is required to provide a capability for manually configuring the NGNe-BC node, such as the network configuration, the consensus algorithm selection, the node identity and authorization and access configuration, etc.

It is required to provide a capability for automatically configuring the NGNe-BC node, such as downloading and enabling the configuration profiles from a centralized node management entity.

- Monitoring and alarm capability

The monitoring and alarm capability enables the operator and maintenance engineer of the NGNe-BC services to keep tracking the operating status of the system.

It is required to provide a capability to monitor the NGNe-BC node operating status, such as the resource occupation status, the network connection status, etc.

It is required to provide a capability to monitor the NGN-BC operating status, such as the generation rate of the block, the generation rate of the transaction, the message broadcasted status and so forth.

It is required to provide a capability to monitor the service related operating status based on the NGN-BC, such as the reading/writing status from/to the ledger, the deployment status of the smart contract.

It is required to provide a capability for an alarm based on monitoring depending on a predefined threshold.

- Account management capability

The account management capability provides the account related management for the services based NGNe-BC. The account management module could be divided between the centralized part and the node accompanied part.

It is required to provide a capability to create a new account and retrieve the account when the password/private key is lost for the participant.

It is required to provide a capability to manage the account related parameters, such as the basic participant information, the access permission, the secret key for the data privacy protection and access permission, the smart contract updated record, the digital asset if applicable and so on.

It is required to provide a capability to apply the Certificate Authority (CA) and update the access permission to inquire after some specific transaction data.

It is required to provide a capability to allow deployment of the smart contract.

- CA management capability

The CA management capability is responsible for the CA issue in the NGNe-BC. The CA management module could be logically deployed in a centralized way.

It is required to provide a capability to issue the CA to the NGNe-BC nodes to access the NGNe-BC.

- IaaS resource management capability

The IaaS resource management capability is required to provide a capability to allocate computing/storage/network resources according to demand to the NGNe-BC node.

It is required to provide a capability to monitor the resource usage of the NGNe-BC node.

8.7 NGNe-BC Cross layer capability requirements

The NGNe-BC cross layer capability is used to implement specific functions which need the cooperation of multiple layers in the NGNe-BC framework. The cross layer capability could include the privacy protection capability, the regulation capability, the policy capability and the big data/AI capability, etc.

- Privacy protection capability

It is necessary to protect the privacy of the NGNe-BC participants to avoid exposing the sensitive data.

It is required to provide a capability to allow the sensitive data to be read only by the participants authorized.

It is required to provide a capability to broadcast the messages including the sensitive data among specific participants.

It is required to provide a capability to leverage efficient security algorithms such as ring signature and zero knowledge proof to avoid the privacy data exposure.

- Regulation capability

It is necessary to fulfil the audit requirements from the organizations and government.

It is required to provide a capability to collect and deliver the operation logs, ledger data, smart contract logs and other information required according to the audit requirements.

- Policy capability

The policy capability is utilized by the NGNe-BC to implement the intervention to the transaction and the smart contract execution.

The policy module is required to provide a capability to mark the data storage in the NGNe-BC ledger for intervention according to the policies and regulations.

- Big data/AI capability

It is recommended to provide a capability to analyse the operation and maintenance data to optimize the performance of the NGNe-BC.

9 Security consideration

This Recommendation is considered as an enhancement of NGNe, thus it supports the security features for NGN and follows the security considerations identified in [ITU-T Y.2701] and [ITU-T Y.2340]. In addition, since the NGNe-BC could be underlying technology for lot of applications, it is necessary for the NGNe-BC to meet the security requirements of the specific applications.

Appendix I

Use cases of NGNe-BC

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

I.1 NGNe-BC use case of international roaming

Title	NGNe-BC use case of international mobile roaming
Description	<p>International mobile roaming is a service that allows mobile users to continue to use their mobile phone for voice, data and message services, while visiting another country. Traditionally, international mobile roaming needs to be negotiated by participating operators with an agreement to use data clearing houses (DCH) for accounting and billing purposes. There are some disadvantages of using DCH in practice:</p> <ol style="list-style-type: none"> 1) Both home public mobile networks (HPMNs) and visited public mobile networks (VPMNs) have to pay hefty fees to DCH as the central authority to execute the contract for roaming services. 2) Roaming rated call detail records (CDRs) are exchanged in terms of transferred account procedures (TAP) files in offline mode which leads to delays in billing and hence revenue sharing among the roaming partners. 3) The dispute resolution processes are long because it is also executed offline by the DCH by validating the CDRs and contracts of both the partners. <p>However, the consortium NGNe-BC could be implemented between every pair of operators which have a roaming agreement. HPMN and VPMN could have an instantaneous settlement using blockchain-based smart contracts which take away the offline billing information exchange between roaming partners through DCH, resulting in great cost savings.</p>
Chain's type	Consortium NGNe-BC, which includes operators' accounting and billing nodes.
Pre-conditions (optional)	Participating operators' international mobile roaming CDR nodes have already joined the NGNe-BC.
Post-conditions (optional)	None.
Figure and operational flows (optional)	<p style="text-align: center;"> CDR generator NGNe-BC node Smart contract </p> <p style="text-align: right; font-size: small;">Y.2342(19)_FI.Tab1</p>

	<p>Operational flows:</p> <p>When the mobile subscriber roaming in a visited network uses the mobile services, it triggers the CDR Generator to generate CDR.</p> <p>The CDR Generator broadcasts the CDR information as a transaction to the NGNe-BC node in its home realm, and triggers the execution of the smart contracts.</p> <p>The smart contract verifies the CDR (e.g., the data format), and appends this CDR to the NGNe-BC ledger. Then the CDR is also synchronized to other NGNe-BC ledger nodes through the consensus procedure. The smart contract could have more functions such as real-time settlement and payment, and validation of usage in VPMN.</p>
Derived requirements	<p>Requirements for NGNe:</p> <p>It is required that the NGNe provides the capability to identify international mobile roaming events, and send the CDR to the NGNe-BC ledger node.</p> <p>It is required that the NGNe provides normalized data format for the transactions recorded in the ledger.</p> <p>Requirements for NGNe-BC:</p> <p>It is required that the NGNe-BC provides the smart contracts to implement the settlement.</p> <p>It is required that the NGNe-BC provides the ledger to record the bills of the roaming.</p> <p>It is required that the NGNe-BC provides the consensus mechanism to guarantee the consistent bill records.</p> <p>It is required that the NGNe-BC provides sufficient reading/writing performance from/to the ledger.</p>

I.2 NGNe-BC use case of mobile number portability

Title	NGNe-BC use case of mobile number portability
Description	<p>Mobile number portability (MNP) is an important service in NGNe, which enables users to keep their mobile telephone number when changing from one mobile network operator to another. It is necessary to build an intermediary database for the mobile operators to synchronize the status of mobile numbers provisioned by the MNP service to provide the correct service routing. The intermediary database has direct impact on the basic telecommunication services of the mobile operator:</p> <ol style="list-style-type: none"> 1) The intermediary database has the risk of single point failure. 2) Serial verification procedure for leveraging intermediary database means there is a long period for provisioning the MNP service. 3) For the 3rd party service providers, such as the Internet APPs, real-time synchronization of the mobile number status is important, e.g., when using the short message service (SMS) verification code. 4) The intermediary database needs a new operation and maintenance entity independent of any of the mobile operators. <p>Therefore, the MNP needs a database which could be accessed by multiple participants and meet the real-time synchronization of the mobile number status.</p>
Chain's type	Consortium NGNe-BC, which is built among multiple mobile operators supporting the MNP. The regulators and 3 rd party service providers could join the consortium NGNe-BC.
Pre-conditions (optional)	<ol style="list-style-type: none"> 1) The mobile network operators support the MNP service. 2) The regulator has the requirements to supervise the mobile number utilization. 3) The 3rd party service providers are sensitive to the reachability of the mobile subscribers via the mobile number.

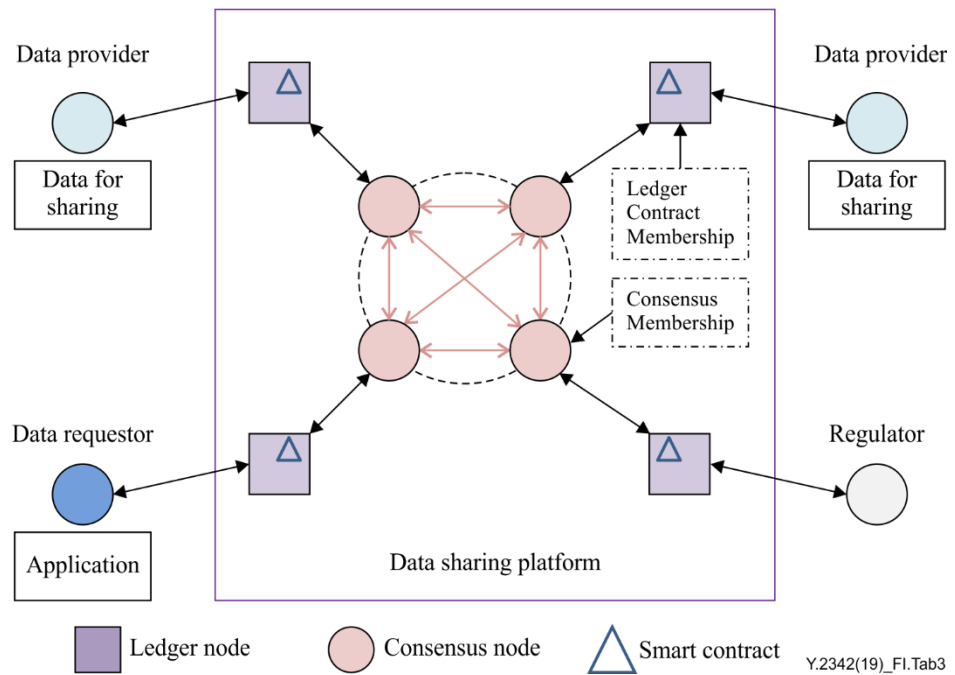
Post-conditions (optional)	None.
Figure and operational flows (optional)	<div data-bbox="502 257 1372 1108" data-label="Diagram"> <p style="text-align: right; font-size: small;">Y.2342(19)_FI.Tab2</p> </div> <p data-bbox="446 1120 670 1153">Operational flows:</p> <ol data-bbox="446 1153 1436 1792" style="list-style-type: none"> 1) A subscriber of the mobile operator A applies to provision the MNP service to change mobile network operator A to mobile network operator B at the MNP service provision node. 2) The MNP service provision node provides necessary transaction parameters including the mobile number, the account status, source mobile operator ID, targeted mobile operator ID, etc., to the consensus/ledger node. 3) The consensus/ledger nodes verify the MNP service application, record the transaction, consent the block and add the block to the ledger. 4) The service networks of mobile network operator A/B make use of the records in the distributed ledgers to route the calls and messages correctly for the mobile numbers ported. 5) The regulator could supervise the transactions and ledger. For specific transactions, the regulator could participant in the consensus based on the policies previously defined. 6) The 3rd party service providers could access the ledger maintained locally and keep up with statuses of the mobile number porting in real time, as the distributed ledgers are updated nearly at the same time in a consortium NGNe-BC.

Derived requirements	<p>Requirements for NGNe: It is required that the NGNe provides the capability to record the MNP number and necessary transaction parameters to the NGNe-BC ledger.</p> <p>Requirements for NGNe-BC: It is required that the NGNe-BC provides the ledger to record the MNP numbers. It is required that the NGNe-BC provides the consensus mechanism to guarantee the consistent record.</p> <p>It is required that the NGNe-BC provides sufficient reading/writing performance from/to the ledger.</p> <p>It is required that the NGNe-BC provides the smart contracts to implement the MNP numbers reading/writing.</p> <p>It is required that the NGNe-BC provides the access control and membership management.</p> <p>It is required that the NGNe-BC provides necessary privacy protection of the MNP data and regulation capability.</p>
----------------------	---

I.3 NGNe-BC use case of data sharing

Title	NGNe-BC use case of data sharing
Description	<p>There is plenty of high value data in the operator networks, such as the identity, location, bill, terminal and access status data, etc. On one hand the data could be used in network optimization and service experience improvement for both the operators and over the top (OTT) service providers; on the other hand, the data could be exchanged and monetized for supporting credit investigation, risk management, marketing, and innovative services of the 3rd party.</p> <p>However, the data is scattered in different domains of the operator network, e.g., BSS, OSS, core network, access network, which leads to the data islands and makes it hard to aggregate the different dimensions data. The centralized data sharing platform is not only costly, but also has security risk on managing the costumer's data and tracing the data transactions. Most importantly, the data sharing should have tight control on the privacy and sensitive data, by avoiding to access to the raw data itself.</p> <p>The NGNe-BC could be a potential solution to build the data sharing platform. The data sharing platform based NGNe-BC would be a decentralized, secure and multi-party participated data marketplace, where the data is aggregated, shared, exchanged and monetized in a distributed manner.</p>
Chain's type	Consortium NGNe-BC, which includes the data providers, the data requesters and the regulators.
Pre-conditions (optional)	<ol style="list-style-type: none"> 1) The data providers and the data requesters have got the certificates from the regulator, and access to the NGNe-BC. 2) The data provider registers the data for sharing on the NGNe-BC, which could include the data characteristic description, the data format, the data digest, and also smart contract address processing the data requests and the reference of the data stored off-chain optionally.
Post-conditions (optional)	None.

Figure and operational flows (optional)



Y.2342(19)_FI.Tab3

Operational flows:

- 1) The data requestor inputs the keywords on the web client which connects to the ledger nodes to search the sharing data information, which could include the data characteristic description, the data format, the data digest, smart contract address, price, etc. The data requestor selects the data to purchase.
- 2) The data requestor accesses the smart contract deployed by the data provider for processing the shared data and applies for the data.
- 3) Depending on the data type, the smart contract may have different actions:
 - i) For the static data without privacy and sensitive information, the smart contract may return the data reference directly;
 - ii) For the static data with privacy and sensitive information, the smart contract only returns an analysis result but not the raw data, in this case, the data requestor need deploy a smart contract to execute the analysis;
 - iii) For the dynamic data, the smart contract only returns an analysis result but not the raw data, in this case, the data requestor need deploy a smart contract to execute the analysis.
- 4) The smart contract returns the data or the analysis result, and completes the payment. The transaction is recorded in the NGNe-BC for auditability and traceability. The data sharing process completes.
- 5) For example, the finance company who provides loans online could be the potential data requestors. While the NGNe operators could be the data providers. The finance company raises the requests to the NGNe operators to evaluate the credit conditions of its customers based on the bills data of the subscribers leveraging specific analysis algorithms. The finance company pays for the data exchange to the NGNe operators.

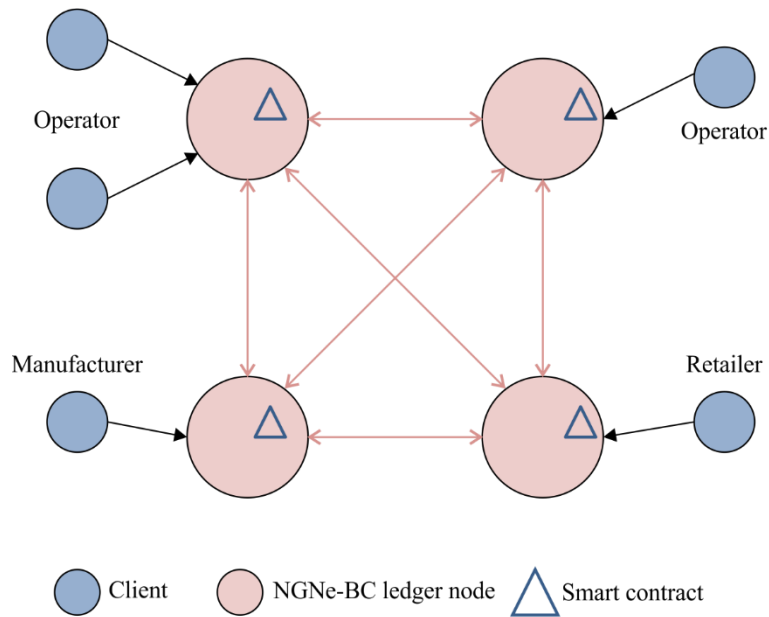
The data for sharing may be stored on-chain or off-chain depending on the data property and polices. The NGNe-BC provides the execution environment and computing resource for the smart contracts which could contain complex logic.

Derived requirements	<p>Requirements for NGNe: It is required that the NGNe provides the capability to collect the data for sharing and record the data to the NGNe-BC ledger.</p> <p>Requirements for NGNe-BC: It is required that the NGNe-BC provides the ledger to record the data for exchange.</p> <p>It is required that the NGNe-BC provides the consensus mechanism to guarantee the consistent record.</p> <p>It is required that the NGNe-BC provides sufficient reading/writing performance from/to the ledger.</p> <p>It is required that the NGNe-BC provides the smart contracts to implement the data entries reading/writing, and transaction billing if applicable.</p> <p>It is required that the NGNe-BC provides the access control and membership management.</p>
----------------------	--

I.4 NGNe-BC use case of network elements management

Title	NGNe-BC use case of network elements management
Description	<p>In NGNe there are thousands of items of network equipment supplied by hundreds of manufacturers and retailers. As an important asset, it is necessary for the operators to manage the network equipment effectively and clearly.</p> <p>It is necessary to keep consistency between the operators and the manufacturers on the records of the purchased network equipment to avoid disputes, especially when the equipment needs repair and replacement. The record could include pictures, certification, serial numbers, manufacturer identity, and so on.</p> <p>In addition, the network equipment, both on the network side and on the subscriber side, should be traced in their lifecycle from being deployed to when they are removed from the network.</p> <p>Leveraging NGNe-BC, each item of network equipment both in physical and virtual manner has a specific management thread to record the equipment characteristic and status such as deploying, relocating, changing and removing. That makes the network elements management transparent, traceable and trustworthy.</p>
Chain's type	Consortium NGNe-BC or private NGNe-BC, which includes the NGNe operators, the manufacturers and retailers.
Pre-conditions (optional)	The NGNe operators, the manufacturers and retailers have access to the NGNe-BC.
Post-conditions (optional)	None.

Figure and operational flows (optional)



Y.2342(19)_FI.Tab4

Operational flows:

- 1) The manufacturer and retailer record the purchased network equipment to the NGNe-BC through specific smart contracts leveraging the clients. The smart contract restricts the read privilege of the manufacturer and retailer. The information recorded includes the equipment characteristic such as serial number, manufacturer identity, certification, and so on.
- 2) The NGNe operator records the status of the network equipment deploying, relocating, changing and removing through smart contract leveraging the clients. The records would be shared between all the NGNe-BC ledger nodes.
- 3) The NGNe operator queries the network equipment by serial number or searches the network equipment by keywords using smart contract.

Derived requirements

Requirements for NGNe:

It is required that the NGNe provides the capability to record network elements and necessary transaction parameters to the NGNe-BC ledger.

Requirements for NGNe-BC:

It is required that the NGNe-BC provides the ledger to record the network elements.

It is required that the NGNe-BC provides the consensus mechanism to guarantee the consistent record.

It is required that the NGNe-BC provides sufficient reading/writing performance from/to the ledger.

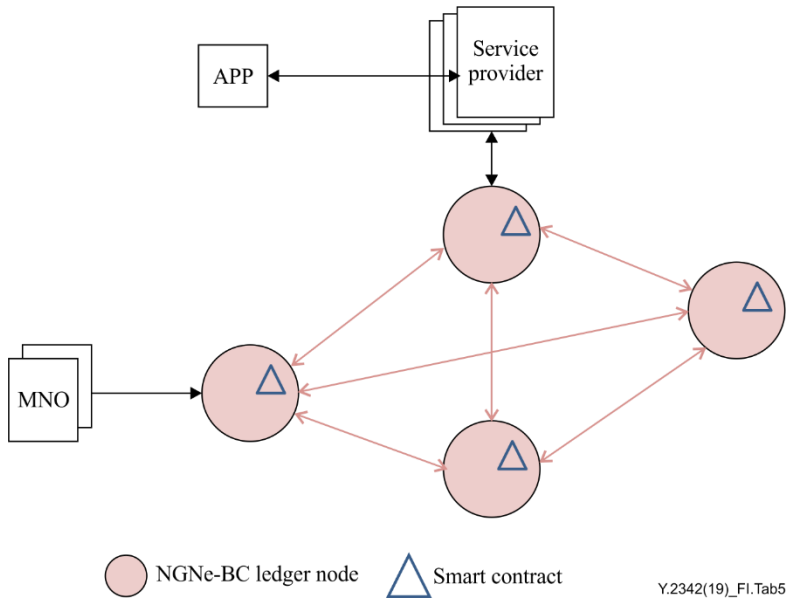
It is required that the NGNe-BC provides the smart contracts to implement the data entries reading/writing.

It is required that the NGNe-BC provides the access control, membership management and authority management.

It is required that the NGNe-BC provides the scalability.

It is required that the NGNe-BC provides the account management.

I.5 NGNe-BC use case of MSISDN as a service

Title	NGNe-BC use case of MSISDN as a service
Description	<p>Digital identity is increasingly important on the Internet. Firstly, for the service providers, it is difficult and costly to develop new customers, especially when the service needs the customer to register and has know your customer (KYC) processes to prove the identity and credential of the customers. Secondly, for the customers, it can be a lot of trouble to remember dozens of account names and passwords. Currently, the service providers allow customers to leverage their accounts of Google, Facebook and Wechat to login and use the APPs, however these accounts may not have KYC processes, which may incur the risk of identity theft, fraudulent purchases and data theft.</p> <p>Mobile subscriber international ISDN number (MSISDN) could be used as a digital identity, as it is unique globally and the customer is verified when applying to use the MSISDN. Based on the NGNe-BC, the NGNe operators could provide the MSISDN-as-a-service, which includes the mobile authentication and account information, etc., to the service providers.</p>
Chain's type	Consortium NGNe-BC, which includes the NGNe operators and service providers.
Pre-conditions (optional)	<ol style="list-style-type: none"> 1) The NGNe operator and the service providers have access to the NGNe-BC. 2) The NGNe operator has uploaded the raw data or the reference of data stored to the NGNe-BC. The data may include the subscriber identification module (SIM) authentication information and user data profile. Depending on the implementation, the reference of the data stored off-chain instead of the raw data could be uploaded. Multiple mobile network operators (MNOs) could share the same NGNe-BC.
Post-conditions (optional)	None.
Figure and operational flows (optional)	 <p>Operational flows:</p> <ol style="list-style-type: none"> 1) The APP accesses to the service provider with the MSISDN as the account name. The access authentication could be SIM-based if the SIM profile and algorithm could be accessed leveraging the smart contract on the NGNe-BC. 2) The service provider could query the user profile of the MSISDN through a smart contract if necessary, such as initial verification or dispute.

	<p>3) The service provider could generate a temporary token which is used for next login in a period after a successful authentication.</p> <p>Depending on the implementation, the access authentication for the APP also can use SMS code.</p>
Derived requirements	<p>Requirements for NGNe: It is required that the NGNe provides the capability to record n MSISDN related data to the NGNe-BC ledger.</p> <p>Requirements for NGNe-BC: It is required that the NGNe-BC provides the ledger to record MSISDN related data.</p> <p>It is required that the NGNe-BC provides the consensus mechanism to guarantee the consistent record.</p> <p>It is required that the NGNe-BC provides sufficient reading/writing performance from/to the ledger.</p> <p>It is required that the NGNe-BC provides the smart contracts to implement the data entries reading/writing.</p> <p>It is required that the NGNe-BC provides the access control, membership management and authority management.</p> <p>It is required that the NGNe-BC provides the privacy protection.</p> <p>It is required that the NGNe-BC provides the scalability.</p>

Bibliography

- [b-ITU-T X.1255] Recommendation ITU-T X.1255 (2013), *Framework for discovery of identity management information*.
- [b-ITU-T FG-DLT-D1.1] Technical Specification FG DLT D1.1 (2019), *Distributed ledger technology terms and definitions*.
<https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d11.pdf>

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