

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



International
Telecommunication
Union
Documents

Document Sharing Hub

ITU-T

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 NGNe;

2) collaborative relationship between the NGNs and the industry participants; 3) collaborative relationship between the NGNe 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.

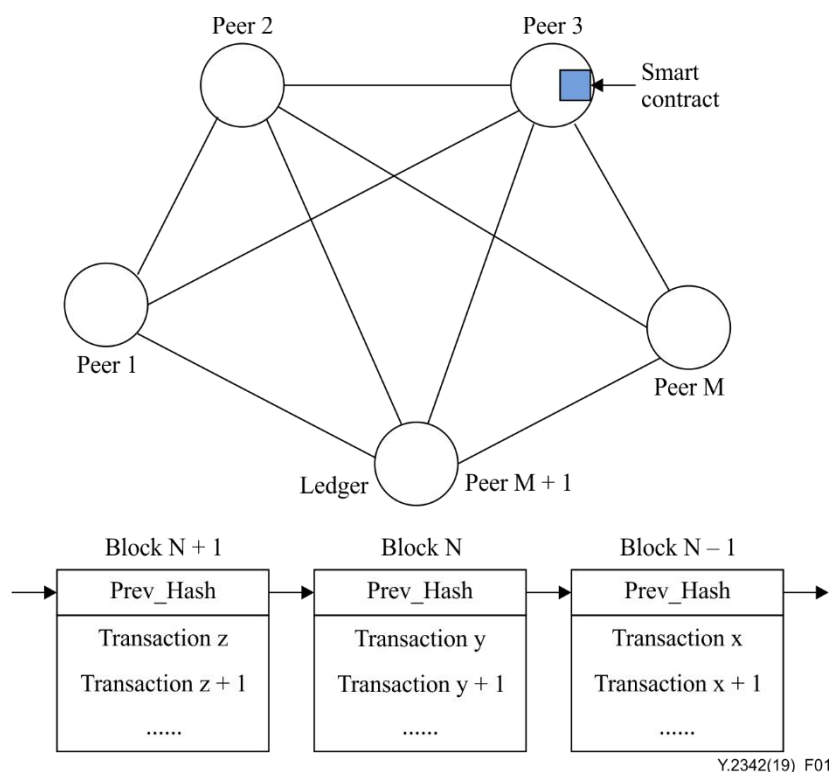


Figure 1 – Blockchain overview

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.