ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

ITU-T Q.4046 (12/2023)

SERIES Q: Switching and signalling, and associated measurements and tests

Testing specifications – Testing specifications for Cloud computing

---

Interoperability testing requirements of blockchain as a service

ITU-T Q-SERIES RECOMMENDATIONS

Switching and signalling, and associated measurements and tests

SIGNALLING IN THE INTERNATIONAL MANUAL SERVICE	Q.1-Q.3
INTERNATIONAL AUTOMATIC AND SEMI-AUTOMATIC WORKING	Q.4-Q.59
FUNCTIONS AND INFORMATION FLOWS FOR SERVICES IN THE ISDN	Q.60-Q.99
CLAUSES APPLICABLE TO ITU-T STANDARD SYSTEMS	Q.100-Q.119
SPECIFICATIONS OF SIGNALLING SYSTEMS NO. 4, 5, 6, R1 AND R2	Q.120-Q.499
DIGITAL EXCHANGES	Q.500-Q.599
INTERWORKING OF SIGNALLING SYSTEMS	Q.600-Q.699
SPECIFICATIONS OF SIGNALLING SYSTEM NO. 7	Q.700-Q.799
Q3 INTERFACE	Q.800-Q.849
DIGITAL SUBSCRIBER SIGNALLING SYSTEM NO. 1	Q.850-Q.999
PUBLIC LAND MOBILE NETWORK	Q.1000-Q.1099
INTERWORKING WITH SATELLITE MOBILE SYSTEMS	Q.1100-Q.1199
INTELLIGENT NETWORK	Q.1200-Q.1699
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR IMT-2000	Q.1700-Q.1799
SPECIFICATIONS OF SIGNALLING RELATED TO BEARER INDEPENDENT CALL CONTROL (BICC)	Q.1900-Q.1999
BROADBAND ISDN	Q.2000-Q.2999
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR THE NGN	Q.3000-Q.3709
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR SDN	Q.3710-Q.3899
TESTING SPECIFICATIONS	Q.3900-Q.4099
Testing specifications for next generation networks	Q.3900-Q.3999
Testing specifications for SIP-IMS	Q.4000-Q.4039
Testing specifications for Cloud computing	**Q.4040-Q.4059**
Testing specifications for IMT-2020 and IoT	Q.4060-Q.4099
PROTOCOLS AND SIGNALLING FOR PEER-TO-PEER COMMUNICATIONS	Q.4100-Q.4139
PROTOCOLS AND SIGNALLING FOR COMPUTING POWER NETWORKS	Q.4140-Q.4159
PROTOCOLS AND SIGNALLING FOR QUANTUM KEY DISTRIBUTION NETWORKS	Q.4160-Q.4179
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR IMT-2020	Q.5000-Q.5049
COMBATING COUNTERFEITING AND STOLEN ICT DEVICES	Q.5050-Q.5069

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

Recommendation ITU-T Q.4046

Interoperability testing requirements of blockchain as a service

Summary

Recommendation ITU-T Q.4046 aims to provide an overview of blockchain as a service (BaaS) interoperability testing and specifies BaaS interoperability testing requirements which are derived from use cases.

History [*]

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T Q.4046	2023-12-14	11	11.1002/1000/15722

Keywords

BaaS, interoperability testing.

[*] To access the Recommendation, type the URL https://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Q.4046

Interoperability testing requirements of blockchain as a service

1 Scope

The scope of this Recommendation consists of:

1) Overview of interoperability testing (IOPT) of blockchain as a service (BaaS) based on [ITU-T Y.3530].
2) IOPT requirements of BaaS between CSP:BaaS provider and CSN:BaaS developer.
3) IOPT requirements of BaaS between CSP:BaaS provider and CSP:BaaS provider.
4) IOPT requirements of BaaS between CSP:BaaS provider and CSC:BaaS customer.
5) IOPT requirements of BaaS between CSP:BaaS provider and management entity.

This Recommendation also gives typical use cases of BaaS to derive the IOPT requirements.

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 F.751.0] Recommendation ITU-T F.751.0 (2020), *Requirements for distributed ledger systems*.

[ITU-T Q.4040] Recommendation ITU-T Q.4040 (2016), *The framework and overview of cloud computing interoperability testing*.

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

[ITU-T Y.101] Recommendation ITU-T Y.101 (2000), *Global Information Infrastructure terminology: Terms and definitions*.

[ITU-T Y.3502] Recommendation ITU-T Y.3502 (2014), *Information technology – Cloud computing – Reference architecture*.

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

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 blockchain [ITU-T F.751.0]: A type of distributed ledger that 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.

3.1.2 blockchain as a service (BaaS) [ITU-T Y.3530]: A cloud service category in which the capabilities provided to the cloud service customer are the ability of setting up blockchain platforms, and developing decentralized applications using blockchain technologies.

NOTE – Blockchain technology includes consensus algorithms, smart contracts, cryptography, etc.

3.1.3 interoperability [ITU-T Y.101]: The ability of two or more systems or applications to exchange information and to mutually use the information that has been exchanged.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API Application Programming Interface

BaaS Blockchain as a Service

BDaaS Big data as a Service

CSC Cloud Service Customer

CSN Cloud Service Partner

CSP Cloud Service Provider

DL Distributed Ledger

DLT Distributed Ledger Technology

IaaS Infrastructure as a Service

IDE Integrated Development Environment

IOPT Interoperability Testing

P2P Peer-to-Peer

PaaS Platform as a Service

SaaS Software as a Service

5 Conventions

In this Recommendation:

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

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

6 Overview of interoperability testing of BaaS

6.1 Introduction of BaaS

Blockchain as a service (BaaS) is defined as a cloud service category in which the capabilities provided to the cloud service customer (CSC) are the ability of setting up blockchain platforms, and developing decentralized applications using blockchain technologies [ITU-T Y.3530].

As a cloud service category, BaaS supports blockchain core features based on cloud computing infrastructure, in which an integrated development environment (IDE) for users to create, develop,

test, host, deploy and operate blockchain related applications is provided. Blockchain users (e.g., cloud service customers) can utilize and reuse this BaaS service platform and may focus more on the selection of consensus algorithms and smart contract programming aspects rather than rebuilding their own blockchain platform from scratch. In addition, seamless service provisioning, interoperability with other platform as a service (PaaS) services, and simple development experience are also benefits of BaaS.

The ecosystem of BaaS [ITU-T Y.3530] consists of roles, sub-roles and their activities based on cloud computing reference architecture defined in [ITU-T Y.3502] as shown in Figure 6-1, including:

– CSN:BaaS partner (CSN:BaaS developer);

– CSP:BaaS provider (CSP:BaaS provider);

– CSC:BaaS customer (CSC:BaaS customer).

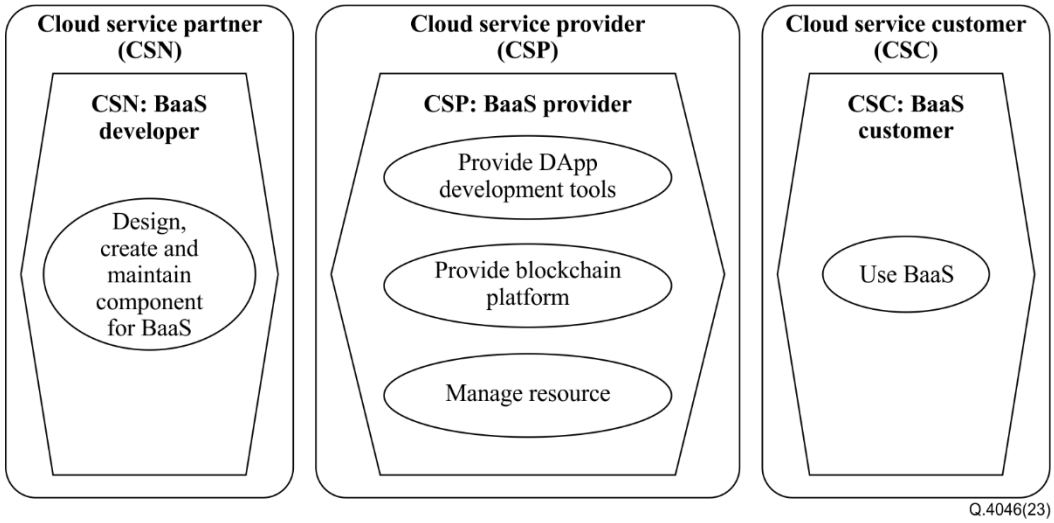


Figure 6-1 – BaaS ecosystem and roles [ITU-T Y.3530]

CSN:BaaS developer is the sub-role of cloud service partner (CSN) which is engaged in supporting activities of CSP: BaaS provider and developing blockchain services.

CSP:BaaS provider is the sub-role of CSP performing and managing blockchain related core features (i.e., consensus mechanism, smart contract, transaction, cryptography, peer-to-peer (P2P) connectivity, ledger management) and supporting the provision of blockchain services.

CSC:BaaS customer is the sub-role of CSC performed by end users in order to use the blockchain services from the CSP:BaaS provider.

6.2 Interoperability testing of BaaS

BaaS interoperability is a capability to interact between CSP:BaaS provider and CSN:BaaS developer, CSP:BaaS provider and CSC:BaaS customer, among different CPS:BaaS providers or between CSP:BaaS provider and management entity. During the interaction, CSN:BaaS developer allocates resources to support BaaS services development, the CSC:BaaS customer interacts with BaaS services and exchange information, one BaaS service works with other BaaS services to meet the CSC:BaaS customer's demands, and the management entity of the CSP interacts with CSP:BaaS provider to manage, monitor, maintain and optimize BaaS services.

BaaS IOPT is used to verify functions and interaction capabilities that realize the BaaS interoperability.

As described in [ITU-T Q.4040], the interoperability testing in different cloud capabilities types is different. There are three major IOPT scenarios: infrastructure capabilities type IOPT, platform capabilities type IOPT, and application capabilities type IOPT [ITU-T Q.4040]. Since BaaS is regarded as one of the capabilities of the PaaS, BaaS IOPT should be considered as a platform capability type IOPT.

According to Figure 6-2, there are 4 different target areas of IOPT of BaaS in this document as follows:

1 "CSP:BaaS provider-CSN:BaaS developer", dealing with interactions between CSP:BaaS provider and CSN:BaaS developer.

2 "CSP:BaaS provider -CSP:BaaS provider", dealing with collaboration among different CSP: BaaS providers.

3 "CSP:BaaS provider-CSC:BaaS customer", dealing with interactions between CSP: BaaS provider and CSC:BaaS customer.

4 "CSP:BaaS provider-management entity", dealing with interactions with CSP management functions.

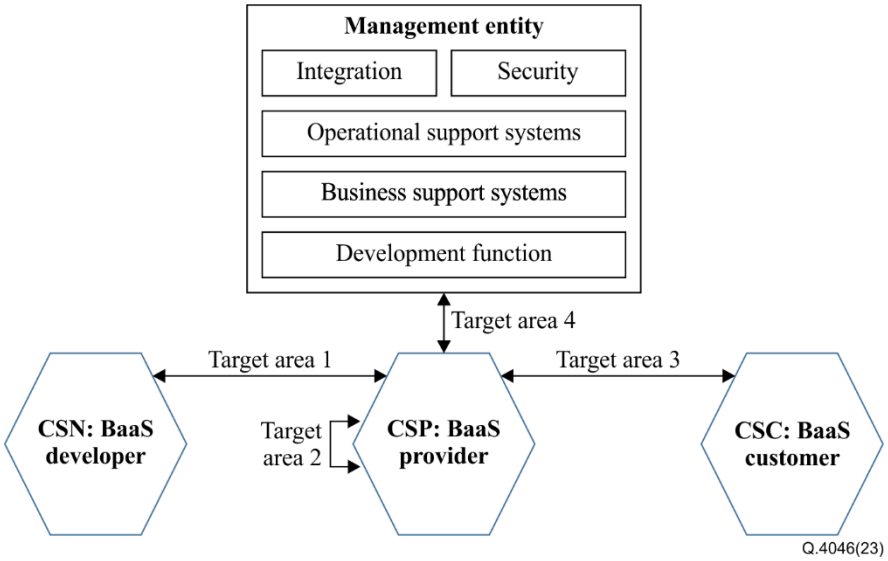


Figure 6-2 – Target areas of BaaS IOPT

It is necessary to consider these four target areas in BaaS IOPT. For each target area, specific relevant use cases need to be provided to derive testing requirements in different aspects. These requirements can be classified into the following 12 aspects: service design and development, resource management, scalability and portability, node management, smart contract, P2P connectivity, transaction processing, block record storage, data storage, consensus mechanism, authentication management and security.

7 Interoperability testing requirements of BaaS between CSP:BaaS provider and CSN: BaaS developer

It is required that CSP:BaaS provider could record the transactions in new blocks after consensus by blockchain nodes.

NOTE – Blockchain nodes are devices or processes that participate in a distributed ledger network.

It is required that CSP:BaaS provider could average block generation time in the initial design to ensure the stable interoperation of the BaaS.

It is required that CSP:BaaS provider could provide a unified application programming interface (API) for accessing cloud resources and monitoring resource allocation.

It is required that CSP:BaaS provider could provide scalability and portability for CSN:BaaS developer, such as dynamic adjustment of consensus algorithm, portability of data and portability of smart contracts.

It is required that CSN:BaaS developer could provide a BaaS component request interface for CSP:BaaS provider.

It is required that CSP:BaaS provider could integrate blockchain services for general demand by interacting with CSN:BaaS developers.

It is recommended that CSP:BaaS provider could provide development tools and the ability of remote deployment for CSN:BaaS developer.

It is recommended that CSP:BaaS provider could provide cross cloud deployment of blockchain nodes for CSN:BaaS developer to reduce the costs of deployment.

8 Interoperability testing requirements of BaaS between CSP: BaaS provider and CSP: BaaS provider

It is required that CSP:BaaS provider could provide access rights of the blockchain network for other CSP:BaaS providers and could access the blockchain network of other CSP:BaaS providers.

It is required that CSP:BaaS provider could provide an interface for querying BaaS information for other CSP:BaaS providers.

NOTE 1 – The BaaS information includes blockchain type, blockchain capability, consensus type, etc.

It is required that CSP:BaaS provider could query the information of current transaction records for other CSP:BaaS providers.

NOTE 2 – Information includes information of the block header and transaction, which contains a timestamp, a hash of the previous block, transaction fees, etc. [ITU-T X.1400].

It is required that CSP:BaaS provider could query the history information of transaction records for interoperable CSP:BaaS providers.

NOTE 3 – Transaction information contains all the information exchanged between blockchain nodes, including the transaction initiator, the transaction recipient, the interaction content, and the digital signature of the transaction initiator, etc.

It is required that CSP:BaaS provider could provide smart contracts deployment and debug capability to other CSP:BaaS providers.

It is required that CSP:BaaS provider could provide consensus configuration capability to other CSP:BaaS providers.

9 Interoperability testing requirements of BaaS between CSP: BaaS provider and CSC:BaaS customer

It is required that CSP:BaaS provider could provide a service interface and interconnect with CSC:BaaS customer.

It is required that CSP:BaaS provider could provide CSC:BaaS customer with user account management.

It is required that CSP:BaaS provider could authenticate and authorize the CSC:BaaS customer.

It is required that CSP:BaaS provider could provide encryption key management function for CSC:BaaS customer.

It is required that CSP:BaaS provider could provide the ability to query transaction information.

It is required that CSC:BaaS customer could query the status of the service, including the status of smart contracts, the status of consensus algorithms, etc.

It is required that CSP:BaaS provider could design, debug, deploy and invoke asmart contract for CSC:BaaS customer.

It is recommended that CSP:BaaS provider could design and configure consensus algorithms for the CSC:BaaS customer to confirm and record the transactions into a distributed ledger (DL).

10 Interoperability testing requirements of BaaS between CSP:BaaS provider and management entity

It is required that CSP:BaaS provider could provide a connection and management interface for management entity.

It is required that CSP:BaaS provider could execute the management instructions received from management entity.

NOTE – Management instructions are a series of control instructions issued by the management entity to CSP:BaaS provider, including data collection instructions, function configuration instructions, etc.

It is required that the management entity could integrate multiple CSP:BaaS providers and manage them in a unified manner.

It is required that the management entity could monitor, manage, maintain and optimize the services provided by CSP:BaaS providers.

It is required that the management entity could balance business hosting among CSP:BaaS providers.

It is recommended that the management entity and CSP:BaaS provider could provide encryption and decryption mechanisms supporting encrypted transmission and storage.

Appendix I

Use cases of interoperability of blockchain as a service

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

This appendix presents the following blockchain as a service interoperability use cases:

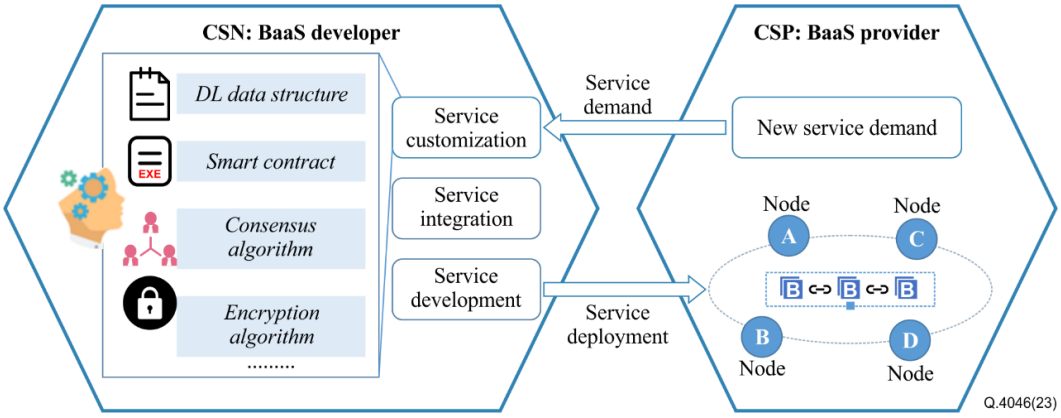
– use case of service design and development between CSP:BaaS provider and CSN:BaaS developer,

– use case of block record storage between CSP:BaaS provider and CSP:BaaS provider,

– use case of authentication management between CSP:BaaS provider and CSC:BaaS customer,

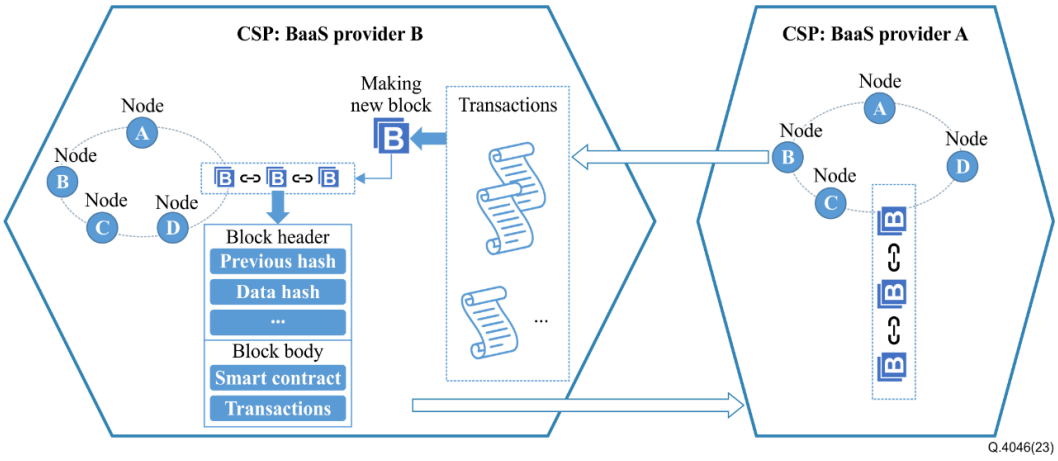
– use case of security management between CSP:BaaS providers and management entity.

I.1 Use case between CSP:BaaS provider and CSN: BaaS developer

Title	Use case of service design and development between CSP:BaaS provider and CSN:BaaS developer
Description	Service design and development is important for the interoperability of the CSP:BaaS provider and CSN:BaaS developer. CSP:BaaS provider launches service component demands to CSN:BaaS developer. CSN:BaaS developer receives the demands and provides the service design and development function including service customization, service integration, service development and service deployment to develop corresponding services. Then the corresponding distributed ledger (DL) data structure, smart contract, consensus algorithm, encryption algorithm, etc. can be supplied to CSP:BaaS provider.
Roles	CSP:BaaS provider CSN:BaaS developer
Figure and operational flows	 **Figure I.1 – Interoperability between CSP:BaaS provider and CSN: BaaS developer** 1 CSP:BaaS provider launches a new BaaS service demand to CSN:BaaS developer. 2 CSN:BaaS developer receives and analyzes the service demand, and starts the service customization process to develop corresponding BaaS function modules, including DL data structure, smart contract, consensus algorithm, etc. 3 CSN:BaaS developer integrates the BaaS function modules as a service and deploys the service to CSP:BaaS provider.
Derived requirements	It is required that CSP:BaaS provider could provide scalability and portability for CSN:BaaS developer, such as dynamic adjustment of consensus algorithms, portability of data and portability of smart contracts.

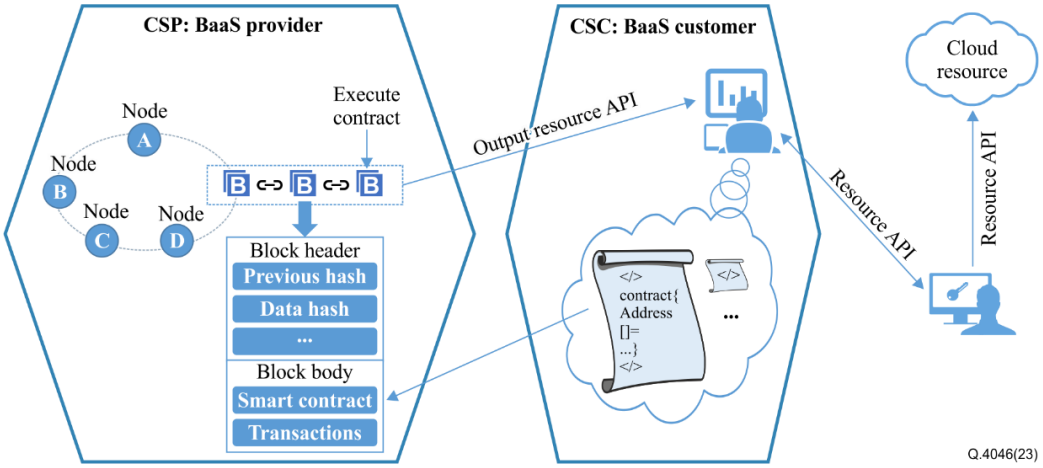
	It is required that CSN:BaaS developer could provide a BaaS component request interface for CSP:BaaS provider. It is required that CSP:BaaS provider could integrate blockchain services for general demand by interacting with CSN:BaaS developers. It is recommended that CSP:BaaS provider could provide development tools and the ability of remote deployment for CSN:BaaS developer. It is recommended that CSP:BaaS provider could provide cross cloud deployment of blockchain nodes for CSN:BaaS developer to reduce the cost of deployment.

I.2 Use case between CSP:BaaS provider and CSC:BaaS provider

Title	Use case of block record storage between CSP:BaaS provider and CSP:BaaS provider
Description	Blockchain is a type of distributed ledger technology (DLT) in which nodes can create new blocks containing the transactions and smart contracts. This use case provides a scenario for block record storage, demonstrating the storage capability by sending transactions between CSP:BaaS provider A and CSP:BaaS provider B.
Roles	CSP:BaaS provider
Figure and operational flows	 **Figure I.2 – Interoperability between CSP:BaaS provider and CSP: BaaS provider** 1 CSP:BaaS providers could interconnect firstly and create at least one BaaS user on each platform. 2 CSP:BaaS provider A sends a transaction to CSP:BaaS provider B using cross-chain technology. 3 CSP:BaaS provider B receives and collects transaction details per Node, such as Node D. 4 Node D creates a block and records the information of the previous block, transaction, etc. As shown in the figure, the block header contains the previous hash, root hash generated from transactions, data hash, etc. 5 CSP:BaaS provider A queries the details information and history information of the record to trace the transaction status.
Derived requirements	It is required that CSP:BaaS provider could provide access rights of the blockchain network for other CSP:BaaS providers and could access the blockchain network of other CSP:BaaS providers. It is required that CSP:BaaS provider could provide an interface for querying BaaS information for other CSP:BaaS providers.

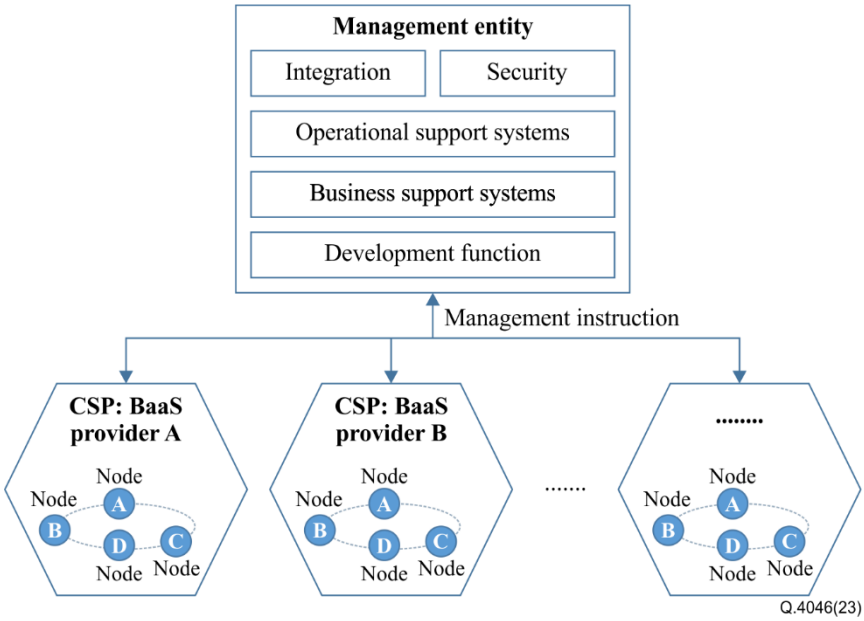
	It is required that CSP:BaaS provider could query the information of the current transaction record for other CSP:BaaS providers. It is required that CSP:BaaS provider could query the history information of the transaction record for interoperable CSP:BaaS provider.

I.3 Use case between CSP:BaaS provider and CSC: BaaS customer

Title	Use case of authentication management between CSP:BaaS provider and CSC: BaaS customer
Description	Authentication management is fundamental to interoperability. BaaS with access management capabilities can better allocate resources according to a permission level list. This use case provides a cloud resource sharing scenario of authentication management capability between a CSP:BaaS provider and CSC: BaaS customer.
Roles	CSP:BaaS provider CSC:BaaS customer
Figure and operational flows	 **Figure I.3 – Interoperability between CSP:BaaS provider and CSC: BaaS customer** 1 CSC:BaaS customer requests a cloud resource by metadata of resource, which are provided by CSP:BaaS provider. 2 CSC:BaaS customer writes the resource request into the contract code according to the contract rules and sends it to the CSP:BaaS provider. 3 CSP:BaaS provider receives this contract request and records it to a new block and estimates the resource access authority of CSC:BaaS customer. 4 The resource API is sent to the CSC:BaaS customer automatically from the CSP:BaaS provider if the permissions are met. 5 CSC:BaaS customer uses this API to acquire the cloud resource.
Derived requirements	It is required that CSP:BaaS provider could provide a service interface and interconnect with the CSC:BaaS customer. It is required that CSP:BaaS provider could provide CSC:BaaS customer with user account management. It is required that CSP:BaaS provider could authenticate and authorize the CSC:BaaS customer. It is required that CSP:BaaS provider could provide an encryption key management function for CSC:BaaS customer. It is required that CSP:BaaS provider could provide the ability to query transaction information.

	It is required that CSC: BaaS customer could query the status of the service, including the status of smart contracts, the status of consensus algorithms, etc.

I.4 Use case between CSP:BaaS provider and management entity

Title	Use case of security management between CSP:BaaS providers and management entity
Description	Management entity can monitor and manage multiple CSP:BaaS providers. CSP:BaaS providers can adjust the security configuration (e.g., encryption mechanism) according to the directives of the management entity. This use case shows the security management capability of the management entity to adjust the security configuration between CSP:BaaS providers.
Roles	CSP:BaaS provider Management entity
Figure and operational flows	 **Figure I.4 – Interoperability between CSP:BaaS provider and management entity** 1 Management entity monitors multiple CSP:BaaS providers and collects their status information. 2 Management entity delivers the encryption and decryption mechanism configuration instruction. 3 CSP:BaaS providers receive the instruction and configures the mechanism. 4 CSP:BaaS providers realize encrypted transmission and storage based on the set of encryption and decryption mechanisms.
Derived requirements	It is required that CSP:BaaS provider could provide a connection and management interface for the management entity. It is required that CSP:BaaS provider can execute the encryption and decryption mechanism configuration instructions received from the management entity. It is required that management entity could integrate multiple CSP:BaaS providers and manage them in a unified manner. It is recommended that the management entity and CSP:BaaS provider could provide encryption and decryption mechanisms supporting encrypted transmission and storage.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	**Switching and signalling, and associated measurements and tests**
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Published in Switzerland
Geneva, 2024