



INTERNATIONAL TELECOMMUNICATION UNION

# ITU-T

TELECOMMUNICATION  
STANDARDIZATION SECTOR  
OF ITU

# Y.3530

(09/2020)

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

Cloud Computing

---

## Cloud computing – Functional requirements for blockchain as a service

**CAUTION !**

***PREPUBLISHED RECOMMENDATION***

This prepublication is an unedited version of a recently approved Recommendation. It will be replaced by the published version after editing. Therefore, there will be differences between this prepublication and the published version.

## 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/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.

## **Draft new Recommendation ITU-T Y.3530 (formerly Y.BaaS-reqts)**

### **Cloud computing – Functional requirements for blockchain as a service**

#### **Summary**

Blockchain as a service (BaaS) is a cloud service category in which the capabilities provided to the cloud service customer are the ability of setting up blockchain platform, and development decentralized application using blockchain technologies. In BaaS, an integrated developing environment (IDE) for CSCs is provided to create, deploy and operate decentralized applications. This Recommendation introduces blockchain and blockchain as a service. This Recommendation also provides functional requirements of blockchain as a service which is derived from use cases.

#### **Keywords**

blockchain; BaaS; blockchain as a service; cloud computing

# CONTENTS

|                                                                                      | Page |
|--------------------------------------------------------------------------------------|------|
| 1 Scope.....                                                                         | 4    |
| 2 References.....                                                                    | 4    |
| 3 Definitions.....                                                                   | 4    |
| 3.1 Terms defined elsewhere: .....                                                   | 4    |
| 3.2 Terms defined in this Recommendation .....                                       | 6    |
| 4 Abbreviations and acronyms.....                                                    | 6    |
| 5 Conventions.....                                                                   | 7    |
| 6 Overview of blockchain .....                                                       | 7    |
| 6.1 Introduction to blockchain.....                                                  | 7    |
| 6.2 Block and hash function .....                                                    | 8    |
| 6.3 Consensus of blockchain .....                                                    | 9    |
| 6.4 Transaction confidentiality .....                                                | 10   |
| 6.5 Blockchain network .....                                                         | 10   |
| 6.6 Decentralized application .....                                                  | 10   |
| 6.7 Smart contract.....                                                              | 10   |
| 7 Blockchain as a Service .....                                                      | 10   |
| 7.1 Introduction to BaaS .....                                                       | 10   |
| 7.2 System context of BaaS .....                                                     | 11   |
| 8 Functional requirements of BaaS .....                                              | 13   |
| 8.1 Node configuration requirements .....                                            | 13   |
| 8.2 Operation and monitoring of blockchain platform requirements .....               | 14   |
| 8.3 Decentralized application development support requirements.....                  | 14   |
| 8.4 Security requirements .....                                                      | 15   |
| 9 Security considerations .....                                                      | 16   |
| Appendix I Use cases and scenarios of blockchain as a service .....                  | 17   |
| Appendix II Use cases and scenarios of applications for blockchain as a service..... | 26   |
| Bibliography.....                                                                    | 29   |

## List of Figures

|                                                                                  | Page |
|----------------------------------------------------------------------------------|------|
| Figure 6-1 – Conceptual of blockchain .....                                      | 7    |
| Figure 6-2 – Chaining blocks with hash value .....                               | 8    |
| Figure 6-3 – Process of creating and storing a block in blockchain network ..... | 8    |
| Figure 6-4 – Block diagram .....                                                 | 9    |
| Figure 7-1 – System context of blockchain as a service .....                     | 11   |

# Draft new Recommendation ITU-T Y.3530 (formerly Y.BaaS-reqts)

## Cloud computing - Functional requirements for blockchain as a service

### 1 Scope

This Recommendation introduces blockchain as well as blockchain as a service. This Recommendation also provides the system context of BaaS includes sub-roles and activities in terms of cloud computing as well as functional requirements for blockchain as a service in cloud computing environment. The functional requirements in this Recommendation are derived from use cases.

### 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.3500] Recommendation ITU-T Y.3500 (2014), *Information technology – Cloud computing – Overview and vocabulary*.
- [ITU-T Y.3501] Recommendation ITU-T Y.3501 (2013), *Cloud computing framework and high-level requirements*.
- [ITU-T Y.3502] Recommendation ITU-T Y.3502 (2014), *Information technology – Cloud computing – Reference architecture*.

### 3 Definitions

#### 3.1 Terms defined elsewhere:

**3.1.1 account** [b-FG-DLT Terms]: Representation of an entity whose data is recorded on a distributed ledger.

**3.1.2 activity** [ITU Y.3502]: A specified pursuit or set of tasks.

**3.1.3 block** [b-FG-DLT Terms]: Party which is in a business relationship for the purpose of using cloud services.

**3.1.4 blockchain** [b-FG-DLT Terms]: 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.

**3.1.5 cloud service customer** [ITU-T Y.3500]: Party which is in a business relationship for the purpose of using cloud services.

**3.1.6 cloud service provider** [ITU-T Y.3500]: Party which makes cloud services available.

**3.1.7 cloud service partner** [ITU-T Y.3500]: Party which is engaged in support of, or auxiliary to, activities of either the cloud service provider or the cloud service customer, or both.

**3.1.8 consensus** [b-FG-DLT Terms]: Agreement that a set of transactions is valid.

**3.1.9 consensus mechanism** [b-FG-DLT Terms]: Rules and procedures by which consensus is reached

**3.1.10 cryptography** [ITU-T b-X.800]: The discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use.

NOTE – Cryptography determines the methods used in encipherment and decipherment. An attack on a cryptographic principle, means, or method is cryptanalysis.

**3.1.11 decentralized application** [b-FG-DLT Terms]: Application that runs in a distributed and decentralized computing environment.

**3.1.12 digital signature** [b-FG-DLT Terms]: Data appended to, or a cryptographic transformation (see cryptography) of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, e.g., by the recipient.

NOTE – Consider the definition ‘digital signature’ as “Data appended to data units, or cryptographic changes made to data units, which allows the recipient of the data unit to confirm the origin and integrity of the data and protect the data from being forged.”

**3.1.13 distributed ledger** [b-FG-DLT Terms]: A type of ledger that is shared, replicated, and synchronized in a distributed and decentralized manner.

**3.1.14 fork** [b-FG-DLT Terms]: Creation of two or more different versions of a distributed ledger.

NOTE – There are two types of forks. See clause 3.1.15 (hard fork) and clause 3.1.26 (soft fork).

**3.1.15 hard fork** [b-FG-DLT Terms]: Change to the protocol or rules that result in a fork that is not backward compatible.

**3.1.16 hash function** [b-FG-DLT Terms]: A function that maps a bit string of arbitrary length to a fixed-length bit string.

**3.1.17 ledger** [b-FG-DLT Terms]: Information store that keeps final and definitive (immutable) records of transactions.

**3.1.18 node** [b-FG-DLT Terms]: Device or process that participates in a distributed ledger network.

NOTE – Nodes can store a complete or partial replica of the distributed ledger.

**3.1.19 peer** [b-ITU-T X.1161]: Communication node on P2P network that functions simultaneously as both "client" and "server" to the other nodes on the network.

**3.1.20 peer-to-peer** [b-ISO CD 22739]: Relating to, using, or being a network of peers that directly share information and resources with each other without relying on a central entity.

NOTE – In the context of a distributed ledger system, peers are nodes.

**3.1.21 proof of work** [b-FG-DLT Terms]: Consensus process to solve a difficult (costly, time-consuming) problem that produces a result that is easy for others to correctly verify.

NOTE – Producing a proof of work can be a random process with low probability so that a lot of trial and error is required on average before a valid proof of work is generated.

**3.1.22 proof of stake** [b-FG-DLT Terms]: Consensus process, where an existing stake in the distributed ledger system (e.g., the amount of that currency that you hold) is used to reach consensus.

**3.1.23 public key cryptography** [b-FG-DLT Terms]: Cryptography in which a public key and a corresponding private key are used for encryption and decryption, where public key is disseminated, and private key is known only to the key owner.

NOTE – Users can digitally sign data with their private key, and the resulting signature can be verified by anyone using the corresponding public key.

**3.1.24 role** [ITU Y.3502]: A set of activities that serves a common purpose.

**3.1.25 smart contract** [b-FG-DLT Terms]: 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.

**3.1.26 soft fork** [b-FG-DLT Terms]: Change to the protocol or rules that result in a fork that is backward compatible.

**3.1.27 sub-role** [ITU Y.3502]: A subset of the activities of a given role.

**3.1.28 transaction** [b-FG-DLT Terms]: Whole of the exchange of information between nodes. A transaction is uniquely identified by a transaction identifier.

## 3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

**3.2.1 Blockchain as a Service (BaaS):** A cloud service category in which the capabilities provided to the cloud service customer are the ability of setting up blockchain platform, and developing decentralized application using blockchain technologies.

NOTE – Blockchain technology includes consensus algorithm, smart contract, cryptography, etc.

**3.2.2 blockchain network:** A network to perform blockchain platform among nodes.

**3.2.3 blockchain platform:** Implementation of blockchain (3.1.4) to process data in a node (3.1.18).

## 4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

|             |                                     |
|-------------|-------------------------------------|
| <b>BaaS</b> | Blockchain as a Service             |
| <b>CSC</b>  | Cloud Service Customer              |
| <b>CSN</b>  | Cloud Service partNer               |
| <b>CSP</b>  | Cloud Service Provider              |
| <b>DApp</b> | Decentralized Application           |
| <b>DLT</b>  | Distributed Ledger Technology       |
| <b>IDE</b>  | Integrated Developing Environment   |
| <b>PII</b>  | Personally Identifiable Information |
| <b>P2P</b>  | Peer-to-Peer                        |
| <b>PoS</b>  | Proof of Stake                      |
| <b>PoW</b>  | Proof of Work                       |
| <b>TPS</b>  | Transactions per second             |

## 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 document 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.

## 6 Overview of blockchain

### 6.1 Introduction to blockchain

Blockchain is a type of distributed ledger technology (DLT) 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. Blockchain platform in a node creates block containing ledgers which has final and definitive (immutable) records of transactions. And the block is shared, replicated, and synchronized in a distributed and decentralized manner among nodes.

Figure 6-1 shows the concept of blockchain. The blockchain platform within a node is the implementation of the blockchain technology necessary for the operation and management of the blockchain. The blockchain platform support verifying transactions, creating and distributing blocks, consensus algorithm, smart contract etc. The blockchain platform also provides cryptographic algorithm such as hash function, and digital signatures.

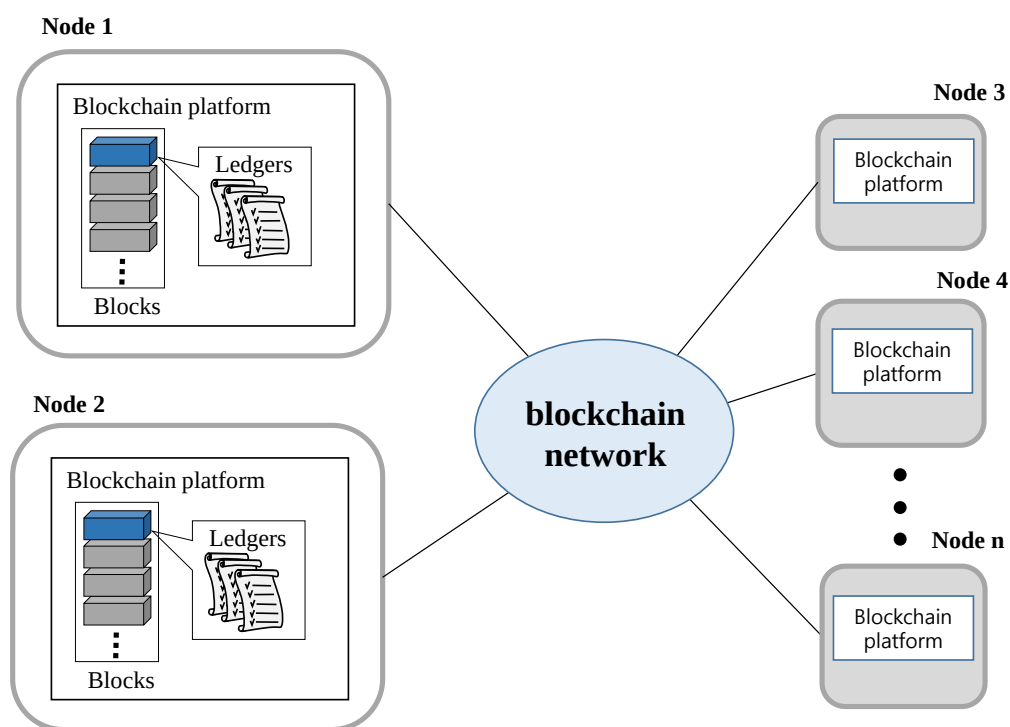


**Figure 6-1 – Conceptual of blockchain**

In blockchain, all blocks are chained through the hash value. As an example, Block #n contains the hash value of the previous block #n-1 as shown in Figure 6-2. By linking the previous hash value to the block creation, it prevents changing or inserting a block between two existing blocks (Block #n-1 and Block #n, or Block #n and Block #n+1 in Figure 6-2).

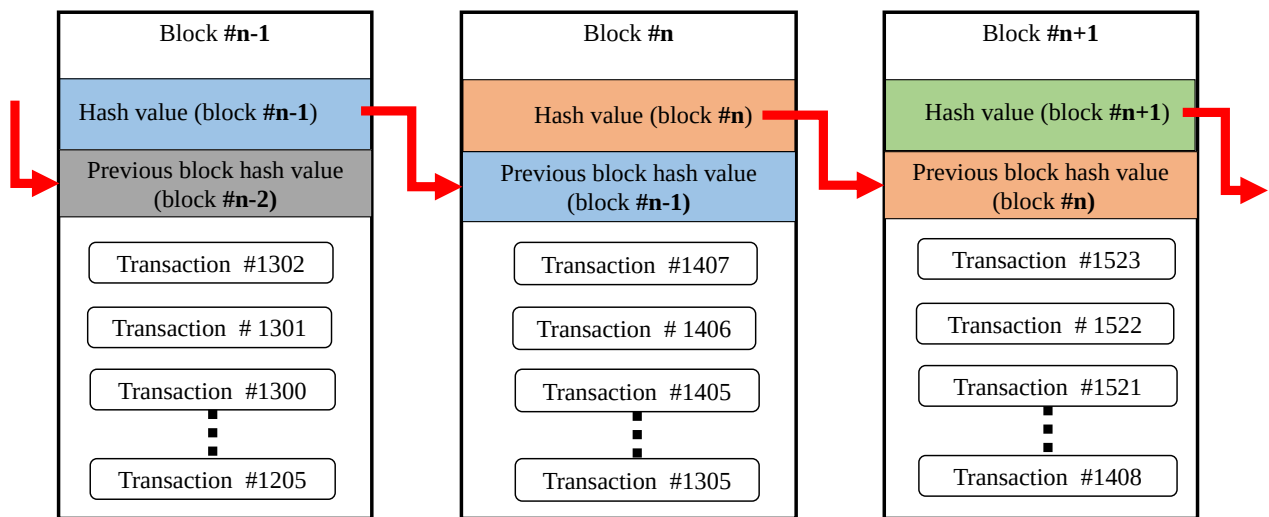


**Figure 6-2 – Chaining blocks with hash value**

Figure 6-3 shows a process of creating and storing a block in blockchain network in details. When a transaction occurs in any node, blockchain platform in node transmits the transaction to all other nodes. Blockchain platform in each node tries to create block including the transactions. If a block is generated, the block is transmitted to all other nodes in the blockchain network, and blockchain platform verify the block. If there is no problem, the block is stored in each node's storage.

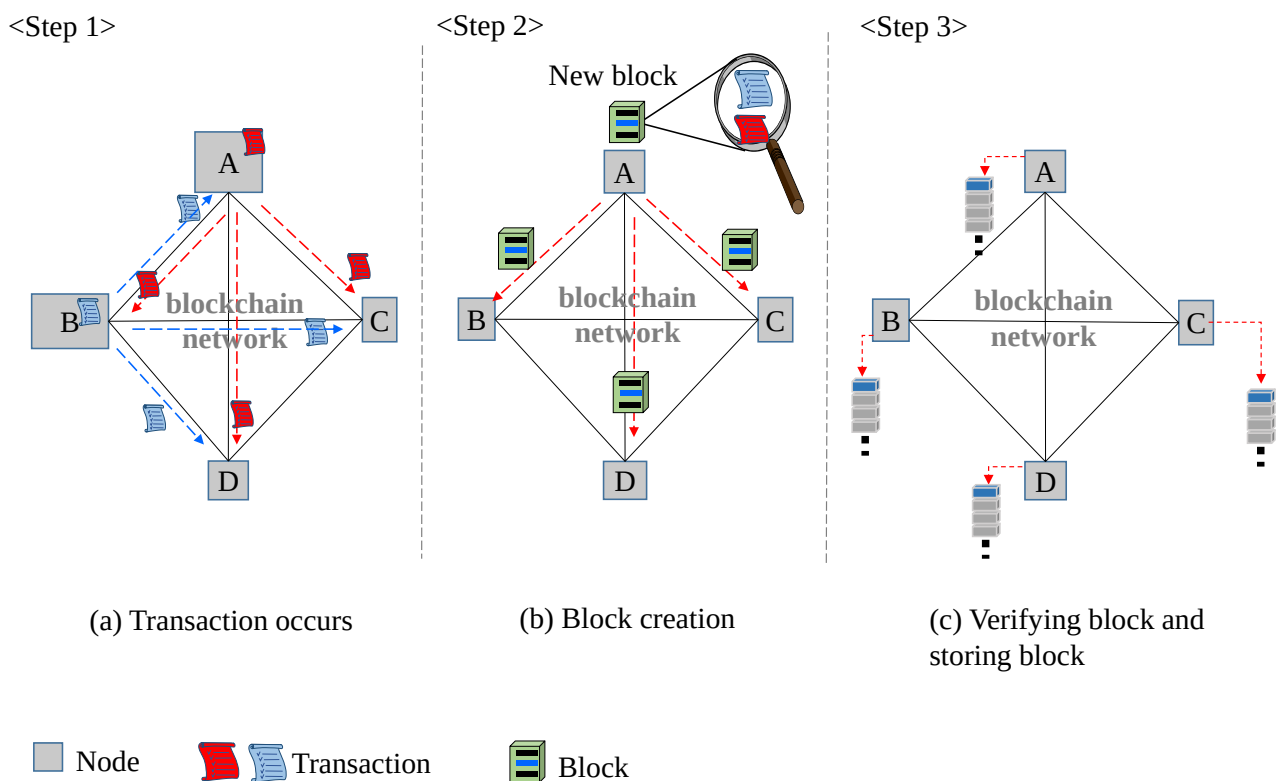


**Figure 6-3 – Process of creating and storing a block in blockchain network**

## 6.2 Block and hash function

The block consists of block number, block hash, block header, transactions, other values (block size, version, etc.) and hash tree as shown in Figure 6-4. In blockchain, the root hash is included in block header. In order to get the root hash, first, a hash value corresponding to transaction is generated, and