ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

ITU-T M.3366 (04/2023)

SERIES M: Telecommunication management, including TMN and network maintenance

Telecommunications management network

Requirements for management of blockchain systems

ITU-T M-SERIES RECOMMENDATIONS

Telecommunication management, including TMN and network maintenance

Introduction and general principles of maintenance and maintenance organization	M.10-M.299
International transmission systems	M.300-M.559
International telephone circuits	M.560-M.759
Common channel signalling systems	M.760-M.799
International telegraph systems and phototelegraph transmission	M.800-M.899
International leased group and supergroup links	M.900-M.999
International leased circuits	M.1000-M.1099
Mobile telecommunication systems and services	M.1100-M.1199
International public telephone network	M.1200-M.1299
International data transmission systems	M.1300-M.1399
Designations and information exchange	M.1400-M.1999
International transport network	M.2000-M.2999
Telecommunications management network	**M.3000-M.3599**
Integrated services digital networks	M.3600-M.3999
Common channel signalling systems	M.4000-M.4999

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

Recommendation ITU-T M.3366

Requirements for management of blockchain systems

Summary

Recommendation ITU-T M.3366 introduces requirements for management of blockchain systems, and includes configuration management, performance management, fault management and log management related to blockchain nodes, blockchain ledgers, smart contracts, consensus, accounts, etc., in blockchain systems. This Recommendation proposes management requirements for private chains or permissioned chains.

History *

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T M.3366	2023-04-29	2	11.1002/1000/15519

Keywords

Blockchain node, blockchain system, distributed ledger.

* 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/.

© ITU 2023

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

Table of Contents

Recommendation ITU-T M.3366

Requirements for management of blockchain systems

1 Scope

This Recommendation proposes requirements for management of blockchain systems. This Recommendation considers configuration management, performance management, fault management and log management related to nodes, blockchain ledgers, smart contracts, consensus, accounts, etc., in blockchain systems. This Recommendation proposes management requirements for private chains or permissioned chains.

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.751.2] Recommendation ITU-T F.751.2 (2020), *Reference framework for distributed ledger technologies.*

[ITU-T M.3400] Recommendation ITU-T M.3400 (2000), *TMN management functions.*

[ITU-T M.3705] Recommendation ITU-T M.3705 (2013), *Common management services – Log management – Protocol neutral requirements and analysis.*

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

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 account [ITU-T X.1400]: Representation of an entity whose data is recorded on a distributed ledger.

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

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

3.1.3 blockchain [ITU-T X.1400]: A type of distributed ledger which is composed of digitally recorded data arranged as a successively growing chain of blocks with each block cryptographically linked and hardened against tampering and revision.

3.1.4 blockchain system [ITU-T X.1400]: A system that implements a blockchain.

3.1.5 decentralized application [ITU-T X.1400]: Application that runs in a distributed and decentralized computing environment.

3.1.6 distributed ledger [ITU-T X.1400]: A type of ledger that is shared, replicated, and synchronized in a distributed and decentralized manner.

3.1.7 distributed ledger network [b-ISO 22739]: Network within a distributed ledger system.

3.1.8 distributed ledger system [b-ISO 22739]: System that implements a distributed ledger.

3.1.9 node [ITU-T X.1400]: Device or process that participates in a distributed ledger network.

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

3.1.10 permissioned distributed ledger system [ITU-T X.1400]: Distributed ledger system in which permissions are required to maintain and operate a node.

3.1.11 permissionless distributed ledger system [ITU-T X.1400]: Distributed ledger system where permissions are not required to maintain and operate a node.

NOTE – Examples of permissionless ledgers are the Bitcoin and Ethereum blockchains, where any user can join the network and start mining.

3.1.12 private DLT system [ITU-T X.1400]: A distributed ledger technology (DLT) system which is accessible for use only to a limited group of DLT users.

3.1.13 public DLT system [ITU-T X.1400]: A distributed ledger technology (DLT) system which is accessible to the public for use.

3.1.14 record [b-ISO 22739]: Information created, received and maintained as evidence and as an asset by an organization or person, in pursuit of legal obligations or in the transaction of business.

Note 1 to entry: This term applies to information in any medium, form or format.

Note 2: The term refers specifically to transaction records in the blockchain.

3.1.15 smart contract [ITU-T X.1400]: A 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.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 blockchain management system: A system that manages one or more blockchain systems, providing configuration management, performance management, fault management, and log management for blockchain systems.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

BFT Byzantine Fault Tolerance

CEV Consensus Mechanism based on Election and Verification

CPU Central Processing Unit

DLT Distributed Ledger Technology

IT Information Technology

P2P Peer to Peer

PBFT Practical Byzantine Fault Tolerance

TMN Telecommunications Management Network

TPS Transactions Per Second

5 Convention

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 or service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with this Recommendation.

6 Overview

According to [ITU-T F.751.2], the functional structure of blockchain mainly includes the core layer, service layer and application layer. The core layer realizes the blockchain data sharing capability, the service layer provides the application layer with a mechanism to access the blockchain capability (such as user authorization, smart contract compiler), and the application layer implements the decentralized application functions that meet specific business scenarios (such as certificate storage system, traceability system, and invoice system) based on the blockchain technology.

When instantiating blockchain-based functions to form specific application systems, it is necessary to decouple blockchain capabilities and application capabilities to ensure the universality of blockchain capabilities. Generally, the core layer and service layer capabilities in the blockchain functional structure are instantiated as blockchain systems, and the application layer capabilities are instantiated as application systems based on the blockchain technology.

This Recommendation only involves the management of the blockchain systems, that is, to ensure the normal, safe and reliable operation of blockchain systems, so as to provide the required quality of data sharing services for blockchain technology-based application systems. However, the management of application systems based on blockchain technology belongs to the general IT management category and is not within the scope of this Recommendation.

According to [ITU-T F.751.2], the core layer of the blockchain includes the resource layer and the protocol layer. The resource layer blockchain provides the network, computing and storage environment required for operation. The protocol layer implements blockchain core service capabilities such as blockchain data storage, consensus mechanism operation, account management and smart contract. When the blockchain function is instantiated as a blockchain system, from the perspective of management, the functional entities of the core layer of the blockchain will form management objects such as blockchain nodes, blockchain, smart contracts, consensus mechanisms, accounts, etc. Therefore, this Recommendation will mainly involve the management of these objects.

According to the basic principles of the telecommunications management network (TMN) and the management characteristics of the blockchain system, the main management functions include configuration management, performance management, fault management and log management for the above management objects.

In order to implement the above management capabilities, it is necessary to obtain the corresponding management information of the above managed objects that constitute the blockchain system. The above management information can be achieved from a blockchain management interface, and the corresponding management interface location, type and corresponding management information should be specifically standardized. For this, a separate Recommendation for the blockchain management interface will be provided according to the requirements in this Recommendation.

At the same time, because the blockchain system is an integral part of an IT application system for a specific application scenario (blockchain system only providing the data sharing capability for the IT application system), and the management system of the IT application system needs to take into account the management of various IT resources (such as network, application, data, and process) including blockchain, the management capability of the blockchain system either exists as a separate blockchain management system or is integrated into the management system of the IT application system. When using the former method to develop and build a separate blockchain management system, it is necessary to achieve the management capability specified in this Recommendation, and the blockchain management system needs to provide a northbound interface (to the IT management system); When the latter method is adopted, the corresponding management capability will exist as the management entities of the IT application management system. This Recommendation will adopt the former method to specify the blockchain management system, which does not affect the application of the latter way.

Blockchain systems can be classified in two ways: public or private blockchain systems; permissioned or permissionless blockchain systems. A public blockchain system has transaction records that are readable by anyone, while a private blockchain system limits the transaction records read access to some authorized groups. In a permissionless blockchain system, any computer can be a full functional node. In a permissioned blockchain system, only an authorized terminal can join the blockchain system network as a fully functional node. This leads to different requirements for management of different types of blockchains. From the perspective of management, the management requirements of a private chain or a permissioned chain are a superset of the management capabilities of a public chain and a permissionless chain. Therefore, this Recommendation proposes management requirements for private chains or permissioned chains.

7 Framework of management function for a blockchain system

The functional framework of blockchain management is shown in Figure 1. The managed blockchain system is composed of multiple distributed blockchain nodes. The blockchain capabilities configured by each blockchain node may be different. Some blockchain nodes provide data sharing services to distributed applications (through s reference point), and all blockchain nodes provide management information to the blockchain management system (through q reference point). The q reference point is the management interface between the blockchain management system and the blockchain system, and it will be described in detail in another Recommendation.

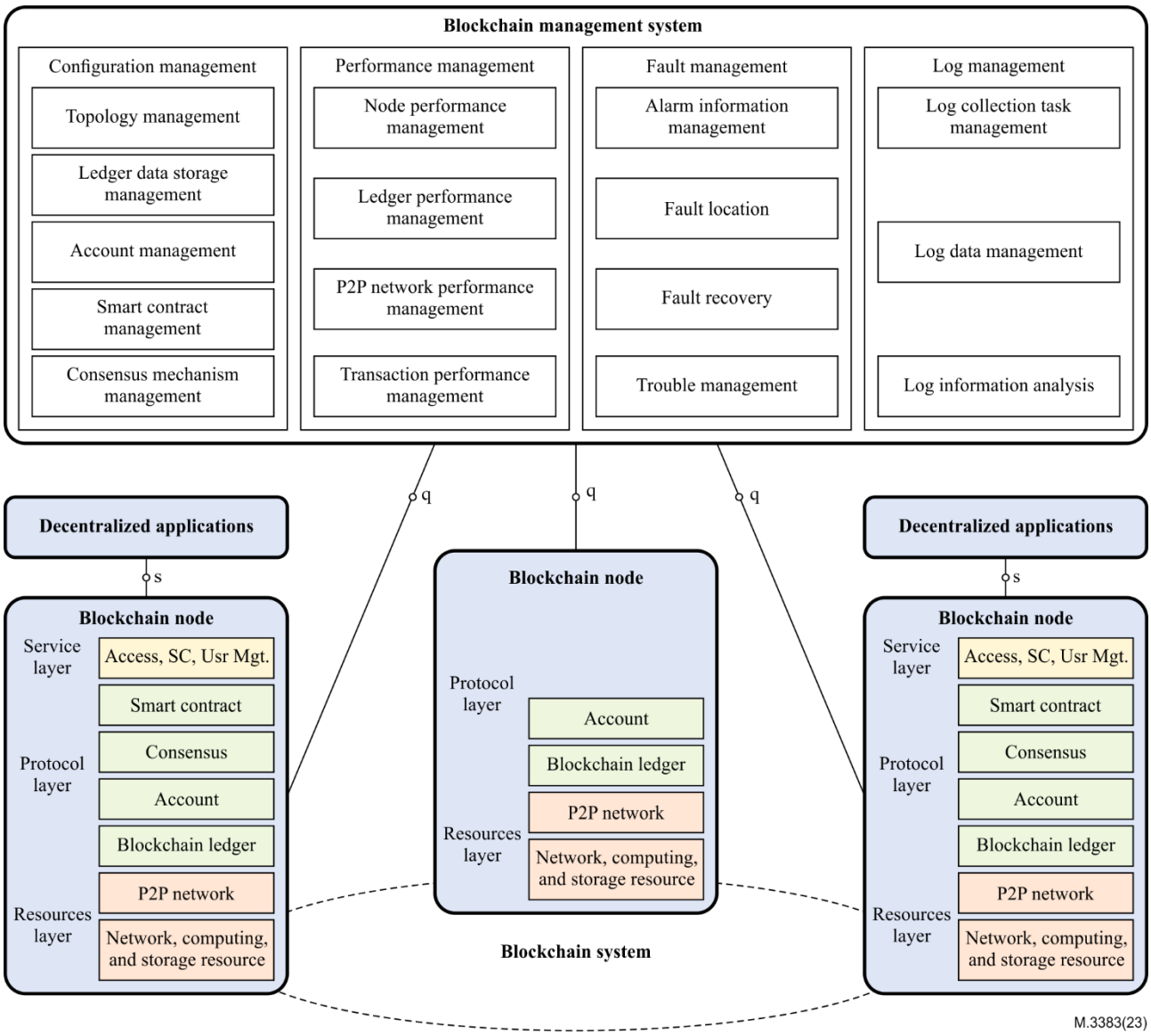

Figure 1 – Framework of management functions for a blockchain system

In order to ensure the normal operation of a blockchain system, the blockchain management system needs to manage the blockchain nodes and the functional entities in the nodes. The objects to be managed include but are not limited to:

a) Blockchain nodes;

b) Resources required for blockchain node operation (includes network, computing, storage resources, and peer to peer (P2P) network functional entities);

c) Blockchain ledger, which stores on-chain data in the block-chain structure;

d) Smart contracts;

e) Consensus mechanism for storing data in blockchain;

f) Account.

In order to realize the unified management of the above management object resources and the effective monitoring of its operation status, the blockchain management system mainly needs to implement the management capabilities such as configuration management, fault management, performance management and log management. The main capabilities of these functions are as follows:

a) The configuration management function is mainly used to manage the configuration information of all blockchain management objects, and to change the service capability of blockchain nodes by modifying the configuration information of related management objects. For example, by deploying different functional entities in the blockchain nodes, the corresponding nodes have only the ability to participate in consensus, the ability to store blockchain data, the ability to support smart contract deployment and resolution, or all blockchain capabilities. Or in the process of blockchain operation, activate or deactivate smart contracts to make relevant smart contracts valid or invalid.

b) The performance management mainly monitors the operation performance of each functional entity that constitutes the blockchain in real time, collects performance data of relevant functional entities, executes performance analysis, and gives early warning for performance parameters that exceed the threshold by setting the threshold range of various performance indicators. For example the performance management function monitors the operation performance of network, computing or storage resources in the blockchain nodes to provide a basis for resource allocation decisions, or monitors the operation performance of smart contracts to track the operation efficiency of contracts and monitor the possibility of contract deadlock.

c) The fault management function mainly monitors the operation status of various entities constituting the blockchain in real time, locates the blockchain entities with abnormal status, and cooperates with the configuration management function to deal with abnormal problems. Faults to be handled include but are not limited to: blockchain node faults, account abnormality, authentication certificate invalidation, smart contract disputes and consensus node abnormality and illegal cross-chain transactions in the blockchain system, etc. The fault management functions mainly include the management of node faults, account abnormality, authentication certificate invalidation, smart contract disputes and consensus node abnormality and illegal cross-chain transactions in the blockchain system.

d) As a distributed system with complex functions, the interaction process of functional entities constituting the blockchain system is complex and frequent. For this reason, it is difficult to track and locate the cause of the failure for individual functional entity failures and performance overruns. Fortunately, when the internal entities of the blockchain system are running, the system can synchronously record the relevant logs. Through the analysis of the blockchain logs, the fault location can be quickly determined, and the system crisis can be solved in a timely manner. Therefore, log management has become an extremely important means in the blockchain operation, maintenance and management process. The log management function mainly includes log data sequence record management, and log analysis of operation commands, spontaneous events, process changes, and entity activities that affect system operation. It also includes blockchain functional entity design defects and security vulnerability analysis. Relevant log management functions are applicable to blockchain system node operation logs, account operation logs, smart contract execution logs and consensus process logs.

8 Requirements for management of a blockchain system

8.1 Requirements for configuration management

The requirements of configuration management include the common configuration management functions, such as query, modification and statistics of configuration information in the blockchain system according to [ITU-T M.3400]. In addition, the blockchain management system also has the following functions:

a) Topology management

The architecture of blockchain system involves multiple "layer networks", including the resource layer network, protocol layer network, and business layer network that carry the blockchain system, and the blockchain application layer network that the blockchain system serves. It is required to manage the single-layer topology that constitutes these "layer networks", and the bearing, association and other relationships between different "layer networks" to support the flexible deployment of various blockchain system functional entities. At the same time, in the application scenario of managing multiple blockchain systems, it is optional to manage the single-chain topology such as sub-chain, side-chain, multi-chain, and the inter-chain association topology.

b) Blockchain ledger data storage capacity management

The blockchain ledger in the blockchain system uses the blockchain structure to store data in order to ensure that data is difficult to tamper with without authorization, which will lead to continuous growth of data on the chain. However, the limited storage space and data query efficiency of blockchain nodes cannot allow unlimited extension of the blockchain, so it is necessary to adjust the blockchain ledger data storage configuration strategy in time according to the length of the blockchain to achieve effective data storage and improve the query efficiency. Therefore, it is necessary to adjust the blockchain ledger itself and the data blocks constituting the ledger in time according to the blockchain operation. It is required to manage the blockchain ledger data storage strategy (such as block length, and block index mechanism), blockchain ledger data block configuration (such as optimal block size, maximum block size, and block timeout), blockchain ledger data on-chain and off-chain storage adjustment, etc.

c) Blockchain account management

Participants who contribute data to the blockchain and use the data stored on the blockchain are called blockchain accounts, which are different from the accounting management in [ITU-T M.3400]. Therefore, the blockchain account needs to be managed throughout its life cycle. It is required to manage account creation/deletion, permission configuration, behaviour monitoring, and account audits, etc. In particular, accounts contain public and private key pairs. The creation is recommended for launch by a client or by a smart contract or other automated functionality components. If an account name is recommended for customization, the account name is required to be unique in the system.

d) Smart contract management

A smart contract is a program written on the blockchain system that encodes the rules for specific types of distributed ledger system transactions in a way that can be validated, and triggered by specific conditions. Therefore, the whole life cycle management of smart contracts is required. It is required to manage smart contract script management (version configuration, parser configuration, etc.), smart contract instance deployment (automatic triggering conditions, running policies, etc.), active activation/deactivation of smart contracts, etc.

e) Consensus mechanism management

The consensus formed by different participants on the method of writing data into the blockchain is formalized as a consensus mechanism. A consensus mechanism is a set of rules and procedures by which mutual agreement is reached. A data consistency mechanism is used on a blockchain system to achieve the necessary agreement on a single data value or a single state of the network among distributed processes or multi-agent systems. To ensure the effectiveness of the consensus mechanism, sufficient nodes to participate in the consensus process are required, aligned with the objectives of the blockchain system, e.g., some blockchain systems only require a specific number of master node participants, while others require all token holders. Therefore, it is required to manage the specific consensus

mechanism template, the selection of multiple consensus mechanisms such as Byzantine fault tolerance (BFT), consensus mechanism based on election and verification (CEV), and practical Byzantine fault tolerance (PBFT), the deployment mode of consensus mechanism, and the activation/deactivation conditions of consensus mechanism. It should be emphasized that in the scenario of multi-chain unified management, the consensus mechanism for different blockchains needs to be configured separately. In the cross-chain scenario, the cross-chain consensus mechanism needs to be managed uniformly.

8.2 Requirements for performance management

The requirements of blockchain system performance management include the following functions consistent with [ITU-T M.3400]: performance monitoring, performance control and performance analysis in the blockchain system. It is recommended to support the analysis of performance data graphically.

Specific objects and performance parameters applicable to blockchain system performance management include but are not limited to:

a) Blockchain node performance management

It mainly manages the operation performance of the resource layer functional entities running the blockchain system. It is required to manage the number, status and resource usage of nodes in the blockchain, including but not limited to the status of the central processing unit (CPU), memory, storage and communication links between nodes. Through the measurement and analysis of the operational performance parameters of these resources, the basis for configuration change is provided for the allocation and recovery of resources such as communication, computing and storage.

b) Blockchain ledger performance management

It is recommended to manage the operational performance of functional entities related to blockchain ledgers, including but not limited to performance parameters such as the number of blocks, block generation time, block transactions per second (TPS) in the blockchain system. At the same time, it is recommended to cooperate with the configuration management function to obtain and analyse performance data by setting the optimal block size, maximum block size, block timeout and other configuration parameters to provide configuration strategies for improving the performance of the blockchain ledger.

c) P2P network performance management

The performance of the P2P network plays a decisive role in data transmission and blockchain ledger synchronization. Through monitoring and analysis of key performance indicators of the P2P network, it can provide the decision-making basis for adjusting the P2P network and optimizing the underlying bearer network that carries the P2P network. It is recommended to manage the number of hit/miss requests, the number of active users, and the number and structure of P2P traffic, etc.

d) Transaction performance management

Transaction refers to an incident or an operation that leads to a change in the status of a ledger, such as adding a record or an equivalent exchange based on currency. Transaction is the smallest unit of data written into the blockchain. Multiple transactions form blocks, and the blockchain ledger is formed through the trusted connection of blocks. Therefore, the performance of transactions is a direct reflection of the blockchain data sharing service capability. It is recommended to manage number of transactions completed, TPS (the number of transactions that can be processed per second), transaction completion time, etc. in the blockchain system.

8.3 Requirements for fault management

The requirements for fault management mainly include alarm information management, fault location, fault recovery, and trouble management.

a) Alarm information management

When the functional entities in the blockchain system run abnormally, alarm messages will be generated which mainly include node data out of synchronization, account abnormality, authentication certificate invalidation, smart contract disputes, consensus node abnormality, and illegal cross-chain transactions, etc.

At the same time, in the process of performance management, if the monitored performance parameters exceed the limit, an alarm will also be generated.

Blockchain failures may be caused by abnormal operation of functional entities such as the blockchain system resource layer, protocol layer and service layer. It is necessary to effectively manage the collection strategy of alarm information.

It is required to support the following functions consistent with [ITU-T M.3400] to manage the alarm information collection policy setting: alarm policy function set, alarm status modification function set, alarm reporting function set, and allow querying of existing alarm conditions.

b) Fault location

The generation of an alarm may mean that the operation quality of the functional entity itself has declined, the functional entity has failed, or the operation status of the associated functional entity is abnormal. Through the in-depth analysis of single functional entity alarms or the comprehensive analysis of multiple functional entity alarms, we can find the fault causes behind the blockchain system, locate the fault points, and guide the management personnel to carry out troubleshooting work.

It is recommended to accurately locate the cause of the fault in a blockchain system.

It is recommended to support the following functions consistent with [ITU-T M.3400]: fault localization policy function set, and running of diagnostic function set.

The failure of the resource layer of the blockchain system may come from the lack of network, computing and storage resources running the blockchain nodes or the failure of resource hardware and software.

The failure of the protocol layer and service layer may come from data inconsistency, process deadlock, algorithm defects, program bugs, etc.

c) Fault recovery

It is recommended to take corrective measures to eliminate the cause of the fault, either automatically or manually.

It is recommended to support the following functions consistent with [ITU-T M.3400]: management of repair process function set, and automatic restoration function set.

For node failures and resource layer failures, the redundancy of the blockchain system can ensure data consistency, and the relevant fault recovery methods are relatively simple. Generally, it can be solved through replacement or configuration change of single node equipment and software.

Due to the diversity of participants in the blockchain system and the complexity of multi-party joint debugging as a distributed system, the failure recovery process of the protocol layer and the service layer will be very complex. The minimum requirement in the recovery process is to ensure that the blockchain does not fork.

d) Trouble management

It is recommended to support trouble administration, which supports action to investigate and clear the trouble and provides access to the status of services and the progress in clearing each trouble.

If a smart contract or consensus failure causes data modification in the blockchain ledger, the blockchain will be forked. For this kind of failure, the blockchain participants need to agree again on whether to recognize the forking or data fallback, and re-run the blockchain at a new starting point.

It is recommended to support the following functions consistent with [ITU-T M.3400]: trouble information query function set, and trouble ticket administration function set.

8.4 Requirements for log management

The requirements for log management include log collection task management, log data management, log information analysis, etc.

a) Log collection task management

It is recommended to manage the log data collection by task. The blockchain log data collection strategy can be set according to the factors such as the management object, log content, log format, and collection frequency, and the manual and automatic log collection task activation/deactivation is supported.

b) Log data management

The operation log data of each functional entity in the blockchain can be obtained in real time or non-real time in the form of log data acquisition task. Relevant log data needs to be organized, pre-processed and indexed according to different dimensions to support data analysis for different purposes.

It is recommended to support different types of logs, including component operation logs, account operation log, contract execution logs, consensus process logs (block generation process logs), etc.

Referring to [ITU-T M.3705], it is recommended to support the query list of logs, backup of log data.

c) Log information analysis

Conduct in-depth analysis of blockchain operation log data from different nodes and functional entities to provide data and service support for fault location, fault recovery, and fault management.

It is recommended to conduct analysis of logs to find out the security risks of the blockchain system and the reasons for the weakening of performance, so as to increase the security and performance level of the blockchain.

Bibliography

[b-ITU-T X.1255] Recommendation ITU-T X.1255 (2013), *Framework for discovery of identity management information*.

[b-ISO 22739] ISO 22739:2020, *Blockchain and distributed ledger technologies – Vocabulary*.

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

Printed in Switzerland
Geneva, 2023