ITUPublications

International Telecommunication Union
Standardization Sector

ITU-T Technical Report

(12/2025)

XSTR.sg-lmcs

Technical Report: Security requirements and guidelines for distributed ledger technology (DLT)-based lifecycle management of computing services

Technical Report ITU-T XSTR.sg-lmcs

Technical Report: Security requirements and guidelines for distributed ledger technology (DLT)-based lifecycle management of computing services

Summary

In the computing service ecosystem, users subscribe to service from computing service providers who utilize computing resources supplied by various resource providers. As computing resources are naturally distributed and heterogeneous and are owned by multiple resource providers, there is a lack of trust among the different participants in this ecosystem. Consequently, the credibility and security of computing services is a major concern. From the computing service providers' perspective, coordinating and managing distributed resources securely and efficiently are both essential and challenging. From the perspective of users, the credibility and security of the service are primary considerations. Additionally, protecting the fair rights and interests of resource providers in a secure manner is also highly important.

In this Technical Report, ITU-T XSTR.sg-lmcs, distributed ledger technology (DLT) is used to establish trust among all participants in the computing service ecosystem. Security requirements and guidelines for DLT-based lifecycle management of computing services are provided.

Keywords

Computing service, computing power network (CPN), coordination of networking and computing (CNC), DLT, security, trust.

Note

This is an informative ITU-T publication. Mandatory provisions, such as those found in ITU-T Recommendations, are outside the scope of this publication. This publication should only be referenced bibliographically in ITU-T Recommendations.

Table of Contents

Technical Report ITU-T XSTR.sg-lmcs

Technical Report: Security requirements and guidelines for distributed ledger technology (DLT)-based lifecycle management of computing services

1 Scope

This Technical Report provides security requirements and guidelines for distributed ledger technology (DLT)-based lifecycle management of computing services.

2 References

[ITU-T X.1400] Recommendation ITU-T X.1400 (2026), *Terms and definitions for distributed ledger technology.*

[ITU-T Y.2501] Recommendation ITU-T Y.2501 (2021), *Computing power network – Framework and architecture.*

[ITU-T Y.3400] Recommendation ITU-T Y.3400 (2023), *Coordination of networking and computing in IMT-2020 networks and beyond – Requirements.*

3 Definitions

3.1 Terms defined elsewhere

This Technical Report uses the following terms defined elsewhere:

3.1.1 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.

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

3.1.3 distributed ledger technology (DLT) [b-ISO 22739]: Technology that enables the operation and use of distributed ledgers.

3.1.4 DLT system [[b-ISO/TC 307]: A system that implements a distributed ledger.

3.1.5 ledger [ITU-T X.1400]: Information store that keeps final and definitive (immutable) records of transactions.

3.2 Terms defined in this Technical Report

None.

4 Abbreviations and acronyms

This Technical Report uses the following abbreviations and acronyms:

ABAC Attribute-Based Access Control

ACL Access Control List

CA Certificate Authority

CNC Coordination of Networking and Computing

CPN Computing Power Network

DLT Distributed Ledger Technology

RBAC Role-Based Access Control

SLA Service Level Agreement

5 Overview

With the development of computing power networks (CPNs) [ITU-T Y.2501] [b-ITU-T Y.2502] and the coordination of networking and computing (CNC) [ITU-T Y.3400], computing service has become one of the most fundamental services. Within this service, users subscribe to service providers and utilize computing resources supplied by various resource providers. As computing resources are naturally distributed and heterogeneous and are owned by multiple different resource providers [b-ITU-T Q.4140] [b-ITU-T Q.4142], there is a lack of trust among the different participants in this ecosystem. Consequently, the security of computing services is a major concern. From the perspective of computing service providers, coordinating and managing distributed resources [b-ITU-T M.3347] securely and efficiently are both essential and challenging. From the perspective of users, the credibility and security of the service are primary considerations. Additionally, protecting the fair rights and interests of resource providers in a secure manner is important.

The lifecycle of a computing service can be divided into three stages: pre-service, in-service and post-service. Each stage involves distinct security requirements and challenges. Throughout these stages, distributed ledger technology (DLT) [b-ISO/TC 307] [ITU-T X.1400] is employed to establish trust among all participants in the computing service ecosystem. The security requirements and guidelines for DLT-based lifecycle management of computing services are also provided.

6 Security requirements of DLT-based lifecycle management for computing services

6.1 Security requirements for the pre-service stage

(1) An effective decentralized identity management mechanism is necessary, due to the multiple participants and dynamically changed resources of computing services.

In computing services, multiple roles are involved, including resource users, resource providers and service providers. Each role possesses unique identity information and employs distinct identity management mechanisms. The key challenge in managing computing services is effectively coordinating these diverse identities to establish mutual trust, recognition and interoperability among all participants.

Furthermore, within computing services, each resource collected from diverse providers carries unique identity information. Subsequently, these resources are dynamically allocated to service users at different intervals. Ensuring the authenticity of these resources is crucial for service providers to deliver computing services effectively.

By utilizing DLT, a decentralized identity management capability can be established in computing services. This capability facilitates interoperability between users and resource providers who possess varying identity credentials. It also enables the verification of the authenticity of all identity information.

(2) A dynamic and flexible access control mechanism is necessary due to the variety of computing resources and users' requirements.

The requirements for computing resources vary among different users. Therefore, service providers need to implement corresponding access control policies for different users. Both the access control list (ACL)-based and the role-based access control (RBAC) mechanisms are necessary and suitable for different scenarios within computing services. Attribute-based access control (ABAC) is also required for specific algorithm operators or dataset users to enable fine-grained access control.

Some resources are provided by third-party providers, each of which may offer distinct access control capabilities. Integrating these varied capabilities to enable seamless and efficient access control is critical and must be addressed during the operation of computing services.

By leveraging DLT, multiple access control strategies can be deployed and executed automatically for different users.

6.2 Security requirements for the in-service stage

(1) With numerous computing resource providers participating in computing service, a fair resource-matching mechanism is essential.

Computing service operates in an environment characterized by diverse and widely distributed computing resources. As CPN/CNC technologies evolve, an increasing number of providers are expected to participate in these services. A major challenge for service providers is to fairly and equitably select the most suitable resources from a large pool of computing resource providers for the computing service users. Establishing a trusted, fair and impartial resource-matching mechanism is essential. Such a mechanism should ensure efficiency and equitability, taking into account the reputation of various providers.

Leveraging the multi-party consensus mechanism and data immutability of DLT, a fair and transparent reputation management system can be established for computing services. Each computing resource provider is assigned a reputation value, which serves as a foundation for conducting computing services. This approach protects the interests of high-quality resource providers and promotes the progression of computing services.

(2) The management and orchestration of computing resources in computing service are difficult. An efficient and automatic data synchronization mechanism is necessary.

In computing services, resources are spatially distributed across various data centres and edge nodes. Temporally, these resources change dynamically and can be accessed or released on demand. The requirements of resource users are also flexible, dynamic and highly variable. These characteristics impose significant demands on collaborative resource scheduling within computational services. In particular, efficient and automated synchronization mechanisms for information such as resource scheduling strategies, end-to-end service level agreements (SLAs) and security mechanisms for user services, as well as business and user data, become critically important.

Leveraging multi-party consensus mechanisms of DLT, data across resource scheduling and management nodes can achieve automatic synchronization. This enables high consistency in scheduling strategies and business configurations, thereby improving the overall efficiency of computing services.

(3) As many participants are involved in the computing service, corresponding mechanisms need to be provided, to ensure the fairness, credibility and traceability of the entire service lifecycle.

Computing service involves multiple participants, including computing resource users, computing resource providers and service providers. It is also common for a single service to engage multiple resource providers simultaneously. Due to the inherent lack of trust among these different participants, ensuring fairness and impartiality throughout the lifecycle of computing services, as well as credibility and traceability of each transaction, becomes critically important.

By leveraging DLT, all participants can record relevant information from the computing service process in a distributed ledger. This makes transaction-related information trustworthy and traceable. Furthermore, the consensus mechanism of DLT ensures all participants acknowledge the transaction process, thereby reducing the potential for disputes in the service lifecycle.

6.3 Security requirements for the post-service stage

The computing service involves multiple participants, underscoring the need to develop a fair and mutually trusted service settlement model to improve settlement efficiency.

Establishing a new and equitable service settlement mechanism is essential to facilitate settlement between users and providers after computing services. Improving the accuracy and integrity of accounting information and the settlement period is critical for both service providers and computing resource providers. Such an initiative will not only benefit all involved parties but also promote the broader development of computing services.

By leveraging DLT, a decentralized computing service accounting model can be established. This model supports automated reconciliation between computing resource providers and service providers. Furthermore, DLT offers robust technical support for sharing security threat intelligence and coordinating risk mitigation strategies across the computing services network.

7 Security guidelines for DLT-based lifecycle management of computing services

7.1 Security guidelines for the pre-service stage

(1) Identity management mechanism

In computing services, multiple resource providers are involved. Each resource provider possesses unique identity information and utilizes distinct identity management mechanisms. To coordinate these diverse identities and establish mutual trust between the various resource providers and service providers, a distributed identity management mechanism based on DLT is proposed. By leveraging DLT and smart contracts, different identities and credentials can be mutually recognized and trusted.

The DLT-based distributed identity management mechanism is illustrated in Figure 1. Computing resource providers can hold multiple verifiable identities and credentials issued by the third certificate authority (CA), which can be presented to service providers as required.

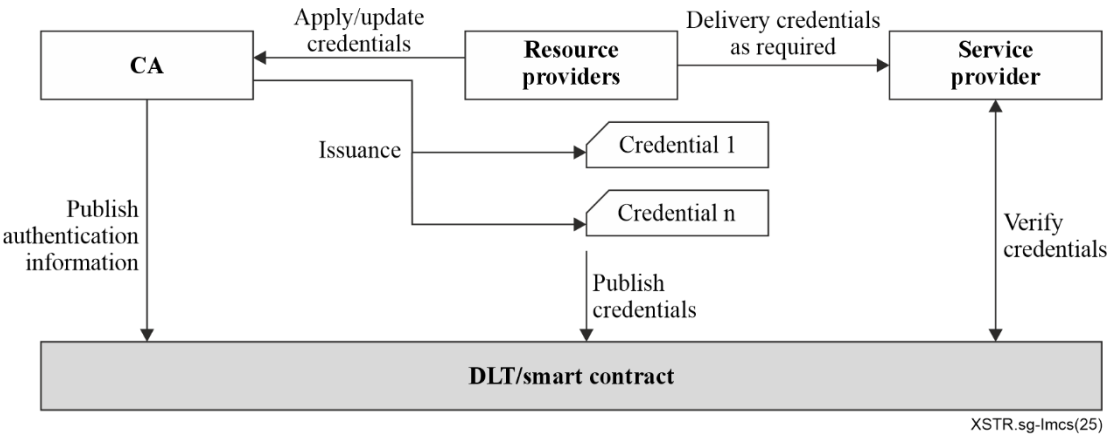

Figure 1 – Distributed identity management mechanism

The identity authentication process based on credentials consists of the following steps:

1) Credential application: resource providers apply for identity credentials from the CA.

2) Credential issuance: upon validating the identity information of the resource provider, the CA issues the credential and subsequently uploads both the identity documents and the verifiable credentials to the DLT.

3) Credential verification: when applying to provide computing services, the resource provider submits their credential information as required to the service provider. The service provider

then accesses the DLT to retrieve the relevant credential information for credential verification.

This mechanism allows all resource providers in computing services to own their different credentials issued by different CAs. Based on the credentials and corresponding information stored on the DLT, the service provider makes identity authentication decisions.

(2) Access control mechanism

To accommodate diverse computing service requirements from different users and their applications for various computing resources, it is essential to flexibly implement differentiated access control strategies based on DLT, thereby ensuring the security of both computing resources and services.

When delivering computing services, operators need to preconfigure and support multiple access control mechanisms. These access control policies are encoded into smart contracts and deployed on the DLT.

When a user applies for computing services, service operators receive the application. The operator then processes the request and submits an access control query to the DLT. Once an access control decision is generated by the DLT, the operator receives the result and provides a final response to the service applications.

If the computing services request satisfies the conditions defined in the relevant smart contract of the DLT, the contract automatically executes to determine the user's eligibility for the requested computing resources. This automated process ensures secure, efficient and transparent management of access to computing services, in accordance with established policies.

The smart contracts on the DLT specify various types of access control mechanisms, such as ACL, RBAC and ABAC. Service operators can also dynamically update these strategies according to resource management needs, enabling more flexible and effective access control for users.

7.2 Security guidelines for the in-service stage

(1) Resource-matching mechanism

A resource-matching mechanism is established by incorporating the reputation of various computing resource providers. The detailed process is illustrated in Figure 2.

When a user applies for computing services, the service operator receives the request and queries the DLT to obtain a list of computing resource providers that meet the specified requirements. This list includes relevant information, such as the providers' capabilities, reputation ratings and availability. The operator then returns the list of suitable providers to the user, who selects the most appropriate one based on their needs. Following this selection, the computing service is delivered by the chosen provided.

The smart contract on the DLT automates request handling and the provider-matching process. It automatically retrieves a list of qualified providers from the DLT and, once the user makes a selection, triggers the corresponding service agreement. This ensures that the rights and obligations of both parties are clearly defined and programmatically enforced.

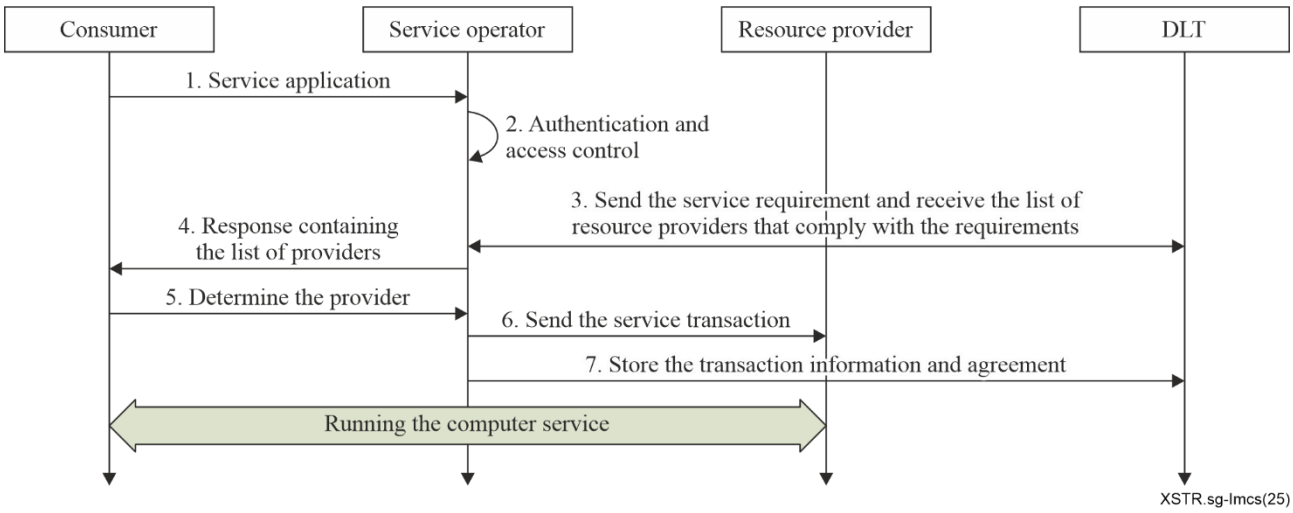

Figure 2 – Flows of resource-matching mechanism

By leveraging the immutability of DLT, a decentralized reputation rating system for computing resource providers is established. Upon completing a computing service, the user may submit an evaluation of the provider. The assessment is permanently recorded on the DLT, serving as a trustworthy reference for future users. Providers with high reputations will receive more frequent and higher-priority recommendations for computing service opportunities. This mechanism enhances transparency, fairness and trust throughout the service process, while encouraging continuous quality improvement in the service.

(2) Data synchronization mechanism

By leveraging DLT, a data synchronization mechanism enables the automatic synchronization of distributed data between the computing service management system and the regional resource management system across different providers. All relevant data, including resource status, task allocation, and network operation and management information, can be updated and shared in real time.

By utilizing smart contracts on the DLT, the computing service management system can encode orchestration and scheduling strategies into automated workflows. The regional resource management system then automatically executes scheduling tasks according to the rules defined in the smart contracts, minimizing manual intervention and enhancing operational efficiency and accuracy.

This mechanism also records network operational information (such as resource usage, fault logs and performance metrics) and ensures the authenticity and immutability of such data through the consensus mechanisms of DLT. This provides reliable data support for the operational maintenance and management of the computing services.

By leveraging these capabilities, computing services achieve enhanced coordination, transparency and efficiency, thereby ensuring optimal resource utilization and operational integrity across multiple providers.

(3) Transparent and traceable service processes

By utilizing smart contracts and the consensus mechanisms of DLT, the mechanism ensures that all transactions and interactions among participants are immutably recorded and automatically verified. This eliminates trust barriers, reduces disputes and improves the overall efficiency of the computing service process. Service-related data, such as service requests, resource allocations, task execution logs and payment details, are stored on the ledger, with each transaction cryptographically hashed and linked to previous records, forming a tamper-resistant and auditable chain of events.

Furthermore, encoding SLAs and business rules into the smart contracts of DLT ensures that all actions are transparent and traceable. Every service-related operation and transaction is recorded on the DLT, providing full visibility to all participants. Each step throughout the service process is immutably preserved, enabling comprehensive end-to-end traceability and auditability.

7.3 Security guidelines for the post-service stage

(1) Settlement process

A decentralized and trustworthy settlement mechanism is established using DLT. By leveraging the consensus mechanisms of DLT, settlements between service operators and providers, as well as between service operators and users, can be triggered automatically in a fair, accurate and efficient manner.

When a computing service user utilizes resources from a provider, the usage details are recorded on the DLT ledger. Upon service completion, the service operator retrieves the settlement information from the DLT, whether recorded individually by operator or jointly by both parties. Based on this information, the operator calculates the payment and completes the settlement with the provider. The settlement details are recorded on the DLT ledger to ensure future reference and auditability. The detailed process is illustrated in Figure 3.

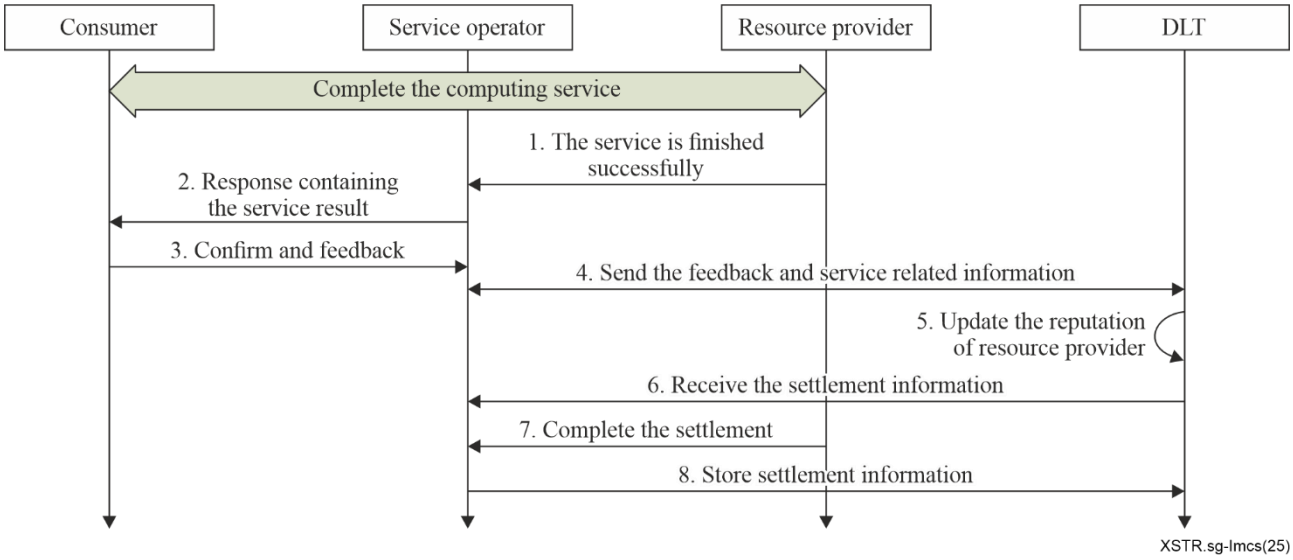

Figure 3 – Flows of decentralized and trustworthy settlement

(2) Reputation update

Upon completion of computing services, the service operator records and stores all relevant transaction information, including details of the interaction between the resource provider and the user, as well as the user's service feedback, on the DLT. Based on this order and feedback data, smart contracts of DLT automatically update the reputation of the resource providers. These updated reputations are also stored immutably on the DLT.

The reputation rating of resource providers is determined based on multiple factors, such as:

– Number of service transactions: the more frequently a provider is selected and participates in computing services, the higher their reputation value becomes.

– Service feedback: after completing the computing services, the user submits an evaluation. Providers receiving positive feedback are assigned a higher reputation score.

– Quality of computing resources: this includes the scarcity of resources (e.g., specialized data model processing capabilities and unique algorithms), the scale of resources and the level of service specifications.

– Other relevant data: additional metrics may include the provider's qualifications, years of service and other performance indicators.

Based on these factors, the reputation of computing resource providers is automatically calculated in real time using the smart contracts of DLT. This ensures that high-quality providers receive priority in service providing and motivates all providers to participate more actively in computing services.

Appendix I

Scenario and security requirements for aggregation and integration of computing resources

I.1 Scenario of aggregation and integration of computing resources

In this scenario, service operators and computing resource providers collaborate to deliver scalable and flexible computing services. Each provider operates its own infrastructure, such as data centres, edge nodes and cloud platforms which are distributed across diverse geographical locations and exhibit heterogeneous capabilities. A key challenge lies in aggregating these distributed resources into a unified pool and integrating them seamlessly to enable efficient service delivery to end users.

In the context of computing resource aggregation and integration, three specific modes are defined:

(1) Operational integration mode

In this mode, the service operator's operational system serves as a centralized entry point through which third-party resource providers connect and register their available computing resources. This enables the aggregation of resources from multiple providers into a unified resource pool, accessible via the operator's platform.

The service operator acts as the primary interface for end users, offering a single point of access to a diverse set of computing resources. Its role is focused on facilitating connection between resource users and third-party providers. Unlike deeper integration models, the operator in this mode does not undertake orchestration, scheduling or direct invocation of third-party resources. Rather, its responsibility concludes at providing a platform for resource discovery and request facilitation.

(2) Orchestration management integration mode

In this model, computing services are delivered through the service operator's resource orchestration management system, which aggregates resources from multiple providers. The service operator interfaces with the third-party resource orchestration platforms to manage and schedule computing resources, while the third-party systems collaborate to deliver and maintain those resources.

For resource users, all interactions occur exclusively with the service operator, with no direct engagement with the underlying computing resource providers. The service operator supplies the computing resources directly to users and manages all aspects of service settlement.

(3) Computing resource direct integration model

By deploying plug-ins or agents directly onto third-party computing resources, the computing service operator gains the ability to uniformly orchestrate and schedule all available resources. This enables the direct provision of computing services to end users. Centralized control of resources ensures efficient utilization and streamlined operations, resulting in faster and more reliable service delivery.

I.2 Security requirements for aggregation and integration of computing resources

Security requirements, including trust, transparency, data protection and compliance, must be addressed consistently across all three integration models to ensure a secure and reliable environment for computing resource management and service delivery.

(1) Operational integration mode

In this model, computing resources are supplied directly by third-party resource providers via the service operator's resource orchestration management system. The operator does not directly manage the orchestration or invocation of these resources; these responsibilities are retained by the third-party providers.

In this scenario, both users and providers require a security mechanism capable of recording resource usage information in a trusted, traceable and tamper-proof manner. This mechanism helps prevent disputes and ensures transparency and fairness throughout the transaction process. The use of DLT for recording resource usage in an immutable manner offers a high level of security and trust for all transactions.

(2) Orchestration management integration mode

In this model, the service operator aggregates computing resources from third-party providers through its resource orchestration management system. Users interact exclusively with the service operator which supplies the computing resources directly and manages all settlement activities.

In this scenario, operators must ensure that resource usage information, such as allocation, duration of use and settlement details, is recorded securely to prevent tampering. DLT enables all parties to access a verifiable and transparent view of resource usage and settlement records. By recording all transactions on a shared and immutable ledger, DLT facilitates quick and fair dispute resolution.

Furthermore, DLT provides a detailed and unalterable audit trail of all transactions and resource usage records. This traceability supports the precise identification of the root cause of any operational or settlement issues.

(3) Computing resource direct integration model

a) Fair and transparent measurement of computing resources

Providers must ensure that the computing resources they supply are measured accurately and transparently. This is essential for maintaining trust and guaranteeing that providers receive fair compensation for their contributions.

b) Security and efficient matching of computing resources

Providers require a mechanism to match their resources with demand in a manner that maximizes utilization, security and efficiency. This includes ensuring a fair and transparent matching process, giving all providers an equal opportunity to participate in resource allocation.

c) Differentiated services for providers

The system should support differentiated services for distinct providers. For instance, certain providers may qualify for higher-priority matching or more favourable compensation terms. Such differentiation can incentivize providers to contribute more resources or higher-quality services, thereby enhancing the overall efficiency and appeal of the platform.

DLT is particularly valuable in this context. It offers transparent metrics for resource management and matching while ensuring equitable treatment of all providers during allocation. Through smart contracts, DLT enables intelligent scheduling algorithms that incorporate factors such as resource availability, demand patterns and specific task requirements. Additionally, DLT provides an immutable record of all transactions, ensuring integrity and transparency throughout the resource management processes.

Bibliography

[b-ITU-T M.3347] Recommendation ITU-T M.3347 (2012), *Requirements for the NGN service activation across the interface between the network management system and the element management system.*

[b-ITU-T Q.4140] Recommendation ITU-T Q.4140 (2023), *Signalling requirements for service deployment in computing power networks.*

[b-ITU-T Q.4142] Recommendation ITU-T Q.4142 (2024), *Signalling architecture for service orchestration in computing power networks.*

[b-ITU-T Y.2502] Recommendation ITU-T Y.2502 (2025), *Computing power network – Authentication and orchestration architecture.*

[b-ISO 22739] ISO 22739:2024, *Blockchain and distributed ledger technologies – Vocabulary*.

[b-ISO/TC 307] ISO/TC 307:2016, *Blockchain and distributed ledger technologies*.