ITUPublications

International Telecommunication Union
Standardization Sector

ITU-T Technical Paper

(04/2024)

HSTP-DLT-CG

Construction guidelines for city-level distributed ledger technology (DLT) infrastructure

Technical Paper ITU-T HSTP-DLT-CG

Construction guidelines for city-level distributed ledger technology (DLT) infrastructure

Summary

This Technical Paper ITU-T HSTP-DLT-CG specifies the city-level distributed ledger technology (DLT) infrastructure framework including stakeholders, construction principles and key processes. Stakeholders are divided into governance parties, business parties, users, technical providers and third-party support parties. Construction principles include compliance principles, security principles, hierarchical authorization principles, high availability principles, and traceability principles. The key process is divided into a design system reference architecture, construction of a standard specification system and construction of a security assurance system.

Keywords

Construction principles, distributed ledger technology, infrastructure, key process.

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.

Editor:

Weiwei Qiu
Hangzhou Qulian Technology Co., Ltd.,
China
Tel: +86 13777825451
E-mail: qiuweiwei@hyperchain.cn

Xiaofeng Chen
Zhejiang University,
China
Tel: +86 15088675364
E-mail: chenxf.alfred@zju.edu.cn

Xiangjuan Jia
Hangzhou High-Tech Zone (Binjiang) Institute of Blockchain and Data Security
China
Tel: +86 18794770902
E-mail: jiaxiangjuan@bcds.org.cn

Xiaohu Yang
Zhejiang University,
China
Tel: +86 13605709130
E-mail: yangxh@zju.edu.cn

Yi Sun
Institute of Computing Technology, Chinese Academy of Sciences,
China
Tel: +86 18611907658
E-mail: sunyi@ict.ac.cn

Table of Contents

Technical Paper ITU-T HSTP-DLT-CG

Construction guidelines for city-level distributed ledger technology (DLT) infrastructure

1 Scope

This Technical Paper proposes a framework for city-level distributed ledger technology infrastructure construction. The framework includes stakeholders, construction principles and key processes of city-level infrastructure construction based on distributed ledger technology (DLT). This Technical Paper applies to:

- Provide a reference for stakeholders and organizations planning and constructing city-level DLT infrastructure.
- Provide system reference and technical guidance for city-level DLT infrastructure service providers.

2 References

[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 Technical Paper uses the following terms defined elsewhere:

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

3.1.2 DLT [ITU-T X.1400]: A kind of distributed ledger with confirmed blocks organized in an append-only, sequential chain using cryptographic links. DLTs are designed to be tamper resistant and to create final, definitive and immutable ledger records.

3.1.3 smart contract [ITU-T X.1400]: A program written on a 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 Technical Paper

None.

4 Abbreviations and acronyms

This Technical Paper uses the following abbreviations and acronyms:

DDoS	Distributed Denial of Service
DLT	Distributed Ledger Technology
FL	Federated Learning
IDE	Integrated Drive Electronics
IP	Internet Protocol
MPC	Multi-party Computation

SDK	Software Development Kit
SSL	Secure Socket Layer
TEE	Trusted Execution Environments

5 Conventions

The following conventions are used in this document.

– The keywords "**is required to**" indicate a requirement which must be strictly followed and from which no deviation is permitted, if conformance to this Technical Paper is to be claimed.

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

– The keywords "**can optionally**" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

6 Framework of city-level DLT infrastructure construction

The framework for city-level distributed ledger technology (DLT) infrastructure includes stakeholders, construction principles, and key processes, as shown in Figure 1.

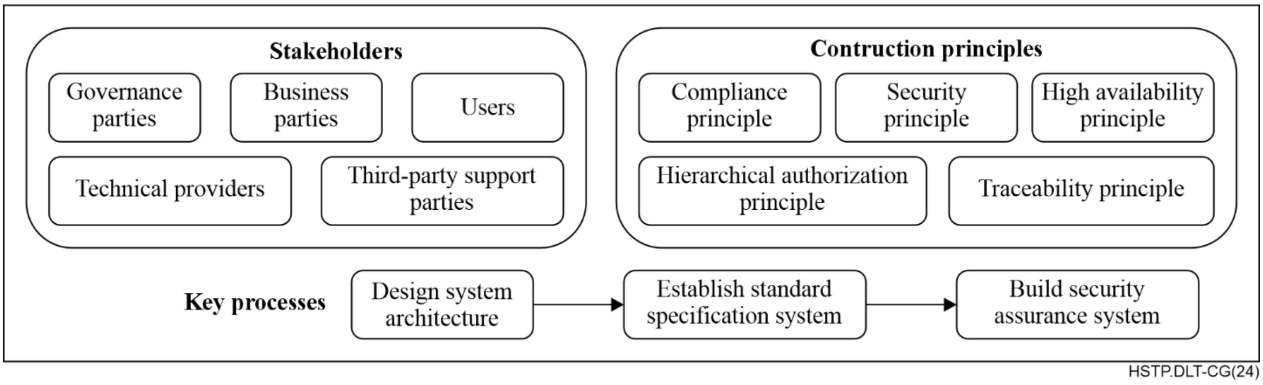
Stakeholders
Governance parties
Business parties
Users
Technical providers
Third-party support parties
Contruction principles
Compliance principle
Security principle
High availability principle
Hierarchical authorization principle
Traceability principle
Key processes
Design system architecture
Establish standard specification system
Build security assurance system
HSTP.DLT-CG(24)

Figure 1 – Framework of city-level DLT infrastructure construction

Stakeholders include governance parties, business parties, users, technical providers and third-party support parties.

Construction principles include compliance principles, security principles, hierarchical authorization principles, high availability principles, and traceability principles.

The key processes includes three parts: design system reference architecture, establish standard specification system, and build security assurance system.

7 Stakeholders

7.1 Governance parties

The governance parties are institutions or organizations that conduct governance audits on DLT businesses in its jurisdiction and implements end-to-end joint governance before, during, and after the entire chain. The activities of the governance party are recommended to include but are not limited to:

- Providing a governance platform that supports different governance roles in compliance testing and monitoring the entire data of DLT businesses within its jurisdiction.
- The unified governance platform for DLT joint defence and joint control needs to support the access of heterogeneous chains. The access method is recommended to follow the principle of low threshold and high efficiency to reduce the access costs of businesses while ensuring real-time governance and penetration depth of governance.
- Configuring DLT data intelligent management platforms that support the collection, parsing, analysis of on-chain data, and real-time reporting of abnormal behaviours. Analyse and judge the governance results and carry out corresponding control and disposal. Monitor and provide early warning through situational analysis and visualize the governance results and analysis results.
- Constructing a DLT with identity, and its nodes are endorsed by authoritative identity certification agencies.
- Supporting the governance of the content on the chain. Establish governance rules according to relevant laws and governances, conduct keyword matching on the on-chain content by accessing the thesaurus, and deal with the chains that violate the governances.
- Supporting pre-, during-, and post-governance of DLT through functions such as pre-chain inspection, on-chain control, information reporting, and command execution, tracking the behaviour of DLT nodes, and realizing penetration governance.
- Providing data desensitization and privacy computing capabilities to carry out joint governance while ensuring the privacy and security of business data.
- In terms of intervening in violations, the regulator needs to obtain the entity identity mapped by the address on the chain to carry out targeted intervention.
- Understanding the standardized specifications of DLT technology to supervise and manage city-level DLT applications and ensure the technical norms and standards of the applications.

7.2 Business parties

The business parties are entities responsible for operating, maintaining, and managing city-level DLT construction business. Generally, it is an enterprise or institution. The activities of the business party are recommended to include but are not limited to:

- Determining core requirements and forming development and maintenance requirements materials.
- Designing, developing, and maintaining city-level DLT construction business systems.
- Conducting tests and acceptance for relevant functions in the system.
- Providing multiple development language interfaces for the technical personnel to use.
- Providing deployment-related documents, materials and tools.
- Providing corresponding software development kits (SDKs).
- Possessing the operation and maintenance capabilities of business heterogeneous chains. The business party needs to report events and data related to business heterogeneous chains to the main chain to complete governance access.
- Supporting the full lifecycle management of business chains including registration, review, freezing, unfreezing, cancellation, and so on.
- Possessing business basic information management function. When the application is accessed, it is recommended to provide basic information about the application including the unique identification of the application chain, the name of the application chain, the company, Internet protocol (IP), etc.

- Possessing business interface management function, different permissions are set for different interfaces.
- Possessing a business chain control function, when the business chain has serious violations, it freezes and other operations are performed.

7.3 Users

The users are the users who use the DLT business system. The activities of the user party are recommended to include but are not limited to:

- Using physical identity services to log in and operate the business system.
- Users need to register a unified digital identity on the identity chain firstly, and the identity management smart contract of the identity chain completes the import of the heterogeneous chain accounts and the mapping between the unified digital identity.
- For regulators, the business activities of the same business user in different DLTs are tracked and located by its unified digital identity, further improving the efficiency of the governance intervention.
- Possessing a multi-level permission management function, different permissions are set for different roles.
- Supporting unified digital identity management, supporting digital identity interconnection and intercommunication across regions, departments, institutions and chains.
- Supporting full life cycle management of users including user creation, update, freezing, unfreezing, cancellation, and other operations.
- Supporting role-based user access control. Effectively ensure that the users access according to the set access range and access method, and provide preventive measures to avoid unauthorized tampering by the users.
- Supporting trusted digital identity services to complete transaction requests and event subscriptions between business heterogeneous chains.

7.4 Technical providers

Technical providers refer to the entities that provides DLT technology services. The activities of the technical providers are required to include but are not limited to:

- Determining the requirements of the DLT technology.
- Designing a reasonable and complete plan for the DLT technology requirements.
- Designing, developing and maintaining service components or smart contracts in the DLT system.
- Testing and validating the relevant functions in the DLT system.
- Planning for the correct implementation and deployment of the DLT services.
- Providing full-process maintenance services for the system.

7.5 Third-party supporters

The third-party supporter is recommended to be responsible for improving external third-party support services for the construction of city-level DLT infrastructure, such as certificate authentication services, identity authentication services, etc., to strengthen the system and improve its functions.

8 Construction principles

8.1 Compliance principle

The establishment and operation of city-level DLT applications and supporting facilities are recommended to meet compliance requirements and consider the following conditions:

- The design document clearly specifies the responsibilities and permissions of the ledger system, making the operation of the ledger system standardized.
- The system adopts the encryption protection and security management for the user personal information.
- Compliance management is carried out in accordance with scientific management principles such as independence, systematicity, full participation, mandatory, clear management status and responsibilities.
- Comply with relevant data privacy and protection governances.

8.2 Security principle

City-level DLT applications are recommended to meet security principles and consider the following conditions:

- Have conditions such as system confidentiality and security protection, selection of private key encryption algorithms, and transmission security of data at all levels of the system.
- Have security mechanisms and emergency handling mechanisms and measures that are continuously improved.
- Ensure the security and reliability of the identities of the parties joining the nodes, ensure the authenticity and legality of assets, and the controllability of node permissions.
- Ensure the security of data generation, transmission, storage and access. It is advisable to separate keys from the data to ensure confidentiality.

8.3 Hierarchical authorization principle

The authorization division, granting, and revocation of city-level DLT applications are recommended to be included in the system lifecycle management and consider the following conditions:

- Establish and improve the account management system of stakeholders such as account management, relevant party management, permission management, authorization scope, etc.
- Reduce unnecessary information collection, adopt the principle of least privilege and a multi-role authorization scheme.
- Grant corresponding permissions according to the clear division of the level of stakeholders, without exceeding authority. Different levels of stakeholders follow the principle of least privilege to obtain the corresponding data access permissions.

8.4 High availability principle

Considering the application field of the DLT technology, high availability is one of the characteristics that the ledger system is recommended to fully plan for, and the system is recommended to consider the following conditions:

- The city-level DLT is recommended to always provide effective service to prevent server failures and other issues from causing service unavailability.
- Avoid and reduce downtime caused by system crashes and attacks or maintenance operations.
- Possess high response processing capability and be able to ensure its core functional requirements when facing high concurrency traffic.

- Possess automatic backup and restoration capabilities, and the system is restored to the nearest backup point when it crashes or is attacked.
- Possess disaster recovery capabilities such as establishing a dual-active centre in the same city, a remote disaster recovery data centre, etc.
- Support fault tolerance mechanism and automatically switch to standby nodes when the system fails, ensuring the continuity and stability of the system.
- Support automated operation and maintenance tools and technologies such as automated deployment, monitoring, fault diagnosis and recovery, etc., to improve the reliability and availability of the system.

8.5 Traceability principle

The city-level DLT application system based on the DLT is recommended to have data traceability capabilities, and is recommended to consider the following conditions:

- Generate unique identification and certification of asset-related data during the entire life cycle.
- Traceable data includes data generation time, data type, data source, data query information, authorization information, ownership changes, historical records, data change and access records, and so on.
- The traceability of a system, user, and authorization information data are recommended to be divided according to the sensitivity and importance of the data, and the corresponding traceability schemes are recommended to be adopted according to the different natures.
- The system displays different amounts of data based on the sensitivity and importance of the data to meet different tracing requirements.

9 Key process

9.1 Designing system architecture

The design of the reference architecture for the construction of the city-level DLT infrastructure is recommended to include the DLT basic technology layer, DLT protocol extension layer, DLT middleware service layer, and DLT industry application layer.

9.1.1 DLT basic technology layer

The DLT basic technology layer is recommended to include but is not limited to:

- A complete and robust DLT underlying framework and module components.
- The underlying platform is compatible with business models such as data certification, account management, and complex smart contract logic.
- The underlying platform meets requirements for high concurrency, low latency, and massive data storage.
- Supporting multiple consensus algorithms.
- Providing privacy protection mechanisms such as partition consensus, private transactions, and ledger encryption.
- Possessing security governance functions such as identity authentication / access control mechanisms, account user systems, multi-level permission management, and system security audits.
- Providing a variety of data management modules including DLT basic technology foundation functions such as data archiving, data indexing, trusted file sharing, and trusted data sources.

- Supporting the storage of various data types including structured and unstructured data such as text, images, and audio and video storage.
- Supporting dynamic addition and deletion of nodes to achieve horizontal expansion of the node network.
- Supporting multi-level hierarchical networking of various node types including consensus nodes, non-consensus nodes, and light nodes to meet the needs of large-scale networking.
- Providing a permission system and governance mechanism to protect business commercial privacy and comprehensively ensure system security.

9.1.2 DLT protocol extension layer

The DLT protocol extension layer is recommended to include but is not limited to:

- On-chain and off-chain collaborative components including trusted storage, data sharing, and federated computing modules, to meet the data value transfer needs under privacy protection requirements.
- Cross-chain components including verification engines, cross-chain gateways, and cross-chain protocols, to provide a unified cross-chain specification and standard framework for homogeneous/heterogeneous chains.

9.1.3 DLT middleware service layer

The DLT middleware service layer is recommended to include but not be limited to:

- Providing an integrated management service platform for construction, management, development, and application, connecting the supply and demand sides of the DLT application industry.
- Providing visual monitoring of the DLT's operating status, underlying resources, and DLT alliance organization, as well as system log analysis and alerts.
- Supporting customizable alarm services, allowing users to define monitoring indicator thresholds, log keywords, and alarm channels.
- Providing multi-level log management capabilities including node operation logs, host logs, and system logs.
- Providing DLT development services that meet the customization and personalized deployment requirements of upper-layer applications.
- Providing convenient DLT application development tools and environments, including DLT software development kits (SDK), smart contract development, security audit services, one-stop programming environments, key management, etc.
- Supporting the creation of various types of contracts such as Solidity/Java/Go, and implementing online editing, viewing of historical code, debugging, and other functions through online integrated drive electronics (IDE).
- Possessing security testing functions, fully ensuring the security of smart contracts by analysing contract code and scanning language vulnerabilities.
- Providing a visual contract code generation tool that supports flexible configuration from multiple dimensions such as business permissions, data table configuration, and function configuration, helping users reduce learning costs and quickly creating contract templates.

9.1.4 DLT industry application layer

The DLT industry application layer is recommended to meet the following requirements:

- Compliance principles
- Security principles

- Graded authorization principles
- High availability principles
- Traceability principles

9.2 Establishing a standard specification system

The construction of the standard specification system for the city-level DLT infrastructure includes, but is not limited to:

- Establishing basic standard specifications including terminology definitions, method standards, coding standards, etc.
- Establishing data access standard specifications.
- Establishing a classification and grading model.
- Establishing standards for compiling on-chain data directories, collecting on-chain data, governing the quality of on-chain data, and exchanging on-chain data.
- Establishing guidelines for building on-chain systems.
- Establishing guidelines for building on-chain applications.
- Establishing guidelines for on-chain application security.
- Establishing performance evaluation standard specifications.
- Providing practical guidelines for different types of business and scenarios.
- Establishing responsibility lists, evaluation indicators, evaluation methods, and evaluation improvements for DLT applications in various fields.

9.3 Establishing a security assurance system

The construction of the security guarantee system for the city-level DLT infrastructure includes but is not limited to:

- Ensuring that the DLT infrastructure does not support DLT applications and businesses that exceed its security protection level.
- Ensuring that the DLT infrastructure has node identity management and access control to prevent malicious nodes from joining the DLT infrastructure.
- Providing node identity verification mechanisms such as public key infrastructure (PKI) certificates to restrict node access.
- Adopting a dynamic configuration node communication network to avoid single point failures affecting the entire DLT network communication.
- Establishing an interface layer access control policy to strictly limit the access rights of different types of users to DLT infrastructure resources such as read and write permissions.
- Providing smart contract security collaboration specifications for users and establishing a smart contract security inspection mechanism.
- Conducting basic security checks on uploaded smart contracts, including baseline security checks and framework security checks, and informing users of the inspection results and risk situations.
- Supporting secure transmission layer (secure socket layer (SSL)) technology that complies with standards to ensure data integrity, confidentiality, and source credibility.
- Supporting privacy computing technologies, including secure multi-party computation (MPC), trusted execution environments (TEE), federated learning (FL), etc., to fully utilize data value without leaking the original data.

- Using password algorithms, technologies, products, and services that comply with national password management department and industry standard specifications.
- Being able to resist active network security attacks such as distributed denial of service (DDoS).
- Developing sound emergency response plans to deal with security incidents and vulnerabilities in a timely manner.
- Conducting regular security evaluations and vulnerability scans to promptly discover and fix security issues.