

ICS 35.240
CCS L 70



**NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GB/T 47700-2026

**Blockchain and distributed ledger technology - Industry
application - Guidelines for cross-border trade services**

区块链和分布式记账技术 行业应用 跨境贸易服务指南

Issued on: May 25, 2026

Implemented on: September 1, 2026

**Issued by: State Administration for Market Regulation;
Standardization Administration of the PRC**

Table of Contents

2	Normative references
5	Service Principles
6	Service Framework
7	Relevant Parties
8	Key Processes
8.1	Digital Identity Services
8.2	Electronic Business Services
8.3	Digital Document Service
8.4	Documentary Rights Certificate Services
8.5	Electronic Data Interchange Service
8.6	Regulatory Data Services
9	Blockchain Platforms

2 Normative references

This document has no normative references.

4. Abbreviations The following abbreviations apply to this document. URI. Uniform Resource Identifier

5 Service Principles

5.1 Traceability Principle Blockchain platforms provide services for digital identity, electronic business, digital documents, document rights certificates, and electronic data interchange. Key processes such as service provision and regulatory data services are made fully traceable.

5.2 Data Standardization Principles International trade documents conform to the requirements for trade document format and data item (data element) layout, and are prepared in accordance with GB/T 17699 (all parts). EDI message exchange.

5.3 Data Privacy and Security Principles Blockchain platforms ensure data privacy and the security of sensitive information storage, transmission, and application.

5.4 Principle of Regulatory Compliance The blockchain platform complies with relevant national policies and regulations, as well as international trade practices and rules. Its application architecture design includes provisions for regulatory functions and access control. To meet the regulatory requirements of regulatory agencies.

6 Service Framework

The blockchain-based cross-border trade service framework consists of three layers. stakeholders, key processes, and the blockchain platform (see Figure 1). Stakeholders include technology service providers, identity providers, service users, and service regulators. Key processes include digital identity services and electronic industries. Service functions, digital document services, document rights certificate services, electronic data interchange services, and regulatory data services. The blockchain platform includes a platform department. The service framework includes deployment, computing services, storage services, and communication services. Typical application scenarios are shown in Appendix A.

7 Relevant Parties

7.1 Technical Service Provider A technology service provider is an organization or institution that provides blockchain platform design, development, and operation and maintenance services. Its main activities should include.

- a) Identify the relevant requirements for blockchain technology;
- b) Design a reasonable and comprehensive blockchain technology requirement solution;
- c) Design, develop, and maintain service components or smart contracts in a blockchain system;
- d) Test and accept the relevant functions of the blockchain system;
- e) Plan the proper implementation and deployment of blockchain services;
- f) Provide full-process system maintenance services.

7.2 Identity Provider An identity provider is an organization or institution that provides identity services to parties involved in cross-border trade. Its main activities should include.

- a) Identify the identity authentication and management needs of stakeholders in cross-border trade;
- b) Design a reasonable and comprehensive cross-border trade identity authentication and management solution;
- c) Implement and maintain the identity service system;
- d) Issuing and managing digital certificates or identity-verifiable credentials;
- e) Establish digital certificates or identity-verifiable credentials on the blockchain platform to verify smart contracts.

7.3 Service Users The service user is a cross-border trade organization or institution using

the blockchain platform, whose main activities should include.

8.1 Digital Identity Services

8.1.1 Digital Identity Creation User-generated digital identities on blockchain platforms should meet the following requirements.

- a) Generate public-private key pairs, digital identities, and documents through blockchain applications;
- b) Submit the digital identity identifier and the corresponding digital identity identifier document URI to the blockchain platform;
- c) Store the URI of the digital certificate or verifiable credential issued to the user by the identity provider in the digital identity document;
- d) Store the user-signed digital certificate or verifiable credential URI in the digital identity document.

8.1.2 Creation of Authentication Smart Contracts Identity providers creating identity verification smart contracts on blockchain platforms should meet the following requirements.

- a) Create verifiable identity credentials and verifiable identity expression verification smart contracts issued by the blockchain platform;
- b) Create a smart contract in the blockchain platform that uses a digitally issued certificate to verify the contract.

8.1.3 Verifiable Credentials Service To provide verifiable credential services on a blockchain platform, the following requirements should be met.

- a) The service user submits an application for verifiable identity credentials to the identity provider;
- b) The identity provider issues verifiable identity credentials to the service user;
- c) The identity provider sends the verifiable identity credentials and the address of the identity verification smart contract to the service user;
- d) Service users store the verifiable credentials and the address of the identity verification smart contract in the identity document.

8.1.4 Digital Certificate Service When providing digital certificate services on a blockchain platform, the following requirements should be met.

8.2 Electronic Business Services

8.2.1 Issuance of Identity Declaration When relevant parties publish identity declarations on

a blockchain platform, they should meet the following requirements.

- a) Create an identity statement that includes its identifier, organization name, legal representative, seal, and other information;
- b) Electronically sign the statement and store it in an identity document.

8.2.2 Electronic Business Agreement Signing When relevant parties and business partners sign electronic business agreements, the following requirements should be met.

- a) Both parties shall jointly sign the agreed electronic business agreement using their respective digital identities. The agreement shall consist of the following parts. scope, communication and operation. Message processing, validity and enforceability, data content requirements, responsibilities and general terms;
- b) Agree on the communication methods, security procedures, and storage formats for data to protect data and its records from accidental or misuse. Harmful effects include improper access, alteration, or loss.

8.2.3 Electronic Business System Setup When relevant parties configure electronic business systems in blockchain applications, they should meet the following requirements.

- a) Exchange their respective identity tokens and identity token documents;
- b) Verify the other party's identity on the blockchain platform, as well as the verifiable credentials and digital certificate in the identity document;
- c) After verification, the electronic business system settings shall be carried out in the respective blockchain applications in accordance with the agreement.

8.3 Digital Document Service

8.3.1 Digital Document Creation When creating digital documents, relevant parties should meet the following requirements.

- a) It conforms to international trade document standards, including its components, structural model, description rules, and methods;
- b) It complies with international trade document electronic data interchange standards, including message structure, syntax rules and business information entity specifications.

8.3.2 Digital Document Signature When relevant parties sign digital documents, they should meet the following requirements.

- a) Conforms to digital signature data formats, including basic data format, verification data format, signature policy format, etc.;
- b) Supports separate signatures, inner-seal signatures, and cover signatures;
- c) Supports digital identity digital signatures, self-signed digital certificate digital signatures,