ICS 35.240
CCS L 70

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 43575-2023

Blockchain and distributed ledger technology-System testing specification

区块链和分布式记账技术 系统测试规范

Issued on: December 28, 2023 **Implemented on: April 1, 2024**

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

Table of Contents

1 Scope

This document establishes the testing principles for blockchain systems. It specifies the requirements for function, performance, security, and reliability tests. It also describes the corresponding test methods.

This document is applicable to: providing a reference for third-party evaluation agencies or other relevant agencies to conduct blockchain system testing; providing an internal testing basis for blockchain system builders; providing a basis for blockchain system users to conduct system selection and acceptance; providing technical support for the supervision work of industry regulatory authorities.

2 Normative references

GB/T 11457-2006

GB/T 22239-2019

GB/T 25069-2022

GB/T 29835.1-2013

3 Terms and definitions

For the purposes of this document, the terms and definitions defined in GB/T 11457- 2006, GB/T 25069-2022 as well as the followings apply.

3.1 Peer-to-peer network

A computer network that contains only nodes with equivalent control and operation capabilities.

[Source: GB/T 5271.18-2008, 2.18.04.05, modified]

b) It has node management functions such as node server information query, node service startup and shutdown control, node service configuration, node network status monitoring, node authorization management, etc.

c) It has the book application functions such as publishing and interacting with content on the blockchain system, setting multi-signature permission control for specific transaction processing, and executing contract logic based on smart contract functional components.

6.1.4 Core functional layer

Core functional layer testing requirements include but are not limited to:

a) It shall have consensus mechanism functions such as multi-node consensus

confirmation, independent node submission and record information validity verification, consensus mechanism fault tolerance, and consensus mechanism scalability;

b) It shall have account book record functions such as persistent storage of account book records, multiple nodes with complete data records, custom account book permissions, and node data consistency;

c) It shall have digital signature functions such as signing and signature verification;

d) It shall have timing service functions such as unified account book records, timing fault tolerance, and third-party timing services;

e) It is recommended to have encryption algorithm functions such as international mainstream encryption algorithms, international mainstream commercial encryption algorithms, privacy protection algorithms, and key management;

f) It is recommended to have summary algorithm functions such as international mainstream commercial secret summary algorithm, commercial secret summary algorithm, and system summary algorithm verification;

g) It is recommended to have functions such as formal verification of smart contracts, contract virtual machines, interaction between external system data and smart contracts, tamper-proofing of smart contracts, access control of smart contracts, smart contract upgrades, and writing contracts into ledgers.

6.1.5 Infrastructure layer

Infrastructure layer testing requirements shall include but not be limited to:

a) It has peer-to-peer network functions such as secure communication between nodes, node multicast function, and node dynamic management;

b) It has the functions of node data writing, querying and node stable storage;

authorization, monitoring, and auditing of management members.

6.3.3 Service interface layer

Service interface layer security testing requirements include but are not limited to:

a) It shall have reasonable encryption algorithm and authentication mechanism;

b) It shall have a privacy protection mechanism. It is advisable to adopt technologies such as homomorphic encryption and zero-knowledge proof;

c) It shall have a mechanism for encrypting storage and transmission block data, and it is advisable to use the national encryption algorithm;

d) It shall have an identity authentication mechanism. It shall use digital certificates and

electronic signature technologies.

6.3.4 Core function layer

The security test content of the core functional layer includes but is not limited to:

a) A consensus mechanism with high fault tolerance shall be provided;

b) It shall be able to resist double-spending attacks, replay attacks, fork attacks, bribery attacks, computing power attacks, etc.

c) It is advisable to have two or more consensus mechanisms;

d) It shall have Turing-complete, verifiable and auditable smart contracts, external query and call operations;

e) Smart contracts shall be able to prevent attacks such as logic errors, function errors, integer overflows, and vulnerabilities in virtual machines and operating environments;

f) It is recommended to support national encryption algorithms such as SM2, SM3, and SM4.

6.3.5 Infrastructure Layer

The security test content of the infrastructure layer shall include but not be limited to:

a) It has a P2P network security mechanism to prevent DDoS, witch, solar eclipse and other attacks;

b) It has a hardware device security mechanism to prevent attacks such as DNS pollution, routing broadcasts, Trojan viruses, etc.

6.4 Requirements for reliability test

The reliability test content shall include but not be limited to:

a) Meet the node reliability requirements, including the completeness of basic transactions of new nodes, consistency of ledger information, etc., support node access configuration and multi-node consensus completeness;

b) Meet the transaction execution reliability requirements, including the success rate and stability of load account query, load block query, load basic transaction query, load basic transaction, etc.;

c) Comply with the reliability requirements of encryption technology, including key management schemes, data privacy protection, transaction information encryption, etc.;

d) Comply with the reliability requirements of smart contracts, including completeness of change records, consensus on contract content upgrades, external data interaction, and