

ICS 35.240.40
CCS A 11

JR

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

JR/T 0184-2020

**Technical specification for financial distributed ledger
technology
(English Translation)**

Issued on: February 5, 2020

Implemented on: February 5, 2020

Issued by: People's Bank of China

Table of Contents

Foreword	
Introduction	
1 Scope	
2 Normative references	
3 Terms and definitions	
4 Abbreviations	
5 Security System Framework	
6 Basic hardware	
6.1 Basic requirements	
6.2 Physical Security	
6.3 Network Security	
7 Basic Software	
7.1 Basic requirements	
7.2 Ledger structure	
7.3 Consensus module	
7.4 Distributed networking	
7.5 Data Storage	
7.6 Smart Contract	
7.7 Interface Design	
7.8 Data Transmission	
7.9 Time synchronization	
7.10 Operating System	
8 Cryptographic Algorithm	
8.1 Basic requirements	
8.2 Confidentiality	
8.3 Completeness	
8.4 Authenticity	
8.5 Non-repudiation	
8.6 Randomness	
8.7 Key Management	
9 Node Communication	
9.1 Basic requirements	

- 9.2 Node authentication
- 9.3 Communication integrity
- 9.4 Communication confidentiality
- 10 Ledger Data
 - 10.1 Completeness
 - 10.2 Consistency
 - 10.3 Confidentiality
 - 10.4 Validity
 - 10.5 Ledger data redundancy
 - 10.6 Access and use
 - 10.7 Security Audit
- 11 Consensus Agreement
 - 11.1 Basic requirements
 - 11.2 Legality
 - 11.3 Correctness
 - 11.4 Finality
 - 11.5 Consistency
 - 11.6 Unforgeability
 - 11.7 Availability
 - 11.8 Robustness
 - 11.9 Fault tolerance
 - 11.10 Supervisability
 - 11.11 Low Latency
 - 11.12 Incentive compatibility
 - 11.13 Scalability
- 12 Smart Contract
 - 12.1 Basic requirements
 - 12.2 Version Control
 - 12.3 Access Control
 - 12.4 Complexity Limitation
 - 12.5 Atomicity
 - 12.6 Consistency
 - 12.7 Security Audit
 - 12.8 Life Cycle Management
 - 12.9 Attack Defense

- 12.10 Security Verification
- 13 Identity Management
 - 13.1 Basic requirements
 - 13.2 Identity definition
 - 13.3 Identity Registration
 - 13.4 Identity Verification
 - 13.5 Account Management
 - 13.6 Credential Lifecycle Management
 - 13.7 Identity Authentication
 - 13.8 Node ID Management
 - 13.9 Identity renewal and revocation
 - 13.10 Identity Information Security
 - 13.11 Identity supervision audit requirements
- 14 Privacy protection
 - 14.1 Privacy protection principles
 - 14.2 Privacy protection content
 - 14.3 Privacy Protection Policy
 - 14.4 Privacy protection technical requirements
 - 14.5 Privacy protection monitoring and auditing
- 15 Regulatory Support
 - 15.1 Basic requirements
 - 15.2 System Supervision
 - 15.3 Information Management
 - 15.4 Event handling
 - 15.5 Transaction Intervention
 - 15.6 Smart Contract Supervision
- 16 Operation and maintenance requirements
 - 16.1 Basic requirements
 - 16.2 Device Management
 - 16.3 Node Monitoring
 - 16.4 Node version upgrade
 - 16.5 Bug fixes
 - 16.6 Backup and Restore
 - 16.7 Emergency plan management
 - 16.8 Rights Management

- 16.9 Proposal Mechanism
- 17 Governance Mechanism
 - 17.1 Basic requirements
 - 17.2 Governance structure
 - 17.3 Key Points of Control
- References

Foreword

This standard was drafted in accordance with the rules given in GB/T 1.1-2009.

This standard was proposed by the Digital Currency Research Institute of the People's Bank of China.

This standard is under the jurisdiction of the National Financial Standardization Technical Committee (SAC/TC 180).

The organization responsible for drafting this standard. Digital Currency Research Institute of the People's Bank of China.

Participated in the drafting of this standard. Science and Technology Department of the People's Bank of China, Industrial and Commercial Bank of China, Agricultural Bank of China, Bank of China, China Construction Bank, China Development Bank, Ping An Bank, China Merchants Bank, Shenzhen Qianhai WeBank Co., Ltd., Zhejiang Netshang Bank Co., Ltd.

Company, Tsinghua University, Shanghai Jiaotong University, Nanjing University, Zhejiang University, China Banknote Hangzhou Blockchain Technology Research Institute, China Information and Communication Research Institute Research Institute, CICC Guosheng Certification Co., Ltd., Bank Card Testing Center, JD Digital Technology Holdings Co., Ltd., Baidu Online Network Technology (North Beijing) Co., Ltd., Chengdu Weishitong Information Industry Co., Ltd.

Introduction

Distributed ledger technology is a high integration of multiple core technology systems such as cryptographic algorithms, consensus mechanisms, peer-to-peer communication protocols, and distributed storage.

A distributed infrastructure and computing paradigm formed by the combination. At the stage when the form of distributed ledger technology is still plastic, it is necessary to formulate key Technical safety regulations, so that financial institutions can deploy and maintain systems in accordance with appropriate safety requirements, avoid security