ICS 35.030
CCS L80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 42571-2023

Information security technology - Security specification for blockchain information service

信息安全技术 区块链信息服务安全规范

Issued on: May 23, 2023 **Implemented on: December 1, 2023**

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

Table of Contents

Foreword

This document is in accordance with the provisions of GB/T 1:1-2020 "Guidelines for Standardization Work Part 1: Structure and Drafting Rules for Standardization Documents" drafting: Please note that some contents of this document may refer to patents: The issuing agency of this document assumes no responsibility for identifying patents: This document is proposed and managed by the National Information Security Standardization Technical Committee (SAC/TC260): This document was drafted by: Institute of Information Engineering, Chinese Academy of Sciences, Zhejiang University, Hangzhou Qulian Technology Co:, Ltd:, Ant Technology Group Co:, Ltd: Co:, Ltd:, Shenzhen Tencent Computer System Co:, Ltd:, China Electronics Standardization Research Institute, Chongqing University of Posts and Telecommunications, and the Third Ministry of Public Security Research Institute, National Computer Network Emergency Coordination Center, China Academy of Information and Communications Technology, Pudong New Area People's Government Office, National Industrial Information Security Development Research Center, Institute of Computing Technology, Chinese Academy of Sciences, Shanghai Information Security Evaluation and Certification Center, Shaanxi Provincial Network and Information Security Evaluation Center, Sichuan Digital Economy Research Center, First Research Institute of the Ministry of Public Security, Peking University, Tsinghua University, Beijing Dongfangtong Netcom Technology Co:, Ltd:, State Grid Blockchain Technology (Beijing) Co:, Ltd:, China Electronics Technology Network Information Security Co:, Ltd:, Lenovo (Beijing) Co:, Ltd: Beijing) Co:, Ltd:, Beijing Baidu Netcom Technology Co:, Ltd:, Venustech Information Technology Group Co:, Ltd:, Inspur Electronic Information Industry Shares Co:, Ltd:, National Energy Administration Information Center, JD Technology Holdings Co:, Ltd:, China Electric Power Research

Institute Co:, Ltd:, Taikangbao Insurance Group Co:, Ltd:, Shenzhen Nuchuangxinan Technology Development Co:, Ltd:, New H3C Technology Co:, Ltd:, Chengdu Lianan Technology Co:, Ltd: Company, Beijing Zhongxiang Bit Technology Co:, Ltd:, Xingtang Communication Technology Co:, Ltd:, Beijing iQiyi Technology Co:, Ltd:, Beijing Digital Certification Co:, Ltd: Co:, Ltd:, Matrix Element Technology (Shenzhen) Co:, Ltd:, Beijing Rongshu Lianzhi Technology Co:, Ltd:, Beijing Xiaomi Electronic Software Technology Co:, Ltd:, Zhengzhou Xinda Jiean Information Technology Co:, Ltd:, Beijing Yuanlian Network Technology Co:, Ltd:, Beijing People Online Network Co:, Ltd:, Beijing Tianrongxin Network Security Technology Co:, Ltd:, Shenzhen OneConnect Intelligent Technology Co:, Ltd:, Biaoxin Smart Chain (Hangzhou) Technology Development Co:, Ltd:, Zhejiang Commercial Bank Co:, Ltd:, China Automotive Engineering Research Institute Co:, Ltd: The main drafters of this document: Zhang Xiaodan, Guo Tao, Cai Liang, Wang Huili, Hu Jingyuan, Zhou Xi, Han Jizhong, Yao Xiangzhen, Li Wei, Chen Xiaofeng, Chang Wenting, Zhang Hanwen, Wu Yang, Zheng Peiyu, Wang Lei, Shao Yu, Huang Yonghong, Cui Tingting, Lu Honglei, Shi Hongbin, Zhou Wei, Liu Zongzhen, Wang Yuhang, Xie Anming, Liu Xiangang, Sun Yi, Chen Yan, Zhi Liangliang, Li Rengang, Feng Wei, Liu Weihua, Wu Tong, An Gaofeng, Wang Haitang, Huang Dezhi, Jiang Rongsheng, Wan Xiaolan, Yu Yuzhou, Lu Zhigang, Mei Qiuli, Zou Chao, Zhu Yan, Bai Jian, Fan Qingjun, Wang Danchen, Gao Rui, Zhang Meijuan, Zang Cheng, Wu Xinyong, Ren Zejun, Huang Jingyi, Wang Wenlei, Zhang Yongqiang, Pang Shutian, Luo Xinhui, Zhang Yuanyuan, Yan Ximin, Chen Hong, Zhang Subo, An Li, Wang Yunhao, Li Kepeng, Zhang Hu, Xie Hongjun, Li Ruirong, Jing Bo, Quan Daiyong, Wang Mengnan, Fu Shijian: Information Security Technology Blockchain information service security specification

1 Scope

GB/T 42571-2023 applies security requirements to the operator of a blockchain information service rather than to the chain itself. The distinction matters. A blockchain's own guarantees are narrow and well understood: once a record is written and confirmed, altering it is impractical. Almost everything a user actually depends on lies outside that guarantee - how the information was generated before it was written, who was allowed to submit it, how it is processed and released, how it propagates, and what happens to the keys that authorise all of it. This document specifies the security technical requirements and the security management requirements for blockchain information service providers, and describes the corresponding testing and evaluation methods. It opens with an overview of what such services are and of the security risks that attach to them, then sets out the technical requirements along the life of the information - generation, processing, release, dissemination - before turning to the management side. It applies to the secure construction, operation, management and assessment of blockchain information services. Under ICS 35.030 and CCS L80, it is the reference for service providers registering under China's blockchain information service rules and for the assessors who examine them.

This document specifies the security technical requirements and security management requirements for blockchain information service providers, and describes the corresponding testing and evaluation methods: and check assessment methods: This document applies to services such as security construction, security operation, security management, and security assessment for blockchain information services:

2 Normative references

The contents of the following documents constitute the essential provisions of this document through normative references in the text: Among them, dated references For documents, only the version corresponding to the date is applicable to this document; for undated reference documents, the latest version (including all amendments) is applicable to this document: GB /Z 20986-2007 Guidelines for Classification and Classification of Information Security Technology and Information Security Incidents

GB/T 25069-2022 Information Security Technical Terminology

GB/T 32915-2016 Binary sequence randomness detection method for information security technology

GB/T 35273-2020 Personal Information Security Specifications for Information Security Technology

GB/T 40645-2021 Information Security Technology Internet Information Service Security General Requirements GM/T 0033-2014 Timestamp Interface Specification

3 Terms and Definitions

Defined in GB/T 25069-2022, GB/T 35273-2020 and GB/T 40645-2021 and the following terms and definitions apply in this document: 3:

1 Based on blockchain technology or systems, information services provided through internet sites, applications and other network platforms: 3:

2 Organizations or individuals using blockchain information services:

Note: Blockchain information service users are referred to as "users": 3:

3 An organization that provides blockchain information services to blockchain information service users:

Note: Blockchain information service providers include but are not limited to blockchain business operators and blockchain technology providers: 3:4 timestamp timestamp The data obtained by signing the time and other data to be signed, and used to indicate the time attribute of the data: