ICS 35.030
CCS L80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 42570-2023

Information security technology - Security framework for blockchain technology

信息安全技术 区块链技术安全框架

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 is drafted by: Tsinghua University, Digital Currency Research Institute of the People's Bank of China, China Institute of Electronic Technology Standardization, National Information Technology Security Research Center, Ant Technology Group Co:, Ltd:, Jingdong Technology Information Technology Co:, Ltd:, Beijing Baidu Netcom Technology Co:, Ltd: Company, Hangzhou Secret Ape Technology Co:, Ltd:, Shenzhen Nuchuangxinan Technology Development Co:, Ltd:, Shandong University, Shandong Blockchain Research Institute, Ali Cloud Computing Co:, Ltd:, Huawei Technologies Co:, Ltd:, Dinglian Digital Technology (Shenzhen) Co:, Ltd:, Matrix Element Technology (Shenzhen) Co:, Ltd:, Shenzhen City Tencent Computer System Co:, Ltd:, Zhejiang University, Shanghai Jiaotong University: The main drafters of this document: Wang Xiaoyun, Mu Changchun, Di Gang, Jia Keting, Guo Xiaolei, Wang Haijun, Zhang Shuang, Wang Haitang, Zhang Ren, Wang Zongyue, Yu Yu, Wei Puwen, Duan Sisi, Pan Guozhen, Wang Bo, Su Nianle, Jin Tao, Gong Zihong, Chang Wenting, Jing Bo, Zhang Haibin, He Chao, Wang Hailong, Qiu Pengcheng, Chen Yu, Wang Anyu, Chen Ping, Guo Shanqing, Zhang Guoyan, Ren Kui, Zhang Yuguang, Sun Xiaoli, Liu Jian, Qin Lingyue, Li Kepeng: Information Security Technology Blockchain Technology Security Framework

1 Scope

GB/T 42570-2023 is the framework document of China's blockchain security series, the one that lays out the pieces before the other standards specify them. Blockchain security is easy to discuss badly because the technology's own guarantee - that a confirmed record is impractical to alter - is often mistaken for a guarantee about the system as a whole, when the cryptography, the node software, the operational practice and the division of responsibility between the parties all sit outside it. This document gives the security framework: the cryptographic support the technology rests on, the security functional components that make up a blockchain system, the security management and operation that keep it running, and the security responsibilities attaching to each role in it. It is written to guide blockchain service providers in overall planning during design, development and deployment, rather than to be certified against directly. Under ICS 35.030 and CCS L80, its audience is platform architects and service providers, the enterprises building on their platforms, and the assessors who need a common map before examining any particular part. It is the companion to GB/T 42571-2023 on blockchain information service security.

This document gives the blockchain technology security framework, which includes blockchain cryptographic support, blockchain security functional components, blockchain security Full management operation and blockchain role security responsibilities and other parts: This document is applicable to guide blockchain service providers to conduct overall planning in the process of blockchain design, development, deployment, management and operation and maintenance: Planning and security framework design can also provide reference for blockchain security assessment:

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/T 20518 Information Security Technology Public Key Infrastructure Digital Certificate Format

GB/T 21053 Information Security Technology Public Key Infrastructure PKI System Security Level Protection Technical Requirements

GB/T 22239-2019 Basic Requirements for Network Security Level Protection of Information Security Technology

GB/T 25069 Information Security Technical Terms

GB/T 30998 Information Technology Software Security Assurance Specification

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

Technology

GB/T 37092-2018 Security requirements for cryptographic modules of information security technology

GB/T 39786-2021 Basic Requirements for Cryptography Application in Information Security Technology Information System GM/T 0005 Random Testing Specification

3 Terms and Definitions

The following terms and definitions defined in GB/T 25069 apply to this document: 3:1 block block A basic data structure consisting of a series of information units: [Source: ISO 22739:2020, 3:2, with modifications] 3:2 blockchain blockchain The blocks are connected in sequence, and the tamper-resistant and unforgeable data are guaranteed by cryptographic methods such as consensus protocols, digital signatures, and hash functions: Distributed ledger: [Source: ISO 22739:2020, 3:6, with modifications] 3:3 node node Independently functioning blockchain components with specific functions: