

ICS 35.240
CCS L 70



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

GB/T 43579-2023

**Blockchain and distributed ledger technology-Technical
specification of smart contract lifecycle management**

区块链和分布式记账技术 智能合约生命周期管理技术规范

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

Preface/ Introduction	II
1 Scope	1
2 Normative references	1
3 Terms and Definitions	1
4 Overview	2
5 General technical requirements	2
5:1 Design and Development	2
5:2 Compile and deploy	3
5:3 Trigger execution	4
5:4 Maintenance Management	6
6 General Assessment Methods	7
6:1 Design and Development	7
6:2 Compile and deploy	8
6:3 Trigger execution	8
6:4 Maintenance management	11
Appendix A (informative) Common smart contract vulnerabilities	13
Reference	15

Foreword

This document complies with the provisions of GB/T 1:1-2020 "Standardization Work Guidelines Part 1: Structure and Drafting Rules of Standardization Documents" Drafting:

Please note that some content in this document may be subject to patents: The publisher of this document assumes no responsibility for identifying patents:

This document is proposed by the Ministry of Industry and Information Technology of the People's Republic of China:

This document is under the jurisdiction of the National Blockchain and Distributed Accounting Technology Standardization Technical Committee (SAC/TC590):

This document was drafted by: Ant Blockchain Technology (Shanghai) Co., Ltd., China Electronics Technology Standardization Institute, Zhongan Information Technology Service Co., Ltd., Shenzhen Qianhai Intelligent Copyright Innovation and Development Research Institute, Shanghai Wanxiang Blockchain Co., Ltd., Sichuan Changhong Electric Co., Ltd:

Company, Nanjing Xinzhilian Technology Information Co., Ltd., Hunan Tianhe Guoyun Technology Co., Ltd., Southwest Forestry University, Ant Technology Group Co., Ltd:

Co., Ltd., Hangzhou Qulian Technology Co., Ltd., Shenzhen Tencent Computer Systems Co., Ltd., Fudan University, ICBC Technology Co., Ltd., Xi'an Jiaotong University, China Southern Power Grid Big Data Service Co., Ltd., National Application Software Product Quality Inspection and Testing Center, Shanghai Distribution Information Technology Co., Ltd:

Co., Ltd., Datai Robot Co., Ltd., Tencent Cloud Computing (Beijing) Co., Ltd., Beijing Big Data Advanced Technology Research Institute, Shanghai Zhenfang Technology Co., Ltd., Zheshang Bank Co., Ltd., Shanghai Lingshu Zhonghe Information Technology Co., Ltd., Guangzhou Southern Investment Group Co., Ltd:

Company, Yongqi Holdings (Beijing) Co., Ltd., EVOC Intelligent Technology Co., Ltd., JD Technology Information Technology Co., Ltd., China Mobile Information Technology Co., Ltd., Beijing Telyingfu Technology Co., Ltd., the Fifth Institute of Electronics of the Ministry of Industry and Information Technology, China Unicom Digital Technology Co., Ltd., National Industrial Information Security Development Research Center, Huawei Cloud Computing Technology Co., Ltd., Huawei Technologies Co., Ltd., Peking University Computing and Digital Economic Research Institute, Digital China Information Services Co., Ltd., State Grid Blockchain Technology (Beijing) Co., Ltd., Shanghai Aurora Information Technology Group Co., Ltd., Beijing Microchip Blockchain and Edge Computing Research Institute, China Civil Aviation Information Network Co., Ltd., Zhejiang University, Hong Kong Polytechnic Institute University of Technology, Guangzhou Saixi Standard Testing Research Institute Co., Ltd., Minyuxing (Beijing) Technology Co., Ltd., Hengbao Co., Ltd., Beijing Hesi Information Technology Co., Ltd., Shenzhen Jiangxinglianjia Intelligent Technology Co., Ltd., Shenzhen Bosi Internet Technology Co., Ltd., Beijing Guojin Huide Engineering Management Co., Ltd., Zhejiang Chucai Intelligent Technology Co., Ltd., Jiangxi Chuangchuang Digital Technology Co., Ltd., and China Academy of Information and Communications Technology:

The main drafters of this document: Li Ming, Yan Ying, Peng Jin, Chang Wenting, Zhou Ping, Qiu Yingying, Du Yu, Hao Han, Li Kepeng, Ou Yun, Wang Dong, Yu Xiuming, Li Nucheng, Yang Zheng, Liang Zhihong, Wang Haijun, Zhang Yan, Zhang Xiaomeng, Cai Liang, Tao Lichun, Wang Shaogang, Wang Chenhui, Wang Wei, Xie Hui, Liu Tingshan, Lao Weilun, Liu Tiancheng, Kan Haibin, Da Hongfei, Gong Zihong, Yang Guozheng, Lan Chunjia, Wang Yi, Ai Songpu, Xiangli Peng, Wang Wencheng, Pan Yan, Zhang Ziyi, Zhang Liangliang, Ren Fengli, Yang Wenfeng, Wu Yang, Ren Changrui, Sun Lin, Chen Xiaofeng, Hao Yukun, Kang Xinwei, Shi Na, Yu Yansheng, Tan Lin, Huang Yuxiang, Fan Ming, Wu Meng, Qiu Weiwei, Liu Mianchen, Jin Xiaona, Liang Jun, Zhong Libin, Song Wenpeng, Yang Zhen, Wang Xin, Wang Hailong, Tian Sen, Bao Xiaomin, Peng Tao, Sun Lin, Zhong Fahui, Zhang Xiaojun, Qu Qiang, Li Da, Yan Haihai, Yang Rongxia, Su Qinghui, Du Juan, Jia

Xiangjuan, Zhou Gang, Zhang Dong, Cao Jiannong, Wang Baochun, Pang Weiwei, Yan Aijun, Qian Jing, Fan Xiaoyi, Chen Dong, Zhou Ziming, Zhang Jinwei, Ma Chunquan, Hua Chongxin, Wei Kai, Zhang Yihui, Shi Zhuyu, Huang Dejun, Qin Rizhen, Xie Yunlong, Guo Dongsheng, Ji Jingting, Chen Zhilie, Pang Guanshi:

Introduction

In recent years, driven by industrial policies, laws and regulations, technological progress, market development and other aspects, blockchain technology is accelerating the trend of "moving away from virtual reality":

"real" to help the rapid development of the real economy: A smart contract is a computer program stored in a distributed accounting technology system: Any part of the program Execution results are recorded on the distributed ledger: Smart contracts bring the blockchain into a programmable and intelligent era: However, with smart contracts With its increasingly widespread application, non-standard design, development, testing and maintenance have brought many risk issues and caused serious losses:

In order to provide implementable standards for various industries, enterprises and related organizations that apply blockchain connections, this document introduces blockchain smart contracts Conducted an in-depth analysis of the life cycle of smart contracts and sorted out each stage of the smart contract life cycle, including design and development, compilation and deployment, trigger execution and Maintenance management: At each stage of the life cycle, this document refines the relevant requirements that need to be followed to build an implementable set of requirements that can An execution process that avoids possible risks in smart contracts and provides operable and instructive smart contracts for various industries connected by the blockchain:

Implementation specifications:

Blockchain and distributed accounting technology Smart contract life cycle management technical specifications

1 Scope

This document stipulates the technical requirements for design and development, compilation and deployment, trigger execution, maintenance and management in the smart contract life cycle, describing The evaluation methods for each link are described:

This document is suitable for blockchain related parties to carry out the construction, application and audit of smart contracts:

2 Normative reference documents

This document has no normative references:

3 Terms and definitions

The following terms and definitions apply to this document: 3:1 blockchain blockchain A distributed ledger formed by appending consensus-confirmed blocks in sequence using cryptographic links:

Note: Blockchain is designed to resist tampering and create final, deterministic, immutable ledger records: [Source: GB/T 43572-2023,3:6] 3:2 smart contract smartcontract A computer program stored in a distributed accounting technology system, and any execution results of the program are recorded in the distributed ledger:

Note: Smart contracts can legally represent contract terms and create enforceable obligations under the laws of the applicable jurisdiction:

[Source: GB/T 43572-2023,3:72] 3:3 datatype datatype A defined collection of data objects that specifies a data structure and a set of permitted operations that, when any of these operations are performed, Data objects are treated as operands:

[Source: GB/T 5271:17-2010,17:05:08] 3:4 formalverification A method to verify the certainty and completeness of smart contract programs through mathematical formal expression of algorithm logic: 3:5 Oracle A service that uses data external to the distributed accounting technology system to update the distributed ledger:

[Source: GB/T 43572-2023,3:28]