ICS 35.030
CCS L 80

中华人民共和国密码行业标准

GM/T 0111—2021

区块链密码应用技术要求

Technical requirements for blockchain cryptography application

2021-10-19 发布　　2022-05-01 实施

国家密码管理局　　发布

目　　次

前言 …… Ⅲ
引言 …… Ⅳ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　缩略语 …… 2
5　区块链密码应用技术架构 …… 3
6　区块链密码应用需求 …… 4
7　区块链密码应用总体要求 …… 4
7.1　密码算法要求 …… 4
7.2　数字签名要求 …… 4
7.3　密码设备安全要求 …… 4
7.4　密钥管理安全要求 …… 4
7.5　证书管理要求 …… 5
7.6　数据安全要求 …… 5
7.7　共识协议安全要求 …… 5
7.8　智能合约安全要求 …… 5
8　区块链的各业务环节的密码应用技术要求 …… 5
8.1　用户注册 …… 5
8.2　实名认证 …… 6
8.3　交易创建 …… 6
8.4　交易验证 …… 6
8.5　账本存储 …… 6
8.6　链外交易 …… 6
8.7　节点和用户的身份管理 …… 7
8.8　交易监管 …… 7
附录 A（资料性）　基于区块链的电子存证应用方案 …… 8
A.1　方案概述 …… 8
A.2　密码应用设计 …… 9

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位：三未信安科技股份有限公司、国家密码管理局商用密码检测中心、北京数字认证股份有限公司、数安时代科技股份有限公司、清华大学、北京交通大学、山东大学软件学院、国家信息中心、武汉大学、齐鲁工业大学、山东师范大学、暨南大学、中国人民银行数字货币研究所、浪潮集团有限公司、格尔软件股份有限公司、公安部第一研究所、航天信息股份有限公司、阿里巴巴（北京）软件服务有限公司、山大地纬软件股份有限公司、北京智芯微电子科技有限公司、北京信安世纪科技股份有限公司、中国电力科学研究院有限公司、兴唐通信科技有限公司、深圳市金证科技股份有限公司、北京信任度科技有限公司。

本文件主要起草人：刘晓东、李国友、张永强、汪宗斌、谭武征、罗清彩、翟峰、林巍、樊海宁、孔凡玉、许涛、刘蓓、亢洋、卢伟龙、傅大鹏、张大伟、曹永峰、张庆胜、王绍刚、涂因子、甄平、胡进、刘伟、张妍、何德彪、陈国伟、孔兰菊、赵华伟、王皓、龚自洪、梅秋丽、霍云、彭晋、张海龙、顾伟平、冯云、马臣云。

引　言

区块链是分布式数据存储、点对点传输、共识机制、密码算法等技术在互联网时代的创新应用模式。随着国内外区块链技术的迅猛发展，区块链已延伸到物联网、智能制造、供应链管理、数字资产交易等多个领域。

为了保障我国区块链技术应用的健康发展，推动国产密码算法在区块链中的应用，制定区块链密码应用技术要求是非常必要的。

本文件对区块链技术，重点是对联盟链技术的密码安全要素以及需要遵循的相关技术要求做出规定，指导密码技术在区块链中的使用。

区块链密码应用技术要求

1 范围

本文件规定了联盟区块链的密码安全要素以及密码应用的技术要求。

本文件适用于指导联盟区块链密码应用及产品的设计、使用。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 20518 信息安全技术 公钥基础设施 数字证书格式

GB/T 25056 信息安全技术 证书认证系统密码及其相关安全技术规范

GB/T 32905 信息安全技术 SM3 密码杂凑算法

GB/T 32907 信息安全技术 SM4 分组密码算法

GB/T 32915 信息安全技术 二元序列随机性检测方法

GB/T 32918 信息安全技术 SM2 椭圆曲线公钥密码算法

GB/T 35275 信息安全技术 SM2 密码算法加密签名消息语法规范

GB/T 35276 信息安全技术 SM2 密码算法使用规范

GB/T 37092 信息安全技术 密码模块安全要求

GB/T 38635.1 信息安全技术 SM9 标识密码算法 第 1 部分：总则

GB/T 38635.2 信息安全技术 SM9 标识密码算法 第 2 部分：算法

GM/T 0033 时间戳接口规范

GM/T 0037 证书认证系统检测规范

GM/T 0038 证书认证密钥管理系统检测规范

GM/Z 4001 密码术语

3 术语和定义

GM/Z 4001 界定的以及下列术语和定义适用于本文件。

3.1

区块链 blockchain

一种采用分布式数据存储、点对点传输、共识机制、密码算法、智能合约等技术的新型应用模式和融合技术。

3.2

共识机制 consensus mechanism

区块链系统中实现不同节点之间建立信任、获取权益的算法。

3.3

智能合约 smart contract

一套以数字形式定义的约定。