ICS 35.240.40
CCS A 11

团　　体　　标　　准

T/SZBA 003—2021

基于区块链的元宇宙支付清算规范体系

Metaverse payment and clearing specification system based on blockchain

（征求意见稿）

（本稿完成日期：2021.12.21）

2021－12－01 发布　　2022－02－01 实施

深圳市信息服务业区块链协会　　发 布

目　次

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。

请注意本文件的某些内容可能涉及专利，本文件的发布机构不承担识别专利的责任。

本文件由深圳市千画科技有限公司提出。

本文件由深圳市信息服务业区块链协会归口。

本文件起草单位：深圳市千画科技有限公司、深圳市信息服务业区块链协会。

本文件主要起草人：XXX、XXX。

本文件为首次发布。

基于区块链的元宇宙支付清算规范体系

1 范围

本文件规定了基于区块链的元宇宙支付清算规范体系的术语和定义、基本原则、体系架构、性能要求和安全要求。

本文件适用于基于区块链的元宇宙支付清算规范体系。

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 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 35273-2020 信息安全技术 个人信息安全规范

JR/T 0184-2020 金融分布式账本技术 安全规范

JR/T 0193-2020 区块链技术金融应用 评估规则

3 术语和定义

下列术语和定义适用于本文件。

3.1

区块链 blockchain

一种由多方共同维护，使用密码学保证传输和访问安全，能够实现数据一致存储、防篡改、防抵赖的技术体系。

注：典型的区块链是以块链结构实现数据存储的。

[来源：JR/T 0193-2020，3.1]

3.2

节点 node

提供分布式账本的所有功能或者部分功能的实体。

[来源：JR/T 0184-2020，3.22]

3.3

区块链网络 blockchain network

使用区块链技术构建的网络。

3.4

人民币跨境支付系统 cross-border interbank payment system

由中国人民银行组织开发的独立支付系统，为境内外金融机构人民币跨境和离岸业务提供资金清算与结算服务，是重要的金融基础设施。

3.5

用户 user

参与到区块链上实际责任主体的基本单位。

3.6

原子性 atomicity

智能合约在执行过程中发生错误，会被回滚到智能合约开始前的状态。

[来源：JR/T 0184—2020，3.36]

3.7

资产 asset

能够在区块链上发行、流通、存储、交易，用于完成支付清算业务的权益。

3.8

联盟链 consortium blockchain

由业务相关的多个机构参与者组建的区块链网络，共同协作完成一个或多个特定的业务场景。

3.9

私有链 private blockchain

由单个机构内部组建的区块链网络，通常支撑机构内部的业务场景。

3.10

智能合约 smart contract 一种旨在以信息化方式传播、验证或执行合同的计算机协议，其在分布式账本上体现为可自动
执行的计算机程序。

[来源：JR/T 0184—2020，3.22]

3.11

访问控制 access control

一种保证数据处理系统的资源只能由被授权主体按授权方式进行访问手段

3.12

共识协议 consensus protocol

分布式账本系统中各节点间为达成一致采用的计算方法。

[来源：JR/T 0184—2020，3.17]

4 基本原则

4.1 合法合规原则

应遵守国家相关法律法规和金融监管要求，应为监管审计需求提供技术支持。

4.2 可追溯原则

业务与活动都应有记录，可追溯，可审计。

4.3 数据一致性原则

链上、链下存取的数据应保证数据库的一致性，区块链各个节点之间的数据也应保持一致性。

4.4 安全原则

应采取各种必要的安全手段，保障链上资产和交易等信息的安全，防范攻击。

4.5 隐私保护原则

应保障链上的用户隐私安全，防止泄露用户隐私。

5 体系架构

5.1 业务系统层

a) 业务系统应满足以下功能：
   1) 用户汇款：当用户发起汇款时，申请报文应能够通过区块链网络传输至 CIPS，并由 CIPS 完成资金结算，同时将处理的结果记录在区块链；
   2) 业务查询：用户如对发出或接收业务有疑问，应可通过区块链报文的形式向发起行或接收行发起查询；
   3) 业务状态查询：用户应能向区块链网络发送业务状态查询报文，查询发起行发出的业务在 CIPS 的处理情况；
   4) 支付管理：机构用户应能通过区块链查看本机构发起的交易列表以及交易的详情信息；
   5) 用户管理：应能对用户进行注册、查询、修改、冻结。
b) 业务系统应遵循以下原则：
   1) 敏感的业务数据不宜明文上链，需经过脱敏后上链；
   2) 应遵循上链数据最小化原则，需要协作的数据上链，不需要协作的数据链下存储即可；
   3) 应通过前置系统与区块链系统进行通信，实现交易代理转发，保证通信的安全性。

5.2 区块链系统层

区块链系统中账本数据、节点通信、共识机制、密码算法等模块应遵循 JR/T 0184-2020 的相关要求。

6 性能要求

6.1 响应时间

响应时间应能够满足以下要求：

——应保证在95%的情况下，业务系统与区块链网络交互的响应时间不超过3秒；

——应保证高峰时段网络拥堵的情况下，和区块链网络交互的响应时间不超过5秒。

6.2 交易吞吐率

应保障平均吞吐率为50笔/秒，最大吞吐率为100笔/秒。

6.3 系统可用性

系统可用性应能够满足以下要求：

——增加或删除节点，应不降低区块链网络的可用性，整个网络应能正常处理业务请求；

——具备异常处理机制，保障系统在该并发场景下7x24小时不间断运行；

——保障每百万次交易中，最多出现1次系统重启的情况；

——保障每运行1500小时最多发生一次故障；

——保障全年累计故障停运时间不超过10个小时。

6.4 系统可复原性

系统可复原性应能够满足以下要求：

——95%的故障能在20秒内完成重启并能正常处理业务请求；

——提供问题节点识别机制，并能在30秒之内移除或恢复问题节点；

——数据库异常连接中断后，可以自动重连并能保证数据写入的原子性；

——提供数据备份和恢复功能，保证系统因各种原因引起数据丢失或者数据损坏的情况下，能够迅速恢复和还原数据。

7 安全要求

7.1 基础硬件

应遵循 GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》中三级以上的物理安全和网络安全相关要求。

7.2 基础软件

7.2.1 应符合 GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》中三级以上的主机安全、应用安全、数据安全及备份恢复相关规定。

7.2.2 宜采用联盟链或私有链的结构，对接入节点或用户进行一定限制及严格的身份验证。

7.2.3 宜采用白名单控制区块链网络节点与业务系统的相互访问。

7.2.4 应提供区块链网络节点及系统运行日志管理及安全审计功能，可追踪系统的历史使用情况。

7.3 智能合约

智能合约应遵循JR/T 0184—2020中针对智能合约的相关要求。

7.4 密码算法

密码算法应遵循JR/T 0184—2020中针对密码算法的相关要求。

7.5 账本数据

7.5.1 完整性

应保证账本数据在生成、传输、存储和调用过程中的完整性，不被非法篡改。

7.5.2 一致性

应保证各节点的账本数据写入、修改、存储和调用的一致性。

7.5.3 保密性

应通过密码学技术保证敏感数据传输、存储的保密性，确保无关方不可知、不可读。

7.5.4 授权使用

应确保数据访问和使用符合认证授权和访问控制要求，仅授权方可访问账本数据。

7.6 共识协议

共识协议应遵循JR/T 0184—2020中针对共识协议的相关要求。

7.7 身份管理

7.7.1 身份鉴权

为防止在无任何身份标识的情况下访问区块链网络，需严格进行身份鉴权，具体要求如下：

——应在金融机构接入区块链网络之前，颁发用户身份凭证；

——应使用安全且符合国家密码管理规定的公钥密码算法实现用户身份认证；

——应在交易过程中对数据进行电子签名，保证不可抵赖性；

——应保证采用的匿名身份认证机制的匿名性、不可伪造性和不可链接性。

7.7.2 访问控制

鉴于跨境支付平台的重要性和特殊性，应对接入的机构用户作相应的访问控制，具体要求如下：

——金融机构应在授权的前提下，凭用户身份凭证访问区块链网络，非授权金融机构，不能访问区块链网络；

——应采用最小权限原则，最小化金融机构的权限，只允许其进行权限范围内的操作及访问相应的数据；

——宜支持监管机构作为监管节点加入，作为监管节点对用户身份、交易信息、业务有效性和流 程合规性进行实时监督和审核。

7.8 隐私保护

交易者身份及交易内容的隐私保护应满足以下要求：

——应符合GB/T 35273-2020的规定，且不违反金融业相关监管要求；

——应遵循最小化原则，仅通过区块链传输、存储必要的数据；

——应采用符合国家密码管理规定的加密算法或链下授权等方式，确保仅相关方知道交易者身份信息和交易内容信息，无关方仅能获知交易是否成功，同时保证验证节点可正常对交易进行验证而无需向其透漏任何信息。

7.9 监管支撑

监管支撑应遵循JR/T 0184—2020中针对监管支撑的相关要求。

7.10 运维安全

运维安全应遵循JR/T 0184—2020中针对运维安全的相关要求。

7.11 治理机制

治理机制应遵循JR/T 0184—2020中针对治理机制的相关要求。

7.12 节点管理

节点管理应满足以下要求：

——应具有确保系统安全运行所需的成员节点管理机制；

——应满足共识节点高可靠、高可用的安全管理要求。

参 考 文 献

[1] GB/T 5271.18—2008 信息技术词汇
[2] GB/T 32915—2016 信息安全技术 二元序列随机性检测方法
[3] GM/T 0045—2016 金融数据密码机技术规范
[4] GM/T 0054—2018 信息系统密码应用基本要求
[5] JR/T 0171—2020 个人金融信息保护技术规范
[6] DB52/T 1466-2019 区块链 应用指南
[7] DB43/T 1842-2020 区块链应用安全技术测评标准
[8] 《中华人民共和国网络安全法》