ICS 35.240.99
CCS L 78

团　　体　　标　　准

T/SZBA 002—2021

基于区块链的元宇宙身份认证规范体系

Metaverse identity authentication specification system based on blockchain

点击此处添加与国际标准一致性程度的标识

（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身份认证规范体系

1 范围

本文件规定了基于区块链的元宇宙身份认证规范体系的术语和定义、技术要求、基本要求。

本文件适用于基于区块链的元宇宙身份认证规范。

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 信息安全技术 网络安全等级保护基本要求

GB/T 25058 信息安全技术 网络安全等级保护实施指南

GB/T 25070 信息安全技术 网络安全等级保护安全设计技术要求

GB/T 35273 信息安全技术 个人信息安全规范

GB/T 39477 信息安全技术 政务信息共享 数据安全技术要求

GB/T 39786 信息安全技术 信息系统密码应用基本要求

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

《中华人民共和国电子签名法》

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

电子签名技术 electronic signature technology

电子签名技术是指数据电文中以电子形式所含、所附用于识别签名人身份并表明签名人认可其中内容数据的技术。

3.4

共识算法 consensus algorithm

区块链系统中各节点间为达成一致采用的计算方法。

3.5

数字身份证书

由用户提交、身份生成机构生成的包含用户身份信息、公钥、数字签名及其他信息的身份凭证，存储于区块链中用以证明用户身份，并可授权处理相关事务。

4 技术要求

4.1 共识机制

区块链网络中各节点对在区块链系统中进行事务或状态的验证、记录、修改等行为达成一致确认的方法。在区块链系统中，根据不同的业务需求，区块链网络选择不同的共识算法来实现其功能，共识机制应包括以下功能：

a) 支持多个节点参与共识和确认；
b) 支持独立节点对区块链网络提交的相关信息进行有效性验证；
c) 支持系统实现节点容错，容忍不超过一定比例（存证系统应注明容错比例）的节点存在物理或网络故障的非恶意错误，或节点遭受非法攻击（控制、篡改、拒绝服务等）的恶意错误，以及节点产生不确定行为的不可控错误时，共识过程不会被阻断，共识结果依旧安全可靠。

4.2 分布式账本

区块链中分布式数据的存储机制，通过不同节点对账本的共同记录与维护，形成区块 链系统中数据的公共管理、防篡改、可信任的机制。账本记录应包括以下功能：

a) 支持持久化存储账本记录；
b) 支持多节点拥有完整的数据记录；
c) 支持向获得授权者提供真实的数据记录；
d) 确保有相同账本记录的各节点的数据一致性。

4.3 时序服务

对于区块链系统中的行为或数据需记录相应的一致性的时序，可以选择特定的时序机制或工具。区块链系统时序服务应包括以下功能：

a) 支持统一账本记录时序；
b) 支持系统实现一定程度的时序容错；
c) 保证区块时间的可信，应至少采用以下方式的一种：
   - 对必要的一些区块，采用锚定可信时间等方式；
   - 节点采用可信时间源；
   - 其他能够提供可信时间的方法。

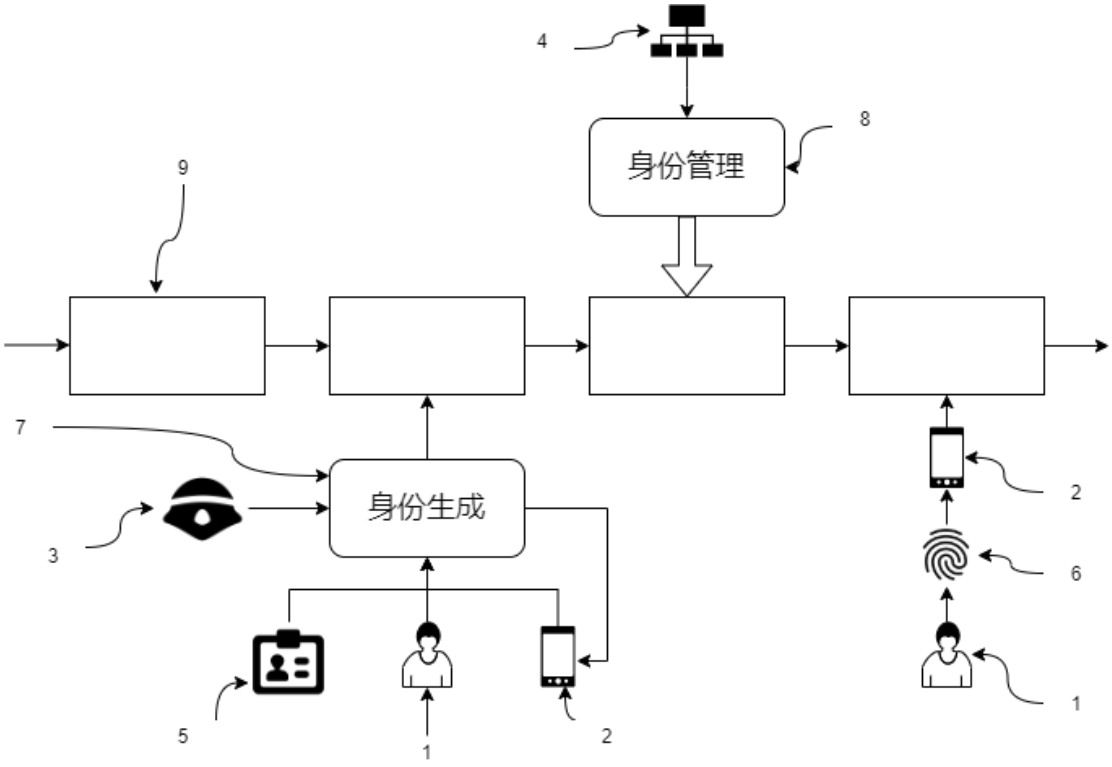
4.4 KPI 技术

PKI (Public Key Infrastructure)是基于公开密码理论建立起的安全基础设施，是电子签名的一种，在区块链系统中根据签字的数据电文进行存储、识别、认证，保证系统可靠安全性。根据《中华人民共和国电子签名法》规定，数字签名与手写签名具有同等法律效力。

5 业务流程

5.1 业务流程图

业务流程如图 1 的所示。



标引序号说明：

1——用户；2——智能手机；3——身份生成机构；4——身份管理员；5——身份证明；6——生物信息：如指纹、面容；7——数字身份生成；8——数字身份管理；9——区块链系统。

图1 身份认证管理示意图

5.2 提供身份证明

用户提供可验证的身份信息和具备生物信息检测的智能手机。

5.3 内容审核

区块链系统对接收的数据进行内容审核并保存审核数据，内容审核包括但不限于以下内容：

a) 身份证明的合法性；

b) 身份证明与用户的匹配程度。

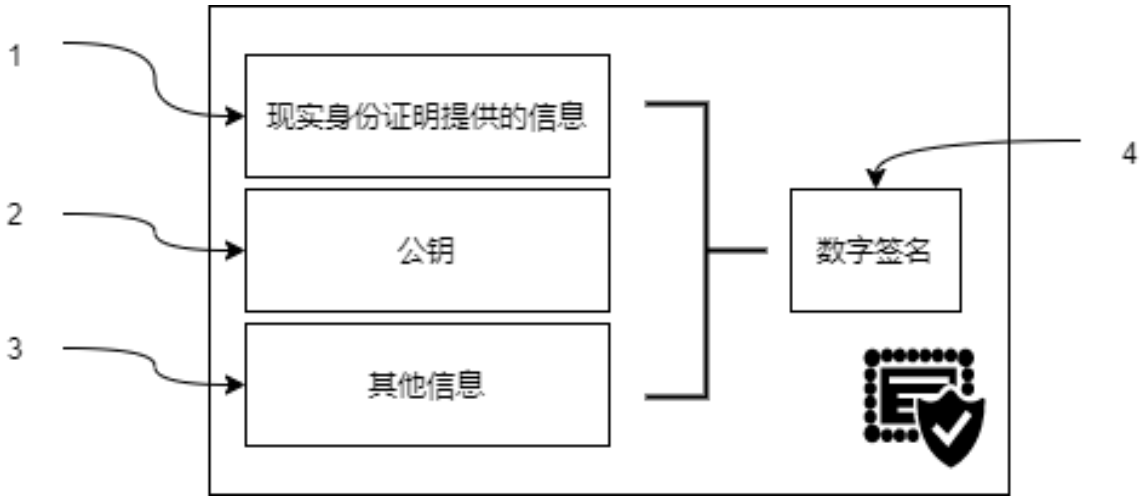
5.4 数字身份生成

用户将具备生物信息检测的智能手机提供给身份生成机构并使用生物信息解锁智能手机，身份生成机构和智能手机使用KEYGEN算法产生公钥和私钥，私钥保存在智能手机的TEE环境里，不可篡改。

身份生成机构从身份证明里获取与用户相关的身份信息：如性别、年龄、岗位等，并创建包含公钥和身份信息的身份证书。

5.5 数据上链

身份证书被提交并储存在区块链，管理节点对身份证书进行验证，并完成更新区块链。身份证书的结构见图 2。



标引序号说明：

1——用户现实身份证明（如身份证、驾驶证、工作证等）提供的信息（如姓名、性别、岗位等；

2——KEYGEN算法产生的公钥pk；

3——其他信息，如使用的加密算法，ph及TEE的版本等；

4——用户创建身份证书的数字签名。

图2 身份证书（cert）的结构示意图

5.6 数字身份的使用

用户需要智能手机来使用其区块链身份。具体步骤如下：

a) 用户从区块链获取需要验证身份的事务；

b) 用户确认事务，并使用其区块链身份授权事务，用户使用生物信息解锁智能手机,并用私钥对事务进行电子签名；

c) 用户将签名后的事务提交到区块链；

d) 其它区块链用户收到签名后的事务，在区块链找到对应普通用户的身份证书，验证私钥和公钥是否匹配。根据共识算法，若成功匹配，签名后的事务将被添加到区块链。

5.7 数字身份管理

数字身份管理由一组区块链管理节点组成。数字身份管理操作包括增加和删除区块链身份。

a) 增加区块链身份

新生成的身份证书被提交的区块链，管理节点通过共识算法决定身份证书里的身份信息是否合法，合法的身份证书被储存在区块链中。

b） 删除区块链身份

用户丢失了其私钥，可以提交注销其身份证书的申请，该申请须由一个或多个管理节点背书，身份证书注销后，将不能使用旧的私钥来授权区块链事务，必须重新申请新的身份证书。

6 基本要求

6.1 数据传输

信息传输应采用 HTTP、FTP 等方式。

6.2 数据共享原则

6.2.1 实用性

数据共享应科学合理，满足数据使用方的应用需求。

6.2.2 统一性

同一数据分享方式应统一，公共数据的代码应参考国家相关标准。

6.2.3 可扩展性

数据共享设计时应充分考虑数据范围扩充、时间增量等问题。

6.2.4 完整性

数据分享应充分保留数据原始信息，不做主观删减等特殊化处理。

6.3 安全要求

6.3.1 系统安全应符合 GB/T 22239、GB/T 25058、GB/T 25070 的规定。

6.3.2 密码应用应符合 GB/T 39786 的规定。

6.3.3 数据交换安全应符合 GB/T 39477 的规定。

6.3.4 个人信息安全应符合 GB/T 35273 的规定。

参 考 文 献

[1] GB/T 5271.18 信息技术 词汇 第18部分:分布式数据处理
[2] GB/T 20520 信息安全技术 公钥基础设施 时间戳规范
[3] GA/T 756 法庭科学 电子数据收集提取技术规范
[4] DB52/T 1466-2019 区块链 应用指南
[5] DB43/T 1842-2020 区块链应用安全技术测评标准
[6] 《中华人民共和国网络安全法》