

ICS 35.240.99
CCS A 00

DB 14

山西 地方 标准

DB14/T 3529—2025

工伤保险区块链技术应用规范

2025-07-23 发布

2025-11-01 实施

山西省市场监督管理局 发布

目 次

前言	III
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 总体要求	2
6 工伤保险区块链应用平台架构	2
7 工伤保险区块链应用	4
8 工伤保险区块链平台技术要求	6
9 运行维护要求	8
参考文献	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。

本文件由山西省人力资源和社会保障厅提出、组织实施和监督检查。

山西省市场监督管理局对本文件的组织实施情况进行监督检查。

本文件由山西省人力资源和社会保障标准化技术委员会（SXS/TC25）归口。

本文件起草单位：山西省人力资源和社会保障数据中心（山西省社会保障卡管理中心）、山西省检验检测中心（山西省标准计量技术研究院）。

本文件主要起草人：曹晓岚、马春艳、余晓阳、王康童、郭小玉、侯毅、史天福、原野、陈晓丰、韩琪、李锋艳。

工伤保险区块链技术应用规范

1 范围

本文件给出了工伤保险区块链技术应用总体要求及平台架构，规定了工伤保险区块链应用、工伤保险区块链平台技术要求、运行维护要求。

本文件适用于工伤保险业务领域的区块链技术应用。

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 31596.5 社会保险术语 第5部分：工伤保险
- 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 32918.2 信息安全技术 SM2椭圆曲线公钥密码算法 第2部分：数字签名算法
- GB/T 35273-2020 信息安全技术 个人信息安全规范
- GB/T 42571-2023 信息安全技术 区块链信息服务安全规范
- GB/T 42752-2023 区块链和分布式记账技术 参考架构
- GB/T 43572 区块链和分布式记账技术 术语

3 术语和定义

GB/T 31596.5、GB/T 43572界定的以及下列术语和定义适用于本文件。

3.1 密码算法

描述密码处理过程的一组运算规则或规程。

[来源：GB/T 34923.5-2017, 3.2]

3.2 对等网络

一种仅包含对控制和操作能力等效的节点的计算机网络。

[来源：GB/T 5271.18-2008, 18.04.05]

3.3 区块链

使用密码技术链接将共识确认过的区块按顺序追加形成的分布式账本。

[来源：GB/T 43572-2023, 3.6]

3.4 联盟链

节点加入需要许可的区块链系统。

3.5

业务链

承载一类特定业务的联盟链系统。

4 缩略语

下列缩略语适用于本文件。

API: 应用编程接口 (Application Programming Interface)

PBFT: 实用拜占庭容错(Practical Byzantine Fault Tolerance)

Raft: 分布式共识机制(Replicated And Fault Tolerant)

RBAC: 基于角色访问控制 (Role-Based Access Control)

RESTful: 表述性状态传递 (Representational State Transfer)

RPC: 远程过程调用 (Remote Procedure Call)

SDK: 软件开发工具包 (Software Development Kit)

WASM: 一种运行在现代网络浏览器中的新型代码(Web Assembly)

5 总体要求

5.1 安全可靠

应实现工伤保险业务数据的链上加密存储与分布式验证，确保核心数据不可篡改，保障数据安全、系统稳定和业务连续性。

5.2 国产化兼容

应具备国产芯片、存储器、操作系统、数据库、国家商用密码算法等国产化软硬件的兼容性。

5.3 隐私保护

应依法保护参保人员个人信息和隐私，保障链上用户隐私安全，防止隐私泄露。

5.4 便捷应用

支持第三方快速接入，降低技术对接成本，实现数据共享和业务协同。

5.5 灵活扩展

工伤保险业务规模扩大或新增业务场景时，链节点与存储容量可灵活扩展。横向跨部门扩展时，底层区块链平台应具备可扩展性，支持通过动态新增节点的方式实现省级各业务相关部门的系统互联互通。纵向跨层级扩展时，应支持跨链、新增节点或标准化接口的方式，与上下级区块链平台互联互通，实现跨层级数据交叉核验。

6 工伤保险区块链应用平台架构

6.1 概述

6.1.1 基于区块链技术的工伤保险应用平台架构分为工伤保险应用层、区块链服务组件层、区块链基础服务层及基础设施层，其关联如下：

- 工伤保险应用层执行相关用户区块链前端应用；
- 区块链服务组件层为工伤保险应用层提供区块链访问和使用支持；
- 区块链基础服务层提供区块链底层基础服务，并为区块链服务组件层提供相关支持；
- 基础设施层提供区块链基础服务层正常运行所需的环境和基础组件。

工伤保险区块链应用平台功能架构图见图 1。

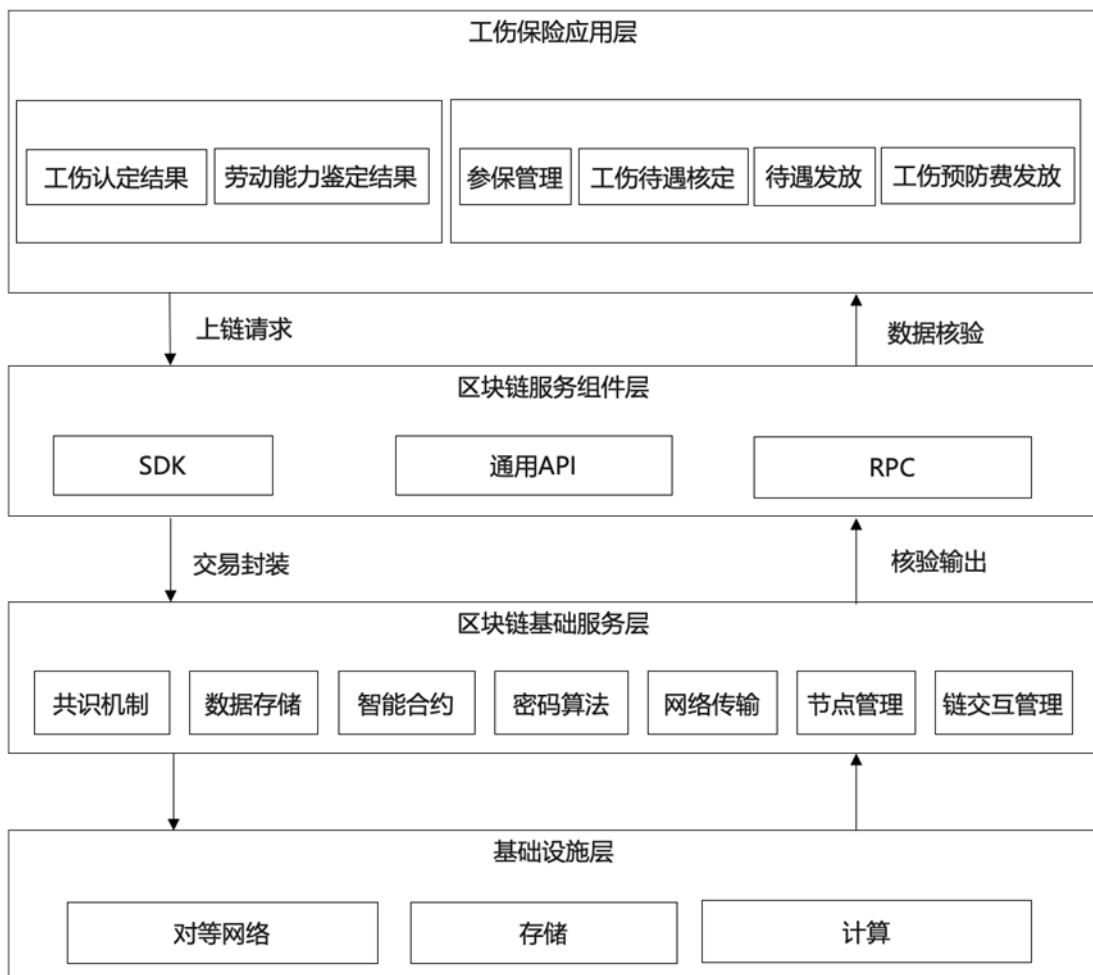


图1 工伤保险区块链应用平台功能架构图

6.1.2 基于区块链技术的工伤保险应用平台在网络结构上应支持高弹性可扩展，包括横向可扩展省级其他行业部门节点，纵向可向上对接部级节点，实现数据的横向互联和纵向互通。工伤保险区块链应用平台网络架构图见图 2。

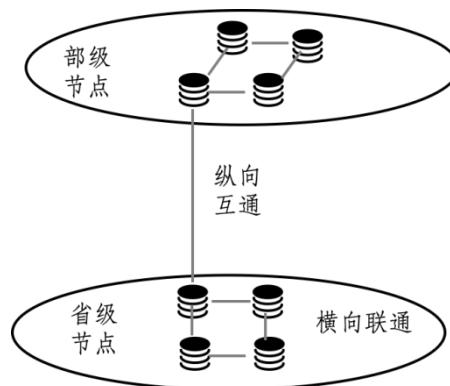


图2 工伤保险区块链应用平台网络架构图

6.2 工伤保险应用层

工伤保险具体业务生成，包括工伤认定结果和劳动能力鉴定结果数据应用，参保管理、工伤待遇核定、待遇发放、工伤预防费发放等核心业务应用。

6.3 区块链服务组件层

负责数据接入和输出，接收业务系统的上链请求。SDK通过客户端指定的用户私钥对交易进行签名，再对交易进行RPC协议封装，传输到区块链基础服务层。SDK、RPC用于实现区块链服务组件层与区块链基础服务层之间的交互。通用API服务用于实现工伤保险应用层和区块链服务组件层之间的交互。

6.4 区块链基础服务层

提供区块链底层基础服务，为上层应用相关数据上链提供基本保障。包括共识机制、数据存储、智能合约、密码算法、网络传输、节点管理、链交互管理等核心模块。

6.5 基础设施层

提供区块链平台运行所需的环境和基础组件，包括对等网络、计算及存储资源。

7 工伤保险区块链应用

7.1 参保管理

7.1.1 单位/建筑项目参保

在单位/建筑项目参保阶段，区块链技术应用如下：

- 业务触发：社会保险经办机构人员通过工伤保险应用层提交单位参保信息，完成业务审批；
- 区块链服务组件层处理：工伤保险应用层后端将单位/建筑项目参保数据推送至区块链服务组件层，区块链服务组件层进行交易封装和发出交易请求；
- 上链存证：交易广播至区块链基础服务层，完成共识存证，返回交易哈希作为参保凭证。

7.1.2 人员参保

在人员参保阶段，区块链技术应用如下：

- 业务触发：社会保险经办机构人员通过工伤保险应用层完成参保登记、暂停、暂停恢复、续保业务，系统终审通过后，完成业务审批；
- 区块链服务组件层处理：工伤保险应用层后端将人员参保数据推送至区块链服务组件层，区块链服务组件层进行交易封装和发出交易请求；
- 上链存证：交易广播至区块链基础服务层，完成共识存证，返回交易哈希作为参保凭证。

7.2 工伤认定和劳动能力鉴定

7.2.1 在工伤认定和劳动能力鉴定阶段，有关部门将最终合法有效的认定工伤决定书和劳动能力鉴定结论书上链。

7.2.2 在工伤认定阶段，区块链技术应用如下：

- 业务触发：工伤认定工作人员作出最终合法有效的认定工伤决定书并送达；
- 区块链服务组件层处理：工伤保险应用层后端将工伤认定最终结果等上链数据信息推送至区块链服务组件层，区块链服务组件层进行交易封装并发出交易请求；
- 上链存证：交易广播至区块链基础服务层，完成共识存证，返回交易哈希作为工伤认定上链凭证。

7.2.3 在劳动能力鉴定阶段，区块链技术应用如下：

- 业务触发：劳动能力鉴定工作人员作出劳动能力鉴定结论书并送达（含初次鉴定、复查鉴定、再次鉴定）；
- 区块链服务组件层处理：工伤保险应用层后端将劳动能力鉴定最终结果等上链数据信息推送至区块链服务组件层，区块链服务组件层进行交易封装并发出交易请求；
- 上链存证：交易广播至区块链基础服务层，完成共识存证，返回交易哈希作为劳动能力鉴定上链凭证。

7.3 工伤待遇核定

在工伤待遇核定阶段，区块链技术应用如下：

- 业务触发：社会保险经办机构人员根据工伤认定结果、劳动能力鉴定结果完成待遇计算操作；
- 区块链服务组件层处理：工伤保险应用层后端将核定待遇项目、待遇金额、待遇起止时间等上链数据信息推送至区块链服务组件层，区块链服务组件层进行交易封装并发出交易请求；
- 上链存证：交易广播至区块链基础服务层，完成共识存证，返回交易哈希作为工伤待遇核定上链凭证。

7.4 待遇发放

在待遇发放阶段，区块链技术应用如下：

- 业务触发：社会保险经办机构人员发起待遇支付流程，由待遇代发银行通过社银直连方式接收发放指令，支付完成并向工伤保险业务系统反馈支付结果；
- 区块链服务组件层处理：工伤保险应用层后端将支付金额及收款账户信息等上链数据信息推送至区块链服务组件层，区块链服务组件层进行交易封装并发出交易请求；
- 上链存证：交易广播至区块链基础服务层，完成共识存证，返回交易哈希作为待遇发放上链凭证。

7.5 工伤预防费发放

在工伤预防费支付阶段，区块链技术应用如下：

- 业务触发：社会保险经办机构人员根据工伤预防项目实施进度分别发起预付款、中期款、尾款的付款流程，由代发银行通过社银直连方式接收发放指令，支付完成并向工伤保险业务系统反馈支付结果；
- 区块链服务组件层处理：工伤保险应用层后端将支付金额及收款账户信息等上链数据信息推送至区块链服务组件层，区块链服务组件层进行交易封装并发出交易请求；
- 上链存证：交易广播至区块链基础服务层，完成共识存证，返回交易哈希作为工伤预防费发放上链凭证。

8 工伤保险区块链平台技术要求

8.1 安全技术要求

- 8.1.1 应支持用户身份、资产信息等敏感数据的脱敏处理，采用最小化原则对敏感数据进行授权访问，限制数据暴露面，进行隐私保护。
- 8.1.2 信息生成过程中应满足密码技术、采集规范、数字签名、信息记录等方面的要求，相关内容符合 GB/T 42571—2023 中 6.1.1.1 c)、d)、e)，6.1.1.2，6.1.1.3 b)、c)、e) 的规定。
- 8.1.3 信息处理过程中应满足信息识别、验证和权限管理等要求，相关内容符合 GB/T 42571—2023 中 6.2.1.1，6.2.2.2 的规定。
- 8.1.4 信息传播过程中应满足智能合约的编译和管理、节点状态和风险预警等要求，相关内容符合 GB/T 42571—2023 中 6.4.1.1，6.4.2.1 a)，6.4.2.2 的规定。
- 8.1.5 应制定安全事件响应处置应急预案，应急预案中明确对发布违法、不良的信息及其节点或账号的处置规则，相关内容符合 GB/T 42571—2023 中 6.4.3 的规定。

8.2 用户权限管理

8.2.1 用户权限管理体系

区块链平台采取四级用户权限管理体系：

- 1 级用户：机构管理员，可使用机构管理，对机构下所有成员和资源进行管理；
- 2 级用户：监管审计员，可进行区块链审计，对区块链数据进行监控、归档、下载等管理操作；
- 3 级用户：普通用户，可按规则参与链上交易；
- 4 级用户：开发运维人员，可使用开发运维功能和工具，对区块链和上层应用进行管理。

8.2.2 用户权限管理要求

应满足以下要求：

- 平台采用基于 RBAC 的账户权限体系，根据用户账号、角色、权限、组织四个维度设计访问控制；
- 每个角色有不同权限，通过对用户赋予不同角色来赋予其对应权限。

8.3 基础设施层要求

应符合GB/T 42752—2023中7.5的规定。

8.4 区块链基础服务层要求

8.4.1 共识机制

8.4.1.1 应支持不少于 2 类共识算法，如 PBFT、Raft 等。

8.4.1.2 应支持不超过 1/3 的节点发生故障时，系统依然能稳定运行。

8.4.2 数据存储

8.4.2.1 应支持全部节点或部分节点的区块数据同步。

8.4.2.2 各节点上的数据应满足最终一致性、完整性和安全性。

8.4.2.3 宜支持存储动态扩容，支持对大规模数据的存储，如分布式存储、数据归档等。

8.4.3 智能合约

8.4.3.1 应支持图灵完备的智能合约，包含算术运算、关系运算、逻辑运算、条件运算、赋值运算等。

8.4.3.2 应支持智能合约生命周期管理功能，包括部署、升级、冻结、解冻、销毁。

8.4.3.3 应支持智能合约运行状态监测和异常回滚功能。

8.4.3.4 应采用自主可控的智能合约执行引擎。

8.4.3.5 宜支持主流智能合约语言，如 Solidity、WASM、Go 合约、Java、C++ 等。

8.4.4 密码算法

8.4.4.1 应符合 GB/T 32918.2、GB/T 32905、GB/T 32907 等相关国家密码管理规范。

8.4.4.2 非对称加密算法应支持国家商用密码数字签名算法，如 SM2、SM9，同时支持密钥协商和管理。

8.4.4.3 杂凑算法应支持国家商用密码杂凑算法，如 SM3。

8.4.4.4 对称加密算法应支持国家商用密码对称算法，如 SM4。

8.4.5 网络传输

8.4.5.1 应支持节点间安全通信，传输数据涉及个人信息，符合 GB/T 35273—2020 中 6.3 的规定。

8.4.5.2 应支持动态组网，包括节点动态加入网络、退出网络。

8.4.6 节点管理

8.4.6.1 应支持对节点的增加、删除、停止和启动功能。

8.4.6.2 应支持对节点的存储和监控的功能。

8.4.6.3 应支持对节点数据进行归档存储，可查询已归档存储的账本数据，避免账本数据膨胀导致的区块链服务异常。

8.4.6.4 应支持对节点数据的备份与恢复功能，以全量或增量方式备份数据，当节点故障或数据异常损坏时通过备份数据进行恢复。

8.4.7 链交互管理

8.4.7.1 应支持业务链和链上节点的配置管理功能，包括业务链创建、节点配置、状态查询等。

8.4.7.2 应支持跨链接入认证配置管理功能，如业务链与链上节点进出策略配置、认证管理等。

8.4.7.3 应支持联盟链配置管理功能，如联盟成员管理、成员权限管理等。

8.4.7.4 应支持动态建立业务链功能，如动态建链的场景配置、流程创建、组员管理等。

8.5 区块链服务组件层要求

8.5.1 SDK

8.5.1.1 应通过 SDK 访问区块链、开发合约编写业务逻辑，实现用户管理、事件订阅以及灵活配置。

8.5.1.2 宜具有多语言 SDK 支持，如 JavaSDK，GoSDK，JSSDK 等。

8.5.2 通用 API

8.5.2.1 应使用通用 API 作为区块链服务组件层的标准化服务接口。

8.5.2.2 应具有简单、轻量、易扩展等特点，如 RESTful API 等。

8.5.3 RPC

8.5.3.1 宜支持采用如 JSON-RPC、gRPC 等主流协议。

8.5.3.2 应支持通过 RPC 执行各种操作，如查询账户余额、发送交易和调用智能合约。

9 运行维护要求

9.1 制度管理要求

应制定相应的制度管理要求对平台进行管理，包括建立监测预警机制，设立安全管理机构配备管理人员、制定人员管理和培训制度等，相关内容符合GB/T 42571—2023中7.1、7.2的规定。区块链备案的相关要求按《区块链信息服务管理规定》执行。

9.2 后期运维要求

应做好日常维护、异常处理、平台监管、升级等运维工作，保证平台有序运行，相关内容符合GB/T 42571—2023中7.4的规定。

参 考 文 献

- [1] GB/T 5271.18-2008 信息技术 词汇 第18部分：分布式数据处理
 - [2] GB/T 34923.5-2017 路灯控制管理系统 第5部分：安全防护技术规范
 - [3] GB/T 42570-2023 信息安全技术 区块链技术安全框架
 - [4] GB/T 43579-2023 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
 - [5] LD/T 04-2021 工伤保险经办服务规范
 - [6] 区块链信息服务管理规定（国家互联网信息办公室令第3号）
-