

基于区块链的就医费用一站式结算规范

Unified settlement of medical expenses based on blockchain
platform technical guide

2026 - 08 - 19 发布

2026 - 10 - 01 实施

目 次

前言 II

引言 III

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 技术架构 2

5 业务流程 3

6 功能要求 4

 6.1 患者信息管理 4

 6.2 费用明细管理 4

 6.3 信用结算管理 4

 6.4 支付接口 5

7 区块链支撑服务技术要求 5

 7.1 区块链技术要求 5

 7.2 医疗区块链服务要求 5

8 接口要求 6

 8.1 标准化接口要求 6

 8.2 安全接口要求 6

 8.3 功能接口要求 6

 8.4 可扩展性接口要求 6

9 性能与安全要求 6

 9.1 性能要求 6

 9.2 数据安全保障措施 7

 9.3 异常处理和故障恢复 7

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。

请注意本文件的某些内容可能涉及专利。本文件发布机构不承担识别专利的责任。

本文件由山东省卫生健康委员会提出。

本文件由山东省大数据局归口。

本文件起草单位：山东健康医疗大数据管理中心、日照市妇幼保健院、德州市卫生健康事业发展中心、山东省立第三医院、济南市康养事业发展中心、潍坊市卫生健康发展服务中心、淄博市市级机关医院、济宁市爱国卫生和健康促进中心、山东省标准化研究院。

本文件主要起草人：李磊、朱永宝、姜伟、张玉龙、王正福、朱兴国、王佳、娄迎曦、刘翀、高国亮、张庆华、林松、隋文玲、王鹏。

引 言

随着信息技术的迅猛发展，区块链技术作为一种分布式数据库技术，以其去中心化、数据不可篡改和可追溯的特点，在多个领域展现出了广阔的应用前景。在卫生健康领域，区块链技术的应用为提升服务效率、确保数据安全和促进医疗信息共享提供了新的解决方案。为了实现就医费用的高效结算，提高患者就医体验，并加强医疗数据的可信度和安全性，探索基于区块链的就医费用一站式结算系统建设。

标准旨在明确区块链技术在就医费用一站式结算平台中的基础作用和要求。构建了采用区块链技术进行就医费用一站式结算的平台技术架构，明确了以信用授权为前提、无感支付为核心的七步业务流程，描述了区块链在费用结算、数据安全、追溯审计等方面的应用模式。

基于区块链的就医费用一站式结算规范

1 范围

本文件规定了山东省内采用区块链技术进行就医费用一站式结算的平台技术架构、业务流程、功能要求、区块链支撑服务要求、接口要求、性能与安全要求。

本文件适用于山东省内规划基于区块链技术开展就医费用一站式结算的医疗卫生机构，及其他相关技术和服务提供商。

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 25069 信息安全技术 术语
GB/T 35273 信息安全技术 个人信息安全规范
GB/T 38645 信息安全技术 网络安全事件应急演练指南
GB/T 42570-2023 信息安全技术 区块链技术安全框架
WS 218 卫生机构(组织)分类与代码
WS/T 363（所有部分） 卫生信息数据元目录
WS/T 364（所有部分） 卫生信息数据元值域代码
WS 445（所有部分） 电子病历基本数据集
WS/T 500（所有部分） 电子病历共享文档规范
WS 537 居民健康卡数据集
WS/T 543（所有部分） 居民健康卡技术规范
WS/T 790（所有部分） 区域卫生信息平台交互标准
YD/T 3203 网络电子身份标识eID术语和定义
T/CESA 1048 区块链 存证应用指南
T/CESA 1049 区块链 隐私保护规范
T/CHIA 001 手术、操作分类与代码

3 术语和定义

GB/T 25069、GB/T 42570-2023、YD/T 3203界定的以及下列术语和定义适用于本文件。

3.1

区块链 blockchain

将区块顺序项链，并通过共识协议、数字签名、杂凑函数等密码学方式保证的抗篡改和不可伪造的分布式账本。

[来源：GB/T 42570-2023，3.2]

3.2

信用就医 credit-based medical care

患者在就医前通过信用评估获得授信额度，在诊疗过程中无需即时付费即可接受检查、化验、取药等服务，诊疗结束后在约定账期内统一结算费用的服务模式。

3.3

无感支付 frictionless payment

在信用就医模式下，系统根据预先授权，在患者完成诊疗后自动触发结算流程，无需患者主动操作即可完成费用支付的服务方式。

3.4

存证 proof of existence

为了保证存证信息（电子数据）的完整性和真实性，采用区块链技术实现多节点共识的存证服务。

3.5

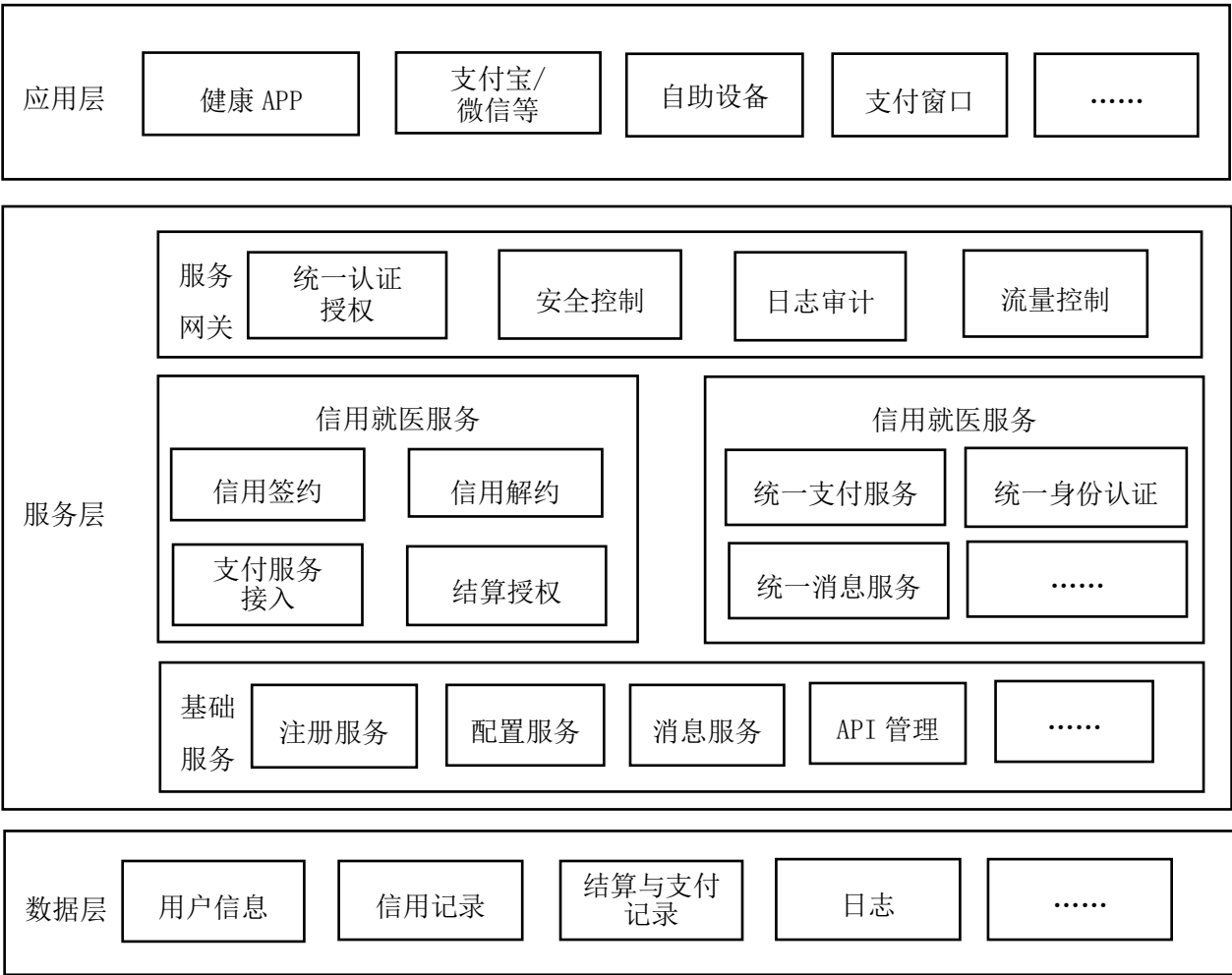
智能合约 smart contract

存储在分布式记账技术系统中的计算机程序，该程序的任何执行结果都记录在分布式账本中。

注：智能合约可以在法律上代表合同条款，并在适用司法管辖区的法律下产生可强制执行的义务。

4 技术架构

平台技术架构宜采用“分层设计、模块化集成”原则，分为区块链支撑层、数据层、服务层、应用层四层，参考架构见图 1。



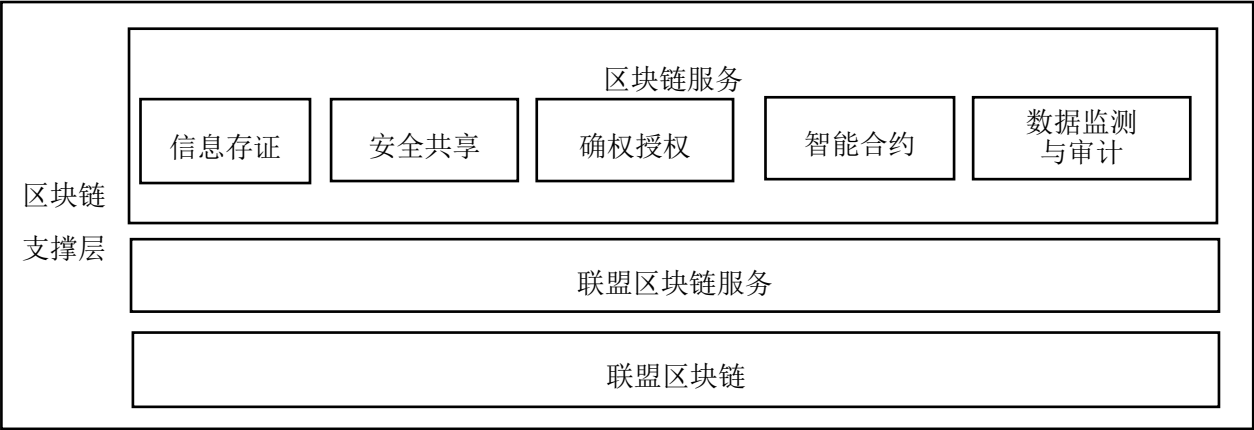


图1 技术架构图

- 各层功能应满足以下要求：
- a) 区块链支撑层：提供信息存证、信息安全共享、确权授权、智能合约、数据检测和审计等服务；
 - b) 数据层：提供数据存储与管理，包括用户信息、信用记录、计算与支付记录、日志等数据的链上共享账本记录及链下安全交换存储；
 - c) 服务层：提供基础服务、信用就医服务、安全支付服务以及服务网关。基础服务包括注册服务、配置服务、消息服务、API 管理等；信用就医服务包括信用签约、信用解约、支付服务接入、结算授权等；安全支付服务包括统一支付服务、统一身份服务、统一消息服务等；服务网关提供统一认证授权、安全控制、日志审计、流量控制等；
 - d) 应用层：支持健康 APP、支付宝/微信等应用接入，支持自助设备以及窗口支付等应用。

5 业务流程

平台将信用支付与就医服务项结合，实现诊间不付费直接检查、化验和取药，看完病后进行信用就医、无感支付。业务流程见图2。

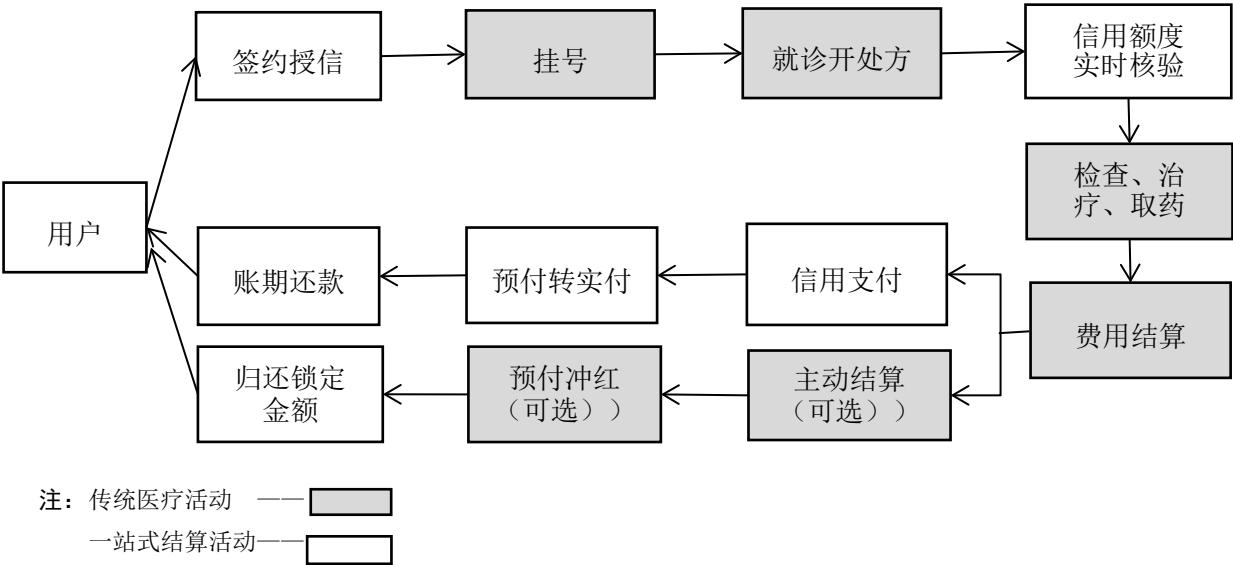


图2 业务流程

平台业务流程以信用授权为前提、无感支付为核心、统一结算为目标，整合传统医疗流程与区块链结算能力。关键步骤操作如下：

- a) 签约授信：患者在选择信用就医服务前，应与医疗机构或第三方支付平台进行签约。签约过程中，进行授信评估，根据患者的信用状况给予对应的信用额度；
- b) 挂号：患者通过线上平台或医院自助终端进行挂号，选择就诊科室和医生，选择“信用就医”支付方式，系统自动关联信用账户；
- c) 就诊开处方：患者前往诊室就诊，医生根据患者病情开具处方和治疗方案；
- d) 信用额度实时核验：系统根据处方、检查单预估费用，从患者信用额度中锁定对应金额（不实际扣除），锁定记录实时上链；
- e) 检查、治疗、取药：患者凭借处方和治疗方案进行检查、化验和取药，无需现场付费；
- f) 费用结算：患者完成全部医疗服务后，系统自动计算并生成最终的费用清单，详细列出各项服务的费用和总金额。结算方式如下：
 - 1) 信用支付：患者选择使用信用额度进行支付，系统自动从患者的信用额度中扣除相应的费用；
 - 2) 预付转实付：如患者在就医前预付了部分费用，结算时应自动转为实际支付金额；
 - 3) 账期还款：患者应在一定的账期内还清使用的信用额度，逾期产生违约金并影响信用记录；
 - 4) 主动结算（可选）：患者在就医过程中可通过自助终端或线上平台，主动结算部分或全部费用；
 - 5) 预付冲红（可选）：如预付锁定的金额超过实际费用，超出部分自动冲红处理，退回至患者的信用支付账户；
 - 6) 归还锁定金额：患者完成费用结算后，系统自动解除对预付锁定金额的冻结，归还至患者的信用支付账户。其中账期的长度和还款方式应在签约时明确说明。

6 功能要求

6.1 患者信息管理

- 6.1.1 支持患者通过身份证、医保卡、人脸识别采集基本信息（姓名、性别、年龄、联系方式、参保类型），信息需符合 WS 537、WS/T 543 要求。
- 6.1.2 支持自动校验患者信息与医保系统的一致性，避免重复建档。
- 6.1.3 支持患者修改联系方式、紧急联系人等非核心信息，核心信息（如身份证号、医保号等）需经人工审核。
- 6.1.4 支持患者查询本人历史就诊记录、信用账户信息，医疗机构可按权限查询患者诊疗相关信息。

6.2 费用明细管理

- 6.2.1 支持与相关医疗信息系统对接，自动获取并整合患者的费用明细数据，数据格式符合 WS 363、WS 364、WS 445 要求。
- 6.2.2 具备对费用明细的编辑功能，医疗机构可根据实际情况对费用进行调整。

6.3 信用结算管理

信用结算管理功能要求如下：

- a) 信用授权：支持多种信用授权方式，包括授信机构信用授权和支付宝等第三方支付平台的信用授权。授权过程中应明确授权的具体条件和流程，确保授权的合法性和有效性；

- b) 信用支付：支持授信额度、第三方支付平台的信用支付功能。系统应明确支付的具体流程和规定，确保支付的顺畅和安全；
- c) 信用结算：若患者在约定的结算时间内未完成费用结算，系统应自动进行结算扣费。扣费过程中应遵循相关的法律法规和行业规定，确保扣费的合法性和公正性，系统应提供扣费明细的查询功能，以便患者核对费用情况；
- d) 消息提醒：系统应根据设定的规则判断，实时推送消息提醒患者完成费用结算等相关操作。消息内容应清晰明了，消息推送渠道包括但不限于短信、邮件、APP 推送等，以确保患者能及时接收到相关信息；
- e) 退费规则：系统应明确退费的条件、流程和途径，确保患者在符合规定的情况下能够顺利办理退费手续。退费过程中应保证资金的安全性和可追溯性；
- f) 对账要求：系统应提供对账单功能，支持医疗机构与患者进行对账。对账流程应与医院现有的对账流程保持一致，以确保对账的准确性和高效性。同时，系统还应支持对账单的查询、打印和导出功能，以便医疗机构进行财务管理和审计。

6.4 支付接口

支付接口应满足以下要求：

- a) 应支持患者和医疗机构工作人员通过操作界面进行支付操作；
- b) 设计应符合 GB/T 22239 三级等保要求，确保支付过程的安全性和稳定性；
- c) 应提供友好的交互流程要求，以使用户能够轻松完成支付操作；
- d) 应支持多种支付方式，包括但不限于在线支付、扫码支付等，以满足不同用户的需求。

7 区块链支撑服务技术要求

7.1 区块链技术要求

宜采用联盟区块链，满足以下技术要求：

- a) 采用高性能共识算法，确保系统性能和响应速度；
- b) 提供高效的智能合约执行引擎，以提升节点内的处理速度；
- c) 确保交易数据和业务信息的隐私安全，可通过命名空间隔离、隐私交易机制、节点密钥管理和数据加密存储等技术手段来实现；
- d) 应支持动态成员的准入与退出，并确保在节点失效时能够快速恢复，以保持系统的高可用性；
- e) 应支持与其他区块链系统的跨链交互，实现数据和信息的互通互联，提升整体系统的灵活性和可扩展性。

7.2 医疗区块链服务要求

应提供下列医疗健康区块链服务，并满足相应的服务要求：

- a) 数据存证：应符合 T/CESA 1048 要求，并确保所有医疗数据和信息在区块链上得到安全、不可篡改的存证，支持数据溯源和验证；
- b) 安全共享：应符合 T/CESA 1049 要求，通过区块链的分布式存储和加密算法，实现医疗数据的安全共享，保护患者隐私；
- c) 确权授权：通过数据存证明确数据的所有权和使用权，通过智能合约等技术手段对数据进行确权，并实现细粒度的访问控制；
- d) 智能合约：应能通过智能合约实现统一结算与支付业务流程的自动化执行，提高医疗服务的效率和准确性；

- e) 数据监测与审计：应能通过区块链上的数据监测和审计功能，确保数据的完整性和合规性，及时发现并处理潜在的风险和问题。

8 接口要求

8.1 标准化接口要求

接口应提供与相关医疗信息系统集成的对接，并根据不同数据内容，满足以下要求：

- a) 患者信息接口：应符合 WS 218 的规定；
- b) 费用明细接口：应符合 WS/T 363、WS/T 364、WS 445 的规定；
- c) 处方、检查单接口：应符合 WS/T 500、T/CHIA 001 的规定；
- d) 结算接口：应符合 WS/T 790 的规定。

8.2 安全接口要求

平台应满足以下安全接口要求：

- a) 身份验证：接口应支持身份验证机制，确保合法用户可以访问接口；
- b) 授权控制：接口应实现授权机制，限制对敏感数据和功能的访问；
- c) 数据保护：通过接口传输的数据均应进行加密和保护，防止数据泄露或被篡改。

8.3 功能接口要求

平台应满足以下功能接口要求：

- a) 患者信息管理接口：支持与相关医疗信息系统交互的接口，以实现患者信息的实时更新和查询；
- b) 费用明细管理接口：应与相关系统对接，获取并管理患者的费用明细信息；
- c) 自动结算管理接口：支持信用授权、信用支付、信用结算、消息提醒、退费以及对账等功能的接口，以实现一站式自动结算服务。

8.4 可扩展性接口要求

8.4.1 接口应采用模块化、松耦合设计，确保在添加新功能模块时，不影响现有接口的正常运行。

8.4.2 应支持接口参数的灵活配置与扩展，可通过配置文件或后台管理系统调整参数规则，无需修改核心代码即可适应系统业务逻辑变化。

8.4.3 接口版本管理机制应完善，新增功能时需进行版本迭代。

9 性能与安全要求

9.1 性能要求

9.1.1 处理能力

平台处理能力应满足以下要求：

- a) 系统响应时间：对于用户发起的请求，系统的响应时间不应超过 2 min，其中核心交易（如支付、结算）响应时间宜≤3 s；
- b) 处理速度：系统应在最短时间内完成数据的处理，对于复杂计算或数据检索，处理时间宜≤30 s；
 - 1) 挂号：用户通过“信用就医”支付方式；处理时间为账户关联≤10 s，挂号确认及凭证生成≤10 s；

- 2) 信用额度实时核验：处理时间为费用预估 ≤ 10 s，额度锁定 ≤ 15 s，锁定记录上链 ≤ 5 s，结果反馈 ≤ 5 s，总耗时 ≤ 30 s；
- 3) 检查、治疗、取药：交互场景为患者凭处方至相关科室，科室调取信用锁定信息确认资格；处理时间为信息调取 ≤ 5 s，资格确认 ≤ 5 s；
- 4) 主动结算（可选）：交互场景为患者发起部分/全部费用结算申请；处理时间为费用计算 ≤ 30 s，结算确认 ≤ 15 s，结果反馈及记录上链 ≤ 15 s；
- 5) 信用支付：信用支付交互场景为患者选择信用额度支付，处理时间 ≤ 15 s；
- 6) 预付转实付交互场景为结算时系统自动抵扣预付金额，处理时间 ≤ 30 s；
- c) 并发用户数：系统应能支持至少 1000 名用户同时在线操作，不出现明显的性能下降。

9.1.2 稳定性和可用性要求

平台应满足以下稳定性和可用性要求：

- a) 稳定性：系统应保证 7×24 h 的稳定运行，无故障时间应达到 99.99%；
- b) 可用性：系统应提供友好的用户界面，确保用户能够方便地进行操作；
- c) 容错能力：在出现硬件或网络故障时，系统应自动切换到备用资源，确保服务的连续性。

9.1.3 兼容性、可扩展性要求

平台应满足以下兼容性可扩展性要求：

- a) 兼容性：系统应能与相关医疗信息系统无缝对接，实现数据互通和流程协同；
- b) 可扩展性：系统设计应预留足够的扩展空间，包括硬件资源的增加、软件功能的拓展等。扩展操作应简便易行，不影响现有系统的正常运行。

9.2 数据安全保障措施

平台应满足GB/T 22239、GB/T 35273信息安全标准安全要求，并采取以下加密措施，提供数据可信安全保障：

- a) 数据加密：宜使用 SM2/SM3/SM4 国密算法，对传输和存储的数据进行加密处理。加密过程应覆盖数据的全生命周期，包括数据的采集、传输、存储和访问等各个环节：
 - 1) 对用户账户的管理宜使用 SM2 算法生成国密账户的公私钥对；使用 SM3 算法对账户公钥进行哈希计算，得到账户地址；使用 SM4 对私钥进行加密/解密；
 - 2) 对病历、处方、检查检验项目、药品购销及结算信息，使用 SM3 计算消息摘要值；使用 SM2 公私钥对进行数据加解密；
 - 3) 数字签名：宜使用国密账户对应的私钥对交易进行签名，签名算法采用 SM2。
- b) 用户身份认证：采用多因素认证方式，如用户名/密码+动态令牌或生物识别技术（如指纹识别、面部识别等），确保用户身份的真实性和合法性；
- c) 数据防护：应对敏感数据进行脱敏处理，并定期进行安全审计和风险评估。建立数据泄露应急响应机制，发生数据泄露时应能迅速采取措施进行处置。

9.3 异常处理和故障恢复

9.3.1 异常处理

系统遇到异常情况时，应采取以下处理流程和报警机制：

- a) 异常报警：当系统检测到异常情况时，应自动触发报警机制，并通过邮件、短信等方式通知管理员；
- b) 异常记录：系统应自动记录异常信息；

- c) 宜提供自我修复尝试。如无法修复，系统应进入安全模式并等待管理员介入处理。

9.3.2 故障恢复

9.3.3 应定期对数据进行全面备份，并存储在安全可靠的位置。

9.3.4 建立灾难恢复计划并定期进行应急演练，应急演练宜按 GB/T 38645 相关规定执行。确保在紧急情况下迅速恢复正常运行。

参 考 文 献

- [1] ITU-T X.509 信息技术 开放系统互连 号码簿：公开密钥和属性证书框架
 - [2] WS/T 483（所有部分） 健康档案共享文档规范
-