ICS 35.020
CCS L 73

T/ZADT

团　　体　　标　　准

T/ZADT 005-2022

基于区块链的医疗服务数据管理技术要求

Technical requirements of blockchain-based data management for medical service

（征求意见稿）

20XX-XX-XX 发布　　20XX-XX-XX 实施

浙江省国际数字贸易协会 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这些专利的责任。

本文件由杭州趣链科技有限公司提出。

本文件由浙江省国际数字贸易协会归口。

本文件起草单位：

本文件主要起草人：

引　言

医疗服务数据分布十分广泛，并伴有数据采集节点众多，数据类型多元，数据使用范围广，以及数据之间的业务关联性复杂等特点。随着医学科技的进步，人们越来越注重个人健康数据的管理，但是，因为个人的医疗服务诊断数据没有地方进行统一地存储与管理，导致在治疗相关疾病，或者管理个人健康数据时，无法查询到个人所有的历史健康数据。这对改善个人健康、治疗慢性疾病等问题，带来了巨大的挑战。

传统的数据管理方式一般采用中心化的存储方式，将数据存储在集中式的数据库或大型的数据中心，并由单一的机构对数据存储进行管理和维护。这种数据管理方式存在以下缺点：（1）仅数据的拥有者可对数据进行使用；（2）存储数据的基础设施使用效率较低、扩展成本较高，在处理大量数据时性能受限；（3）数据集中存储，数据拥有者可能篡改后者访问数据，存在破坏数据完整性和泄露隐私的风险。而基于区块链的数据管理方式具备信息难篡改、可追溯、集体维护和高度透明等特点，相较于传统集中式的存储方式而言，能够更好地管理数据，帮助数据生产者、消费者维护自身的合法利益。

通过本文件的编制实施，依托区块链上数据可信不可篡改的特点及区块链天然具备的权限管理能力，提出医疗服务数据管理框架模型，规范了基于区块链技术的医疗服务数据管理的技术要求和环境要求。帮助医疗机构实现隐私保护条件下的可信数据共享，提高医疗服务数据的安全性。并且，所有针对医疗服务数据的调用和分享操作都将在链上进行实时记录与溯源，为追溯医疗服务事故的责任界定，提供可信依据。

基于区块链的医疗服务数据管理技术要求

1 范围

本文件提出了基于区块链的医疗服务数据管理框架，规定了基于区块链的医疗服务数据管理的技术要求和环境要求。

本文件适用于为使用区块链技术的医疗服务建立数据管理、进行数据分析和数据交易提供技术参考；也为监管机构提供药品溯源追踪或医疗流程审计的监管依据。

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 25069-2010 信息安全技术 术语

CBD-Forum-001-2017 区块链 参考架构

ISO 22739:2020 区块链和分布式账本技术-术语（Blockchain and distributed ledger technologies — Vocabulary）

3 术语

3.1

区块链 blockchain

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：ISO 22739，定义 3.6]。

3.2

智能合约 smart contract

存储于分布式账本中的计算机程序。

注：用于程序化的记账或自动化交易执行，其共识执行结果都记录在分布式账本中。

3.3

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]

3.4

共识算法 consensus algorithm

区块链系统中各节点间为达成一致所采用的计算方法。

[来源：CBD-Forum-001-2017，定义 2.2.3]。

3.5

用户 user

用户是指参与到分布式账本上实际责任主体的基本单位，责任主体一般指自然人、法人或者机构等。用户只有通过分布式账本上的账户才能参与分布式账本的业务，一个用户至少拥有分布式账本上的一个账户。

4 缩略语

下列缩略语适用于本文件。

API	Application Programming Interface	应用编程接口
TEE	Trust Execution Environment	可信执行环境
P2P	Peer-to-Peer	对等网络
PBFT	Practical Byzantine Fault Tolerance	实用拜占庭容错
POW	Proof of Work	工作量证明
POS	Proof of Stake	权益证明
DPOS	Delegated Proof of Stake	股份授权证明机制
IoT	Internet of Things	物联网

5 医疗服务数据管理框架

基于区块链技术对医疗服务数据管理框架进行整体设计，满足医疗服务数据采集、数据记录、数据共享及数据管理的需求。如图1所示，基于区块链的医疗服务数据管理框架由5个构建块组成，自上而下分别是应用层、服务层和承载层，相关方垂直置于水平层左侧，右侧包含了管理决策方。

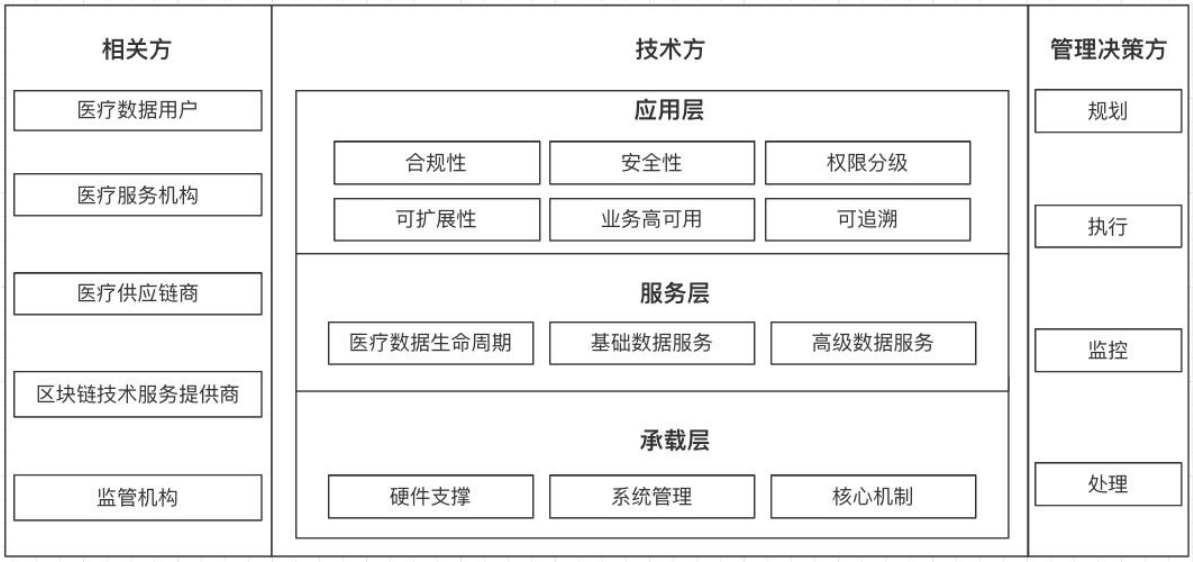

图 1 医疗服务数据管理框架

相关方是基于区块链的医疗服务参与方，根据不同的医疗服务场景，可包括医疗服务数据用户、医疗服务机构、医疗服务供应商、区块链技术服务提供商和监管机构等。

技术方是为基于区块链的医疗服务提供技术支撑，主要包括应用层、服务层和承载层，本文件的第6、7、8章分别对承载层、服务层和应用层提出了规范性技术要求。

管理决策方是为整个医疗服务数据管理从计划设计到最后整个过程的控制。主要包括规划阶段、执行和监控阶段以及处置阶段。规划阶段为响应医疗服务数据用户的请求奠定了基础，包括数据用途、数据规范和资源预算。执行和监控阶段包括数据生成、数据收集、数据处理、数据应用和性能评估几个阶段。最后，处置阶段结算费用，审核记录，总结和审查结果，最后根据数据所有者在计划中商定的条款，删除、转移或重用在数据管理生命周期中收集和处理的数据阶段或数据管理系统设计，具体取决于系统的特定用途。

6 承载层技术要求

承载层提供了基于区块链的医疗服务系统正常运行所需的操作环境和基本组件。包括硬件支撑、区块链技术核心机制、系统管理等。这一层是大多数软件系统所依赖的资源，是基于区块链技术的医疗服务系统的基础支撑。承载层应提供所需要的基础软硬件模块、区块链底层运行系统配置，以及对各组件模块的管理。满足了系统正常运行的需求，并为上层应用提供技术支持，保证链上数据可追溯、不可篡改和数据管理可审计。承载层主要解决数据的一致性和信任问题，使分散的分布式节点能够快速对分块医疗服务数据达成一致，进而实现医疗服务数据的快速认证，保证数据管理的可靠性。区块链医疗服务数据管理的承载层，如图2所示。

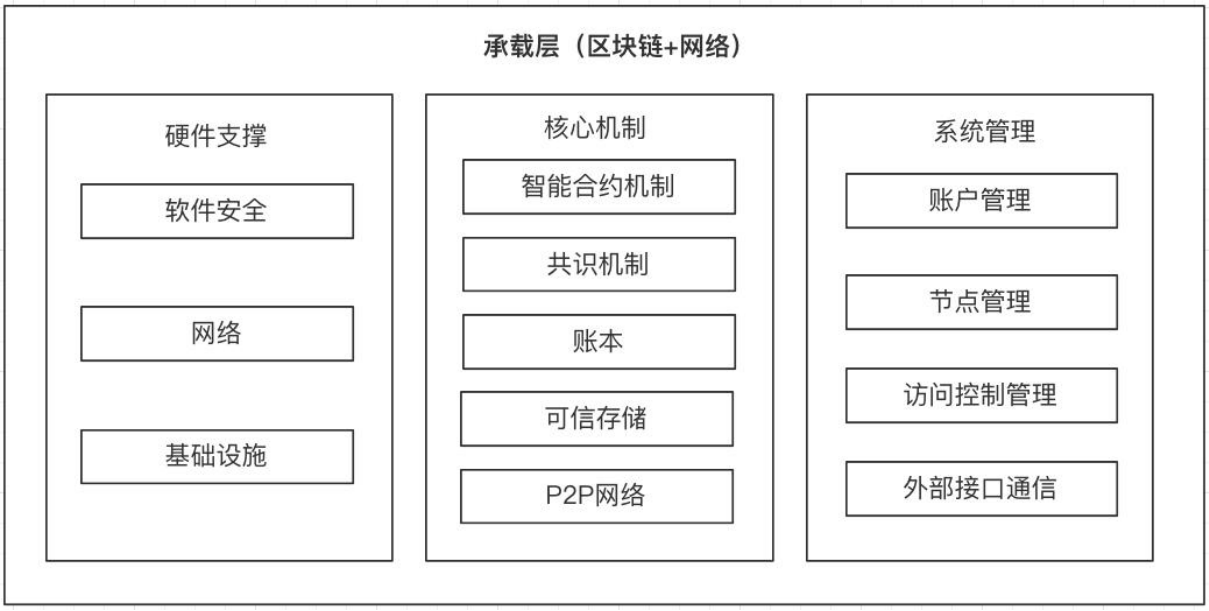

图 2　医疗服务数据管理框架的承载层

6.1 硬件支撑

硬件支撑包括软件安全，网络和基础设施。硬件支撑需要满足以下要求：

a) 软件安全能力需要硬件运行环境的支持，基于区块链的医疗服务系统的硬件需要具备防止物理攻击的能力。推荐使用可信执行环境(TEE)，是指使区块链系统支持高性能数据隐私增强的一种选择，给医疗服务设备提供一个安全的运行环境；

b) 保障通信网络正常运转；

c) 硬件支撑需要满足网络管理的要求。特别是在无权限的区块链系统中，每个节点都具有相同的特权，节点所有者能够决定节点本身的贡献，网络管理提供基本的能力来控制网络中的节点；

d) 医疗服务基础设施需要满足医疗服务系统的结构、通信设施、控制措施、运行调度机制的要求，确保医疗服务系统基础设施的可靠和安全。

6.2 核心机制

核心机制包括智能合约机制、共识机制、账本、可信存储、P2P 网络。核心机制需要满足以下要求：

a) 智能合约的部署、调用、升级等需要通过电子签名等方式授权。智能合约需要进行安全性审核，保证智能合约的安全运行。区块链信息服务提供者需提供符合其业务范围的智能合约；

b) 区块链系统应使用基于共识算法的共识机制，共识算法包括但不限于实用拜占庭算法（PBFT）、工作量证明机制（POW）、权益证明机制（POS）、股权授权证明机制(DPOS)；

c) 账本信息存储需要制定信息存储策略，明确账本信息存储方式、存储流程、同步方式等关键策略要素。需要配备相应的硬件存储资源和设施设备。需具备账本信息保护的技术措施。需要定期对账本信息进行查验，防止信息篡改；

d) 核心机制需满足可信存储的要求，可信存储应具有链上存储，并可组成链上和链下存储的组合，

以支持隐私监管要求；

e) 核心机制需包含 P2P 网络，P2P 是区块链系统的重要基石，基于 P2P 网络，每个节点都可以提供全网所需的全部服务。P2P 网络设计时需要满足分布式、可靠性高、可以容忍部分节点失效的要求。

6.3 系统管理

系统管理包括账户管理、节点管理、访问控制管理和外部接口通信管理。系统管理需要满足以下要求：

a) 系统管理需要提供账户管理的功能，帐户管理者对系统账户进行统一管理，可根据不同业务设置超级管理员、管理员的角色；

b) 系统管理需要支持节点管理，节点管理提供了区块链系统管理的“操作维护”功能，包括节点部署和节点管理。区块链系统中的每个节点都由节点所有者维护；

c) 系统管理需要包含访问控制管理，依据安全策略控制用户对数据的访问，制定访问控制策略，为账户分配访问权限；

d) 系统管理需要支持外部交互管理功能，一个开放网络假设的区块链系统能够与外部系统交互/互操作，外部交互管理是外部资源管理的运行时引擎。

7 服务层技术要求

数据服务层由数据生命周期管理、基础数据服务和高级数据服务等组成，如图 3 所示。作为整个医疗服务业务所需数据服务的提供方，应实现对数据服务过程的全流程管理需求，目的是持续让数据用起来，让成为资产的数据作为生产资料融入业务价值的创造过程，持续产生价值。

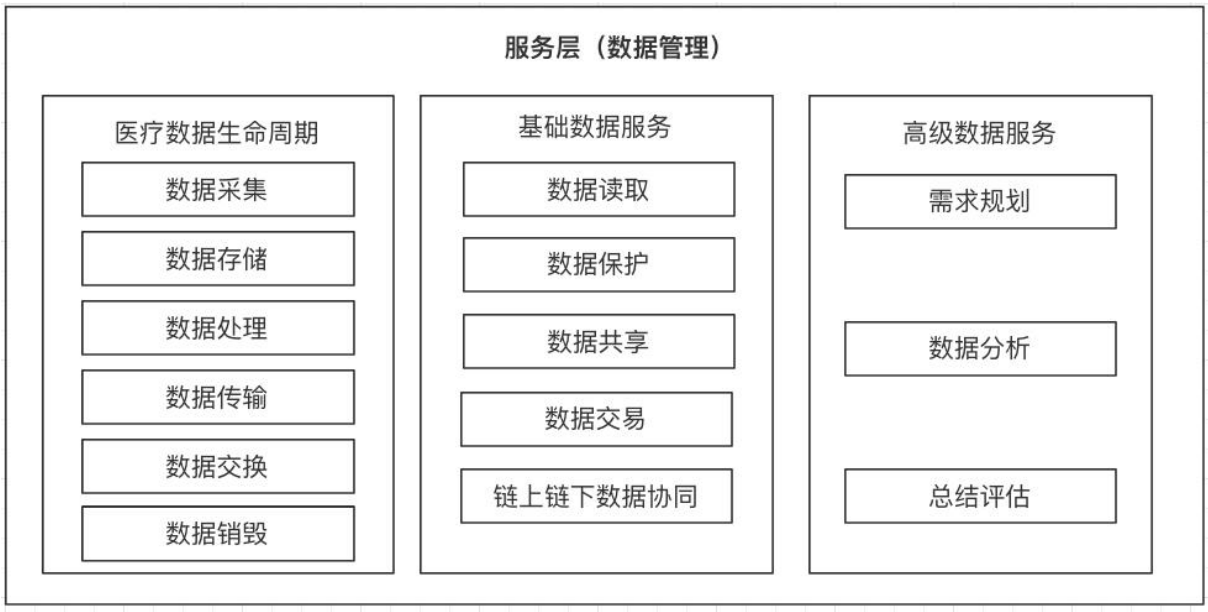

图 3 区块链医疗服务数据管理服务层

7.1 数据生命周期

从数据管理顺序的角度来看，数据生命周期包括数据采集、数据存储、数据处理、数据传输、数据交换、数据销毁的全部流程。数据生命周期需要满足以下要求：

a) 数据采集也就是数据来源，主要包括IoT设备（医疗服务设备检查数据）、Oracle、物资/合同数据和通用数据的采集等，可通过配备硬件加密、TEE(可信执行环节)等来最大限度的提高数据来源的准确性；

b) 数据存储需要对数据进行加密存储，保证业务信息内容的完整性和保密性，设置数据访问权限。对账户数据、区块数据、配置数据、证书等不同类型数据进行分类存储、分开管理。隐私数据保存在本地；
c) 数据处理需要对数据进行分类分级管理；
d) 数据传输需满足链上数据审核的能力。需要保障数据链路安全，采用加密传输协议；
e) 数据交换宜采用加密技术及记账节点之间的共识算法，确保数据资产及交换过程的安全性；
f) 数据销毁需要明确信息销毁方式、销毁流程。数据的销毁包括但不限于对区块链浏览器、客户端、移动端等平台上信息的销毁；并且对信息销毁过程存证，记录销毁人员、销毁时间、销毁内容、销毁方式等关键信息。

7.2 基础数据服务

基础数据服务包括但不限于数据读取、数据保护、数据共享、数据交易、链上链下数据协同等基本数据服务，为数据应用层提供数据支撑。通过区块链接口读取所需的数据，以完成网格信息数据交互。这些服务通过存储功能的数据 API 与收集和处理的数据进行交互，数据服务对外暴露的不是数据而是接口，数据消费者不用直接获取数据，而是通过接口服务获取。

a) 数据读取需要提供数据的访问权限；
b) 数据保护需要建立和实施适当的安全措施，包括物理措施和技术措施，确保数据安全；
c) 数据共享需要保障数据链路安全，采用加密传输协议；
d) 数据交易是将数据作为资产进行交易，应符合资产交易的要求；
e) 链上链下数据协同有助于提高数据的关联性和一致性。链上即区块链，链下即所有传统的信息系统。数据哈希链上铆定存储，链上授权和记录、链下数据交换，基于区块链进行细粒度权限控制，交换记录上链，保证后期数据不可篡改，数据使用和流转可追溯审计。

7.3 高级数据服务

高级数据服务不仅包括需求规划、数据分析和汇总评估过程，还应包括针对不同场景不断优化和调整数据以满足新的计划业务需求：

a) 需求规划阶段应提前准备好相关数据需求资料，包括数据规划、数据用途、数据规范、数据资源预算等；
b) 数据分析阶段，利用数据分析工具、手段、方法或思维，从安全、可靠、有效的基础数据中挖掘数据价值；
c) 总结评估阶段包括评估、总结、审计、数据重用等，作为决策依据。

8 应用层技术要求

应用层利用服务层和承载层提供的数据服务，为医疗服务数据用户提供可定制的、可展示的、交互式数据应用。医疗服务区块链的应用主要集中在医疗服务、医疗安全、医疗保险、医疗报销、医疗服务健康档案管理、医疗服务供应链监控和药品溯源等方面。基于分布式账本技术的特性，可以针对不同的业务场景构建特定的链，在保证企业或机构数据隐私的同时满足个性化需求。应用层应满足以下技术要求：

8.1 合规性

医疗服务应用及配套设施的建立、运行等应满足合规性要求，宜考虑以下条件：

a) 设计文档中对于账本系统的职责、权限等规范明确，使账本系统的运作有规范可循；
b) 系统对于用户个人信息采取加密保护和安全管理措施；
c) 遵循独立性、系统性、全员参与、强制性、管理地位与职责明确的科学管理原则进行合规管理。

8.2 安全性

医疗服务应用需满足安全性原则，宜考虑以下条件：

a) 具备系统的保密与安全防护、私钥密钥算法的选取、系统各层数据的传输安全保障等条件；
b) 具备安全保障机制，配有可不断完善、改进的应急处理机制与实际措施；

c) 确保加入节点的各方身份安全可靠，资产真实合法，节点权限可控；
d) 确保数据的生成、传输、存储、调用的数据安全，宜将密钥与数据分离，确保其保密性。

8.3 权限分级

医疗服务应用的权限划分、授予、收回等宜纳入系统生命周期管理中，宜考虑以下条件：
a) 建立并完善相关方的账户管理体系，如账户管理、相关方管理、权限管理、授权范围等；
b) 减少非必要信息采集，采取最小权限原则和多角色授权方案；
c) 根据相关方级别授予对应权限，不越权、划分明确，不同级别相关方获取对应的数据访问权限。

8.4 可扩展性

医疗服务应用满足可拓展性的要求，宜考虑以下条件：
a) 供应链金融服务的建立与评价考虑到其系统内部功能的可拓展性，充分考虑系统未来的成长；
b) 系统的建设宜对未来发展趋势做科学预判，系统架构组件设计具有延展性，能够满足未来新的需求与发展；
c) 设计文档对系统的模块化、组件化等宜进行充分考量与规划，设计良好的代码以允许更多的功能被添加到适当的位置。

8.5 业务高可用

考虑到分布式账本的应用领域，高可用性是账本系统宜充分规划的特性之一，宜考虑以下条件：
a) 医疗服务时刻保持提供有效服务时间，防止服务器故障等问题导致服务不可用；
b) 避免和减少运营维护操作以及突发应急的系统崩溃、受攻击所导致的停机时间；
c) 具备高应对处理能力，在面对高并发流量时，能够保障其核心功能需求；
d) 具有自动备份与还原能力，系统崩溃或受攻击可还原至最近备份点；
e) 具有灾备处理能力，如建立同城双活中心、异地容灾数据中心等。

8.6 可追溯

医疗服务应用系统基于区块链技术，应具备数据可追溯能力，宜考虑以下条件：
a) 对全生命周期间产生的资产相关的数据进行唯一性标识和存证；
b) 可追溯数据考虑包括：数据生成时间、数据类型、数据来源方、数据查询方信息、授权信息、权属变更、追溯历史记录、数据更改与访问记录等；
c) 系统、用户、授权信息等数据的追溯宜根据数据的敏感程度和重要性划分，根据性质的不同采取对应的追溯方案；
d) 系统根据数据的敏感程度和重要性依次展示类型不同的数据量，用以满足不同的追溯需求。

9 医疗服务数据环境要求

医疗服务数据分布非常广泛，数据采集节点众多，数据类型多元，数据之间的业务关联性也更加复杂，数据应用更加广泛。因此，为方便医疗服务机构或医疗服务企业之间的数据存储、数据交换、数据共享等，构建数据安全可信的存储环境，提高数据的可靠性、完整性和准确性，对医疗服务机构和医疗服务企业的运营具有重要意义。

从数据管理的角度来看，区块链本质上是一个点对点网络组件，提供数据库系统可靠的数据管理功能。可信数据库管理系统涉及三个方面来保证系统的可信性，包括存储信任、处理信任、外部信任，如图 4 所示。

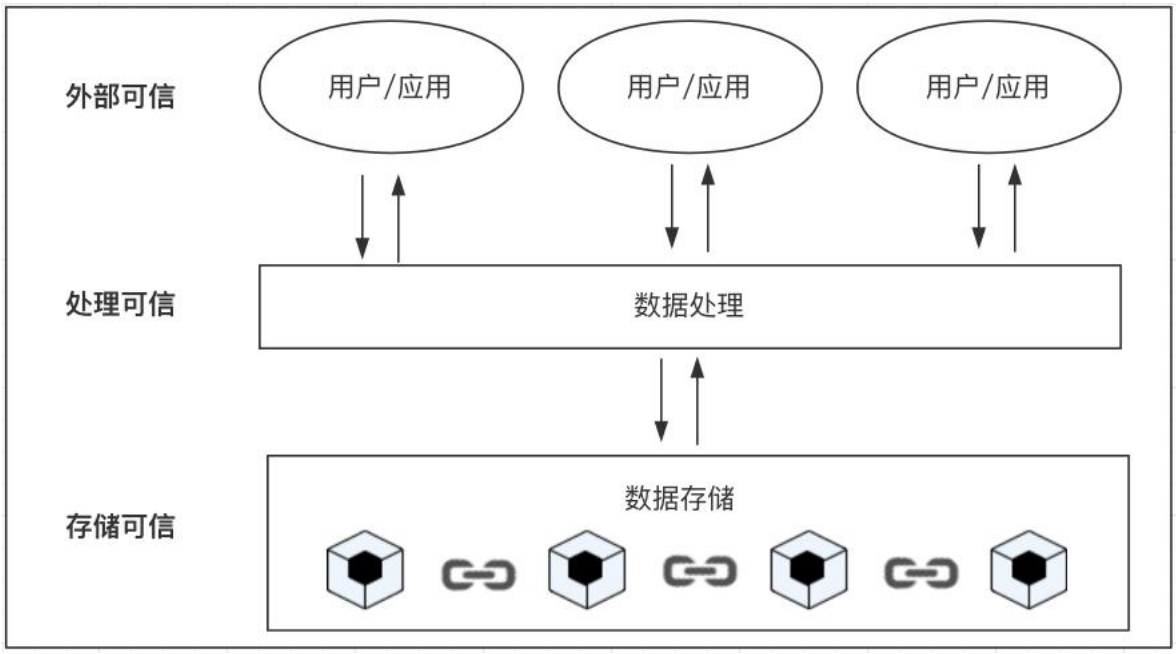

图 4　基于区块链的医疗服务数据管理外部数据环境

9.1　存储可信

存储可信性是指数据处理结果一旦被确认，不会丢失或被篡改，它要求系统提供传统数据库管理系统和事务处理中所要求的的事务持久性，但同时也要求系统在存储、通信故障，甚至在蓄意攻击时，仍能确保数据存储的正确性。

9.2　处理过程可信

一方面，要求数据管理整个过程是可信性的。另一方面，要求整个数据管理的过程是可追溯和可审计的。前者需要对数据处理的正确性进行把控，而后者需要系统保存最终状态以及数据处理的过程。数据处理的正确性是传统数据管理系统的基本要求。

9.3　外部环境可信

外部环境可信是指人员、设备、网络、运维等基础设施环境，及物理环境的可信。运行区块链系统的网和主机应处于受保护的环境，其保护措施根据具体业务的监管要求不同，可采用不限于 VPN 专网、防火墙、物理隔离等方法，对物理网络和主机进行保护。