基于双链架构的医药商业资源公有区块链

毕 娅[1,2] 周 贝[2] 冷凯君[2] 王存法[3]

(华中科技大学公共管理学院 武汉 430074)[1] (湖北经济学院物流与工程管理学院 武汉 430205)[2]

(武汉理工大学管理学院 武汉 430070)[3]

摘 要 区块链技术是一种去中心化的共享总账系统和计算范式。作为一种核心的底层支撑技术,它与分布式经济系统有极高的契合度。基于公共服务平台的医药商业资源分布式调度模式是解决当前医药商业行业"散、小、乱、弱"局面的综合性解决方案,在聚合分散性资源和按需调度方面发挥着重要作用。针对公共服务平台当前存在的一些关键问题,提出了一种基于双链架构的医药商业资源公有区块链,重点研究了公有区块链的双链结构及其存储方式、隐私保护、资源寻租与匹配机制和共识算法等问题。研究结果表明,基于双链架构的医药商业资源公有区块链能够兼顾交易信息的开放性、安全性和企业信息的隐私性,自适应地完成资源的寻租和匹配,并大幅提高公共服务平台的公信力和系统的整体效率。

关键词 公有区块链,共识机制,医药商业资源,公共服务平台

中图法分类号 TP315 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2018.02.007

Public Blockchain of Pharmaceutical Business Resources Based on Double-chain Architecture

BI Ya[1,2] ZHOU Bei[2] LENG Kai-jun[2] WANG Cun-fa[3]

(College of Public Administration, Huazhong University of Science and Technology, Wuhan 430074, China)[1]

(School of Logistics and Engineering Management, Hubei University of Economics, Wuhan 430205, China)[2]

(School of Management, Wuhan University of Technology, Wuhan 430070, China)[3]

Abstract Blockchain is a decentralized shared ledger system and computational paradigm. As a core underlying support technology, it is highly compatible with the distributed economic system. The distributed scheduling model of pharmaceutical business resources based on the public service platform is a comprehensive solution to the current situation of pharmaceutical industry which is "scattered, small, disorderly and weak", and plays an important role in integrating decentralized resource and making on-demand schedule. Aiming at some key problems in the current public service platform, this paper proposed a public blockchain of pharmaceutical business resources based on double chain architecture, and mainly studied the double-chain structure and its storage mode, privacy protection, resource rent-seeking and matching mechanism, and consensus algorithm. The results show that the public blockchain of pharmaceutical business resources based on double-chain architecture can take into account the openness and security of transaction information and the privacy of enterprise information, self-adaptively complete rent-seeking and matching of resources, and greatly enhance the credibility of the public service platform and the overall efficiency of the system.

Keywords Public blockchain, Consensus mechanism, Pharmaceutical business resources, Public service platform

1 引言

医药商业行业是负责药品在市场上流通的独立经济部门。医药商业资源作为医药产品流通的载体,是满足人们对医药产品需求以及维持其质量和安全的重要保障。目前,我国有1万余家医药商业企业,其中绝大部分为中小企业,医药商业资源的分散性十分显著。由于利益的驱动,医药商业资源对发达地区的覆盖率较高,资源投入明显过剩;但对偏远和不发达地区的覆盖率极低,医药商业企业很难自发地满足偏远和不发达地区对医药产品的需求,社会矛盾突出。

随着计算机技术和分布式计算的快速发展,以"分散资源集中管理、集中资源分散服务"为目标的公共服务平台成为解决医药商业资源需求和供给矛盾的关键。公共服务平台是一种基于第三方和非盈利的网络系统,能够通过对分散性医药

到稿日期:2017-10-14 返修日期:2017-11-30 本文受国家自然科学基金(70160376),中国博士后基金项目(2015M580648),中国博士后特别资助项目(2017T100560),湖北物流发展研究中心资助。

毕 娅(1978—),女,博士,副教授,主要研究方向为离散系统仿真与优化,E-mail:idabiya@126.com(通信作者);周 贝 主要研究方向为物流工程;冷凯君 博士,副教授,主要研究方向为物流工程、区块链技术;王存法 硕士,高级工程师,主要研究方向为PPP工程、招投标管理。

商业资源的虚拟化聚合和调度,以点对点的形式直接向资源需求方提供质优价廉的标准化服务。其运行的一般过程为:首先,医药商业资源的供需双方向公共服务平台提供自己的各项信息,包括身份 ID、资源的需求量和供给量、资源类型和寻租条件等;其次,公共服务平台在各种云端化技术[1-2]的支持下对各种分散性医药商业资源进行虚拟化集成[3],并对这些资源进行封装,形成标准化服务[4],实现"分散资源的集中管理"[5];最后,公共服务平台对医药商业资源的需求和供给进行动态的寻租和匹配[6],以实现"集中资源的分散服务"[5]。公共服务平台由于在资源配置的全过程中对资源供需双方透明,而且还能够提供"以用户为中心"的推送式公共服务[7],因此在很大程度上降低了资源供需双方对具体资源管理的复杂性,为资源供需双方提供了广阔、个性化和规则化的资源使用环境[8]。由此可见,公共服务平台打破了真实世界中软管理和硬资源之间的紧密耦合关系,去除了资源与其所有者之间的隶属关系,标准化了资源服务的内容和价格,改变了传统资源管理模式中供需双方单一的服务映射关系,协同了各层次和各环节上资源的运作,是一个能够从宏观层面上对分散性资源进行优化配置的综合性解决方案[9-11]。

虽然上述文献对公共服务平台及其调度模式的研究已较为具体和深入,但仍存在一些尚未解决的关键问题。

1)资源供需双方自适应寻租和匹配问题

公共服务平台是一个分布式系统,需根据医药商业资源的分散性、海量性、随机性、公益性和异构性等特征对其供需进行去中心化的聚合和调度。但目前,公共服务平台尚未建立起资源的自适应寻租和匹配机制,医药商业资源的利用率和系统的整体效益不理想,这不仅会提高交易成本,而且容易触发资源供需双方退出公共服务平台的策略选择行为。

2)交易信息的安全与透明性及用户信息的隐私性问题

公共服务平台一方面要保证交易信息的安全与开放性,另一方面还要保证用户信息的隐私性。但目前,公共服务平台还没有一套成熟可靠的信息安全保障机制,既无法保障资源供需双方寻租和交易的安全与透明性,也无法保障用户信息的隐私性,容易引发公共服务平台上的信息被非授权获取和篡改、资源分配权和使用权被非法滥用或挪用,以及延期支付等问题。

3)平台公信力问题

公共服务平台是一个去中心化的中介组织,在没有政府部门主导和直接参与的情况下,其公信力难以建立,容易引发公共服务平台的违规经营、医药商业资源需求与供给信息的不实或虚假发布以及恶意违约等问题。这无疑会伤害公共服务平台各参与主体的利益。因此,利用技术手段而非权力机构建立公共服务平台的公信力,是建立基于公共服务平台的医药商业资源分布式调度和管理模式的关键。

针对上述问题,本文提出一种双链架构的医药商业资源公有区块链,并将其引入到公共服务平台,为公共服务平台提供运行环境和技术支撑。该区块链不仅能够为去中心化的公共服务平台提供用户隐私信息保护机制与分布式的资源寻租和匹配机制,而且还能够根据公共平台上不同类型信息的要求,为其提供安全保障机制,从而大幅提高医药商业资源的利用率、公共服务平台的公信力和系统的整体效率。

2　区块链技术

2.1　区块链的基本概念和数据结构

区块链是一种由多节点集体维护、点对点传输、加密算法、共识机制等计算机技术[12]实现的分布式记账系统,即一种分布式数据库,具有高度的可靠性、数据完整性、去中心化和去信任化特征,能够实现在没有任何第三方背书的前提下,任意节点之间安全地进行信息传输和交易。

区块链具有链式数据结构,其每个区块主要由两部分组成[13]:1)区块头,包含前驱区块的 Hash 散列值(Hash 散列值由区块头、区块主体和随机数共同构成),用于链接前驱区块,同时为用户提供查询、追踪和验证信息的功能;2)区块主体,包含本区块的主要信息,如交易的时间、位置、数量、金额和规则等。区块链的数据结构如图 1 所示。

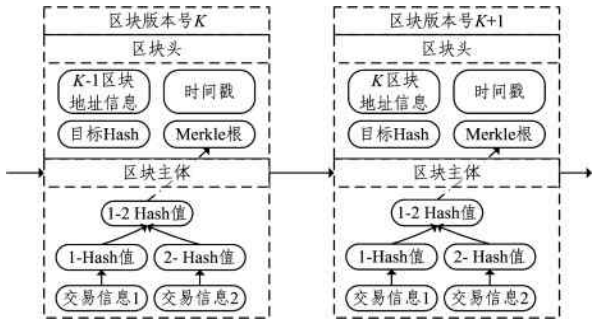

图 1　区块链的数据结构

Fig. 1　Data structure of blockchain

区块链的这种链式数据结构使得每一个区块都存储了前驱区块的信息,同时也将自己的信息放到了后续区块的头部;非对称密钥系统和智能合约则保证了恶意攻击无法篡改信息[14],确保了区块链中数据的真实性和完整性。因此可以说,区块链不仅是一种分布式的共享总账系统,而且是一种可编程的基础架构和计算范式[15]。这种特性使得区块链在以去中心化、资源分散、供需自适应匹配和交易自动执行为特征的经济系统中具有非常高的应用可能性。

2.2　区块链技术应用于医药商业资源分布式管理的可行性分析

1)资源供需之间的自适应寻租和匹配

区块链上所有的节点都将自己的信息和交易规则写在区块体内,并向全网广播。每一个资源供给节点根据最新区块内的信息进行自动搜索,寻找与自己适配的需求节点。一旦交易达成,节点之间可以进行点对点的数据互操作,因此交易达成、执行和完成的效率都非常高。这在很大程度上解决了小体量医药商业企业参与实时批发市场交易时容易导致的效率低下的问题,弥补了单一用户的可控资源和资源可调度性十分有限的缺陷,降低了由单一用户的策略选择性行为为交易带来的不确定性风险。同时,区块链允许需求节点将选择性激励机制写入交易规则,引导交易按照既定的方向运行,可

形成更倾向于偏远和不发达地区的选择偏好。这对实现医药商业资源的公益性属性具有十分重要的现实意义。

2)去中心化的集体维护和共识机制

传统记账系统是集权管理的。一旦集权节点“不忠诚”或发生意外,则会导致整个系统不可信。区块链上没有集权节点,所有节点都参与系统的运行和维护。这意味着每个节点都包含了同样的账本信息,需要共识机制来保证数据的一致性。区块链使用椭圆曲线密码对链中的所有数据进行加密。任意节点上一个极微小的变化都极易被发现并迅速纠正。这使得所有节点都能够在决策权高度分散的去中心化系统中对数据的安全性、真实性、有效性、完整性、防篡改性和可追溯性达成共识。由此可见,区块链技术不仅能够为拥有海量分散性医药商业资源的公共服务平台提供强鲁棒性的数据安全保障,而且还能够为同样具有去中心化特性的公共服务平台提供契合度极高的应用环境。

3)智能合约

智能合约赋予交易双方相应的权利和义务,并管理和控制区块链中交易的执行情况[16]。智能合约把交易的规则和逻辑编制成合约代码,可适用于各种程序化的规则情境。智能合约由加密算法保护,其对数据的真实性和完整性有很高的保证。也就是说,在公共服务平台上,一旦资源的需求和供给匹配成功,智能合约将促使交易自动执行,无需人为的干预和第三方监管。交易的全部过程将被记录,且记录不会被篡改。由此可见,智能合约不仅能够保证交易记录的真实性、可靠性和强制性,还能够为交易的执行提供证据,大幅提升了公共服务平台的公信力。

3 基于双链架构的医药商业资源公有区块链的设计

针对医药商业资源和公共服务平台的特点以及当前存在的共性问题,本文设计了基于用户信息链和交易链的双链医药商业资源公有区块链。该设计重点解决 3 个问题:1)公共服务平台上资源的自适应寻租和匹配问题;2)公共服务平台上数据的安全与隐私保护问题;3)区块链上节点数据的共识算法问题。

3.1 双链区块链的框架及其存储机制的设计

按照节点的记录权限对区块链进行分类,其可以分为公有链和私有链。公有链上的每个节点都有平等的读写权限,能够实现完全的去中心化,但存在由于数据量巨大而导致的共识和交易速度慢、用户信息的隐私性无法保护的问题。私有链中只有少数集权节点拥有完全的读写权利,由于记录节点较少,因此共识速度和交易速度较快,但所有节点的地位不平等,这有悖于区块链去中心化的思想。

公共服务平台若要实现资源的自适应寻租和匹配,则要求各节点必须是平等的且能够进行数据互操作。因此,作为公共服务平台的应用基础,医药商业资源区块链必须采用公有链结构。但考虑到公有区块链无法保护企业信息的隐私性,本文设计了基于“用户信息链”和“交易链”双链架构的医药商业资源公有区块链。其中,“用户信息链”用于记录和存储公共服务平台各医药商业企业的用户信息;“交易链”用于记录和存储所有的交易数据。双链结构的总体架构如图 2 所示。

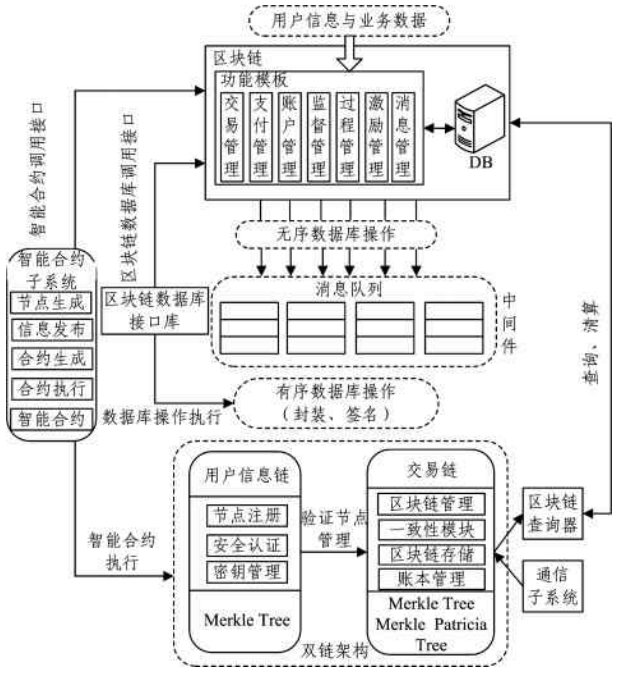

图 2 医药商业资源区块链的双链结构

Fig. 2 Double-chain structure of pharmaceutical business resources blockchain

在医药商业资源公有区块链中采用双链架构有 3 个好处:1)链上的任意节点可以在不知道企业隐私信息的情况下,查看公共服务平台上所有的资源情况,既保证了交易数据的真实性、完整性与不可篡改,同时又保证了用户信息的隐私性;2)将企业信息和交易数据进行分流,能够减少节点记录信息的冗余量,在一定程度上提高系统的吞吐率和共识速度;3)易于实现未来平台与平台、平台与金融机构之间的业务扩展。

由于医药商业资源公有区块链采用了双链架构的设计,每条链记录的内容和实现的功能均不一样,因此其存储类型和数据结构也不相同。

用户信息链主要保证参与主体个人信息的真实性、完整性和隐私性,因此仅采用 Merkle Tree 结构存储即可。Merkle Tree是 Hash List 的一种泛化,结构比较简单,具有检错功能。其唯一的 Hash 值可以满足用户信息链对数据安全的要求。

交易链主要保证交易过程的真实性、完整性和开放性,以及交易结果的真实性、完整性、开放性、可追溯性、可查阅性和可扩展性,因此本文采用 Merkle Tree 结构对交易过程数据进行记录和存储,用 Merkle Patricia Tree 结构对交易结果数据进行记录和存储。Merkle Patricia Tree 结构的实质是一种加密认证的数据结构,可以用来存储所有的(key,value)对,除了可以保证交易结果的真实性和完整性之外,还易于通过 key 值查询和追溯交易结果,为今后业务的链式扩展预留下环境友好的接口。

3.2 可扩展子链机制的设计

医药商业企业的隐私信息是使用医药商业资源区块链时

需要重视的内容,因为医药商业企业的隐私信息一旦泄露则会对其造成极大的危害。由于存储在区块链全局账本中的数据无法被删除和篡改,即使某些医药商业企业发现部分地址或者交易数据已经曝光,也无法采取挽救措施,因此医药商业资源区块链系统应该更加重视隐私问题,提高隐私防护能力[17]。

当前,区块链的应用通常是将所有的数据放置在一条单链上(如欧洲中央银行模型),链上所有的节点均能够访问这些数据。这种单链区块链结构不仅无法有效保护用户的隐私数据,而且还会因为交易量和节点的增加,引发系统的计算速度急剧下降、吞吐量变低、延迟越来越高等问题。基于此,本文设计了一种基于双链区块链架构的可扩展子链机制。该机制允许当用户数量超过一定限制后,用户信息链可被分割成多条用户信息子链,并由不同的计算机(服务器)托管。设计可扩展子链机制有两个目的:1)作为双链医药商业资源区块链的具体实现形式,进一步加强对医药商业企业隐私信息的保护;2)为医药商业资源区块链系统提供良好的扩展性、强平衡性、高计算性和低延迟性。该机制的功能和运行模式如图 3 所示。

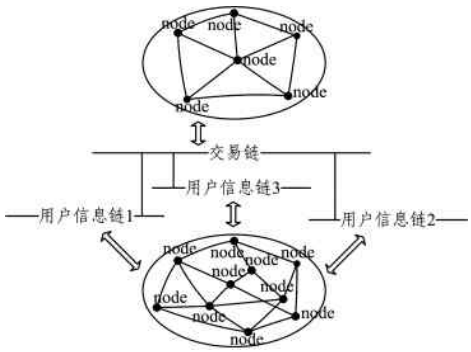

图 3　基于双链区块链架构的可扩展子链机制

Fig. 3　Extensible sub-chain mechanism based on double-chain blockchain architecture

根据可扩展子链机制,交易链仅负责创建交易区块和执行交易,是医药商业资源交易和结算的场所,不保存交易双方的用户信息。用户信息链(子链)仅负责建立到公共服务平台上注册的医药商业企业的用户账户区块和存储用户账户信息,是查询用户账户信息的场所,不执行相关交易。由于所有的医药商业企业的用户信息均由用户信息链(子链)单独存储和查询,与交易链进行了有效的隔离,且相关的用户信息仅在用户所在的用户信息子链中被共享,并被 Hash 函数保护,因此该机制能够为公共服务平台上医药商业企业的用户信息提供更高的隐私性和安全性保护。

同时,由于医药商业企业在公共服务平台上的注册数量将远远大于资源交易的数量,即用户信息链上的用户账户数量将远远超过交易链上的交易数量,因此可扩展子链机制还为医药商业资源区块链提供了良好的可扩展功能,具体如图 4 所示。

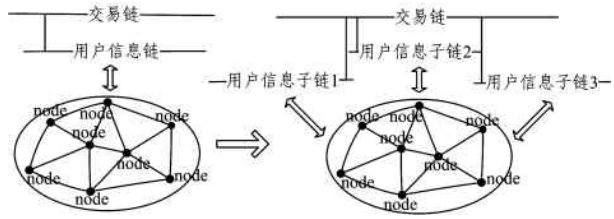

图 4　可扩展子链的工作原理

Fig. 4　Working principle of extensible sub-chain

从图 4 可以看出,由于用户账户数量巨大,原来的 1 条用户信息链被分割成为 3 条用户信息子链。而这 3 条用户信息子链都是独立的区块链,由不同的服务器支持,且每条子链上的节点都仅存储该子链上用户的信息,独立作业,相互监督,因此能够均衡系统的总负载,具有很高的吞吐量和很低的延迟[18]。

3.3　资源自适应寻租和匹配机制设计

假设在公共服务平台上存在资源需求 DU 集合和资源供给 SU 集合,则 DU 和 SU 基于双链医药商业资源公有区块链的交易过程如图 5 所示。

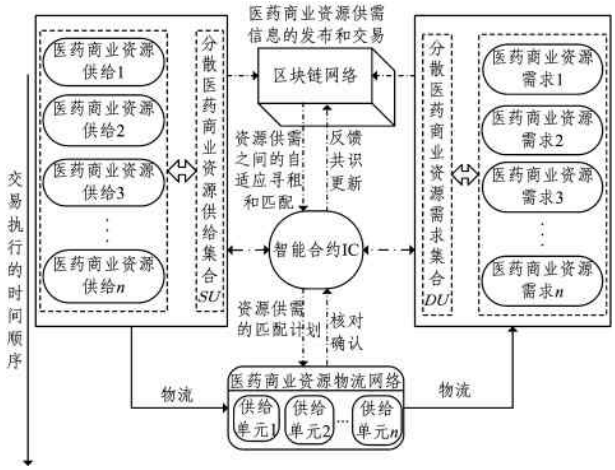

图 5　医药商业资源区块链的交易流程

Fig. 5　Transaction process of pharmaceutical business resources blockchain

在医药商业资源区块链运行的过程中,资源的自适应寻租和匹配过程设计如下。

Step1　初始化医药商业资源公有区块链(见式(1))。其中,BN 是初始化后的区块链;DU 是资源需求单元集合,SU 是资源供给单元集合,DU 和 SU 共同构成了 BN 上的节点集合;BN_{info} 和 $BN_{\text{transaction}}$ 分别是用户信息子链和交易子链;CA 是共识算法;IC 是智能合约;$T=\{t_i \in DU \times SU\}$ 为资源交易的笛卡尔集合。

$$BN=(DU,SU,BN_{\text{info}},BN_{\text{transaction}},CA,IC,T) \tag{1}$$

Step2　公共服务平台生成自己的公钥和私钥(见式(2))。

$$BN_{\text{public}}=Hash(BN_{\text{private}}) \tag{2}$$

Step3　du_i 和 su_j 分别是 DU 和 SU 中任意的资源需求点和供给点。du_i 和 su_j 为了参与交易,需要生成自己的密钥

对和地址，用于后续信息的加密和传递（见式(3)－式(6)）。

$$du_{i.\,\text{public}} = Hash(du_{i.\,\text{private}}) \tag{3}$$

$$Address_{du_i} = Hash(du_{i.\,\text{public}}) \tag{4}$$

$$su_{j.\,\text{public}} = Hash(su_{j.\,\text{private}}) \tag{5}$$

$$Address_{su_j} = Hash(su_{j.\,\text{public}}) \tag{6}$$

Step4 du_i 和 su_j 在公共服务平台上广播自己的消息（见式(7)和式(8)）。其中，$Message.du_i$ 是 du_i 发起的资源需求，E_{du_i} 是 du_i 在公共服务平台上广播的消息，E_{du_i} 内的参数依次为 du_i 的身份、资源需求量、地理位置、响应时间和激励性选择权重等。$Message.su_j$ 是 su_j 在公共服务平台上广播的消息。E_{su_j} 内的参数依次为 su_j 的身份、资源供给量、资源价格、资源类型、地理位置、响应时间和各参数的权重集合。所有节点都在网上监听其他节点的信息，并根据其他节点提供的位置生成距离矩阵 $\vec{D}$。

$$Message.du_i = (E_{du_i}(ID_{du_i}, r_i, d_i, t_i, c_i) \parallel du_{i.\,\text{public}} \parallel Address_{du_i}) \tag{7}$$

$$Message.su_j = (E_{su_j}(ID_{su_j}, s_j, p_j, g_j, d_j, t_j, W) \parallel su_{j.\,\text{public}} \parallel Address_{su_j}) \tag{8}$$

Step5 系统根据各 su_j 提供的信息内容对所有的 du_i 进行自适应的寻租和匹配，并综合权衡各方面的因素，生成总权益值最小的智能合约（见式(9)）。其中，$\sum_{i=1}^{n} p_j.Q_C.\vec{D}.T_c.W$ 表示资源的价格、最终供给量、距离、最终响应时间与相应权重乘积的累加和。该智能合约用公共服务平台的私钥加密。

$$IC = \min\left(\sum_{i=1}^{n} p_j.Q_C.\overrightarrow{D_{ij}}.T_c.W\right)_{BN_{\text{private}}} \tag{9}$$

Step6 按照智能合约，为 du_i 提供服务的 su_j 首先到 $Address_{du_i}$ 上寻找 du_i 的公钥，并和 du_i 自己提供的 $du_{i.\,\text{public}}$ 进行比对，以验证 du_i 的身份。如果身份确认，则 su_j 向 du_i 回传消息 $p_{\text{respond}}.su_j$（见式(10)）。该消息用 du_i 的公钥加密。其中，C_{ij} 是 su_j 为 du_i 提供资源的具体内容，$Sign.su_j$ 是用 su_j 的私钥加密的数字签名。

$$p_{\text{respond}}.su_j = (C_{ij}(ID_{du_i}, ID_{su_j}, Q_C, p_j, g_j, d_{ij}, t_j, W) \parallel Sign.su_{j.\,su_{j.\,\text{private}}} \parallel Address_{su_j})_{du_{i.\,\text{public}}} \tag{10}$$

Step7 du_i 在收到消息后，首先用自己的私钥解密，得知是 su_j 反馈的消息。通过 su_j 提供的地址 $Address_{su_j}$ 找到 su_j 的公钥，解密 su_j 的数字签名，确认 su_j 的身份。其次，du_i 查看信息内容 C_{ij}，如果没有异议，则生成合约脚本（见式(11)）。其中，N_{version} 为交易的序列号，N_{time} 为交易达成的时间。由于交易成功后，公共服务平台要向所有节点广播该合约信息，并更新区块链中的信息，完成新一轮的共识，因此合同脚本需要 du_i、su_j 和公共服务平台三方共同的数字签名。

$$Script = [N_{\text{version}} \parallel N_{\text{time}} \parallel Sign.du_i.Sign.su_j.Sign.BN(C_{ij})] \tag{11}$$

Step8 在医药商业资源供需交易达成后，各资源供给节点 su_j 按照合约向需求节点 du_i 进行实际的医药产品的物流配送。同时，区块链和实际的医药商业资源物流网络不断交互信息，对交易的执行情况进行记录、确认、审核和监督，以确保交易顺利地完成[19]。在这个过程中，交易过程和交易结果的信息将记录到区块链中，并在所有节点中即时共识和更新。

Step9 若 du_i 和 su_j 在交易过程中违约，公共服务平台可以根据约定给予它们相应的惩罚。假设 du_i 违约，式(12)表示对 du_i 给予在资金和信誉方面的惩罚。其中，M 为 du_i 需要在此次交易中付出的资源报酬；C 为 du_i 当前的信誉；W_n 是 du_i 违约条款的权重系数，可根据不同的违约情况设置不同的数值。该信息被公共服务平台的私钥加密并广播。

$$Punish.du_i = [(M \parallel C)W_n]_{BN_{\text{private}}} \tag{12}$$

3.4 共识算法的设计

区块链没有中心化的记账机构，因此区块链从建立到每一次的数据更新和存储都需要利用共识算法完成一次所有节点的“一致性过程”。共识算法是区块链的核心技术，是区块链建立公信力的重要保障。公有区块链由于参与节点众多且其可靠性不高，信息量巨大，因此一般采用工作量证明（PoW）、权益证明（PoS）和授权股份证明（DPoS）等共识算法。

PoS 共识算法的思想是采用权益证明代替基于 SHA256 问题的 Hash 算力（矿工），即由区块链中拥有最高权益的节点获取区块的记账权。相比 PoW 需要大量的算力，PoS 仅需要少量的计算时间和能力就能保证区块链的正常运转[20]。考虑到公有区块链共识速度慢，以及在对医药商业资源调度的过程中要通过选择性激励权重引导医药商业资源向偏远和不发达地区流动，以实现医药商业资源的公益性属性，本文基于 PoS 共识算法，提出一种考虑权重、更简洁和更适用于医药商业资源区块链的共识算法。该算法的伪代码如算法 1 所示。

算法 1

```
1. Begin
2. transaction X (ID,request,t);
    /* 节点 X 产生了新的交易，要求更新，t 为时间戳，保证该要求只会提出一次 */
3. listen by every node;
    /* 所有节点保持监听 */
4. broadcast by every node (ID,R);
    /* 各节点向全网广播自己的信息 R */
5. Weight=comp(∑(i=1..n) Ri · Wi) for every node;
    /* 每个节点根据事先约定的权重，计算所有节点的权益值 weight */
6. primary =Max(Weight);
    /* 根据最高的权益值，选出记账节点 */
7. block=comp(X) by primary;
    /* 记账节点计算节点 X 的区块值 */
8. MS=broadcast(block) by primary;
    /* 记账节点向全网广播节点 X 的区块值 */
9. if MS is received
    /* 如果节点收到了消息 */
10. No. =count(MS);
    /* 记录节点收到信息的数量 */
11. if the No. >=N for any node
    /* 如果任意节点收到的信息数量超过 N 个以上，N 与系统容错数有关 */
12.   then updating for every node (X,block);
    /* 所有节点更新节点 X 的新区块值 */
13. else give up;
    /* 否则，放弃更新 */
14. End
```

4　仿真实验

4.1　参数说明

为了验证双链区块链技术在基于公共服务平台的医药商业资源调度上的适用性和优越性，本文设计了 3 组实验方案，使用 Matlab 构建了相应的调度仿真模型，并对实验结果进行了分析和讨论。

对仿真模型做以下几点假设和说明：

1）存在一个医药商业资源需求节点集合，具体参数如表 1 所列；存在一个医药商业资源供给节点集合，具体参数如表 2 所列，参数权重如表 3 所列，医药商业资源类型权重如表 4 所列。

表 1　需求节点和需求量

Table 1　Demand nodes and demanded quantity

unit	需求量	响应速度	选择性激励权重
du_1	740	≤0.8	0.2
du_2	270	≤0.7	1.0

表 2　供给节点和供给量

Table 2　Supply nodes and supplied quantity

unit	供给量	供给价格	响应速度	资源类型	距离 du_1	距离 du_2
su_1	10000	2.3	0.9	冷链专列	1300	180
su_2	200	5.5	0.6	厢式多温区冷链车	1800	240
su_3	300	4.6	0.7	厢式单温区冷链车	1200	80
su_4	1150	6.5	0.8	甩挂＋冷链集装箱	1900	120
su_5	70	5.3	0.8	厢式多温区冷链车	1100	340
su_6	100	15.8	0.5	冷链航空专线	1700	550
su_7	400	2.5	0.7	普通厢式车＋冷链箱	900	680
su_8	300	4.2	0.7	厢式单温区冷链车	2100	350
su_9	60	5.2	0.6	厢式单温区冷链车	1900	200
su_{10}	80	6.1	0.8	甩挂＋冷链集装箱	1500	400

表 3　参数的权重

Table 3　Weights of parameters

参数属性	权重参考值
量	0.5
价格	0.2
距离	0.5（d_{ij}≤100） 0.6（100<d_{ij}≤300） 0.7（300≤d_{ij}≤500） 0.8（d_{ij}>500）
响应速度	0.6
资源类型	0.7

表 4　资源类型的权重

Table 4　Weights of resource types

资源类型	权重参考值
冷链专列	0.4
厢式多温区冷链车	0.7
厢式单温区冷链车	0.6
甩挂＋冷链集装箱	0.5
普通厢式车＋冷链箱	0.8
冷链航空专线	0.9

2）所有资源类型对需求点可达。

3）对所有参数的权重做归一化处理。

4）为了突出研究对象的典型性，对于表 1 中的两个需求节点，将其中一个设置在中心城市，另一个设置在偏远地区。

5）所有节点均在 BN 上，并按照 BN 的规则和算法完成医药商业资源供需之间的寻租、匹配和交易。

4.2　3 组仿真实验

实验 1　计算表 1 和表 2 中的医药商业资源供需节点在区块链技术下自适应寻租和匹配的结果，目的是验证区块链技术对分散性资源进行调度和管理的可行性和适用性。实验 1 的仿真结果如表 5 所列。

表 5　医药商业资源供需节点的自适应寻租与匹配结果

Table 5　Self-adaptive rent-seeking and matching results of pharmaceutical business resource supply and demand nodes

需求节点	选择的供给节点	供给量
du_1	su_7	400
	su_3	30
	su_5	70
	su_{10}	80
	su_9	60
	su_8	100
du_2	su_3	270

实验 2　在资源供应一定的前提下，计算基于传统资源调度模式和基于区块链技术调度的需求节点的平均最优成本，目的是验证通过区块链技术对分散性资源进行调度，在系统成本方面获得的优越性。实验 2 的仿真结果如图 6 所示。

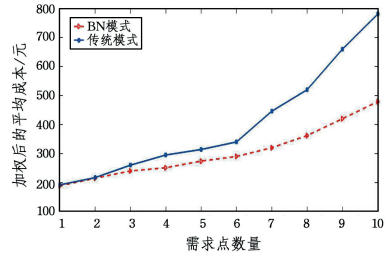

图 6　不同模式下需求节点的平均最优成本

Fig. 6　The average optimal costs of demand nodes under different modes

由于传统资源调度模式没有对参数的权重进行设置，因此为了让不同调度模式下的成本具有可比性，实验 2 只考虑节点的需求量、供给量、供给价格、供需节点的位置和最终交易量，不考虑参数对应的权重。其中，资源供给节点和供给量从表 2 提取；需求节点的规模从 1 逐步扩大到 10，需求量通过随机函数在[1,500]区间内产生；节点之间的距离矩阵通过随机函数在[50,2000]区间内产生。根据文献[21]中集合覆盖模型的思想，基于传统模式的需求节点权益成本的计算公式如式(13)－式(16)所示。式(13)表示需求节点的最优平均成本是价格、供需节点之间的距离、需求量和权重之积的最小累加和的平均值；式(14)表示每个需求点被至少 1 个、最多 3 个供给点覆盖。

$$\min \sum_{i=1}^{n}(P_j.\overrightarrow{d_{ij}}.Q_C)/n \tag{13}$$

$$\text{s.t. } 1\leqslant\sum_j c_{ij}du_i\leqslant 3,\forall j\in J \tag{14}$$

$$du_i=1,\forall i\in I \tag{15}$$

$$c_{ij}=\begin{cases}1, & \text{if } su_j \text{ cover } du_i\\ 0, & \text{if } su_j \text{ not cover } du_i\end{cases} \tag{16}$$

实验 3　比较单链区块链与双链区块链的特性和计算能

力，目的是验证双链区块链在用户信息的隐私保护和平衡计算负载方面的优越性。实验 3 的仿真结果如表 6 所列。

表 6 单链区块链和双链区块链的计算比较

Table 6 Comparison of computing between single-chain blockchain and double-chain blockchain

	单链区块链	用户信息链	交易链
参数特性	1 条链； 链上共有 100 个节点	10 条子链； 每条子链共有 10 个节点	1 条链； 每条链共有活动节点(即参与交易)10 个， 不参与交易的节点不参与计算
创建区块计算次数/node. s	$4*100*100=4*10^4$	$4*10*10=400$	$4*10*10=400$
创建区块的加密次数/ node. s	$4*40000=1.6*10^5$	$4*400=1600$	$4*400=1600$
交易查询计算次数/node. s	$10^5/(4*60*60)=6.94$	$10^5*4/(10*4*60*60)=2.78$ 注：设每次交易均有 4 个参与者	$10^5*4*10/(100*4*60*60)=2.76$ 注：设每次交易均有 4 个参与者
交易加密计算次数/node. s	$4*6.94=27.76$	$4*2.78=11.12$	$4*5.55=22.20$
运行模式	单链运行	多条用户信息链并行运行，同时可以和交易链并行运行	单链运行
隐私性	无或低	高	高

实验中假设：每个节点对每个信息的确认需要 4 次通信(签名、解签名、加密和解加密)；每天区块链工作 4 小时；每天区块链上共有 10^5 次交易量。

4.3 对实验结果的分析与讨论

1)从实验 1 的结果可以看出，在仅有 10 个资源供应节点的前提下，有 6 个资源供应节点共同满足了 du_1 的需求，有 1 个资源供应节点满足了 du_2 的需求。在选中的 7 个资源供应节点中，有 3 个是供应量不足 100 的小体量资源供应点(模型中一共只有 4 个小体量资源供应点)。这充分说明区块链技术能够让分散性的医药商业资源完成自适应性的寻租和匹配，能够让资源的调度仅与资源自身的能力和交易规则相关，与资源所有者和资源所有者掌握的信息无关，从而能够让更多的小体量医药商业资源进入市场并公平地参与交易。这与传统模式下资源的调度和管理有本质的区别。

2)在资源需求上设置选择性激励权重的目的是鼓励医药商业资源自发地向偏远和不发达的地区流动，实现医药商业资源的公益性属性。通过计算可知，实验 1 中 10 个资源供应节点对需求节点 du_1 和 du_2 的覆盖顺序依次是：$su_3(du_2)-su_7(du_1)-su_9(du_2)-su_2(du_2)-su_3(du_1)-su_8(du_2)-su_5(du_1)-su_{10}(du_1)-su_9(du_1)-su_8(du_1)-su_2(du_1)-su_{10}(du_2)-su_7(du_2)-su_4(du_1)-su_6(du_1)-su_6(du_2)$。从这个顺序可以看出，两个地理位置不同的需求节点在被供应节点覆盖时，没有明显的先后次序，符合系统的既定目标。多次实验证明，选择性激励权重与节点规模、距离矩阵和响应速度这 3 个参数强相关。

3)从实验 2 的结果可以看出，在资源供应一定的前提下，随着需求节点的增多，基于传统资源调度模式的需求节点的平均成本显著上升，其成本的增长率也显著放大。这是因为：第一，传统资源调度模式存在信息壁垒，交易成本很高。虽然资源供需双方的交易存在一定的偶然性和随机性，但总体来说比较固定，资源的碎片率很高。第二，在利益的驱动下，优势资源会先满足成本更低的需求节点，而成本较高的偏远和不发达地区的需求节点往往到最后才会被更为劣势的资源覆盖，从而提高了需求节点的平均成本。但在区块链技术下，资源信息是透明的，一个需求节点可以被若干个供应节点同时覆盖，供应节点的“碎片化资源”非常少，交易成本可以低到忽略不计。这使得需求节点的平均成本及其增长率明显低于传统模式，而且这一成本优势在海量资源环境下将体现得更加明显。

4)由实验 3 的结果可知，在相同的用户和交易数量的前提下，双链区块链每节点在每秒内的区块创建和加密次数与交易查询和交易加密次数均远远少于单链区块链。而且当交易链上的参与用户和交易量海量增长时，由于双链区块链具有良好的可扩展性，因此交易链也可以像用户信息链一样被分割成若干子链，实现并行处理，从而降低每条交易子链上的计算次数。由此可见，双链区块链不仅可以保证用户信息的隐私性，而且还可以平衡节点负载，大幅度提高区块创建和交易查询的速度。

结束语 在“互联网+”和分布式计算背景下，医药商业资源的特性和调度模式发生了巨大的变化。本文针对基于公共服务平台的医药商业资源分布式调度模式中存在的关键技术问题，提出了双链架构的医药商业资源区块链。研究结果表明，基于双链架构的医药商业资源区块链能够为公共服务平台提供自适应性的资源寻租和匹配机制，能够同时保障交易信息的透明性、安全性和企业信息的隐私性，能够大幅提高公共服务平台的公信力和系统的整体效率，是公共服务平台的核心技术支撑和友好的应用环境。

以下几方面需要深入研究：第一，公共服务平台上的节点和资源具有海量特征，这对共识算法的速度和效率提出了要求。本文设计的基于 PoS 的共识算法虽然考虑了参数的权重，但在算法的速度和效率方面还有待改进。第二，本文设计的仿真实验环境比较理想，有很多现实情况尚未考虑，比如冷藏车辆的碳排放和折旧问题等。第三，选择性激励机制是实现医药商业资源公益性属性的关键，选择性激励策略的实施对象、规则、方式和强度等应该如何设置才不会触发企业的策略性选择行为也需进一步研究。

参 考 文 献

[1] YIN C, HUANG B Q, LIU F. Common key technology system of cloud manufacturing service platform for small and medium enterprises [J]. Computer Integrated Manufacturing Systems, 2011, 17(3): 495-503. (in Chinese)

尹超,黄必清,刘飞. 中小企业云制造服务平台共性关键技术体系[J]. 计算机集成制造系统,2011,17(3):495-503.

[2] REN L,ZHANG L,ZHANG Y B,et al. Resource virtualization in cloud manufacturing [J]. Computer Integrated Manufacturing Systems,2011,17(3):511-518. (in Chinese)
任磊,张霖,张雅彬,等. 云制造资源虚拟化研究题[J]. 计算机集成制造系统,2011,17(3):511-518.

[3] DU A Y,DAS S,RAMESH R. Efficient risk hedging by dynamic forward pricing: a study in cloud computing [J]. Informs Journal on Computing,2013,25(4):625-642.

[4] LI W F,ZHONG Y,WANG X,et al. Resource virtualization and service selection in cloud logistics [J]. Journal of Network and Computer Applications,2013,36(6):1696-1704.

[5] LI B H,ZHANG L,REN L,et al. Further discussion on cloud manufacturing [J]. Journal of Network and Computer Applications,2011,17(3):449-457. (in Chinese)
李伯虎,张霖,任磊,等. 再论云制造[J]. 计算机集成制造系统,2011,17(3):449-457.

[6] CHANG V,WALTERS R J,WILLS G. The development that leads to the Cloud Computing Business Framework [J]. International Journal of Information Management,2013,33(3):524-538.

[7] XU X L,LI W D. Research on public service model of push type based on cloud computing [J]. Research of Administration Science,2014,1(2):36-39. (in Chinese)
徐晓林,李卫东. 基于云计算的推送式公共服务模式研究[J]. 行政科学坛,2014,1(2):36-39.

[8] WANG S L,SONG W Y,KANG L,et al. Manufacturing resource allocation based on cloud manufacturing [J]. Computer Intergrated Manufacturing Systems,2012,18(7):1396-1405. (in Chinese)
王时龙,宋文艳,康玲,等. 云制造环境下的制造资源优化配置研究[J]. 计算机集成制造系统,2012,18(7):1396-1405.

[9] BI Y,ZHANG S H . Research on resource integration decision problem in cloud mode based on the view of open cooperation and innovation [J]. Logistics Engineering and Management,2014,36(9):100-102. (in Chinese)
毕娅,张曙红. 开放合作创新视角下基于云模式的物流资源一体化集成决策研究[J]. 物流工程与管理,2014,36(9):100-102.

[10] MARIAN M,TEO Y M. Dynamic Resource Pricing on Federated Clouds[C]// 10th IEEE/ACM International Conference on Cluster,Cloud and Grid Computing. 2010:513-517.

[11] LIN A,CHEN N C. Cloud computing as an innovation:Percepetion,attitude,and adoption [J]. International Journal of Information Management,2012,3(6):533-540.

[12] YUAN Y,WANG F Y . Blockchain:The State of the Art and Future Trends [J]. Acta Automatic Sinica,2016,42(4):481-494. (in Chinese)
袁勇,王飞跃. 区块链技术发展现状与展望[J]. 自动化学报,2016,42(4):481-494.

[13] SWS Research. Block chaining technology:disruptive innovation-Block chain and digital currency series report (two)[R]. Shanghai:SWS Research,2016:1-35. (in Chinese)
申万宏源研究所. 区块链:颠覆式创新-区块链和数字货币系列报告之二[R]. 上海:申万宏源研究所,2016:1-35.

[14] China Blockchain Technology and Industrial Development Forum. Chinese block chain technology and application development white paper(2016)[R]. China Blockchain Technology and Industrial Development Forum,2016:1-65. (in Chinese)
中国区块链技术和产业发展论坛. 中国区块链技术和应用发展白皮书(2016)[R]. 中国区块链技术和产业发展论坛,2016:1-65.

[15] HUCKLE S,BHATTACHARYA R,WHITE M,et al. Internet of things,blockchain and shared economy applications [J]. Procedia Computer Science,2016,98:461-466.

[16] KOSBA A,MILLER A,SHI E,et al. Hawk:the blockchain model of cryptography and privacy-preserving smart contracts [C]// Proceedings of 2016 IEEE Symposium on Security and Privacy(SP). San Jose,USA:IEEE,2016:839-858.

[17] ZHU L H,GAO F,SHEN M,et al. Survey on Privacy Preserving Techniques for BlockchainTechnology [J]. Journal of Computer Research and Development,2017,54(10):2170-2186. (in Chinese)
祝烈煌,高峰,沈蒙,等. 区块链隐私保护研究综述[J]. 计算机研究与发展,2017,54(10):2170-2186.

[18] CAI W D,YU L,WANG R,et al. Blockchain Application Development Techniques[J]. Journal of Software,2017,28(6):1474-1487. (in Chinese)
蔡维德,郁莲,王荣,等. 基于区块链的应用系统开发方法研究[J]. 软件学报,2017,28(6):1474-1487.

[19] SHE W,HU Y,YANG X Y,et al. Virtual power plant operation and scheduling model based on energy blockchain network [J]. Chinese Society for Electrical Engineering,2017,37(13):3729-3736. (in Chinese)
余维,胡跃,杨晓宇,等. 基于能源区块链网络的虚拟电厂运行与调度模型[J]. 中国电机工程学报,2017,37(13):3729-3736.

[20] HE P,YU G,ZHANG Y F,et al. Survey on Blockchain Technology and Its Application Prospect [J]. Computer Science,2017,44(4):1-7,15. (in Chinese)
何蒲,于戈,张岩峰,等. 区块链技术与应用前瞻综述[J]. 计算机科学,2017,44(4):1-7,15.

[21] BI Y. The location-allocation problem research in cloud logistics based on collaborative inventory and covering [D]. Wuhan:Wuhan University of Technology,2012. (in Chinese)
毕娅. 云物流下基于协同库存和覆盖的选址-分配研究[D]. 武汉:武汉理工大学,2012.