STBM：安全可信的基于区块链的网络安全服务交易模型

朴桂荣，朱建明
（中央财经大学信息学院，北京 102206）

摘　要：为了应对传统网络安全服务交易模型面临的众多挑战，适应产业数字化发展的需求，克服网络安全服务交易不方便、不透明的困难，提出了一种安全可信的基于区块链的网络安全服务交易模型，为网络安全服务提供安全、高效和可控的交易方式。通过网络安全服务的分类和全生命周期管理，引入双链结构和智能合约，旨在提高网络安全服务的可追溯性、透明性和安全性。首先，对网络安全服务进行多维度的分类，包括使用权、许可权、控制权和所有权，有助于更清晰地理解和有效地管理这些服务。进一步，构建服务链，以实现网络安全服务的全生命周期管理，包括创建、发布、配置、运行、维护、更新和结束等关键阶段，从而提高网络安全服务的可追溯性和透明性。此外，构建交易链用于自动化的服务交易，形成先服务后支付模式，确保交易的安全性和完整性。最后，通过实例与实验验证了这些组件在网络安全服务交易中的有效性和可信性。

关键词：网络安全服务；区块链；双链；交易模型；全生命周期管理
中图分类号：TN39
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2024158

STBM: secure and trustworthy blockchain-based model for cybersecurity service transactions

PIAO Guirong, ZHU Jianming
School of Information, Central University of Finance and Economics, Beijing 102206, China

Abstract: To overcome the numerous challenges faced by traditional models of cybersecurity service transactions, adapt to the needs of industrial digitalization, and address the inconveniences and opacity of cybersecurity service transactions, a secure and trustworthy blockchain-based model for cybersecurity service transactions was proposed, which could provide a secure, efficient, and controllable means of transaction for cybersecurity services. By categorizing cybersecurity services and managing the full lifecycle, and incorporating a dual-chain structure and smart contracts, the model sought to enhance the traceability, transparency, and security of cybersecurity services. Firstly, cybersecurity services were categorized into multiple dimensions, including usage rights, licensing rights, control rights, and ownership rights, to aid in clearer understanding and effective management of these services. Furthermore, a service chain was constructed for the full lifecycle management of cybersecurity services, covering key stages such as creation, publication, configuration, operation, maintenance, updating, and termination, thereby improving cybersecurity service traceability and transparency. In addition, a transaction chain was established for automated service transactions, adopting a post-service payment model to ensure the security and integrity of transactions. Finally, the effectiveness and trustworthiness of these components in cybersecurity service transactions were validated through case studies and experiments.

Keywords: cybersecurity service, blockchain, dual-chain, transaction model, full lifecycle management

收稿日期：2024–04–10；**修回日期：**2024–08–17
通信作者：朱建明，zjm@cufe.edu.cn
基金项目：国家自然科学基金资助项目（No.62372493）
Foundation Item：The National Natural Science Foundation of China (No.62372493)

0　引言

随着信息技术的高速发展和数字化转型的推进，网络安全领域面临的挑战也变得日益严峻[1-2]，网络黑客、数据泄露、恶意软件等形式多样的网络安全威胁层出不穷。全球性的网络攻击事件，如WannaCry 和 NotPetya 勒索软件的肆虐，不仅对用户造成了巨大的经济损失，也严重干扰了企业的正常运营。网络安全威胁的形式从传统的病毒和恶意软件演变为复杂的勒索软件和高级持续性威胁，展现出了多样化和不断演变的特点，这要求用户必须采取更加全面和多层次的防御策略[3-5]。与此同时，这些网络安全威胁的隐蔽性和持久性进一步凸显了用户采取主动和有效网络安全措施的紧迫性。高度专业化的网络安全威胁要求用户与专业网络安全服务提供商之间紧密合作，以构建更加坚固和全面的网络安全防护体系[6-7]。

《关于开展网络安全服务认证工作的实施意见》（国市监认证规〔2023〕3 号），由国家市场监管总局、中央网信办、工业和信息化部、公安部于 2023 年 3 月 15 日共同发布，标志着对网络安全服务市场的规范化管理和对服务提供商的监督指导进入了新阶段。在当前的网络安全服务领域，用户需求展现出了高度的多样性与个性化趋势。然而，现有的服务交易模式常受限于较高的交易成本和有限的适应性，导致其难以充分满足用户需求的多元性与特异性。特别是在服务交易渠道建设方面，缺少一套既低成本又高度可信的交易机制，这一局限性降低了服务供给与需求之间对接的效率，进而影响了网络安全服务市场的稳定发展。在这一背景下，如何构建一个可靠、高效且安全的服务交易模型成了一个亟待解决的问题[8-9]。

现有的网络安全服务交易模式主要有以下 2 种。第一种是直接在网络安全服务提供商的官方网站上购买网络安全服务，这种模式的优势在于可以保证服务的原生性和正版性。然而，该模式对服务提供商的可信程度有较高要求，因此对中小企业的服务提供商不友好。此外，由于签订合同和审批流程涉及合规要求，需要相关部门进行多次审核和批准，增加了时间成本，无法满足用户及时部署安全措施的需求。购买的过程相对不够透明，用户难以准确地了解服务的可行性和价格的合理性，导致用户的网络安全防护能力难以得到有效保障，需要投入更多的信息成本[10]。第二种是通过第三方平台购买网络安全服务，这种模式的优势在于第三方平台提供了大量的服务提供商，用户可以根据价格、服务介绍、用户评价等因素进行选择。但第三方平台的加入增加了交易成本[11-12]。总体而言，当前网络安全服务市场信息较为分散，用户需要花费大量时间成本搜集和比较各服务提供商的服务和价格，增加了选择供应商的难度和信息成本。同时，交易过程烦琐且缺少透明度，影响了网络安全防护的效率，增加了交易成本。

当前针对网络安全服务交易模型的研究处于起步阶段。在金融、医疗、制造等行业，由于其数据和系统具有高价值和高敏感性，容易受到复杂的网络威胁，因此对网络安全服务过程提出了更高的要求。缺乏有效的交易模型可能导致交易过程不稳定、效率低和缺乏保障，进而限制了网络安全服务市场的发展和服务潜力的增长。近年来，区块链技术因其去中心化、可追溯性、透明性等特点受到广泛关注[13-14]。区块链作为一种分布式账本技术，通过去中心化的共识机制确保交易的透明性和安全性，为传统网络交易过程中的信任问题提供了新的解决方案[15-17]。尤其在金融行业，区块链技术已经被广泛应用于交易结算、跨境支付等领域，取得了显著成果[18-21]。

此外，许多研究人员将区块链技术应用于网络安全领域。陈迪等[22]主要对区块链在域间路由安全的应用进行介绍。陈烨等[23]介绍了区块链在网络数据安全和隐私保护、物联网设备的权限管理和分布式拒绝服务（DDoS, distributed denial of service）防御 3 个方面的应用。Salman 等[24]对基于区块链的网络安全服务进行介绍，其中只涉及公钥基础设施（KPI, public key infrastructure）、数据隐私和溯源 3 个方面。现有的研究主要关注的是采用区块链技术的特性解决网络安全服务问题[25-26]，本文利用区块链技术为网络安全服务提供可靠交易支撑。网络安全服务是一系列旨在减轻、检测和应对网络安全威胁的专业服务[27]。本文基于网络安全服务的特性，总结了以下 3 个关键挑战。

1) 网络安全服务的高度专业性，容易造成服务提供商与用户之间的信息不对称。从网络安全服务客体来看，主要是非物质性保护，即数字化资产，如数据、信息、应用程序和网络资源。网络安

全服务提供商采用一系列技术手段，如加密、访问控制、认证等，以确保数字化资产在数字环境中的安全性[28-30]。实施和维护这些技术需要高度专业的技术知识和经验。这导致用户难以准确评估网络安全服务的质量和适用性，也无法确定服务提供商是否真正符合其需求。此外，用户在使用服务之前难以准确预测服务的实际效果，因为安全事件可能在未来发生，且结果难以预测。这使得用户很难评估服务提供商的能力和服务的实际效益。特别是在网络安全软件服务中，通常采用订阅模型，该模型涉及用户以预付费的方式获取特定服务的连续访问权限或权益，而不是根据实际使用情况进行计费[31]。

2) 网络安全服务是一种多方持续协作的模式，具有较长的服务周期和难以追溯的特点。从网络安全服务过程来看，该服务是一项连续性的任务，需要不断监控、评估和更新，以应对不断演变的威胁和攻击，强调持续监测和响应[32]。由于网络安全威胁的复杂性和多样性，保障网络安全需要不断地更新和改进，以适应不断演变的威胁环境。另外，网络安全服务具有定制化的特点。不同组织之间存在不同的网络安全威胁和风险，这受行业、规模和业务需求的影响[33-34]。因此，网络安全服务提供商需要根据用户的具体情况提供个性化的解决方案，以确保最大程度的保护。与一次性产品交付不同，网络安全服务专注于建立长期合作的关系，以便于协同制定灵活的防御策略。这有助于确保防御策略能够与不断演变的威胁环境保持同步，从而持续地保护用户的数字化资产，使其免受各种威胁的侵害。但这种服务通常难以追溯和量化，且服务过程无法直接观测，服务信息无法被有效记录、监测和追溯。

3) 网络安全服务交易模型面临多重挑战，如信息分散、交易烦琐、信任成本高、价格不透明等，可能会阻碍网络安全服务的有效价值交换。特别是在隐私性和保密性方面，因为用户的安全事件和漏洞可能涉及商业机密、知识产权等敏感信息，泄露安全漏洞将会对用户的利益和声誉造成严重损害。因此，信任是确保网络安全服务过程的重要前提，网络安全服务提供商需要具备高度的信誉度和可靠性，以满足金融、医疗、制造等行业对安全性和数据保护的严格要求。

为此，本文提出了一种安全可信的基于区块链的网络安全服务交易模型，命名为STBM（secure and trustworthy blockchain-based model），优化网络安全服务的交易模式，提升服务过程的安全性，确保交易的透明性和可信性。首先，设计了一种基于区块链的全生命周期管理框架，用于跟踪服务提供商在创建和运营阶段关键安全服务的执行情况。其次，利用区块链技术的透明性和不可篡改性构建了一个分布式交易市场，设计了一种先服务后支付模式，降低用户的初期投资风险并鼓励服务提供商提供更高质量的服务。区块链生成的唯一凭证可追溯整个服务过程，增加了交易的透明性和可信性。此外，智能合约的自动化触发机制提高了服务的效率和可靠性。最后，区块链确保了整个交易过程的可信性以及交易后信息的安全存储，也为服务质量评估提供了可信的数据来源。本文主要的研究工作如下。

1) 提出了网络安全服务的全生命周期管理模型，对网络安全服务进行了多维度的分类，包括使用权、许可权、控制权和所有权，有助于更清晰地理解和有效地管理这些服务。此外，通过引入区块链技术，实现了网络安全服务的全生命周期管理，包括创建、发布、配置、运行、维护、更新和结束等关键阶段，提高了服务的可追溯性和透明性。

2) 提出了双链结构的网络安全服务交易模型，构建的双链结构，包括服务链和交易链。服务链用于网络安全服务的全生命周期管理，而交易链用于支撑自动化的分布式网络安全服务交易，形成先服务后支付模式，降低交易成本与信息成本，确保交易的安全性和完整性。

3) 设计了智能合约并进行了实验验证，研究中设计了4个关键的智能合约，包括服务管理合约、服务评估合约、服务匹配合约和服务交易合约，用于管理、评估、匹配和执行网络安全服务交易。这些智能合约实现了网络安全服务交易的有效性和可信度。

1 相关文献

区块链技术运用密码学、智能合约、共识算法等技术，促进了分布式的可信数据和价值交换机制的实现[35]。该技术的应用范围已经从最初的金融领域拓展至科技服务、知识产权保护、能源交易等多个领域，为这些领域中存在的安全性、透明度与交易效率问题提供了创新性的解决方案。

在科技服务领域，陈冬林等[36]针对科技服务的高产权特性与隐私脆弱性，设计了基于区块链的科技服务交易零知识验证方案，增强了去中心化服务交易的保密性。张垺豪等[37]构建了基于区块链的科技服务交易信任模型，通过区块链技术保证服务质量评估参数以及服务信息的可信性，由此作为服务质量评估的依据。王晟典等[31]针对软件服务提出了一种基于区块链智能合约的服务交易方法，解决软件即服务所依赖的订阅模式面临软件服务金融化和法律化的挑战。通过实例验证了区块链在服务交易中的合理性与有效性。李妃养等[38]讨论了区块链技术在交易中的应用，指出区块链在消除交易双方信息不对称并促进技术成果交易方面具有优势。区块链技术与科技服务的融合在减少传统中心化平台弊端、实现科技服务可信管理等方面展现出良好的应用前景。

在知识产权保护领域，Hu 等[39]指出传统专利交易模式面临着专利追溯性与安全性挑战，为此构建了一个区块链环境来模拟专利注册和交易过程，旨在提高信息的安全性、不可变性、透明性和可追溯性。Zhuang 等[40]针对知识产权争端时需要追踪用户身份信息的问题，提出了基于区块链的隐私保护和可追溯的知识产权身份管理方案，以确保用户身份信息的安全性和可追溯性。李向阳等[41]提出了异步需求收集和权益人变更方案，通过智能合约实现交易撮合与多方收益分配，提高了在线交易的成功率。区块链技术可以跟踪知识产权的历史交易记录，包括所有权转移情况和许可情况。这有助于确保知识产权的可追溯性和合规性。

在其他领域的基于区块链的交易模型中，黄华梅等[42]针对家政服务领域构建了去中心化的服务交易智能合约区块链模型。该模型将交易信息和合约信息存储在区块链上，确保交易的安全性，并通过粒子群算法进行交易匹配，提高了交易的智能化水平。Liu 等[9]指出了传统网络安全交易平台受不诚实买家和中介的影响，交易服务受到众多限制。为此，提出了一种基于区块链的服务交易生态系统，通过智能合约确保在不需要可信第三方的情况下实现多方间的安全一致性。Yahaya 等[43]提出了基于区块链的能源交易模型，用于管理和监督交易过程。在该模型中，提出了基于能源信誉度生成和消费的共识机制，以解决现有共识机制所带来的高计算成本和巨大货币投资问题。Liu 等[44]针对电力数据设计了基于区块链的交易模型，以解决传统基于 Web 页面的电力数据交易中存在的隐私保护、交易安全、数据可靠性等问题。

尽管现有文献在上述领域取得了一定进展，但对于网络安全服务交易的研究尚且有限，特别是在如何系统化和透明化网络安全服务过程方面。区块链与服务交易方面的研究现状忽视了服务交易需求的异质性、交易匹配机制以及在分布式环境下确保服务质量的策略等关键问题。此外，关于如何利用区块链技术优化网络安全服务管理、提升服务安全性、确保交易透明性和可信性的研究也不足。鉴于此，本文构建了一个基于区块链的网络安全服务交易全生命周期管理框架和双链结构交易模型，将技术、专利、知识产权、软件等要素视为网络安全服务的关键组成部分，旨在优化网络安全服务管理流程、提升服务交易的安全性、确保交易的透明性和可信性。此外，本文进一步探讨将区块链技术与网络安全服务交易过程融合的方法，以期在提高网络安全领域的效能和可信性方面取得突破。

2　系统模型

为提升网络安全服务交易的安全性与效率，确保服务提供商与用户之间的紧密互联，本文提出了一种基于区块链的网络安全服务交易模型，如图 1 所示。考虑到网络安全服务的特性及区块链技术所具备的核心优势，该模型充分利用了区块链的分布式特性，旨在提升服务交易的安全性、透明性和可追溯性。交易流程从新成员注册身份开始，继而由系统分发密钥以确保交易的安全性。服务提供方随后在区块链上公开其服务的详细信息，如服务范围和级别，借此保障信息的不变性和可验证性。一旦服务信息通过共识机制的验证并被记录在区块链上，用户即可依据个人需求匹配并订阅相应的网络安全服务。在服务提供过程中，供应商负责更新进度与交付物，最终由用户完成支付。在此过程中，利用区块链技术的去中心化、不可篡改和可追溯等特性，为网络安全服务的交易提供可信度和安全的保障。同时，通过运用智能合约等技术，实现自动化的交易流程，减少中介和第三方的参与，降低交易成本。

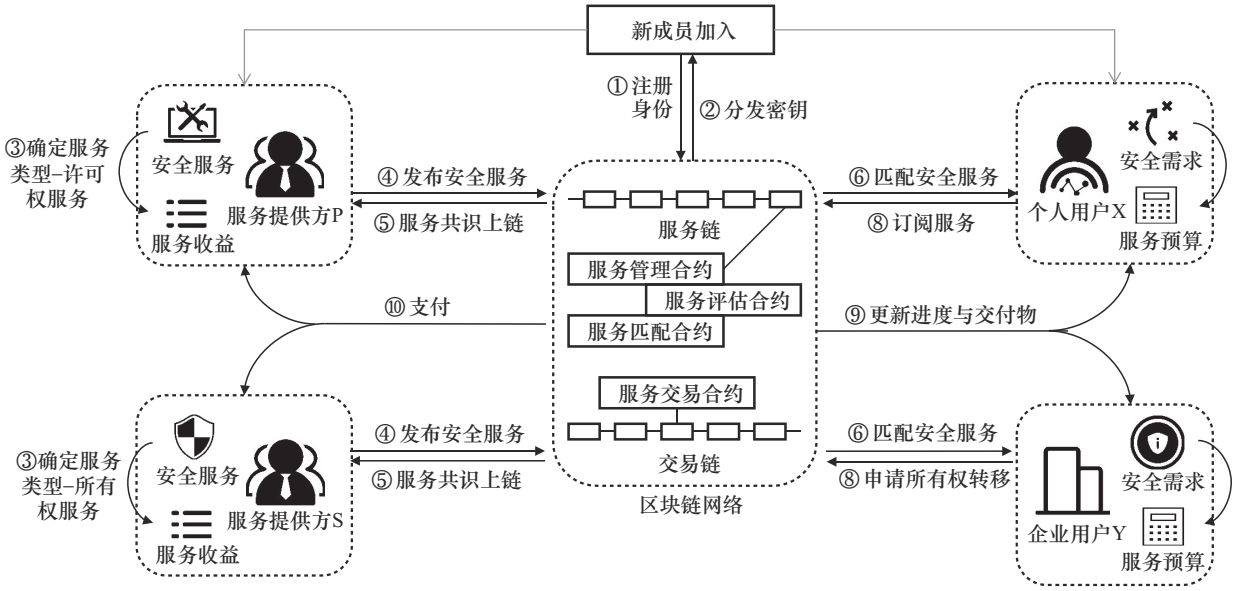

图1　基于区块链的网络安全服务交易模型

首先，通过新成员注册身份和系统分发密钥的步骤，建立了一个安全的网络环境，保证了交易双方身份的真实性和通信的安全性。服务提供方确定服务类型所有权服务并将其发布在区块链上，这一步骤利用了区块链技术的不可篡改性，确保了服务信息的真实性和可靠性，同时也便于用户根据公开透明的信息做出选择。共识校验机制的引入不仅进一步保障了上链信息的准确性，也增强了整个系统的抗攻击能力。用户匹配安全服务的过程中，区块链技术提供了一个去中心化的平台，减少了中介成本，提高了效率。根据用户订阅服务和服务提供商更新进度与交付物的步骤，通过区块链实现信息的即时更新和透明共享，提高了服务的可追踪性和用户的信任度。最后，用户支付环节利用区块链技术确保了交易的安全性和不可逆性。利用智能合约技术强制执行特性，构建了一种先服务后支付模式，激励服务提供方提高服务质量和效率，减少用户的风险与顾虑，形成了一个自我调节的服务交易生态系统，其中服务提供的价值直接影响收益，促使双方在交易过程中追求最高标准的透明度、诚信和责任感。整体而言，该模型通过引入区块链技术，不仅提升了网络安全服务交易的效率和透明度，也极大地增强了服务交易过程中的安全性和可信度。

2.1　参与实体

参与实体共同构建了基于区块链的网络安全服务生态系统，以保护数字化资产免受各种网络威胁。区块链的参与节点主要包括网络安全服务提供商节点与网络安全服务用户节点。

1) 区块链平台。去除了传统中心化机构或第三方，使各方之间能够直接交互，从而降低交易成本，为安全、透明和高效的交易提供了可能。数据以区块的形式存储，每个区块包含前一个区块的哈希值，保证了网络安全服务数据的链接和安全。由于区块链的分布式特性，使其具有更高的抗攻击能力和容错性，不容易遭受单点故障或篡改。

2) 网络安全服务提供商。网络安全服务提供商是提供网络安全服务的专业机构，负责为用户提供各种安全解决方案，包括威胁检测、防御、漏洞修复等。主要作用是设计、部署和管理网络安全服务，确保用户的数字化资产得到保护。

3) 网络安全服务用户。网络安全服务的终端用户可以是企业也可以是个人。企业用户依赖网络安全服务提供商来保护他们的数字资产，包括敏感数据、应用程序和网络资源。个人用户根据自身的安全需求，选择适当的网络安全服务，并遵守安全策略以维护数字化资产的安全。

2.2　双链结构

构建了双层区块链架构，包括服务链和交易链。服务链用于记录和管理网络安全服务的全生命周期，确保服务信息的透明性和可追溯性。交易链用于记录和管理网络安全服务的交易信息，确保交易过程的自动化和安全性。

1) 服务链。网络安全服务提供商通过服务链上的智能合约发布服务信息、管理服务的配置选

项、记录维护和更新操作，以及收集用户反馈。智能合约自动执行预先设定的条款，减少了人工介入的需求，简化了合同签订和审批流程。服务链主要包含3个关键组件：服务管理模块、服务匹配模块和反馈评估模块。服务管理模块用于更新和管理服务信息，包括服务类型的创建与更新、配置选项、价格等，确保服务在全生命周期内的安全性和一致性。该模块记录服务的运行、维护和更新信息，利用区块链的不可篡改性确保数据的完整性和可靠性，保障服务的持续有效性。服务匹配模块通过服务匹配合约，根据用户需求和服务提供商的能力进行自动化匹配合适的网络安全服务。这一过程提高了服务供需对接效率，确保用户能获得符合其安全需求的网络安全服务。反馈评估模块允许用户在服务结束后对服务进行评分和评价，并提供反馈意见，帮助服务提供商改进服务质量。该模块将用户的反馈记录在区块链上，同时将这些反馈映射到具体的服务质量指标上，为用户选择网络安全服务提供依据。

2) 交易链。交易链记录网络安全服务交易，包括许可权交易、控制权交易、使用权交易和所有权交易。由服务交易合约定义并自动执行预先设定的条款和条件，生成交易参与者、交易时间、交易性质和交易的细节信息，自动触发支付、服务交付等操作，确保了交易的快速和高效执行。通过区块链平台提供的共识算法验证交易的合法性和完整性，并通过非对称加密技术保护交易过程中记录的敏感信息，确保只有交易参与者可以解密和查看交易详细信息。此外，使用Merkle树结构存储服务交易信息的哈希值，以确保数据的完整性和不可篡改性。用户可以查看相应的服务提供商的历史记录、服务质量和定价情况，作为其可信的决策依据。交易链上的所有记录公开透明，可通过区块链浏览器查看和验证，确保交易过程的透明性和可追溯性。

2.3　智能合约

为了实现安全可信的网络安全服务交易模型，设计了4个关键的智能合约，分别是服务管理合约、服务匹配合约、服务评估合约和服务交易合约。这些智能合约在网络安全服务的管理、质量评估、需求匹配和交易执行方面发挥着关键作用。

1) 服务管理合约。用于管理服务的全生命周期，确保服务状态信息的透明性和实时更新。服务管理合约通过创建和记录服务状态信息，将服务数据存储在区块链上并监控服务执行，有效地管理了服务的全生命周期，确保了服务的可追溯性和可验证性。

2) 服务匹配合约。通过分析用户需求和服务提供商的能力，进行自动化服务匹配并排序，确保用户选择到最适合的网络安全服务。

3) 服务评估合约。根据用户对网络安全服务质量和效果的反馈，将反馈映射到具体的服务质量指标上，并为服务提供商生成评分，为服务质量提供了客观的度量标准。

4) 服务交易合约。定义了交易的条款，并自动执行交易，以确保交易的安全性和及时性。服务交易合约将交易的条款映射到智能合约代码中，减少了人为干预，同时确保了交易的顺利进行。

2.4　网络安全服务全生命周期

通过构建服务链对网络安全服务进行全生命周期管理，其模型如图2所示。网络安全服务的全生命周期管理包括服务的创建、发布、配置、运行、维护、更新和结束等关键阶段。

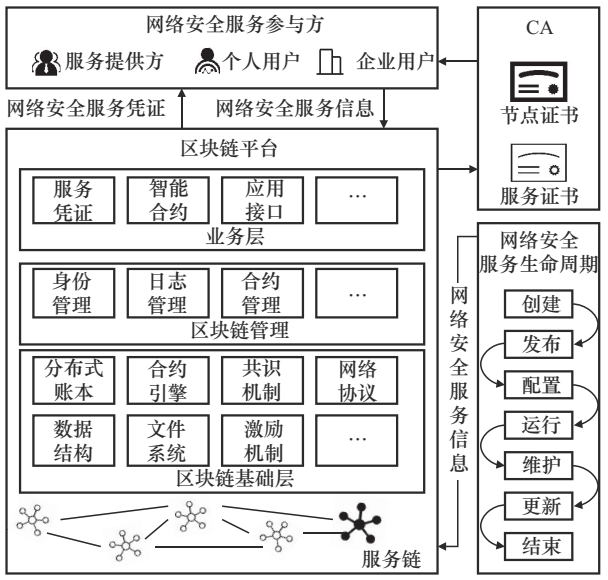

图2　全生命周期管理模型

在创建阶段，需求分析和规划确定了服务针对的需求R、目标O和范围S，随后设计和开发完成了服务的基本版本V。接下来，发布阶段涉及确定服务的类型T，如使用权、许可权、控制权和所有权服务，并通过服务管理智能合约将唯一标识ID记录在区块链上。在配置阶段，服务根据用户的需求进行自动化匹配，记录配置信息C^R，包括参数、

功能和权限等配置。将配置信息记录在服务链上，增加配置过程的可追溯性和减少非授权的更改。

服务进入运行阶段，启动服务并进行持续监控，确保服务按预期运行。其中服务被启动的同时记录监控信息M^C，利用服务链记录关键运行数据和监控日志，增强数据的安全性和完整性。维护和更新阶段包括漏洞修复、服务更新和性能优化，更新记录用U^C表示，服务链中记录每次更新和维护的详细信息，提供可验证的维护历史，以确保服务的安全性和高效性。最后，结束阶段涉及服务的评估E和终止，服务链中记录服务的终止过程和评估结果，以确保服务的效果和质量，如果需要，还需要进行数据迁移和清理。这7个阶段共同确保网络安全服务的有效运作、持续改进和安全性。即完整的网络安全服务全生命周期（CSSC, cyber security service full lifecycle）可表示为

$$\mathrm{CSSC}=\{\mathrm{ID}, T, R, O, S, V, C^R, M^C, U^C, E\} \quad (1)$$

从使用权、许可权、控制权和所有权4个维度对网络安全服务进行了系统的分类与定义，有助于更清晰地理解和有效地管理网络安全服务。以下是这4个维度的定义和解释。

1) 使用权服务。使用权服务允许用户在特定条件下使用网络安全资产，但不涉及资产的所有权转移。通常用户只是获得使用特定网络安全软件、硬件或资源的权利，无权修改或再分发该服务。例如，用户使用云端杀毒软件作为服务，可以按需使用该杀毒软件来保护其网络环境。用户仅获得该软件的使用权，无法对该软件进行修改。

2) 许可权服务。网络安全服务提供商授予用户特定网络安全服务的许可权服务，这些服务通常依据明确的许可协议进行规范，该许可协议规定了使用的条件、期限、付款方式等。许可权服务通常采用订阅模型，即用户在许可协议下支付费用，服务提供商提供网络安全软件的许可和保障，使用户能够合法使用该软件来保护其网络环境。这种许可权服务允许用户持续使用并享受网络安全功能，只要许可有效。

3) 控制权服务。控制权服务涉及将网络安全资产的管理和控制权限授予用户，使用户能够管理、监控和操作特定的网络安全资产。允许用户根据其具体需求和威胁情况来调整配置和行为，主动参与和管理其网络安全资产的配置、操作和响应威胁。控制权服务通常采用外包模型，将特定的网络安全服务、操作或监控职能委托给专业的外部服务提供商，用户仅保留对其网络安全策略的最终决策权，同时受益于外部专业知识和资源。

4) 所有权服务。所有权服务涉及将网络安全资产的实际所有权从一个实体转移到另一个实体。用户获得对网络安全资产的完全控制权和拥有权，可以自由使用、修改、转让和利用这些网络安全资产。出售专有网络安全技术的知识产权，如专利、商标和版权的转让。这使用户能完全拥有和控制这项技术，可以自由使用或做进一步开发研究。

3 系统流程

在本文所提基于区块链的服务交易模型中，整体交互过程被细分为认证、匹配、服务和交易4个关键阶段，以确保服务交易的透明性、安全性和效率。在认证阶段，所有参与方通过区块链技术进行身份验证和授权，建立信任基础。在匹配阶段，允许服务供应商发布其服务，而需求方则根据自身的需求进行服务匹配，确保服务供需之间的最佳对接。在服务阶段，涉及实际服务的执行与完成后用户对服务的评分，促进服务质量的提升。在交易阶段，通过智能合约技术自动执行的支付机制确保交易的及时性和安全性，完成服务价值的转移。

3.1 认证阶段

在认证阶段，服务供应商和需求方均需要通过区块链网络中的认证机制来验证其身份的合法性和可信度。该过程旨在确保交易双方身份的真实性，防止欺诈行为，提高交易的安全性。认证机制采用数字签名和公钥基础设施，确保每个参与者的身份信息被安全地加密和存储在区块链上。此外，认证过程还包括资质证明的验证，以确保服务供应商具备提供所声明服务的能力和资格。每个成员都被分配一个公钥PK和一个私钥SK来证明其身份，这反过来决定了参与者对记录的访问权限。首先为新成员提供身份验证信息，随后系统为其建立一个唯一的数字身份，并为其授权访问系统的权限。用户的数字身份是通过生成加密密钥对实现。该密钥对包括公钥和私钥，分别用于身份验证和交易签名。用户的公钥是其数字身份的一部分，它被存储在区块链系统的用户信息记录中。这个公钥将用作用户的地址，以便其他用户可以向其发送网络安全服务请

求。私钥是其数字身份的核心，用于交易签名和用户数据访问，由其持有方自行保管。此体系保障了用户身份信息的安全性和不可篡改性。

为了不失一般性，假设共有 n 个网络安全服务提供商（CSP, cyber security provider）和 m 个网络安全服务用户（CSR, cyber security user），分别表示为

$$\mathrm{CSP} = \{\mathrm{CSP}_1, \mathrm{CSP}_2, \cdots, \mathrm{CSP}_n\} \tag{2}$$

$$\mathrm{CSR} = \{\mathrm{CSR}_1, \mathrm{CSR}_2, \cdots, \mathrm{CSR}_m\} \tag{3}$$

为任意一个 CSP_i 生成椭圆曲线数字签名算法（ECDSA, elliptic curve digital signature algorithm）密钥对，表示为

$$(\mathrm{PK}_{\mathrm{CSP}_i}, \mathrm{SK}_{\mathrm{CSP}_i})$$

为任意一个 CSP_j 生成ECDSA密钥对，表示为

$$(\mathrm{PK}_{\mathrm{CSR}_j}, \mathrm{SK}_{\mathrm{CSR}_j})$$

其地址是通过散列其公钥计算得到的，若 CSP_i 注册 x 个服务，则网络安全服务（CSS, cyber security service）可表示为

$$\mathrm{CSS}_{\mathrm{CSP}_i} = \{\mathrm{CSS}^1_{\mathrm{CSP}_i}, \mathrm{CSS}^2_{\mathrm{CSP}_i}, \cdots, \mathrm{CSS}^x_{\mathrm{CSP}_i}\} \tag{4}$$

3.2　匹配阶段

匹配阶段是服务提供商发布其能够提供的网络安全服务的详细信息，包括服务范围、能力水平、预期成本等。同时，需求方基于其具体的服务需求，在区块链网络中进行搜索匹配服务。此过程通过智能合约自动执行，智能合约根据预设的基于属性匹配算法分析服务属性与需求之间的匹配程度，再结合服务提供商的历史表现综合确定服务提供商，从而实现最优的服务匹配。匹配结果将保证需求方能够找到最适合其需求的服务提供商，同时也为服务提供商提供了服务分享渠道。

网络安全服务提供商确定网络安全服务的类型，包括使用权、许可权、控制权和所有权服务。为了确保每种服务的唯一标识和全生命周期管理，网络安全服务提供商生成每种服务类型的唯一标识，并将其记录在区块链上。这确保了服务的唯一标识经过验证并与服务类型关联。在此过程中，区块链技术采用共识机制，确保服务类型经过验证并且达成一致。一旦服务类型和唯一标识成功上链，验证机制便可以确保服务类型的合法性，即确保服务类型符合网络安全服务的定义和标准。随着网络安全服务的不断演进，服务提供商可以进行版本迭代，为每种服务类型创建新的版本，如算法1所示。这些不同版本的服务将在区块链上链接到前一个版本，以确保版本之间的连接和可追溯性。这种机制可以轻松追踪服务的历史版本，并了解版本更新的详细信息。这一流程通过区块链技术的应用，增强了网络安全服务的可信度、透明性和安全性。

算法1　网络安全服务创建算法

输入　网络安全服务，上一版本的哈希值

输出　交易TXc

1) 执行每一个网络安全服务
2) 追溯上一版本的网络安全服务
3) 将网络安全服务信息发送至存储节点
4) 存储节点返回哈希值HD=Hash(网络安全服务)
5) 获取时间戳Tgs=getTimeStamp()
6) 生成网络安全服务的签名Sigh
7) 生成创建交易的唯一标识IDCS
8) TXc={上一版本的哈希值, HD, Tgs, Sigh, IDCS}
9) return TXc

此后，用户通过区块链进行需求匹配，以寻找适合的服务及其服务提供商。具体步骤如算法2所示，主要涉及综合评估2个方面：一是服务属性与需求之间的匹配程度；二是服务提供商的历史表现。明确需求方在寻找服务提供商时考虑的关键属性，如服务类型、服务质量、响应时间、价格等。使用基于属性匹配算法，为每个服务提供商计算一个匹配得分，反映其服务属性与需求方需求之间的匹配程度。将服务提供商的历史表现评分纳入考虑范围，通过加权平均的方式计算综合得分，其中权重反映了匹配得分和评分在最终决策中的相对重要性。即综合得分=（匹配得分×匹配得分权重）+（评分×评分权重）。根据综合得分对所有可选的服务提供商进行排序。通过这种方式，匹配合约不仅考虑了服务提供商能否满足需求方的具体需求，还考虑了他们的信誉和历史表现，从而提供了一个更全面、更客观的服务匹配和选择机制。这种方法有利于提高匹配的准确性和满意度，同时也鼓励服务提供商保持高质量的服务，以提高他们的综合得分和市场竞争力。

算法2　匹配确认算法

输入　网络安全服务

输出 网络安全服务的顺序数组 S

1) CSR_j 请求网络安全服务 R_{CSR_j}

2) for r=1 to k do

3) MS[r]=匹配(R_{CSR_j},$\mathrm{CSS}_{\mathrm{CSP}_r}$)

4) RS[r]=评分($\mathrm{CSS}_{\mathrm{CSP}_r}$)

5) CS[r]=αMS[r]+βRS[r]

6) end for

7) S = 根据CS将网络安全服务降序排列

8) return S

3.3 服务阶段

在服务阶段，用户与网络安全服务提供商之间的互动进一步具体化，用户获得和利用不同类型的网络安全服务，服务信息存储在服务链内。

1) 使用权服务允许用户在特定条件下使用网络安全资产，但并不转移资产的所有权。对于用户 CSR_j 和特定网络安全服务 $\mathrm{CSS}^x_{\mathrm{CSP}_i}$，使用权授予可表示为

$$\mathrm{CSR}_j \xrightarrow{\text{use}} \mathrm{CSS}^x_{\mathrm{CSP}_i}$$

用户通过区块链界面浏览和选择适用于其网络环境的网络安全服务。每个服务的详细信息、使用条件和用户评价都以区块链上的智能合约形式进行存储和展示。用户向智能合约提交使用申请，将使用权授予情况记录在区块链中。用户获得网络安全服务的使用权后，可以按需使用该服务以保护其网络环境。这包括使用特定的网络安全软件、硬件或资产，但不包括资产的实际拥有权。使用权服务的状态信息被记录到服务链中，以确保服务的透明性和实时性。用户可以随时跟踪其使用权服务的状态，包括剩余使用时间和服务性能。

2) 许可权服务在使用权服务的基础上需要签署订阅合约，涉及用户与服务提供商之间的合法许可协议。在区块链系统中，许可权服务的执行得以实现，确保用户合法使用网络安全软件和保障。网络安全服务提供商 CSP_i，将网络安全服务 $\mathrm{CSS}^x_{\mathrm{CSP}_i}$ 的许可权授予用户 CSR_j，智能合约确保该许可权交易遵循特定的许可协议，包括许可的有效期、费用等细节信息。许可权授予可表示为

$$\mathrm{CSP}_i \xrightarrow{\text{license}} \mathrm{CSR}_j{:}\mathrm{CSS}^x_{\mathrm{CSP}_i}$$

一旦用户选择了网络安全服务，智能合约将自动生成明确的许可权合约。这个许可权合约包括许可的条件、期限和费用，以确保用户与服务提供商之间的合法关系。用户和服务提供商通过区块链系统上的数字身份进行合约签署，确保了合约的安全性和不可篡改性。合约签署后，智能合约自动执行许可权的授予和管理，包括在合约期限内的持续服务。用户可以持续访问网络安全服务，只要许可权有效，费用也会按照合约规定的方式自动扣除。一旦许可权协议到期，智能合约将自动停止提供服务。此时用户和服务提供商可以选择续订许可权合约，或者终止许可权合约，具体操作根据合约规定进行。

许可权服务的实施和管理利用区块链系统的智能合约和不可篡改性，确保了用户的权益和服务的可持续性。

3) 控制权服务涉及用户被赋予网络安全资产的管理和控制权限，以主动管理、监控或操作特定的网络安全资产。在控制权服务交易过程中，用户 CSR_j 可以接受特定网络安全资产的管理和控制权限。智能合约确保该交易仅授予用户合法的管理权限。控制权授予可表示为

$$\mathrm{CSP}_i \xrightarrow{\text{control}} \mathrm{CSR}_j{:}\mathrm{CSS}^x_{\mathrm{CSP}_i}$$

用户通过区块链系统配置其网络安全资产的权限和策略。这可能涉及设置特定的访问控制列表、监控规则或响应威胁策略。控制权服务通常采用外包模型，用户可以将特定的网络安全服务、操作或监控职能委托给专业的外部服务提供商。这些服务提供商可能利用智能合约来管理用户的网络安全资产。用户仅保留对其网络安全策略的最终决策权。区块链系统记录所有的操作和更改，以确保其透明性和不可篡改性。

4) 所有权服务涉及网络安全资产的实际所有权转移，用户获得对这些资产的完全控制权和拥有权。将网络安全资产的实际所有权从一个实体转移到另一个实体，可表示为

$$\mathrm{CSP}_i \xrightarrow{\text{wonership}} \mathrm{CSR}_j{:}\mathrm{CSS}^x_{\mathrm{CSP}_i}$$

一旦用户决定获得所有权服务，智能合约将生成资产转让合约。这个合约明确规定了资产转让的条件、所有权转移的细节和费用等。用户获得对网络安全资产的实际控制权，包括使用、修改、转让和利用这些资产的权利。这使用户能完全拥有和控

制这项技术，可以自由使用或做进一步开发。所有权服务的实施和交易记录被存储在交易链中，以确保交易的不可篡改性。这有助于验证交易和所有权转移的合法性。

这一系统架构能够提供更高的透明性、安全性和可信度，有助于用户和服务提供商之间的合法交互。

3.4　交易阶段

服务提供先于支付，即消费者在接受服务后再进行结算。用户和服务提供商之间的交互受智能合约的约束，确保了安全、透明和高效的资金流转。通过对服务链区块链信息校验，触发交易过程执行，完成用户与网络安全服务提供商之间的支付。此模式显著降低了用户的预先风险，因为用户不需要提前支付费用，而是在评估服务后再作出支付决定。与此同时，该模式激励服务提供商提升了服务质量，以确保能够获得相应的报酬，从而提高整体交易的公平性和效率。

智能合约充当交易的自动执行引擎，确保了交易的可靠性。接下来，通过区块链网络的节点验证交易的有效性和合法性，包括检查用户的身份、账户余额和服务提供商的资格，确保交易的合规性。一旦交易得到验证，智能合同将自动执行交易，确保交易条件得到满足，包括资金的转移、服务许可权的颁发和其他权益的变更。交易的细节被记录到交易链上作为区块链的一部分。这个记录是不可篡改的，确保了交易的安全性和可追溯性。最后，一旦交易完成，参与者可以查看交易的细节，包括时间戳和交易状态，从而确保了交易的透明性。

4　理论分析与实验验证

4.1　实例分析

网络安全服务提供商专注于为金融机构提供实时风险预警服务。这项服务旨在及时识别并预警各种网络安全威胁，如钓鱼攻击、恶意软件传播、异常登录活动等，帮助用户防范未知风险。在认证阶段，网络安全服务提供商通过提交其服务能力的证明（包括公司资质、服务团队专业证书、以往成功案例等）到区块链平台进行认证。同时，一家寻求风险预警服务的金融机构也通过上传其企业认证文件到同一区块链平台完成认证。这一过程通过数字证书和非对称加密技术确保了双方身份的真实性和可信度。在匹配阶段，网络安全服务提供商在区块链平台上发布其风险预警服务的详细信息，包括监测能力范围、服务响应时间、以往客户反馈等。金融机构根据其面临的网络安全威胁等级，在区块链平台上搜索并筛选合适的风险预警服务。系统将通过智能合约自动推荐与金融机构需求最匹配的服务提供商，网络安全服务提供商因其最高的综合得分被匹配成功。

当匹配成功后，网络安全服务提供商开始对金融机构的网络环境进行实时监控，使用高级算法分析潜在网络安全威胁，并提供即时预警信息。在此过程中，金融机构被赋予特定的网络安全资产控制权，如调整监控参数、实时查看威胁分析结果等。权限信息、服务活动和交互数据通过区块链记录，确保了服务过程的透明性和可审计性。当服务完成后，金融机构根据网络安全服务提供商提供的服务效果，通过区块链平台进行评分和反馈。基于服务结果和满意度，智能合约将自动计算服务费用并执行支付过程，确保了交易的安全性和不可逆性。一旦网络安全服务提供商收到付款，区块链就会记录交易细节，为双方提供不可否认的交易证明。

在基于区块链的风险预警服务交易中，利用区块链的分布式架构和不可篡改等特性，降低了人为干预与重复审核的必要性，加速了服务的部署和响应时间。通过智能合约的精确自动执行，不仅提高了操作的准确性，而且通过程序代码的透明化增强了交易过程的可验证性，进一步提升了系统的整体透明度和增强了所有参与方对交易流程的信任。此外，采用基于区块链的支付机制，消除了传统金融中介的介入，允许直接在交易双方之间进行资金转移，减少了交易成本和时延，提高了交易效率和降低了操作风险。

4.2　理论分析

1) 安全性。通过在网络安全服务的全生命周期管理中应用区块链技术，显著增强了服务过程的透明性和可追溯性。通过对网络安全服务进行详细的分类，包括使用权、许可权、控制权和所有权4个维度，有助于更精确地识别和管理潜在的网络安全风险，提升整体服务的安全性和可靠性。首先，非对称加密技术的应用保障了数据传输过程中的安全性和隐私性，确保只有授权用户才能访问和处理相关数据。其次，引入双链结构，构建网络安全服务交

易模型，为系统安全性提供了双重保障。服务链致力于管理网络安全服务的全生命周期，而交易链专注于自动化服务交易的安全性和完整性。这种分离策略使数据存储和交易过程相互独立，有效降低了单点故障的风险，同时增加了系统的鲁棒性和抗攻击能力。最后，智能合约的自动执行机制确保了交易过程中各项条件的严格遵守，有效避免了传统交易过程中可能出现的违约或欺诈行为，提高了服务的效率和可靠性。

2) 可审计性。交易过程和结果能够被可信第三方验证的能力，对于增强网络安全服务交易的透明性和信任至关重要。双链结构记录了服务的全生命周期和交易的每一个环节，每一笔交易都被永久记录在区块链上，且不可篡改、易于追溯。智能合约的执行结果同样被记录在区块链上，为交易的每一方提供了清晰和不可否认的证据。因此，任何利害关系人都可以通过区块链查询交易记录和智能合约的执行状态，确保了交易过程的可审计性，增强了参与方之间的信任。数字签名技术进一步增强了模型的可审计性。通过为交易和消息提供一个唯一的、验证性强的数字身份标识，确保了数据来源的真实性和完整性，同时验证了交易双方的身份真实性。这不仅为交易的每一方提供了不可否认的证据，而且确保了即使在长期存储之后，交易记录和服务记录的真实性和完整性也得到了保证。

3) 完整性。保护交易模型中的数据在全生命周期内的一致性、没有被未授权地修改或破坏。首先，智能合约的不可变性确保了合约一旦被部署，其逻辑就不可更改，从而保证了执行过程的一致性。其次，区块链技术的双链结构特性，即每个区块都包含前一个区块的哈希值，加强了数据不可篡改的特性，任何对数据的非法修改都会被网络其他节点检测到并拒绝。最后，区块链技术的权限配置机制确保只有授权的参与方可以进行特定的操作，从而保护了数据不受未授权访问或篡改，确保了交易模型的完整性。

4.3　性能分析

为了验证基于区块链的网络安全服务交易模型的性能，采用基于Docker的Fabric区块链模拟平台进行实验验证。实验环境配置包括5个对等节点（Peer 0: org 1至Peer 0: org 5）和一个排序节点，采用的共识策略要求参与节点对交易进行签名，验证模型在不同组织机构数量下的性能表现。根据上述模型设计，实现网络安全服务交易的几项关键功能，包括新成员创建账户、匹配网络安全服务以及创建网络安全服务交易信息。此外，选择测量平均交易时延和平均交易吞吐量作为关键性能指标，评估交易系统在实际运行过程中的效率和可扩展性。

图3给出了共识节点数量从1变化到5时，其对平均交易时延的影响。平均交易时延代表从提交交易到交易被确认所需的时间，直接反映了系统处理请求的速度。在网络安全服务交易的背景下，较低的平均交易时延意味着系统可以更快地响应安全服务需求。由图3可知，随着共识节点数量的增加，新成员创建账户和创建网络安全服务交易信息时的平均交易时延略有上升。这一现象表明，随着共识节点数量的增加，需要更多的时间来验证交易的有效性，从而导致平均交易时延与共识节点数量呈线性相关增加。相比之下，共识节点数量对于匹配网络安全服务过程的平均交易时延影响相对较小。由于匹配操作主要依赖于节点自行调用智能合约，而不需要参与共识过程，因此这一部分的平均交易时延受共识节点数量增加的影响较小。随着共识节点数量的增加，平均交易时延逐渐增长，反映出系统在处理每个交易时需要更多的时间来达成共识，确保交易的安全性和正确性。

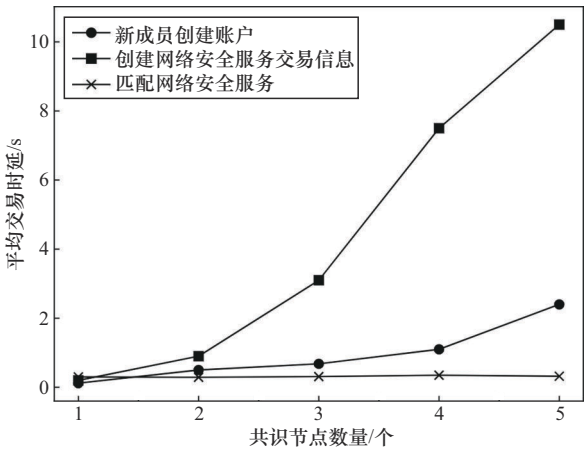

图3　共识节点数量对平均交易时延的影响

图4给出了新成员创建账户、创建网络安全服务交易信息和匹配网络安全服务操作的平均交易吞吐量随共识节点数量变化的趋势。平均交易吞吐量表示单位时间内系统能够处理的交易数量，它衡量了系统的处理能力。由图4可知，随着共识节点数

量的增加，这些操作的平均交易吞吐量呈线性下降趋势，尤其对新成员创建账户和创建网络安全服务交易信息操作更为明显。这一结果表明，增加共识节点数量虽然可以提高系统的安全性和可靠性，但同时也会对系统的性能产生影响，尤其是在交易处理能力方面。匹配网络安全服务的整体趋势保持相对稳定，说明系统在扩展性方面表现良好，能够在增加共识节点数量的情况下维持合理的性能水平。

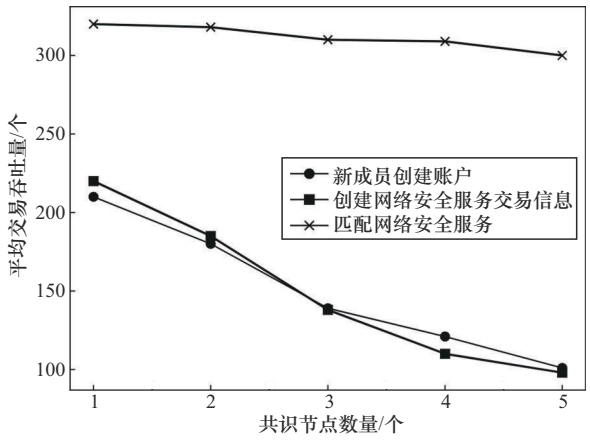

图4　平均交易吞吐量随共识节点数量变化趋势

本文对基于区块链的网络安全服务交易模型进行了深入分析。实验结果揭示了该模型在不同共识节点数量下的性能表现，提供了对模型处理效率和扩展性方面的见解。这些发现为本文模型的进一步优化和在复杂网络环境中的应用提供了有意义的参考。

5　结束语

本文探讨了安全可信的基于区块链的网络安全服务交易模型，旨在提高网络安全服务的可追溯性、透明性和安全性。首先，对网络安全服务进行了分类，包括使用权、许可权、控制权和所有权 4 个维度，并为不同类型的服务提供了清晰的定义。接着，引入了双链结构，包括服务链和交易链，以实现网络安全服务的全生命周期管理。服务链用于记录和管理服务的详细信息，而交易链用于自动化的服务交易，形成先服务后支付模式。此外，设计了 4 个智能合约，分别用于服务管理、评估、匹配和交易执行。最后，通过实验验证，证明了这些智能合约的有效性和可信度。研究结果表明，本文模型为网络安全服务提供了一种更安全、高效和可管理的交易方式。

参考文献：

[1] YU Z H, GAO H X, CONG X Y, et al. A survey on cyber-physical systems security[J]. IEEE Internet of Things Journal, 2023, 10(24): 21670-21686.

[2] 杨毅宇, 周威, 赵尚儒, 等. 物联网安全研究综述: 威胁、检测与防御[J]. 通信学报, 2021, 42(8): 188-205.
YANG Y Y, ZHOU W, ZHAO S R, et al. Survey of IoT security research: threats, detection and defense[J]. Journal on Communications, 2021, 42(8): 188-205.

[3] ALZOUBI H M, GHAZAL T M, HASAN M K, et al. Cyber security threats on digital banking[C]//Proceedings of the 2022 1st International Conference on AI in Cybersecurity (ICAIC). Piscataway: IEEE Press, 2022: 1-4.

[4] SHEIKH M S, LIANG J, WANG W S. A survey of security services, attacks, and applications for vehicular ad hoc networks (VANETs)[J]. Sensors, 2019, 19(16): 3589.

[5] 王冬, 秦倩倩, 郭开天, 等. 联邦学习中的模型逆向攻防研究综述[J]. 通信学报, 2023, 44(11): 94-109.
WANG D, QIN Q Q, GUO K T, et al. Survey on model inversion attack and defense in federated learning[J]. Journal on Communications, 2023, 44(11): 94-109.

[6] QURESHI A, DASHTI W, JAHANGEER A, et al. Security challenges over cloud environment from service provider prospective[J]. Cloud Computing and Data Science, 2020: 12-20.

[7] VESTAD A, YANG B. Adoption of cybersecurity innovations—a systematic literature review[C]//The International Conference on Cybersecurity, Situational Awareness and Social Media. Berlin: Springer, 2024: 285-304.

[8] LI J J, LI J Q, WANG X, et al. Multi-blockchain based data trading markets with novel pricing mechanisms[J]. IEEE/CAA Journal of Automatica Sinica, 2023, 10(12): 2222-2232.

[9] LIU W, FENG W L, HUANG M X, et al. STEB: a secure service trading ecosystem based on blockchain[J]. PLoS One, 2022, 17(6): e0267914.

[10] 李永明, 赖利娜. 区块链背景下数字版权全链条保护的困境与出路[J]. 科技管理研究, 2022, 42(10): 140-150.
LI Y M, LAI L N. The dilemma and solution of full chain protection of digital copyright based on blockchain[J]. Science and Technology Management Research, 2022, 42(10): 140-150.

[11] TAN T M, SARANIEMI S. Trust in blockchain-enabled exchanges: future directions in blockchain marketing[J]. Journal of the Academy of Marketing Science, 2023, 51(4): 914-939.

[12] NAMASUDRA S, DEKA G C, JOHRI P, et al. The revolution of blockchain: state-of-the-art and research challenges[J]. Archives of Computational Methods in Engineering, 2021, 28(3): 1497-1515.

[13] 霍如, 程祥凤, 孙闯, 等. 区块链网络拓扑优化和转发策略设计[J]. 通信学报, 2022, 43(12): 89-100.
HUO R, CHENG X F, SUN C, et al. Topology optimization and forwarding strategy design for blockchain network[J]. Journal on Communications, 2022, 43(12): 89-100.

[14] XU J, WANG C, JIA X H. A survey of blockchain consensus protocols[J]. ACM Computing Surveys, 2023, 55(13s): 1-35.

[15] YAVAPRABHAS K, POURNADER M, SEURING S. Blockchain as

the “trust-building machine” for supply chain management[J]. Annals of Operations Research, 2023, 327(1): 49-88.

[16] 孙俨, 熊翱, 蒋承伶, 等. 基于区块链的计算与无线通信资源联合管理双向拍卖模型[J]. 通信学报, 2022, 43(11): 14-25.
SUN Y, XIONG A, JIANG C L, et al. Blockchain-based computing and wireless communication resource joint management double auction model[J]. Journal on Communications, 2022, 43(11): 14-25.

[17] 张海波, 曹钰坤, 刘开健, 等. 车联网中基于区块链的分布式信任管理方案[J]. 通信学报, 2023, 44(5): 148-157.
ZHANG H B, CAO Y K, LIU K J, et al. Distributed trust management scheme based on blockchain in Internet of vehicles[J]. Journal on Communications, 2023, 44(5): 148-157.

[18] BELCHIOR R, VASCONCELOS A, GUERREIRO S, et al. A survey on blockchain interoperability: past, present, and future trends[J]. arXiv Preprint, arXiv: 2005.14282, 2020.

[19] SANKA A I, IRFAN M, HUANG I, et al. A survey of breakthrough in blockchain technology: adoptions, applications, challenges and future research[J]. Computer Communications, 2021, 169: 179-201.

[20] 龚强, 班铭媛, 张一林. 区块链、企业数字化与供应链金融创新[J]. 中国社会科学文摘, 2021(6): 89-90.
GONG Q, BAN M Y, ZHANG Y L. Blockchain, enterprise digitalization and supply chain finance innovation[J]. Chinese Social Science Digest, 2021(6): 89-90.

[21] 蔡晓晴, 邓尧, 张亮, 等. 区块链原理及其核心技术[J]. 计算机学报, 2021, 44(1): 84-131.
CAI X Q, DENG Y, ZHANG L, et al. The principle and core technology of blockchain[J]. Chinese Journal of Computers, 2021, 44(1): 84-131.

[22] 陈迪, 邱菡, 朱俊虎, 等. 基于区块链的域间路由策略符合性验证方法[J]. 软件学报, 2023, 34(9):4336-4350.
CHEN D, QIU H, ZHU J H, et al. Blockchain-based validation method for inter-domain routing policy compliance[J]. Journal of Software, 2023, 34(9): 4336-4350.

[23] 陈烨, 许冬瑾, 肖亮. 基于区块链的网络安全技术综述[J]. 电信科学, 2018, 34(3): 8-16.
CHEN Y, XU D J, XIAO L. Survey on network security based on blockchain[J]. Telecommunications Science, 2018, 34(3): 8-16.

[24] SALMAN T, ZOLANVARI M, ERBAD A, et al. Security services using blockchains: a state of the art survey[J]. IEEE Communications Surveys & Tutorials, 2019, 21(1): 858-880.

[25] 冯涛, 陈李秋, 方君丽, 等. 基于本地化差分隐私和属性基可搜索加密的区块链数据共享方案[J]. 通信学报, 2023, 44(5): 224-233.
FENG T, CHEN L Q, FANG J L, et al. Blockchain data sharing scheme based on localized difference privacy and attribute-based searchable encryption[J]. Journal on Communications, 2023, 44(5): 224-233.

[26] 王苗苗, 芮兰兰, 徐思雅. 面向文化资源可信共享的多因子身份认证方案[J]. 通信学报, 2023, 44(10): 34-45.
WANG M M, RUI L L, XU S Y. Multi-factor identity authentication scheme for trusted sharing of cultural resources[J]. Journal on Communications, 2023, 44(10): 34-45.

[27] LAMBA A, SINGH S, DUTTA N, et al. Uses of different cyber security service to prevent attack on smart home infrastructure[J]. SSRN Electronic Journal, 2014, 1(11): 5809-5813.

[28] 王利朋, 关志, 李青山, 等. 区块链数据安全服务综述[J]. 软件学报, 2023, 34(1): 1-32.
WANG L P, GUAN Z, LI Q S, et al. Survey on blockchain-based security services[J]. Journal of Software, 2023, 34(1): 1-32.

[29] 林莉, 储振兴, 刘子萌, 等. 基于区块链的策略隐藏大数据访问控制方法[J]. 自动化学报, 2023, 49(5): 1031-1049.
LIN L, CHU Z X, LIU Z M, et al. A policy-hidden big data access control method based on blockchain[J]. Acta Automatica Sinica, 2023, 49(5): 1031-1049.

[30] 张淑娥, 田成伟, 李保罡. 基于区块链技术的身份认证研究综述[J]. 计算机科学, 2023, 50(5): 329-347.
ZHANG S E, TIAN C W, LI B G. Review of identity authentication research based on blockchain technology[J]. Computer Science, 2023, 50(5): 329-347.

[31] 王晟典, 陈娥, 朱岩, 等. 一种基于区块链智能合约的软件服务交易方法[J]. 工程科学学报, 2023, 45(3): 475-488.
WANG S D, CHEN E, ZHU Y, et al. A software service transaction approach based on blockchain smart contracts[J]. Chinese Journal of Engineering, 2023, 45(3): 475-488.

[32] NASEER H, MAYNARD S B, DESOUZA K C. Demystifying analytical information processing capability: the case of cybersecurity incident response[J]. Decision Support Systems, 2021, 143: 113476.

[33] XIANG X Y, CAO J, FAN W G. Decentralized authentication and access control protocol for blockchain-based e-health systems[J]. Journal of Network and Computer Applications, 2022, 207: 103512.

[34] VISHWAKARMA L, NAHAR A, DAS D. LBSV: lightweight blockchain security protocol for secure storage and communication in SDN-enabled IoV[J]. IEEE Transactions on Vehicular Technology, 2022, 71(6): 5983-5994.

[35] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[J]. Consulted, 2008, 28(1): 21260-21268.

[36] 陈冬林, 唐艺倩, 聂规划, 等. 基于零知识证明的科技服务交易数据保密机制[J]. 科技管理研究, 2021, 41(20): 80-86.
CHEN D L, TANG Y Q, NIE G H, et al. Data confidentiality mechanism of science and technology service transaction based on zero knowledge proof[J]. Science and Technology Management Research, 2021, 41(20): 80-86.

[37] 张垿豪, 冯文龙, 黄梦醒, 等. 基于区块链的科技服务质量信任评价方案[J]. 计算机工程, 2022, 48(5): 127-135, 144.
ZHANG X H, FENG W L, HUANG M X, et al. Trust evaluation scheme for technology quality of service based on blockchain[J]. Computer Engineering, 2022, 48(5): 127-135, 144.

[38] 李妃养, 黄何, 张宏丽. 区块链技术在技术成果交易领域应用探索[J]. 科学管理研究, 2020, 38(3): 55-60.
LI F Y, HUANG H, ZHANG H L. Application exploration of block chain technology in the field of technology trading[J]. Scientific Management Research, 2020, 38(3): 55-60.

[39] HU J, ZHU P, QI Y, et al. A patent registration and trading system based on blockchain[J]. Expert Systems with Applications, 2022, 201: 117094.

[40] ZHUANG C X, DAI Q Y, ZHANG Y. BCPPT: a blockchain-based privacy-preserving and traceability identity management scheme for intellectual property[J]. Peer-to-Peer Networking and Applications,

2022, 15(1): 724-738.

[41] 李向阳, 刘扬, 闫志全, 等. 基于区块链的知识产权交易平台研究与实现[J]. 计算机工程与应用, 2023, 59(3): 308-316.
LI X Y, LIU Y, YAN Z Q, et al. Research and implementation of intellectual property trading platform based on blockchain[J]. Computer Engineering and Applications, 2023, 59(3): 308-316.

[42] 黄华梅, 陆建波, 李文敬, 等. 基于区块链的家政服务交易群智合约算法研究[J]. 计算机应用与软件, 2023, 40(9): 137-144, 204.
HUANG H M, LU J B, LI W J, et al. Blockchain-based housekeeping service transaction group smart contract algorithm[J]. Computer Applications and Software, 2023, 40(9): 137-144, 204.

[43] YAHAYA A S, JAVAID N, JAVED M U, et al. Blockchain-based secure energy trading with mutual verifiable fairness in a smart community[J]. IEEE Transactions on Industrial Informatics, 2022, 18(11): 7412-7422.

[44] LIU Z W, HU C Q, XIA H, et al. SPDTS: a differential privacy-based blockchain scheme for secure power data trading[J]. IEEE Transactions on Network and Service Management, 2022, 19(4): 5196-5207.

[作者简介]

朴桂荣（1997– ），女，朝鲜族，黑龙江牡丹江人，中央财经大学博士生，主要研究方向为信息安全、数字经济等。

朱建明（1965– ），男，山西太原人，博士，中央财经大学教授、博士生导师，主要研究方向为信息安全、区块链、金融科技等。