前　言

信任是现代社会运行的基石.在社会经济各领域数字化转型的今天,构建支持信任管理的基础设施信息系统,对于提高社会运行效率,降低社会协作成本,及时发现和应对各类风险,乃至创新协作模式,助力新数字经济产业的产生和发展都具有重要意义.区块链的本质是用技术手段构建信任,是利用计算机和数学支持和促进社会进步的信任机器,也是我国在社会进步和新的国际竞争格局中形成核心竞争力的关键领域之一.区块链是分布式网络、加密技术、智能合约等多种技术集成的新型数据库软件,是基于数据进行信任管理的信息系统基础设施.作为基础设施,单一技术路线的区块链系统无法解决多方协同面临的数据交换和交叉验证问题,目前缺乏开放互联的系统架构层面的理论和技术支撑;作为应用的基础,区块链系统不仅涉及数据存储、事务处理、智能合约执行、安全和隐私保护等核心技术,还必须解决方便开发、易于运维、软硬件适配,以及人才培养等生态建设问题.

为推动我国在区块链技术的创新与发展,我们组织了本期“区块链数据管理与安全”专题,旨在征集区块链技术的创新发展,特别是区块链数据管理与安全等领域的前沿技术与应用.本专题2023年4月初征稿结束,经过两轮评审,最终收录了10篇论文,内容涵盖了区块链数据存储、智能合约、高效的共识协议、跨链和互操作性、区块链隐私保护、区块链新型应用等方面的最新研究进展,希望能够为同行学者带来帮助和启发.

数据查询在数据溯源等领域中非常关键.为解决现有图式区块链查询面临的效率低、验证难等问题,常健等人对此开展了深入研究,论文“基于学习索引的图式区块链高效可验证查询机制”提出了一种基于学习索引的高效可验证的图式区块链查询机制Lever,通过引入学习索引技术对图式区块链中时序数据分布特征进行学习实现对索引过程的优化,提高了图式区块链查询的效率和可验证性.

分片技术通过在多个子网并行执行交易使得执行性能随着子网数成比例提升.为解决跨片交易执行成本高昂的问题,阙琦峰等人对此开展了深入研究,论文“面向分片许可链的无协调者跨片交易处理”提出了一个针对分片许可链的跨片交易执行方法,将确定性引入跨片交易执行,避免了额外的协调开销,从而提高了系统执行跨片交易的效率.

区块链预言机将外界数据写入区块链,是区块链获取外界数据的一般方法.为解决现有依赖虚拟货币抵押对节点身份授信的方法难以适应国内场景的问题,张鹏展等人对此开展了深入研究,论文“基于去中心化身份的开放区块链预言机方案”应用非同质化通证映射节点身份,支持区块链预言机服务所有者治理节点身份,与全局公钥更新过程结合,使节点加入状态可跟踪.

共识机制是区块链技术的重要组成部分.为解决联邦学习的学习模型的本地训练和最终参与方贡献度计算需消耗大量算力资源的问题,张宝晨等人对此开展了深入研究,论文“一种支持自适应联邦学习任务的可信公平区块链框架”提出了一种支持自适应联邦学习任务的可信公平区块链框架TFchain,利用原本共识机制中耗费的大量算力来提高联邦学习的效率.

异构/同构区块链间的互联互通的需求在快速增长.为解决架构可扩展性与跨链需求多样性挑战问题,段田田等人对此开展了深入研究,论文“PieBridge:一种按需可扩展的跨链架构”

提出一种按需可扩展的跨链架构 PieBridge，以 4 层跨链交互协议栈，解耦跨链传输、验证、事务与应用，满足不同跨链应用在隐私、安全、性能等方面的差异化需求.

跨链数字资产交换可实现数据共享、业务合作和价值流通.为解决现有跨链方案出块和确认速度慢、订单类型和功能较少的问题，马宇航等人对此开展了深入研究，论文“基于分布式密钥生成和属性基密码的多方跨链交易方案”通过分布式密钥生成与属性密码实现去中心化的多方交易方案，将用户的资产质押到分布式网络中，实现去中心的资产管理模式.

区块链技术在提供了不可篡改性、透明性的同时也带来严重的隐私泄露问题.为解决现有基于公钥基础设施体系的方案管理证书成本过高、国密算法具有局限性的问题，安浩杨等人对此开展了深入研究，论文“基于 SM9 数字签名的环签名及其在区块链隐私保护中的应用”提出了一种基于 SM9 数字签名的常数级大小环签名方案，在随机谕言机模型下证明了该方案满足不可伪造性和匿名性，实现了对交易方身份的隐私保护.

去中心化身份让用户完全控制自己的身份.为解决现有的身份验证方法存在的用户身份凭证管理繁重、安全性不足等问题，冉津豪等人对此开展了深入研究，论文“基于区块链和可信执行环境的属性签名身份认证方案”提出一种基于区块链和可信执行环境的属性签名身份认证方案，使用户可利用属性签名生成指向应用服务的持久性凭据，并且凭据是可扩充的.

联邦学习在服务器端仍然存在安全性隐患.为解决将服务器端替换为区块链系统之后无法利用所有可用网络连接，且缺少了针对联邦学习任务的区块结构设计的问题，施宏建等人对此开展了深入研究，论文“基于区块链辅助的半中心化联邦学习框架”提出了基于区块链辅助的半中心化联邦学习框架，构建了半中心化的物联网场景，利用可信网络连接来支撑联邦学习任务，通过区块链为不可信、远距离客户端之间构建了不可篡改的模型库，从而降低通信开销、提升普适性.

联邦学习是一种被广泛使用的隐私保护技术.为解决中心服务器不稳定和联邦学习服务器与参与方交互造成的隐私泄露等问题，刘炜等人对此开展了深入研究，论文“基于区块链和动态评估的隐私保护联邦学习模型”提出了一种基于区块链和动态评估的隐私保护联邦学习模型，利用区块链解决中心服务器的问题，通过本地训练使用稀疏化、全局模型更新使用差分隐私解决联邦学习过程中的隐私泄露问题，本地训练完成后用数字签名和双重哈希对比验证参与方身份和训练模型的所属权.

区块链数据管理与安全是区块链系统的重要内容，希望本专题能够抛砖引玉，促进我国相关研究的进一步发展.由于专题篇幅有限，无法全面覆盖区块链数据管理与安全领域的所有研究进展，不足之处敬请各位学者谅解和批评指正.衷心感谢《计算机研究与发展》提供了宝贵的机会出版该专题的论文，感谢评审专家、编辑部工作人员的辛勤工作，感谢各位作者对本专题组织者的信任和支持，使得本专题顺利出版！

李颉（上海交通大学）
阚海斌（复旦大学）
金澈清（华东师范大学）
2023 年 9 月