中国科学: 信息科学 2020 年 第 50 卷 第 3 期: 461–462
SCIENTIA SINICA Informationis
《中国科学》杂志社
SCIENCE CHINA PRESS

刊讯

区块链应用中的安全隐私专题简介

仲盛[1], 黄欣沂[2*]

1. 南京大学, 南京 210093
2. 福建师范大学, 福州 350007
* 通信作者. E-mail: xyhuang@fjnu.edu.cn

区块链技术最早由中本聪 (Satoshi Nakamoto) 在 2008 年提出, 是支持和实现比特币的关键技术. 区块链是一种按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构, 并以密码学方式保证不可篡改和不可伪造的分布式账本. 区块链技术是分布式数据存储、点对点传输、共识机制、加密算法等技术的新型应用模式. 它具有去中心化、开放性、防篡改、匿名性、可追溯性等特点. 得益于这些优点, 区块链技术在最近几年成为了金融、电子政务、物联网、公共服务、食品药品监管追溯、供应链金融等领域的研究热点, 被认为将引领全球新一轮技术变革和产业变革.

随着区块链技术的发展和广泛应用, 区块链也逐渐暴露出安全隐私问题, 必须得到足够的重视. 和传统中心化结构相比, 区块链技术不依赖于某个特定的中心节点, 系统中的每个区块链节点分别独立存储数据和处理数据, 有效避免了单点失败的问题. 然而, 为了达到公开验证, 区块链中所有的交易记录 (数据) 必须公开, 这将导致隐私泄露问题. 当区块中交易信息是敏感信息时, 比如个人健康记录、银行账号信息或者是军事相关的数据, 将对个人安全和国家安全造成严重威胁. 因此, 区块链技术在真正从理论到现实应用之前, 必须解决数据安全隐私问题. 针对上述目标, *SCIENCE CHINA Information Sciences* 在 2020 年 63 卷第 3 期组织出版了 “Special Focus on Security and Privacy in Blockchain-based Applications” (区块链应用中的安全与隐私专题), 致力于介绍区块链的最新进展, 涵盖了该领域广泛的主题. 专题共收录了 5 篇论文.

群数据共享方案能够实现多用户之间高效的数据共享. 然而现有方案只支持属于同一个组织/机构里的用户数据共享. Huang 等人的论文 “Blockchain-based multiple groups data sharing with anonymity and traceability” 讨论了如何实现属于不同群组用户之间的数据共享, 提出了一个基于区块链的不同群组用户之间的数据共享方案. 该方案支持匿名性和可追踪性. 任何一个用户很容易就可以验证共享数据的有效性, 其过程不需要和第三方审计员交互.

具有鲁棒性和可延展性的群组管理基础设施在需部署高密度设备的应用中起着重要作用, 而众包模式是实现群组管理的有效方法. Lin 等人的论文 “SecBCS: a secure and privacy-preserving blockchain-based crowdsourcing system” 指出广泛使用的众包模式存在安全隐患, 比如敏感信息的泄露、单点失败和不公平评判. 最近比较流行的解决众包模式中存在问题的方法是使用区块链技术. 然而, 现有的基于区块链技术的众包系统并没有考虑系统的安全性. 据此, 该论文研究了基于区块链技术众包系统中的安全隐私问题, 并提出了一个具体的解决方案, 称为 SecBCS. 论文最后基于 JUICE 对提出的方案进行模型实现.

引用格式: 仲盛, 黄欣沂. 区块链应用中的安全隐私专题简介. 中国科学: 信息科学, 2020, 50: 461–462, doi: 10.1360/SSI-2020-0031

在比特币网络中, 简化支付验证协议 (SPV) 允许轻量级设备参与其中, 且无需下载和存储比特币系统中的所有区块. 比特币中 SPV 节点通过比特币钱包软件对交易进行验证. 因此, 比特币钱包的安全性对 SPV 节点就显得非常重要了. 安全用户认证协议可以有效地解决 SPV 节点的安全缺陷. 最近, Park 等人提出一个适用于移动设备的双方可验证密钥交换协议, 并声称他们的方案能够抵抗多种攻击且能高效部署. Zhou 等人的论文 “A privacy preserving two-factor authentication protocol for the Bitcoin SPV nodes” 针对 Park 等人的协议进行安全分析, 发现他们的协议存在伪造攻击和智能卡被盗攻击, 且无法提供用户的隐私保护. 据此, 论文针对 SPV 节点提出一个适用于移动设备的高效安全用户认证协议. 该协议能够解决 Park 等人协议的安全问题. 最后, 通过对提出的协议进行性能分析, 指出该协议适用于比特币网络中的 SPV 节点.

比特币的核心技术是区块链协议, 为保证协议的安全性, 应分析其在具有网络延时的异步网络中的安全性. Wei 等人研究了长时间延时攻击对协议的影响, 但是他们的证明需要假设所有的矿工都是诚实的. Yuan 等人的论文 “Analysis of blockchain protocol against static adversarial miners corrupted by long delay attackers” 使用一个更强的模型, 对 Wei 等人的结果进行改进, 允许攻击者执行长时间延时攻击和合谋部分矿工. 论文提出一个分析收敛事件 (converge event) 的新方法, 并在提出的强模型下证明, 该方法的链增长 (chain growth)、公共前缀 (common prefix) 和链质量 (chain quality) 性质在合理的参数下依然成立.

Ni 等人的论文 “Analysis of bitcoin backbone protocol in the non-flat model” 在非平坦 (non-flat) 模型中分析了比特币的主干协议. 作者重新思考和定义了计算智力游戏答案的模型, 以便于刻画现实协议的执行. 在新模型中, 每一个参与者拥有不同的计算能力并有序独立的计算智力游戏的答案. 在分析比特币主干协议的安全性中, 该论文得到更好的结果. 除了大部分参与者是诚实的假设之外, 不需要任何额外的假设条件. 最后, 论文指出在该模型中, 可基于比特币骨干协议建立一个安全鲁棒的公共交易账本.