Contents lists available at ScienceDirect

Engineering

journal homepage: www.elsevier.com/locate/eng

Research
6G Requirements, Vision, and Enabling Technologies—Article

下一代无线网络中基于区块链的透明数据管理

沈学民[a]，刘栋骁[a,*]，黄橙[a]，薛靓[a]，尹涵[a]，庄卫华[a]，Rob Sun[b]，Bidi Ying[b]

[a] *Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON N2L 3G1, Canada*
[b] *Huawei Technologies Canada, Kanata, ON K2K 3J1, Canada*

ARTICLE INFO

Article history:
Received 31 December 2020
Revised 6 July 2021
Accepted 18 July 2021
Available online 6 October 2021

关键词
区块链
数据管理
去中心化
透明
隐私

摘要

未来第六代无线网络（6G）需要依赖丰富的数据实现网络智能化和自动化。在这种情况下，考虑到数据的异构性和动态性，基于区块链的去中心化的数据管理（DM）被认为是实现跨网络域的透明数据操作的潜在解决方案之一。然而，在6G网络中，不断增加的数据量和严格的数据隐私保护需求为平衡基于区块链的去中心化数据管理的透明、效率以及隐私需求带来巨大的技术挑战。本文中，首先，我们探索区块链的共识协议和可扩展机制，并讨论区块链构架下如何管理利益相关者的角色；其次，我们探讨针对数据管理利益相关者的认证与授权需求；再次，我们归类数据管理的隐私需求，并研究基于区块链的协同数据处理机制；随后，我们从上述三个方面探讨面向6G的基于区块链数据管理的研究问题和潜在解决方案；最后，我们对本文进行总结并讨论未来的研究方向。

1. 引言

无线网络的普及提供了无处不在的网络覆盖和无缝链接，这极大地影响了我们的生活和工作方式。伴随无线网络的不断发展，第六代无线网络（6G）将进一步整合异构接入和网络切片技术[1–2]，以支持具有动态服务质量需求的各类服务。更重要的是，网络智能不仅在改善网络资源利用方面扮演重要角色，同时在提供定制化服务和提升用户体验方面也意义重大[3]。

1.1. 面向6G的数据管理

丰富的用户数据和人工智能（AI）技术的进步是面向6G网络智能的核心。伴随大量终端设备被部署和连接，无线网络中的数据量越来越多，规模越来越大[4]。通过基于AI的数据处理，这些大数据对面向6G的高效网络管理具有重要价值。例如，可以利用不同接入点的用户轨迹和关联历史进行基于AI的网络流量预测和边缘内容缓存，以实现动态的网络资源分配[1,5]。因此，如何有效且高效地管理用户数据——数据管理（DM），包括在用户数据生命周期内从数据生成到删除的多种数据操作[6–7]——成为未来网络智能的关键推动因素。然而，6G网络的高动态性和异构性对数据管理提出四个需求。

（1）去中心化：数据管理需要多方数据利益相关者的协作，包括不同用户和设备（数据来源）、提供数据收集

* Corresponding author.
E-mail address: dongxiao.liu@uwaterloo.ca (D. Liu)

英文原文：Engineering 2022, 8(1): 74–85
引用本文：Xuemin (Sherman) Shen, Dongxiao Liu, Cheng Huang, Liang Xue, Han Yin, Weihua Zhuang, Rob Sun, Bidi Ying. Blockchain for Transparent Data Management Toward 6G. *Engineering*, https://doi.org/10.1016/j.eng.2021.10.002

和传输服务的移动运营商以及提供数据存储和处理服务的技术供应商（如边缘/云服务提供商）。这些利益相关者通常来自不同的网络域，他们很难仅通过单一数据管理权威进行协商，达成一致。因此，对于数据利益相关者来说，构建一个可以协同管理用户数据生命周期事件的去中心化构架十分必要[8]。

（2）透明：由于数据利益相关者之间缺乏相互信任，因此数据管理过程应该是透明且可验证的。数据拥有者应该知道执行在他们数据上的任何操作[9]。出于管理的目的，参与协作处理数据的利益相关者的“各自的责任”应该被明确界定且透明[10]。

（3）效率：数据管理利益相关者的异构性、不断增加的用户数据量和数据生命周期事件的复杂性引发对分布式构架设计、数据管理利益相关者的认证与授权（AA）管理以及数据处理机制三个方面的效率保障的广泛关注。

（4）隐私：数据管理中的隐私保护涉及数据利益相关者的身份隐私和个人数据的内容机密性。尽管具体的隐私需求随不同数据操作变化，但最新的隐私规范，比如欧盟通用数据保护规范（GDPR）[10]，规定了通用隐私保护条款。例如，用户可以完全控制对具有其可识别信息的数据的任何操作[11]。此外，应该提前制定用于定义利益相关者责任的数据使用协议并严格遵守。

目前，实现满足效率和隐私需求的去中心化透明数据管理仍然是一个艰巨的任务。

1.2. 基于区块链的数据管理

区块链由一个存储点到点（P2P）交易的账本组成[12]。区块链由网络分布式节点维护，每个（全）节点维护一个该账本的拷贝。从功能角度来看，区块链与传统的分布式数据库具有一些共同特征[13]，但区块链利用安全共识协议维护互不信任节点的账本的一致性。此外，区块链利用可编程性和智能合约技术控制账本更新[14]。

区块链对于面向6G的数据管理是一项潜力十足的技术，因为它满足其去中心化和透明的需求。首先，数据管理利益相关者可以将区块链作为可信共享存储来记录关键的数据管理事件[8,15]。每个数据管理利益相关者都可以维护一个共享账本的拷贝，无需依赖中心化的实体。其次，共享账本是透明的，且账本更新对相关区块链节点是可验证的。数据管理利益相关者可以设计智能合约进行各种数据操作的协同处理。区块链的优点引发了许多基于区块链数据管理方案[16–17]的最新讨论，这些方案着眼于未来智能网络[3,18]以及其他应用，如信息中心网络[7]、供应链管理[19]、物联网（IoT）[20–22]和智能医疗[23]。

鉴于区块链的去中心化和透明特性，基于区块链的解决方案可能导致实现数据管理效率和隐私保护需求的复杂性[24]。首先，在区块链节点上进行分布式数据存储会增加整体存储开销。为了维护共享账本的一致性，数据管理利益相关者通过共识协议进行交易和区块认证，这可能限制交易的吞吐量，增加数据处理负荷。其次，区块链存储透明导致链上数据对于相关区块链节点是可视的，这与用户数据的隐私需求相矛盾。为了解决效率和隐私问题，新的基于区块链的数据管理方案设计和实际应用还需要更多的探索。

1.3. 文章结构

本文中，我们讨论面向6G的基于区块链的数据管理。为了解决效率和隐私问题，我们总结了最新的研究进展和潜在解决方案。本文结构如下。

第2节研究针对数据管理的区块链构架设计。我们总结现有的区块链机制，比如高效的共识协议和混合链设计。此外，通过对比最新的基于区块链数据管理方案，我们讨论数据管理利益相关方如何作为区块链的组成部分。第3节，我们探索基于区块链的认证与授权机制，实现对数据管理利益相关方进行高效且隐私保护的身份管理。第4节，我们探讨基于区块链的数据处理机制。在明确基于区块链数据处理的隐私需求后，我们讨论链上/链下计算模型。同时，我们总结具有特定隐私保护需求的数据操作的研究成果，包括数据共享和数据分析。第5节，我们详细讨论基于区块链数据管理的构架设计、认证与授权以及数据处理方面的研究问题和潜在解决方案。最后，我们对本文进行总结并讨论未来研究方向。

2. 基于区块链数据管理的构架设计

区块链作为去中心化的透明构架可以用于面向6G的数据管理。然而，将区块链作为黑盒应用于数据管理并非易事。首先，区块链的特征是维护分布式节点存储和状态更新的一致性。实际应用中，由于节点之间的信任度差异极大，因此区块链可以支持不同的构架以平衡账本的安全和可扩展性。当区块链应用于数据管理时，有必要区分不同数据管理应用场景的需求。其次，由于参与数据管理的利益相关者的能力和动机各不相同，基于区块链的构架包含各种角色，比如矿工和客户。但目前如何在区块链中管理数据管理利益相关者的角色仍不清楚。

为了解决这一难题，我们探索两个基本问题：①适用于数据管理的区块链构架应该是怎样的？②数据管理利益

相关者在该构架中扮演什么角色？我们首先回顾现有的区块链构架在数据管理中的特点，然后讨论两个典型的基于区块链数据管理的应用场景：车联网（V2X）[25]和云/边缘计算。

2.1. 区块链构架

区块链构架可以粗略地分为两类：非许可链[14]和许可链[26]。非许可链主要由两类实体组成：矿工和客户[12]。非许可链使用加密货币激励实体在公共网络中进行自我组织。相反，许可链是一种自顶向下的构架，它主要包括三类实体：权威、矿工和客户。通常情况下，工业组织可以形成联盟，该联盟作为许可链的控制实体。矿工和客户在加入区块链之前必须获得现有联盟实体的同意。上述两种构架中，共识机制是维护账本一致性的基本要素。

在共识协议方面，非许可链相较于许可链必须抵御更多的恶意参与者。如果拥有绝大多数计算能力的矿工诚实地遵守工作量证明（PoW）共识协议[27]，比特币中区块链设计已经被证明是安全的。然而，当矿工数量很大时，该构架可能出现低交易吞吐率和高交易确认延迟的问题。许可链，比如Hyperledger Fabric [26]，依赖联盟委员会来提供成员管理和交易验证服务。这种自顶向下的构架对共识协议限制较少，可以采用实用的拜占庭容错协议（PBFT）或Raft协议。近来，为了进一步改善区块链可扩展性，新型区块链构架被提出。对于非许可链，Prism [28]和OHIE [29]是两种新型区块链构架，支持并行交易处理。它们将单链分解成多链，将矿工细分为多个角色以执行不同的任务。

尽管非许可链和许可链具有不同的性质，但大部分都支持两个极具吸引力的功能：分布式存储和智能合约。这意味着，计算机程序可以在分布式环境（区块链）下执行，这使得区块链适用于构建面向6G的数据管理平台[30–31]。

2.2. 基于区块链数据管理的应用场景

下面，我们提出两个典型的基于区块链数据管理的应用场景：车联网（V2X）和边缘/云计算。我们主要关注数据管理利益相关方如何参与维护区块链构架。

2.2.1. 车联网的基于区块链数据管理

车联网衍生出许多车载应用，比如车载信息娱乐和基于位置的服务[25,32–33]。为了为车联网中的行人和司机提供更加有效且高效的服务，车联网服务提供商必须协同通信并交换部分用户隐私信息。然而，该需求在当前车联网系统中并不容易得到满足，因为车辆相关数据由车联网服务提供商独立管理，且不恰当的数据共享可能导致严重的隐私信息泄露[34]，违背隐私规范要求。为了解决这个问题，区块链被引入车联网系统。这使得大量车联网服务提供商可以建立去中心化信任。特别是，车辆信息交换可以记录在区块链上。区块链允许第三方审计员追踪相关信息流动，预防潜在信息泄露。此外，对于不同的车联网服务，区块链记录的信息是不同的。这些信息可能包括车辆保险信息、司机驾照信息、车速和位置等。

一个基本的基于区块链的车联网包含以下利益相关方：车辆、路侧单元（RSU）、基站、服务提供商、边缘节点和云服务器。对于车联网服务来说，基于非许可链的数据管理构架和基于许可链的数据管理构架[34]的最大区别在于构建区块链的利益相关方不同。部分现有方案[30–31]依靠公有链作为车联网服务的第三方，例如，基于公钥基础设施（PKI）的车联网安全通信方案就依赖于公有链平台[30]。该方案中，车辆和其他利益相关方是以太坊的用户。它们可以从公有账本中读取/写入信息并触发已部署的智能合约。这种情况下，原始车联网的网络构架及其利益相关方不需要明显改变，但利益相关方需要与外部公有链进行通信。尽管基于非许可链的数据管理构架被认为是简单且有效的，但由于系统可扩展性和隐私方面的要求，无法适用于所有的车联网服务。非许可链平台是公开的，可以被任意一方访问。因此，部分数据可以发布在区块链上，如公钥证书和证书撤销列表（CRL），而其他数据应该受到保护，如个人驾驶记录。此外，非许可链平台数据处理延迟高，这使得非许可链构架很难适用于对时延要求高的车联网服务。

为了解决这些问题，许多研究将许可链引入车联网服务[35–42]。在这些解决方案中，区块链由车联网利益相关者自己维护。根据车联网的应用场景，维护区块链的利益相关方可以是车辆、路侧单元和云服务器。例如，移动边缘节点和路侧单元可以作为全节点维护许可链，因为它们具备强大的计算和存储能力。车辆通常作为轻节点，因为它们移动性强但资源有限。相较于基于非许可链的构架，基于许可链的构架通过控制区块链的矿工数量和采用混合共识协议实现更强的可扩展性，其代价是复杂的构架设计和安全模型。具体来说，大多数先进的构架都有一个前提，即车联网系统中存在根信任权威来初始化系统。

2.2.2. 云/边缘计算的基于区块链数据管理

基于云/边缘计算的数据管理构架建立在集中模型之上，具体来说，后端云服务提供商整合前端接口（比如移动电话）实现简单有效的数据处理和数据共享。然而，由

于第三方服务提供商缺乏过程的透明性，这种构架对于内部攻击来说是脆弱的。因此，云/边缘计算必须有一个更加透明的数据管理框架。该框架中，所有数据处理操作都能被审计，甚至恶意的内部攻击者可以被检测到。为了获得具有监控和审计能力的透明数据管理，区块链可以被引入基于云/边缘的数据管理架构。

在分层边缘计算或云际构架[43–44]中，区块链对于管理多域协作具有很大前景。近来，许多针对云计算的基于区块链数据管理的解决方案被提出，包括基于非许可链或许可链。一个基本的针对云计算的基于区块链数据管理主要包括以下利益相关方：用户、云服务器和应用服务提供商，而数据管理操作包括数据审计、数据共享、数据完整性检测和数据搜索。

大多数基于非许可链的云数据管理构架采用外部区块链平台[45–51]，因为它们对数据处理的吞吐量和时延没有很高的要求。区块链主要作为诚信账本存储额外信息，而大数据则被存储在云服务器上。由于在非许可链上处理数据代价较高，非许可链上不能执行复杂的数据操作，仅可执行轻量级操作，比如数据时间戳和操作记录追踪。链下数据管理操作仅在执行后被记录在链上。此外，数据加密是保护云存储数据或区块链存储数据隐私的通用方法。

针对基于许可链的云数据管理架构，区块链由授权的利益相关方管理，比如云服务器、边缘节点甚至用户[52–56]。许可链可以提升不同利益相关者的跨域信任。由于许可链的链上操作开销较低，因此链上可以执行较复杂的数据操作。此外，其数据隐私保护机制不局限于数据加密。由于授权的利益相关者控制链上数据，因此它们可以制定链上数据的访问策略。尽管这种构架具有很多优点，但它依赖于作为区块链管理者的授权利益相关者的可信度。如果这些利益相关者信任度下降，那么该构架的安全与隐私不能得到保障。

适用于数据管理的区块链构架如图1所示。基于不同的共识协议、分布式账本存储和智能合约，基于区块链的数据管理支持各种车联网和云/边缘应用。表1总结了适用于上述应用场景数据管理的区块链构架。

3. 基于区块链数据管理中的认证和授权

3.1. 数据管理利益相关者的认证与授权需求

认证与授权是基于区块链数据管理必不可少的组成要素[57]。它解决了数据管理的两个基本问题：你是谁和你能做什么。首先，数据管理可以有多个参与者，比如用

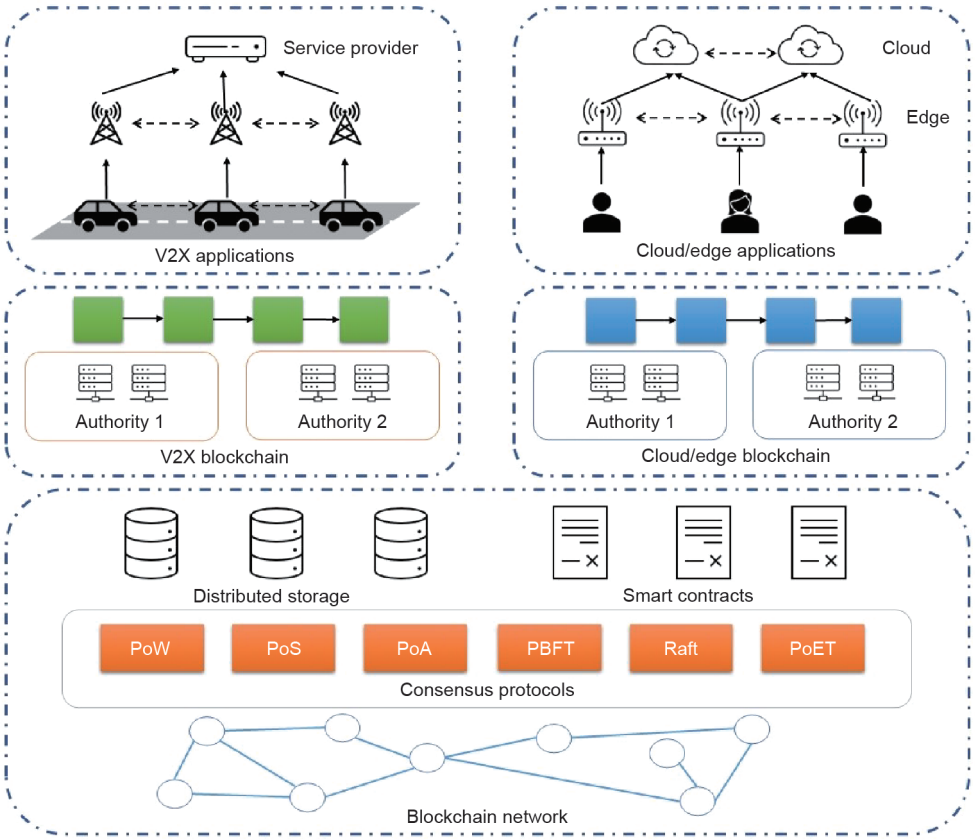

图1. 基于区块链的数据管理。PoS：持有量证明；PoA：权威证明；PoET：已用时间证明。

表1 基于区块链的数据管理构架——应用场景

Use case	Application	Blockchain architecture	Consensus protocol	Maintainer of blockchain
V2X	On-road infotainment and location-dependent services	Permissionless	PoW/PoS	Third-party
		Permissioned	PBFT/Raft	RSU and edge nodes
Cloud/edge computing	Data auditing, data sharing, and data searching	Permissionless	PoW/PoS	Third-party
		Permissioned	PBFT/Raft	User and cloud/edge server

户、存储节点和计算节点。认证帮助数据管理系统确认数据管理利益相关者的身份和准确的角色。其次，根据各自的角色，数据管理利益相关者被授以可执行的操作，比如读取数据和修改数据状态。除了上述基本功能，认证与授权还可以进一步帮助数据管理利益相关者建立安全机密的通信信道。此外，在任何争议中，基于认证与授权的不可否认性是确定数据管理利益相关者责任的关键。

面向6G的基于区块链数据管理对认证与授权机制提出了新的需求。

（1）分布式管理：由于不存在单一权威，数据管理的认证与授权机制应该由一组权威以透明的方式执行。

（2）效率和隐私：由于数据管理利益相关者的角色可以动态变化，因此基于区块链的认证与授权机制应该支持高效的证书更新和撤销。同时，为了实现条件的隐私保护，必要情况下，数据管理利益相关者的真实身份应该对特定应用场景保密。接下来，我们讨论现有的实现了透明、高效且隐私保护的基于区块链数据管理的认证与授权的研究工作。

3.2. 基于区块链的认证与授权

在复杂的数据管理环境中，不同利益相关者都可以为其用户生成身份，为对应数据操作进行授权，如图2所示[50]。这种模型中，由于利益相关者之间信息交换频繁，需要实现跨域认证与授权。但每个利益相关者都有自己的证书管理权威（CA），因此协同证书管理可能成为一个难题。部分利益相关者可能存在安全隐患，进而发布或使用假证书进行数据操作。为了减少跨域认证与授权的管理开销和安全风险，可以引入一个管理者进行集中身份管理，比如单一登入服务提供商，如图2所示[50]。然而，该模型需要数据管理利益相关者协商出统一的管理者，这在6G中并不总是适用。如图3所示，基于区块链的去中心化身份管理[50–52]，可以使利益相关者以透明的分布式的方式协同管理用户身份、认证用户和更新授权策略。具体来说，区块链由联盟委员会管理，它可以为外部服务提供商提供认证与授权服务。即使部分利益相关者存在安全隐患，对所有链上的成员更新和撤销操作仍然可追踪和可负责。

目前，已经有大量研究运用区块链增强认证与授权系统[58]。相较于传统的基于证书的认证与授权机制，基于区块链的机制被提出，以保证基于区块链数据管理的证书透明和撤销透明[59–60]。具体来说，证书权威向利益相关者和用户发布证书，同时一组利益相关者在公有链上更新自己的证书。链上证书的有效性不仅依赖于证书权威的安全，也依赖于这组利益相关者，大多数利益相关者必须是诚实的。除了关注证书透明，其他工作将区块链视为公开的、不可更改的证书生成、更新和撤销日志服务器，以解决利益相关者之间认证与授权管理的审计问题[61–62]。

与基于证书的认证与授权系统相反，自主身份管理是一种基于区块链的身份管理机制[63]。具体来说，该机制代替了依靠证书权威管理用户身份，用户自己可以通过区块链创建、存储、转发和撤销自己的身份证书。这种方式大大降低单一权威的单点故障风险。为了实现细粒度的数据访问控制，区块链可以结合基于属性的认证与授权机

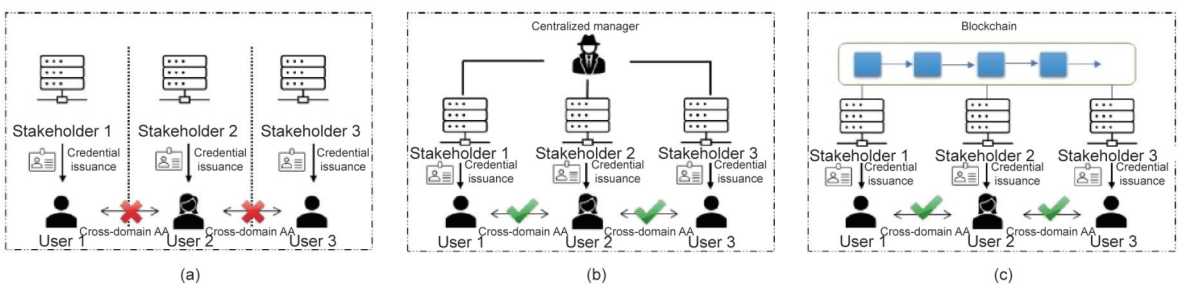

图2. 身份管理的演变——从独立到去中心化。（a）数据管理中的独立管理；（b）数据管理中的集中式身份管理；（c）数据管理中的去中心化身份管理。

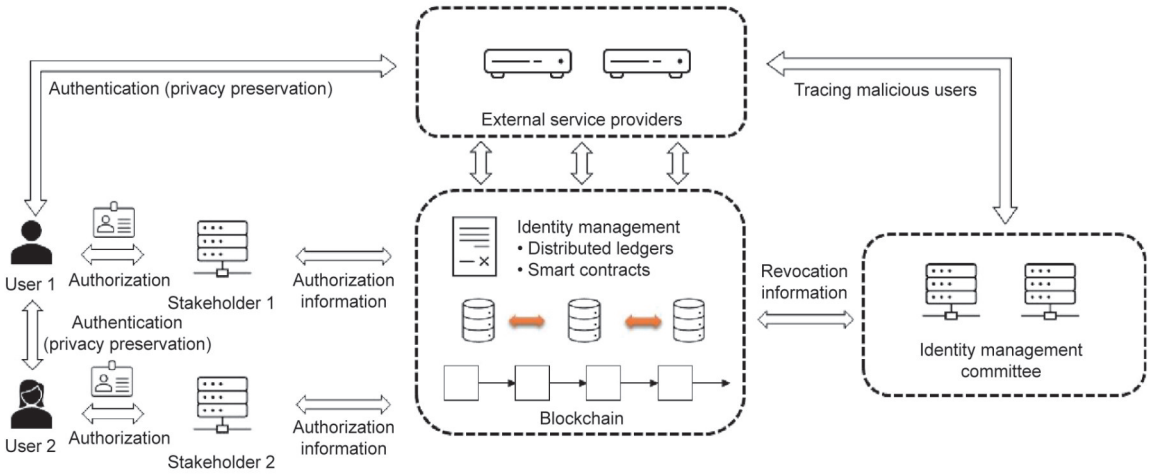

图3. 基于区块链的认证与授权的一般过程。

制，如基于属性的加密（ABE），将用户属性嵌入账本或智能合约中。用户通过自身属性可以访问数据，取回解密密钥[64]。此外，区块链结合变色龙哈希函数可以实现区块链中的动态属性更新[65]。

区块链在管理用户身份方面具有很大优势，它可以满足数据管理的不同安全属性。然而，区块链也可能导致隐私问题，因为所有存储在区块链上的信息都是透明的。因此，基于区块链的认证与授权方案可以结合隐私保护机制为数据管理提供隐私保护。其中，假名化是一个基本的机制。每个用户都可以为了认证与授权保留大量假名。区块链数据共享系统Ghostor隐藏了用户身份，但允许用户对远程存储数据进行完整性验证[66]。匿名可以通过“匿名分布式共享能力”技术实现。由于假名被用户存储在本地，如果数据较大时，管理将会很困难，因此考虑采用其他机制来保护基于区块链数据管理的用户身份隐私，比如群签名和环签名。通过群/环签名生成的用户的匿名身份可以被存储在用户端，用于跨应用的认证与授权。这种身份隐私保护机制已经被一些区块链平台所采用，如Moreno [67]。

群/环签名方案是在Fiat-Shamir方法的基础上建立的，它可以用于区块链上的自主身份管理[68]。匿名证书可以被授予不同的等级，从而激发更多的数据管理应用[69]。在这种情况下，该方案不仅可以保护身份隐私，也可以履行追踪恶意用户的责任。例如，在某些严格的条件下，基于区块链的认证与授权方案可以追踪用户身份[70–71]。单个或多个利益相关者可以利用零知识证明技术为其用户生成匿名证书。当用户表现出恶意行为时，利益相关者可以相应地追踪其身份。通过这种方式，隐私和问责需求同时得到满足。针对区块链的基于属性的访问控制，通用的隐私保护方法是通过设计属性隐藏的基于属性的加密方案隐藏访问策略[72]。该方法不同于以往的机制，它保护的是数据属性和策略而非用户身份。

4. 基于区块链数据管理中的数据处理

数据处理指在数据生命周期内的一系列操作[7–8]。在基于区块链的数据管理中，我们主要关注需要与多个数据管理利益相关者交互的数据操作，包括数据共享和协同数据分析。本节中，我们首先讨论一般隐私保护模型和计算模型的需求。针对这些需求，我们总结关于基于区块链的数据共享和数据分析的现有工作。

4.1. 隐私需求和隐私模型

针对在区块链数据管理中的数据处理，一般的隐私需求是控制数据泄露。具体来说，数据泄露可以由以下问题描述。

（1）数据的敏感性怎么样？首先，根据应用程序的不同，数据的敏感性可能存在很大差异。例如，金融应用中的用户身份数据具有较高的机密性，任何身份数据泄露都可能导致经济损失。其次，数据敏感性随数据量变化。例如，单次用户位置暴露可能导致的损失是有限的，但用户位置的持续暴露可能揭露用户的日常生活规律[73]。再次，数据敏感性随时间变化。许多类型的数据，比如法律文件[74]，存在“密封期”。数据在“密封期”内不应该被暴露。“密封期”结束后，该数据可以被公众或特定群体访问。

（2）数据泄露给谁？数据处理可能涉及各种各样的实体，它们可以被粗略地分为内部/外部参与者和区块链。内部参与者指参与数据处理的数据管理利益相关者。相

反，外部参与者指不参与数据处理的实体，如外部攻击者。在基于区块链的数据管理中，区块链的参与者具有共享视野。对此，区块链可以被看成一个用于数据公开的特殊实体。

从上述两个问题出发，基于区块链数据管理的隐私需求可以被划分为四个等级。

（1）来自用户匿名的隐私：数据处理前，要求将用户身份信息从数据库中分离出来。然而，具有强知识背景的数据处理器（比如，执行数据处理操作的实体）极有可能从数据库中恢复出用户身份信息。

（2）对外部参与者保密：敏感性较低的数据可以被数据处理器以明文的形式处理，但是不能暴露给外部参与者。该需求依赖于数据处理器的可信度。

（3）对内部参与者保密：对于敏感性高的数据，数据处理过程应该尽可能少地向数据处理器暴露信息，包括数据内容、用户身份和数据访问模式。

（4）对区块链保密：敏感数据不应该直接存储在区块链上。类似地，敏感数据操作不应该被智能合约执行。

在基于区块链的数据管理中，不同数据管理应用的隐私需求会随着数据敏感性和数据利益相关者的角色发生显著变化。因此，GDPR [10]没有规定具体的隐私需求，而是定义一般性原则。具体来说，它要求用户能够完全控制自身数据上的数据管理操作。

内部参与者，比如数据管理者和数据处理器，必须与用户就数据使用规则达成一致，并在数据处理过程中严格遵守该协议。同时，禁止向外部参与者共享未经授权的数据。

由于隐私需求有时是模糊的，因此必须设计隐私模型。隐私模型可以帮助用户、数据管理系统设计者和监管者以可执行和可实现的方式理解隐私规范。数据流图是一种优秀的数据管理建模方法。数据流图与软件工程中的过程流程图类似，它可以整合GDPR元素和数据生命周期事件[75]。不同于基于数据生命周期事件的模型，数据管理利益相关者的资源和能力需求可以被用于实现符合GDPR的数据管理[76]。此外，基于区块链的数据管理中，可以采用可执行隐私模型自动管理智能合约涉及的云数据操作[77–78]。

4.2. 效率需求和计算模型

关于区块链数据管理中的数据共享和数据分析，一个简单的方法是一切存储和计算都在链上进行。这意味着，需要将整个数据库存储在区块链上，并通过智能合约进行数据处理。这需要惊人的存储空间，并且会给区块链参与者带来沉重的计算负荷。为了解决这个问题，可以引入链下存储/计算节点。它们可以更高效地存储和处理数据，并仅将关键信息上传到区块链上。这一范式被称为链上/链下模型[79]。

对于一般的链上/链下模型，外部数据存储提供商可以将数据的散列值存储在区块链上[80]。由于链上的散列值不能被修改，因此该模型可以确保所有链下数据存储的完整性。此外，该方法还可以避免将隐私数据直接暴露在区块链上。散列法依赖于外部数据存储提供商的可信的数据操作。在基于区块链的数据管理中，允许为存储提供商设置更弱的安全假设，为验证链下数据操作的正确性设计更灵活的链上验证系统。例如，多个数据记录的聚合可以通过链下云服务器计算，然后仅将可验证的计算结果发送至区块链。下面我们讨论关于构建链上/链下模型的相关研究工作。链上/链下模型的主要需求是具备可验证的链下执行，可以通过零知识简洁的非交互式证明（SNARG）和可信执行环境（TEE）构建链上/链下模型。

在SNARG系统中，证明者可以说服验证者，使其相信存在一个适用于公共关系的秘密。这种关系可以用代数电路表示，用于一般可验证计算[81]。

SNARG的验证过程是高效的，并且该过程不会直接暴露计算的输入和输出，可以做到隐私保护。因此，SNARG被广泛地应用于为基于区块链的数据管理构建链上/链下计算模型[24]。其验证效率的代价是公共参数的可信建立和证明者的昂贵计算开销。因此，有必要为SNARG合理地设置通用的或可更新的公共参数[82]，或者使用安全多方计算协议为SNARG系统生成公共参数。此外，针对恶意的内部参与者，SNARG无法保证数据隐私。数据处理器必须能够访问原始数据，这对于数据管理应用来说并不总是可行。

可验证执行环境（TEE），比如英特尔软件防护扩展（SGX）[83]，提供了另一种证明计算的方法。TEE中，代码在执行之前被加载到一个安全的enclave，enclave是具有受保护内存的安全硬件。为了保证加载的代码和数据可信，SGX提供远程证明服务，即TEE生成一个对远程证明服务的证明请求，以保证代码执行的完整性和准确性。不同于SNARG，TEE不需要公共参数的可信建立，它可以更高效地生成计算证明。因此，TEE作为一个可信且被认证的链下计算单元，可以协助设计链上/链下计算模型[84–85]。此外，通过集成密钥管理器，基于TEE的解决方案可以在enclave和外部环境之间实现经过认证和加密的通信，从而抵御恶意的数据处理器，提供隐私保护。然而，TEE在实际应用中存在一些挑战：首先，TEE的全面的形

式化安全分析[86]仍处于讨论中；其次，远程证明很大程度上依赖于服务提供商，该服务提供商可能是区块链环境中的单一信任节点。

除了使用SNARG或TEE证明计算结果以外，也可以使用博弈论在多个链下资源提供者之间建立竞争关系，以达到消除欺骗的目的[87]。例如，给两个云服务器分配相同的计算任务。通过设置适当的金钱奖励和惩罚，可以激励两个云服务器正确地完成计算任务。

4.3. 基于区块链的数据处理机制

基于SNARG/TEE/双服务器模型的链上/链下模型为数据处理任务提供了一般性解决方法。然而，对于特定的任务，需要特殊的设计策略（如新型数据结构）以满足隐私和效率需求。

4.3.1. 数据共享

在基于区块链的数据管理中收集和存储数据时，数据共享和数据交易对于支持数据密集型应用来说十分重要[18,88]。

使用不同的技术可以实现数据共享不同的隐私需求。数据拥有者和接收者的身份隐私可以通过假名[89]或基于群签名的匿名证书实现。数据加密机制和密钥管理技术可以用于保护链上数据的机密性。对于数据共享中的细粒度访问控制，可以使用基于属性的加密和功能加密[90–91]。数据加密密钥或密文可以决定访问策略。不同于基于加密密钥管理的方法，信任评价管理[92]也可以集成到数据共享中。在信任评价管理中，数据发送者和接收者可以评价数据共享过程[93]。累计评价分数可以作为访问评估的标准。例如，研究者为边缘数据共享设计了一种协作证明共识协议[94]。该协议中，基于协作的名誉被量化。近来，研究者也在考虑数据共享中GDPR需求[95–96]。具体来说，一个基于区块链的解决方案可以使用户完全控制自己的个人数据，这满足基于许可的数据管理的GDPR需求。

数据拥有者经常将自身数据外包给第三方存储提供商，比如云服务器，依赖存储提供商管理自身数据。在这种模型中，区块链可以作为数据共享过程中的可信审计者[97]。为了降低数据拥有者的密钥管理开销，可以采用一个可信的密钥管理器进行数据加密和解密。门限密码，如(t,n) Paillier密码（其中，t是阈值，n是共享秘密的数量）可以用于保护云存储数据和区块链共享数据[98]。与此同时，必须安全地选择一组委员会成员进行密钥管理。区块链可以用于管理云存储上的数据修改[46]，修改过程由信任权威（TA）和智能合约共同完成。

除了数据共享，数据交易可以进一步挖掘数据价值。比如，有研究者提出了一种适用于金融机构的基于区块链的身份交换方案[99]。该方案中，SNARG以一种隐私保护的方式证明身份的真实性。TEE则可以用于建立一个数据交易平台[100–101]，该平台既维护买卖双方的公平性，又保障链上数据处理的隐私[102]。

4.3.2. 数据分析

区块链可以支持智能6G网络中的各种数据分析任务[103]。文献[104]提出一种基于区块链的学习框架，它结合Paillier门限算法实现模型参数更新的安全计算。另一种重要的数据分析机制是支持灵活的查询。对于存储在区块链上的数据，查询应该是高效的，其正确性可以被低代价的方式验证[13]，其中，针对区块间或跨区块查询，可以生成认证的数据结构。为了维护区块链上的数据隐私，可以使用可搜索加密链上的数据[105]，然后构建智能合约进行索引查询，其查询结果可验证。当搜索基于位置的数据时，可以建立基于范围的可搜索索引[106]。当数据存储在链下时，数据拥有者可以通过SNARG或密码累加器建立数据索引的链上认证系统。通过这种方法，查询操作可以在链下执行，查询结果可以在链上认证。结合数据库查询技术可以支持更多可验证的查询[107]。

由于区块链的透明性和不可变性，它本质上可以作为一个日志系统[108–109]。这意味着，存储在区块链上的数据可以用于事件驱动的系统调试和分析。为了支持细粒度的数据溯源操作，可以在原始区块链数据的基础上建立数据索引[13,110]。同时，可以利用区块链为数据管理构建日志系统。文献[111]提出轻量级的区块链日志记录机制，该机制采用一种面向数据密集型应用的新型日志存储结构。为了实现跨链通信，跨链互操作性得到了进一步研究[112]。相较于直接将区块链应用于日志存储，链下存储敏感日志数据可以减少链上开销，防止隐私泄露。特别是，文献[113]提出的一种物联网数据溯源方案。利用SNARG可以将溯源数据简洁地存储在每个网络管理员处，同时结合简洁的区块链认证系统进行跨域网络溯源查询。密码累加器可以作为单独的日志服务器为正确的日志更新提供证明，正如文献[114]中关于证书透明的讨论一样。表2总结了基于区块链的隐私保护数据处理的相关工作[24,84,87,89–91,96,100,104–105,108,115]。

5. 研究问题和潜在解决方案

尽管基于区块链的解决方案对于研究面向6G的数据

表2 区块链中的隐私保护数据处理概要

Design goals	References	Functionalities	Privacy guarantee
Computation model	[24]	Design a tool chain from SNARG to compile an off-chain program into an Ethereum smart contract	Achieve program execution privacy against the blockchain
	[84]	Design an on-/off-chain computation framework from TEE	Achieve program execution privacy against the blockchain
	[87]	Design a two-server model and use game theory to achieve verifiable computations	NA
Data sharing	[89]	Data sharing on the blockchain	Achieve on-chain data confidentiality and identity privacy for senders/receivers
	[90,91,115]	Data sharing on the blockchain with access control	Achieve data confidentiality and fine-grained access control
	[96]	Data sharing on the blockchain with GDPR compliance	Achieve on-chain data confidentiality and consent-based access control
	[100]	TEE-assisted data trading on the blockchain	Achieve data confidentiality against buyers by only revealing data analysis results
Data analytics	[104]	Blockchain-based learning framework	Achieve confidentiality of local gradients
	[105]	Blockchain-based data search	Achieve on-chain data and index confidentiality
	[108]	Blockchain-based data provenance framework	Achieve pseudonymity for data subjects and on-chain data confidentiality

NA: not applicable.

管理具有很大的潜力，但仍存在许多尚未解决的研究挑战。本节中，我们从三个方面详细讨论基于区块链数据管理的研究问题和潜在解决方案，包括基于区块链数据管理的构架设计、认证与授权以及数据处理。

5.1. 基于区块链数据管理的构架设计

虽然目前已经有许多针对数据管理的区块链构架，但大多数都是为应用设计的，而且与数据管理构架设计相关的各种挑战仍然存在，如下所示。

（1）激励和管理机制设计：非许可链对参与者采用金钱激励，而许可链则依赖于联盟委员会管理程序。事实上，面向6G的数据管理利益相关者是高度异构的，它们可以拥有不同的能力、利益考虑和管理架构。因此，如何为基于非许可链的数据管理设计激励机制，以及为基于许可链的数据管理设计管理规则仍然是一个具有挑战性的问题。多项技术，如博弈论和门限密码，可以被用于提供有效的群体和组织行为管理。

（2）区块链构架与网络切片：网络功能虚拟化（NFV）支持在通信网络中相同物理基础设施下的资源灵活共享。NFV被认为将在未来无线网络中扮演重要角色[1]。在NFV中，一个网络切片可以包含来自多个物理资源提供商的一组虚拟化功能。网络切片可以由本地或集中式软件定义网络（SDN）控制器管理，这使得数据管理变得更加复杂。为了管理虚拟化的网络功能中的数据流动，数据管理构架设计应该考虑新的6G利益相关者角色，比如第三方资源提供商和基于云的切片管理者。随着支持NFV的6G业务模式和实施细节在未来变得更加清晰，它们对数据管理构架设计的影响值得被进一步研究。

（3）混合区块链构架设计：针对数据管理的区块链构架是基于许可链或非许可链设计的。这两种构架都具有自身的优势与劣势，它们的核心组成部分是共识协议，共识协议影响系统的安全和可扩展性。为了在满足安全需求的情况下进一步提高系统可扩展性，应该采用灵活的混合区块链构架，该构架支持根据数据管理中的不同应用需求切换共识协议。此外，由于区块链在面向6G的数据管理的新信息基础设施中发挥着关键作用，因此区块链可以成为提供插件式数据管理构架设计[26]的一种潜在解决方案，该框架集成了新兴技术，如轻量级客户[116]和无状态区块链[117]。

（4）高效的跨链互操作与隐私保护：当前的数据管理构架仅基于单个账本设计，没有充分考虑跨链互操作。对于多个应用的数据管理，可采用异构区块链构架[118]。每个应用都可以构建自己的子链，管理自己的数据，实现隐私保护。这种方式与许可链中的秘密信道概念类似。未来需要进一步研究支持高效的跨链互操作的新型数据管理区块链构架，尤其是从隐私保护的角度出发。分层的区块链构架可以提供不同的共识协议，实现跨链通信管理。此外，还可以设置跨链操作的代理节点。通过对代理节点的

身份管理，促使跨链通信安全进行。

5.2. 基于区块链数据管理的认证与授权

尽管基于区块链的认证与授权机制有许多优点，但也带来了一些有待解决的效率和隐私问题。

（1）轻量级的认证与授权：基于区块链的认证与授权方案和传统的认证与授权方案的主要不同点在于用户仅需上传必要信息至区块链就可以自主维护身份信息。在多个利益相关者共存的复杂数据管理构架中，具有有限计算能力和存储能力的用户可能在不同的应用场景中拥有不同的身份证书。与此同时，区块链的存储资源和计算资源十分昂贵。因此，如何实现基于区块链的轻量级身份管理成为面向6G的数据管理的重要课题。一个可能的解决方案是利用外部证书服务器进行证书管理。为了使用户能够完全控制自己的证书，还应该实现额外的安全保障，如基于密码累加器的可验证证书更新[9]和基于TEE的证书管理。

（2）分布式认证与授权和动态更新：为了进一步消除对单一实体的信任需求，关键的认证与授权操作应该由一组密钥管理器执行，比如分布式证书分发和撤销[70]。这种模式涉及密钥管理器之间的大量通信，并且需要有效的激励机制来管理它们的行为。

门限密码可以用于降低密钥管理器的计算负荷。同时，密钥管理器的成员资格可以随时间变化，因此需要经常更新。当密钥管理器集发生变化时，应该保证身份证书的前向安全和后向安全。这意味着，如何实现安全高效的密钥管理器更新成为一个具有挑战性的问题。一个潜在的解决方案是主动秘密共享技术[119]。该方案中，密钥管理器之间的共享秘密可以经常更新。关键的管理操作也可以在安全的硬件执行环境下进行。

（3）平衡认证与授权中的隐私和责任：数据管理中的身份隐私可以有细粒度的分级，仅在隐私规范的要求下显示必要的身份信息，如组织成员资格和利益相关者属性。对于不同的数据管理应用场景，灵活的隐私保护建模可以结合智能合约来实现认证与授权中的隐私管理[77]。然而，在面向6G的数据管理中，身份隐私保护不应该是无条件的。当发生争议时，基于区块链的认证与授权机制应该能恢复利益相关者的真实身份，这可以通过门限加密技术实现。在这种情况下，需要一个明确的标准用于决定恢复利益相关者身份的条件和方式。可以使用专门的监督框架设计一个分层的身份管理委员会。

5.3. 基于区块链数据管理中的数据处理

目前，对于基于区块链的数据管理已经有了广泛研究，包括基于SNARG/TEE的通用计算解决方案以及针对数据共享和数据分析的专门设计。然而，对于面向6G的基于区块链的数据管理，如何平衡功能、效率和隐私的问题，仍然存在以下技术挑战。

（1）链上过程设计：区块链为数据管理利益相关者提供一个可信赖的数据管理过程的共享视角。由于链上的存储和计算资源有限且可能导致的隐私问题，数据管理利益相关者必须谨慎决定共享什么信息。应该共享和不应该共享的信息可能存在非常细微的差别，这些信息可能包含用于完整性验证的原始数据散列值、数据管理生命周期事件的日志或者仅仅是数据管理操作的存在证明。考虑到效率和隐私问题，应该只共享关键信息，而且这些信息应该选择性地暴露给必要参与者[69]。同时，也存在链上数据需要被移除的情况。可编辑区块链技术是处理该情况的一种潜在方案。

（2）隐私模型设计：基于区块链的数据管理因其在各种应用中的异构的动态的参与者而变得复杂，这可能导致隐私需求快速变化[74]。因此，应考虑在隐私规范下进行隐私建模和评估，以便在区块链上实现灵活的隐私管理[77]。

（3）数据处理的模块化设计：许多现有设计可以为不同数据管理操作提供隐私保护。例如，SNARG可以支持实现简洁的链上可验证的一般代数计算，TEE可以高效地进行可验证哈希计算，可搜索加密可以为不同的查询操作提供专门的设计。事实上，一个数据管理实例可能导致多个数据操作，基于单一技术的解决方案不能同时满足效率和隐私需求。模块化设计策略[120]是一个潜在的解决方法，它将数据操作，如关键字查询和身份管理[121]，通过不同技术进行有效实例化。该策略需要全面了解不同的可验证计算系统的特点。通用的可组合安全模型[122]可以用于分析系统安全。

（4）自动化VS透明与责任：隐私保护条款规定，用户有权反对关于自身数据的自动决策，这可能与区块链自动化特性[11]和基于AI的决策相违背。然而，对于基于区块链数据管理中的AI辅助决策过程，通常很难实现透明和问责[9]。一个可能的解决方案是设计高效的算法直接评估自动化过程的输出。同时，应该向用户明确解释自动过程对用户数据的影响，并授予用户反对的权利，以防范隐私问题。对于协同数据处理，重要的是通过建立数据管理操作溯源机制和取证机制，实现对所涉及的数据管理利益相关者进行联合管理。

6. 结论

本文中，我们研究了面向6G的基于区块链的数据管理，强调其去中心化和透明两大优点。通过识别效率和隐私方面的挑战，我们专注于探讨数据管理构架设计、数据管理利益相关者的认证与授权以及基于区块链的数据处理。

为了探索在基于区块链的去中心化数据管理中平衡透明、效率和隐私要求的潜在解决方案，以下问题值得进一步研究。①可以讨论网络虚拟化对数据管理构架设计的影响。基于区块链的数据管理需要一个灵活且通用的构架，该构架具有高效的共识协议、链间可操作性和快速的面向服务的配置。②需要进一步设计可动态更新的轻量级分布式认证与授权机制，从而在基于区块链数据管理的认证与授权中，取得隐私和安全的平衡。③应该实现一个满足不同数据管理操作中的隐私需求的可执行隐私模型，并在该隐私模型下探讨隐私保护的数据处理技术的模块化集成。

Acknowledgements

This work was supported by research grants from Huawei Technologies Canada and from the Natural Sciences and Engineering Research Council (NSERC) of Canada.

Compliance with ethics guidelines

Xuemin (Sherman) Shen, Dongxiao Liu, Cheng Huang, Liang Xue, Han Yin,Weihua Zhuang, Rob Sun, and Bidi Ying declare that they have no conflict of interest or financial conflicts to disclose.

References

[1] Shen X, Gao J, Wu W, Lyu K, Li M, Zhuang W, et al. AI-assisted network-slicingbased next-generation wireless networks. IEEE Open J Veh Technol2020;1:45–66.
[2] Wu W, Chen N, Zhou C, Li M, Shen X, Zhuang W, et al. Dynamic RAN slicing forservice-oriented vehicular networks via constrained learning. IEEE J Sel AreasCommun 2021;39(7):2076–89.
[3] Dai Y, Xu D, Maharjan S, Chen Z, He Q, Zhang Y. Blockchain and deepreinforcement learning empowered intelligent 5G beyond. IEEE Netw2019;33(3):10–7.
[4] Dai HN, Wong RCW, Wang H, Zheng Z, Vasilakos AV. Big data analytics forlarge-scale wireless networks: challenges and opportunities. ACM ComputSurv 2019;52(5):1–36.
[5] Zhou C, Wu W, He H, Yang P, Lyu F, Cheng N, et al. Deep reinforcementlearning for delay-oriented IoT task scheduling in space–air–groundintegrated network. IEEE Trans Wirel Commun 2021;20(2):911–25.
[6] Shen X, Huang C, Liu D, Xue L, Zhuang W, Sun S, et al. Data management forfuture wireless networks: architecture, privacy preservation, and regulation.IEEE Netw 2021;35(1):8–15.
[7] Li R, Asaeda H. A blockchain-based data life cycle protection framework forinformation-centric networks. IEEE Commun Mag 2019;57(6):20–5.
[8] Freund GP, Fagundes PB, de Macedo DDJ. An analysis of blockchain and GDPRunder the data lifecycle perspective. Mob Netw Appl 2020;26(2):266–76.
[9] Abiteboul S, Stoyanovich J. Transparency, fairness, data protection, neutrality:data management challenges in the face of new regulation. J Data Inf Qual2019;11(3):1–9.
[10] General Data Protection Regulation [Internet]. Brussel: EuropeanCommission; [cited 2020 Dec 24]. Available from: https://gdpr-info.eu/.
[11] BlockchainHerian R., GDPR, and fantasies of data sovereignty. Law InnovTechnol 2020;12(1):156–74.
[12] Nakamoto S. Bitcoin: a peer-to-peer electronic cash system. Report. Satoshi:Nakamoto Instityte; 2008.
[13] Xu C, Zhang C, Xu J. vChain: enabling verifiable boolean range queries overblockchain databases. In: Proceedings of the 2019 International Conferenceon Management of Data; 2019 Jun 30–Jul 5; Amsterdam, the Netherlands;2019. p. 141–58.
[14] Wood G. Ethereum: a secure decentralised generalised transactionledger. Report Ethereum Project; 2014.
[15] Vo HT, Kundu A, Mohania MK. Research directions in blockchain datamanagement and analytics. In: Proceedings of the 21st InternationalConference on Extending Database Technology (EDBT); 2018 Mar 26–29;Vienna, Austria; 2018. p. 445–8.
[16] Zyskind G, Nathan O, Pentland AS. Decentralizing privacy: using blockchainto protect personal data. In: Proceedings of 2015 IEEE Security and PrivacyWorkshops; 2015 May 21–22; San Jose, CA, USA; 2015. p. 180–84.
[17] Deepa N, Pham QV, Nguyen DC, Bhattacharya S, Prabadevi B, Gadekallu TR,et al. A survey on blockchain for big data: approaches, opportunities, andfuture directions. 2020. arXiv:2009.00858.
[18] Zhang G, Li T, Li Y, Hui P, Jin D. Blockchain-based data sharing system for AIpowerednetwork operations. J Commun Inf Netw 2018;3(3):1–8.
[19] Wu H, Cao J, Yang Y, Tung CL, Jiang S, Tang B, et al. Data management insupply chain using blockchain: challenges and a case study. In: Proceedingsof 2019 28th International Conference on Computer Communication andNetworks; 2019 Jul 29–Aug 1; Valencia, Spain; 2019. p. 1–8.
[20] Oktian YE, Lee SG, Lee BG. Blockchain-based continued integrity service forIoT big data management: a comprehensive design. Electronics 2020;9(9):1434.
[21] Shi P, Wang H, Yang S, Chen C, Yang W. Blockchain-based trusted data sharingamong trusted stakeholders in IoT. Softw Pract Exper 2021;51(10):2051–64.
[22] Xiong Z, Zhang Y, Luong NC, Niyato D, Wang P, Guizani N, et al. The best ofboth worlds: a general architecture for data management in blockchainenabledInternet-of-Things. IEEE Netw 2020;34(1):166–73.
[23] Shi S, He D, Li L, Kumar N, Khan MK, Choo KKR. Applications of blockchain inensuring the security and privacy of electronic health record systems: asurvey. Comput Secur 2020;97:101966.
[24] Eberhardt J, Tai S. ZoKrates-scalable privacy-preserving off-chaincomputations. In: Proceedings of 2018 IEEE International Conference onInternet of Things and IEEE Green Computing and Communications and IEEECyber, Physical and Social Computing and IEEE Smart Data; 2018 Jul 30–Aug3; Halifax, NS, Canada; 2018. p. 1084–91.
[25] Abboud K, Omar HA, Zhuang W. Interworking of DSRC and cellular networktechnologies for V2X communications: a survey. IEEE Tran Veh Technol2016;65(12):9457–70.
[26] Androulaki E, Barger A, Bortnikov V, Cachin C, Christidis K, De Caro A, et al. Hyperledger fabric: a distributed operating system for permissionedblockchains. In: Proceedings of the Thirteenth EuroSys Conference; 2018Apr 23–26; Porto, Portugal; 2018. p. 1–15.
[27] Garay J, Kiayias A, Leonardos N. The Bitcoin backbone protocol: analysis andapplications. In: Proceedings of EUROCRYPT 2015; 2015 Apr 26–30; Sofia,Bulgaria; 2015. p. 281–310.
[28] Bagaria V, Kannan S, Tse D, Fanti G, Viswanath P. Prism: deconstructing theblockchain to approach physical limits. In: Proceedings of the 2019

ACMSIGSAC Conference on Computer and Communications Security; 2019 Nov11–15; London, UK; 2019. p. 585–602.
[29] Yu H, Nikolic´ I, Hou R, Saxena P. OHIE: blockchain scaling made simple. In:Proceedings of IEEE Symposium on Security and Privacy; 2020 May 18–21;San Francisco, CA, USA; 2020. p. 90–105.
[30] Lin C, He D, Huang X, Kumar N, Choo KKR. BCPPA: a blockchain-basedconditional privacy-preserving authentication protocol for vehicular ad hocnetworks. IEEE Trans Intell Transp Syst. In press.
[31] Li M, Weng J, Yang A, Liu JN, Lin X. Toward blockchain-based fair andanonymous ad dissemination in vehicular networks. IEEE Trans Veh Techol2019;68(11):11248–59.
[32] Cheng HT, Shan H, Zhuang W. Infotainment and road safety service support invehicular networking: from a communication perspective. Mech Syst SignalProcess 2011;25(6):2020–38.
[33] Li M, Zhu L, Lin X. Efficient and privacy-preserving carpooling usingblockchain-assisted vehicular fog computing. IEEE Internet Things J 2018;6(3):4573–84.
[34] Huang C, Lu R, Ni J, Shen X. DAPA: a decentralized, accountable, and privacypreservingarchitecture for car sharing services. IEEE Trans Veh Technol2020;69(5):4869–82.
[35] Aujla GS, Singh A, Singh M, Sharma S, Kumar N, Choo KKR. BloCkEd: blockchain-based secure data processing framework in edge envisioned V2Xenvironment. IEEE Trans Veh Technol 2020;69(6):5850–63.
[36] Jameel F, Javed MA, Zeadally S, Jäntti R. Efficient mining cluster selection forblockchain-based cellular V2X communications. IEEE Trans Intell Transp Syst2021;22(7):4064–72.
[37] Rawat DB, Doku R, Adebayo A, Bajracharya C, Kamhoua C. Blockchain enablednamed data networking for secure vehicle-to-everything communications.IEEE Netw 2020;34(5):185–9.
[38] Yang Z, Yang K, Lei L, Zheng K, Leung VCM. Blockchain-based decentralizedtrust management in vehicular networks. IEEE Internet Things J 2018;6(2):1495–505.
[39] Su Z, Wang Y, Xu Q, Zhang N. LVBS: lightweight vehicular blockchain forsecure data sharing in disaster rescue. IEEE Trans Dependable Secur Comput.In press.
[40] Lin X, Wu J, Mumtaz S, Garg S, Li J, Guizani M. Blockchain-based on-demandcomputing resource trading in IoV-assisted smart city. IEEE Trans Emerg TopComput. In press.
[41] Li C, Fu Y, Yu FR, Luan TH, Zhang Y. Vehicle position correction: a vehicularblockchain networks-based GPS error sharing framework. IEEE Trans IntellTransp Syst 20201;22(2):898–912.
[42] Qian LP, Wu Y, Xu X, Ji B, Shi Z, Jia W. Distributed charging-recordmanagement for electric vehicle networks via blockchain. IEEE InternetThings J 2021;8(4):2150–62.
[43] Yang H, Liang Y, Yuan J, Yao Q, Yu A, Zhang J. Distributed blockchain-basedtrusted multidomain collaboration for mobile edge computing in 5G andbeyond. IEEE Trans Ind Inform 2020;16(11):7094–104.
[44] Yang H, Yuan J, Yao H, Yao Q, Yu A, Zhang J. Blockchain-based hierarchicaltrust networking for JointCloud. IEEE Internet Things J 2020;7 (3):1667–77.
[45] Xu Y, Zhang C, Wang G, Qin Z, Zeng Q. A blockchain-enabled deduplicatabledata auditing mechanism for network storage services. IEEE Trans Emerg TopComput. In press.
[46] Zhu L, Wu Y, Gai K, Choo KKR. Controllable and trustworthy blockchain-basedcloud data management. Future Gener Comput Syst 2019;91:527–35.
[47] Chen L, Lee WK, Chang CC, Choo KKR, Zhang N. Blockchain based searchableencryption for electronic health record sharing. Future Gener Comput Syst2019;95:420–9.
[48] Zhang Y, Xu C, Cheng N, Li H, Yang H, Shen X. Chronos+ : an accurateblockchain-based time-stamping scheme for cloud storage. IEEE Trans ServComput 2020;13(2):216–29.
[49] Zhang Y, Xu C, Lin X, Shen X. Blockchain-based public integrity verification forcloud storage against procrastinating auditors. IEEE Trans Cloud Comput2021;9(3):92337.
[50] Liu Y, He D, Obaidat MS, Kumar N, Khan MK, Choo KKR. Blockchain-basedidentity management systems: a review. J Netw Comput Appl2020; 166:102731.
[51] Wang J, Wu L, Choo KKR, He D. Blockchain-based anonymous authenticationwith key management for smart grid edge computing infrastructure. IEEETrans Ind Inform 2020;16(3):1984–92.
[52] Shen M, Liu H, Zhu L, Xu K, Yu H, Du X, et al. Blockchain-assisted secure deviceauthentication for cross-domain industrial IoT. IEEE J Sel Areas Commun2020;38(5):942–54.
[53] Yang M, Zhu T, Liang K, Zhou W, Deng RH. A blockchain-based locationprivacy-preserving crowdsensing system. Future Gener Comput Syst2019;94:408–18.
[54] Tosh D, Shetty S, Liang X, Kamhoua C, Njilla LL. Data provenance in the cloud:a blockchain-based approach. IEEE Consum Electron Mag 2019;8(4): 38–44.
[55] Rahman MS, Omar AAL, Bhuiyan MZA, Basu A, Kiyomoto S, Wang G. Accountable cross-border data sharing using blockchain under relaxed trustassumption. IEEE Trans Eng Manag 2020;67(4):1476–86.
[56] Liang W, Fan Y, Li KC, Zhang D, Gaudiot JL. Secure data storage and recovery inindustrial blockchain network environments. IEEE Trans Ind Inform 2020;16(10):6543–52.
[57] Gilani K, Bertin E, Hatin J, Crespi N. A survey on blockchain-based identitymanagement and decentralized privacy for personal data. In: Proceedings of2020 2nd Conference on Blockchain Research & Applications for InnovativeNetworks and Services (BRAINS); 2020 Sep 28–30; Paris, France; 2020. p. 97–101.
[58] Patsonakis C, Samari K, Roussopoulos M, Kiayias A. Towards a smart contractbased, decentralized, public-key infrastructure. In: Proceedings ofInternational Conference on Cryptology and Network Security; 2017 Nov30–Dec 2; Hong Kong, China; 2017. p. 299–321.
[59] Wang Z, Lin J, Cai Q, Wang Q, Zha D, Jing J. Blockchain-based certificatetransparency and revocation transparency. IEEE Trans Dependable SecurComput. In press.
[60] Kubilay MY, Kiraz MS, Mantar HA. CertLedger: a new PKI model withcertificate transparency based on blockchain. Comput Secur 2019;85: 333–52.
[61] Xu R, Joshi J. Trustworthy and transparent third-party authority. ACM TransInternet Technol 2020;20(4):31.
[62] Chen J, Yao S, Yuan Q, He K, Ji S, Du R. CertChain: public and efficientcertificate audit based on blockchain for TLS connections. In: Proceedings ofIEEE INFOCOM 2018; 2018 Apr 15–19; Honolulu, HI, USA; 2018. p. 2060–8.
[63] Kondova G, Erbguth J. Self-sovereign identity on public blockchains and theGDPR. In: Proceedings of the 35th Annual ACM Symposium on AppliedComputing; 2020 Mar 30–Apr 3; 2020. p. 342–5.
[64] Fan K, Pan Q, Zhang K, Bai Y, Sun S, Li H, et al. A secure and verifiable datasharing scheme based on blockchain in vehicular social networks. IEEE TransVeh Technol 2020;69(6):5826–35.
[65] Yu G, Zha X, Wang X, Ni W, Yu K, Yu P, et al. Enabling attribute revocation forfine-grained access control in blockchain–IoT systems. IEEE Trans Eng Manag2020;67(4):1213–30.
[66] Hu Y, Kumar S, Popa RA. Ghostor: toward a secure data-sharing system fromdecentralized trust. In: Proceedings of NSDI; 2020 Feb 25–27; Santa Clara, CA,USA; 2020. p. 851–77.
[67] Yuen TH, Sun SF, Liu JK, Au MH, Esgin MF, Zhang Q, et al. RingCT 3.0 forblockchain confidential transaction: shorter size and stronger security. In: Bonneau J, Heninger N, editors. Financial cryptography and data security.Cham: Springer; 2020. p. 464–83.
[68] Hardjono T, Pentland A. Verifiable anonymous identities and access control inpermissioned blockchains. 2019. arXiv:1903.04584.
[69] Camenisch J, Drijvers M, Dubovitskaya M. Practical UC-secure delegatablecredentials with attributes and their application to blockchain. In: Proceedings of the 2017 ACM SIGSAC Conference on Computer andCommunications Security; 2017 Oct 30–Nov 3; Dallas, TX, USA; 2017. p.683–99.
[70] Sonnino A, Al-Bassam M, Bano S, Meiklejohn S, Danezis G. Coconut: thresholdissuance selective disclosure credentials with applications to distributedledgers. 2018. arXiv:1802.07344.
[71] Yu Y, Zhao Y, Li Y, Du X, Wang L, Guizani M. Blockchain-based anonymousauthentication with selective revocation for smart industrial applications.IEEE Trans Ind Inform 2020;16(5):3290–300.
[72] Gao S, Piao G, Zhu J, Ma X, Ma J. TrustAccess: a trustworthy secure ciphertextpolicyand attribute hiding access control scheme based on blockchain. IEEETrans Veh Technol 2020;69(6):5784–98.
[73] Zhou L, Du S, Zhu H, Chen C, Ota K, Dong M. Location privacy in usage-basedautomotive insurance: attacks and countermeasures. IEEE Trans Inf ForensicsSecur 2018;14(1):196–211.
[74] Frankle J, Park S, Shaar D, Goldwasser S, Weitzner D. Practical accountabilityof secret processes. In: Proceedings of the 27th USENIX

Security Symposium;2018 Aug 15 – 17; Baltimore, MD, USA; 2018. p. 657 –74.

[75] Antignac T, Scandariato R, Schneider G. A privacy-aware conceptual model forhandling personal data. In: Margaria T, Steffen B, editors. Leveragingapplications of formal methods, verification and validation: foundationaltechniques. Cham: Springer; 2016. p. 942–57.

[76] Labadie C, Legner C. Understanding data protection regulations from a datamanagement perspective: a capability-based approach to EU-GDPR. In: Proceedings of the 14th International Conference on Wirtschaftsinformatik;2019 Feb 24 – 27; Siegen, Germany; 2019. p. 1292 –306.

[77] Barati M, Rana O, Theodorakopoulos G, Burnap P. Privacy-aware cloudecosystems and GDPR compliance. In: Proceedings of 2019 7th InternationalConference on Future Internet of Things and Cloud; 2019 Aug 26–28;Istanbul, Turkey; 2019. p. 117–24.

[78] Corrales M, Jurc ˇ ys P, Kousiouris G. Smart contracts and smart disclosure:coding a GDPR compliance framework. In: Corrales M, Fenwick M, Haapio H, editors. Legal tech, smart contracts and blockchain. Singapore: SpringerNature Singapore Pte Ltd.; 2019. p. 189–220.

[79] Bowe S, Chiesa A, Green M, Miers I, Mishra P, Wu H. ZEXE: enablingdecentralized private computation. In: Proceedings of 2020 IEEE Symposiumon Security and Privacy (SP); 2020 May 18–21; San Francisco, CA, USA; 2020.p. 947–64.

[80] Ma Z, Wang X, Jain DK, Khan H, Gao H, Wang Z. A blockchain-based trusteddata management scheme in edge computing. IEEE Trans Ind Inform 2019;6(3):2013–21.

[81] Parno B, Howell J, Gentry C, Raykova M. Pinocchio: nearly practical verifiablecomputation. In: Proceedings of 2013 IEEE Symposium on Security andPrivacy; 2013 May 19–22; Berkeley, CA, USA; 2013. p. 238–52.

[82] Maller M, Bowe S, Kohlweiss M, Meiklejohn S. Sonic: zero-knowledge SNARKsfrom linear-size universal and updatable structured reference strings. In: Proceedings of the 2019 ACM SIGSAC Conference on Computerand Communications Security; 2019 Nov 11 – 15; London, UK; 2019.p. 2111–28.

[83] Costan V, Devadas S. Intel SGX explained. 2016. Cryptology ePrint Archive:86.

[84] Cheng R, Zhang F, Kos J, He W, Hynes N, Johnson N, et al. Ekiden: a platformfor confidentiality-preserving, trustworthy, and performant smart contracts. In: Proceedings of IEEE European Symposium on Security an Privacy; 2019Jun 17–19; Stockholm, Sweden; 2019. p. 185–200.

[85] Ayoade G, Karande V, Khan L, Hamlen K. Decentralized IoT data managementusing blockchain and trusted execution environment. In: Proceedings of IEEEInternational Conference on Information Reuse and Integration (IRI); 2018 Jul6–9; Salt Lake City, UT, USA; 2018. p. 15–22.

[86] Pass R, Shi E, Tramèr F. Formal abstractions for attested execution secureprocessors. In: Coron JS, Nielsen JB, editors. Advances in cryptology—EUROCRYPT 2017. Cham: Springer; 2017. p. 260–89.

[87] Dong C, Wang Y, Aldweesh A, McCorry P, van Moorsel A. Betrayal, distrust, and rationality: smart counter-collusion contracts for verifiable cloudcomputing. In: Proceedings of 2017 ACM SIGSAC Conference on Computerand Communications Security; 2017 Oct 30 – Nov 3; Dallas, TX, USA; 2017.p. 211–27.

[88] Brewster C, Nouwt B, Raaijmakers S, Verhoosel J. Ontology-based accesscontrol for FAIR data. Data Intell 2020;2(1–2):66–77.

[89] Bhaskaran K, Ilfrich P, Liffman D, Vecchiola C, Jayachandran P, Kumar A, et al. Double-blind consent-driven data sharing on blockchain. In: Proceedings of2018 IEEE International Conference on Cloud Engineering (IC2E); 2018 Apr17–20; Orlando, FL, USA; 2018. p. 385–91.

[90] Li H, Pei L, Liao D, Chen S, Zhang M, Xu D. FADB: a fine-grained accesscontrol scheme for VANET data based on blockchain. IEEE Access2020;8:85190–203.

[91] Koutsos V, Papadopoulos D, Chatzopoulos D, Tarkoma S, Hui P. Agora: aprivacy-aware data marketplace. 2020. Cryptology ePrint Archive:865.

[92] Liu D, Alahmadi A, Ni J, Lin X, Shen X. Anonymous reputation system for IIoTenabledretail marketing atop pos blockchain. IEEE Trans Ind Inform 2019;15(6):3527–37.

[93] Lone AH, Mir RN. Reputation driven dynamic access control framework forIoT atop PoA ethereum blockchain. 2020. Cryptology ePrint Archive:566.

[94] Xu C, Wang K, Li P, Guo S, Luo J, Ye B, et al. Making big data open in edges: aresource-efficient blockchain-based approach. IEEE Trans Parallel Distrib Syst2019;30(4):870–82.

[95] Makhdoom I, Zhou I, Abolhasan M, Lipman J, Ni W. PrivySharing: ablockchain-based framework for privacy-preserving and secure datasharing in smart cities. Comput Secur 2020;88:101653.

[96] Truong NB, Sun K, Lee GM, Guo Y. GDPR-compliant personal datamanagement: a blockchain-based solution. IEEE Trans Inf Forensics Secur2020;15:1746–61.

[97] Zheng X, Mukkamala RR, Vatrapu R, Ordieres-Mere J. Blockchain-basedpersonal health data sharing system using cloud storage. In: Proceedings ofIEEE 20th International Conference on e-Health Networking, Applicationsand Services (Healthcom); 2018 Sep 17 – 20; Ostrava, Czech Republic; 2018.p. 1–6.

[98] Zheng BK, Zhu LH, Shen M, Gao F, Zhang C, Li YD, et al. Scalable and privacypreservingdata sharing based on blockchain. J Comput Sci Technol 2018;33(3):557–67.

[99] Gunasinghe H, Kundu A, Bertino E, Krawczyk H, Chari S, Singh K, et al. PrividEx: privacy preserving and secure exchange of digital identity assets. In: Proceedings of the World Wide Web Conference; 2019 May 13 – 17; SanFrancisco, CA, USA; 2019. p. 594–604.

[100] Dai W, Dai C, Choo KKR, Cui C, Zou D, Jin H. SDTE: a secure blockchain-baseddata trading ecosystem. IEEE Trans Inf Forensics Secur 2019;15:725 –37.

[101] Schuster F, Costa M, Fournet C, Gkantsidis C, Peinado M, Mainar-Ruiz G, et al. VC3: trustworthy data analytics in the cloud using SGX. In: Proceedings of2015 IEEE Symposium on Security and Privacy; 2015 May 17–21; San Jose,CA, USA; 2015. p. 38–54.

[102] Dziembowski S, Eckey L, Faust S. Fairswap: how to fairly exchange digitalgoods. In: Proceedings of the 2018 ACM SIGSAC Conference on Computer andCommunications Security; 2018 Oct 15 – 19; Toronto, ON, Canada; 2018. p.967–84.

[103] Liu X, Sun SX, Huang G. Decentralized services computing paradigm forblockchain-based data governance: programmability, interoperability, andintelligence. IEEE Trans Serv Comput 2019;13(2):343–55.

[104] Weng J, Weng J, Zhang J, Li M, Zhang Y, Luo W. DeepChain: auditable andprivacy-preserving deep learning with blockchain-based incentive. IEEETrans Dependable Secur Comput 2021;18(5):2438–55.

[105] Hu S, Cai C, Wang Q, Wang C, Luo X, Ren K. Searching an encrypted cloudmeets blockchain: a decentralized, reliable and fair realization. In: Proceedings of IEEE INFOCOM 2018; 2018 Apr 16 – 19; Honolulu, HI, USA; 2018. p. 792–800.

[106] Nguyen K, Ghinita G, Naveed M, Shahabi C. A privacy-preserving, accountableand spam-resilient geo-marketplace. In: Proceedings of the 27th ACMSIGSPATIAL International Conference on Advances in GeographicInformation System; 2019 Nov 5–8; Chicago, IL, USA; 2019. p. 299–308.

[107] Zhang Y, Genkin D, Katz J, Papadopoulos D, Papamanthou C. A zeroknowledgeversion of VSQL. 2017. Cryptology ePrint Archive:1146.

[108] Neisse R, Steri G, Nai-Fovino I. A blockchain-based approach for dataaccountability and provenance tracking. In: Proceedings of the 12thInternational Conference on Availability, Reliability and Security; 2017 Aug29–Sep 1; Reggio Calabria, Italy; 2017. p. 1–10.

[109] Cucurull J, Puiggalí J. Distributed immutabilization of secure logs. In: BartheG, Markatos E, Samarati P, editors. Security and trust management. Cham:Springer; 2016. p. 122–37.

[110] Ruan P, Chen G, Dinh TTA, Lin Q, Ooi BC, Zhang M. Fine-grained, secure andefficient data provenance on blockchain systems. In: Proceedings of the 45thInternational Conference on Very Large Data Bases; 2019 Aug 26 –30; LosAngles, CA, USA; 2019. p. 975–88.

[111] Tang YR, Xing Z, Xu C, Chen J, Xu J. Lightweight blockchain logging for dataintensiveapplications. In: Zohar A, Eyal I, Teague V, Clark J, Bracciali A, Pintore F, et al., editors. Financial cryptography and data security. Berlin:Springer Verlag GmbH; 2018. p. 308–24.

[112] Ahmad A, Saad M, Njilla L, Kamhoua C, Bassiouni M, Mohaisen A. BlockTrail: ascalable multichain solution for blockchain-based audit trails. In:Proceedings of 2019 IEEE International Conference on Communication (ICC); 2019 May 20–24; Shanghai, China; 2019.

[113] Liu D, Ni J, Huang C, Lin X, Shen XS. Secure and efficient distributed networkprovenance for IoT: a blockchain-based approach. IEEE Internet Things J2020;7(8):7564–74.

[114] Tomescu A, Bhupatiraju V, Papadopoulos D, Papamanthou C, TriandopoulosN, Devadas S. Transparency logs via append-only authenticated dictionaries. In: Proceedings of the 2019 ACM SIGSAC Conference on Computer andCommunications Security; 2019 Nov 11– 15;

London, UK; 2019. p. 1299–316.
[115] Ding S, Cao J, Li C, Fan K, Li H. A novel attribute-based access control schemeusing blockchain for IoT. IEEE Access 2019;7:38431–41.
[116] Matetic S, Wüst K, Schneider M, Kostiainen K, Karame G, Capkun S. BITE: bitcoin lightweight client privacy using trusted execution. In: Proceedings ofthe 28th USENIX Conference on Security Symposium, 2019 Aug 14–16; SantaClara, CA, USA; 2019. p. 783–800.
[117] Chepurnoy A, Papamanthou C, Zhang Y. Edrax: a cryptocurrency withstateless transaction validation. 2018. Cryptology ePrint Archive:968.
[118] Jiang Y, Wang C, Wang Y, Gao L. A cross-chain solution to integrating multipleblockchains for IoT data management. Sensors 2019;19(9):2042.
[119] Maram SKD, Zhang F, Wang L, Low A, Zhang Y, Juels A, et al. CHURP: dynamiccommitteeproactive secret sharing. In: Proceedings of the 2019 ACM SIGSACConference on Computer and Communications Security; 2019 Nov 11–15;London, UK; 2019. p. 2369–86.
[120] Campanelli M, Fiore D, Querol A. LegoSNARK: modular design andcomposition of succinct zero-knowledge proofs. In: Proceedings of ACMSIGSAC Conference on Computer and Communications Security; 2019 Nov11–15; London, UK; 2019. p. 2075–92.
[121] Lim SY, Fotsing PT, Almasri A, Musa O, Kiah MLM, Ang TF, et al. Blockchaintechnology the identity management and authentication service disruptor: asurvey. Int J Adv Sci Eng Inf Technol 2018;8:1735–45.
[122] Canetti R. Universally composable security: a new paradigm forcryptographic protocols. In: Proceedings of 42nd IEEE Symposium onFoundations of Computer Science; 2001 Oct 8–11; Newport Beach, CA, USA; 2001. p. 136–45.