一种用于管理低内存设备的上下文感知多区块链架构

Marco Fiore巴里理工大学电气与信息工程系意大利巴里 marco.fiore@poliba.it

Marina Mongiello巴里理工大学电气与信息工程系意大利巴里 marina.mongiello@poliba.it

Giuseppe Acciani巴里理工大学电气与信息工程系意大利巴里 giuseppe.acciani@poliba.it

arXiv:2305.03545v1 [cs.SE] 5 May 2023

摘要——**区块链技术改变了我们构想分布式架构的方式。区块链系统使我们能够构建数据不可篡改、防篡改的平台，但在吞吐量和存储账本所需的内存量方面存在一些限制。本文旨在解决内存和性能需求问题，开发一种多区块链架构，结合公有区块链和私有区块链各自的优势。这种方法使内存和性能受限的小型传感器能够加入网络，而无需担心需要存储的数据量。本文采用上下文感知方法进行开发，使该架构具备可扩展性，并易于应用于不同场景。**

索引词—**多重区块链、上下文感知、架构、物联网传感器、提案**

I. 引言

区块链技术——一种分布式账本技术（DLT）——可用于安全地存储信息。它可以表示为一个分布式数据库，由一系列逻辑链接的区块组成，每个区块包含多笔交易。区块链是一种只能追加的数据存储方案：数据只能添加并与先前的数据串接，因此篡改变得非常困难，因为修改单个区块可能需要破坏整条链。当归档数据的完整性受到多个可同时访问数据的用户威胁时，建议使用区块链。区块链平台最常见的应用涉及加密货币和食品溯源。

针对基于区块链的可追溯性架构，可以分析多种方案，涵盖从农食领域 [1]–[5] 到医疗保健领域 [6]–[8]以及智慧城市 [9]。大多数经过分析的架构都提出了一种利用物联网（IoT）设备的方案 [10], [11]：在这些情况下，区块链和分布式账本技术能够确保供应链中交换和存储的数据可用且可追溯。其他实现则只采用一种区块链架构，要么是公有链 [12] ，要么是私有链 [13], [14], ，也有与星际文件系统（IPFS）结合使用的情况 [15]。

这些方法的一个常见问题是，尽管设备内存容量小、性能较差，仍要保证高性能。区块链系统需要具备充足内存的设备，但目前尚无方案提出将私有区块链与公有区块链结合起来，以正确管理来自传感器的数据。数据一致性通过两个账本的通用接口来解决：信息以 JSON 格式交换，既作为私有侧的输出，也作为公有侧的输入。

本文的主要目标是提出一种新型架构，将多条区块链结合起来，以便在存储和性能资源有限的设备（如物联网传感器）上实现良好性能。为此，我们开发了一款情境感知型智能合约应用。该方法确保即使是从物联网传感器采集的数据也能保持不可篡改，尽管在这一领域应用区块链技术时，仍需考虑其局限性（数据大小、吞吐量、实时数据分析）。我们采用私有区块链作为安全且不可篡改的中间层，连接负责上传数据的物联网传感器，以及负责收集从数据中提取的价值并将这些新信息传播到网络中的公有区块链。总而言之，我们通过一个场景说明系统的工作方式，并概述该方法的优势与局限性。

II. 区块链技术

Blockchain 字面意思是区块链：它的主要特点是将数据库去中心化并分布到多个设备上。图 1 展示了一个区块链示例。区块链和分布式账本并非建立在中心化系统之上：这意味着数据不会存储在

单一位置（即服务器）中，也不会由单一实体控制和共享。在分布式账本中，网络中的每个节点都持有一份账本副本：数据变更会广播给每位参与者。这样，区块链便值得信赖，且不依赖中央机构。

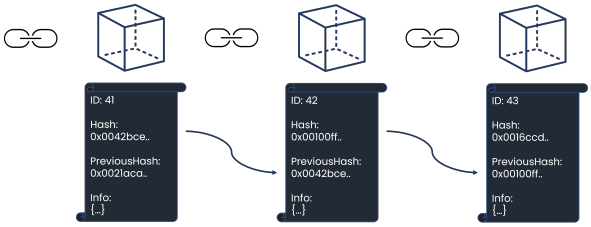


图 1. 简单的区块链架构：区块通过“PreviousHash”字段依次连接。

在区块链平台中，两个参与者之间的每笔交易都会被永久记录。这些记录称为区块，而用于处理区块链的每台计算机称为节点。交易可通过挖矿操作添加，这一过程会将一条或多条记录加入区块链。挖矿过程基于计算复杂的哈希函数。对共享信息进行加密可提供高级别的安全性。变更必须经公众共识接受。

区块链分为三种类型：公有区块链、私有区块链以及联盟链或联合区块链。其主要特征总结于表一[16]。

- 公有区块链
  公有区块链没有控制网络的节点；任何人都可以加入分布式账本，并插入或读取其中存储的信息。公有区块链开放且透明；用于支持共识的算法包括工作量证明、权益证明或权威证明。

- 私有区块链
  私有区块链由组织或个人管理，他们对网络拥有控制权。挖矿权可以授予任何人，但决定权掌握在该组织手中。在这种情况下，与公有区块链相比，账本可以被视为更加中心化，因为有一个实体拥有比其他实体更多的权力。私有区块链的成本低于公有区块链。

- 联盟区块链
  联盟区块链试图兼具公有区块链和私有区块链的优势。在这种情况下，账本的所有者是多个节点，而不是单个节点。这使得该区块链比私有区块链更加去中心化，但成本又不像公有区块链那么高。所有者群体负责管理区块链并维持网络运行。

表一 公有、私有和联盟区块链的比较。

	公有	私有	联盟
共识确定	所有矿工	一个组织	选定的节点集合
读取权限	公共	公共或受限	公共或受限
不可篡改性	无法篡改	可能被篡改	可能被篡改
效率	Low	High	High
中心化	No	Yes	部分
共识过程	无需许可	许可型	许可型

III. 提出的架构

我们提出的架构如图 2 所示。它主要由以下部分组成：(a) 容器（用于实现 Hyperledger Fabric）、(b) 智能合约、(c) 边缘计算单元和 (d) 物联网传感器。这里重点展示了不同区块链之间的交互。主系统基于以太坊[1]，，以确保使用公有区块链所带来的全部优势：透明性、数据不可篡改性和可靠性。以太坊节点由一些边缘计算单元组成，负责管理所有内部低内存设备。这些设备不会依赖论文 [17], [18] 作者所描述的某些 NoSQL 数据库来进行通信和存储数据；它们使用容器化的私有区块链，具体而言，我们采用 Hyperledger Fabric[2] ，但为此也可以使用任何私有区块链。这种方法为平台提供了模块化和可扩展性。每个边缘计算单元同时也是一个 Hyperledger 对等节点和一个以太坊节点：从 Hyperledger 侧来看，它可以从物联网传感器获取数据，并对数据进行管理和转换，使其成为有价值的数据；从以太坊侧来看，它可以上传计算结果（即月度数据的均值和标准差），从而减轻区块链的负载。由于内存和计算能力有限，物联网传感器只能受益于我们方法的应用：传感器的账本成本低于以太坊账本，因为它们只记录其容器内部收集的信息。一个容器的行为独立于其他所有容器，从而确保平台具备模块化和可扩展性。

智能合约用于管理公有和私有区块链。在 Hyperledger Fabric 方面，智能合约按照上下文感知方法开发：它们可以接收来自《传感器》的任意类型输入数据，并使用 JSON 格式将其插入数据库。图 3 展示了用于更新数据或向数组中添加新信息的 JavaScript 链码。图 4 展示了此类函数在食品追溯系统中的输出，其中更新了一个值（植物密度），并在农事操作数组中插入了一条新信息。边缘计算单元读取插入的数据，将其转换为有价值的数据，并将最终信息发送至以太坊。这样，得益于所应用的算法，发送至以太坊并存储在 Hyperledger Fabric 子系统中的数据量得以减少。在这种方法中，数据一致性并不是问题，因为使用了统一接口：平台之间的信息交换采用 JSON 格式，而该格式

[1]https://ethereum.org/en/ [2] https://hyperledger-fabric.readthedocs.io/en

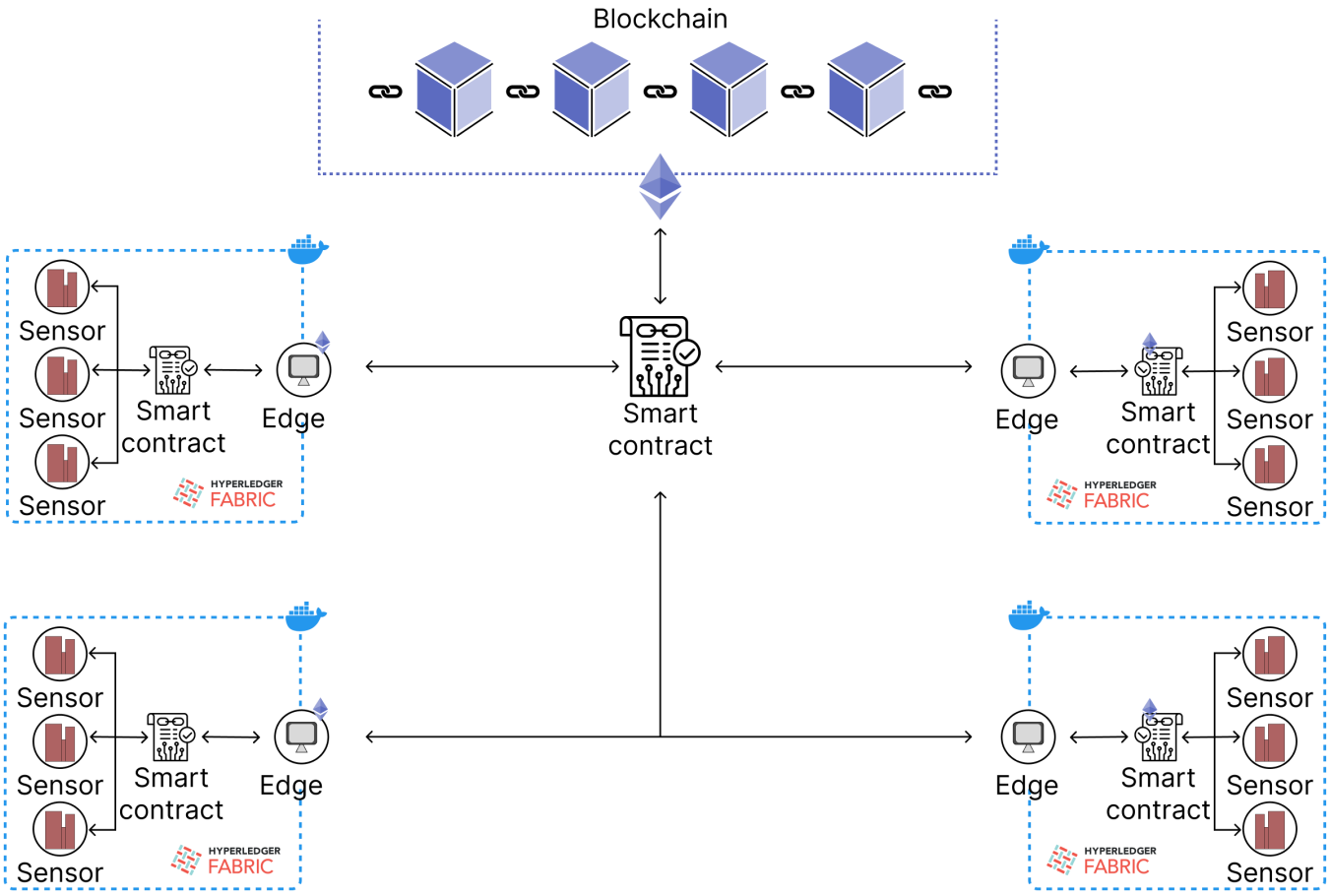


图 2. 所提出平台的架构

由 JavaScript 链码和 Solidity 智能合约进行管理。

```
async updateDocData(ctx, id, oldData, updatedData) {
    const old_data = JSON.parse(oldData);
    const updated_data = JSON.parse(updatedData);

    const updatedDoc = {
        ...old_data,
        ...updated_data,
    };

    await ctx.stub.putState(id, Buffer.from(JSON.stringify(updatedDoc)));
    console.log(updatedDoc);
}


async addData(ctx, id, oldData, category, newData) {
    const new_data = JSON.parse(newData);
    const doc = JSON.parse(oldData);

    if (!Array.isArray(doc[category])) {
        throw new Error(`Given category is not of Array type!`);
    }
    doc[category].push(new_data);
    await ctx.stub.putState(id, Buffer.from(JSON.stringify(doc)));
}
```

图 3. 采用上下文感知方法编写的 Hyperledger Fabric 链码。

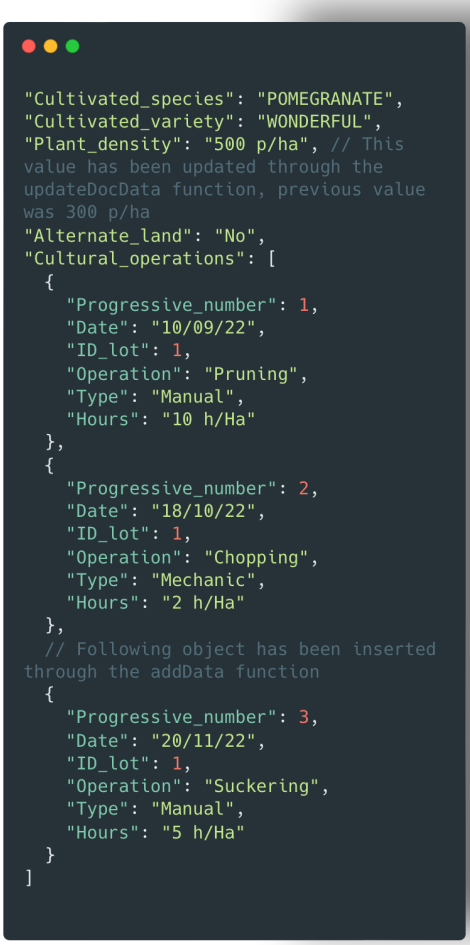
IV. 场景

所提出的系统采用以下场景实现：农食供应链追溯系统的设计与开发。我们的方案与论文 [19]–[21]中介绍的方法有所不同。

该场景提出了五个不同的领域，每个领域都涵盖一种农产品：芦笋、石榴、杏仁、番茄和硬粒小麦。该系统分为三个主要部分：收集数据、将数据转化为价值，以及将价值发送到公有区块链。

A. 收集数据

通过田间的一些物联网传感器，可以采集数据。这些传感器测量温度、湿度和气象参数，范围从每日降雨百分比到风速。这些数据单独来看并无价值，但应将它们汇集起来，以提取有用信息。此外，这些大数据占用大量内存，因此低内存设备不可能完整存储来自所有传感器的信息。通过创建本地私有区块链，设备可以轻松管理较小规模的数据。与 MongoDB 等通用数据库相比，使用私有区块链还能在这一处理阶段确保数据的不可篡改性。任何人都无法篡改数据，从而避免造假。



```
"Cultivated_species": "POMEGRANATE",
"Cultivated_variety": "WONDERFUL",
"Plant_density": "500 p/ha", // This
value has been updated through the
updateDocData function, previous value
was 300 p/ha
"Alternate_land": "No",
"Cultural_operations": [
  {
    "Progressive_number": 1,
    "Date": "10/09/22",
    "ID_lot": 1,
    "Operation": "Pruning",
    "Type": "Manual",
    "Hours": "10 h/Ha"
  },
  {
    "Progressive_number": 2,
    "Date": "18/10/22",
    "ID_lot": 1,
    "Operation": "Chopping",
    "Type": "Mechanic",
    "Hours": "2 h/Ha"
  },
  // Following object has been inserted
through the addData function
  {
    "Progressive_number": 3,
    "Date": "20/11/22",
    "ID_lot": 1,
    "Operation": "Suckering",
    "Type": "Manual",
    "Hours": "5 h/Ha"
  }
]
```

图 4. 基于区块链的可追溯系统中 Hyperledger Fabric 链码的执行。

B. 将数据转化为价值

每块田地都配备了一个边缘计算单元，负责读取传感器存储在私有区块链中的所有信息。这些单元获取数据并将其转换为有价值的信息，同时对所收集信息的重要性和优先级进行初步分析。该过程的输出是一组轻量级信息，可存储在公有区块链中，供任何人访问。

C. 向公有区块链发送价值

每个边缘计算单元都是私有区块链中的一个对等节点，也是公有区块链中的一个节点。只有这些单元才能向公有区块链上传新信息，因此公众只能查看每块田地的最终报告。这一过程使可追溯系统更加透明，并让最终用户产生信任。消费者在超市购买农产品之前，可以通过扫描二维码了解该产品的相关信息，例如产品的产地、田地的温度以及农事操作的次数。

D. 优势与局限

所提出的架构易于在新系统和现有系统中实现，因为它只需少量硬件组件即可正常运行。只需一个边缘计算单元即可搭建该平台，因为它既可连接 Hyperledger Fabric（用于物联网设备），也可连接以太坊（用于上传数据）。模块化是该平台的固有特性：每组物联网设备都可以采用基于容器的方法（如 Docker）创建新的 Hyperledger Fabric 镜像。这种方法可在涉及大量物联网设备的场景中实现高性能和可扩展性。此外，安全性也十分重要：在这种架构中，物联网设备不包含任何敏感信息，尽管它们经常且容易遭受攻击。事实上，数据处理由边缘计算单元执行。

此外，借助智能合约，可以设置控制机制，自动将因物联网传感器故障或篡改而产生的超量程值排除在分析和处理阶段之外。

敏感数据由边缘计算单元生成，并直接写入以太坊：由于区块链的存在，这一过程确保了传输安全，但同时也使该单元成为架构中的故障点。无论如何，增加一个边缘计算单元有助于实现数据冗余并避免故障，尤其是在该单元位于不同地点时。从安全性角度来看，可以将系统访问次数降至最低，并避免可疑的人工访问。

如前所述，区块链是一种只能追加的存储方案，但我们将其用于由低内存设备构成的场景。图 5 展示了已写入 N 个值后，再插入一批 100 个新值时私有区块链的占用空间；表二则展示了私有区块链中交易占用的内存，以及添加一批 100 笔新交易所需的时间。为实现我们的目标，私有区块链（Hyperledger Fabric）可以在有限时间内（即一个月）收集数据，随后对收集的数据进行降维，将其上传至以太坊，并丢弃旧信息（即重置私有账本）。这对我们的方案并无影响，因为数据仍保留在系统中：其价值已上传至公有区块链，因此不再需要单条数据。

V. 结论

本文提出了一种多区块链方法，借助上下文感知智能合约，可适用于多种场景。该框架基于模块化架构，能够支持低内存设备，同时不牺牲安全性。所提出的场景基于农食产品可追溯性，表明这种方法在实现模块化方面很有用：可以轻松添加新的字段和新的容器化物联网设备。

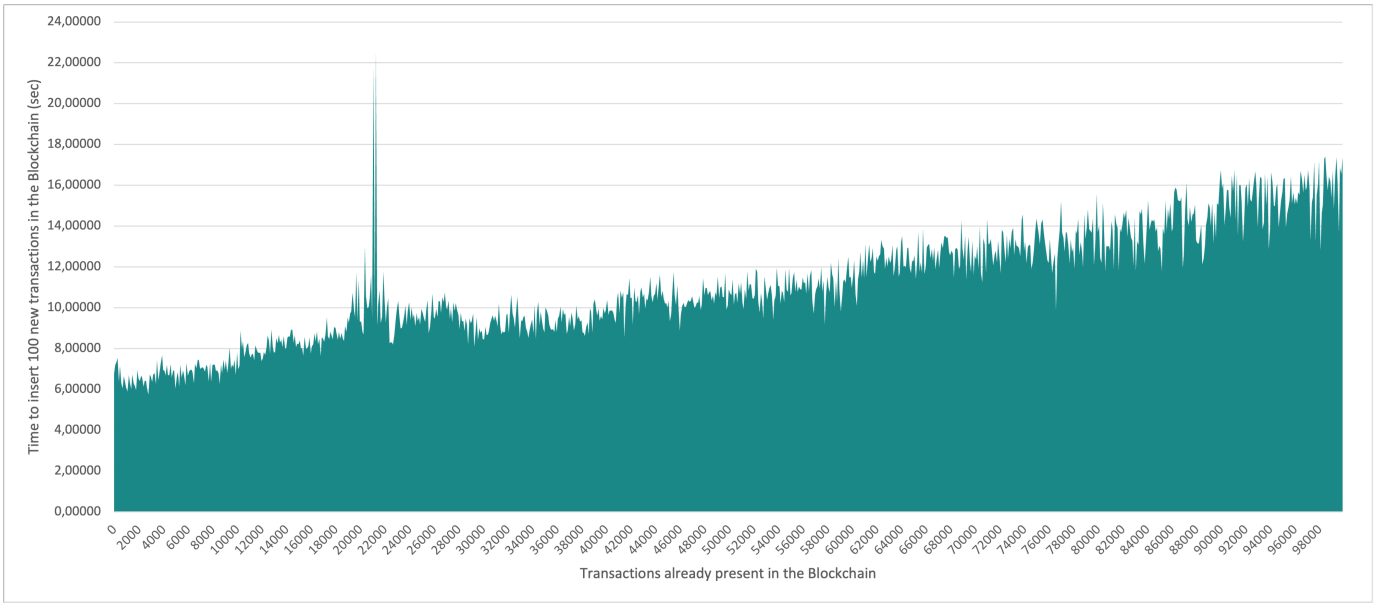


图 5. 当区块链中已有 N 个值时，管理 100 个新值所需的时间。

表二

内存 N　　在区块链中存储交易所需的内存，以及上传 100 笔新交易所需的时间　　S

区块链中的交易	占用的存储空间（MB）	添加 100 笔交易所需时间 [秒]
0	0,219	0
5	0,272	0,36
10	0,339	0,84
50	0,635	4,44
100	0,892	8,46
500	2,5	40,26
1000	6,3	86,46
5000	32,4	421,26
10000	64,5	912,66
50000	335,7	5508,66
100000	670,6	14688,66
500000	3400	62688,66

私有区块链（例如 Hyperledger Fabric）使用单个边缘计算单元来收集和转换数据，并将新信息上传至以太坊。采用两种不同的区块链，使用户能够构建安全的基础设施：数据自通过物联网设备创建起，经过边缘计算单元转换，直至最终上传至公有账本，全程不可篡改。为进一步提高安全性，可考虑增加一些边缘计算单元用于备份；也可以如论文 [22], 所述，将数据转换工作委托给特定的智能合约，从而在性能与可靠性之间找到平衡。

参考文献

[1] A. M. Shew、H. A. Snell、R. M. Nayga Jr 和 M. C. Lacity，“美国消费者对牛肉区块链可追溯性的估值”，应用经济学观点与政策，第 44 卷，323，2022 年 1，299 页。[2] T. K. Dasaklis、T. G. Voutsinas、G. T. Tsoulfas 和 F. Casino，“区块链赋能的供应链可追溯性实施的系统性文献综述”，可持续发展，第 14 卷，第 4 期，第 2439 页，2022 年。

[3] H. Feng、X. Wang、Y. Duan、J. Zhang 和 X. Zhang，“应用区块链技术改善农食产品可追溯性：发展方法、优势与挑战综述”，《清洁生产杂志》，第260卷，第121031页，2020年。[4] F. Tian，“基于RFID与区块链技术的中国农食供应链可追溯系统”，载于*2016*年第*13*届服务系统与服务管理国际会议（*ICSSSM*），第1–6页，IEEE，2016年。[5] M. P. Caro、M. S. Ali、M. Vecchio 和 R. Giaffreda，“农食供应链管理中的基于区块链的可追溯性：一种实际实施方案”，载于*2018*年物联网农业垂直与专题峰会——托斯卡纳（*IOT Tuscany*），第1–4页，IEEE，2018年。[6] I. A. Omar、M. Debe、R. Jayaraman、K. Salah、M. Omar 和 J. Arshad，“新冠肺炎个人防护装备的基于区块链的供应链可追溯性”，《计算机与工业工程》，第167卷，第107995页，2022年。[7] V. Kamath、Y. Lahari、K. Mohanchandra、等，“医疗保健系统中用于安全共享药品供应链数据的区块链框架”，《国际人工智能杂志》，第9卷，第1期，第32–28页，2022年。[8] I. Yaqoob、K. Salah、R. Jayaraman 和 Y. Al-Hammadi，“医疗保健数据管理中的区块链：机遇、挑战与未来建议”，《神经计算与应用》，第34卷，第14期，第11475–11490页，2022年。[9] M. Fiore 和 M. Mongiello，“用于改善智慧城市的区块链：一种架构提案”，载于2023年第7届国际会议关于

计算机、软件与建模（*ICCSM 2023*），已接收，2023年。[10] S. Balamurugan、A. Ayyasamy 和 K. S. Joseph，“物联网区块链驱动的可追溯技术：提升食品供应链安全措施”，《国际信息技术期刊》，第14卷，第2期，第1087–1098页，2022年。[11] M. S. Ali、K. Dolui 和 F. Antonelli，“通过区块链和星际文件系统实现物联网数据隐私”，载于第七届国际物联网会议论文集，第1–7页，2017年。[12] L. Cocco、K. Mannaro、R. Tonelli、L. Mariani、M. B. Lodi、A. Melis、M. Simone 和 A. Fanti，“农食中小企业中的基于区块链的可追溯系统：一家传统面包店的案例研究”，*IEEEAccess*，第9卷，第62899–62915页，2021年。[13] M. Uddin，“区块链 MedLedger：基于 Hyperledger Fabric 的制药行业假药药品可追溯系统”，《国际药剂学杂志》，第597卷，第120235页，2021年。[14] K. Gao、Y. Liu、H. Xu 和 T. Han，“基于 Hyperledger Fabric 的食品供应链可追溯系统设计与实现”，《国际计算科学与工程期刊》，第23卷，第2期，第185–193页，2020年。[15] H. Huang、X. Zhou 和 J. Liu，“基于区块链和EPC技术的食品供应链可追溯方案”，载于智能区块链国际会议，第32–42页，施普林格，2019年。[16] Z. Zheng、S. Xie、H. Dai、X. Chen 和 H. Wang，“区块链技术概述：架构、共识与未来趋势”，载于*2017*年*IEEE*国际大数据大会（大数据大会），第557–564页，IEEE，2017年。[17] Z. Ge、D. Loghin、B. C. Ooi、P. Ruan 和 T. Wang，“混合区块链数据库系统：设计与性能”，《*VLDB*捐赠会刊》，第15卷，第5期，第1092–1104页，2022年。[18] M. Nasreen 和 S. K. Singh，“使用 Java Eclipse 和 MongoDB 实现基于区块链的电子健康记录系统”，载于*2022*年*IEEE*区块链与分布式系统安全国际会议（*ICBDS*），第1–6页，IEEE，2022年。[19] M. Madine、K. Salah、R. Jayaraman、Y. Al-Hammadi、J. Arshad 和 I. Yaqoob，“appxchain：区块链网络的应用层互操作性”，*IEEE Access*，第9卷，第87777–87791页，2021年。[20] Y. Jiang、C. Wang、Y. Wang 和 L. Gao，“整合多条区块链的物联网数据管理跨链解决方案”，《传感器》，第19卷，第9期，第2042页，2019年。[21] Y. E. Oktian、S.-G. Lee 和 H. J. Lee，“面向可扩展物联网环境的分层多区块链架构”，《电子学》，第9卷，第6期，第1050页，2020年。[22] S. S. Kushwaha、S. Joshi、D. Singh、M. Kaur 和 H.-N. Lee，“以太坊区块链智能合约安全漏洞的系统性综述”，*IEEE Access*，2022年。