2023年IEEE智能信息系统与技术会议 (SIST)2023年5月4日至6日，阿斯塔纳，哈萨克斯坦

探索无需许可的区块链网络中的隐私问题及潜在解决方案

Talgar Bayan 计算机科学系 曼彻斯特大学 曼彻斯特，英国
talgar.bayan@manchester.ac.uk ORCID ID:0000-0001-8783-2229

Richard Banach 计算机科学系 曼彻斯特大学 曼彻斯特，英国
ric hard.banach@manchester.ac.uk ORCID ID:0000-0002-0243-9434

摘要— 近年来，无需许可区块链凭借其保障交易安全并提高交易透明度的能力，受到了广泛关注。区块链技术的发展已从加密货币扩展至去中心化金融，使数百万没有银行账户的人受益，并成为 Web3 的基础。Web3 旨在打造互联网的下一代，让用户拥有自己的数据。非同质化代币的兴起也帮助艺术家和创意工作者保护知识产权，并从自己的作品中获益。然而，与无需许可区块链相关的隐私风险已成为个人和机构关注的主要问题。区块链在 Web2 向 Web3 转型中的作用至关重要，而这一转型正在迅速发展。随着越来越多的个人、机构和组织采用这项技术，密切关注无需许可区块链相关的新风险并提供更新的缓解方案，变得愈发重要。

本文旨在探讨无需许可区块链中固有的隐私风险，包括远程过程调用（RPC）问题、以太坊域名服务（ENS）、矿工可提取价值（MEV）机器人、链上数据分析、数据泄露、交易关联、交易元数据等。本文还将分析针对这些隐私风险的现有解决方案，例如零知识证明、环签名、Hyperledger Fabric 和隐匿地址。最后，本文将提出关于未来如何改进无需许可区块链领域隐私解决方案的建议。

关键词— 无许可区块链；隐私

I. 引言

无许可区块链是一种去中心化的分布式账本，可实现安全、透明且防篡改的交易。它运行于点对点网络之上，所有参与者都能平等访问该网络及其数据，并参与交易验证。由于此类区块链是开源的，任何人都可以加入网络并验证交易。所有参与者均可访问公共账本，这增强了问责性、提升了安全性并增进了信任。然而，这种透明性也引发了隐私问题，因为参与者的数字资产、个人信息和金融交易都可能被任何人轻易查看，从而可能导致黑客攻击和盗窃。

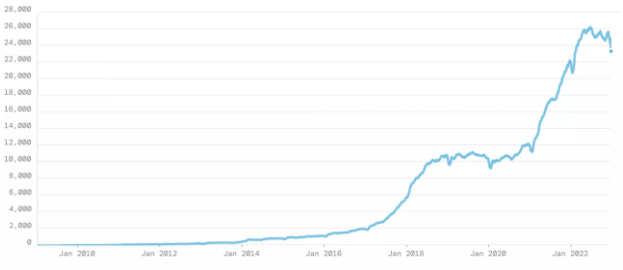


图1. 自2009年以来的月活跃开发者。

我们对领先的无需许可区块链进行了全面分析，重点关注用户参与度最高且活跃开发者社区规模最大的项目（如图1所示）。分析结果见表1。过去七年间，无需许可区块链领域实现了巨大发展与创新，月活跃开发者人数显著增加，目前已超过22,000 [2]。

表 I. 热门无需许可区块链

区块链	Type	TVL	交易次数（每日）	协议s	月度活跃开发者s
以太坊	层1	27B [3]	1.2M [4]	693 [3]	5734 [2]
BSC	层1	4.9B [3]	3.1M [3]	540 [6]	150 [2]
Solana	层1	245M [3]	0.13M [7]	93 [3]	2200 [2]
Polygon	层2	1.17B [3]	3M [5]	367 [3]	1100 [2]
Cosmos	层1	1B [3]	N/A	281 [3]	1500 [2]

BTC	层 1	131M [3]	300092	4 [3]	920 [2]
Near	层 1	81M [3]	374268 [8]	15 [3]	830 [2]

无需许可的区块链技术迅速普及，引发了各行各业乃至各国的广泛关注。随着资本涌入，越来越多的初创企业、组织和国家拥抱区块链，公有区块链相关的潜在风险也日益迫切。尽管区块链具有透明度方面的优势，但网络的开放性也带来了隐私问题。近期的 FTX 事件凸显了应对链上数据固有隐私风险的迫切性。必须认真考虑并应对这些挑战，才能确保区块链行业持续发展并取得成功。

本文深入探讨了无许可区块链中透明性与隐私之间持续存在的冲突。我们旨在全面分析该领域近来出现的隐私风险，从 MEV 机器人到智能合约漏洞。本文的主要目标有两个：

- 考察并重点阐述无需许可的区块链领域中最紧迫的隐私问题，包括 MEV 机器人、RPC、名称服务提供商（如 ENS）以及最新智能合约风险所带来的风险。

- 提出应对这些隐私风险的潜在解决方案，包括零知识证明、zkEVM 区块链、环签名技术，以及 Hyperledger Fabric 等模块化区块链的实现。通过这些举措，我们旨在为快速发展的无需许可区块链行业提供有价值的见解和建议，帮助降低隐私风险。

II. 相关研究

本节总结了有关无需许可的区块链网络隐私保护的相关研究及一些替代方案。在 [1] 惩罚而非奖励（PnR）区块链架构旨在解决以太坊和比特币等无需许可的区块链网络中隐私与开放性之间的平衡问题。作者提出了两种方法：对应用实施拒绝服务和/或撤销匿名性，以替代传统的区块创建奖励机制，从而维护网络隐私。

在 [10] 中，对工程数据的隐私保护方法进行了定性比较，所涉及的方法包括代理加密、同态加密、零知识证明和可信执行环境。结果表明，在现代数据生态系统中，依赖可信第三方保护参与者隐私的方法，无法充分保证敏感数据不会遭到泄露。在 [11] 中，提出了一种基于 Hyperledger Fabric 网络、通过实现零知识证明来确保患者数据隐私的隐私保护型许可型区块链解决方案，并采用 Idmix 套件保留匿名性和不可链接性等特征。在 [12] 中，对当前区块链隐私保护研究解决方案和机制的最新进展进行了系统综述，并讨论了区块链应用场景中的挑战，例如抗后量子计算、恶意好奇型可信第三方以及法规。表 II 展示了针对无需许可环境下的隐私问题，对最相关解决方案进行比较的结果。

表 II。　　相关解决方案比较

[12] [15] [9]		✓		✓	✓	
[1]		✓				✓
[11] [13]			✓			
[18]		✓		✓		
[14] [16] [17]		✓			✓	
[10]		✓	✓			
我们的工作	✓	✓	✓	✓	✓	✓

总体而言，随着无需许可的区块链领域迅速发展，涌现出 Web3、非同质化代币、去中心化应用和社交图谱等各种应用与领域。与其他作者不同，我们还探讨了多重签名技术、最大可提取价值机器人等方面。我们注意到，产业快速发展与研究探索之间存在差距，因此定期探索和分析无需许可的区块链网络十分重要。

III. 探索无需许可的区块链网络中的隐私问题

区块链的透明架构伴随着隐私风险。过去，这些风险较为基础且易于管理，但随着去中心化金融、非同质化代币和 Web3 去中心化应用的迅速发展，新的风险也随之出现。本文将探讨一些最新的典型风险。

A. 与私钥管理相关的风险　　*nt*

公有区块链中的私钥是一种秘密数字代码，用于访问和管理用户的资产与交易。私钥就像密码，允许用户签署交易并更改其区块链资产。用户务必妥善保管私钥，因为任何能够访问私钥的人都可以控制和操纵与该私钥关联的资产。私钥管理不善可能导致严重风险，包括：

- 资金损失：如果用户丢失或忘记其私钥，将无法再访问其在区块链上的资产，从而实际上失去其资金。
- 黑客攻击或盗窃：如果用户的私钥被盗或被恶意行为者获取，他们就可以利用它来控制和操纵用户在区块链上的资产和交易。
- 数据泄露：在联网环境中存储私钥或与他人共享私钥，可能导致数据泄露和遭受黑客攻击的风险，危及用户资产和交易的安全。

私钥管理不善所造成的后果，可从 Mt. Gox 事件中窥见一斑。当时，该交易所遭遇重大黑客攻击，导致 85 万枚比特币被盗，按当时的价格计算价值超过 4.5 亿美元。事后调查发现，此次攻击归因于私钥管理不善：私钥存储在联网环境中，攻击者很容易就能访问。

对于无需许可的区块链网络用户而言，了解私钥管理相关的风险并采取措施确保私钥安全至关重要，例如使用硬件钱包，或遵循私钥存储和管理的最佳实践。

B. 交易关联与链上分析

无需许可的区块链中的交易关联与链上分析可能会通过分析公开可见的交易数据，揭示用户的身份和行为，从而给用户带来隐私风险。这可能会暴露金融交易或个人数据等敏感信息。为降低这些风险，用户可以采用隐私增强技术，但这些方法并非万无一失，仍可能受到复杂分析技术的攻击。用户和更广泛的社区都应了解这些风险，并共同努力提升无需许可的区块链技术的隐私性和安全性。

C. 区块链交易元数据风险

区块链交易元数据可能带来隐私风险，因为它可能会泄露交易发送方和接收方的信息、他们的行为以及其他敏感信息。例如，交易元数据可用于：

- 解除用户匿名性：通过分析交易模式并将交易与现实世界身份关联起来，用户的匿名性可能会受到损害。
- 追踪资金流向：交易元数据可用于追踪区块链网络上的资金流向，从而可能泄露敏感的财务信息。
- 识别行为模式：分析交易元数据可以揭示用户的行为模式和习惯，例如消费习惯或偏好的基于区块链的服务。

这些隐私风险在公有区块链网络中尤为突出，因为交易是公开可见的，且很容易被分析。

D. 区块链名称服务与唯一地址风险

区块链钱包地址是区块链网络上交易的唯一标识符。虽然这些地址以复杂字符串的形式生成，但第三方服务可以提供 ENS 等更便于用户使用的选项，ENS 可用作区块链域名。然而，这种便利也伴随着风险：用户在生成过程中可能会失去对私钥的控制，从而导致资产丢失，并面临潜在的黑客攻击。了解并应对私钥管理方面的挑战，对于确保区块链资产的安全与保护至关重要。

E. RPC 隐私风险

RPC（远程过程调用）是一种协议，允许客户端通过网络向服务器发送请求。在公有区块链网络中，RPC 用于与网络中的节点通信并与区块链交互。虽然 RPC 提供了便捷高效的区块链交互方式，但如果安全措施不到位，也可能带来安全风险。

公有区块链网络中与 RPC 相关的一些风险包括：

- 中间人攻击：如果客户端与服务器之间的通信未加密，恶意行为者就可能拦截并篡改传输中的数据，从而可能危及客户端和区块链的安全。
- 未授权访问：如果攻击者能够访问 RPC 接口，就可能控制并操纵区块链节点，危及网络的安全性和完整性。
- 不安全的身份验证：如果访问 RPC 接口的身份验证过程不安全，攻击者可能绕过身份验证，未授权访问 RPC 接口。

为降低这些风险，必须妥善保护 RPC 接口，例如采用加密通信并实施严格的身份验证措施。此外，还应遵循保护区块链节点和网络的最佳实践，例如定期更新软件并监测安全威胁。

F. MEV 机器人风险

MEV（矿工可提取价值）机器人是利用区块链协议中的漏洞，从网络中获取利润或价值的计算机程序。换句话说，MEV 机器人旨在操纵区块链网络，从交易或区块奖励中获取利润。

MEV 机器人可以通过多种方式运作，例如抢先交易、审查交易或操纵资产价格。例如，抢先交易型 MEV 机器人可能会在大额订单之前下单，利用该大额订单可能导致的价格变动获利。这可能使 MEV 机器人以牺牲其他交易者的利益为代价赚取利润。

MEV 机器人被视为对区块链网络完整性的威胁，并可能对网络的整体健康状况和稳定性造成负面影响。

G. 智能合约风险

智能合约为在区块链网络上自动执行和落实合同协议提供了有价值的工具。然而，无需许可区块链的透明性和公开可访问性也可能带来隐私风险，尤其是在智能合约未经过适当审计和安全加固的情况下。例如，过时代码、错误的数学条件或糟糕的设计都可能导致意外后果，并使合约遭受第三方攻击者利用。

开发者遵循智能合约开发的最佳实践至关重要，包括进行全面测试和审计，以尽量降低这些风险，并确保无需许可区块链中智能合约的安全性和隐私性。智能合约漏洞的一个著名案例是2016年去中心化自治组织（DAO）遭到攻击：黑客利用智能合约代码中的漏洞窃取了大量资金。这一事件凸显了规范开展智能合约开发的重要性，也说明了持续提升区块链技术中智能合约的安全性和可靠性的必要性。

IV. 潜在解决方案

A. 多重签名技术

多重签名钱包可以帮助开始进入无许可区块链的参与者保护其数字资产。与单密钥管理相比，来自不同来源的更多私钥可以帮助参与者降低隐私风险。多重签名（多签）是一种可以帮助解决与公有区块链相关的隐私风险的技术，要求各方在交易得到处理之前对其进行签名。设想这样一种场景：三位用户 A、B 和 C 在区块链上持有一个多重签名地址的私钥。要执行一笔交易，三个私钥中至少需要使用两个进行签名。例如，如果 A 和 B 对一笔交易进行签名，该交易就会在区块链上得到处理，但无法确定是这两位用户中的哪一位签署了该交易。

虽然它可以提高安全性并增强对交易的控制，但也有一些缺点需要考虑，例如实现复杂、交易时间更长、若某一方无法提供签名或不愿签名则失败风险增加、依赖多方可能导致争议或分歧，以及成本增加。在实现多重签名之前，务必权衡这些潜在缺点与其带来的益处。

B. 零知识证明

零知识证明（ZKP）是解决区块链技术中隐私问题的一种有前景的方法。零知识证明（ZKP）使一方能够向另一方证明某个陈述为真，而无需透露该陈述本身以外的任何信息。因此，零知识证明（ZKP）是维护区块链交易隐私的有效工具。

在区块链交易中，各方可以使用零知识证明（ZKP）证明某些条件已得到满足，而无需透露有关交易或相关各方的任何细节。这使得区块链上的交易既安全又私密（P_1, P_2） → （$P_1|P_2$），P_1 证明交易有效，P_2 验证证明，而无需透露任何额外信息。

P_1 代表发起交易的一方，P_2 代表验证交易的一方。通过使用零知识证明，各方能够在不牺牲透明度和信任的前提下，确保交易的隐私和安全。图2展示了零知识证明的简化框架，即证明者和验证者。该框架的实现包括以下三个阶段：见证阶段、挑战阶段和响应阶段。在上述阶段中，不会泄露任何私人数据。

虽然零知识证明有望提升安全性和隐私保护，但也有一些缺点需要考虑。实现零知识证明可能很复杂，并且可能需要较高水平的技术专长，这会导致某些用户难以有效利用这项技术。此外，零知识证明可能是计算密集型的，并可能导致交易时间变长，因此在某些应用中的效率较低。

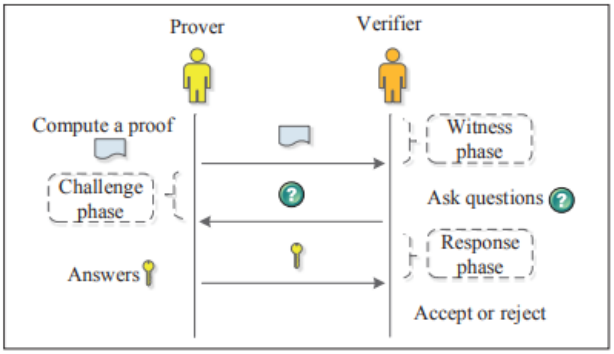


图2. 零知识证明框架。

这凸显了零知识证明作为解决区块链技术隐私问题的一种方案的潜力。未来的研究可以探索将零知识证明与其他隐私保护技术相结合，以增强区块链交易的安全性和隐私保护。

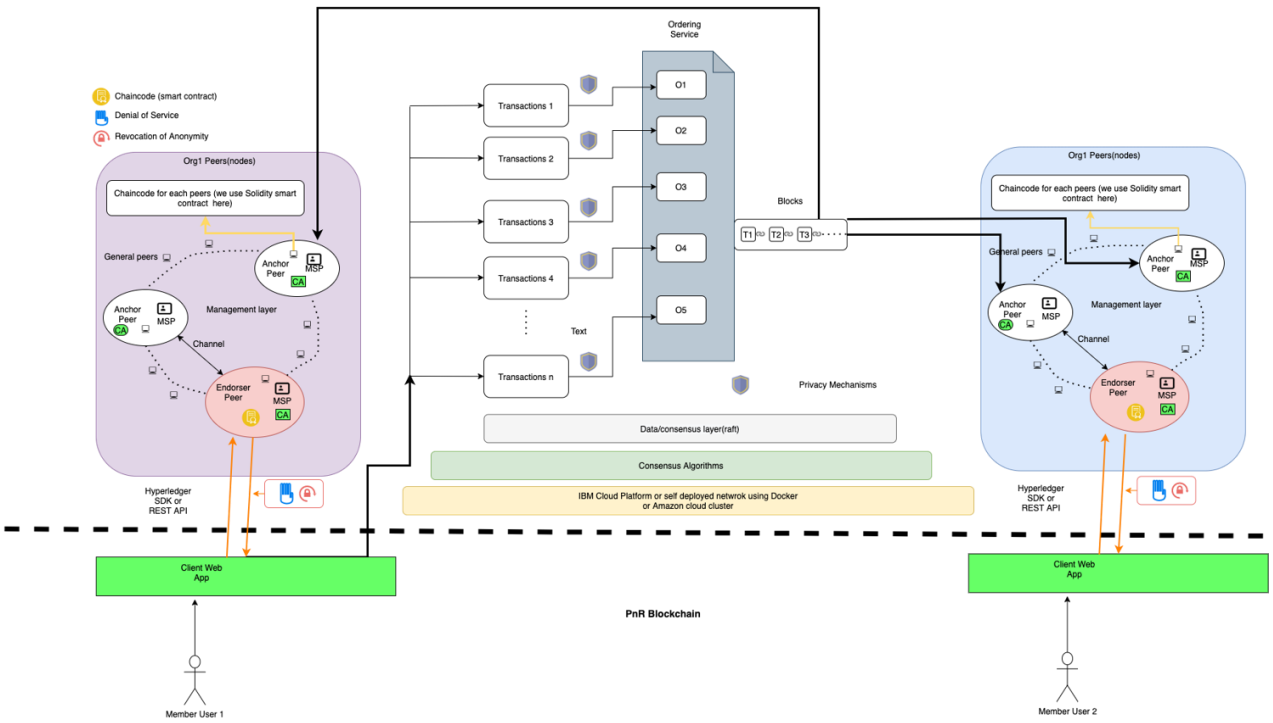


图 3. PnR 区块链架构测试原型。

C. Hyperledger Fabric

Hyperledger Fabric 通过实施许可型网络模型来解决公有区块链中的隐私问题，在该模型中，只有经过授权的实体才能访问账本数据。它还通过通道对敏感信息进行选择性披露，仅允许有正当需求的各方查看特定交易。这一方案为企业在区块链网络上进行交易提供了更安全、可控的环境，并确保其数据的机密性。在 [9] 中，作者阐述了区块链的基本属性，分析了当时的潜在威胁，并探讨了无许可区块链独特的隐私需求。

在 [1] 作者提出了惩罚而非奖励（PnR）区块链架构的设计。图 3 展示了我们为 PnR 架构搭建的测试网络原型。可以看到，模块化 Hyperledger 区块链为开发隐私保护区块链网络提供了灵活的解决方案。

D. 环签名

环签名通过允许一组用户（例如 $U_1, U_2, ..., U_n$）在不透露签名者身份的情况下对消息 m 进行签名，为与公有区块链相关的隐私风险提供了解决方案。环签名可以用数学形式表示为（$m, U_1, U_2, ..., U_n, \sigma$），其中 σ 是在该组用户的公钥下对消息 m 有效的签名，因此签名者的身份与组内其他成员无法区分。这使观察者难以确定这组用户中究竟是谁签署了该消息。通过使用环签名，公有区块链可以为希望在不透露身份的情况下进行交易的用户提供更高的隐私性，同时不透露其身份。此外，环签名还可用于在公有区块链上实现匿名投票和安全的多方计算，使这些系统对更广泛的应用场景更具吸引力。

E. 隐匿地址隐私增强技术

隐匿地址也称为一次性地址，是一种可用于区块链技术的隐私增强技术。它旨在通过隐藏接收方的地址来保护交易接收方的隐私。隐匿地址由接收方生成，随后发送方使用该地址发送资金。交易记录在区块链上，但接收方的地址仍然保密，且无法与其身份关联。

从数学上看，隐身地址可表示为一个单向函数 $H(x)$，其中接收方的公钥 P 用作输入 x。随后，发送方可以使用该函数为每笔交易生成唯一的隐身地址。接收方则可以使用自己的私钥访问此地址中的资金。我们采用（Courtois6，2016）第 21 张幻灯片中的符号，总结并测试了（用户“bytecoin”，2011年）提出的原始方法。

- 接收方拥有一个公钥。
- 发送方使用公钥。
- 现在，迪菲-赫尔曼算法使发送方和接收方都能计算出某个值 S。

$$S = a.B = b.A \in E(\mathbb{F}\rho) \quad (1)$$

- 随后，临时转账地址就是$H(s)$。G 在$E(\mathbb{F}\rho)$中，私钥为$c = H(S) \bmod Q$ ，而在比特币的常规操作中，当代币发送至$pk = H(S)$时，最初只会公开$H'(H(S))$。G。

- 接收方会主动监控区块链或其他通道，以查找所有可能的A，并检查是否有人正向某个$H'(H(b.A).G)$发送代币。他可以花费所有此类输出。

通过这种方式，隐匿地址隐藏接收方的地址，使其能够在不向公众透露身份的情况下接收资金，从而为区块链交易提供额外的隐私保护层。对于希望对其金融活动保密的接收方而言，这一点尤为重要。

F. zkEVM

zkEVM 是以太坊虚拟机（EVM）的一种实现，它使用零知识证明验证计算，并确保智能合约执行过程的隐私。zkEVM 使智能合约能够在不向以太坊网络透露任何机密信息的情况下运行。与传统 EVM 相比，这提供了更高程度的隐私保护，并有助于降低公有区块链中的隐私风险。通过隐藏敏感信息，zkEVM 可用于保护区块链上存储的用户数据、金融交易及其他敏感信息。

V. 结论

与无需许可区块链相关的隐私风险是个人和企业面临的一项重大问题。目前应对此类隐私风险的解决方案包括零知识证明、环签名、Hyperledger Fabric、zkEVM 和隐匿地址。这些方案能够提供一定程度的隐私保护，但也存在局限性。未来，无需许可区块链领域的隐私解决方案应着重提升隐私保护能力和可扩展性，以满足无需许可区块链日益增长的隐私保护需求。

参考文献

[1] Banach, R. 加密货币赌场之外的区块链应用：惩罚而非奖励区块链架构。Concurrency Computat Pract Exper. 2021; 33:e5749. https://doi.org/10.1002/cpe.5749.[2] “Electric Capital 对开源加密货币开发者的分析”，开发者报告，2023年1月17日。[在线]。可访问：https://www.developerreport.com/developer-report。[访问日期：02月01日，2023]年。[3] “所有链的总锁定价值”，DefiLlama。[在线]。可访问：https://defillama.com/chains。[访问日期：02月01日，2023]年。[4] “以太坊（ETH）区块链浏览器”，以太坊每日交易量。 [在线]。可访问：https://etherscan.io/chart/tx。[访问日期：02月01日，2023]年。[5] “Polygon PoS 链每日交易量图表”，Polygon（MATIC）区块链浏览器。[在线]。可访问：https://polygonscan.com/chart/tx。[访问日期：02月01日，2023]年。[6] “BNB 智能链每日交易量图表”。[在线]。可访问：https://bscscan.com/chart/tx。[访问日期：02月01日，2023]年。[7] “Solana 每日交易量（总计）”，Dune 仪表板。[在线]。可访问：https://dune.com/queries/390045。 [访问日期：02月01日，2023]年。[8] “探索 NEAR 区块链”，NEAR Explorer。 [在线]。可访问：https://explorer.near.org/。[访问日期：02月01日，2023]年。[9] L. Peng、W. Feng、Z. Yan、Y. Li、X. Zhou 和 S. Shimizu，《无许可区块链中的隐私保护：一项调查》，Digital Communications and Networks，第7卷，第3期，第295–307页，2021年。[10] Jones M、Johnson M、Shervey M、Dudley JT、Zimmerman N，《利用区块链进行特征工程的隐私保护方法：综述、评估与概念验证》，J Med Internet Res 2019;21(8):e13600 doi: 10.2196/13600。[11] C. Stamatellis、P. Papadopoulos、N. Pitropakis、S. Katsikas 和 W. Buchanan，《基于 Hyperledger Fabric 的隐私保护医疗保健框架》，Sensors，第20卷，第22期，第6587页，2020年11月，doi: 10.3390/s20226587。[12] J. Bernal Bernabe、J. L. Canovas、J. L. Hernandez-Ramos、R. Torres Moreno 和 A. Skarmeta，《区块链隐私保护解决方案：综述与挑战》，发表于 IEEE Access，第7卷，第164908–164940页，2019年，doi: 10.1109/ACCESS.2019.2950872。[13] D. Arora、S. Gautham、H. Gupta 和 B. Bhushan，《保护数据隐私与完整性的区块链安全解决方案》，2019年国际计算、通信与智能系统会议（ICCCIS），印度大诺伊达，2019年，第468–472页，doi: 10.1109/ICCCIS48478.2019.8974503。[14] T. T. Huynh、T. D. Nguyen 和 H. Tan，《区块链技术的安全与隐私问题调查》，2019年国际系统科学与工程会议（ICSSE），越南洞海，2019年，第362–367页，doi: 10.1109/ICSSE.2019.8823094。[15] D. Wang、J. Zhao 和 Y. Wang，《区块链隐私保护综述：技术与应用》，发表于 IEEE Access，第8卷，第108766–108781页，2020年，doi: 10.1109/ACCESS.2020.2994294。[16] M. B. Yassein、F. Shatnawi、S. Rawashdeh 和 W. Mardin，《区块链技术：特征、安全与隐私问题及解决方案》，2019年 IEEE/ACS 第16届计算机系统与应用国际会议（AICCSA），阿布扎比，阿拉伯联合酋长国，2019年，第1–8页，doi: 10.1109/AICCSA47632.2019.9035216。[17] R. Henry、A. Herzberg 和 A. Kate，《区块链访问隐私：挑战与方向》，发表于 IEEE Security & Privacy，第16卷，第4期，第38–45页，2018年7/8月，doi: 10.1109/MSP.2018.3111245。[18] Aisha Zahid Junejo、Manzoor Ahmed Hashmani 和 Abdullah Abdulrehman Alabdulatif，《无许可区块链中的隐私漏洞调查》，International Journal of Advanced Computer Science and Applications（IJACSA），11(9)，2020年。http://dx.doi.org/10.14569/IJACSA.2020.0110915