区块链在 BGP 路由泄露防护中的应用研究

王群[1,2]，李馥娟[1,2]，马卓[1,2]

（1. 江苏省电子数据取证分析工程研究中心，江苏 南京 210031；
2. 江苏警官学院计算机信息与网络安全系，江苏 南京 210031）

摘　要：组成边界网关协议（BGP）的自治系统（AS）之间存在不同的利益关系和路由策略，当实际的路由宣告超出预期范围时，可能产生路由泄露，从而导致因路由重定向引起的网络安全事件。然而，在 BGP 路由信息传播过程中，AS 会无条件信任和接受邻居 AS 对外宣告的路由，而每个 AS 自主配置本地策略且信息保密，增加了路由策略验证的难度，成为 BGP 安全领域一直备受关注且尚未有效解决的难题。区块链以其独有的去中心化、可溯源、防篡改、开放透明等特征，可为 AS 间的数字资源认证与信任建立提供基础设施保障，有望成为应对路由泄露威胁的关键技术。首先，界定了邻居 AS 之间以及 GR（Gao-Rexford）模型与 BGP 路由策略之间的关系，明确了导致路由泄露的根源和防御挑战；然后，梳理了针对路由泄露的传统解决方案的研究脉络，重点分析了其优缺点以及尚未解决的问题；接着，提出了区块链技术在 BGP 路由泄露防护中的优势及技术思路，探讨了典型解决方案的实现原理和应用特点；最后，在阐述存在问题和挑战的基础上，对下一步研究进行了展望。

关键词：区块链；域间路由安全；路由源认证；路由泄露；IP 地址前缀

中图分类号：TP391　　**文献标志码：**A　　**DOI：**10.19678/j.issn.1000-3428.0070248

Research on Application of Blockchain in BGP Route Leakage Prevention

WANG Qun[1,2], LI Fujuan[1,2], MA Zhuo[1,2]

(1. Jiangsu Electronic Data Forensics and Analysis Engineering Research Center, Nanjing 210031, Jiangsu, China;
2. Department of Computer Information and Cybersecurity, Jiangsu Police Institute, Nanjing 210031, Jiangsu, China)

【Abstract】 Autonomous Systems (ASes) that constitute the Border Gateway Protocol (BGP) have different interests and route policies. When actual route announcements exceed expected boundaries, route leakages can occur, leading to network security incidents caused by route redirection. In the propagation of BGP route information, ASes unconditionally trust and accept the routes declared by neighboring ASes. Additionally, each AS independently configures its own local policies and keeps this information secret, which complicates the verification of this route policy. This has been a persistent and unresolved challenge in the field of BGP security. Blockchain technology, with its inherent characteristics of decentralization, traceability, immutability, and transparency, offers a promising infrastructure for digital resource authentication and trust among ASes, potentially serving as a key technology for addressing the threat of route leakages. This study first clearly defines the relationships between neighboring ASes, as well as between the GR (Gao-Rexford) model and BGP route policies, elucidating the root causes of route leakages and the challenges in their prevention. Additionally, it reviews the research on traditional solutions to route leakages, focusing on their strengths, weaknesses, and unresolved issues. Subsequently, it proposes the advantages and technical approaches of using blockchain technology to defend against BGP route leakages and explores the principles and application characteristics of typical solutions. Finally, it discusses the existing challenges and outlines future research directions.

【Key words】 blockchain; interdomain route security; Route Origin Attestation (ROA); route leakage; IP address prefix

0　引言

整个互联网由大量分布在不同国家和地区、由不同机构管理和运维的自治系统（AS）组成，这些系统数量庞大且分布广泛。每个 AS 是一个自治域，不同 AS 之间通过域间路由协议交换路由信息，边界网关协议（BGP）是互联网域间路由网络中事实上的协议标准。在 BGP 中，每个自治域分别属于不同的管理机构，负责本地路由策略的制定，具体细节由管理机构控制且一般不对外公开。每个自治域根据

收稿日期：2024-08-13　　**修回日期：**2024-11-20

基金项目：国家自然科学基金（62202209）；公安部科技计划项目（2023JSZ09）；教育部人文社会研究规划基金（24YJAZH158）。

通信作者 E-mail：wqun@jspi.edu.cn

自己的路由策略独立地选择路由，并将其结果宣告给邻居 AS。与域内网络中的路由策略相比，域间路由具有以下特点：1）因为需要综合考虑 AS 之间的利益关系、地缘政治、审查政策等复杂关系，所以路由策略的制定更为复杂[1-2]；2）因为 BGP 设计之初没有提供针对路由真实身份的验证机制，所以利用路由身份伪造虚假路由信息会构成安全威胁；3）任何一个 AS 都不会拥有一个完整的路径信息库，所有 AS 都在努力维护一个邻居 AS 关系，任何一次违反路由策略的错误配置或人为攻击都会导致 BGP 路由错误。在此情况下，BGP 安全威胁日趋严重，导致 IP 地址前缀劫持、AS 路径伪造和路由泄露事件频繁发生。

2021 年 4 月 16 日，沃达丰建在印度的自治系统（AS55410）发生路由泄露事件，将本该由 AS270497 对外宣告的前缀 24.152.117.0/24 劫持到了 AS55410，致使 AS55410 的 BGP 入站流量激增了 13 倍，包括谷歌在内的 2 万多个 AS 受到了该事件的影响[3]。2023 年 5 月 25 日，因对 BGP 路由策略的错误配置，从澳大利亚通往美国 Akamai（AS20940）和亚马逊 AWS（AS16509）的路由被劫持到了安哥拉电缆（AS37468），出现网络大面积严重延迟，这次路由泄漏持续了约 3 h[4]。可以看出，即使在全球普遍关注 BGP 安全的情况下，路由泄露事件依然频发，并造成流量黑洞、流量重定向、网络不可达、网络延迟等严重事件的发生。

针对 BGP 存在的安全威胁，互联网工程任务组（IETF）的安全域间路由（SIDR）工作组为路由源认证（ROA）[5]提出了一个标准化安全框架，即资源公钥基础设施（RPKI）[6]，用来验证路由宣告源 AS（origin AS）的合法性，从而防止 IP 地址前缀劫持攻击。BGPsec[7]利用数字签名机制，通过提供路由宣告 AS_path 属性中 AS 序列信息与真实传播路径的一致性验证机制来确保 AS 路径的完整性和正确性，从而有效防范 AS 路径伪造攻击。针对 BGP 存在的安全威胁，学术界、电信运营商和政府部门纷纷将希望寄托在 RPKI&BGPsec 身上，但终因中心化部署过程中存在的种种弊端（如增加计算开销、需要修改 BGP 协议、存在隐私泄露风险等）而未能得到广泛应用[8]。另外，RPKI&BGPsec 自身强调了对前缀劫持和路径伪造的检测和防御，并未提出针对路由泄露的有效解决方法。由于域间路由系统具有的大规模分布式特性，基于当前主流 RPKI&BGPsec 的域间安全模式难以实现不同 AS 之间的资源认证和可信协作。与此同时，快速发展的区块链技术因具有的去中心化、防篡改、公开透明、可溯源等属性，可以作为互联网不同实体之间资源认证和信任建立的基础设施[9]。另外，区块链技术在不依赖中心机构的前提下可有效保护不同 AS 之间的商业关系以及 AS 希望对外保密的路由策略，避免路由泄露事件的发生[10]。为此，在全面系统梳理已有成果及存在问题的基础上，加强对基于区块链的路由泄露防护技术的研究具有前瞻性和紧迫性。

如何将区块链技术应用于 BGP 安全增强，解决域间路由安全面临的难题，国内外研究者进行了积极探索，涌现出了一些新颖的方法和思路，如基于区块链的 ROA[11-12]、基于区块链的路由策略符合性验证[13-14]、智能合约在域间路由安全中的应用[15-16]、基于区块链的域间路由安全研究综述[17-18]等。然而，这些成果中专门将区块链应用于路由泄露防护的研究相对较少且不够系统。本文工作主要包括：首先，在系统梳理域间安全问题的基础上，重点分析路由泄露产生的内在原因以及传统安全机制存在的缺陷；其次，重点对区块链技术应用于路由泄露防护领域的研究进展进行详细梳理和深入讨论；最后，指出基于区块链的路由泄露防护技术的优势及亟待解决的问题，并对该领域的研究进行总结和展望。

1 背景知识

1.1 AS 之间的关系

在绝大多数情况下，AS 之间的关系的实质是一种商业利益关系。AS 之间根据事先建立的业务关系来交换流量，这些关系决定并形成了 BGP 路由策略，主要分为 3 类[19]：客户到服务提供商（C2P）关系，是指一个 AS 选择服务较好的邻居 AS，通过支付费用的方式将其负责运营的 customer 流量接入互联网；实体到实体（P2P）关系，是指两个服务提供商所拥有的网络或客户之间以免费方式来转发流量；兄弟到兄弟（S2S）关系，是指同一机构的 AS 之间交换流量时不受任何限制。在域间路由系统中，网络运营商一般根据与邻居 AS 之间的商业关系来确定自己的路由策略。

1.2 GR 模型与 BGP 路由策略

BGP 是基于策略的路径矢量域间路由协议，其核心功能是基于路由策略来发现和维护一条能够到达目的网络的路径。每一个自治域根据自身需要独立定义本地路由策略，而且本地路由策略的配置细节通常对外保密。

虽然 BGP 没有限定路由策略的具体细节，但 GAO 等[20]基于大部分自治域在商业利益、网络性

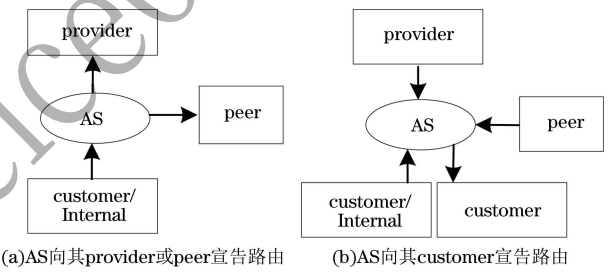
能、路由安全及流量工程等方面的需求，提出 GR(Gao-Rexford)模型，并建议各自治域能够执行。然而，各自治域出于自身利益的最大化一开始并未按照 GR 模型约定来配置本地路由策略，标准的缺失导致因错误配置和人为攻击引发的路由泄露行为严重威胁 BGP 安全。BGP 本地路由策略的对外保密性，使得邻居 AS 无法感知到已经发生的路由泄露行为，只会被动地将接收到的路由信息向下游 AS 继续转发，导致被泄露的路由信息以“合法”方式快速扩散。在意识到路由泄露问题的严重性后，大量自治域开始重新按照 GR 模型来配置本地路由策略，GR 模型再次引起了各 BGP 运营商的关注。

当一个自治域从其邻居 AS 接收到通往目的前缀的 BGP Update 消息时，首先根据路由表选择下一跳 AS，并将自己的 AS 号添加到 AS_path 属性列表中，从而完成路由宣告的转发。BGP 路由器在转发一个分组时需要同时考虑路由表和路由策略，其中路由策略是指自治域接收路由、选择路由和宣告路由的策略。BGP 路由策略主要包括入站策略和出站策略两部分，其中，BGP 入站策略是指自治域为其选择最佳本地路由的策略，即自治域根据自己的优先级过滤进入的路由宣告，具体通过对 BGP 的路径属性的设置来实现。与入站策略相关的路径属性主要包括 AS 路径 AS_path、本地优先级 Local_pref 和多出口标识符 Multi_exit_disc，其优先级表示为 Local_pref＞AS_path＞Multi_exit_disc，即本地优先级最高、AS 路径更短和多出口标识符最小的路由将会被选定为最佳路由。GR 模型的入站策略使用 customer 优先原则，即两个相邻 customer 之间的 Local_pref 高于两个相邻 peer 或相邻 provider 的 Local_pref。

BGP 出站策略是指自治域向其邻居宣告的最佳路由策略，即本自治域决定向其他自治域宣告的路由消息。在自治域完成路由选择后，将通过出站策略决定把选择的最佳路由宣告给哪些邻居 AS。出站策略的设置一般取决于 AS 之间的商业利益，一般是不对外公开的。GR 模型的出站策略设置遵循无谷底规则。

无谷底规则[21]作为 BGP 路由的一个属性，定义了一种可选择性地发布 BGP 路由且以最大限度地减小系统开销的路由模式。无谷底规则被广泛应用到 BGP 路由策略的制定中，它指出 AS 路径应符合以下模式之一：1）$n\times R_{C2P}+m\times R_{P2C}$；2）$n\times R_{C2P}+R_{P2C}+m\times R_{P2C}$，其中，$n$、$m\geqslant 0$。另外，S2S 连接可以存在于网络连接的任何位置。遵循其他模式的路由被认为是非无谷底规则的。出于经济利益考虑，AS 通常尽量避免在非客户之间直接传输流量，以节约网络宽带资源。根据 BGP 路由的无谷底规则，BGP 路由器的出站策略一般设置为[22]：将来自 customer 的路由宣告给所有 AS，而来自 provider 和 peer 的路由只宣告给本地 customer。另外，假设某一 AS 的 provider、peer 和 customer 都向其宣告了到达某一 IP 地址前缀的不同路由，AS 选择最佳路由的依据为：customer＞peer＞provider。

如图 1 所示，基于无谷底规则，根据不同 AS 之间的业务关系，可以将任意两个 AS 之间的有效路由宣告定义为以下两种情形之一[23]：如图 1(a)所示，当一个 AS 向其 provider 或 peer 宣告一条路由时，这条路由是 AS 的内部路由或其 customer 的一条路由；如图 1(b)所示，当一个 AS 向其 customer 宣告一条路由时，这条路由可以是 AS 内部路由、从 customer 学到的路由、从其他 peer 学到的路由或从 provider 学到的路由。



(a)AS向其provider或peer宣告路由　(b)AS向其customer宣告路由

图 1　AS 间的有效路由宣告

Fig. 1　Valid route advertisement between ASes

1.3　路由泄露

由于 BGP 在设计之初强调了功能实现而弱化了安全保障，致使 BGP 协议存在的设计缺陷和安全漏洞在应用中逐渐显现出来。BGP 设计上存在的最大缺陷是在路由传播过程中 AS 会无条件地信任和接受邻居 AS 对外宣告的任何路由，即使一个 AS 向外宣告了一个原本不属于自己的虚假 IP 地址前缀，也会被邻居 AS 无条件地接受并继续向下游传播，即 BGP 缺乏一个安全可信的路由检测和认证机制，其路由信息传播的真实性和完整性无法得到有效验证。BGP 路由泄漏是指实际的路由宣告超出了其预期范围，即一个 AS 向其邻居 AS 发布的路由违反了接收方、发送方以及上游某个 AS 的预期策略[24]。人为错误配置、软件缺陷和恶意攻击是产生路由泄露的主要原因，在出现路由泄露后，错误的 BGP 路由信息会在互联网上传播，将造成由网络流量重定向而引起的网络堵塞、次优路由、拒绝服务(DoS)攻击、流量窃听以及互联网运行的不稳定等现象发生。

路由泄露具有“虽然路由信息真实，但是路由传播非法”的特点，根据不同自治域之间存在的商业关系，可以将 BGP 路由泄露主要分为 customer 路由泄露和 peer 路由泄露两类[25]。customer 路由泄露的示例如图 2(a)所示，AS 4 是目的前缀 p 的真实拥有者，AS 4 在向外传播到达前缀 p 的路径过程中，AS 3 错误地将从本地 provider AS 2 处获得的路径传播给了本地的另一个 provider AS 1，根据 customer 优先选择原则，AS 1 优先选取从其 customer AS 3 处获得的路径 p:[3,2,4]作为最佳路径，从而使 AS 1 到 AS 4 的流量被重定向到 AS 3。图 2(b)所示的是 peer 路由泄露的一个示例，AS 3 是目的前缀 p 的真实拥有者，AS 5 在从 provider AS 2 处获得到达目的前缀 p 的路径后，错误地将其传播给本地的 peer AS 4，AS 4 会优先选取从 peer 处获得的路径 p:[5,2,3]，导致本来通过 AS 4→AS 1→AS 3 的流量变为 AS 4→AS 5→AS 2→AS 3，违反了无谷底规则。

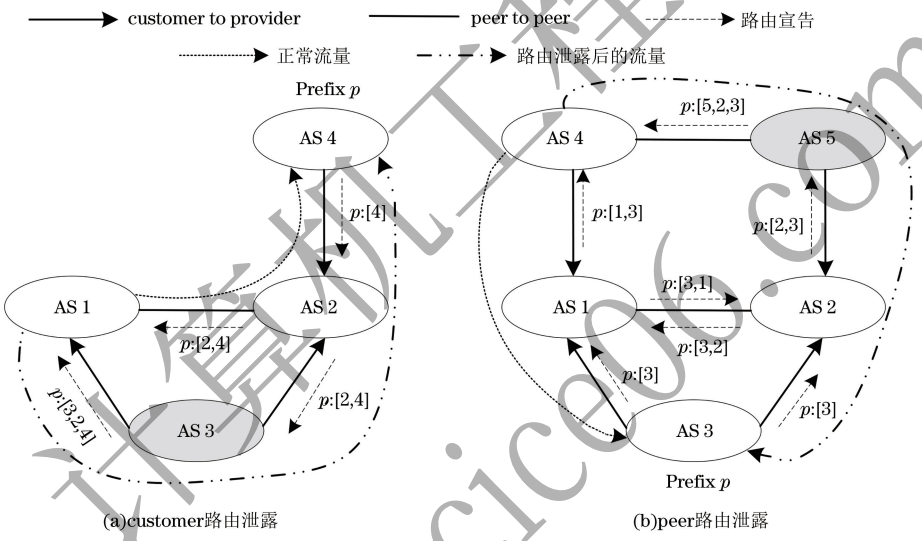


图 2 路由泄露典型示例

Fig. 2 Typical examples of route leakage

2 针对路由泄露的典型传统解决方案

虽然 GR 模型和无谷底规则为防范路由泄露提供了依据和参考，但如何通过有效的检测机制来发现路由泄露事件进行有效防范存在较大的挑战。本节针对路由泄露问题，对传统解决方案进行了梳理和分析。

2.1 互联网路由注册

互联网路由注册(IRR)[26]是一个开源的公共分布式数据库(http://www.irr.net/)，用于为 AS 提供注册和共享路由策略服务。通过使用 IRR 中的路由策略信息，AS 能够检测到被泄露的路由信息。然而，IRR 数据库由不同的区域互联网注册管理机构(RIR)或非权威机构(主要是一些私人组织)管理，这对信息的同步和全局一致性提出了挑战。

从目前应用看来，由于 IRR 提供的数据库质量不高，即 IRR 中不同网络服务提供商对 IP 地址、AS 号、路由策略等互联网资源的有效性得不到保障，因此 IRR 的服务功能并没有得到有效发挥。另外，庞大的注册数据对路由器产生了非常大的负担，同时 IRR 缺乏相应的监管机制，无法确保注册信息的真实性和完整性。此外，由于 IRR 自身存在大量的安全漏洞和不完善之处，因此现在很少有互联网运营商直接使用 IRR。

2.2 域间路由验证

域间路由验证(IRV)[27]是在 IRR 的基础上，结合 S_BGP[28]的设计思想提出的一个 BGP 安全方案。IRV 与 BGP 配合使用，用于验证 BGP 数据并获取与 AS 相关的附加路由信息，即一个 AS 能够为其他 AS 提供路由信息验证服务。具体而言，每个 AS 都专门提供了一台验证服务器，验证服务器中保存着该 AS 曾经向外宣告和传播过的路由信息以及本地路由策略信息，当其他 AS 需要对某条接收到的路由信息的有效性进行验证时，可以通过服务器完成。

IRV 的设计同样没有避开 S-BGP 的局限性，致使 IRV 的实现思路看起来简单明了，但却存在着无法回避的设计缺陷：一是无法确保验证服务器提供的验证信息的真实性和完整性，难以发现管理员的错误配置和 BGP 可能遭受的攻击行为，无法保障验证服务器的可信性；二是无法防范某些 AS 可能的作恶行为，恶意 AS 中的验证服务器可以对外提供

虚假的路由信息验证服务，欺骗 AS 对路由信息的验证。IRV 原本希望通过省略 S-BGP 中的地址证书来提高便捷性和效率，但却因此带来了严重的安全威胁，在互联网环境中无法得到大规模部署应用。

2.3 路由泄露保护

路由泄露保护(RLP)[29]通过在 BGP Update 消息中增加一个称为 Down-only 的共同体属性，用于检测和缓解路由泄露。当收到一条新路由消息时，AS 将会检查 Down-only 共同体的值，以决定是否将该条路由转发给上游 provider 或 peer。如果该路由来自 customer 或邻居 AS，而共同体没有向上游 AS 转发该路由，则将该路由标记为已泄露的路由。

然而，在路由传播过程中，缺乏相应的加密机制会导致 BGP 共同体的错误配置和 Down-only 的恶意修改或丢弃，影响 RLP 的服务质量和性能。从应用现状和技术发展来看，RLP 作为一种通过对 BGP Update 的功能扩展而实现的路由保护机制并未得到有效应用，但可以将 RLP 应用到其他存在加密机制的解决方案(如 BGPsec)中，以提升这些方案的性能。

2.4 RPKI&BGPsec

2008 年，IETF 成立 SIDR 工作组，综合 S-BGP 等方案的优点，提出了轻量化的 RPKI 架构。其核心标准(如 RFC 6480)于 2012 年发布，专注于 ROA。RPKI 充分借鉴了 S-BGP 的设计思想，依托现有的 IP 地址前缀和 AS 号等互联网资源分配层次结构，利用基于公钥密钥的数字签名和安全证书为互联网号码资源(INR)的所有权提供认证服务，相当于为合法数字资源分配一个可供全网查询的数字身份，从源路由的真实性、AS_path 属性中路径的完整性和路由传播过程的合规性等方面增强域间路由系统的安全性。其中，ROA 机制提供了针对 AS 的权限证明，即证明只有 ISP 机构已经被授权其 AS 使用某 IP 地址前缀时，该 AS 才是此 IP 地址前缀可达路由宣告的合法发起者。ROA 机制保证了 BGP 路由宣告中 origin AS 的合法性，即通过对 ROA 信息的认证来验证 AS_path 中的 origin AS 是否得到网络层可达信息(NLRI)的授权，从而可以有效防范路由劫持攻击的发生。

BGPsec 通过对 BGP 协议的扩展，利用路由器证书[30]和相应的数字签名机制保证 AS_path 属性中 AS 号序列与实际传播路径之间的一致性。AS 号拥有者为其 BGP 路由器签发数字证书，当一个路由器从其上一跳路由器接收到 AS_path 信息时，使用自己的私钥进行签名，并利用上一跳路由器的公钥证书验证路由宣告中数字签名的有效性，然后将签名结果作为 BGP Update 的一部分进行转发，以此来逐跳确保 AS 路径传播的真实性和完整性。

虽然 SIDR 工作组一直在推动 RPKI&BGPsec 的全球化部署，但由于 RPKI 主要是为了解决 BGP 路由劫持问题，因此 ROA 在应用于路由泄露的防护过程中显得无能为力。BGPsec 机制需要在全网部署后才能发挥其作用，然而受成本和系统开销等因素的限制，BGPsec 并未得到大部分 ISP 机构的认可。另外，BGPsec 只是利用签名机制实现了对包括错误配置的 AS 路径信息的可靠传播和有效验证，但却无法防范因错误配置而导致的路由泄露。由此可见，虽然 RPKI&BGPsec 作为一项 BGP 安全增强技术被业界寄予厚望，并希望通过大规模部署来解决互联网面临的路由安全威胁，但因其对路由系统带来的负担以及在增强 BGP 安全中存在的局限性，目前仅有约 50%的 IP 地址前缀使用 RPKI，并未实现预期的效果，尚有一些关键问题需要进一步研究解决。

2.5 ASPA

受 soBGP[31]机制中 AS 邻居间关系认证思想的启发，2021 年，IETF 在 RPKI 基础上提出了自治域提供商授权(ASPA)[32]方案，由 SIDROPS 工作组推动标准化，用于增强 BGP 路径验证。ASPA 采用 provider 和 customer 的概念来描述 AS 之间的关系，其中 provider 是指提供 BGP 路由的 AS(称为上游)，而将路由信息传播给 AS 的对象称为 customer(下游)，customer 的 AS 号添加在 AS_path 属性列表中。ASPA 通过对预先确认的 provider 发布的路由进行数字签名来验证路由信息的正确性，进而实现互联网信息基础设施的安全性和连通性。ASPA 对象的创建和部署方式与 ROA 相同，但是 ROA 表示哪些 AS 被授权发布给定的 IP 地址前缀，而 ASPA 表示哪些 AS 被允许传播它们的路由。例如，2022 年 12 月 17 日，AS945 创建的 ASPA 对象显示允许 AS1299、AS6939、AS32097、AS50058 这 4 个服务提供商传播其路由[33]。当某个 AS(如 AS61138)不在 ASPA 对象中时，就会返回“无效 AS”信息。ASPA 的记录可以在 RPKI 客户端或网站(https://console.rpki-client.org/aspa.html)上找到，或使用 rpki-client 工具(https://github.com/rpki-client/rpki-client-portable)查看 ASPA 对象。

ASPA 企图借助 RPKI 机制来对 AS_path 属性中的完整路径、AS 之间的可达性以及路由信息的

转发关系进行整体验证，其验证过程因不涉及复杂的密码学问题，所以对路由系统并未带来较大的负担。但是，ASPA 在设计之初对互联网路由的复杂性考虑不周，从而并未取得预期的效果。

另外，路由安全相互协议规范（MANRS）[34]是由国际互联网协会（ISOC）支持的倡议项目，该项目并非一项独立的技术解决方案，主要通过制度的确立和执行来提供一套服务和保障机制，鼓励和支持所有有助于减少路由误发和路由泄露的技术加入其中，同时建议所有网络运营商不仅要为其所有地址空间创建 ROA，而且要朝着验证这些路由的方向发展，即实现基于 RPKI 的源路由验证（ROV）[35]。一旦 ASPA 成为标准并被推广，就会有效记录和验证网络运营商之间的 BGP 关系。然而，MANRS 项目在推进过程中遇到了与 RPKI 类似的困难，其未来发展仍不明朗。

2.6 BGP Community

BGP Community[36]是一种用于简化路由策略配置与执行的内嵌于 BGP Update 报文的标识，可根据不同的业务应用（如语音通信、视频通信等）实现不同的路由处理策略。具体而言，通过引入 BGP Community 属性，可以为不同的业务应用分配不同的属性值，以便于在后续路由操作中基于这些属性值来执行路由策略，而不需要在每台路由器上逐条进行配置，既简化了策略的配置，又提高了策略执行过程的安全性和可控性。例如，在一个由多个 AS 组成的大型网络中，可以在其中一台路由器上为不同的业务应用配置相应的 Community 属性值，其他路由器可以通过匹配属性值的方式来间接地匹配本地路由条目。

Community 属性值的设置缺乏统一规范，因此需要该功能的多个 AS 必须协商一致，并约定共同遵守的私有标准，所以 Community 属性值的设置无法做到全网统一。另外，Community 属性是 BGP Update 报文中一个 4 Byte 的可选择功能项，其属性值以明文方式传输，易遭受攻击，其中代表不同业务应用的路由条目（Community 属性值）可能被篡改、伪造或删除，存在较大的安全威胁。

基于以上分析，表 1 分别从尚未解决的安全威胁、对现有路由的影响、是否更改 BGP 协议、部署情况等方面对典型的传统路由泄露防护方案进行了比较。

表 1 典型路由泄露防护方案比较

Table 1 Comparison of typical route leakage prevention schemes

解决方案	对现有路由的影响	是否更改 BGP 协议	未解决的安全威胁	部署情况
IRR	大	否	互联网数字资源质量不高，缺乏监控机制	曾经部署
IRV	较大	否	验证信息的质量不高，无法防范 AS 的作恶行为，会篡改或伪造 IRV 数据库	未部署
RLP	较小	是	缺乏保密机制，无法保障验证信息的真实性	未部署
RPKI&BGPsec	大	否	对路由泄露的防范有限，对现有路由系统带来了较大的负担，无法保障 RPKI 的安全性	部分部署
ASPA	小	否	无法实现对 AS_path 属性中传播路径的完整保护，无法防范作恶路由器对传播路径的篡改和伪造	未部署
BGP Community	小	否	缺乏全网统一的实施标准，Community 属性以明文传输，易遭受篡改、伪造或删除等攻击	私有部署

综上，虽然传统方案在解决路由泄露问题中发挥了重要作用，但这些方案存在部署困难、管理复杂以及单点故障、单边操作和单一信任等问题。目前，迫切需要通过一种机制的变革来从根本上寻求解决问题的途径。区块链技术具备去中心化、防篡改、公开透明、不需要信任支持以及提供增量部署等特征，保证了互联网数字资源分配与管理的真实性和一致性，并通过分布式账本为信息查询与验证提供了保障，为有效解决 BGP 路由泄露问题提供了一种全新的解决思路和实现路径。

3 区块链在防御 BGP 路由泄露中的应用

针对传统 BGP 路由泄露防护方案中存在的不足，区块链技术通过有效保护 AS 之间存在的不同利益关系，实现路由策略的对外保密，防止路由泄露。

3.1 区块链技术应用于防御路由泄露的具体思路

代表商业利益关系的路由策略独立于 BGP 协议，而且路由泄露问题并非 BGP 协议存在的安全问题，也没有违背协议的运行规则，只是因为人为失误

或关键路由设施遭受攻击后向外泄露了本不该对外公开的路由信息，这将导致传统针对 BGP 安全的检测技术失去了作用，增大了防御的难度。为此，在整个 BGP 安全研究中，对路由泄露的研究远比 IP 前缀劫持[37]、AS 路径伪造[38]等安全问题的研究复杂得多。路由泄露防护除需要在不同自治域间建立相互信任的资源认证和多方协作机制以外，更需要有效保护 AS 间的商业利益关系，保护 AS 路由策略的隐私性。研究表明：即使在全网部署 RPKI&BGPsec 的情况下，路由泄露仍然无法避免[39]，路由泄露问题是一个一直困扰 BGP 安全且尚未有效解决的问题。解决路由泄露问题存在两个难以协调的矛盾：1）难以协调好路由策略的可验证性与隐私保护需求之间的矛盾，实现可验证的前提是策略信息的共享和公开透明，而隐私保护对待信息的要求却恰好相反；2）难以处理好路由策略的全网一致性与 AS 策略的私有属性之间的矛盾，检测路由策略是否发生变化需要全网一致的路由信息支持，但 AS 策略却具有私有性和自治性特征。

区块链[40]是基于去中心化网络的分布式账本技术，通过特定数据结构将交易打包为按时间顺序连接的数据区块，通过密码学方式实现账本中数据的不可篡改和不可伪造，经数字签名的轻量级交易数据以开放方式供外部验证使用，共识机制在不可靠的异步网络节点之间实现了状态和数据的最终一致性和正确性。近年来，研究者开始将区块链技术应用于 BGP 安全增强，主要解决传统 BGP 安全方案在路由认证和 AS 间信息共享与协作中存在的问题，其研究思路[18,41-42]主要为：1）利用区块链的去中心化、开放共享、防篡改的信任机制，解决目前中心化安全机制带来的弊端，主要有单点故障、单边操作和单一信任；2）利用区块链的匿名性和分布式数据库特性，解决目前不同 AS 间信息彼此独立，无法实现信息协作共享的问题；3）利用区块链智能合约功能，实现互联网数字资源（主要包括 IP 地址前缀、AS 号等）在不同 AS 间的智能转移（区块链中的代币与 IP 地址之间存在着可转让但不能同时分配给多个持有者的共同之处），以及路由策略变化后的动态管理，解决 BGP 路由配置中存在的操作复杂和出错率高等问题。

将区块链应用于 BGP 路由泄露防护的核心思想是将区块链作为一个用于记录和验证路由策略并有效检测和验证 BGP Update 消息在传输过程中是否存在违背策略约定的平台，发挥区块链技术在解决传统安全问题时所具有的独有功能。具体内容为：1）将区块链作为域间路由信息的存储库，利用区块链的去中心化和不可篡改的特性，为域间路由建立一个不受任何第三方机构支配和控制的分布式、安全、可信的存储库；2）利用区块链创建一个功能类似于 RPKI 的分布式身份验证架构，并将其作为 RPKI 的替代方案，为资源管理建立一个简单有效的信任模型和开放的管理系统，其内容主要包括 IP 地址和 AS 号管理等；3）区块链可作为路由策略的分布式存储库，所有策略信息以公开透明、不可篡改的方式记录在链上，支持实时查询，确保策略数据的真实性与可验证性，并且利用区块链的匿名性可实现对路由策略隐私属性的有效保护。

3.2 基于区块链的去中心化路由泄露防护技术

通过对已有基于区块链的 BGP 安全增强技术的相关文献的梳理，本节选取了 ISRchain、基于区块链的路由验证模型（BRVM）、基于分布式处理方式的路由泄漏防护（PRLuDA）这 3 类典型的技术方案和应用场景。通过对这 3 类基于区块链的去中心化路由泄露防护方案架构和应用场景的讨论，分析区块链技术在解决路由泄露问题中的具体应用。

3.2.1 ISRchain

ISRchain[15]是一个基于区块链技术的域间安全路由框架，可以防御 IP 前缀劫持、AS 路径伪造和路由泄漏。该方案主要针对 RPKI 存在的单一信任缺陷，基于区块链和智能合约实现分布式验证和防篡改功能，尤其是利用智能合约的控制功能，允许用户在区块链上注册、分配、更新和撤销互联网信息资源。同时，ISRchain 通过提供的 IP 地址聚合功能，可以将路由条目聚合后存储在区块链中，可在确保功能实现的前提下尽量减少上链数据，优化数据存储结构。在 ISRchain 中，RIR 或本地互联网注册管理机构（LIR）等互联网信息资源管理机构可以将其持有的 IP 地址进行逐级分配，如 RIR 分配给 LIR，LIR 再分配给互联网服务提供商（ISP），然后将 IP 地址前缀与 AS 号进行绑定，并将 ROA 记录信息注册到区块链上进行管理。

ISRchain 采用 Raft 共识算法[43]，当 AS 需要加入 ISRchain 时，需要在 BGP 发言人路由器上运行一个区块链节点，并用公钥密码机制实现节点身份的标识与验证等功能，其中用公钥的哈希值标识节点的身份，而对应的私钥用于身份验证和签署交易数据。BGP 发言人的另一个主要功能是利用智能合约对接收到的 BGP Update 报文中的 AS 路径序列信息进行验证。如图 3 所示，ISRchain 提供了 IRM 合约和 ASI 合约这两类智能合约，其中 IRM

合约主要用于防御 IP 前缀劫持和 AS 路径伪造，ASI 合约主要用于防御路由泄露。IRM 合约称为互联网资源管理合约，它由互联网名称与数字地址分配机构（ICANN）创建和拥有，并由 xIR（RIR、NIR 和 LIR）共同管理，负责跟踪互联网资源的分配情况。具体而言，IRM 合约主要用于记录、更新和同步 AS 账号地址以及 IP 地址前缀与 AS 号之间的映射关系，使其他 AS 可以验证某个 IP 地址前缀与 AS 号之间的绑定关系。ASI 合约也称为 AS 信息合约，为每个 AS 所有，由其 BGP 发言人管理，用于跟踪 AS 邻居的业务关系和路由策略。AS 管理员负责每天在本地 ASI 合约中添加或删除策略信息，并将其广播到 ISRchain。因此，其他 AS 可以通过查询特定的 ASI 合约来验证 AS 间的关系和业务策略是否存在违背路由策略的现象，进而判断是否发生了路由泄露。

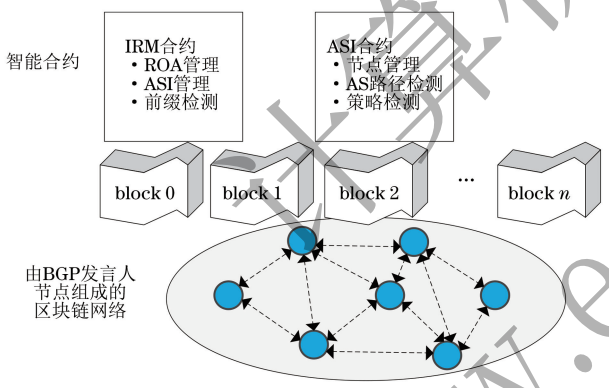


图 3 ISRchain 中的区块链与智能合约

Fig.3 Blockchain and smart contracts in ISRchain

ISRchain 架构具有 3 个明显优势：1）实现了 AS 之间的分散信任，得益于区块链内置的分布式账本特征，ISRchain 能够在不需要 RPKI 等中央权威机构介入的情况下实现 AS 之间的可信交互；2）高效的路由验证，BGP 路由消息通过本地解析 ISRchain 进行验证，只有必需的互联网资源和状态更新信息才被记录在区块链中，这种轻量级部署符合区块链对上链数据的要求，减轻了区块链上数据存储的压力；3）向后兼容，ISRchain 的应用无须修改 BGP 协议和现有的域间路由框架，因此可以实现增量级部署。同时，ISRchain 作为一个基于区块链的安全框架，力求同时解决 BGP 安全存在的 IP 前缀劫持、AS 路径伪造和路由泄露等问题，检测和防范路由泄露仅仅是其实现的部分功能。因此，ISRchain 对路由泄露问题缺乏针对性和系统性的解决方案。

ISRchain 基于无谷底规则，通过 AS 策略合规性检测以应对路由泄漏问题，是区块链应用于域间路由安全的较早的有效探索。在已有研究的基础上，该研究团队对增量部署的激励机制、可定制化的共识机制、复杂业务关系下的路由策略治理等方面展开了进一步研究。

3.2.2 BRVM

BRVM[14]的主要思想是利用区块链技术构建路由证明链，用于验证路由是否符合既定策略。BRVM 是针对安全和私有域间路由（SPIDeR）[44]无法应对多个作恶 AS 实施合谋攻击的情况下提出的一个优化方案，其不但能够发现单点攻击场景中的攻击源，而且能够发现多点攻击场景中的合谋者。在资源验证过程中，信息公开要求与隐私保护之间是相互矛盾的；在路由选择过程中，SPIDeR 能够在确保隐私保护的前提下验证接收到的 BGP 路由消息是否违反了路由策略。SPIDeR 将一个完整的策略划分成若干相关的子策略，然后通过子策略之间的协作来验证原有策略，同时对隐私进行保护。但是，SPIDeR 只有在存在单个作恶实体的情况下才能检测到违反策略的事件，同时在多个作恶实体相互串通时，该策略会失去功效，串通攻击有可能成功。

BRVM 使用了路由承诺来决定路由选择过程，AS 从接收到的多条路由中选择其中的一条作为“承诺”宣告给邻居 AS，邻居 AS 接受该承诺并将其加入路由表。然而，当两个相邻 AS 间建立了承诺后，如果一方在不遵守承诺的情况下宣告了一条次优或错误的路由，邻居 AS 并不会检查对方传入的路由是否正确，从而出现了恶意的路由泄露攻击。私有域间路由（PIDeR）的思想是协作验证承诺，处理方式是当某一 AS x 对从邻居 AS y 处接收到的路由存在怀疑时，AS x 可以向 AS y 的任一邻居 AS z 发送验证信息，并根据从 AS z 接收到的 AS_Path 属性中的 AS 路径长度进行判断。但是，如果 AS x 的邻居 AS z 与 AS y 进行合谋，AS x 同样会被欺骗。BRVM 不再使用 PIDeR 中 AS 间的协同验证方式，而是引入了一种基于区块链的分布式路由验证系统，它由用于验证路由证明的验证模块和用于存储路由证明的证明存储模块组成。验证模块由验证节点组成，证明存储模块由路由证明组成。当一个 AS 向邻居 AS 宣告一条路由的同时会向路由验证系统发送一个与该路由相对应的路由证明，该路由证明通过共识算法写入路由验证系统的区块中，这样在整个路由传输过程中，一个前缀的所有路由证明将形成

一条路由证明链。路由接收方通过查询区块链中是否存在相应的路由证明来确定接收到的路由是否符合路由承诺。

图 4 给出了 BRVM 工作过程的一个示例，主要有 4 个工作步骤：1）AS t 向其邻居 AS d 宣告一条带有自己数字签名的路由 d；2）AS d 对接收到的路由 d 的一些信息进行签名，并将签名结果回复给 AS t，其表示 AS d 收到了路由 d；3）AS t 用自己的签名构造一个路由证明 RP(d)，然后发送到验证系统的证明存储模块，验证系统对收到的路由证明进行验证，并将通过验证的路由证明写入区块链；4）AS d 接收到路由 d 时，将向验证系统中的验证模块发送一个用于验证路由 d 真实性的请求，在得到回复结果后决定如何处理路由 d。由此可以看出，BRVM 可以同时检测单点攻击和多点合谋攻击，而且能够发现其中的攻击者。

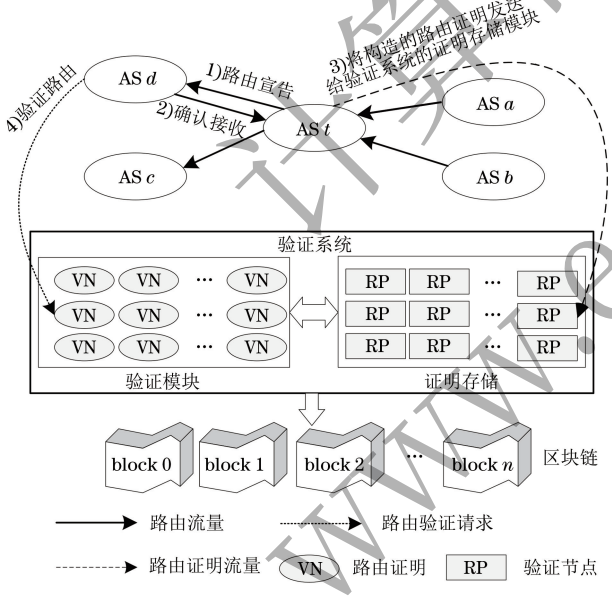


图 4 BRVM 工作示例

Fig. 4 BRVM working example

BRVM 的关键在于记录在区块链上的路由证明的正确性和完整性，违反承诺攻击发生的概率取决于区块链中的实用拜占庭容错(FBPT)[45]共识算法。BRVM 创新性地利用区块链技术来检测由单点和多点合谋引起的违反最短 AS 路径策略的攻击机制，但仍然有一些问题需要在下一步研究中进行解决：1）验证节点通过收集路由证明来推断其他 AS 的详细路由信息存在隐私泄露风险；2）路由验证系统的性能和可扩展性尚不能适应增量部署的要求；3）验证规则比较单一，只能验证 AS 是否违反了最短路径，不能验证除最短路径策略以外的其他路由策略。

3.2.3 PRLuDA

在域间路由安全中，路由泄露是指某个 AS 违反与对等 AS 商定的路由策略，擅自传播本不应共享的路由信息。虽然路由泄露的原理较为简单，但对网络安全的影响很大，解决方案也非常复杂。这是因为路由策略中包含了部分 AS 持有者不愿对外公开的信息，而且缺乏正式和规范的计算机语言来描述路由策略，同时 BGP 受自身算力和存储等资源的限制而缺乏足够的基于加密的安全性。针对此问题，GALMES 等[46]提出一种 PRLuDA 解决方案。该方案使用形式化语言表达路由策略，并将路由策略存储在区块链分布式账本中，供验证过程中查询。该方案还使用区块链架构来确保路由策略在传输过程中的安全性。在该方案中，将表示路由策略的形式化语言转换为标准的 BGP 路由过滤器，由参与 AS 且通过下载和安装标准的 BGP 路由过滤器来执行路由策略，防止路由泄漏。该方案的实现不需要更改 BGP 协议和 BGP 共同体，对现有 BGP 路由的影响较小，可实现增量部署。

在 PRLuDA 方案中，作者定义了一种形式化的表达语言，使用 BGP 共同体来表达路由策略，尽量避免路由策略的错误配置。形式化语言在基于区块链的解决方案中安全传输，同时加入方案的 AS 可以下载其他 AS 的策略，并使用标准的 BGP 路由过滤器自动安装，不需要更改 BGP 数据平面的路由策略。图 5 是 PRLuDA 工作过程的一个示例：1）定义一种表达式和形式化语言，该形式化语言可以让网络运营商能够以标准化的方式定义不同的路由策略，一旦路由策略被定义，就将其上传到区块链中，不同的 AS 之间可以共享区块链中的信息，并可以安全地传输由 AS 各自定义的路由策略；2）生成 BGP 路由过滤器，利用 BGP 路由过滤器的功能，使得 AS 之间已经存在的业务关系在得到彼此信任的同时也能使 AS 隐私能够得到有效保护，其中，BGP 路由过滤器[47]是域间路由系统中普遍使用的路由信息检测技术，该方案中使用编译器将形式化语言转换为标准 BGP 路由过滤器；3）安装 BGP 过滤器，参与的 AS 分别下载路由策略并安装到本地 BGP 路由器中，已安装的路由过滤器可以阻止可能导致路由泄漏的 BGP 更新消息的传播。

PRLuDA 方案还总结了用于定义不同路由策略的形式化语言，其建议的语言包含 5 个属性，即 ASN(AS 号)、CN(BGP 共同体号)、Rule(路由策

略)、Value(此属性为可选项,仅应用于某些类型的规则)和 To(此属性也为可选项,是指 Value 的规则所指的对象)。此外,该研究团队使用 Hyperledger 构建一个原型系统来对方案进行评估,同时使用真实网络中的 BGP 数据集对其性能进行了分析,结果达到了预期。

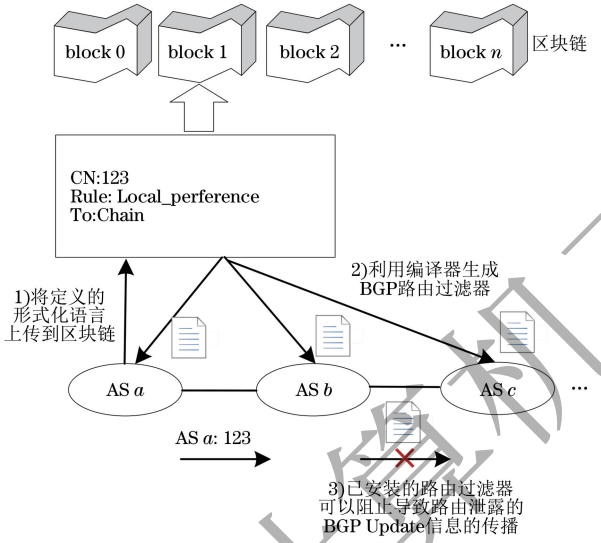


图 5 PRLuDA 工作示例

Fig.5 Working example of PRLuDA

除以上重点讨论的典型方案以外,ZENG 等[48]通过综合分析 AS 间业务关系的隐私性来研究路由泄漏问题,提出了一种基于区块链和联邦学习框架的路由泄漏检测方法,在不直接暴露业务关系的情况下,AS 可以训练全局检测模型。此外,该方法还提供了一种自我验证方案,通过将 AS 三元组(AS v –1 和 AS v+1 分别是 AS v 的邻居)标记为本地路由策略,从而减轻路由泄漏检测中缺乏有效参考值的问题。陈迪等[13]提出了一种基于区块链的域间路由策略合规性验证(IRPC)方案来防御路由泄漏,该方案包含策略期望和路由证明两种事务类型,AS 根据需求发布策略期望,如果需要指定一个 AS 来验证策略期望,则使用指定的 AS 公钥加密策略期望。IRPC 引入路由证明机制,为每条更新路由生成路由证明,并发布到区块链上,保证路由的真实传播。IRPC 不但可以通过路由策略的灵活配置来有效防御路由泄露,而且可以较好地保护 AS 的策略隐私。

表 2 分别从使用的共识算法、是否提供了策略的隐私保护功能、向后兼容性、区块链发挥的优势、区块链在防御路由泄露中的解决思路、方案目前存在的不足和应用效能等方面进行了比较。

表 2 典型基于区块链的路由泄露防护方案比较

Table 2 Comparison of typical blockchain-based route leakage defense schemes

解决方案	共识算法	隐私保护	向后兼容性	区块链的优势	区块链解决思路	存在的不足	应用效能
ISRchain	Raft	具备	兼容	存储策略和资源信息	由 BGP 发言人组成区块链网络,管理员维护本地策略并上传到区块链,然后利用智能合约检测违背路由策略的事件	缺乏激励机制,难以应对复杂策略的治理	本地模拟系统
BRVM	PBFT	需要加强	不兼容	构建一条路由证明链	构建基于区块链的分布式路由验证系统,一个 AS 向邻居 AS 宣告的路由都以路由证明方式写入区块链,AS 通过区块链验证路由的正确性	只能验证最短路由优先策略,可扩展性较差,仍存在隐私泄露风险,难以增量部署	原型系统
PRLuDA	PBFT	具备	兼容	存储路由策略	AS 将已定义的表达式和形式化语言上传到区块链,编译器生成路由过滤器,安装过滤器的路由器可以阻止可能发生的路由泄露	不能保证路径的真实性,恶意 AS 仍然可以篡改和宣告虚假路径进行攻击	开源原型系统

4 总结与展望

考虑到 BGP 的重要性以及 BGP 安全威胁愈加严峻,美国联邦通信委员会(FCC)在 2024 年 4 月通过《恢复网络中立性规则》[49]决议,虽未直接提出 BGP 监管条款,但其国家安全条款隐含对互联网路由安全(包括 BGP 漏洞)的关注,MANRS[50]在 2024 年 5 月举办的社区会议上将未来全球路由安全作为本次会议的主题。从近期全球各大组织和学术会议对 BGP 的重视程度也可以看出,在推进信息技术革命和全球信息化浪潮中,互联网的安全极其重要,而影响互联网运行安全的 BGP 协议的安全研究非常关键。在此情况下,研究 BGP 的安全问题尤其是路由泄露问题显得非常紧迫。区块链作为一项创新技术,在网络安全领域逐渐得到了探索性的应用[51-52],也为解决目前路由泄露问题存在的困难以及 BGP 安全挑战提供了方法和路径,但目前仍然存在一些需要进一步研究解决的问题和尚待明确的具

体研究方向。

4.1 基于区块链的去中心化方案

针对路由泄露的特殊性，在 RPKI&BGPsec 基础上融入区块链技术的安全方案无法有效防御路由泄露问题。根据现有研究，考虑到 RPKI&BGPsec 在域间路由安全研究和应用中的重要性，在解决路由泄露问题上，区块链技术的应用主要有两种不同的途径：一种是将区块链技术融入 RPKI&BGPsec，以此解决目前存在的问题；另一种是完全放弃 RPKI&BGPsec，构建一个基于区块链的去中心化平台。考虑到 RPKI&BGPsec 目前的应用现状，研究者也尝试将区块链技术作为一项附加功能融入 BGP 安全增强，构建一个融入区块链技术的以 RPKI 为主体的中心化方案，但这种设想在解决路由泄露问题上是不可行的，其原因为：

1）RPKI&BGPsec 未提供防御路由泄露的功能。RPKI 是一种专门针对 BGP 安全开发的基于 PKI 的安全基础设施，主要通过将 PKI 与 ICANN 分层数字资源相结合来保障 BGP 在平面路由信息控制中的安全性和完整性。具体而言，RPKI 在防御 IP 前缀劫持方面的表现优秀，但在防御 AS 路径伪造方面需要 BGPsec 的支持，而 RPKI&BGPsec 在防御路由泄露方面无能为力。

2）缺乏必要性。根据功能划分，可以将 RPKI 分为用于管理 IP 地址与 AS 号的证书授权（CA）侧以及提供认证服务的依赖方（RP）[53]侧，CA 侧和 RP 侧的功能都可以迁移到区块链上，但失去 CA 侧和 RP 侧功能的 RPKI 也将丧失了其功能定位。因此，单纯从解决路由泄露问题的角度出发，如何发挥区块链技术独有的功能特点和应用优势是未来的研究方向。

4.2 区块链应用于路由泄露防护的优势

与传统防御路由泄露方案相比，基于区块链的去中心化机制防御路由泄露方案的优势主要体现在提高管理效能和实现信任机制的去中心化部署 2 个方面：

1）提高管理效能。传统方案采用集中式管理方式，而且在许多情况下需要人工干预，可能存在因错误配置而出现的路由泄露风险，而这种路由泄露现象很难被发现，对路由泄露的排查和处理带来了极大的困难。基于区块链的路由泄露防护机制可以规避因集中部署带来的管理复杂、出错率高和单点故障等问题，可基于区块链的分布式认证方式来确认资源的唯一性和策略的专属性，同时区块链智能合约的应用可实现策略管理的自动化，可在没有专门第三方机构和其他分布式系统协同的情况下，自动完成策略信息的配置、更新和事件触发等任务，而且可以在各自治域间高效共享信息，有效提高管理效能。

2）实现信任机制的去中心化部署。本文介绍的 IRR、IRV、RLP、ASPA、BGP Community 等传统路由泄露防护方案存在着信任的中心化带来的管理的复杂化、易遭受恶意攻击、信任机构的监管困难等问题，尤其是几乎所有的互联网数字资源和路由策略存放在资源数据库中，很难保证数据的真实性、完整性和安全性。基于区块链技术，可以构建一个去中心化的分布式信任体系，有效解决传统方案存在的缺陷，主要优势有：(1)基于区块链分布式部署具有的抗攻击能力可以避免单点故障带来的风险；(2)基于密码学技术按时序生成的隐含哈希指针的链式数据结构，以及经数字签名后打包进区块的交易记录，可实现对路由策略的分布式存储和溯源，并可避免因集中式权威机构的不当操作带来的安全隐患；(3)证书的生成和管理不再依赖中心化的 RPKI 或 PKI，可以通过信任网络（WoT）[54]等机制生成和管理数字证书，建立灵活高效的信任机制；(4)基于区块链技术，提供了精准的策略与 AS 身份之间的对应关系，而身份标识的匿名性增加了路由策略的隐私保护能力。

4.3 基于区块链的去中心化路由防护方案存在的问题和挑战

作为一个崭新的研究领域，区块链应用于防御路由泄露研究和具体实践尚处于起步阶段，区块链自身存在的效率、兼容性、安全性等问题以及这些问题对区块链应用于防御路由泄露时的影响还需要进一步研究。

1）区块链的效率问题。目前比特币和以太坊平均每秒能处理的交易量分别为 3～7 笔和 7～20 笔[55]，根据 The BGP Instability Report[56]提供的信息，过去 14 天中 BGP 系统平均每秒处理 22.94 条 Update 报文，涉及 11.21 个路由前缀。虽然该站点没有对路由泄露进行专门分类，但路由泄露事件在整个 BGP 安全事件中的占比相对较小，所以从理论上讲比特币和以太坊等公有链提供的交易时延和吞吐量都能够满足路由策略管理的性能需求，但以太坊具有更大的应用和可扩展优势，同时可以结合侧链[57]、支付通道网络[58]、分片[59-60]等区块链扩展技术提升其性能，而且可以通过进一步优化或专门定制共识算法来提高系统的安全性。

2）兼容性问题。RPKI 部署中遇到的困难在基

于区块链的路由泄露防护机制中同样会遇到，其核心问题同样是系统之间的兼容问题，即如何使用区块链来记录 BGP 路由策略及更新信息，还需要考虑与现有 BGP 协议之间的兼容问题，以及与防御 IP 前缀劫持、AS 路径伪造等攻击的融合问题，其核心思想是在不影响 BGP 协议正常运行的前提下，跟踪且记录 BGP 路由宣告信息，并提供验证功能。同时，BGP 安全增强机制的实现需要全网协同才能取得预期效果，其间需要综合考虑现行 BGP 协议和 RPKI 机制之间的协调问题。这是一个系统工程，既要有系统的规划，又需要详细可行的实施计划。

3）区块链自身的安全问题。区块链技术为解决路由泄露问题提供了新思路，但在具体研究和实践探索过程中需要注意区块链自身的安全问题。遵循自底而上的基于体系结构的研究思路，区块链自身的安全问题主要表现为：

（1）数据层安全，主要涉及密码学技术在应用过程中的安全，重点为非对称加密和哈希函数的安全。

（2）网络层安全，主要涉及区块链目前采用的点对点[61]网络的安全，重点防范通过控制部分节点将受害节点从网络中进行隔离的日蚀攻击[62]，以及控制平面劫持某个 IP 地址或 AS 号并将其独立起来且不让矿工打包进区块的路由劫持攻击[63]等。

（3）共识层安全。共识算法的主要功能是实现网络中共识的最终一致性，由于区块链系统容忍恶意节点的数量是有限的，因此攻击者会通过控制一定数量的节点来破坏共识机制的运行。共识层存在的典型攻击方式主要有专门针对工作量证明（PoW）共识算法的 51%攻击[64]和自私挖矿攻击[64]，针对 PoS 共识算法的长程攻击[65]和无利害攻击[66]，以及针对 PBFT 共识算法的女巫攻击[67]等。

（4）智能合约层安全。智能合约[68]是一套以数字形式定义的由事件驱动的具有状态的承诺，其安全威胁主要为智能合约在实现过程中存在的安全漏洞，涉及智能合约的安全性验证[69]、攻击防范[70]等。

（5）应用层安全。应用层关联到不同的应用场景，涉及 API 接口、跨链[71]和监管等技术，每个方面都需要针对 BGP 路由泄露问题进行深入研究。

在将来的基于区块链的路由泄露防护机制研究中，如何有针对性地解决区块链自身存在的主要安全问题是下一步的研究方向和重点。

5 结束语

路由泄露是指路由器实际的对外宣告超过了其预期范围，即一个 AS 在将自身学习的 BGP 路由向另一个 AS 宣告时违反了接收方、发送方和/或上游 AS 路径上的某个 AS 的预期策略，从而产生流量的重定向，进而出现流量被窃听或控制等现象。从对历史数据的分析来看，路由泄露在绝大多数情况下是因意外的错误配置引起的，只有少数情况下是由恶意攻击所致的。本文在对传统路由泄露方案存在的问题进行系统分析的基础上，提出基于区块链的去中心化路由泄露防护技术的实现思路，并通过对典型解决方案实现原理的介绍和对比分析，对问题的关键点和解决问题的具体路线进行了梳理。然而，路由泄露因其发生机理的特殊性和不确定性，如何有效稳妥解决在目前还是一个难题，有待研究者更加深入的探究。下一步，本研究团队将集中对区块链技术自身的发展以及区块链与深度学习等技术的结合开展深入研究，为解决 BGP 路由泄露问题提供更加有效的方法与路径。

参考文献

[1] GILL P, SCHAPIRA M, GOLDBERG S. A survey of interdomain routing policies[J]. ACM SIGCOMM Computer Communication Review, 2013, 44(1): 28-34.

[2] XIANG Q, ZHANG J X, GAO K, et al. Toward optimal software-defined interdomain routing[C]//Proceedings of the IEEE Conference on Computer Communications. Washington D. C., USA: IEEE Press, 2020: 1529-1538.

[3] SHARMA A. Major BGP leak disrupts thousands of networks globally[EB/OL]. [2024-07-21]. https://www.bleepingcomputer.com/news/security/major-bgp-leak-disrupts-thousands-of-networks-globally/.

[4] SIDDIQUI A. BGP route leak at angola cables slows connectivity for many Australians[EB/OL]. [2024-07-21]. https://manrs.org/2023/05/bgp-route-leak-at-angola-cables-slows-connectivity-for-many-australians/.

[5] LEPINSKI M, KENT S, KONG D. A profile for Route Origin Authorizations (ROAs) (RFC 6482)[EB/OL]. [2024-07-21]. https://www.rfc-editor.org/rfc/pdfrfc/rfc6482.txt.pdf.

[6] LEPINSKI M, KENT S. An infrastructure to support secure Internet routing (RFC 6480)[EB/OL]. [2024-07-21]. https://www.rfc-editor.org/rfc/pdfrfc/rfc6480.txt.pdf.

[7] LEPINSKI M, SRIRAM K. BGPsec protocol specification (RFC 8025)[EB/OL]. [2024-07-21]. https://www.rfc-editor.org/rfc/pdfrfc/rfc8205.txt.pdf.

[8] CRONE M. Analyzing adoptability of secure BGP routing proposals[EB/OL]. [2024-07-21]. https://maxcrone.org/assets/docs/2021-02-01-secure-bgp-adoption.pdf.

[9] HARI A, LAKSHMAN T V. The Internet blockchain: a distributed, tamper-resistant transaction framework for the Internet[C]//Proceedings of the 15th ACM Workshop on Hot Topics in Networks. New York, USA: ACM Press, 2016: 204-210.

[10] YUE J R, QIN Y J, GAO S, et al. A privacy-preserving route leak protection mechanism based on blockchain[C]// Proceedings of the IEEE International Conference on Information Communication and Software Engineering (ICICSE). Wahington D.C., USA: IEEE Press, 2021: 264-269.

[11] 刘志辉，孙斌，谷利泽，等. 一种防范 BGP 地址前缀劫持的

源认证方案[J]. 软件学报, 2012, 23(7): 1908-1923.
LIU Z H, SUN B, GU L Z, et al. Origin authentication scheme against BGP address prefix hijacking[J]. Journal of Software, 2012, 23(7): 1908-1923. (in Chinese)
[12] HE G B, SU W, GAO S, et al. ROAchain: securing route origin authorization with blockchain for inter-domain routing [J]. IEEE Transactions on Network and Service Management, 2021, 18(2): 1690-1705.
[13] 陈迪, 邱菡, 朱俊虎, 等. 基于区块链的域间路由策略符合性验证方法[J]. 软件学报, 2023, 34(9): 4336-4350.
CHEN D, QIU H, ZHU J H, et al. Blockchain-based validation method for inter-domain routing policy compliance [J]. Journal of Software, 2023, 34(9): 4336-4350. (in Chinese)
[14] LIU Y P, ZHANG S, ZHU H J, et al. A novel routing verification approach based on blockchain for inter-domain routing in smart metropolitan area networks[J]. Journal of Parallel and Distributed Computing, 2020, 142: 77-89.
[15] CHEN D, BA Y, QIU H, et al. ISRchain: achieving efficient interdomain secure routing with blockchain [J]. Computers & Electrical Engineering, 2020, 83: 106584.
[16] 魏双, 吴旭, 张震. 工业物联网中基于区块链的跨域信任认证机制[J]. 小型微型计算机系统. 2024, 45(4): 975-983.
WEI S, WU X, ZHANG Z. Blockchain-based cross-domain trust authentication mechanism in industrial Internet of things. Journal of Chinese Computer Systems [J]. 2024, 45(4): 975-983. (in Chinese)
[17] 陈迪, 邱菡, 朱俊虎, 等. 区块链技术在域间路由安全领域的应用研究[J]. 软件学报, 2020, 31(1): 208-227.
CHEN D, QIU H, ZHU J H, et al. Research on blockchain-based interdomain security solutions [J]. Journal of Software, 2020, 31(1): 208-227. (in Chinese)
[18] MASTILAK L, HELEBRANDT P, GALINSKI M, et al. Secure inter-domain routing based on blockchain: a comprehensive survey[J]. Sensors, 2022, 22(4): 1437.
[19] LUCKIE M, HUFFAKER B, DHAMDHERE A, et al. AS relationships, customer cones, and validation [C]// Proceedings of the 2013 Conference on Internet Measurement Conference. New York, USA: ACM Press, 2013: 243-256.
[20] GAO L X, REXFORD J. Stable Internet routing without global coordination [C]// Proceedings of the 2000 ACM SIGMETRICS International Conference on Measurement and Modeling of Computer Systems. Washington D. C., USA: IEEE Press, 2001: 681-692.
[21] GIOTSAS V, ZHOU S. Valley-free violation in Internet routing—analysis based on BGP community data [C]// Proceedings of the IEEE International Conference on Communications (ICC). Washington D. C., USA: IEEE Press, 2012: 1193-1197.
[22] HUSTON G. The ISP column/leaking routes [EB/OL]. [2024-07-21]. https://www.potaroo.net/ispcol/2025-05/leak.pdf.
[23] GAO L. On inferring autonomous system relationships in the Internet [J]. IEEE/ACM Transactions on Networking, 2001, 9(6): 733-745.
[24] SRIRAM K, MONTGOMERY D, MCPHERSON D, et al. Problem definition and classification of BGP route leaks(RFC 7908) [EB/OL]. [2024-07-21]. https://www.rfc-editor.org/rfc/pdfrfc/rfc7908.txt.pdf.
[25] SRIRAM K, MONTGOMERY D, MCPHERSON D, et al. RFC 7908: problem definition and classification of BGP route leaks[EB/OL]. [2024-07-21]. https://www.rfc-editor.org/rfc/pdfrfc/rfc7908.txt.pdf.
[26] KUERBIS B, MUELLER M. Internet routing registries, data governance, and security[J]. Journal of Cyber Policy, 2017, 2(1): 64-81.
[27] GOODELL G, AIELLO W, GRIFFIN T, et al. Working around BGP: an incremental approach to improving security and accuracy of interdomain routing [EB/OL]. [2024-07-21]. https://www.cs.purdue.edu/truselab/readings/ndss03.pdf.
[28] KENT S, LYNN C, SEO K. Secure Border Gateway Protocol (S-BGP) [J]. IEEE Journal on Selected Areas in Communications, 2002, 18(4): 582-592.
[29] SRIRAM K, MONTGOMERY D. Methods for detection and mitigation of BGP route leaks [EB/OL]. [2024-07-21]. https://www.ietf.org/proceedings/92/slides/slides-92-idr-8.pdf.
[30] REYNOLDS M, TURNER S, KENT S. A Profile for BGPsec router certificates, certificate revocation lists, and certification requests (RFC 8209) [EB/OL]. [2024-07-21]. https://www.rfc-editor.org/rfc/pdfrfc/rfc8209.txt.pdf.
[31] WHITE R. Securing BGP through secure origin BGP (soBGP) [J]. Business Communications Review, 2003, 33(5): 47-53.
[32] UMEDA N, KIMURA T, YANAI N. The juice is worth the squeeze: analysis of autonomous system provider authorization in partial deployment[J]. IEEE Open Journal of the Communications Society, 2023, 4: 269-306.
[33] SIDDIQUI A. Unpacking the first route leak prevented by ASPA[EB/OL]. [2024-07-21]. https://manrs.org/2023/02/unpacking-the-first-route-leak-prevented-by-aspa/.
[34] GALLO A. MANRS as fire code[EB/OL]. [2024-07-21]. https://manrs.org/2024/06/manrs-as-fire-code/.
[35] HLAVACEK T, HERZBERG A, SHULMAN H, et al. Practical experience: methodologies for measuring route origin validation[C]//Proceedings of the 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). Washington D. C., USA: IEEE Press, 2018: 634-641.
[36] DONNET B, BONAVENTURE O. On BGP communities [J]. ACM SIGCOMM Computer Communication Review, 2008, 38(2): 55-59.
[37] SPADACCINO P, BRUZZESE S, CUOMO F, et al. Analysis and emulation of BGP hijacking events [C]// Proceedings of the 2023 IEEE/IFIP Network Operations and Management Symposium. Washington D. C., USA: IEEE Press, 2023: 1-4.
[38] ZHANG C W, MIAO C C, AN C Q, et al. Metis: detecting fake AS-PATHs based on link prediction[C]//Proceedings of the IEEE Symposium on Computers and Communications (ISCC). Washington D. C., USA: IEEE Press, 2023: 656-662.
[39] GOLDBERG S, SCHAPIRA M, HUMMON P, et al. How secure are secure interdomain routing protocols[J]. ACM SIGCOMM Computer Communication Review, 2010, 40(4): 87-98.
[40] 张亮, 刘百祥, 张如意, 等. 区块链技术综述[J]. 计算机工程, 2019, 45(5): 1-12.
ZHANG L, LIU B X, ZHANG R Y, et al. Overview of blockchain technology [J]. Computer Engineering, 2019, 45(5): 1-12. (in Chinese)
[41] SAAD M, ANWAR A, AHMAD A, et al. RouteChain: towards blockchain-based secure and efficient BGP routing [J]. Computer Networks, 2022, 217: 109362.
[42] YANG Q, MA L, TU S S, et al. Towards blockchain-based secure BGP routing, challenges and future research directions [J]. Computers, Materials & Continua, 2024, 79(2): 2035-2062.
[43] ONGARO D, OUSTERHOUT J. The raft consensus algorithm[EB/OL]. [2024-07-21]. https://raft.github.io/slides/riconwest2013.pdf.
[44] ZHAO M C, ZHOU W C, GURNEY A J T, et al. Private and verifiable interdomain routing decisions[J]. IEEE/ACM

Transactions on Networking, 2015, 24(2): 1011-1024.
[45] SAKHO S, ZHANG J B, ESSAF F, et al. Research on an improved practical Byzantine fault tolerance algorithm[C]// Proceedings of the 2nd International Conference on Advances in Computer Technology, Information Science and Communications (CTISC). Washington D.C., USA: IEEE Press, 2020: 176-181.
[46] GALMES M F, AUMATELL R C, CABELLOS-APARICIO A, et al. Preventing route leaks using a decentralized approach[C]// Proceedings of 2020 IFIP Networking Conference. Washington D.C., USA: IEEE Press, 2020: 509-513.
[47] GILAD Y, COHEN A, HERZBERG A. Are we there yet? On RPKI's deployment and security[EB/OL]. [2024-07-21]. https://eprint.iacr.org/2016/1010.pdf.
[48] ZENG M, LI D D, ZHANG P, et al. Federated route leak detection in inter-domain routing with privacy guarantee[J]. ACM Transactions on Internet Technology, 2023, 23(1): 1-22.
[49] The United States Federal Communications Commission. Safeguarding and securing the open Internet[EB/OL]. [2024-07-21]. https://docs.fcc.gov/public/attachments/DOC-401676A1.pdf.
[50] MANRS. MANRS community meeting-15 May 2024[EB/OL]. [2024-07-21]. https://manrs.org/event/manrs-community-meeting-may-2024/.
[51] MANIMURGAN S, ANITHA T, DIVYA G, et al. A survey on blockchain technology for network security applications[C]// Proceedings of the 2nd International Conference on Computing and Information Technology (ICCIT). Washington D.C., USA: IEEE Press, 2022: 440-445.
[52] 徐恪, 凌思通, 李琦, 等. 基于区块链的网络安全体系结构与关键技术研究进展[J]. 计算机学报, 2021, 44(1): 55-83.
XU K, LING S T, LI Q, et al. Research progress of network security architecture and key technologies based on blockchain[J]. Chinese Journal of Computers, 2021, 44(1): 55-83. (in Chinese)
[53] FRIESS J, MIRDITA D, SCHULMANN H, et al. Byzantine-secure relying party for resilient RPKI[EB/OL]. [2024-07-21]. https://arxiv.org/pdf/2405.00531.
[54] SYTA E, TAMAS I, VISHER D, et al. Keeping authorities "honest or bust" with decentralized witness cosigning[C]// Proceedings of the IEEE Symposium on Security and Privacy (SP). Washington D.C., USA: IEEE Press, 2016: 526-545.
[55] WILKIE A, SMITH S S. Blockchain: speed, efficiency, decreased costs, and technical challenges[M]. [S.l.]: Emerald Publishing Limited, 2021.
[56] The BGP instability report[EB/OL]. [2024-07-21]. https://bgpupdates.potaroo.net/instability/bgpupd.html.
[57] SINGH A, CLICK K, PARIZI R M, et al. Sidechain technologies in blockchain networks: an examination and state-of-the-art review[J]. Journal of Network and Computer Applications, 2020, 149: 102471.
[58] PAPADIS N, TASSIULAS L. Blockchain-based payment channel networks: challenges and recent advances[J]. IEEE Access, 2020(8): 227596-227609.
[59] CHOW S S M, LAI Z L, LIU C, et al. Sharding blockchain[C]//Proceedings of the IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). Washington D.C., USA: IEEE Press, 2018: 1665.
[60] 黄华威, 孔伟, 彭肖文, 等. 区块链分片技术综述[J]. 计算机工程, 2022, 48(6): 1-10.
HUANG H W, KONG W, PENG X W, et al. Survey on blockchain sharding technology[J]. Computer Engineering, 2022, 48(6): 1-10. (in Chinese)
[61] DELGADO-SEGURA S, PÉREZ-SOLÀ C, HERRERA-JOANCOMARTÍ J, et al. Cryptocurrency networks: a new P2P paradigm[J]. Mobile Information Systems, 2018(1): 2159082.
[62] DAI Q Y, ZHANG B, DONG S Q. Eclipse attack detection for blockchain network layer based on deep feature extraction[J]. Wireless Communications and Mobile Computing, 2022(1): 1451813.
[63] SAAD M, COOK V, NGUYEN L, et al. Partitioning attacks on Bitcoin: colliding space, time, and logic[C]// Proceedings of the IEEE 39th International Conference on Distributed Computing Systems (ICDCS). Washington D.C., USA: IEEE Press, 2019: 1175-1187.
[64] NAYAK K, KUMAR S, MILLER A, et al. Stubborn mining: generalizing selfish mining and combining with an eclipse attack[C]//Proceedings of the IEEE European Symposium on Security and Privacy (EuroS&P). Washington D.C., USA: IEEE Press, 2016: 305-320.
[65] DEIRMENTZOGLOU E, PAPAKYRIAKOPOULOS G, PATSAKIS C. A survey on long-range attacks for proof of stake protocols[J]. IEEE Access, 2019, 7: 28712-28725.
[66] LI W T, ANDREINA S, BOHLI J M, et al. Securing proof-of-stake blockchain protocols[M]. Berlin, Germany: Springer International Publishing, 2017.
[67] PLATT M, MCBURNEY P. Sybil in the haystack: a comprehensive review of blockchain consensus mechanisms in search of strong sybil attack resistance[J]. Algorithms, 2023, 16(1): 34.
[68] KHAN S N, LOUKIL F, GHEDIRA-GUEGAN C, et al. Blockchain smart contracts: applications, challenges, and future trends[J]. Peer-to-Peer Networking and Applications, 2021, 14(5): 2901-2925.
[69] CHU H T, ZHANG P C, DONG H, et al. A survey on smart contract vulnerabilities: data sources, detection and repair[J]. Information and Software Technology, 2023, 159: 107221.
[70] ALKHALIFAH A, NG A, WATTERS P A, et al. A mechanism to detect and prevent ethereum blockchain smart contract reentrancy attacks[J]. Frontiers in Computer Science, 2021, 3: 598780.
[71] OU W, HUANG S Y, ZHENG J J, et al. An overview on cross-chain: mechanism, platforms, challenges and advances[J]. Computer Networks, 2022, 218: 109378.

编辑 陆燕菲