RPKI去中心化安全增强技术综述

秦超逸[1]，张宇[1,2]，方滨兴[2,3]
（1.哈尔滨工业大学网络空间安全学院，黑龙江 哈尔滨 150001；2.鹏城实验室，广东 深圳 518055；
3.广州大学网络空间先进技术研究院，广东 广州 510006）

摘 要：资源公钥基础设施（RPKI）搭建了中心层级化的IP地址资源认证基础设施。在增强互联网域际路由系统安全的同时，RPKI也将中心性引入路由系统。根据证书认证中心职能，提出RPKI体系中的认证中心、操作中心和发布中心，并从3个中心对RPKI去中心化安全增强技术综述。首先，从认证、操作和发布角度细化RPKI中心化风险。其次，从3个风险角度分类RPKI去中心化安全增强技术的技术思路和解决措施。再次，从安全性、可扩展性和增量部署分析比较相关技术。最后，总结存在的问题并展望未来的研究方向。

关键词：边界网关协议；资源公钥基础设施；域间路由安全；区块链；去中心化
中图分类号：TP393
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2024102

Survey on decentralized security-enhanced technologies for RPKI

QIN Chaoyi[1], ZHANG Yu[1,2], FANG Binxing[2,3]
1. School of Cyberspace Science, Harbin Institute of Technology, Harbin 150001, China
2. Pengcheng Laboratory, Shenzhen 518055, China
3. Cyberspace Institute of Advanced Technology, Guangzhou University, Guangzhou 510006, China

Abstract: The resource public key infrastructure (RPKI) deploys a centralized and hierarchical infrastructure for the authorization of IP addresses. It not only enhances the security of the Internet border gateway protocol system, but also introduces centralization into the routing system. According to the functions of the certificate authorities, the authorization center, operation center, and publication center in the RPKI were proposed, and a comprehensive survey on decentralized security-enhanced technologies for the RPKI were presented based on these three centers. Firstly, RPKI centralization risks were refined from the perspective of authorization, operation and publication. Secondly, the technical ideas and solutions of decentralized security-enhanced technologies were classified into these three perspectives. Thirdly, technologies were compared in terms of security, scalability, and incremental deployment. Finally, the existing problems in current technologies were summarized and the future research directions were prospected.

Keywords: border gateway protocol, resource public key infrastructure, secure inter-domain routing, blockchain, decentralization

收稿日期：2023–12–26；**修回日期：**2024–05–08
通信作者：张宇，yuzhang@hit.edu.cn
基金项目：国家重点研发计划基金资助项目（No.2022YFB3104800）；鹏城实验室重大攻关基金资助项目（No.PCL2023A05）
Foundation Items: The National Key Research and Development Program of China (No.2022YFB3104800), The Major Key Project of PCL (No.PCL2023A05)

0　引言

资源公钥基础设施（RPKI, resource public key infrastructure）[1]作为一项边界网关协议（BGP, border gateway protocol）安全增强基础设施，旨在解决IP地址前缀劫持风险。根据互联网数字资源（IP地址和自治域（AS）号）的分配体系，RPKI以公钥基础设施（PKI, public key infrastructure）[2]为基础构建资源认证体系，提供对IP地址前缀路由起源AS号（IP-AS）合法性的保护。RPKI通过签发资源证书[3]对互联网数字资源分配进行授权，并通过签发路由源认证（ROA, route origination authentication）[4]授权IP-AS。

2008年4月，互联网工程任务组的安全域间路由（SIDR, secure inter-domain routing）工作组开始开发RPKI，并于2012年开始正式生产部署[5]。同年，SIDR发布了相关的征求意见稿（RFC）标准文档对RPKI相关基础协议进行标准化[6]。目前有近40篇与RPKI相关的RFC标准文档，包括RPKI基础框架、RPKI各类对象结构、RPKI验证流程、BGP起源验证等内容。

为了支持RPKI的部署，业界按照RPKI标准化文档实现RPKI相关的软件。RPKI证书颁发机构（CA, certificate authority）软件负责RPKI证书、ROA等对象的管理。目前公开的CA软件有Krill和rpki.net[7]。Krill是由NLnet Labs开发的基于Rust语言的开源免费CA软件；rpki.net由美国互联网号码注册中心（ARIN, American Registry for Internet Numbers）和美国国土安全部资助，Dragon Research Labs开发，并基于Python实现。依赖方（RP, replying party）[8]软件负责获取、验证RPKI对象，从有效的ROA中提取IP-AS数据发送给路由器。目前常用的RPKI依赖方软件有8种[7]，如表1所示。Friedemann等[9]从安装易用性、性能、结果一致性、代码质量、适用性和功能丰富性6个方面对RP软件进行了评估，发现Routinator在各个方面均表现较好，因此在实际生产部署中推荐使用Routinator。

RPKI网络覆盖规模持续增加[5,10-14]。截至2023年12月，RPKI已覆盖互联网48.03%的IP地址前缀，而47.35%的IPv4前缀和51.26%的IPv6前缀被ROA覆盖。

然而RPKI采用的中心层级化体系造成了IP地址权力失衡，也阻碍了RPKI的全面部署。Cooper等[15]在2013年首次提出了RPKI存在的中心化风险。人工运维不可避免地出现误配置、误操作等失误，甚至蓄意破坏；而中心层级化体系将高层级人工运维的失误和破坏向下扩散，导致低层级需承受自身之外的风险，令低层级的合法BGP路由通告丧失保护，甚至无法在互联网中传播。RFC 8211[16]中总结了高层级CA各种可行恶意操作及其带来的影响，这种中心化风险降低了低层级机构部署RPKI的积极性。此外，RPKI的中心化风险可能加剧域间路由的安全问题，位于RPKI高层级的攻击者可以通过RPKI单边操作发布对应ROA配合劫持攻击，若劫持攻击的路由条目起源验证结果为有效，则会使非法的劫持“合法化”[14]，导致劫持攻击更容易成功。RPKI的中心化体系是中心化风险存在的根本原因，可采用去中心化方案，通过减弱或者分散单一CA的权力来解决中心化风险。

目前，许多工作力求化解和应对RPKI的中心化风险。苏莹莹等[17]从RPKI技术现状、RPKI存在问题及研究进展和RPKI功能扩展等方面展开了综述，在RPKI存在问题方面简述了对RPKI资料库对象的恶意操作问题以及基于区块链的去中心化解决

表1　RPKI依赖方软件

名称	开发语言	开发团队	发布年份	是否仍在维护
FORT Validator	C	NIC.MX	2019年	是
rpki.net	Python/C	Dragon Research Labs	2012年	否
rpki-client	C	OpenBSD project	2019年	是
OctoRPKI	Go	Cloudflare	2019年	是
Routinator	Rust	NLnet Labs	2019年	是
RIPE NCC Validator 3	Java	RIPE NCC	2019年	否
RPSTIR2	Go	ZDNS	2020年	是
rpki-prover	Haskell	Mikhail Puzanov等	2020年	是

方案，并未专门针对去中心化方案进行分析。Su等[18]将基于区块链的域间路由认证分为RPKI替代方案和RPKI增强方案两类，并讨论了基于区块链的方案在性能、部署以及安全性方面的问题。Mastilak等[19]从区块链类型、起源验证、路径验证、策略验证和可扩展性角度比较分析了基于区块链的域间路由技术，重点总结了区块链对域间路由带来的增强、现有区块链方案及技术特点、共识机制选择对性能的影响、区块链性能对BGP可扩展性的影响以及区块链膨胀的解决这5个方面的问题。徐恪等[20]分析了基于区块链的RPKI去中心化相关工作，根据实现目标不同分为构建去中心化RPKI和实现路径验证两类。上述工作仅局限于基于区块链的去中心化方案，缺少对非区块链的去中心化方案的阐述。邹慧等[6]综述了RPKI研究现状，包括层级信任模型引入的安全风险与保障技术，并根据部署实体将保障技术分为基于CA和基于RP两类展开分析，但分析涉及相关技术较少。

本文与以上相关工作的区别在于将RPKI中心化安全增强技术按照认证中心、操作中心和发布中心划分为3个维度分类介绍，包含基于区块链和基于非区块链的RPKI去中心化方案，并就安全性、可扩展性和增量部署能力3个方面进行比较分析。

本文的主要工作如下。

1) RPKI安全增强技术机制总结介绍。从RPKI体系的认证中心、操作中心、发布中心3个维度，分析RPKI中心化安全增强技术解决中心化安全风险的主要技术思路。

2) 安全增强技术分析。从安全性、可扩展性和增量部署能力3个方面比较分析RPKI安全增强技术：安全性上，除新机制的风险之外，技术方案均可解决部分或全部的中心化风险；可扩展性上，各技术方案均可满足BGP日常运维需求；增量部署上，部分技术方案依赖一定基础设施搭建后才可支持增量部署。

1 RPKI中心化安全风险

1.1 RPKI中心性

RPKI构建了一套中心层级化的IP地址分配和IP-AS认证体系，体系由地区性互联网注册机构（RIR, regional Internet register）、国家互联网注册机构（NIR, national Internet register）、本地互联网注册机构（LIR, local Internet register）和互联网服务提供商（ISP, Internet service provider）等IP地址资源相关机构担任CA参与维护。IP-AS认证数据直接由IP地址所有者直接发布，表示为ROA中的IP地址前缀集合与授权声明前缀的AS号；IP地址所有权经由CA实现层级化认证，所有权认证的结果表示为CA证书中的IP地址前缀集合与所有者公钥。

RPKI从数据角度划分为提供IP-AS认证数据的CA侧和使用认证数据的RP侧，如图1所示。CA侧认证IP地址资源分配，签发CA证书和ROA等RPKI对象并维护分布式RPKI资料库。RP侧逐级访问资料库获取RPKI对象，通过以信任锚为起点的CA证书链验证ROA并提取IP-AS数据应用于路由器，实现对BGP路由通告的前缀起源验证（ROV, route origin validation）[21]。

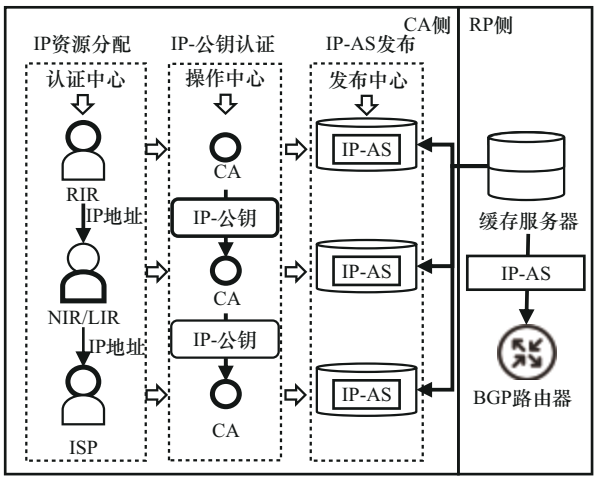

图1 RPKI中心性原理框架

RPKI体系具有中心性，本文将RPKI体系根据职能划分为认证中心、操作中心和发布中心共3个中心。

1) 认证中心表示RPKI认证IP地址分配结果的职能，RIR、NIR、LIR等互联网机构管理CA来发布证书，提供IP地址分配结果的认证；RP侧根据CA证书逐级获得IP地址当前所有者并验证所有者发布的IP-AS。

2) 操作中心表示CA操作RPKI对象的职能，CA可操作自己发布的RPKI对象反映IP地址分配结果的变化，操作由CA单边执行且不受下级CA干预。

3) 发布中心表示资料库发布RPKI对象的职能，每个CA的资料库作为CA签名对象的唯一发布源，由CA或托管的资料库管理者作为唯一维护者，RP侧逐级访问所有资料库获取所有RPKI对象。

1.2　RPKI中心化安全威胁分析

RPKI中心性影响了IP地址资源管理权力的平衡，3个中心导致了3个维度的中心化风险。

1) 认证风险–单点认证。认证反映IP地址所有权分配，层级化架构中每个RPKI对象依赖于从信任锚起始的单一证书链提供IP地址所有权认证。单点认证针对认证中心，导致下级认证受制于上级，一旦上级拒绝为下级认证或为下级提供错误的认证，下级将失去IP地址所有权以及IP再分配的认证能力。

2) 操作风险–单边操作。操作反映IP地址所有权分配变化的结果（IP-公钥），当IP地址所有权发生变化时，RPKI的CA对CA证书采取单边操作（新增、删除、修改）使其与新的IP地址所有权分配结果一致。单边操作针对操作中心，导致CA权力失衡，上级CA可做到未经下级许可收回IP地址资源，导致IP地址所有权发生异常变化。

3) 发布风险–单源发布。发布反映操作后的结果（IP-AS），RPKI唯一发布源是分布式资料库，每个资料库中的对象由相应的CA管理，资料库之间通过CA证书中的资料库统一资源标识符（URI）串联。单源发布针对发布中心，导致数据不一致问题[22]，CA可能为RP侧提供陈旧的RPKI对象，或为不同的RP侧提供不同版本的RPKI数据，或阻止RP侧访问一个下级子资料库的RPKI数据，造成局部破坏BGP路由安全的效果。单源发布也会引入单点故障，RIR停机导致资料库无法访问的事件也偶有发生[23]。

RPKI中心化风险存在难以避免、难以识别和难以纠正的技术难点。除了蓄意攻击之外，人为操作失误、软件故障[24]、配置错误都可能引起中心化风险，影响RP侧路由源验证结果。在数据变化时，RP侧难以利用RPKI自身辨别变化是否合法[25]，同时也缺乏直接从IP地址所有者处获取正确数据纠正错误的手段[26-29]。因此，引入新的安全机制或建立新的安全体系，利用去中心化技术消除中心性障碍是RPKI安全研究领域的重要方向。

2　去中心化安全增强技术

基于以上分析，本文将根据3个维度的中心化风险应对来分析RPKI去中心化安全增强技术。

2.1　去认证中心

去认证中心的核心技术思路是改变中心层级化认证体系，采用多边化、扁平化的认证体系避免单点认证威胁。RPKI认证体系中IP地址遵循“谁分配，谁认证”的机制，而去认证中心技术则引入与IP地址资源相关的多方或其他数据提供新的认证机制，可分为基于RIR集体的认证、基于BGP事实所有权的认证和基于共识的认证。

1) 基于RIR集体的认证[30-31]。利用5个RIR（APNIC、ARIN、RIPE、AFRINIC和LACNIC）协作的集体提供IP地址认证代替单一RIR认证，集体内各方共同参与对IP地址分配的认证，相互制约，消除单点认证风险，如图2所示。RIR之间通过门限协议实现协作，一方面，生成统一的门限公钥，使每个RIR可为其他RIR发布的RPKI对象提供验证；另一方面，每个RIR拥有签名私钥的一部分，RIR作为发布的RPKI对象签名，签名过程中RIR可审核提交的RPKI对象并拒绝未经后代同意或内容错误的签名申请，达成相互限制异常操作的目的。基于RIR集体的认证技术方案的优势在于RP侧不需要配置额外信任锚和改变验证过程，缺点在于仅RPKI最顶层实施，去认证中心虽然解决了RIR的根信任问题，但难以限制下层认证中心风险。

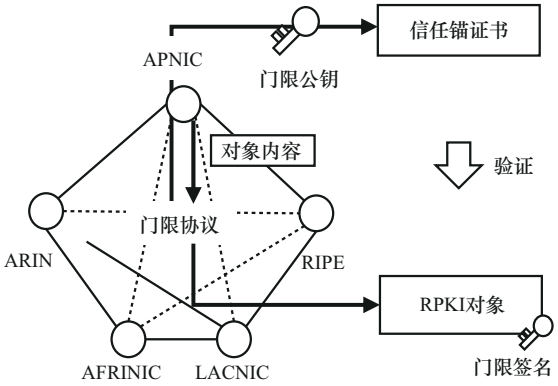

图2　基于RIR集体的认证原理框架

2) 基于BGP事实所有权的认证[32-33]。被互联网长期接受的路由通告反映了IP地址事实上的所有权，DISCO[33]认证方案利用这一思想，采用BGP事实所有权提供IP地址认证，由多个注册中心观测BGP事实所有权判定IP-公钥关系，资料库

收集判定结果并生成认证证书，如图3所示。IP地址的所有者将公钥附加在BGP通告中进行传播，注册中心选择BGP观测点收集上述通告，利用事实所有权判定IP-公钥并将通过判定的IP-公钥签名发送到资料库；事实所有权定义为同一IP-公钥的BGP通告可被一定数量的BGP观测点长时间观测，则判定公钥为IP地址的事实所有者。资料库在收到同一IP-公钥的签名数量占注册中心总数的比例超过一定阈值时，将签名整合生成证书完成IP地址所有权认证。RP侧利用注册中心的公钥验证证书，依据注册中心对外公开采用的BGP观测点信息判断注册中心是否可信。基于BGP事实所有权的认证方法将认证权力分散给了所有的参与者，并且采用了较高的签名数量阈值防止注册中心之间的串通，具有较好的去中心性。但是事实所有权的认证方法无法认证未通告的IP地址，需要额外的扩展来解决。此外，攻击者可持续通告相同的前缀降低原路由通告被观测的比例，从而阻止认证的完成。

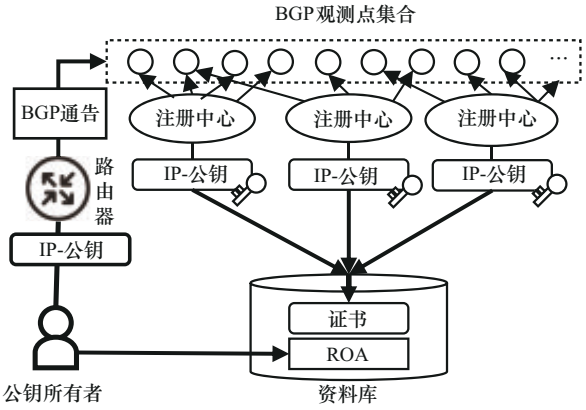

图3　基于BGP事实所有权的认证原理框架

3) 基于共识的认证。以AS集体共识结果提供IP地址认证，由AS提交IP地址所有权事务，共识节点验证事务，如图4所示。该技术方案根据验证依据可分为冲突验证[34-35]和路由起源数据验证[36]，前者以AS声明的BGP通告或者前缀所有权作为事务，共识成员将拒绝与历史中其他AS已声明通告或者所有权信息相冲突的事务；后者以ROA的注册、更新和删除作为事务，共识成员利用RIR路由分配数据库或BGP实时监测数据验证ROA操作的合法性。基于共识的认证的优势在于大多数共识节点正确运行即可保证系统安全，缺点在于维护共识系统需额外协作开销。

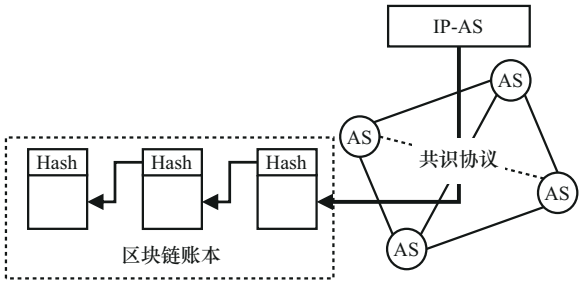

图4　基于共识的认证原理框架

在现有认证中心中，认证者只需要上级单点认证即可，而基于共识的认证需要多节点合作共识，这将带来额外的时间开销。为了降低共识带来的时延，RouteChain[34]使用了一个双层的区块链将自治域划分为子群，每个子群维护较小的内部账簿，减少了新事务验证所需的时间，合理的子群划分也会降低通信时延；去中心化互联网号码资源管理系统（DINRMS）[35]也采用了分组分片的方式降低交互开销；ROAchain[36]则采用了基于信任值和随机性的Cosi集体签名协议，在保证安全性的同时降低了通信和签名验证的时间开销。

2.2　去操作中心

去操作中心的核心思想是利用操作中IP地址关联的后代来限制可能发生异常的操作，在事前制止操作发生或在事后检查发现异常操作，根据制止的手段可分为基于后代同意的限制和基于归还的限制。

1) 基于后代同意的限制。导致后代IP地址减少的操作需经后代同意后才能完成，后代同意可分为上级收集[37-40]和下级上锁[41]，如图5所示。上级收集是指上级撤销、更新IP地址分配的操作需要主动收集所有受影响的后代的同意，否则无法执行操作或者需要额外的处理流程；RP侧在发现资源减少的操作时，可检查后代同意判定操作是否合法，不同意的后代也可利用RP发现上级的异常操作。下级上锁是指后代主动对要保护的RPKI对象上锁，并带外公告上锁对象的正确内容；RP侧监测上锁资料库的上锁对象和对应的带外文件，可在更新时发现导致上锁对象IP地址减少的异常操作。基于后代同意的限制提供了对抗上层级单边操作的手段，上层的恶意操作会难以执行或易于检测，从而降低单边操作带来的影响，但其引入的额外操作和存储对象可能增加额外的时间和空间开销。

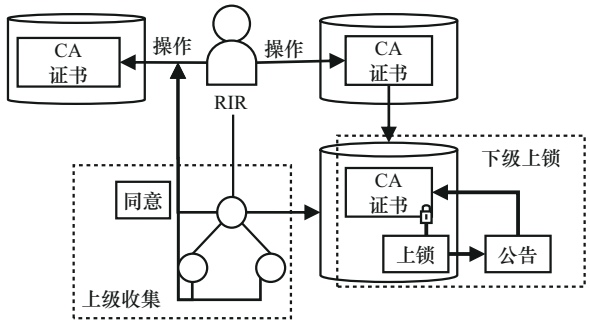

图5　基于后代同意的限制原理框架

2) 基于归还的限制[42-43]。该方案移除了分配者主动撤销的能力，由被分配者归还资源完成撤销操作，选择区块链存储IP分配记录，利用IP地址交易操作实现IP地址块分配，分配操作可表示为有限期IP地址租赁，撤销操作对应被分配者提前或到期归还租用的IP地址块，在租赁未到期前，分配者无法主动收回已分配的IP地址块。基于归还的限制的优点在于可杜绝异常撤销操作的发生，但在下级发生密钥泄露等异常时上级无法协助恢复。

2.3　去发布中心

去发布中心的核心思想是将数据发布源透明化，保证CA侧的历史操作可记录、可追溯，并确保RP侧获取的数据全局一致。哈希链可提供透明、可信的存储，CA侧维护哈希链记录所有IP地址相关操作，为RP侧提供安全数据。根据哈希链数据的验证方式，该技术方案可分为基于RP间比较的验证和基于区块链的验证。

1) 基于RP间比较的验证[37]。CA主动维护自身资料库的哈希链，RP侧利用哈希链与信任的RP比较检查发布威胁。在维持层级化架构的情况下，CA维护新的哈希链资源列表，该资源列表中额外记录了上次更新中资源列表的哈希值以及本次更新中上级资源列表的哈希值；RP侧一方面可利用哈希链资源列表发现遗漏的更新，另一方面可利用哈希链资源列表作为与可信RP侧之间一致性检查的依据，识别自身相较于对方所处的状态（一致、超过、落后或分叉），达到发现和修复数据不一致的目的。

2) 基于区块链的验证。区块链账本采用哈希链存储区块信息，利用共识技术确保RP侧获得全局一致的账本。根据IP地址认证数据的格式，基于区块链的验证方案[34,36,38-40,42-47]可细分为货币式和数据式，技术比较如表2所示。

表2　基于区块链的验证方案的技术比较

技术方案	数据存储形式	账本格式	共识技术	区块链类别
RouteChain[34]	数据式	BGP通告	Clique	许可链
ROAchain[36]	数据式	ROA信息	集体签名	许可链
BGPcoin[38]	数据式	智能合约	PoW	公有链
IPchain[39]	货币式	账户余额	PoS	许可链
IPRV[40]	数据式	前缀管理信息、BGP通告	PoA	许可链
Internet block-chain[42]	货币式	UTXO	PoW	公有链
DRRS-BC[43]	货币式	UTXO	SBFT	许可链
InBlock[44-46]	数据式	智能合约	PoW	公有链
DApp[47]	数据式	智能合约	PoW	许可链

货币式：IP地址以货币的形式直接在区块链账户之间转移。货币式的优点在于逻辑简单直接，IP地址转移后分配者将失去所有权，天然移除了撤销操作。

数据式：IP地址以数据的形式存储，依赖智能合约实现IP地址转移操作的事务。数据式的优点在于资源管理更加灵活，可支持复杂的IP地址转移操作，例如CA主动撤销或续期资源。

区块链技术的引入不可避免地带来了新的问题，如女巫攻击[48]、分叉问题等。ROAchain[36]引入管理认证列表机制来抵抗女巫攻击，管理认证列表提供了包含参与节点公钥和AS信息的白名单，并规定参与节点只能有一个密钥对，限制了节点伪造虚假身份的能力；DApp[47]中参与方需要经过许可才能参与IP资源管理，限制了恶意节点的加入。整体来看，现有基于区块链的RPKI去中心化方案主要针对BGP安全威胁提供解决方法，缺乏引入区块链技术后所带来的安全风险的研究。

3　安全增强技术比较分析

本节将从安全性、可扩展性和增量部署共3个方面比较RPKI安全增强技术。表3中展示了RPKI去中心化安全增强技术比较，包括3个去中心化维度、部署依赖和IP地址认证形式。

3.1　安全性分析

安全性分析主要关注RPKI安全增强技术解决中心化风险的情况，安全性将评估技术是否完全或部分解决中心化风险。

门限信任锚、DISCO、Suspenders、InBlock和DApp都只关注一个中心风险。门限信任锚在5个RIR层级上解决认证风险，在当前RPKI架构中

表3 RPKI安全增强技术比较

技术方案	去认证中心	去操作中心	去发布中心	部署依赖	IP地址认证形式
门限信任锚[30-31]	RIR集体	—	—	5个RIR	层级式
DISCO[32-33]	BGP事实所有权	—	—	注册中心	注册式
RouteChain	共识	—	区块链	5个RIR	注册式
ROAchain	共识	—	区块链	—	注册式
Consent[37]	—	同意	RP间比较	RPKI架构	层级式
Suspenders[41]	—	同意	—	—	层级式
BGPcoin	—	同意	区块链	上级部署	层级式
IPchain	—	同意	区块链	上级部署	层级式
IPRV	—	同意	区块链	5个RIR	注册式
Internet blockchain	—	归还	区块链	上级部署	层级式
DRRS-BC	—	归还	区块链	上级部署	层级式
InBlock	—	—	区块链	以太坊DAO	注册式
DApp	—	—	区块链	以太坊DApp	注册式

RIR直接为LIR和ISP等IP地址直接管理机构认证的情况下，门限签名对对象的审核可对操作风险起到有效的制止作用；但由于每个RIR单独发布自身对象，难以避免由陈旧对象造成的发布风险。DISCO利用BGP事实所有权解决认证风险，同时消除了人为的IP地址分配和撤销等操作；采用多资料库防止单点故障，但RP侧只部署一个资料库也难以避免陈旧对象。Suspenders加锁机制使得RP和资源所有者能够检测违背资源所有者意愿的操作，RP可以拒绝接受这些操作从而减小受到单边操作风险的影响；但Suspenders方案只关注解决操作风险，无法解决认证风险与发布风险。InBlock和DApp以区块链为基础，利用自动化的IP地址分配中心代替了IANA和RIR等机构，实现IP地址到ISP直接认证的同时消除了人为分配操作；但新的分配中心难以与当前IP地址体系兼容，InBlock针对IPv4地址选择由CA注册并由RP侧自行验证的机制，提升了兼容性但也提高了RP侧的验证难度。

此外，其他技术方案选择2个去中心化维度，可基本解决3个中心化风险。去认证中心避免上级单一认证，缓解上级拒绝认证或错误认证风险，保证资源认证可信；去操作中心可记录上级CA的所有操作，增加认证风险的代价；去发布中心可确保认证和操作的数据公开、一致、可溯源，配合注册式的去认证中心可消除人为操作，实现去操作中心效果。

总体上，去中心化技术基本可提供3个中心化风险角度的安全性，但技术引入的新机制也可能带来新风险。基于区块链的技术由于链分叉问题可能产生发布风险，CA可通过双重支付重复分配IP地址，导致RP侧获得不同的IP-AS认证数据。这种风险会对技术部署积极性产生负面影响，只能依赖共识机制等技术的改进来解决。

3.2 可扩展性分析

可扩展性分析主要关注RPKI安全增强技术的新机制产生的新数据开销，以及数据开销能否满足BGP路由日常运维的要求。由于基于区块链的技术改变了RPKI的资料库体系，本节将根据是否采用区块链对技术进行分析。

未采用区块链的技术将分析新机制对比RPKI产生的额外开销能否满足RPKI日常运维要求。基于RIR集体的认证技术方案引入的门限签名算法代替了RIR的签名算法，RPKI历史上每日需要签名的峰值约为8 000个[31]，方案选择的门限协议中最慢和最快的签名量分别为82 080个/天和305 856个/天，可满足RPKI要求。基于BGP事实所有权的认证技术方案直接为IP地址所有者签发证书，在参与的ISP数量一致的情况下，方案对比RPKI在证书和ROA数量上相近，对RP侧验证开销影响不大。基于后代同意的限制技术方案新增了RPKI对象，其中主动收集的方案经测量发现，在历史RPKI数据更新中需要后代同意机制介入的证书操作仅占所有操作的5%，在当前RPKI架构中操作末端证书平均仅需1.6个AS同意，新机制和新对象不会显著提高资料库和RP侧的数据开销；下级上锁的技术方案的每个资料库最多维护一个上锁对象和

带外文件，对数据开销影响不大。

基于区块链的技术需保证区块链的可扩展性满足BGP路由变化的数据开销，如表4所示，数据来自各方案实验部分以及文献[19]，其中，共识时延指达成共识所需要的时间，吞吐量是系统单位时间处理的总负载，一般反映为每秒事务处理量（TPS, transaction per second），开销是交易成本，单位为美元（$）；同时，区块链的共识时延最好不超过BGP收敛时间，保证更新的区块链数据能及时作用到RP侧。以2023年9月1日至9月14日共14天的BGP不稳定性报告[49]以及BGP收敛实验[50]为基准，BGP消息更新平均速率为16.45条/秒，峰值为29 215条/秒；BGP前缀平均更新速率为7.60个/秒，峰值为1 044个/秒；BGP的平均收敛时间为89.6 s。基于区块链的技术方案的吞吐量可基本满足BGP前缀更新的要求，但在高峰时存在拥挤。在共识时延方面，许可链技术方案由于共识技术和节点规模原因，其共识时延通常大于公有链方案，但所有方案的平均共识时延均不超过BGP的平均收敛时间，可保证新更新的IP-AS能够在BGP路由收敛之前在BGP路由器上生效，因此这些区块链技术方案均具有较好的可扩展性。

表4　基于区块链的技术方案的可扩展性比较

技术方案	共识时延/s	吞吐量/TPS	开销/$
Internet blockchain[42]	—	3~7	—
BGPcoin[38]	25	5	0.544（最大值）
IPchain[39]	40	10	—
IPRV[40]	—	90（最大值）	—
DRRS-BC[43]	45.73（最大值）	39	—
RouteChain[34]	54.23	—	—
ROAchain[36]	73	136	—
InBlock[46]	18	13	4.77（最大值）
DApp[47]	2.40（平均值）	—	0.203（平均值）

3.3　增量部署分析

增量部署分析主要关注技术在部分部署的情况下能否提供IP-AS保护，RP侧只需部署技术即可获得IP-AS认证数据实现保护，本节将从CA侧角度分析技术的增量部署效果，即一个CA是否需要其他CA配合部署。

IP地址所有权认证形式影响增量部署。在层级式认证中，上级为下级分配和认证IP地址所有权，CA普遍需要上级先完成部署。一部分技术方案基于RPKI的资料库架构，CA可不依赖其他机构完成部署，其中，门限信任锚只需5个RIR部署即可生效，不需要下级配合；Suspenders只需CA自身额外部署门限签名模块即可生效；而基于同意的机制需上下级协作，且需要所有CA整体部署后才能起效。另一部分技术方案需要搭建新的体系，CA的部署依赖认证链上的上级协作完成，BGPcoin采用层级的分配体系，需要IANA和各个RIR、NIR、LIR和ISP等所有拥有网络资源的组织参与部署；其他方案对认证链的部署顺序要求不高，可支持CA跨层级部署，但当中间的CA加入时，需要一定的开销才能恢复正常的层级架构。注册式技术方案则只需CA申请加入区块链后即可根据角色参与资源管理或发布IP-AS数据，对CA侧增量部署支持更好，大部分方案在搭建好基本架构后，CA可直接加入，其中DApp由于其成员背书机制，需5个RIR作为初始背书机构先加入后其他网络组织才可进行部署。

4　结束语

RPKI中心化风险不能简单地定义为技术上的缺陷，其本质实际上是资源管理需求过于复杂，IP地址资源应由实际使用的机构独立管理，而又依赖于中心化的架构实现认证。当前简单的资源管理操作难以满足资源管理场景的复杂需求，导致资源认证体系在技术和应用上都存在问题。本文针对当前RPKI中心化风险的安全改进技术进行了综述，并讨论了各技术在安全和部署上的可行性，发现这些技术缓解了RPKI中心化风险，且性能可满足日常运维要求，但实际应用存在多种困难。笔者认为RPKI去中心化的未来研究可在以下几个方面进行考虑。

1) 基于区块链的技术方案。①在可扩展性上，部分方案难以满足高峰期吞吐量需求，限制了方案的实用性。一种提高可扩展性的思路是分片技术[51]，同时要避免个别分片内部恶意节点过多的问题。在分片技术中，每个分片片内维护一条内部区块链，各个分片共同维护外部区块链。其难点在于分片内节点总数量相对较少，节点划分不当会导

致部分分片内恶意节点过多，在分片同时保证各分片的安全性是未来改善区块链可扩展性要解决的问题。②研究密钥恢复机制来解决密钥丢失、被盗引起的互联网号码资源丢失问题。一旦发生密钥丢失、被盗，账户被分配的IP资源会丢失，影响互联网号码资源的分配。③解决数据膨胀问题。区块链节点需要存储完整的历史数据集，而随着区块链系统的运行，记录互联网号码资源分配的数据会不断增加，这不仅会给节点带来较大的存储压力，也会影响数据查询、验证的效率，增加共识时延。

2) 基于非区块链的方案需要解决用户间数据的一致性问题。这些方案多依赖于现有的RPKI体系，并采用单源发布、用户定时同步的方式。用户同步时间不同或资料库故意提供不一致的数据等都可能使用户之间同步数据结果不一致，导致用户对相同路由的起源验证结果不同，影响域间路由安全。

参考文献：

[1] LEPINSKI M, KENT S. An infrastructure to support secure Internet routing[J]. RFC, doi.org/10.17487/RFC6480, 2012.

[2] COOPER D, SANTESSON S, FARRELL S, et al. Internet X.509 public key infrastructure certificate and certificate revocation list (CRL) profile[J]. RFC, doi.org/10.17487/RFC5280, 2002.

[3] HUSTON G, MICHAELSON G, LOOMANS R. A profile for X. 509 PKIX resource certificates[J]. RFC, doi.org/10.17487/RFC6487, 2012.

[4] LEPINSKI M, KENT S, KONG D. A profile for route origin authorizations (ROAs)[J]. RFC, doi.org/10.17487/RFC6482, 2012.

[5] CHUNG T, ABEN E, BRUIJNZEELS T, et al. RPKI is coming of age: a longitudinal study of RPKI deployment and invalid route origins[C]// Proceedings of the Internet Measurement Conference. New York: ACM Press, 2019: 406-419.

[6] 邹慧, 马迪, 邵晴, 等. 互联网码号资源公钥基础设施(RPKI)研究综述[J]. 计算机学报, 2022, 45(5): 1100-1132.
ZOU H, MA D, SHAO Q, et al. A survey of the resource public key infrastructure[J]. Chinese Journal of Computers, 2022, 45(5): 1100-1132.

[7] RODDAY N, CUNHA Í, BUSH R, et al. The resource public key infrastructure (RPKI): a survey on measurements and future prospects[J]. IEEE Transactions on Network and Service Management, 2024, 21(2): 2353-2373.

[8] MANDERSON T, SRIRAM K, WHITE R. Requirements for resource public key infrastructure (RPKI) relying parties[J]. RFC, doi. org/10.17487/RFC8897, 2020.

[9] FRIEDEMANN P H, RODDAY N, RODOSEK G D. Assessing the RPKI validator ecosystem[C]//Proceedings of the 2022 Thirteenth International Conference on Ubiquitous and Future Networks (ICUFN). Piscataway: IEEE Press, 2022: 295-300.

[10] WÄHLISCH M, MAENNEL O, SCHMIDT T C. Towards detecting BGP route hijacking using the RPKI[J]. ACM SIGCOMM Computer Communication Review, 2012, 42(4): 103-104.

[11] IAMARTINO D, PELSSER C, BUSH R. Measuring BGP route origin registration and validation[C]//International Conference on Passive and Active Network Measurement. Berlin: Springer, 2015: 28-40.

[12] GILAD Y, COHEN A, HERZBERG A, et al. Are we there yet? on RPKI's deployment and security[C]//Proceedings 2017 Network and Distributed System Security Symposium. Reston: Internet Society, 2017: 1-15.

[13] LI Y B, ZOU H, CHEN Y X, et al. The hanging ROA: a secure and scalable encoding scheme for route origin authorization[C]//Proceedings of the IEEE INFOCOM 2022 - IEEE Conference on Computer Communications. Piscataway: IEEE Press, 2022: 21-30.

[14] KOWALSKI M, MAZURCZYK W. Toward the mutual routing security in wide area networks: a scoping review of current threats and countermeasures[J]. Computer Networks, 2023, 230: 109778.

[15] COOPER D, HEILMAN E, BROGLE K, et al. On the risk of misbehaving RPKI authorities[C]//Proceedings of the Twelfth ACM Workshop on Hot Topics in Networks. New York: ACM Press, 2013: 1-7.

[16] KENT S, MA D. Adverse actions by a certification authority (CA) or repository manager in the resource public key infrastructure (RPKI)[J]. RFC, doi.org/10.17487/RFC8211, 2017.

[17] 苏莹莹, 李丹, 叶洪琳. 资源公钥基础设施RPKI：现状与问题[J]. 电信科学, 2021, 37(3): 75-89.
SU Y Y, LI D, YE H L. Resource public key infrastructure RPKI: status and problems[J]. Telecommunications Science, 2021, 37(3): 75-89.

[18] SU Y, WANG B S, XING Q Q, et al. Research on blockchain-based inter-domain routing authentication technology[C]//Proceedings of the 2021 IEEE 21st International Conference on Communication Technology (ICCT). Piscataway: IEEE Press, 2021: 810-816.

[19] MASTILAK L, HELEBRANDT P, GALINSKI M, et al. Secure inter-domain routing based on blockchain: a comprehensive survey[J]. Sensors, 2022, 22(4): 1437.

[20] 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.

[21] HUSTON G, MICHAELSON G. Validation of route origination using the resource certificate public key infrastructure (PKI) and route origin authorizations (ROAs)[J]. RFC, doi.org/10.17487/RFC6483, 2012.

[22] LIU X, YAN Z, GENG G, et al. RPKI deployment: risks and alternative solutions[C]//Proceedings of the Ninth International Conference on Genetic and Evolutionary Computing. Berlin: Springer, 2016: 299-310.

[23] BUSH R. The resource public key infrastructure (RPKI) ghostbusters record[J]. RFC, doi.org/10.17487/RFC6493, 2012.

[24] MIRDITA D, SHULMAN H, VOGEL N, et al. The CURE to vulnerabilities in RPKI validation[C]//Proceedings 2024 Network and Distributed System Security Symposium. Reston: Internet Society, 2024: 1-18.

[25] HLAVACEK T, SHULMAN H, WAIDNER M. Smart RPKI validation: avoiding errors and preventing hijacks[C]//European Symposium on Research in Computer Security. Berlin: Springer, 2022: 509-530.

[26] HLAVACEK T, JEITNER P, MIRDITA D, et al. Stalloris: RPKI downgrade attack[C]//31st USENIX Security Symposium (USENIX Security 22). Berkeley: USENIX Association, 2022: 4455-4471.

[27] HOVE K V, VOS J V D H D, RIJSWIJK-DEIJ R V. Rpkiller: threat

analysis of the BGP resource public key infrastructure[J]. Digital Threats: Research and Practice, 2023, 4(4): 1-24.

[28] HLAVACEK T, JEITNER P, MIRDITA D, et al. Beyond limits: how to disable validators in secure networks[C]//Proceedings of the ACM SIGCOMM 2023 Conference. New York: ACM Press, 2023: 950-966.

[29] FRIESS J, MIRDITA D, SCHULMANN H, et al. Byzantine-secure relying party for resilient RPKI[J]. arXiv Preprint, arXiv: 2405.00531, 2024.

[30] SHRISHAK K, SHULMAN H. Limiting the power of RPKI authorities[C]//Proceedings of the Applied Networking Research Workshop. New York: ACM Press, 2020: 12-18.

[31] SHRISHAK K, SHULMAN H. Privacy preserving and resilient RPKI[C]//Proceedings of the IEEE INFOCOM 2021 - IEEE Conference on Computer Communications. Piscataway: IEEE Press, 2021: 1-10.

[32] GILAD Y, HLAVACEK T, HERZBERG A, et al. Perfect is the enemy of good: setting realistic goals for BGP security[C]//Proceedings of the 17th ACM Workshop on Hot Topics in Networks. New York: ACM Press, 2018: 57-63.

[33] HLAVACEK T, CUNHA I, GILAD Y, et al. DISCO: sidestepping RPKI's deployment barriers[C]//Proceedings 2020 Network and Distributed System Security Symposium. Reston: Internet Society, 2020: 1-17.

[34] SAAD M, ANWAR A, AHMAD A, et al. RouteChain: towards blockchain-based secure and efficient BGP routing[J]. Computer Networks, 2022, 217: (9): 1-10.

[35] 李江, 徐明伟, 曹家浩, 等. 基于区块链技术的去中心化互联网号码资源管理系统[J]. 清华大学学报(自然科学版), 2023, 63(9): 1366-1379.
LI J, XU M W, CAO J H, et al. Decentralized Internet number resource management system based on blockchain technology[J]. Journal of Tsinghua University (Science and Technology), 2023, 63(9): 1366-1379.

[36] 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.

[37] HEILMAN E, COOPER D, REYZIN L, et al. From the consent of the routed: improving the transparency of the RPKI[C]//Proceedings of the 2014 ACM conference on SIGCOMM. New York: ACM Press, 2014: 51-62.

[38] XING Q Q, WANG B S, WANG X F. BGPcoin: blockchain-based Internet number resource authority and BGP security solution[J]. Symmetry, 2018, 10(9): 408.

[39] PAILLISSE J, MANRIQUE J, BONET G, et al. Decentralized trust in the inter-domain routing infrastructure[J]. IEEE Access, 2019, 7: 166896-166905.

[40] PODILI P, CHERUPALLY S R, BOGA S, et al. Inter-domain prefix and route validation using fast and scalable DAG based distributed ledger for secure BGP routing[J]. Journal of Network and Systems Management, 2022, 30(4): 55.

[41] MANDELBERG D, KENT S. Suspenders: a fail-safe mechanism for the RPKI[R]. 2015.

[42] 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: ACM Press, 2016: 204-210.

[43] LU H M, TANG Y, SUN Y. DRRS-BC: decentralized routing registration system based on blockchain[J]. IEEE/CAA Journal of Automatica Sinica, 2021, 8(12): 1868-1876.

[44] ANGIERI S, GARCÍA-MARTÍNEZ A, LIU B Y, et al. A distributed autonomous organization for Internet address management[J]. IEEE Transactions on Engineering Management, 2020, 67(4): 1459-1475.

[45] ANGIERI S, BAGNULO M, GARCÍA-MARTÍNEZ A, et al. InBlock4: blockchain-based route origin validation[C]//Proceedings of the IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). Piscataway: IEEE Press, 2020: 291-296.

[46] GARCÍA-MARTÍNEZ A, ANGIERI S, LIU B Y, et al. Design and implementation of InBlock—a distributed IP address registration system[J]. IEEE Systems Journal, 2021, 15(3): 3528-3539.

[47] LIU S, YANG F, LI D D, et al. The trusted and decentralized network resource management[C]//Proceedings of the 2020 29th International Conference on Computer Communications and Networks (ICCCN). Piscataway: IEEE Press, 2020: 1-7.

[48] DOUCEUR J R. The sybil attack[C]//International Workshop on Peer-to-Peer Systems. Berlin: Springer, 2002: 251-260.

[49] HUSTON G. The BGP instability report[R]. 2023.

[50] GRIFFIN T G, PREMORE B J. An experimental analysis of BGP convergence time[C]//Proceedings of Ninth International Conference on Network Protocols. Piscataway: IEEE Press, 2001: 53-61.

[51] 潘业达, 陈恭亮, 郭乃网. 区块链吞吐率提升研究[J]. 通信技术, 2019, 52(1): 134-140.
PAN Y D, CHEN G L, GUO N W. Research on block chain throughput improvement[J]. Communications Technology, 2019, 52(1): 134-140.

[作者简介]

秦超逸（1992– ），男，黑龙江哈尔滨人，哈尔滨工业大学博士生，主要研究方向为互联网基础设施安全、资源公钥基础设施增强等。

张宇（1979– ），男，河北乐亭人，博士，哈尔滨工业大学教授，主要研究方向为互联网基础设施安全、互联网体系结构、互联网测量等。

方滨兴（1960– ），男，江西万年人，博士，中国工程院院士，主要研究方向为计算机体系结构、计算机网络、信息安全。