基于区块链的网络安全体系结构与关键技术研究进展

徐恪[1),2),4)] 凌思通[1),2)] 李琦[2),3)] 吴波[5)] 沈蒙[6)] 张智超[1),2)] 姚苏[1),2)] 刘昕[7)] 李琳[7)]

[1)](清华大学计算机科学与技术系 北京 100084)

[2)](北京信息科学与技术国家研究中心 北京 100084)

[3)] (清华大学网络科学与网络空间研究院 北京 100084)

[4)] (鹏城实验室 广东 深圳 518000)

[5)] (华为技术有限公司 2012 实验室 北京 100085)

[6)] (北京理工大学计算机学院 北京 100081)

[7)] (咪咕文化科技有限公司 北京 100088)

摘 要 随着互联网技术的不断演进与用户数量的“爆炸式”增长，网络作为一项基础设施渗透于人们生存、生活的各个方面，其安全问题也逐渐成为人们日益关注的重点。然而，随着网络规模的扩大以及攻击者恶意行为的多样化复杂化，传统网络安全体系架构及其关键技术已经暴露出单点信任、部署困难等诸多问题，而具备去中心化、不可篡改等特性的区块链技术为网络安全所面临的挑战提供了新的解决思路。本文从网络层安全、应用层安全以及 PKI 安全三方面对近几年基于区块链的网络安全体系结构与关键技术研究进行梳理，并将区块链的作用归类为真实存储、真实计算、真实激励三种情形。针对区块链的具体应用领域，本文首先介绍了该领域的安全现状，然后对区块链的具体应用研究进行了介绍，并分析了区块链技术在该领域所存在的优势。本文最后结合现有的解决思路对未来区块链应用中所需要注意的隐私问题、可扩展性问题、安全问题以及区块链结构演进的方向进行了分析，并对未来基于区块链的网络安全体系结构与关键技术研究进行了展望。

关键词 区块链；网络安全体系结构；网络层安全；应用层安全；PKI 安全

中图法分类号 TP393

Research progress of network security architecture and key technologies based on blockchain

XU Ke[1),2),4)] LING Si-Tong[1),2)] LI Qi[2),3)] WU Bo[5)] SHEN Meng[6)]
ZHANG Zhi-Chao[1),2)] Yao Su[1),2)] LIU Xing[7)] LI Lin[7)]

[1)](Department of Computer Science and Technology, Tsinghua University, Beijing 100084)

[2)](Beijing National Research Center for Information Science and Technology, Beijing 100084)

[3)] (Institute for Network Science and Cyberspace, Tsinghua University, Beijing 100084)

[4)] (Peng Cheng Laboratory, Shenzhen 518000)

本课题得到国家重点研发计划课题(2018YFB0803405)、国家杰出青年科学基金(61825204)、国家自然科学基金(61932016, 61802222)、北京高校卓越青年科学家计划项目(BJJWZYJH01201910003011)、国家研究中心项目(BNR2019RC01011)、鹏城实验室大湾区未来网络试验与应用环境项目（LZC0019）、华为技术有限公司委托项目(HF2019015003)资助. **徐恪**(通信作者)，男，1974年生，博士，教授，博士生导师，主要研究领域为互联网体系架构、高性能路由器、P2P网络、物联网和网络经济学.E-mail: xuke@mail.tsinghua.edu.cn. **凌思通**，男，1997年生，硕士研究生，主要研究领域为区块链与网络安全. E-mail: lingst18@mails.tsinghua.edu.cn. **李琦**，男，1979年生，博士，副研究员，主要研究方向为网络安全、隐私保护、大数据安全等. E-mail: qi.li@sz.tsinghua.edu.cn. **吴波**，男，1990年生，博士，主要研究领域为网络体系结构、网络安全、下一代互联网、区块链. **沈蒙**，男，1988年生，博士，副教授，主要研究领域为网络安全和云计算中的隐私保护算法等. **张智超**，男，1995年生，硕士研究生，主要研究领域为联邦学习、网络安全和区块链. **姚苏**，博士，助理研究员，主要研究方向为下一代互联网体系结构和网络安全. **刘昕**，博士，工程师，主导业务包括平台开发、大数据、产品设计和5G等. **李琳**，硕士，工程师，主导业务包括互联网平台开发、产品设计、大数据开发、系统操作和故障排除等.

[5] (2012 Labs, Huawei Technology Co. Ltd. , Beijing 100085)

[6] (School of Computer Science, Beijing Institute of Technology, Beijing 100081)

[7] (Migu Culture Technology Co., Ltd , Beijing 100088)

Abstract With the continuous evolution of Internet technology and the explosively increasing number of users, the network has penetrated all aspects of people's lives, and its security has gradually become the focus of people's attention. Researchers have been doing much research on network security. However, with the expansion of network scale and the diversification of attackers' misbehaviors, some drawbacks have been exposed to traditional network security architecture and its key technologies. For example, most of today's network security infrastructure, such as PKI and RPKI, are all realized as a centralized architecture. And the effectiveness of cybersecurity measures are based on the trust in these centralized architectures, which exposes serious single-point of trust issues. The incidents of Dutch CA certificate provider DigiNotar hacked to issue the malicious certificate for more than 500 websites, and Symantec's misinformation of more than 30,000 certificate extension vouchers indicate that once these trust centers have problems, it will have a severe impact on the entire Internet. Secondly, since the early design of network architecture did not take security into account too much, the deployment of many later proposed security mechanisms not only require modifications to existing network protocols but also affect the efficiency of network operation, which cause difficulties in the actual deployment of these security mechanisms. Besides, with the advent of the era of IoT, the complexity of the network will continue to expand, and network security construction should be participated by many organizations and even the whole people. However, there is a lack of a trustworthy incentive mechanism to coordinate the cooperation between different organizations and mobilize the enthusiasm of users to participate in the network security construction. Nowadays, there is no good solution for these disadvantages, but emerging technology blockchain provides new solutions. Blockchain is a trustworthy distributed database that integrates P2P technology, cryptography, consensus mechanism, and distributed storage technology. Characteristics such as decentralization, immutability, and auditability, have led researchers to devote to the research of blockchain-based application on network security. This paper summarizes these research works from the perspective of network security architecture, and divides them into network-layer security, application-layer security, and PKI security. Specific application areas include collaborative intrusion detection, inter-domain routing security, Vulnerability detection crowdsourcing, access control, and PKI security. And the role of blockchain in these network security applications are classified into true-storage, true-computing, and true-incentive. True-storage is to take blockchain as a storage platform, to ensure the authenticity of stored data, avoid data tampering, and make a true response to the user's data access request. True-computing is based on true-storage, introducing smart contract, and further building a computing platform to ensure the openness, transparency and verifiability of the computing process, as well as the authenticity, credibility and immutability of the computing results. True-incentive is to introduce incentive mechanism based on true-storage and true-computing, to realize transparent reward and punishment measures. For each specific blockchain-based application on network security, this paper first introduces the security status, then introduces the specific research works and show how blockchain is applied to improve the safety, finally analyzes the advantages of blockchain technology applied in this field. In the end, this paper introduce the challenges that should be paid attention to in blockchain-based application on network security, include privacy, scalability, blockchain security, and structure evolution direction. And prospect the future network security architecture and key technologies based on blockchain.

Key words blockchain; network security architecture; network-layer security; application-layer security; PKI security

1　引言

自从 1969 年 ARPANET 正式投入运行，互联网已经发展了 50 余年，从最初的仅有 4 个节点到如今全球接近 44 亿网络用户，从最初仅用于军事研究目的到如今“互联网+”涵盖各个领域，互联网已经作为一项基础设施渗透于人们生存、生活的各个方面。然而，互联网技术在为人们带来诸多便利的同时，其安全隐患也给人们的生活、财产带来了严峻的挑战。从 2018 年 2 月黑客攻击韩国冬奥会致使会场网络中断①到 2018 年 8 月全球最大的半导体制造商台积电遭受 WannaCry 恶意病毒袭击②，再到 2018 年底万豪酒店集团五亿客户隐私数据泄露③，各种网络安全事件都表明，一旦网络遭受攻击，将对人们的生活造成极其严重的影响。因此，如何确保网络安全是网络发展的重点研究对象。

一直以来，研究者们在网络安全领域开展了大量的研究工作，但是随着网络规模的扩大以及恶意攻击行为的多样化复杂化，传统网络安全体系结构已经暴露出诸多弊端。首先，如今的大部分网络安全基础设施都是基于中心化的体系架构，例如公钥基础设施（Public Key Infrastructure，PKI）和资源公钥基础设施（Resource PKI，RPKI）。然而，作为许多现有网络安全技术的信任中心，这些基础设施却暴露出了严重的单点信任问题。荷兰安全证书提供商 DigiNotar 遭受入侵为超过 500 个网站发布恶意证书④，以及证书颁发机构赛门铁克误发超过三万个证书扩展凭证⑤等事件都表明，一旦这些信任中心发生事故，将对整个互联网造成严重的影响。其次，由于网络架构的早期设计并没有详细考虑安全问题，而许多后来提出的安全机制（例如 DNSsec[1]和 BGPsec[2]）不仅需要对现有网络协议进行改动，而且还会严重影响网络的运行效率，从而造成这些机制实际部署上的困境；此外，随着万物互联时代的到来，网络的复杂度将持续扩大，网络安全建设应该由现阶段的不同组织独立参与发展为多组织协同参与甚至全民参与，然而目前还缺乏一套可信的激励机制来协调不同组织之间的合作，并调动大家参与网络安全建设的积极性。针对这些问题，区块链技术的出现提供了新的解决思路。

区块链是一种集成了 P2P 技术、密码学、共识机制以及分布式存储技术的可信分布式数据库，并且具有可审计、去中心化、不可篡改等特点[3]。正是这些特点促使大量研究人员将区块链应用于网络安全领域。然而，现阶段却缺乏对这些研究的系统性梳理工作， 2017 年赵阔等人的工作[4]以及我们的前期工作[5]都是针对物联网安全领域，因此没能对区块链在网络安全领域的应用进行系统性介绍；Chen 等人[6]的工作主要是对区块链在域间路由安全的应用进行介绍；Tara[7]等人的工作虽然对基于区块链的安全服务进行介绍，但并不是主要针对网络安全领域，其中只是涉及 PKI、数据隐私、溯源三个方面；与本文最相似的一篇综述则是来自于 2018 年陈烨等人[8]，该文章介绍了区块链在网络数据安全和隐私保护、物联网设备的权限管理以及 DDoS 防御三方面的应用，但该文章所涉及的区块链应用场景较少，且没能对这些应用研究进行分类梳理，也没能对区块链应用于网络安全所要注意的问题进行分析。本文对近几年基于区块链的网络安全体系结构与关键技术研究进行梳理，以 TCP/IP 网络体系架构为基准，从网络层安全、应用层安全以及 PKI 安全三方面介绍了基于区块链的网络安全体系结构与关键技术研究的最新进展，并系统性地分析了区块链应用于网络安全领域的优势与不足。

本文后续组织如下：第二节对区块链体系结构与原理进行了介绍；第三节对区块链在网络安全的应用进行了概述；之后四、五、六节分别对区块链在网络层安全、应用层安全以及 PKI 安全的应用进行了具体展开介绍；第七节针对区块链应用在网络安全过程中所需要注意的隐私问题、可扩展性问题、安全问题以及区块链结构演进方向进行了分析与展望；最后对全文进行了总结。

2　区块链体系结构

区块链这一概念最早起源于 2008 年中本聪发

① Hackers Targeted the Winter Olympics Opening Ceremony to ‘Embarrass’ South Korea. http://time.com/5155234/hackers-targeted-pyeongchang-opening-ceremony 2018,2,13

② TSMC Chip Maker Blames WannaCry Malware for Production Halt. https://thehackernews.com/2018/08/tsmc-wannacry-ransomware-attack.html 2018,8,7

③ 史上规模最大！万豪旗下酒店发生 5 亿客户信息被泄露. https://tech.sina.com.cn/roll/2018-12-01/doc-ihpevhcm5918790.shtml 2018,12,1

④ DigiNotar. https://en.wikipedia.org/wiki/DigiNotar

⑤ Google takes Symantec to the woodshed for mis-issuing30,000 HTTPS certs. https://arstechnica.com/information-technology/2017/03/google-takes-symantec-to-the-woodshed-for-mis-issuing-30000-https-certs/ 2017,3,24

布的比特币白皮书[9]，之后分别经历了以太坊[10]为代表的智能合约时代和 Hyperledger[11]为代表的联盟链时代的发展，如今区块链已经应用到了数字货币、供应链管理、云游戏等各个领域，其体系结构也呈现出了一种多元化的趋势，但总体上可以概括为数据层、网络层、共识层、智能合约层、应用层以及激励机制六个部分。

（1）数据层是区块链可审计性的来源，其主要定义了区块链的数据结构并借助密码学确保数据的安全性。区块链的数据通常是采用文件系统（例如比特币）或数据库（例如以太坊）进行存储，区块链的具体结构则因为区块链的不同而存在着差异，但交易的组织方式和区块的链接方式都大体相同。每个区块都包含头部区域和数据区域，如图 1 所示，节点在生成区块时，先将交易构建成默克尔树[12]，即将交易作为树的叶子节点，中间节点为其左右子节点数据连接起来后的哈希值，从而得到一个树根节点即默克尔根；默克尔根、前一区块头部哈希以及其它字段一起组成区块头部，默克尔树除去树根以外的部分则作为区块的数据区域。

前一区块头部哈希的存在使得区块之间形成一种链式结构，因此，基于密码学安全性保证，节点只需存储任意区块头部，就可对之前区块头部进行哈希计算并与所存区块头部中的哈希值进行对比，从而验证之前所有区块头部的完整性。

用默克尔树来组织交易则可以实现对单个交易的正确性进行高效验证，如图 1 所示，当用户需要对交易 Tx0 进行验证时，可以请求区块链返回 Hash1、Hash23；然后将 Tx0 进行哈希获得 Hash0，并结合所返回的哈希值计算出一个根哈希；将计算出的根哈希与本地存储区块头部中的根哈希进行比对，即可验证交易的完整性。

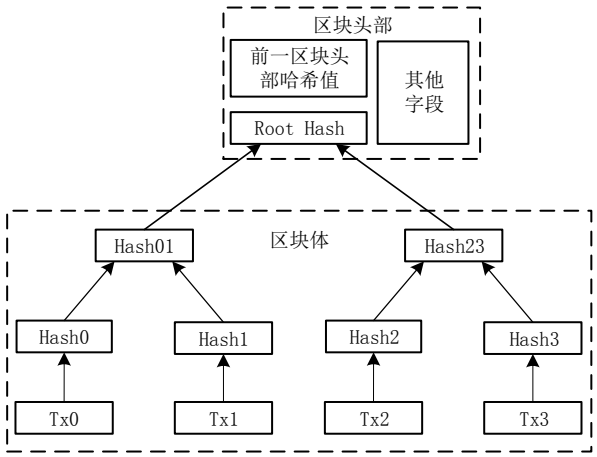

图 1 区块数据结构示意图

（2）网络层是区块链去中心化的来源，其主要定义了区块链节点之间组网流程以及数据在节点间的传播方式。现阶段区块链主要是采用对等网络（Peer to Peer，P2P）构建网络层，每个区块链节点在加入 P2P 网络时，都会试图获取其它节点的地址信息并与多个节点建立邻居关系。当节点产生交易、区块等数据时会将其传播至邻居节点，邻居节点则继续传播直到数据扩散至全网所有区块链节点。每个节点都会根据收到的交易、区块等数据构建本地区块链，节点与节点之间互为冗余备份，从而构成了去中心化的分布式系统，因此可以有效解决单点故障问题。

（3）共识层是区块链一致性、不可篡改的来源，其主要定义了在完全不可信的环境下分布式节点如何对区块链上的数据达成一致。即在每个区块链节点都通过网络层获取到全网所有交易、区块等数据的前提下，即使部分节点可以随意发布恶意信息，也能通过共识算法确保其它诚实节点本地区块链的数据是一致且正确的。现阶段主要共识算法有工作量证明（Proof of Work，PoW）[9]、权益证明（Proof of Stake，PoS）[13]、实用拜占庭容错（Practical Byzantine Fault Tolerance，PBFT）[14]等，在每轮共识过程中，共识算法会选举或竞争出一个领导节点将收集的交易打包成区块并通过 P2P 网络发送给其它节点。每个节点会对区块中的哈希值、签名以及交易的有效性等进行验证，并将通过验证的区块加入到本地区块链。由于在共识过程中所有节点都完成了区块的验证工作，因此区块链解决了矿工节点间的互信问题；此外用户在访问区块链时，可以对多个节点同时访问，并根据少数服从多数原则选择合适的结果，因此在多数节点遵从协议的情况下，区块链具有不可篡改的特性，并可以有效解决中心化系统所存在的单点信任问题。

（4）智能合约层的出现拓展了区块链的应用范围，其建立在共识层之上，主要定义了编写智能合约的语言以及智能合约的执行环境。智能合约以一段程序的形式部署在分布式区块链节点上，当区块链节点对本地区块链达成一致后，若区块中存在交易对智能合约进行调用，或某些状态信息满足要求，区块链节点将自动执行这段程序，并将程序执行结果记录在本地区块链中。基于共识层所实现的全网节点本地区块链的一致性，全网节点共同基于本地一致的区块链数据库执行智能合约并将执行结果记录到本地区块链中，从而全网节点能够对智

能合约的执行结果达成共识。因此基于共识层所提供的一致、不可篡改等特性，智能合约具备自动执行、执行结果不可篡改等特点。

（5）应用层则是通过服务端、前端、app 等现有技术将智能合约的相关接口进行封装，并设计友好的图形用户接口，为用户提供比特币钱包等各种去中心化的应用服务。

（6）激励机制在早期作为激励层体现在区块链架构中，但随着区块链的发展，激励机制可以和区块链各个层次相结合并产生不同的激励效果。与共识层结合时，矿工节点在打包区块时会在其中包含一个将激励发送给自己的交易，因此激励会随着区块的确认自动发放给相应的矿工节点，从而激励矿工节点参与区块链的维护，比特币和以太坊就是采用这种激励机制的典型代表；激励机制与智能合约层相结合则是基于区块链中智能合约对货币的可编程操作性，将激励机制以及获取激励的条件写到智能合约中，并借助智能合约自动执行且执行结果不可篡改的特点确保激励能真实可信的发放到满足条件的用户，从而达到吸引用户的目的；激励机制与应用层相结合则是基于应用直接面向用户的特点，根据区块链记录的用户历史行为对其进行信用评分，并根据信用评分的不同对用户进行区别化服务，从而激励用户保持良好的行为习惯。

上述区块链体系结构的内容可由图 2 进行概括，正是因为区块链各部分所提供的可审计、去中心化、一致性、不可篡改等诸多特点，区块链技术开始被广泛应用于网络安全领域。

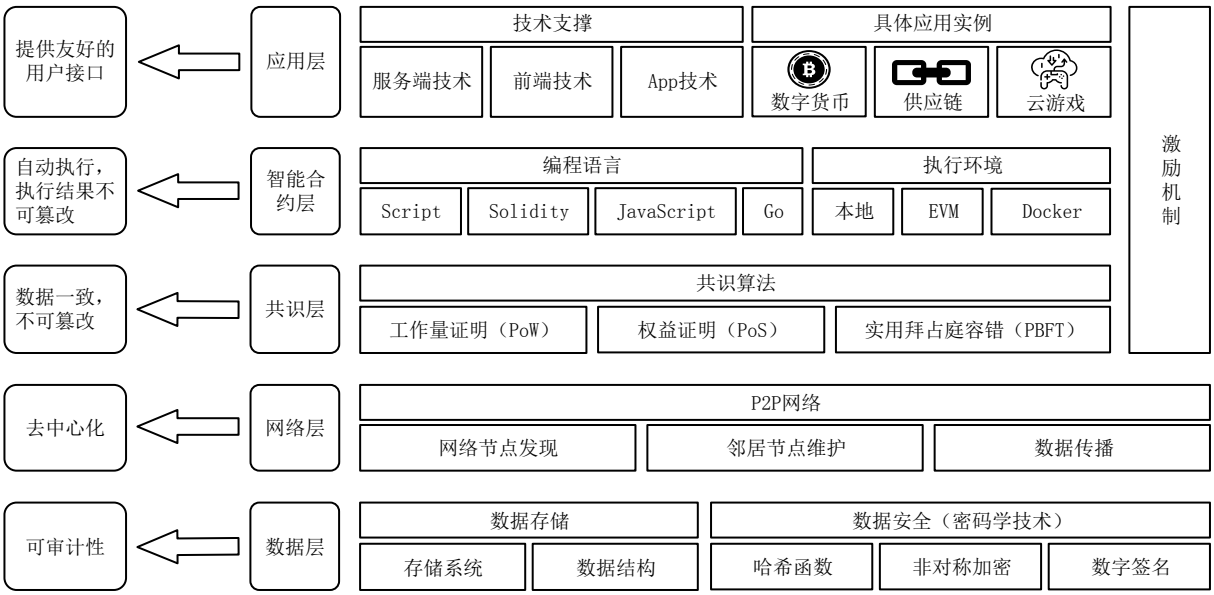

图 2　区块链体系结构图

3　基于区块链的网络安全应用概述

从 TCP/IP 网络体系结构的角度出发，网络安全体系架构应该被划分为链路层安全、网络层安全、传输层安全以及应用层安全。然而，传统网络体系结构在设计之初并没有将安全性纳入设计范围，从而导致如今的大部分网络安全技术都需要基于第三方基础设施才能有效构建，这些第三方基础设施被称为网络安全基础设施。PKI 作为一个重要的网络安全基础设施支撑着整个网络安全体系架构，从不同层次来看，网络层安全中的 IPsec 协议，传输层安全协议（Transport Layer Security，TLS），应用层安全中的邮件安全协议 S/MIME 都是基于 PKI 而建立，因此，PKI 安全支撑着整个网络安全体系架构，是网络安全的技术基础。

区块链在具体应用的过程中根据参与实体的不同可以分类为私有链、公有链以及联盟链。其中私有链的参与方通常都属于一个组织；公有链的参与方则是任何实体；联盟链的参与方则是加入联盟的成员。目前取得广泛应用的区块链类型都属于公有链或联盟链，这两类区块链作为一个分布式可信账本都涉及不同利益体之间的交互，主要用于解决不同利益体之间的信任问题，或者作为一个第三方

可信平台用来解决用户对平台的信任问题。因此，区块链主要在涉及多个平等利益体交互的场景，或者需要引入可信第三方的场景中发挥作用。从网络安全体系结构的角度来看，具备这样特征的场景主要出现在网络层、传输层、应用层、PKI 四个部分。

网络层安全主要涉及数据平面安全和控制平面安全，基于区块链的关键技术则体现在协同式网络入侵检测和域间路由安全两个方面，其中协同式网络入侵检测是为了检测数据平面流量异常并及时对异常流量报警过滤；域间路由安全则是为了确保控制平面域间路由信息的正确性，从而有效指导数据平面的流量转发。传输层安全主要涉及端到端的通信安全，从而确保通信数据的机密性、完整性，现阶段这样一种安全机制是基于 PKI 所建立，因此区块链在传输层安全的应用主要通过在 PKI 安全中的应用来体现。应用层安全主要涉及应用软件自身实现逻辑的安全性以及运行过程中面临潜在恶意用户访问时的安全性，基于区块链的关键技术则主要体现在漏洞检测众包以及访问控制机制两个方面，其中漏洞检测众包的目的是将漏洞检测任务众包出去，从而尽早发现漏洞并及时修补，确保应用本身的安全；访问控制机制则是对资源的访问设置规则，以防止用户资源被非法访问。PKI 即公钥管理设施，负责公钥的分发、撤销等一系列工作，并对公钥持有者的身份进行背书，从而确保网络中通信双方可以互相认证身份。由于现有 PKI 主要是采用中心化架构，因此区块链在 PKI 安全方面的应用主要体现在加强中心化 PKI 安全和构建去中心化的 PKI 两个方面，前者主要目的是在保留原有中心化 PKI 不变的基础上，引入区块链技术使其更安全高效；后者则是用区块链构建一个完全去中心化的 PKI 来取代现有的中心化架构。

在基于区块链构建上述网络安全相关技术的过程中，区块链的主要作用可以总结为真实存储、真实计算、真实激励三个方面：

（1）真实存储是将区块链作为一个真实存储平台，确保用户所存储的数据真实存在，不会被恶意篡改，并且面对用户的数据访问请求也能做出真实的回应。在基于区块链所构建的真实存储平台中，用户以交易的形式请求数据的增加、修改、撤销等操作，其它用户则可以按需对数据库的内容进行读取，并基于这些数据完成后续的计算工作。在对数据存取的整个流程中，区块链数据层提供的可审计性确保用户在访问数据时可以对其完整性进行验证；区块链网络层提供的去中心化特性则可以有效避免单点失效问题；区块链共识层提供的一致性和不可篡改性则确保用户访问所获取数据的真实性。因此相比于传统中心化的存储平台，基于区块链构建的分布式真实存储可以稳定运行，并且有效避免中心服务器宕机、恶意篡改、隐瞒数据，或者对不同用户提供不一致的访问结果等问题。

在基于区块链真实存储所构建的网络安全应用中，存在着数据可验证与不可验证两种情况。数据可验证是指用户所上传数据的有效性存在清晰的判断标准，因此其它用户在获取该数据时可以准确判断其可用性，并基于该数据完成后续的计算工作，例如域间路由安全中的路由宣告信息、访问控制机制中的授权策略信息，PKI 中的证书信息；数据不可验证则是指用户所上传数据的可用性无法显性判断，因此往往需要引入信用评分、用户评价等机制来辅助用户对数据的可用性进行预判，例如协同式入侵检测中各系统上传的报警信息、检测模型信息等。

（2）真实计算是在真实存储的基础之上，引入智能合约，进一步构建一个真实计算平台，确保计算流程的公开、透明、可验证，以及计算结果的真实、可信、不可篡改。在该计算平台中，计算逻辑被编码进智能合约中并部署在区块链上，用户可以通过发布交易来触发智能合约的执行，调用智能合约的交易以及智能合约的执行结果都被真实存储在区块链中。因此相比于传统中心化、分布式计算平台，基于区块链构建的分布式真实计算平台能在承担用户计算开销的同时，有效解决传统中心化计算平台计算流程不透明，计算结果不可验证，无法确保真实性等问题。

在基于区块链真实计算平台所构建的网络安全应用中，根据计算时机的不同可以分为预先计算和实时计算两种情况。

预先计算是指提前将要计算的任务交由区块链执行，并将执行结果保存在区块链中，用户则可以按需直接对计算结果进行访问。预先计算通常在计算任务针对不同用户都一致时使用，因此可以提前计算好对所有用户都适用的结果，例如 PKI 中证书的验证工作，针对同一证书，所有用户对其验证流程都是一致的。在预先计算场景下，由于用户在查询计算结果时只需要进行哈希计算即可验证该结果的完整性，因此当计算任务繁重时，预先计算的方式能显著减小用户获取计算结果的时间开销。

实时计算则是指用户在有计算任务需求时，通过交易调用智能合约，等待交易被打包执行，并获取执行结果。实时计算所涉及的中间数据通常都随着调用者的不同而不同，因此无法像预先计算那样提前计算一个对所有用户都适用的结果。例如访问控制机制中，针对同一资源，不同用户的访问控制策略是不一致的，因此需要在用户请求访问时根据用户的身份实时判定用户的访问权限。在基于实时计算所构建的的网络安全技术中，用户每次调用智能合约都需要等待交易的打包执行，从而造成一定的时间等待开销，为了有效缓解时间等待开销带来的影响，针对时间敏感型的应用，通常可以采用联盟链来增加回应速度，

（3）真实激励是在区块链真实可信的基础上引入激励机制，实现公开透明的奖惩措施，在如今面临网络复杂度持续扩大的情形下，真实激励是调动大家参与网络安全建设积极性的重要手段。现阶段利用区块链真实激励的网络安全应主要可以分为两类，其一是将激励机制与智能合约层结合，该方式主要是利用区块链真实计算的特点实现激励发放、惩罚实施的公开透明性，例如漏洞检测众包中漏洞赏金的的发放，PKI 中恶意证书的举报奖励以及 CA 发布恶意证书的惩罚措施；其二是将激励机制与应用层结合，该方法主要是根据区块链记录的用户历史行为以及被举报、评价历史等计算用户的信用评分，从而对用户进行区别化服务，例如协同式网络入侵检测中根据信用评分选择信息来源。

本文主要内容可以总结为图 3 所示，区块链以真实存储、真实计算和真实激励三种形式支撑着网络安全体系架构及关键技术，但在区块链的具体应用过程中也应该注意区块链隐私性、可扩展性、安全性等问题，本文后续将围绕图 3 具体展开介绍。

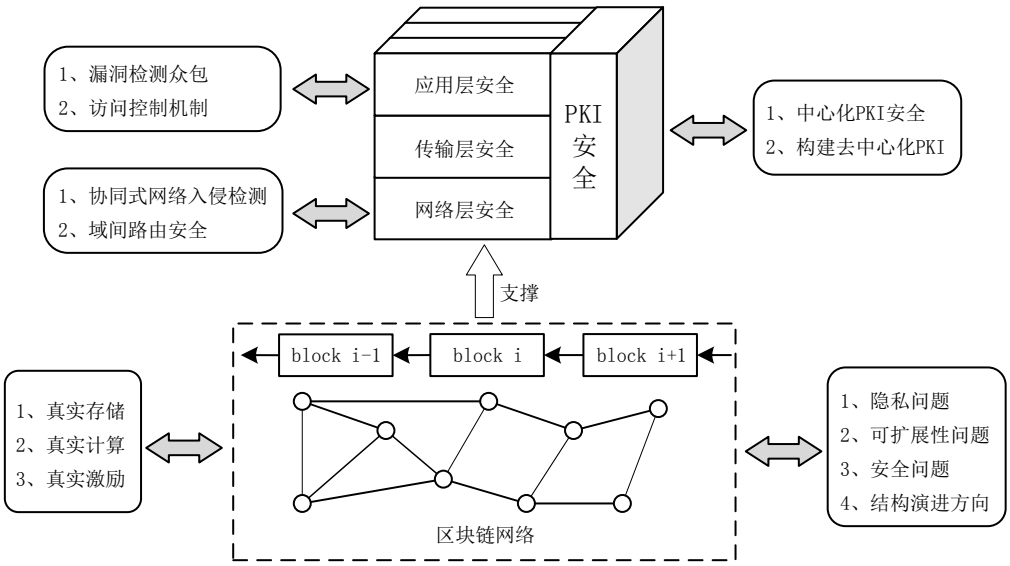

图 3　基于区块链的网络安全体系结构与关键技术研究概括图

4　区块链在网络层安全的应用

在 TCP/IP 协议体系中，网络层主要是确保数据包点到点的传输，并由控制平面和数据平面所组成，其中控制平面负责路由策略的协商，从而指导数据平面的流量转发。因此，网络层安全相应的可以分为控制平面安全和数据平面安全，控制平面安全主要是指路由安全，数据平面安全则是指数据转发平面的流量安全。现阶段区块链在网络层数据平面安全应用主要涉及协同式网络入侵检测领域，在控制平面安全应用则主要涉及域间路由安全领域。本节将从这两个领域详细介绍区块链在网络层安全方面的应用。

4.1　协同式网络入侵检测

网络入侵检测系统（Network Intrusion Detection System，NIDS）通常是部署在网络重要链路旁监听网络流量，当发现异常时及时发出警报并对异常流量进行过滤，从而确保网络数据平面的安全。协同式网络入侵检测系统（Collaborative NIDS，CNIDS）则是指分布在多个区域的网络入侵检测系统互相协作检测大规模的复杂攻击，从而及时做出反应并过滤攻击流量，避免网络遭受更大的损失。

4.1.1 协同式网络入侵检测现状

CNIDS 根据交互信息的流向主要分为集中式、分层式以及分布式三种组织架构，其中集中式架构和分层式架构中都引入了中心服务器，不仅会造成单点故障问题，还会因为涉及不同组织之间的合作而出现对中心服务器的单点信任问题；分布式架构中每个节点都是独立的检测系统，因此完美解决了单点信任和单点故障问题，被认为是 CNIDS 的一种理想实现形式。然而，在现有的分布式系统实现中，单一节点往往无法获得全局信息，使得全局检测准确度低于集中式架构[15]；此外，CNIDS 中每个节点属于不同的组织，恶意节点可能发布虚假的报警信息来协助攻击者，因此存在着节点间的信任问题。针对这个问题，目前主流的方法是建立一套信用评分系统，每个节点根据历史交互行为以及间断性的挑战测试对各节点进行评分，并设定基于评分的协作策略[16-17]。然而这些方法中每个节点都是独立评分，恶意节点可以只针对少部分人进行攻击；尽管在 P2P 网络信任管理方面，大量研究都是通过节点之间评分推荐来获取一个全局评分[18-19]，但却无法有效的应对多个恶意节点的合谋攻击[18]。

4.1.2 区块链的具体应用研究

目前区块链在 CNIDS 的应用研究思路是将区块链作为一个真实存储平台用于信息共享，各参与者将入侵检测的相关信息同步到区块链中共享给其它参与者，从而实现协同式网络入侵检测。根据各检测系统之间共享信息类型的不同，CNIDS 可以分为基于环境信息同步的 CNIDS 和基于模型信息同步的 CNIDS。

基于环境信息同步的 CNIDS 主要思路如图 4 所示，即入侵检测系统之间共享本地检测到的环境信息并对共享的信息达成共识，因此每个单独的入侵检测系统可以掌握全局环境信息，从而进行更全面的网络流量检测。例如 Alexopoulos 等人于 2017 年初步构想了一个基于区块链的协同式网络入侵检测系统框架[20]，该架构由报警信息交换层以及共识层所组成，其中报警信息交换层负责局部报警信息的扩散，共识层则确保区块链中报警信息的一致性。之后 Alexopoulos 等人进行了深入设计并提出了 TRIDEnt[21]，其中引入了激励机制以及信任管理机制，构建了一个报警信息交易市场，参与者可以根据信用评分选择入侵检测系统并向其订阅报警信息，从而激励参与者共享报警信息的同时有效遏制内部节点攻击。在该平台中，参与方以智能合约的形式发布报警信息的出售合约，合约中包含发布者身份、报警信息的价格，出售的报警信息类型；参与者可以进行订阅并与发布者建立连接实现报警信息的接收，并建立一个链下单向支付通道，根据收到的报警信息完成实时付款；信息消费者可以对信息发布者进行评价，历史评价信息被记录在区块链中用于计算信用评分，从而辅助参与者选择报警信息源。与 TRIDEnt 基于评价的信用评分计算机制不同，Meng 等人[22]则是提出基于挑战机制来构建 CNIDS 中的信任管理平台，在该架构中，入侵检测系统在互相共享报警信息的同时随机混入一些挑战信息；每隔一段时间将正常报警信息的反馈序列和挑战信息的反馈序列作为交易参与共识；若该序列中出现异常，即针对挑战信息和针对正常信息给出的反馈存在差异，则认为这个反馈序列对应的入侵检测系统存在异常行为，该异常行为被记录到区块链中并更新对应检测系统的信用评分。

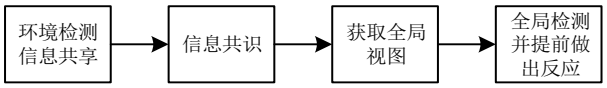

图 4 基于环境信息同步的 CNIDS 流程图

Rodrigues 等人则主要针对分布式拒绝服务（Distributed Denial of Service，DDoS）攻击提出了一个协同式防御系统[23]，在该系统中，当任意区域检测到 DDoS 攻击源后，可将攻击源的地址上传到区块链并同步到各个区域，从而提前预防攻击并在源端过滤潜在的 DDoS 攻击流量；Yang 等人在该方法基础上引入了激励机制，设计了去中心化的互联网资源信任框架 DII[24]，并将其作为 DDoS 流量过滤服务的交易平台，当受害者遭受 DDoS 攻击时可以在线向攻击者所在区域的管理者购买 DDoS 流量过滤服务，请求在源端对攻击流量进行过滤，从而有效防止 DDoS 流量进一步消耗中间网络以及目标网络的带宽资源。

与环境信息同步中各入侵检测系统之间交互实时的环境检测信息不同，模型信息同步的主要思路如图 5 所示，即检测系统之间共享本地检测模型并对共享的模型数据达成共识，检测系统则可以从区块链中筛选模型进行训练从而获得一个具有更强检测能力的综合模型。例如 Golomb 等人[25]提出用区块链来构建一个入侵检测模型共享平台，参与节点用本地信息训练出局部入侵检测模型并将其上传到区块链，然后综合链上的局部模型训练出一个检测能力更强的模型；Li 等人也提出用区块链来

构建一个基于误用检测的协同式网络入侵监测系统[26]，每个检测系统将自己所学习到的入侵特征信息记录到区块链中，从而使整个入侵检测系统的特征库更全；Liang 等人则针对车与万物互联（Vehicle-to-everything，V2X）[27]场景基于区块链设计了一个可以动态更新的协同式入侵检测架构，在该架构中，节点按地理位置不同分为多个区域，每个区域组建一个微型区块链用于收集该区域智能设备上传的入侵样例和入侵检测模型，然后动态训练出最新的综合入侵检测模型，并将该模型部署到进入该区域的智能汽车中。针对如何共享并选择合适的模型来训练综合模型，我们在最近的工作中提出了 SecCL[28]，一个基于区块链技术的联邦学习平台。为了解决用户数据隐私问题并预防攻击者上传恶意模型来对整体模型的训练进行攻击，该平台要求参与者用本地数据集对模型进行训练；每一轮训练结束后参与者上传模型参数的差值；各参与者将区块链中的参数差值分别融合到模型中并用本地数据集进行评估，然后将评估的结果上传到区块链；智能合约根据所有参与者的评估选出最好的模型参数并通知各参与者将其融入到训练模型中，然后继续下一轮训练。SecCL 平台的整个训练流程无需参与者公开本地数据集，且每轮训练的模型是综合所有参与者评价所选出，因此有效解决了用户数据隐私问题和共享恶意模型的问题。Shen 等人[29]则是针对模型训练过程中对用户共享数据的评价问题，提出用 Shapley 值来判定用户上传数据对整体的贡献度，并基于所计算的贡献度对用户发放激励，从而激励用户贡献有效数据。

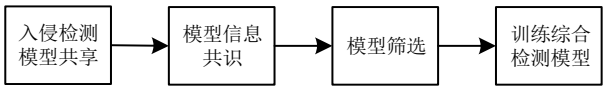

图 5　基于模型信息同步的 CNIDS 流程图

4.1.3　讨论与总结

总而言之，目前基于区块链的 CNIDS 研究主要是将区块链作为一个分布式的真实存储平台实现信息共享。然而，与其它区块链应用中交易存在清晰的对错判断标准不同，报警信息或者是检测模型判断标准相对模糊，节点无法有效判断信息的可用性，因此如何对这些信息设置清晰的选择标准是一个难题。SecCL 平台[28]综合用户的评价实现模型的筛选是一种有效的解决措施，但该方法每次采纳数据前需要等待大家的投票，不适合对实时性要求较高的场景；Shen 等人[29]基于 Shapley 值计算用户贡献度虽然可行，但是当涉及共享数据用户过多时，会造成很大的计算开销；另一种解决方式则是在真实存储的基础上引入真实激励，将激励机制与应用层相结合，根据参与者的历史行为评价为其计算一个全局信用评分，并基于该信用评分设置信息采纳策略，因此各用户可以实时选取所需的数据而不用等待其它用户评价后再做选择。上述三种方式各有优缺点，因此在未来基于区块链的协同式入侵检测系统研究中，如何针对具体场景设计一套共享数据采纳策略需要重点考虑。

4.2　域间路由安全

边界网关协议（Border Gateway Protocol，BGP）作为网络层控制平面中被广泛采纳的域间路由选择协议，其在设计之初并没有考虑安全性，导致各自治域（Autonomous System，AS）宣告的路由会被邻居默认接受。由于 BGP 协议的这个缺陷，恶意 AS 可以宣告虚假的路由源信息或者 AS 路径信息来劫持目标网络的流量，巴基斯坦劫持 YouTube①，以及大量银行地址被劫持②等事件所造成的影响也正体现了目前 BGP 安全问题的严重性，因此如何验证各 AS 所宣告域间路由信息的真实性成为域间路由安全中亟待解决的问题。

4.2.1　域间路由安全现状

现阶段域间路由安全机制主要是建立在资源密钥管理设施（Resource Public Key Infrastructure，RPKI）[30]上，其主要思路是在分配 AS 号与 IP 地址块资源的同时，将每个 AS 号与其对应的 IP 地址块进行绑定，并将这些绑定信息存储在相应的站点供路由器访问[31]，而这些信息则作为 AS 宣告路由源的合理性凭证。正是基于 RPKI 这一架构，预防路由前缀劫持的路由源认证算法[32-33]以及预防路径劫持的真实路径验证算法[2][34]被提出。这些方法虽然在理论上能够有效解决域间路由安全问题，但在实际情况中，RPKI、源路由认证算法以及真实路径验证算法的部署情况并不理想：

（1）RPKI 的部署方面，Wählisch 等人通过测量发现许多大规模的 CDN（Content Delivery Network）都没部署 RPKI[35]，NIST 的最新监测情

① Rensys Blog. Pakistan hijacks YouTube. https://dyn.com/blog/pakistan-hijacks-youtube-1/ 2018,2,24

② Adrien de Beaupre. BGP multiple banking addresses hijacked. https://isc.sans.edu/diary/BGP+multiple+banking+addresses+hijacked/16249 2013,7,29

况[①]也显示只有 16.8%IPv4 地址前缀部署在 RPKI 上；此外 Gilad 等人[36]发现由于人为配置错误原因，RPKI 中存在着大量的错误路由源认证信息（Route Origin Authorization，ROA），造成了 RPKI 体系的信任问题，尽管作者提出了 ROAlert 机制用于发现错误 ROA 并用邮箱或网站对管理者进行警告，但是该机制依靠大家自发参与，缺乏激励机制以及对管理机构的监督惩罚措施。

（2）路由源认证算法部署方面，Gilad 等人[36]测量得出，只有 16%的 AS 部署了基于 RPKI 的路由源认证算法，而针对路由源认证失败的路由信息，只有不到 6%的 AS 选择拒绝接受。

（3）真实路径验证算法部署方面，Lychev 等人[37]提出这些算法的实际部署情况并不理想，并且这些算法只有在全面部署后才能带来极大的安全提升，部分部署情况下不仅无法对域间路由安全做出改善，而且可能会引发严重的逻辑漏洞。

4.2.2 区块链的具体应用研究

将区块链运用于域间路由安全的主要思路是将区块链作为一个真实存储平台，来存储域间路由认证所需要的相关信息，从而确保 AS 可以基于这些信息实现安全的域间路由认证。这些研究根据所实现目标的不同可以分为两大类：（1）基于区块链构建一个去中心化的 RPKI；（2）在去中心化 RPKI 基础上实现源路由认证以及真实路径验证。

基于区块链构建去中心化 RPKI 的主要思想如图 6 所示，即用区块链记录 IP 地址块的分配和交易信息，从而确定每个 IP 地址块的所属身份。例如 Paillisse 等人所提出的 IPchain[38]，他们认为 IP 地址块与数字货币一样，具有流转性（可进行分配与再分配），都能被有限分割，而且在同一时刻都只能被一方拥有，因此用区块链构建一个去中心化的 RPKI 架构，即用区块链来模拟 RPKI 地址分配流程，将 IP 地址的分配历史都记录在区块链上，并提出 PoS 共识比 PoW 共识更适合用来确保 IP 块的安全分配。 Xing 等人[39-40]设计现了基于区块链的资源管理平台 BGPCoin，其中对 RPKI 不同角色之间的地址分配设计了详细的智能合约，参与者调用相应的智能合约进行地址的申请和分配，分配信息则被存储在区块链中提供查询。此外，BGPCoin 引入了用户监管模式，提出 AS 边界路由器可以担任检测者，当发现错误 ROA 时调用 ROA 检测合约，上报错误 ROA 并获得相应的激励。Stefano 等人则将区块链与 IP 地址交易市场结合，提出了 InBlock 架构[41-42]，该架构记录每一笔 IP 地址的交易记录，每笔交易记录都包含具体的 IP 地址块信息以及被授予该地址块的组织账户 ID，而这些交易记录可以像 ROA 一样作为源地址认证的基础，考虑到现有 IPv4 地址已分配完，作者认为 InBlock 可以作为未来 IPv6 地址的交易平台。

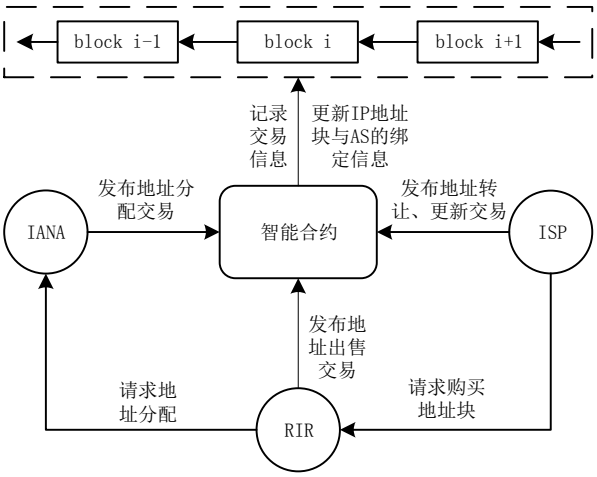

图 6 去中心化的 RPKI 架构图

基于区块链实现源路由认证以及真实路径验证的研究中，根据区块链中记录的信息不同可以分为两种。第一种主要思想如图 7 所示，即通过区块链来记录 AS 的路由源宣告信息以及路径宣告信息，从而判断路由宣告的合法性。

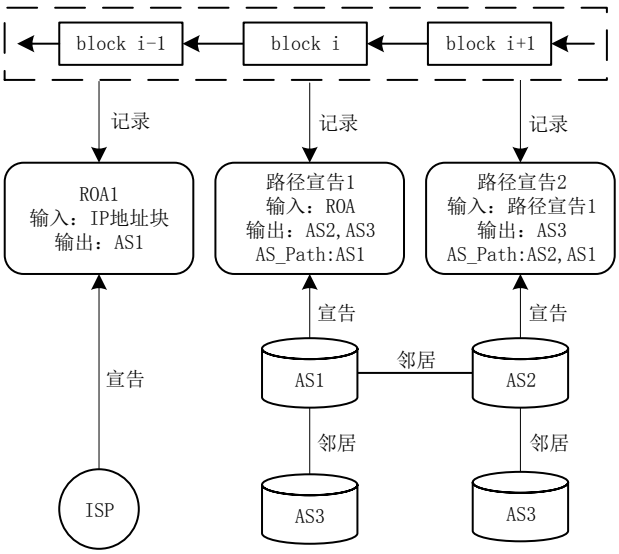

图 7 去中心化的域间路由安全框架

例如 Hari 等人设计的互联网区块链（Internet

① NIST RPKI Monitor. https://rpki-monitor.antd.nist.gov/ 2019,10,6

Blockchain）[43]，其中各 AS 与注册机构参与区块链的维护，并将初始的数字资源分配情况以及 ROA 信息记录到初始区块中；当注册机构发布新的 ROA 信息时，构造 ROA 交易，交易的输入为相应的 IP 地址块（分配新的地址块时）或过期的 ROA 信息（重新分配旧地址块时），输出则为该 IP 地址块绑定的 AS；当 AS 宣告路径时，创建一个路径宣告交易，交易的输入为相应的 ROA 信息（宣告路由源时）或上一个 AS 宣告的路径信息（宣告路径时），输出则为与该 AS 建立了邻居关系的多个 AS；交易经矿工节点验证后被记录到区块链中供边界路由器查询，从而同时实现路由源认证和真实路径验证两种功能。刘冰洋等人设计的 DII[44]以及 Saad 等人设计的 RouteChain[45]也都采取了类似的思想，其中 DII 提出将地址块的转让也以交易的形式记录到区块链中；RouteChain 则提出对 AS 进行划分区域并实现分层管理，使得每个区域能够更快地达成共识，从而降低延迟并增强可扩展性。

第二种思路则是记录各 AS 的路由源信息以及 AS 之间的邻居关系，从而判断路由宣告的合法性。例如 Chen 等人设计在 ISRchain[46]架构中设计了互联网资源管理智能合约（IRMcontract）和 AS 信息智能合约（ASIcontract），IRMcontract 由 IANA，RIR，NIR 等机构创建，负责记录、更新 AS 与 IP 地址块的映射信息；ASIcontract 则由每个 AS 自己创建，负责记录、更新该 AS 与其它 AS 的邻居关系信息以及本地路由策略信息；后续 AS 在接收到路由宣告时，判断该宣告上的 ASPath 字段中的相邻 AS 之间是否满足邻居关系以及各自的路由策略，都满足则接收该路由宣告。

4.2.3　讨论与总结

在基于现有 RPKI 的域间路由安全机制中，由于 RPKI 本身存在单点信任，导致域间路由安全算法所依靠的数据源并不完全可靠，而基于区块链构建一个真实存储平台用于存储域间路由安全验证所需要的信息，由区块链节点共同完成信息的验证工作，是一种有效的解决思路，也因此被基于区块链的域间路由安全研究广泛采用。然而，这些研究工作缺乏对激励机制部署的考虑，传统域间路由安全所面临的低部署率问题依然没能解决。一直以来，研究者们提出通过市场激励、减小末端 AS 部署难度、损失部分安全性来换取高效率等方式来激励各 AS 部署 BGP 安全协议[47-48]，但从现在的部署情况看，这些措施并没有取得很好的效果。而用区块链来实现域间路由安全机制时，区块链的真实激励是提高域间路由安全算法部署率的新思路。在具体应用中，激励机制与区块链不同层次结合所产生的效果也不同，与共识层结合则需要考虑共识所产生的币对 AS 的作用；与智能合约层结合，则 RPKI 由第三方平台负责维护，通过将激励写入智能合约中来吸引 AS 发布 ROA 以及路由宣告信息。InBlock 架构[41-42]用区块链构建地址交易市场是将激励机制与智能合约层相结合的一种实现方式，但该方式只能激励 ROA 信息的快速部署，而针对其它具体场景如何将激励机制融合进来是未来需要考虑的。

4.3　小结

本节从协同式网络入侵检测和域间路由安全两个方面对区块链在网络层安全的应用进行了具体介绍，传统方案及所存在的问题、引入区块链的优势、区块链解决思路总结如表 1 所示。

表 1　区块链在网络层安全应用总结表

网络层安全	传统解决方法	传统方法存在的问题	区块链的优势	区块链解决思路	相关文献
协同式网络入侵检测	多个检测系统共享入侵检测相关信息，并基于评分实现信息采纳策略	缺乏有效的全局信息同步机制	真实存储	环境信息共享同步，获得全局视图	[20-24]
				本地训练模型共享同步，训练综合模型，具有更强检测能力	[25-28]
		缺乏有效的全局评分机制，无法有效应对检测系统共享恶意信息的问题	真实激励	激励机制与应用层结合，根据用户的共享历史计算全局一致的信用评分	[21-22]
				激励机制与智能合约层结合，基于用户共享数据的评价值发放激励	[29]
域间路由安全	RPKI 发布 ROA 信息将 AS 号和 ip 地址块绑定并提供查询，在此基础上实现路由源	RPKI 中存在错误部署的 ROA，暴露出单点信任问题	真实存储	用区块链存储 AS 与 IP 地址块的绑定信息，构建去中心化 RPKI	[38-42]
				基于区块链存储的路由宣告或 AS 关系信息，实现域间路由安全算法	[43-46]

认证算法和真实路径验证算法	ROA 和相关安全算法的部署率非常低	真实激励	用激励机制激励 AS 部署，提高域间路由安全算法的部署率	[41-42]

5 区块链在应用层安全的应用

在 TCP/IP 协议体系中，应用层主要定义了应用程序内部的实现细节，建立在传输层之上直接面向用户，因此应用层安全不仅需要确保应用软件自身实现逻辑的安全性从而避免应用本身被恶意利用；还需要确保应用在运行过程中的安全性，当面临非法访问时及时阻止以确保用户资源不受损害，从而保障用户的利益。现阶段应用层安全中，区块链相关应用主要体现在漏洞检测众包和访问控制机制两个领域，本节将从这两个领域详细介绍区块链在应用层安全方面的应用。

5.1 漏洞检测众包

随着软件的复杂化、多样化，其中的漏洞也越来越多，将漏洞检测任务众包出去已经成为软件提供商检测漏洞的主要手段之一。Google、Microsoft、Facebook 等互联网巨头也纷纷设置了赏金漏洞计划，用于激励大家参与漏洞检测并上交漏洞报告。据目前最大的漏洞赏金平台 HackerOne 统计，其自 2012 年成立到 2018 年累计支出了超过三千万美元赏金①，可见通过设立赏金将漏洞检测众包出去已经成为各软件提供商提升软件安全的重要手段。

5.1.1 漏洞检测众包现状

现阶段漏洞检测任务众包通常是软件提供商出资请求黑客寻找并上报漏洞，从而及时修补以确保其软件安全。具体流程如图 8 所示：软件提供商设置漏洞赏金计划，计划内容包含适用的软件范围以及赏金范围等；黑客通过相关平台查阅各互联网企业发布的赏金计划并选择性参与；黑客在参与赏金计划后下载相应的软件并进行研究测试；发现漏洞之后撰写漏洞报告上交给软件提供商，由其审核测试再根据结果将赏金发放给黑客。漏洞检测众包的顺利进行是基于软件提供商的诚信，然而在实际的运作中却存在部分恶意提供商在收到漏洞测试报告并进行修补后，拒绝发放赏金②；此外，漏洞赏金设置缺乏清晰的标准，如果赏金设置过多，则会造成经济上的损失，如果赏金设置过少，则可能会造成漏洞被扩散并利用的危机；不仅如此，标准在执行过程中也存在单点信任问题，当多个用户先后针对同一漏洞提交报告时，赏金提供商的处理结果难以让所有参与者信服；恶意参与者也可能抄袭伪造漏洞检测报告[49]。

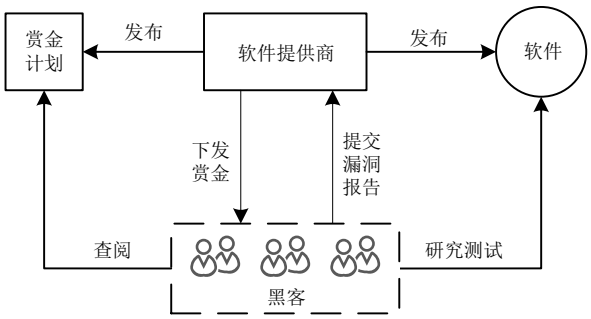

图 8 漏洞检测任务众包示意图

5.1.2 区块链的具体应用研究

基于区块链的漏洞检测众包研究的主要基于区块链构建一个真实激励平台，将激励机制与智能合约层相结合，并以漏洞赏金作为激励，确保赏金发放的公开透明性，从而解决传统漏洞赏金计划中的公平交易问题与单点信任问题。该思路的具体工作流程如图 9 所示，软件提供商以智能合约的形式发布漏洞赏金计划，黑客则下载其发布的软件并测试后向智能合约发布漏洞检测报告，智能合约自动判断报告的正确性并从软件提供商的账户中扣除部分金额发放到黑客的账户中。

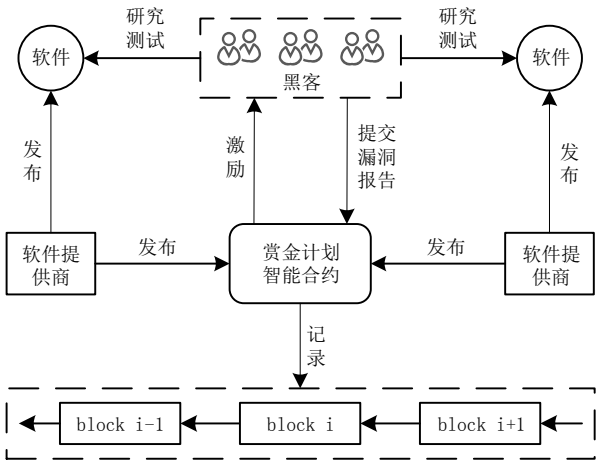

图 9 基于区块链的漏洞赏金平台

Wu 等人[50]正是基于这样一种思路提出了

① The Hacker-Powered Security Report 2018. https://www.hackerone.com/resources/hacker-powered-security-for-startups_2018,

② Researchers Claim Wickr Patched Flaws but Didn't PayRewards. https://www.securityweek.com/researchers-claim-wickr-patched-flaws-didnt-pay-rewards 2016,10,31

SmartCrowd，一个基于区块链的分布式物联网系统漏洞检测平台，试图通过激励机制来吸引众多检测者参与构建一个功能强大的分布式漏洞检测平台。在该平台中，存在着物联网系统提供商、分布式检测者以及用户三种角色，其中物联网系统提供商负责在区块链中发布物联网系统并提交保证金；分布式检测者可以检测系统漏洞并提交漏洞检测报告，报告一旦被接收则自动触发智能合约，从提供商的保证金中扣除一部分作为检测者的激励；用户则可以根据区块链中所记录的检测报告，选择更安全的系统进行使用。该系统借用智能合约自动执行的特点，很好的实现了公平交易的特性，并且利用物联网提供商的保证金来作为对检测者的激励，在吸引更多检测者参与的同时，还能约束物联网提供商并促使其发布更安全的系统，从而营造更安全的物联网环境。针对物联网系统安装后的安全检测，Wu等人还提出了SmartRetro[51]，用于激励有能力的检测者对用户已安装的IoT系统进行回顾性检测，以聚集众人的力量实现更全面的检测，确保物联网环境的安全。在这两篇文章中，作者设计了分阶段提交漏洞检测报告的方法，即第一阶段只上传报告的哈希值，之后再公布具体的报告内容，从而有效地解决了黑客之间公平竞争的问题，然而针对自动确定上交报告正确性的方法以及赏金设置的具体标准，文中并没有提及。

Breidenbach 等人[52]试图用区块链解决漏洞检测众包中存在的公平交易问题以及漏洞赏金的设置难题，提出了Hydra框架，并将其用于智能合约漏洞检测。在该框架中，作者提出了 N 版本编程（N-version Programming，NVP）的变种NNVP，用不同的语言或要求不同的程序员独立编写一种功能的多种实现版本组合成一个并行执行的综合程序。与传统N版本编程追求的容错性不同，NNVP须在所有版本输出结果相同时才正常运行，任一版本运行结果不一致都意味着该版本存在着漏洞，整个程序停止运行并产生一个赏金，等待黑客上报漏洞并领取。黑客也可以选择继续研究找到使N种版本产生共同错误输出的漏洞并进行利用，但却会冒着赏金被其它黑客领走的风险。此外，对于如何设置赏金，作者提出了“漏洞利用缺口”这一概念，其值为使 N 个版本程序中某个版本出错的概率除以使 N 个版本程序共同出错的概率，“漏洞利用缺口”值越大说明程序被利用的可能性越低。作者通过泊松过程模拟漏洞发现过程，并得出了一个和“漏洞利用缺口”有关的赏金设置标准，按照该标准设置可以激励黑客发现漏洞后选择及时上报。然而，该框架只适用于可N版本编程且不以容错为主的应用，因为Hydra是依靠N个版本输出的不同来判断漏洞的出现，并且在任意版本程序输出不同时选择直接停止运行，以确保综合程序的安全运行，因此并不适用于对可用性要求较高的应用中。

5.1.3　讨论与总结

总而言之，区块链真实激励中激励机制与智能合约层相结合的方式有效地解决了传统漏洞众包中的公平交易问题以及公平竞争问题，但是引入区块链也带来了另一大难题，即如何自动判断上交报告的合法性。针对该问题，Hydra 框架虽然给出了一种解决方案，但该方案却只能运用于作者所提出的NNVP场景，而在一般场景下如何设计自动检测报告正确性的智能合约是未来研究需要考虑的。此外，在激励机制的设计方面，SmartCrowd和Hydra都只考虑了金钱这一个角度，然而 Votipka 等人[53]通过对黑客的采访发现黑客主要是通过研究漏洞实战、黑客竞赛、社区交流以及查阅以往的漏洞报告来提升能力。因此，从黑客的角度来看，学习、爱好以及寻求挑战都是必不可少的，如何将这些因素纳入激励机制，在未来研究中也需要重点考虑。

5.2　访问控制机制

访问控制是对计算、存储、服务等资源的访问设置访问条件，从而有效避免恶意应用对资源的不正当访问以及合法应用对资源的越权访问，是确保各应用安全访问资源的一种有效手段。随着万物互联时代的到来，边缘计算与物联网的结合促进了智慧家庭、智慧城市等各种应用场景的发展，催生了大量的新型应用服务，这些新型服务在进一步提升人们生活品质的同时，也给访问控制技术带来了严峻的挑战。这些新型服务相比于传统网络服务更贴近人们的生活，其安全问题也将对人们造成更大的影响。因此，在新网络时代下，如何设计一套安全、高效且能有效保护用户隐私的访问控制技术变得至关重要。

5.2.1　访问控制机制现状

访问控制模型如基于身份的访问控制[54]、基于角色的访问控制[55]、基于属性的访问控制[56]以及基于能力的访问控制[57]等是现阶段主流的访问控制模型，并且已经取得广泛应用。然而，这些访问控制模型在实际运行过程中都是基于中心化的架构，导致应用在获取权限并访问用户数据的过程中缺

乏透明性，因此对于自己的数据何时被何应用收集使用，用户无从得知；此外，在基于云存储的数据共享模式中，用户数据的存储与访问控制都由云端完成，从而也形成了单点信任问题。而随着边缘计算与物联网的到来以及用户隐私观念的提升，传统访问控制模型也呈现出了诸多弊端。

例如 Ouaddah 等人[58]对物联网领域的访问控制研究进行了调研，认为传统访问控制模型中，控制能力都集中在数据中心，而物联网需要一个适用于其分布式性质的访问控制系统，通过该系统，用户可以掌控自己的隐私数据；Fernandes 等人[59]对三星物联网平台 SmartThings 中的的智能 app 安全性进行了研究分析，发现由于粗粒度的授权策略，超过一半的 app 都存在权限高于实际需要的情况；Xiao 等人[60]对物联网时代下边缘计算的安全现状和挑战进行了调研分析，认为边缘计算场景下访问控制涉及的控制场景比传统网络更复杂，并认为未来的细粒度访问控制模型中，应该考虑五个要素，即访问者、访问时间、访问地点、被访问对象以及访问须满足的条件。Mao 等人[61]则是从边缘节点交互的角度对移动边缘计算进行了调研，总结得出边缘服务器之间可以交互协作来实现负载均衡，但是缺乏相应的激励机制使家庭用户用自己部署的边缘服务器与其它服务器协作；并且面对诸多的边缘服务器，也缺乏相应的认证机制、信任管理机制以及用户隐私保护机制来使用户放心的使用边缘服务器所提供的计算存储等服务。

综上，面对新网络时代的到来，现阶段访问控制技术面临的主要问题如下：

（1）如何设计一套访问控制机制在保护用户隐私的过程中确保用户能够自己掌控数据的管理权，并了解自己数据被访问的情况。

（2）在物联网场景下，如何设计一套能够避免单点信任问题，且能够考虑各种细粒度条件的动态访问控制机制。

（3）如何设计一套对边缘服务器资源的访问控制，并能有效协调各服务器之间的协作。

5.2.2 区块链的具体应用研究

根据访问控制保护的对象类型，现阶段基于区块链的访问控制研究主要分为三类：（1）对共享数据的访问控制；（2）对物联网设备的访问控制；（3）对公共服务的访问控制。

在对共享数据的访问控制方面，现有区块链相关研究主要思路是基于区块链真实计算的特点搭建一个访问控制平台，总体思路如图 10 所示，数据提供者以交易的形式共享数据，并添加权限信息，当数据消费者请求访问数据时，智能合约进行权限判定后返回相应数据。由于数据消费者的每次访问请求都会记录在区块链中，数据提供者共享的数据也经过对称密钥加密处理，因此该方法可以确保用户掌握自己数据并确保隐私的同时，知道何人何时访问了自己的哪些数据。

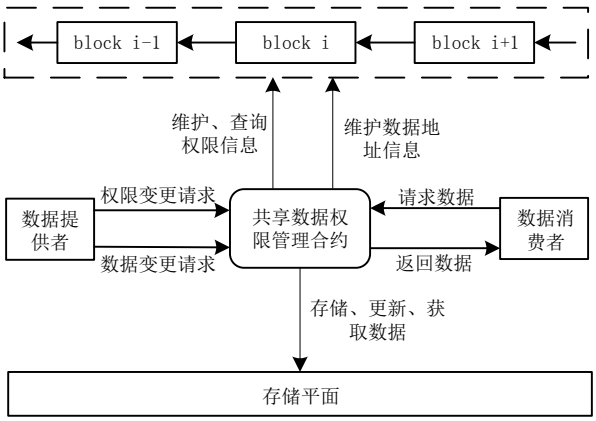

图 11 基于区块链的共享数据访问控制平台

Zyskind 等人[62]正是基于这样一种思想提出了一种用区块链保护私人数据的系统，在该系统中，用户若想将数据授权于数据使用者进行使用，则随机生成一对公私钥并与其协商对称密钥，双方的公钥则组成混合身份，其中数据提供者拥有该混合身份的所有权限，数据使用者则只有该身份的部分权限；用户可以用与混合身份中自己公钥所对应的私钥签名授权交易和数据存储交易发布到区块链中；区块链节点验证后将权限信息以及加密数据以分布式哈希表（Distributed Hash Table，DHT）的方式存储在链下，数据的哈希值则被存在链上作为数据的指针；数据使用者则可以用混合身份中与自己公钥对应的私钥签名数据访问交易请求数据访问；矿工节点验证权限后将加密数据返回给数据使用者，数据使用者则用协商的对称密钥解密数据并使用。由于该方法能确保只有被授权者才能解密数据，且每次数据访问的交易被记录到链上，因此可以确保用户掌握自己隐私数据的同时，了解自己的数据何时被谁所访问。Shafagh 等人[63]提出了一个类似的数据共享架构，但与前者不同的是，该架构中数据消费者直接向存储平面请求数据，然后由存储平面向区块链请求权限验证，通过后再将数据发给数据消费者；此外，为了避免用户在数据共享的过程中与不同的数据消费者分别协商对称密钥，作者使用

再加密技术实现对称密钥的分发与更新，从而减少密钥协商所造成的开销。Dagher 等人[64]则是针对电子健康数据领域提出了基于区块链的数据共享架构 Ancile，该技术在对健康数据实施访问控制中引入再加密技术的同时还引入了盲解密技术，确保区块链节点无法合谋获取数据。

在物联网访问控制方面，现有研究主要是针对物联网设备本身计算性能有限的特点，基于区块链真实计算构建一个去中心化的第三方访问控制平台，并基于智能合约实现更细粒度的动态访问控制。其总体思路如图 12 所示，即由设备管理者通过调用智能合约添加、更新物联网设备的访问权限信息，用户访问物联网设备时，设备请求智能合约验证用户权限。

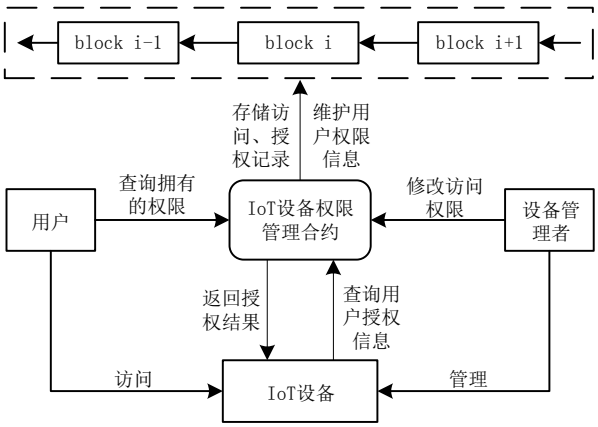

图 12　基于区块链的物联网设备访问控制平台

例如 Ouaddah 等人[65]提出了 FairAccess，一个物联网设备资源访问控制平台，在该平台中，访问权限是以令牌（Token）的形式存在，用户可以选择使用或将其转让给其他用户。资源持有者以交易的形式发布一个 Token 授予某用户对资源的访问权限，交易的输出为被授予权限用户的地址以及一段锁定的脚本程序，该脚本记录了使用该权限需要满足的预先条件，当用户携带 Token 访问物联网设备时，设备请求区块链进行认证并根据返回结果决定是否允许此次访问。Pinno 等人[66]则设计了控制链，其中包括四条区块链，分别是关系链、环境链、责任链以及规则链，其中关系链记录了用户之间朋友、兄弟等关系；环境链则记录了传感器等物联网设备上传的温度、时间、网络流量等环境信息；责任链则记录了用户对资源的请求访问记录以及访问结果；规则链则定义了基于环境信息、关系信息、责任信息以及传统的访问控制模型的细粒度的访问控制规则；Novo 等人[67]提出了区块链与边缘计算相结合的物联网访问控制框架，其中轻量级物联网设备通过边缘管理中心与区块链网络进行交互，每个用户可以注册成为管理者，并在访问控制区块链中注册自己管理的设备以及为设备添加访问控制策略。Zhang 等人[68]则设计了基于智能合约的物联网设备资源访问控制，其中访问控制过程主要涉及访问控制合约与判定合约，访问控制合约定义了被访问资源的静态访问条件，判定合约则根据访问用户的历史行为等信息实施动态判定，当静态判定和动态判定同时通过后才允许用户的该次访问。Ali 等人[69]则考虑了基于事件的动态授权场景，应用服务可以订阅报警信息，当报警触发后，应用自动生成授权交易发往区块链中以添加相应的授权信息。

在公共资源的访问控制方面，现阶段相关研究主要思路如图 13 所示，即将边缘服务器等设备看作是一种公共资源，并借助于区块链中流通的数字货币来实现访问控制。由于公共资源是大家都能够访问的资源，为了实现资源的有效利用，避免大量恶意用户对公共资源的无限访问造成拒绝服务攻击，基于区块链真实激励的特性，用数字货币来换取公共资源的访问是一种有效的方法。由于货币本身也可以用来激励用户贡献资源，因此可以激励拥有相关资源的用户充当资源贡献者，确保公共资源池的可持续性使用。

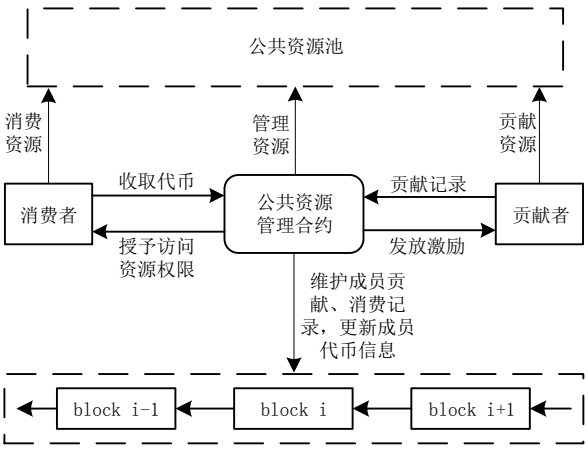

图 14　基于区块链的公共资源访问控制平台

例如 Liu 等人[70]设计了一个基于区块链的电动汽车云与边缘计算架构，在该架构中，同一区域停止或行驶缓慢的电动汽车可以相互合作构成一个云平台；分散在各地快速运行的电动汽车则构成一个边缘计算平台。基于该架构，作者提出了信息交互和能源交互两个应用场景，在信息交互场景中，

电动汽车云平台可以作为快速行驶汽车与路边单元（Road Side Unit，RSU）交互的中间节点，确保移动网络的健壮性；电动汽车边缘计算平台则与相应传感器合作实现道路检测等功能。在能源交互场景中，电动汽车云平台可以充当一个发电厂，为有供电需求的实体充电，电动汽车边缘计算平台可以充当移动电源，平衡不同区域的用电需求，本地聚合器（Local Aggregate，LAG）则作为充放电的中间媒介。在信息交互与能源交互场景中，RSU 和 LAG 分别维护基于数据贡献度的数据区块链和基于能源贡献度的能源区块链，并根据贡献度生成一定数量的数据币和能源币分配给相应的电动汽车，这些币则可以被用来获取能源与路况信息等公共资源。Pan 等人则提出了 Edgechain[71]，用区块链构建的边缘计算服务器资源管理平台，并借助区块链中的货币来限制物联网设备对边缘服务器资源的访问次数。在该架构中，边缘服务器每隔一段时间会发放一定数额的币到物联网设备对应的账户中，当物联网设备需要计算、存储等资源时，通过动态定价策略实施相应的货币收费服务。此外，服务器会对物联网设备的资源请求行为进行检测，当发现异常后会扣除物联网设备的信用分，每轮返还货币时会根据信用分的变化实施货币奖惩，当信用分为零后，物联网设备的任何资源请求都将被拒绝。

5.2.3 讨论与总结

总而言之，基于区块链真实计算来构建访问控制平台是实现访问控制过程公开透明，并确保访问控制结果真实可信的有效手段；而针对边缘计算服务器等公共资源的访问控制中，真实激励能有效避免恶意用户对资源的无线访问。然而，区块链在实际应用于访问控制时也带来了巨大的时间开销，例如 Zhang 等人[68]所设计的基于智能合约的访问控制模型中，部署访问控制合约的燃料消耗为百万级别，且每次访问控制智能合约的调用时间接近 30s。解决开销问题的一个方法是将的访问控制流程进行拆分，区块链只充当一个真实存储平台负责权限信息的存储、更新、删除等操作，而实际的权限验证工作可以放在区块链下用户自己的设备上进行（例如物联网网关，个人服务器等）。但在部分场景中，用户可能并没有可用的设备用于执行访问控制流程，因此如何针对不同应用场景具体设计以减小实际开销，在未来研究中需要重点考虑。

5.3 小结

本节从漏洞检测众包以及访问控制机制两个方面对区块链在应用层安全的应用领域进行了介绍，传统方案及所存在的问题、引入区块链的优势、区块链解决思路总结如表 2 所示。

表 2 区块链在应用层安全应用总结表

应用层安全	传统解决方法	传统方法存在的问题	区块链的优势	区块链解决方案	相关文献
漏洞检测众包	软件提供商发布赏金计划，黑客上报发现的漏洞后，软件提供商发放相应的奖励金	赏金发起方可能不守信用，接收漏洞报告后拒绝发放赏金	真实激励	以智能合约的形式发布漏洞赏金计划，软件提供商提交保证金，漏洞报告被接收后自动扣除作为赏金	[50-52]
		缺乏赏金设置标准，标准执行存在单点信任	真实计算	将赏金标准写入智能合约，实现赏金的公开透明发放，通用标准暂无	[52]
访问控制机制	由中心服务器实现基于角色、基于能力、基于属性等的访问控制	无法确保用户掌握自己隐私数据的管理权以及数据被访问情况	真实计算	用户自定义访问控制策略并上链，区块链根据该策略实施对共享数据的访问控制，每次数据访问请求被记录到区块链上供审计	[62-64]
		物联网场景下存在单点信任、控制粒度粗等问题	真实计算	区块链作为一个真实计算平台执行访问控制流程，基于智能合约图灵完备性编写细粒度访问控制条件	[65-69]
		边缘计算场景下边缘服务器之间的协作问题	真实激励	基于区块链中的货币实现对边缘服务器资源的访问控制，根据贡献度实现激励的发放	[70-71]

6　区块链在 PKI 安全的应用

PKI（Public Key Infrastructure）即公钥管理设施，负责公钥的创建、管理、分发、储存、撤销等一系列流程，并对公钥持有者的身份进行背书，从而确保用户之间能够对各自的身份进行认证。PKI 作为重要的网络安全基础设施支撑着整个网络安全体系结构，如网络层安全中的 IPsec 协议、传输层安全协议 TLS、应用层安全中的邮件安全协议 S/MIME 都是基于 PKI 所建立。PKI 根据信任体系的不同可分为中心化和去中心化两种形式，区块链的相关研究也相应的分为加强中心化 PKI 安全和构建完全去中心化的 PKI 两方面，本节将从这两个领域详细介绍区块链在 PKI 安全方面的应用。

6.1　中心化PKI

现阶段中心化 PKI 主要是指基于证书颁发机构（Certificate Authority，CA）这一套信任体系所建立的 PKI，也是现在最常用的一种 PKI 体系结构。其中 CA 作为信任中心用自己的私钥为用户或其它 CA 签名颁发数字证书，实现用户公钥与身份的绑定。CA 之间组成一个分级架构并形成信任链，根 CA 因为被用户所信任，其证书会被浏览器存储在本地。用户在收到交互端发来的证书后，只需沿着证书信任链上的签名进行逐级验证，基于对本地存储根 CA 证书的信任，当用户成功验证所有签名后将信任证书上所示的身份信息。

6.1.1　中心化 PKI 现状

中心化 PKI 所带来的一个严重问题就是单点信任问题，一旦 CA 的私钥被泄露，攻击者就能利用其发布恶意证书，而这些证书可以被用来发起中间人攻击，从而损害用户的安全。针对这个问题目前的解决方案是采用证书撤销机制和证书透明机制（Certificate Transparency，CT）相结合，其中 CT 主要是用来监督未经授权的证书发布。CA 在签发证书的同时向 CT 服务器进行注册；CT 服务器则存储所有注册证书供第三方审计；当用户发现未经授权的证书被发布，可以立刻申请撤销该证书；每个 CA 则会维护一个证书撤销列表（Certificate Revocation List，CRL）用于记录被撤销的证书；用户可以下载该列表用于查询证书撤销信息，也可以通过 CA 所指定的在线证书状态（Online Certificate Status Protocol，OCSP）服务器来查询证书撤销状态信息。

尽管证书撤销机制与 CT 机制的引入在一定程度上缓解了中心化 PKI 的单点信任问题，但是整个 PKI 环境依然存在着以下问题：

（1）针对证书审查机制，目前大部分的用户都只向少数几个 CT 服务器申请证书注册，导致证书注册信息过于集中，使得目前的 CT 环境相当脆弱[72-73]，且存在着单点信任问题；

（2）针对证书撤销机制，证书撤销列表 CRL 的规模已经越来越大[74]，对用户造成了很大的下载开销；通过 OCSP 服务器查询虽然避免了下载 CRL 列表的开销，但是却要向第三方查询，因此不仅会引入一轮响应等待延迟，还会泄露用户站点访问信息。因此，目前所有的移动端浏览器以及大部分 PC 端浏览器不对证书撤销状态进行验证，证书撤销查询机制的部署情况堪忧。

（3）针对 CA 本身，由于部分 CA 规模非常庞大，以至于一旦对其证书撤销将会造成大范围的网站无法连接[75]，因此很难对这些 CA 的过失行为进行惩罚，致使部分 CA 对自身安全建设并不重视[76]。

6.1.2　区块链的具体应用研究

现阶段基于区块链的中心化 PKI 安全研究主要是在保证原有 PKI 中心化思想不变的基础上，基于区块链构建一个第三方平台确保 PKI 整体环境的安全。而具体应用思路有两种，其一是基于区块链真实激励构建一个第三方激励平台对 CA 签发证书的行为进行监督，激励 CA 加强自身安全的同时降低恶意证书的发布的可能性；其二是基于区块链真实存储构建一个去中心化的证书审计平台，记录所有注册证书供第三方审计，同时又基于区块链真实计算构建一个证书状态信息管理平台，该平台记录 CA 证书的发布、撤销记录，并维护最新的证书状态信息，为用户提供安全、高效的证书验证服务。

Matsumoto 等人[76]所设计的 IKP 平台是第一种思路的典型代表，作者们认为 CA 应该提升自身安全来减少误操作、密钥泄露的可能性，但是并没有激励机制来促使 CA 这样做，因为即使 CA 错发个别证书，对自身并不会造成很大影响；此外，第三方检举恶意证书的过程费时费力且无法获得任何酬劳，从而降低了恶意证书检举者的积极性。基于这些原因，作者用区块链构建一个去中心化的自动激励平台 IKP，监督 CA 重视自身的安全建设的同时吸引各方参与恶意证书的检举。该平台的主要思路如图 15 所示，域名持有者可以发布域名证书政策，该政策说明了颁发给该域名的证书需要满足的

条件；CA 则可以出售回应政策给某域名，回应政策中定义了违反域名政策时所需要赔偿的金额，包括域名持有者的赔偿金以及恶意证书检举者的奖励金；当检举者发现恶意证书并上报后，IKP 平台将该证书与证书持有者的域名政策进行比对，发现违反政策后触发签发该证书 CA 所出售的回应政策，从 CA 的资金池中扣除规定数额的资金用于补偿域名持有者并奖励检举者。

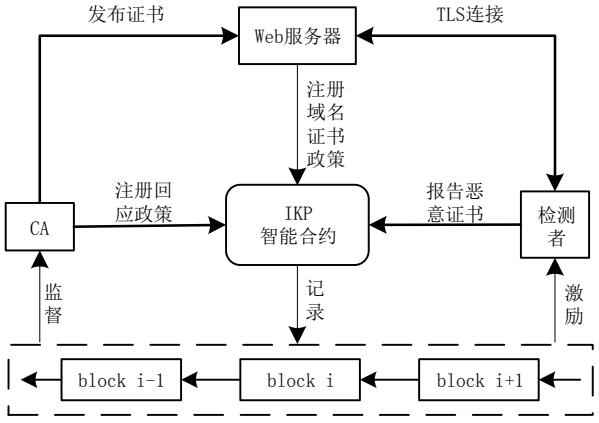

图 15 IKP 架构图[76]

Chen 等人[77]则是采用第二种思路，他们从 CT 同步过程容易受到单点失效攻击以及现有撤销证书状态查询机制开销过大两个方面入手，用区块链构建了一个证书审计平台证书链（Certchain），该平台的主要构建思路如图 16 所示，CA 负责维护整个平台，并将所有的证书操作记录到证书链中，用户在收到证书后可以向该平台查询证书状态。为了实现区块链的高校检索，作者设计了证书操作符数据结构用于记录证书相关操作，其中设置有指针用于记录与该证书相关的上一次操作所在的区块链高度，因此无需检索全部区块链即可高效查询某证书的操作历史；为了实现证书状态的高效查询，作者设计了双计数布隆过滤器，其记录了所有证书的状态信息，并在每个新区块产生时进行更新并包含在该区块中，因此可以实现证书状态的实时快速查询；此外，为了解决区块链的算力集中问题，作者们还设计了基于可靠性排名的共识机制和激励机制，CA 的可靠性根据其过去的行为进行判定（发布的证书量以及恶意行为次数等），可靠性越高的 CA，其产生区块的概率越高，从而激励 CA 保持良好的行为。然而，证书链要求在平台运行之初将所有参与 CA 的信息填入初始区块中，并没有考虑如何进行增量式部署，并且该方法将证书撤销状态查询交由证书链维护节点，不仅增加了身份认证过程的延迟，还会泄露用户的隐私。

为了解决证书链增量式部署问题，以及在证书验证方面的隐私泄露和效率不足等问题，同样采用第二种思路的 Kubilay 等人则是引入了证书预先验证的思想，提出了证书帐本（Certledger）[78]。Certledger 基于门限数字签名方案[79]实现顶级根证书的添加，该方法将一对密钥的私钥分成多份交给不同实体，当超过一定数量的实体提供签名后即可签发顶级证书，顶级证书被默认加入 Certledger 中形成信任根；拥有顶级证书的 CA 可以和传统 PKI 中的 CA 一样继续签发下一级 CA 证书或域名证书；中间 CA 或域名持有者可以选择以交易的形式请求将证书记录到 Certledger 中，矿工节点会完成证书的验证工作，并将通过验证的交易记录到区块链中，相应的证书则记录在本地维护的证书列表中，状态被设置为“有效”；证书持有者可以选择以交易的形式撤销添加的证书，矿工节点验证相关签名信息后将交易记录到区块链中，并将证书状态设置为“撤销”；矿工节点会以默克尔树的形式维护所有证书的状态信息，并将默克尔根记录到区块头部，并随着新区块的产生实时更新；域名持有者则实时从最新区块中获取证明自己证书状态的默克尔证明信息，并在与客户端建立 TLS 连接时随证书一起提供；客户端则实时同步最新的区块链头部信息，因此可以在本地根据域名持有者发来的默克尔证明信息验证证书的状态。Certledger 这种证书预先验证的思想提前将证书的全部验证工作交给区块链，客户端在收到证书后无需进行签名验证，只要在本地进行简单的哈希验证即可完成对证书的验证，因此在实现用户隐私保护的同时，显著提高了证书验证的效率。

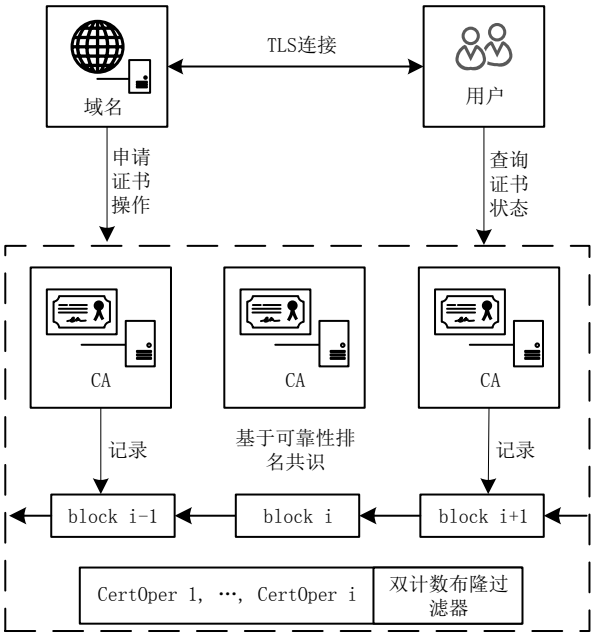

图 16　Certchain 架构图[77]

6.1.3　讨论与总结

总而言之，基于 CA 的中心化 PKI 已经取得广泛应用，是整个互联网得以安全运行的基础，因此很难对 CA 本身做出很大的改变，而基于区块链真实激励构建一个第三方监督激励平台或是基于区块链真实计算建立一个第三方证书验证平台都是行之有效的方案。在对 CA 本身的监督激励方面，由于 CA 的重要性，仅仅建立一个监督平台无法对其产生有效的的惩罚，因此类似 IKP 平台先为 CA 引入额外的利益，再激励网络用户进行 CA 恶意行为监督是一种很好的解决思路，但是在采用该思路的过程中需要有像域名持有者这样合理的利益来源。在辅助证书状态的验证方面，Certchain 仅仅维护最新的证书状态信息并向用户提供证书状态查询服务，虽然该方式能有效解决 CT 和 CRL 所存在的单点信任问题，但是却没能充分利用区块链真实计算的特点，证书的签名验证工作还是在客户端进行；Certledger 则充分利用了区块链真实计算的特点，采用预先计算的思路，将原本客户端的证书验证工作卸载到区块链，并利用比特币中简易支付证明的思想实现客户端本地快速的证书验证。然而，Certledger 因为需要记录所有的证书操作记录并维护证书状态信息，因此会造成巨大的存储开销，而如何实现有效存储是未来的一个研究方向。

6.2　去中心化PKI

与基于 CA 信任体系的中心化 PKI 不同，去中心化的 PKI 是基于信任网络（Web of trust）[80]所构建。在该体系中，每个用户生成一对非对称密钥并自签名一个证书。为了建立信任关系，用户可以选择自己所信任的用户并为其证书签名以表示对该用户的信任，每个证书可以包含多个用户签名，因此用户之间形成一个网状的信任结构，用户可以根据其证书上的签名来决定是否信任该证书。

6.2.1　去中心化 PKI 现状

去中心化的 PKI 因为消除了对 CA 的依赖，每个用户都可以自签名证书并收集他人的签名来提升自己证书的可信性，从而避免了证书申请及后续维护所需要向 CA 缴纳的费用，因此这种形式的 PKI 可以面向普通用户之间的交互提供服务，并主要被用在电子邮件安全中[81-82]。现阶段去中心化 PKI 的一种主要实现形式是由 Phill 于 1991 年所开发的完美隐私（Pretty Good Privacy，PGP）[83]，如图 17 所示，每个用户都自签名一个证书，证书中包含了用户的公钥、身份信息（如姓名、邮箱等）、用户私钥的签名以及一个证明列表，该证明列表包含了其他用户的签名，代表该证书的有效性已被列表中用户所证明，因此用户可以根据证书的签名列表对证书的可信度进行度量。

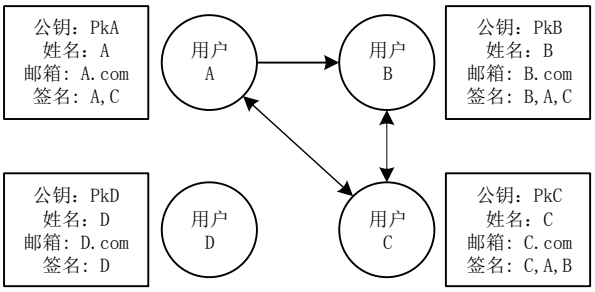

图 17　PGP 信任模型示意图

信任网络所依靠的是人与人之间的社交关系，每个用户都可以创建自己的非对称密钥对并加入信任网络，然后逐渐收集其他用户的信任。这种方法虽然解决了中心化 PKI 中的单点信任问题，且在一定程度上降低了用户使用门槛，从而支持面向普通用户之间交互的应用服务建立[84]，但是却也存在着以下问题：

（1）由于用户证书有效性是依靠用户间互相签名来判断，在缺乏激励机制的情况下，新用户难以有效获取足够多老用户的签名信任，因此基于信任网络的去中心化 PKI 对新用户不友好，容易造成图 15 中用户 D 所面临的局面；

（2）当用户的的密钥丢失或撤销后，证书状态信息很难迅速传播出去，而只能通过中心节点将

状态信息扩散，并且即使收到该信息后也无法证明消息的准确性，因此往往需要依靠中心机构来帮助传播撤销信息。

6.2.2 区块链的具体应用研究

基于区块链的去中心化 PKI 构建思路如图 18 所示，是利用区块链真实存储的特点，记录用户证书的注册、撤销信息以及用户之间的信任建立、解除信息，并存储用户的证书信息，以及该证书的签名列表供用户查询，用户互相交互时可以访问区块链获取用户证书以及该证书的签名列表，并选择是否相信该身份，然后完成互相认证。

在理论研究方面，Fromknecht 等人基于 Namecoin 设计了 Certcoin[85]，其中每个用户拥有一个身份（identity，id），用户可以自行生成线上线下两对密钥并通过交易将两个公钥与身份一起绑定并上传到 Certcoin 链上，后续密钥的更新、撤销都通过私钥签名并以交易的形式记录到链上。当两对密钥其中一对泄露后，为防止攻击者抢先更新密钥，用户可以用两对密钥同时签名密钥撤销信息，此时该交易的权威性比用单个密钥签名的交易更高。此外，作者还提出可以用布隆过滤器、默克尔树等将所有密钥信息压缩存储并记录到区块链中，从而提高身份验证效率，并且采用 DHT 进行公钥信息的传递与存储，提供基于 id 的高效密钥查询。Axom 等人[86]认为 Certcoin 中在密钥更新的过程中，旧密钥与新密钥的联系性被记录到链中，从而损害用户的隐私，于是在 Certcoin 的基础上引入好友认证的方式，消除了新密钥与旧密钥以及 id 的关联性使得无法对用户进行行为追踪。Jiang 等人[87]则认为用户在向区块链请求证书信息时会暴露行为隐私，则引入了私人信息检索技术来确保用户访问区块链的隐私。AI-Bassam 等人考虑了用户之间的签名背书，将信任网络和以太坊结合搭建了一个去中心化的 PKI[88]。在该架构中，用户可以用私钥签名发布自身的各种属性（姓名、邮箱等）信息，用户之间可以互相为特定的属性进行签名以证实该属性的正确性。在交互时，交互端可以根据对方属性的签名列表来选择是否信任该属性。Yakubov 等人也基于类似的思想，将 PGP 与区块链结合并设计了 BlockPGP[89]，作者们提出尽管 PGP 是基于信任网络所建立，但为了确保效率，现在主要的信任中心是由密钥服务器承担（Key Server），而密钥服务器本身可能遭受中间人攻击，且密钥服务器之间存在信息同步问题，因此提出由密钥服务器来组建区块链，并负责维护用户的证书信息和签名信息，确保 PGP 环境的安全性。Shen 等人[90]则是针对基于身份密钥（Identity Based Cryptograph，IBC）场景，提出多个 IBC 域的密钥服务器之间组建联盟链记录各个域认证所需要的参数信息，从而实现物联网场景下的安全跨域认证。

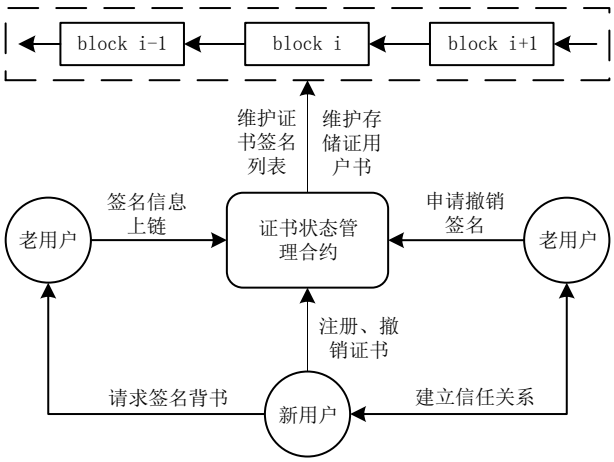

图 18 基于区块链的去中心化 PKI 架构图

在实际部署方面，Ali 等人设计了 Blockstack，第一个投入运行的去中心化 PKI[91]，并于 2017 年 5 月发布了最新的白皮书[92]，Blockstack 目的是为了实现一个去中心化的互联网环境，支持在其上建立去中心化的应用，其架构主要分为区块链层、对等网络层以及存储层。区块链层主要记录用户的操作并对这些操作记录达成共识，该层包括作为底层支撑的区块链以及用于向上层隐藏区块链细节的虚拟链，用户的各种操作记录作为无意义数据存储在区块链中，而虚拟链则将无意义数据提取出来呈现给上层用户；对等网络层则负责存储数据资源的路由信息；数据层则由云存储提供商或用户自建的存储器组成，用于存储用户加密后的数据。由于 Blockstack 是一个去中心化的互联网环境，每个注册的用户都会生成一对公私钥并进行绑定，从而实现用户与用户之间的安全交互，而对公私钥的操作信息（撤销、更新等）都会被记录到区块链中，因此 BlockStack 平台相当于构建了一个面向用户的去中心化 PKI。

6.2.3 讨论与总结

总而言之，基于信任网络的 PKI 依靠用户之间互相签名为各自的身份背书，从而消除了对 CA 的依赖并可以为普通用户之间的交互提供服务。但相比于中心化 PKI，去中心化的 PKI 很难安全有效地传播证书状态信息以及信任签名信息。因为在中心

化 PKI 中，用户只需要存储少数信任 CA 的证书并从 CA 维护的站点获取证书撤销信息就可以对所有证书的可信性进行验证；而去中心化的 PKI 中证书的签发和撤销源是用户本身，因此在不引入中心节点的情况下很难有效传播所有用户的证书状态信息。而将区块链作为一个分布式真实存储平台，是记录并传播用户证书以及信任签名的有效方式；此外，在用区块链构建去中心化 PKI 的过程中，可以考虑引入激励机制，让新用户出资激励老用户进行签名，为解决传统去中心化 PKI 下老用户缺乏签名动力的问题提供了新的思路。然而，现有相关研究并未将区块链真实激励这一特点纳入去中心化 PKI 的设计中。综上，区块链是构建去中心化 PKI 的一种可行方法，而在未来的研究中如何针对用户之间的签名设计合理的激励机制还需要重点研究。

6.3　小结

本节从加强中心化 PKI 安全和构建去中心化 PKI 两个方面对区块链在 PKI 安全的应用进行了介绍，传统方案及所存在的问题、引入区块链的优势、以及区块链解决思路总结如表 3 所示。

表 3　区块链在 PKI 安全应用总结表

传输层安全	传统解决方法	传统方法存在的问题	区块链的优势	区块链解决方案	相关文献
中心化 PKI 安全	CA 作为信任中心为用户颁发数字证书，CT 实现注册证书的透明度，CRL 实现证书撤销状态查询	部分 CA 规模庞大，即使错发证书也很难对其进行有效惩罚	真实激励	激励机制与智能合约层结合，为 CA 引入激励并对错发证书行为进行惩罚	[76]
		证书集中注册在少数 CT 中，存在单点信任问题	真实存储	用区块链记录所有证书信息，构建去中心化的证书审计平台	[77-78]
		撤销状态查询机制开销大造成实际部署率低	真实计算	将证书状态的验证工作交由区块链执行，并保存验证结果供客户端查询	[78]
去中心化 PKI 安全	基于信任网络，用户自签名证书，用户之间互相签名来证实证书的正确性	无法有效传播证书状态信息和签名撤销信息	真实存储	利用区块链记录证书操作，并存储证书信息以及签名列表供用户查询	[85-92]
		老用户缺乏签名动力从而对新用户不友好	真实激励	针对用户签名设计合理的激励机制	暂无

7　研究展望与挑战

尽管区块链为解决网络安全中存在的问题带来了新思路，但在区块链实际应用于网络安全的过程中，还需要考虑区块链的隐私性、可扩展性、安全性以及结构演进方向。

7.1 隐私问题

区块链作为一个分布式帐本由众多矿工节点共同维护，每个节点上都存在一个完整的备份，因此账本上的所有记录对矿工节点都是可见的，从而不可避免的带来隐私问题。而在未来基于区块链构建网络安全应用的过程中，隐私问题将严重影响参与者的积极性，因此在利用区块链的同时需要着重考虑如何保护参与者的隐私。

7.1.1　链下存储

链下存储是目前区块链应用研究中普遍采用的一种方式，也是保护用户数据隐私的主要方法。其主要思想是将重要数据存储在链下，而链上只存储数据的哈希值，该哈希值可以被用来对链下存储的数据进行索引，以及对链下数据的完整性进行验证。链下存储虽然能够保证用户重要数据的隐私，但由于用户所发布的交易公开存储在链中，这些交易可以被用来推测用户的行为隐私；此外，链下存储的数据被访问后可能被进行二次传播从而危害用户数据隐私。

7.1.2　零知识证明

零知识证明是指证明者可以在不提供任何有用信息的情况下证明某论断正确性，因此该技术被研究者用来解决区块链带来的行为隐私泄漏问题。最早将零知识证明运用到区块链的是 Ian 等人于 2013 年所提出的零币 zerocoin[93]，由于当时比特币中，用户所产生的每一笔交易输入都是该用户掌握的某个交易输出，从而造成用户所有交易之间存在关联性，攻击者可以根据这些信息关联用户的多个匿名账号并推断出该用户的行为隐私。zerocoin 则是通过零知识证明让用户无需泄露自己之前交易的信息即可创建交易，从而掩盖了用户交易之间的

关联性并有效地保护了用户行为隐私，Kosba 等人于 2016 年基于零知识证明提出了 Hawk 系统[94]，用于帮助用户创建能够保护隐私的智能合约。

虽然零知识证明有效地解决了区块链所引入的行为隐私泄露问题，但计算开销过大限制了它在区块链领域的应用，然而随着未来计算能力的提高以及用户对隐私重视程度的增长，零知识证明也将在隐私要求高的应用场景中发挥重要作用。

7.1.3 安全多方计算

安全多方计算允许多个数据持有方在不泄露各自数据的前提下协作完成一个函数的计算并得到最终结果，从而能在确保数据隐私的情况下综合利用多方的数据资源，有效避免用户数据的二次传播问题。近几年大量研究人员将区块链技术与安全多方计算相结合并开展研究工作[95-99]，但安全多方计算流程的复杂性限制了它的应用，而未来如何针对更复杂的应用场景设计安全多方计算步骤并提高计算效率是研究者需要着重探索的。

7.2 可扩展性问题

区块链的扩展性问题是一直以来被广泛讨论的问题，也是限制区块链应用的重要问题之一。由于区块链中的每一笔交易都需要由所有的矿工节点达成共识并记录到区块链中，严重限制了区块链的交易执行速率；此外随着时间的增长，区块链中记录的数据量越来越多，对矿工节点的存储也提出了严峻的挑战。因此在未来基于区块链的网络安全体系结构与关键技术研究中，可扩展性问题也是必须要重点注意的一个问题。

7.2.1 限制节点个数

区块链作为一个分布式系统，其去中心化的特性是以共识所消耗的时间为代价的，节点个数越多，去中心化的特性就越强，而各节点通过共识达成一致所需要的时间就越久。因此，限制节点个数牺牲部分去中心化特性来换取区块链的可扩展性是目前研究中采用的主要方法之一。例如 DPoS 共识机制[100]中允许矿工节点将自己的权益委托给其它节点，由它们代为行使投票权；Algorand[101]中则是每轮随机选举出部分节点参与拜占庭共识，从而实现了 125 倍比特币吞吐量。因此在未来区块链用于网络安全的研究中，需要根据实际的应用需求，在区块链去中心化带来的安全性和区块链的可扩展性之间进行衡量。

7.2.2 分片

分片技术在传统数据库中已广泛使用，近些年则作为区块链扩容的主要思路被广泛研究[102-105]。其主要思想是将区块链中的所有节点分为不同的片区，每个片区只处理片区内部的交易，跨片区的交易则由各片区合作完成。然而，在实际分片的过程中，由于对区块链网络进行了分割，可能导致部分分片中恶意节点数量过多，使得这些分片容易遭受攻击，因此在分片的过程中如何确保安全性是区块链分片研究的主要目标。

7.2.3 共识与执行分离

在传统区块链的维护过程中，区块的打包、共识以及交易的执行等一系列工作都是在单一节点上完成，如果能针对具体的应用将任务进行分割交给不同的节点执行，则可以实现多节点并行处理来增加区块链的吞吐量。朱立等人[105]就采取了一种业务逻辑和共识分离方法，设计了高性能联盟链，并将其应用于证券撮合系统，实现了每秒 20 万笔交易的吞吐量；Hyperledger 中也采取了分工并行机制，将节点分为排序节点和链码执行节点，从而将交易的排序打包工作与交易的实际执行工作分离。总而言之，共识与执行分离不仅可以通过多节点的流水线式并行处理增加区块链的吞吐量，在节点资源配置上也可以更具有针对性。因此，共识与执行分离可以作为未来区块链在网络安全应用中提升区块链吞吐量的思考方向。

7.3 区块链自身安全问题

尽管区块链技术的到来给网络安全领域提供了新的解决思路，但在基于区块链的网络安全体系结构与关键技术研究中，也需要注意区块链本身的安全问题。针对区块链自身的安全问题，现有部分工作已经进行了总结[107-108]，而本文接下来将根据第二节所介绍的区块链架构，从数据层、网络层、共识层、智能合约层、应用层分别对区块链安全问题进行简要介绍。

7.3.1 区块链数据层安全

数据层面的安全性主要是由非对称加密、哈希函数等密码学技术来保证，然而随着量子计算的到来，区块链数据层安全将面临巨大的挑战。2019 年 10 月 23 日，谷歌在 Nature 上发表论文[109]，描述所发明的量子处理器在 200s 内完成了最先进的超级计算机一万年才能完成的计算目标。尽管 IBM 对谷歌的结论提出了相应的质疑①，且现有研究已经开始将抗量子融入区块链协议的设计[110]，但面临着未

① On “Quantum Supremacy”. https://www.ibm.com/blogs/research/2019/10/on-quantum-supremacy/. 2019.10.21

来量子计算的发展，如何进一步将抗量子密码融入区块链是确保区块链数据层安全的潜在研究目标。

7.3.2　区块链网络层安全

网络层安全主要是确保节点所产生的交易和区块顺利地到达所有节点，现阶段针对区块链 P2P 网络的主要攻击叫做分区攻击，即将受害节点与外界的通信链路劫持，从而人为的制造分区，其中比较典型的是日蚀攻击[111-112]和路由劫持攻击[113-114]。其中日蚀攻击是通过控制部分数量的节点将通往以及来自受害节点的交易丢弃，从而达到孤立受害节点的目的；路由劫持攻击则是在 AS 层面劫持某个地址块，从而孤立该属于地址块的所有矿工节点。在未来区块链的具体应用研究中，如何应对这些攻击确保区块链网络层安全是潜在的研究目标。

7.3.3　区块链共识层安全

共识层安全主要是确保各矿工节点本地区块链的一致性，目前区块链中所用到的共识算法都只能容忍一定数量的恶意节点，因此相关恶意攻击行为主要是控制更多的节点或资源（如算力、权益等）对共识发起攻击。比较典型的如针对 PoW 共识的 51%攻击①、自私挖矿[115]、顽固挖矿[116]；针对 PoS 的长远攻击②、无利害攻击③；针对 BFT 相关算法的女巫攻击[117]。因此在未来区块链的应用研究中，如何对这些攻击进行有效防御是潜在的研究目标。

7.3.4　区块链智能合约层安全

智能合约层所涉及的主要安全问题是智能合约实现上所存在的安全漏洞，这些漏洞一旦被利用可能造成严重的资金损失。据统计，八年内区块链因智能合约漏洞损失多达 12.4 亿美元④。因此编写安全完善的智能合约也是未来区块链的应用至关重要。而近几年也出现了相关研究致力于对智能合约的安全性进行验证[118-119]，或者保护智能合约免受攻击[120]，因此，如何确保智能合约安全也是未来区块链应用的潜在研究目标。

7.3.5　区块链应用层安全

区块链应用层安全所面临的一个主要问题就是用户密钥丢失、被盗，一旦失去密钥，账户上的所有资金将全部丢失。据统计，截至 2018 年 10 月，永久丢失的比特币数量接近四百万个，为总比特币数量的大约 20%⑤。因此如何设计安全的密钥管理机制，并针对密钥丢失、被盗等情况设置合理的恢复机制，是未来区块链具体应用的潜在研究目标

7.4　区块链结构演进方向

区块链在网络安全方面的应用还处于起步阶段，现阶段还没有实际的部署例子，而网络安全领域相比于区块链应用的其它领域有着自身的特点，因此在未来基于区块链的网络安全体系结构与关键技术研究中，区块链本身也应该做出一些变化去适应网络安全领域的特点。

7.4.1　引入去中心化的身份管理

与比特币交易等无需对身份信息进行考虑的区块链应用不同，许多基于区块链的网络安全应用需要将身份信息作为交易正确性验证的一个因素，例如域间路由安全中每个地址块只能由特定的 AS 进行宣告；PKI 安全中，证书的发布也只能由 CA 来完成。因此当区块链应用于这些领域时，身份管理是必不可少的。

针对身份管理问题，现阶段的联盟链项目如 Hyperledger 已经引入了 PKI 用于给每个参与个体发布 CA 证书，然而基于中心化的 PKI 来实现去中心化的网络安全应用时，依然会存在单点信任等问题。因此，在联盟链中引入去中心化的身份管理，使得每个建立在该联盟链上的网络安全应用都可以基于这套机制实现去中心化身份管理，从而减轻网络安全应用的部署难度。综上，引入去中心化的身份管理，并将其内嵌到区块链中提供身份管理服务，是未来区块链结构演进的方向之一。

7.4.2　引入去中心化的评分管理

网络安全领域中的许多应用都涉及到竞争与合作问题，且交互数据的正确与否缺乏客观判断标准，此时引入评分则可以实现基于评分的决策。例如 Yang 等人在[121]以及 Kang 等人[122]在用区块链构建车联网环境下路况信息交互平台的过程中，就引入了信用评分策略，因为车辆上报的路况信息其它用户无法立刻判断其真实性，因此可以根据用户历史上传信息的可信性评价对其打分，并根据上报信

① 51% Attack. https://www.investopedia.com/terms/1/51-attack.asp. 2019.5.6

② Long-Range Attacks: The Serious Problem With Adaptive Proof of Work. https://blog.ethereum.org/2014/05/15/long-range-attacks-the-serious-problem-with-adaptive-proof-of-work/. 2014.5.15

③ Understanding Proof of Stake: The Nothing at Stake Theory. https://medium.com/coinmonks/understanding-proof-of-stake-the-nothing-at-stake-theory-1f0d71bc027. 2018.6.8

④ 8 年损失 12 亿美元 对于智能合约漏洞你了解多少？ https://baijiahao.baidu.com/s?id=1614352386496493036&wfr=spider&for=pc. 2018.10.15

⑤ 400 万比特币永久丢失！. https://cloud.tencent.com/developer/news/334594. 2018.10.28

息用户的累计信用值来选择合适的信息源；我们最近的工作提出了一个协同边缘计算平台 Blockedge[123]，该平台允许多个边缘计算利益方合作完成从云端卸下到边缘的任务（如协同式边缘计算、协同式内容缓存分发、协同式资源管理），为了确保各利益方筛选合作者，Blockedge 引入了一套评分机制，根据区块链上所记录的用户历史合作记录以及用户资金池对其可信性进行评分。

在区块链应用于网络安全的过程中，也可以引入评分策略帮助用户进行有效决策，而决策对评分的偏好也能实现对参与角色的激励与监督作用。例如在用区块链实现协同式入侵检测时，可以对各实体进行评分，实现基于评分的采纳策略，监督大家良性合作；在区块链实现漏洞赏金时也可以对参与者进行评分，以予放其随意上报漏洞或洪泛恶意漏洞报告等恶意行为；用区块链促进中心化 PKI 安全中，对 CA 评分帮助用户选择 CA，从而实现对 CA 的监督；用区块链构建去中心化 PKI 时可以根据用户的历史签名记录对其进行评分，从而对其监督避免其随意签名。因此在未来的研究中，实现去中心化的评分机制是区块链结构演进方向之一。

7.4.3 构建去中心化的网络安全应用平台

一直以来，研究者们针对如何构建一个更安全的互联网体系结构进行了大量研究[124-126]，而区块链技术的出现为构建新一代互联网体系结构提供了新的解决思路。现阶段基于区块链的网络安全研究主要是局限于某个单独的应用，还缺乏对整个网络安全体系结构的系统性考虑，只有少部分研究在进行初步的探索，例如华为所提出的 DII 架构[44]以及我们最近所提出的去中心化的互联网基础设施架构[127]。尽管以太坊、Hyperledger 等区块链架构已经作为去中心化的应用平台被广泛使用，但这些平台并不是针对网络安全体系结构本身的特点而设计。因此，如何针对网络本身的特点，基于区块链构建一个去中心化的网络安全应用平台，进而构建一个可验证、可追溯、可协同、开放的新一代互联网体系结构，是未来区块链演进方向之一。

总结

本文主要是对近几年基于区块链的网络安全体系结构与关键技术研究进行了梳理总结，帮助读者系统全面地认识区块链在网络安全领域的最新研究进展。尽管这些研究还处于起步阶段，但是面对网络安全目前所显现的单点信任、安全算法部署困难、合作网络安全建设等问题，区块链各个部分所提供的可审计、去中心化、可信性等特性提供了新的解决思路，并以真实存储、真实计算、真实激励三种形式出现在大量网络安全技术研究中。然而，在未来具体应用的过程中，还需要加强对区块链的隐私性、可扩展性、安全性以及结构演进四方面问题重点考虑，相信随着区块链技术的发展，其必将对网络安全产生深远的影响。

参 考 文 献

[1] Arends R, Austein R, Larson M, et al. DNS security introduction and requirements. RFC 4033, 2005

[2] Lepinski M, Sriram K. BGPsec Protocol Specification. RFC 8205, 2017

[3] Xu Ke, Li Qin. Algorithms Rule the World, The Invisible Order of the Smart Economy. Beijing: Tsinghua University Press, 2017(in Chinese)
(徐恪，李沁. 算法统治世界——智能经济的隐形秩序. 北京：清华大学出版社，2017)

[4] Zhao Kuo, XING Yong-Heng. Security Survey of Internet of Things Driven by BlockChain Technology. Netinfo Security, 2017(5):1-6 (in Chinese)
(赵阔，邢永恒. 区块链技术驱动下的物联网安全研究综述. 信息网络安全, 2017(5)：1-6)

[5] XU Ke, WU Bo, SHEN Meng. Blockchain: Describe the new vision of Internet of things security. ZTE communication technology, 2018, 24(06):56-59+68 (in Chinese)
(徐恪，吴波，沈蒙. 区块链:描绘物联网安全新愿景. 中兴通讯技术, 2018, 24(06):56-59+68)

[6] Chen D, Qiu H, Zhu JH, Wang QX. Research on blockchain-based interdomain security solutions. Journal of Software, 2020, 31(1): 208-227 (in Chinese)
（陈迪，邱菡，朱俊虎，王清贤. 区块链技术在域间路由安全领域的应用研究. 软件学报, 2020, 31(1): 208-227）

[7] Tara S , Maede Z , Aiman E , et al. Security Services Using Blockchains: A State of the Art Survey. IEEE Communications Surveys & Tutorials, 2018, 21(1): 858-880

[8] Chen Ye, Xu Dong-Jin, Xiao Liang. Survey on network security based on blockchain. Telecommunications Science, 2018, 34(3): 10-16(in Chinese)
(陈烨，许冬瑾，肖亮. 基于区块链的网络安全技术综述. 电信科学, 2018, 34(3): 10-16)

[9] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. White Paper, 2008.

[10] Wood G. Ethereum: A secure decentralised generalised transaction ledger. Ethereum project yellow paper, 2014, 151: 1-32

[11] Androulaki E, Barger A, Bortnikov V, et al. Hyperledger fabric: a distributed operating system for permissioned blockchains// Proceedings of the Thirteenth EuroSys Conference. Porto, Portugal, 2018: 1-15

[12] Merkle, Ralph C. A digital signature based on a conventional encryption function//Proceedings of the Conference on the theory and application of cryptographic techniques. San Jose, USA, 1987: 369-378

[13] King S, Nadal S. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. White Paper, 2012

[14] Castro M, Liskov B. Practical Byzantine fault tolerance// Proceedings of the Third Symposium on Operating Systems Design and Implementation (OSDI). New Orleans, USA, 1999, 173-186

[15] Vasilomanolakis E, Karuppayah S, Mühlhäuser M, Fischer M. Taxonomy and survey of collaborative intrusion detection. ACM Computing Surveys (CSUR), 2015, 47(4): 551–533

[16] Fung C J, Zhang J, Aib I, et al. Dirichlet-based trust management for effective collaborative intrusion detection networks. IEEE Transactions on Network and Service Management, 2011, 8(2): 79-91

[17] Zhu Q, Fung C, Boutaba R, et al. GUIDEX: A game-theoretic incentive-based mechanism for intrusion detection networks. IEEE Journal on Selected Areas in Communications, 2012, 30(11): 2220-2230

[18] Kamvar S D, Schlosser M T, Garcia-Molina H. The eigentrust algorithm for reputation management in p2p networks//Proceedings of the 12th international conference on World Wide Web. Budapest，Hungary，2003，640~651

[19] Dewan P, Dasgupta P. P2P reputation management using distributed identities and decentralized recommendation chains. IEEE Transactions on Knowledge and Data Engineering, 2009, 22(7): 1000-1013

[20] Alexopoulos N, Vasilomanolakis E, Ivánkó N R, et al. Towards blockchain-based collaborative intrusion detection systems// Proceedings of the International Conference on Critical Information Infrastructures Security. Lucca , Italy, 2017: 107-118

[21] Alexopoulos N, Vasilomanolakis E, Roux S L, et al. TRIDEnT: Building Decentralized Incentives for Collaborative Security. arXiv preprint arXiv:1905.03571, 2019

[22] Meng Weizhi, et al. Enhancing challenge-based collaborative intrusion detection networks against insider attacks using blockchain. International Journal of Information Security, 2019, 19(3): 279-290

[23] Rodrigues B, Bocek T, Lareida A, et al. A blockchain-based architecture for collaborative DDoS mitigation with smart contracts// Proceedings of the IFIP International Conference on Autonomous Infrastructure, Management and Security. Zurich, Switzerland, 2017: 16-29

[24] Yang X, Liu B, Yang F, et al. A Blockchain Based Online Trading System for DDoS Mitigation Services//Proceedings of the 2018 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Ubiquitous Computing & Communications, Big Data & Cloud Computing, Social Computing & Networking, Sustainable Computing & Communications. Melbourne, Australia, 2018: 1036-1037

[25] Golomb T, Mirsky Y, Elovici Y. Ciota: Collaborative iot anomaly detection via blockchain. arXiv preprint arXiv:1803.03807, 2018

[26] Li W, Tug S, Meng W, et al. Designing collaborative blockchained signature-based intrusion detection in IoT environments. Future Generation Computer Systems, 2019, 96: 481-489.

[27] Liang Haoran, et al. MBID: Micro-blockchain-based geographical dynamic intrusion detection for V2X. IEEE Communications Magazine, 2019, 57(10): 77-83

[28] Zhang Z, Xu K, Li Q, et al. SecCL: Securing Collaborative Learning Systems via Trusted Bulletin Boards, IEEE Communications Magazine, 2020, 58(1): 47-53

[29] Shen M, Duan J, Zhu l, et al. Blockchain-based Incentives for Secure and Collaborative Data Sharing in Multiple Clouds. IEEE Journal on Selected Areas in Communications. to appear, 2020

[30] Lepinski M, Kent S. An infrastructure to support secure Internet routing. RFC 6480, 2012..

[31] Huston G, Loomans R, Michaelson G. A Profile for Resource Certificate Repository Structure. RFC 6481, 2012

[32] Bush, Randy. Origin Validation Operation Based on the Resource Public Key Infrastructure (RPKI). RFC 7115, 2014

[33] Mohapatra, Pradosh, et al. BGP prefix origin validation. RFC 6811, 2013

[34] Cohen A, Gilad Y, Herzberg A, et al. Jumpstarting bgp security with path-end validation//Proceedings of the 2016 ACM SIGCOMM Conference. Florianopolis, Brazil, 2016: 342-355

[35] Wählisch M, Schmidt R, Schmidt T C, et al. RiPKI: The tragic story of RPKI deployment in the Webecosystem//Proceedings of the 14th ACM Workshop on Hot Topics in Networks. Pennsylvania, USA, 2015: 11: 1-7

[36] Gilad Y, Cohen A, Herzberg A, et al. Are We There Yet? On RPKI's

Deployment and Security//Proceedings of the Network and Distributed System Security Symposium (NDSS). San Diego, USA , 2017.

[37] Lychev R , Goldberg S , Schapira M . BGP Security in Partial Deployment: Is the Juice Worth the Squeeze?//Proceedings of the 2013 ACM SIGCOMM conference. New York, USA, 2013:171-182

[38] Paillisse J, Ferriol M, Garcia E, et al. IPchain: Securing IP Prefix Allocation and Delegation with Blockchain//Proceedings of 2018 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). Halifax, NS, Canada, Canada, 2018: 1236-1243

[39] Xing Q, Wang B, Wang X. Poster: Bgpcoin: A Trustworthy Blockchain-Based Resource Management Solution for BGP Security//Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. Dallas, USA, 2017: 2591-2593

[40] Xing Q, Wang B, Wang X. BGPcoin: Blockchain-Based Internet Number Resource Authority and BGP Security Solution. Symmetry, 2018, 10(9): 408

[41] Angieri S, Garcá-Martínez A, Liu B, et al. An experiment in distributed Internet address management using blockchains. arXiv preprint arXiv:1807.10528, 2018

[42] Angieri S, Garcá-Martínez A, Liu B, et al. A distributed autonomous organization for Internet address management. IEEE Transactions on Engineering Management, 2019

[43] Hari A, Lakshman T V. The internet blockchain: A distributed, tamper-resistant transaction framework for the internet//Proceedings of the 15th ACM Workshop on Hot Topics in Networks. Atlanta, USA, 2016: 204-210

[44] Liu Bing-Yang, Yang Fei, Ren Shou-Shou, Wei Xin-Peng, Yang Xue, Wang Chuang, Yan Zhi-Wei. Decentralized internet infrastructure. Telecommunications Science, 2019, 35(8): 74-87 (in Chinese)
(刘冰洋,杨飞,任首首,魏鑫鹏,杨雪,王闯,延志伟. 去中心化互联网基础设施. 电信科学, 2019, 35(8): 74-87)

[45] Saad M, Anwar A, Ahmad A, et al. RouteChain: towards blockchain-based secure and efficient BGP routing//Proceedings of the 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). Seoul, Korea , 2019: 210-218

[46] Chen Di, et al. ISRchain: Achieving efficient interdomain secure routing with blockchain. Computers & Electrical Engineering, 2020, 83: 106584

[47] Chan H, Dash D, Perrig A, et al. Modeling adoptability of secure BGP protocol//Proceedings of the ACM SIGCOMM Computer Communication Review. Pisa, Italy, 2006, 36(4): 279-290

[48] Gill P, Schapira M, Goldberg S. Let the market drive deployment: A strategy for transitioning to BGP security//Proceedings of the ACM SIGCOMM computer communication review, Toronto, Canada, 2011, 41(4): 14-25

[49] Miller C. The legitimate vulnerability market: Inside the secretive world of 0-day exploit sales//Proceedings of the Sixth Workshop on the Economics of Information Security. Pittsburgh, USA, 2007: 1-10

[50] Wu B, Xu K, Li Q, et al. SmartCrowd: Decentralized and Automated Incentives for Distributed IoT System Detection//Proceedings of the 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS). Dallas, USA, 2019: 1106-1116.

[51] Wu B, Li Q, Xu K, et al. SmartRetro: Blockchain-Based Incentives for Distributed IoT Retrospective Detection//Proceedings of the 2018 IEEE 15th International Conference on Mobile Ad Hoc and Sensor Systems (MASS). Chengdu, China, 2018: 308-316

[52] Breidenbach L, Cornell Tech I C, Daian P, et al. Enter the Hydra: Towards Principled Bug Bounties and Exploit-Resistant Smart Contracts//Proceedings of the 27th {USENIX} Security Symposium ({USENIX} Security 18). USENIX} Association, Baltimore, USA, 2018: 1335-1352

[53] Votipka D, Stevens R, Redmiles E, et al. Hackers vs. testers: A comparison of software vulnerability discovery processes// Proceedings of the 2018 IEEE Symposium on Security and Privacy (SP). San Francisco, USA, 2018: 374-391

[54] Boneh D, Franklin M. Identity-based encryption from the Weil pairing//Proceedings of the Annual international cryptology conference. Santa Barbara, USA, 2001: 213-229

[55] Sandhu R S, Coyne E J, Feinstein H L, et al. Role-based access control models. Computer, 1996, 29(2): 38-47

[56] Goyal V, Pandey O, Sahai A, et al. Attribute-based encryption for fine-grained access control of encrypted data//Proceedings of the 13th ACM conference on Computer and communications security. Alexandria, USA, 2006: 89-98

[57] Gusmeroli S, Piccione S, Rotondi D. A capability-based security approach to manage access control in the internet of things. Mathematical and Computer Modelling, 2013, 58(5-6): 1189-1205

[58] Ouaddah A, Mousannif H, Elkalam A A, et al. Access control in the Internet of Things: Big challenges and new opportunities. Computer Networks, 2017, 112: 237-262

[59] Fernandes E, Jung J, Prakash A. Security analysis of emerging smart home applications//Proceedings of the 2016 IEEE Symposium on Security and Privacy (SP). San Jose, USA, 2016: 636-654

[60] Xiao Y, Jia Y, Liu C, et al. Edge Computing Security: State of the Art and Challenges. Proceedings of the IEEE, 2019, 107(8): 1608-1631.

[61] Mao Y, You C, Zhang J, et al. A survey on mobile edge computing: The communication perspective. IEEE Communications Surveys & Tutorials, 2017, 19(4): 2322-2358

[62] Zyskind G, Nathan O. Decentralizing privacy: Using blockchain to protect personal data//Proceedings of the 2015 IEEE Security and Privacy Workshops. San Jose, USA, 2015: 180-184

[63] Shafagh H, Burkhalter L, Hithnawi A, et al. Towards blockchain-based auditable storage and sharing of IoT data//Proceedings of the 2017 on Cloud Computing Security Workshop. Dallas, USA, 2017: 45-50

[64] Dagher G G, Mohler J, Milojkovic M, et al. Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustainable Cities and Society, 2018, 39: 283-297

[65] Ouaddah A, Abou Elkalam A, Ait Ouahman A. FairAccess: a new Blockchain based access control framework for the Internet of Things. Security and Communication Networks, 2016, 9(18): 5943-5964

[66] Pinno O J A, Gregio A R A, De Bona L C E. Controlchain: Blockchain as a central enabler for access control authorizations in the iot//Proceedings of the 2017 IEEE Global Communications Conference. Singapore, Singapore, 2017: 1-6

[67] Novo O. Blockchain meets IoT: An architecture for scalable access management in IoT. IEEE Internet of Things Journal, 2018, 5(2): 1184-1195

[68] Zhang Y, Kasahara S, Shen Y, et al. Smart contract-based access control for the internet of things. IEEE Internet of Things Journal, 2018, 6(2): 1594-1605

[69] ALI G, Ahmad N, Cao Y, et al. Blockchain based permission delegation and access control in Internet of Things (BACI). Computers & Security, 2019, 86: 318-334.

[70] Liu H, Zhang Y, Yang T. Blockchain-enabled security in electric vehicles cloud and edge computing. IEEE Network, 2018, 32(3): 78-83.

[71] Pan J, Wang J, Hester A, et al. Edgechain: An edge-iot framework and prototype based on blockchain and smart contracts. IEEE Internet of Things Journal, 2018: 4719 - 4732

[72] Scheitle Q, Gasser O, Nolte T, et al. The Rise of Certificate Transparency and Its Implications on the Internet Ecosystem// Proceedings of the Internet Measurement Conference 2018. Boston, USA, 2018: 343-349

[73] Amann J, Gasser O, Scheitle Q, et al. Mission accomplished?: HTTPS security after DigiNotar//Proceedings of the 2017 Internet Measurement Conference. London, UK, 2017: 325-340

[74] Liu Y, Tome W, Zhang L, et al. An end-to-end measurement of certificate revocation in the web's PKI//Proceedings of the 2015 Internet Measurement Conference. Tokyo, Japan, 2015: 183-196

[75] Szalachowski P, Chuat L, Perrig A. PKI safety net (PKISN): Addressing the too-big-to-be-revoked problem of the TLS ecosystem// Proceedings of the 2016 IEEE European Symposium on Security and Privacy (EuroS&P). Saarbrucken, Germany, 2016: 407-422

[76] Matsumoto S, Reischuk R M. IKP: Turning a PKI around with decentralized automated incentives//Proceedings of the 2017 IEEE Symposium on Security and Privacy. San Jose, USA, 2017: 410-426

[77] Chen J, Yao S, Yuan Q, et al. CertChain: Public and Efficient Certificate Audit Based on Blockchain for TLS Connections// Proceedings of the IEEE INFOCOM 2018-IEEE Conference on Computer Communications. Honolulu, USA, 2018: 2060-2068

[78] Kubilay M Y, Kiraz M S, Manta H A. Certledger: A new pki model with certificate transparency based on blockchain. Computers & Security, 2019, 85: 333-352

[79] Gennaro R, Steven G. Fast multiparty threshold ECDSA with fast trustless setup//Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. Toronto, Canada 2018: 1179-1194

[80] Caronni G. Walking the web of trust//Proceedings of the IEEE 9th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WET ICE 2000). Gaithersburg, USA, 2000: 153-158

[81] Brown M, Cheung D, Hankerson D, et al. PGP in Constrained Wireless Devices//Proceedings of the 9th USENIX Security Symposium. Denver, USA, 2000: 247-262

[82] Elkins M, Del Torto D, Levien R, et al. MIME security with OpenPGP. RFC3156, 2001

[83] Garfinkel S. PGP: pretty good privacy. Sebastopol, USA: O'Reilly Media, 1995

[84] Datta A, Hauswirth M, Aberer K. Beyond" web of trust": Enabling P2P E-commerce//Proceedings of the IEEE International Conference on E-Commerce. Newport Beach, USA, 2003: 303-312

[85] Fromknecht C, Velicanu D, Yakoubov S. A Decentralized Public Key Infrastructure with Identity Retention. IACR Cryptology ePrint Archive, 2014: 803

[86] Axon L, Goldsmith M. PB-PKI: A Privacy-aware Blockchain-based PKI//Proceedings of the 14th International Conference on Security and Cryptography(SECRYPT). Madrid, Spain, 2017: 311-

318

[87] Jiang W , Li H , Xu G , et al. PTAS: Privacy-preserving Thin-client Authentication Scheme in Blockchain-based PKI. Future Generation Computer Systems, 2019, 96: 185-195

[88] Al-Bassam M. SCPKI: a smart contract-based PKI and identity system//Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts. Abu Dhabi, United Arab Emirates, 2017: 35-40

[89] Yakubov A , Shbair W , State R . BlockPGP: A Blockchain-based Framework for PGP Key Servers//Proceedings of the Sixth International Symposium on Computing and Networking. Takayama, Japan, 2018: 316-322

[90] Shen M, Liu H, Zhu L, et al. Blockchain-Assisted Secure Device Authentication for Cross-Domain Industrial IoT. IEEE Journal on Selected Areas in Communications, to appear, 2020

[91] Ali M, Nelson J, Shea R, et al. Blockstack: A global naming and storage system secured by blockchains//Proceedings of the 2016 {USENIX} Annual Technical Conference ({USENIX}{ATC} 16). Denver, USA, 2016: 181-194

[92] Ali M, Shea R, Nelson J, et al. Blockstack: A new decentralized internet. Whitepaper, 2017.

[93] Miers I, Garman C, Green M, et al. Zerocoin: Anonymous distributed e-cash from bitcoin//Proceedings of the 2013 IEEE Symposium on Security and Privacy. Berkeley, USA, 2013: 397-411

[94] Kosba A, Miller A, Shi E, et al. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts//Proceedings of the 2016 IEEE symposium on security and privacy (SP). San Jose, USA, 2016: 839-858

[95] Andrychowicz M, Dziembowski S, Malinowski D, et al. Secure multiparty computations on bitcoin//Proceedings of the 2014 IEEE Symposium on Security and Privacy. San Jose, USA, 2014: 443-458

[96] Bentov I, Kumaresan R. How to use bitcoin to design fair protocols//Proceedings of the Annual Cryptology Conference. Santa Barbara, USA, 2014: 421-439.

[97] Kumaresan R, Bentov I. How to use bitcoin to incentivize correct computations//Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. Scottsdale, USA, 2014: 30-41

[98] Kumaresan R, Moran T, Bentov I. How to use bitcoin to play decentralized poker//Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. Denver, USA, 2015: 195-206

[99] Zyskind G, Nathan O, Pentland A. Enigma: Decentralized comp utation platform with guaranteed privacy. arXiv preprint arXiv:1506.03471, 2015

[100] Larimer D. Delegated proof-of-stake. Bitshare whitepaper, 2014

[101] Gilad Y, Hemo R, Micali S, et al. Algorand: Scaling byzantine agreements for cryptocurrencies//Proceedings of the 26th Symposium on Operating Systems Principles. Shanghai, China, 2017: 51-68

[102] Luu L, Narayanan V, Zheng C, et al. A secure sharding protocol for open blockchains//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. Vienna, Austria, 2016: 17-30

[103] Kokoris-Kogias E, Jovanovic P, Gasser L, et al. Omniledger: A secure, scale-out, decentralized ledger via sharding//Proceedings of the 2018 IEEE Symposium on Security and Privacy (SP). San Francisco, USA, 2018: 583-598

[104] Dang H, Dinh T T A, Loghin D, et al. Towards scaling blockchain systems via sharding//Proceedings of the 2019 International Conference on Management of Data. Amsterdam, Netherlands, 2019: 123-140

[105] Zamani M, Movahedi M, Raykova M. Rapidchain: Scaling blockchain via full sharding// Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. Toronto, Canada, 2018: 931-948

[106] Zhu Li, Yu Huan, Zhan Shi-Xiao, Qiu Wei-Wei, Li Qi-Lei. Research on high-performance consortium blockchain technology. Ruan Jian Xue Bao/Journal of Software, 2019,30(6):1577−1593 (in Chinese).
(朱立, 俞欢, 詹士潇, 邱炜伟, 李启雷. 高性能联盟区块链技术研究. 软件学报, 2019,30(6):1577−1593)

[107] Si Xue-Ming, Xu Mi-Xue, Yuan Chao. Survey on security of blockchain. Journal of Cryptologic Research, 2018, 5(5): 458–469 (in Chinese)
(斯雪明, 徐蜜雪, 苑超. 区块链安全研究综述. 密码学报, 2018, 5(5): 458-469.)

[108] Lin I C, Liao T C. A Survey of Blockchain Security Issues and Challenges. IJ Network Security, 2017, 19(5): 653-659

[109] Arute F, Arya K, Babbush R, et al. Quantum supremacy using a programmable superconducting processor. Nature, 2019, 574(7779): 505-510

[110] Esgin M F, Zhao R K, Steinfeld R, et al. MatRiCT: Efficient, Scalable and Post-Quantum Blockchain Confidential Transactions Protocol//Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. London, UK, 2019: 567-584

[111] Heilman E, Kendler A, Zohar A, et al. Eclipse attacks on bitcoin's peer-to-peer network//Proceedings of the 24th {USENIX} Security

Symposium ({USENIX} Security 15). Washington, USA, 2015: 129-144

[112] Tran M, Choi I, Moon G. J, et al. A Stealthier Partitioning Attack against Bitcoin Peer-to-Peer Network//Proceedings of the 2020 IEEE Symposium on Security and Privacy (SP). San Francisco, USA, 2020: 496-511

[113] Apostolaki M, Zohar A, Vanbever L. Hijacking bitcoin: Routing attacks on cryptocurrencies//Proceedings of the 2017 IEEE Symposium on Security and Privacy (SP). San Jose, USA, 2017: 375-392

[114] Saad M, Cook V, Nguyen L, et al. Partitioning attacks on bitcoin: colliding space, time, and logic//Proceedings of the 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS). Dallas, USA, 2019: 1175-1187

[115] Kwon Y, Kim D, Son Y, et al. Be selfish and avoid dilemmas: Fork after withholding (faw) attacks on bitcoin//Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. Dallas, USA, 2017: 195-209

[116] Nayak K, Kumar S, Miller A, et al. Stubborn mining: Generalizing selfish mining and combining with an eclipse attack//Proceedings of the 2016 IEEE European Symposium on Security and Privacy (EuroS&P). Saarbrucken, Germany, 2016: 305-320

[117] Douceur J R. The sybil attack//Proceedings of the International workshop on peer-to-peer systems. Cambridge, USA, 2002: 251-260

[118] So S, Lee M, Park J, et al. VeriSmart: A Highly Precise Safety Verifier for Ethereum Smart Contracts//Proceedings of the 2020 IEEE Symposium on Security and Privacy (SP). San Francisco, USA, 2020: 718-734

[119] Permenev A, Dimitrov D, Tsankov P, et al. Verx: Safety verification of smart contracts//Proceedings of the 2020 IEEE Symposium on Security and Privacy (SP). San Francisco, USA, 2020: 414-430

[120] Rodler M, Li W, Karame G O, et al. Sereum: Protecting existing smart contracts against re-entrancy attacks. arXiv preprint arXiv:1812.05934, 2018

[121] Yang Z, Yang K, Lei L, et al. Blockchain-based decentralized trust management in vehicular networks. IEEE Internet of Things Journal, 2018, 6(2): 1495-1505

[122] Kang J, Yu R, Huang X, et al. Blockchain for secure and efficient data sharing in vehicular edge computing and networks. IEEE Internet of Things Journal, 2018, 6(3): 4660-4670

[123] Wu B, Xu K, Li Q, et al. Toward Blockchain-Powered Trusted Collaborative Services for Edge-Centric Networks. IEEE Network, 2020, 34(2): 30-36

[124] Xu Ke, Zhu Min, Lin Chuang. Internet Architecture Evaluation Models, Mechanisms and Methods. Chinese Journal of Computers, 2012, 35(10): 5-26 (in Chinese)
（徐恪, 朱敏, 林闯. 互联网体系结构评估模型、机制及方法研究综述. 计算机学报, 2012, 35(10): 5-26.）

[125] Xu Ke, Zhu Liang, Zhu Min. Architecture and key technologies of internet address security. Journal of Software, 2014,25(1):78−97 (in Chinese)
(徐恪, 朱亮, 朱敏. 互联网地址安全体系与关键技术. 软件学报, 2014, 25(1): 78−97)

[126] McCauley J, Harchol Y, Panda A, et al. Enabling a permanent revolution in internet architecture//Proceedings of the 2019 ACM SIGCOMM conference. Beijing, China, 2019: 1-14

[127] Xu Ke, Xu Song-Song, Li Qi. Decentralized trusted Internet infrastructure based on blockchain. Communications of the CCF. 2020, 16(2): 29-34 (in Chinese)
(徐恪, 徐松松, 李琦. 基于区块链的去中心化可信互联网基础设施. 中国计算机学会通讯. 2020, 15(12): 11-16)

XU Ke, born in 1974, Ph. D. , professor, Ph. D. superviser. His research interests include Internet architecture, high performance router, P2P network, Internet of Things and network economics.

LING Si-Tong, born in 1997, M. S. candidate. His research interest is include Blockchain and network security.

LI Qi, born in 1979, Ph. D. , associate professor. His research interests include network and system security, particularly in Internet and cloud security, mobile security, and big data security.

WU Bo, born in 1990, Ph. D. . His research interests include network architecture, network security, next generation Internet and Blockchain.

SHEN Meng, born in 1988, Ph. D. , associate professor. His research interests include network security and privacy-preserving algorithms in cloud computing.

ZHANG Zi-Chao, born in 1995, M. S. candidate. His research interests include federated learning, network security and Blockchain.

YAO Su, Ph. D. , research assistant. His research interests include next generation Internet architecture and network security.

LIU Xin, engineer. His research interests include platform development, big data, product design, and 5G.

LI Lin, engineer. His research interests include internet platform development, product design, big data development, system operation and troubleshooting.

Background

At present, network security faces many problems. For example, most of today's network security infrastructure are all realized as a centralized architecture, which exposes serious single-point of trust issues. Secondly, since the early design of network architecture did not take security into account too much, the deployment of many later proposed security mechanisms not only requires modifications to existing network protocols but also affects the efficiency of network operation, which causes difficulties in the actual deployment. Besides, network security construction should be participated by many organizations. However, there is a lack of trustworthy incentive mechanism to coordinate the cooperation between different organizations and mobilize the enthusiasm of users to participate in the network security construction. Blockchain is a trusted distributed database with characteristics such as decentralization, immutability, and auditability. in blockchain, researchers have tried to apply it to network security and generate much research.

This paper systematically summarizes the research works on network security architecture and key technologies based on blockchain. The authors first introduce principles of blockchain technology and divide blockchain applications into three areas: network-layer security, application-layer security, and PKI security. And then categorize the role of blockchain in network security applications into three situations: true storage, true computing, and true incentives. Furthermore, they concretely introduce the researches, Specific application areas include collaborative intrusion detection, inter-domain routing security, Vulnerability detection crowdsourcing, access control, and PKI security. Lastly, they analyze the privacy issues, scalability issues, security issues, security issues, and structure evolution direction of blockchain. And prospect the future network security architecture and key technologies based on blockchain.

This work is supported by the National Key R&D Program of China (2018YFB0803405), National Science Foundation for Distinguished Young Scholars of China (61825204), National Science Foundation of China (61932016, 61802222), Beijing Outstanding Young Scientist Program (BJJWZYJH01201910003011), Beijing National Research Center for Inf ormation Science and Technology (BNRist) (BNR2019RC01011), PCL Future Greater-Bay Area Network Facilities for Largescale Experiments and Applications (LZC0019), and Huawei Technologies Co. Ltd (HF2019015003)