区块链应用环境下安全保护关键技术研究

◆彭劲杰　龙若兰

(湖南省委党校　湖南　410006)

摘要：区块链作为一种先进的计算机技术，已经成为继大数据、云计算、人工智能后的又一重大发明，成为了当前信息世界的重要组成内容。区块链应用领域广泛，以比特币等数字货币为代表，覆盖了金融、物流、政法、科研、教育等各个领域，因此也吸引了更多的科研机构对其进行研究。目前，许多区块链学者及应用企业联合构建了安全保护架构，引入了 P2P 网络技术、分布式账本技术、非对称加密解密技术、共识机制技术、智能合约技术实现区块链信息保护，能够实现区块链信息一致性、隐私性、不可否认性、数据完整性保护，进一步提高了区块链应用性能，可以在各个领域得到推广。

关键词：区块链；分布式账本技术；共识机制；非对称加密解密

0　引言

区块链是计算机发展到一定阶段的产物，其采用分布式数据存储、共享机制、点对点传输、加密算法等计算机技术，利用数学方法和技术手段成功地解决了电子存储数据被单一控制方修改的问题，从而可以集合所有的参与方建立一个信任机制[1]。一般来说，区块链就是一个公共台账，所有参与方都可以共同维护这个台账，并且监督这个台账的运行，使用者可以在台账上写入记录，同时写入者的身份、操作时间都会保存在台账上。台账上的数据信息不可以被修改或删除，这些数据信息可以被所有参与者实时查阅，不可修改给参与方构建了一个信任平台[2]。区块链的智能合约功能可以加入自动控制器，控制参与者写入的内容，也可以控制参与者不能写入的内容，按照约定自动化地记录写入数据。另外，自动控制器的所有部件都是透明的，可以被所有的参与者审查，整个控制器的信息可以利用互联网进行传输，效率也非常高。区块链诞生之后，其可以有效地解决“互联网+”时代信任问题，已经成功地应用在比特币电子货币体系中，系统的代码是开源的，体系设计也是完备的，因此受到全球金融机构、政府部门的高度关注，目前瑞银、摩根大通、高盛、巴克莱银行等数百家金融机构组建了区块链联盟，研究区块链技术理论，制定区块链在金融信息化中的应用标准，促进区块链的发展、创新和壮大[3]。

1　区块链应用安全现状及存在问题分析

区块链作为一种先进的计算机技术，已经在物流运输、商品生产、金融证券、娱乐游戏、智能旅游等多个方面得到广泛应用，取得了显著的应用成效，为各领域的信息化、智能化和共享化提供了一种崭新的思路，但是也存在一定的安全问题[4]。

1.1 共识算法攻击

区块链技术的最大优点是去中心化，每一个网络节点都可以维护自己拥有的区块链账本备份，并且可以由网络中的共识节点执行共识算法，这样就可以共享记录账本，网络中正确的区块链账本就是大多数节点共同维护的账本。目前，工作量证明算法的51%的算力属于攻击，如果某一个区块链组织掌握超过 51%的算力，此时他们就会将工作的区块链转移到非法区块链上，这样就会导致全网节点在非法区块链上工作。由于比特币使用的工作量证明算法的安全性依赖于网络工作节点消耗的计算力，传统意义上 51%的算力攻击是无法达到的，但是随着 GPU、CPU 等高速处理器件利用矿池的形式集成在一起，此时区块链的某个节点就可以达到 51%的算力，因此 51%的算力攻击威胁始终存在，对于区块链的应用始终是一个安全威胁。

1.2 隐私泄露

目前，区块链的重要应用领域为金融银行，比如以比特币为代表的数字货币等，区块链对于网络中的每一个节点都是透明的，任何一个节点都可以获得区块链中相关数据信息，因此为了保护区块链的隐私，比特币使用非对称加密算法、随机数生成一个地址，这样就可以代替使用者的真实身份信息。这些方法虽然看起来能够保护用户的隐私信息，但是这些地址信息与真实世界的联系比较紧密，因此就会导致隐私泄露。

1.3 哈希碰撞

区块链按照哈希算法生成的数值连接在一起，哈希值是区块链的唯一标识，具有不可篡改的特性，如果构造出一个具有相同哈希值，但内容不同的数据区块，则可以在数据区块上进行严重的篡改，因此一旦足够多的节点共同实施哈希值篡改，就会造成难以区分数据区块，无法更好地利用区块链。

1.4 区块链编程漏洞

区块链技术通常采用数学方法建立一个双方信任关系，因此在区块链应用过程中，程序员需要编写非常复杂的应用程序，但是在数学逻辑以及编程语言方面都不是完美的，不存在无懈可击的算法，因此区块链编程具有较大的漏洞和威胁。

2　区块链应用环境下安全保护关键技术

目前，为了保证区块链的安全应用，人们引入了许多的安全保护技术，包括 P2P 网络技术、共识机制技术、非对称加解密技术等，这样就可以保护区块链数据完整性，保护使用者的隐私性，实现区块链数据的全网一致性和不可否认性[5]。

2.1 P2P 网络技术

P2P 网络是区块链稳定运行的关键技术，具有去中心、容错性强、负载均衡和隐私保护等特点。区块链网络按照 P2P 的安全要求，选择和设计最小世界模型，按照节点选择是否记账划分节点类型，划分为非记账节点和候选记账节点，非记账节点实现交易活动验证；候选记账节点可以记录隐私信息。P2P 网络经过改进，已经发展到了第三代结构化 P2P 网络模式，可以快速地定位问题，取消泛洪算法，有效减少消息发送量，降低区块链的算力攻击发生概率。

2.2 非对称加密技术

非对称加密是区块链应用安全的重要保障，非对称加密技术包含两个关键密钥，分别是公钥和私钥。系统按照 Base58 转换算法或 SHA256 哈希算法生成一个私钥，私钥是一串长度固定的字符串，然后可以利用另外一个算法根据私钥生成公钥，公钥的生成过程具有不可逆性，同时 SHA256 哈希生成的私钥数量为 2^{256} 个，因此当前的区块链算力很难破解。非对称加密技术在区块链

（下转第 33 页）

L3-SW#ping 40.1.1.1（如图 5）。

```
L3-SW#ping 40.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 40.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/12 ms
```

图 5 L3-SW 访问 R3 的连通性

4.2 验证 NAT 服务

（1）在服务器上开启 http 服务，在 index.html 文件下上编写简单的 HTML 语句；

（2）在外网 PC 机上登录 Web Browser，访问转换后的公网 IP，可以访问；

（3）在外网 PC 机上登录 Web Browser，访问其私有 IP，无法访问；

（4）将某一域名与该企业的共有 IP 地址绑定（也可以和私有 IP 绑定）。

在 WEB 服务器上，同时开启 DNS 域名服务，将公网 IP 地址 222.0.0.3 与 www.test.com 绑定；同时在 PC 上设置 DNS 服务器，其 IP 地址为 222.0.0.3，进行域名解析；此时即可在外网 PC 机上登录 Web Browser，访问 www.test.com，可以访问。

5 结论

本文解决了企业内部网络的稳定和与外部网络通信的问题，在企业网内部部署 OSPF 协议，保证企业网内部的稳定和正常通信。对于大型企业来说，其企业网络拓扑结构比较复杂，在其内网配置 OSPF 协议可以使企业网内部链路状态快速收敛，减少网络链路中的信息量。在 IPV4 地址日趋紧张的情况下，企业网使用 NAT 就显得尤为重要，一是可以缓解全球 IPV4 地址紧张的压力，二是可以为企业节约申请 IPV4 地址的资金，在一定程度上还可以抵御来自外网攻击，保证企业网络的安全。

基于单区域中的 OSPF 应用来模拟企业网络，还没有涉及防火墙的配置和 VLAN 的划分，在以后的学习实验中，应该尝试模拟更加全面的企业网，包括 VLAN 的划分、防火墙、WIFI 等。

企业网的稳定和企业内部的路由控制策略也有着很大的关系，这也是我以后学习和研究的主要方向。一个企业网不可能只用某一个单一的路由协议，应该在不同的区域或者不同的场景选择合适的协议，这样从多方面上保证企业网络的安全和稳定。

参考文献：

[1]高霞，陈智罡，袁宗福.网络设备互连学习指南[M].北京:科学出版社，2009.

[2]杭州华三通信技术有限公司.H3C 大规模路由技术 V7.0[M].浙江:杭州华三通信技术有限公司，2017.

[3]谢希仁.计算机网络[M].北京:电子工业出版社，2003.

[4]段宁华.计算机网络应用与实践教程[M].北京:清华大学出版社，2007.

[5]王达.Cisco 路由器配置与管理完全手册（第二版）[M].北京:中国水利水电出版社，2013.

[6]张钢，黄小波.思科虚拟实验平台的构建[J].实验室研究与探索，2010.

[7]陈英，马洪涛.NAT 技术的研究与应用[J].实验室研究与探索，2007.

[8]桑世庆，卢小慧.交换机/路由器配置与管理[M].北京:人民邮电出版社，2010.

项目基金：国家自然科学基金面上项目（编号：61772180）：基于深度学习的非结构化大数据分析算法研究。

（上接第 26 页）

中的应用主要包括数据加密和数字签名。

2.3 共识机制技术

共识机制是区块链应用的关键技术之一，其可以决定区块链网络中的记账节点、并对交易信息进行确认，确保区块链数据一致性。共识机制引入了工作量证明、权益证明、股份授权证明等理论。工作量证明可以解决区块链中计算困难问题，将结算耗费的代价作为新加入块凭证和获得的激励收益。权益证明可以代替工作量证明，由最高权益节点实现，完成新块加入。股份授权证明可以从权益证明中选择某些代表，从代表块中获取收益。共识机制可以使区块链网络中的节点参与安全防御，这样就可以有效抵御网络中的攻击，保障网络的安全性。同时，任何网络攻击者都需要付出最高的代价获取区块，这样就可以保证攻击区块链代价较高，降低了非法人员攻击的概率。

3 结束语

区块链是一种计算机信息技术，因此引用过程难免也会面临着黑客、木马和病毒的攻击，这些安全问题是动态的、实时的，因此区块链安全防御不仅要采用共识机制、P2P 网络技术、非对称加解密技术等技术，同时还可以引入密钥管理技术、密文访问控制技术、防 DDOS 攻击技术等，避免密钥丢失导致财产受损，进一步推动区块链的普及和发展。

参考文献：

[1]蔡蕙敏.基于区块链技术的应用及管理对策研究[J].网络安全技术与应用，2017.

[2]何渝君，龚国成.区块链技术在物联网安全相关领域的研究[J].电信工程技术与标准化，2017.

[3]赵阔，邢永恒.区块链技术驱动下的物联网安全研究综述[J].信息网络安全，2017.

[4]何蒲，于戈，张岩峰等.区块链技术与应用前瞻综述[J].计算机科学，2017.

[5]吴振宇.区块链技术的特点以及应用方法分析[J].网络安全技术与应用，2017.