基于区块链的网络空间安全技术

文/刘永丹

摘要

传统的网络安全模型存在内在脆弱性，难以应对目前不断升级的网络空间安全威胁。区块链技术实现了在去信任的网络空间中可靠地交换信息的能力，因此在网络空间安全领域具有极大的应用潜力。区块链以安全散列算法、反向链接数据结构和共识机制为核心技术要素，可在保护网络数据完整性、网络可靠通信和网上资产管理与溯源领域得到广泛应用。

【关键词】区块链技术 网络空间安全 数据安全 通信安全

网络空间指的是有相互依存的信息基础设施、通信网络和计算机系统构成的全球性空间。随着全球网络空间技术的发展，其安全性问题日益突出，黑客攻击、网络犯罪、网络恐怖主义屡禁不绝，尤其是一些网络强国将网络空间列为军事作战领域，更增加了其安全防护的复杂性。

区块链技术在节点无需互相信任的分布式系统中实现了基于去中心化信用的点对点交易、协调与协作，从而为网络安全空间中的信息内容安全和应用安全提供了新的范式，在网络空间安全领域具有极大的应用潜力。

1 不断升级的网络空间安全威胁

近年来不断涌现各类网络空间安全热点事件。从 2014 年 8 月至 2015 年 10 月，有 9 家大型美国公司和11家联邦机构被黑客入侵，其中最为著名的是索尼、目标公司、摩根大通和白宫等。美国国家情报局局长詹姆斯 • 克拉珀甚至认为，恐怖主义以上的网络攻击威胁是对美国的最大战略威胁。

传统的互联网安全模型具有两个明显的特征，既集中控制和权限分层。集中控制是通过少数几个网络特殊节点负责对用户身份进行鉴别，权限分层则给予不同级别身份的用户相应的权限。但事实证明，这两个特征具有明显的脆弱性，当前的网络攻击大多把集中式的权限管理方式作为主要攻击目标，一旦攻击得手，黑客（或者监守自盗的内部人士）就可以网络空间中为所欲为。目前互联网上的大部分信息系统依然是建立在这种脆弱的安全模型之上的，对网络空间带来很大的安全隐患。

网络空间安全威胁还将面临更多的来源。首先是物联网设备的兴起，带来了更多的安全隐患。苹果计算机公司总裁蒂姆 • 库克最近在接受“时代周刊”采访时表示，即使像 iPhone 这样常见的设备也可能被用来攻击关闭电网。其次，恶意软件的生成与计算设备呈现出类似的趋势，不同的恶意软件签名数量从 2007 年的 700 万增加到 2012 年的 1 亿。最后，国家对网络活动的支持将继续增长，至今至少有 29 个国家承认建设了进攻性的网络力量，49 个国家已经采购了黑客攻击软件。

2 区块链技术及其技术优势

2.1 区块链及其简史

区块链是一种按照时间顺序将数据区块以链条的方式组合成特定数据结构，并以密码学方式保证的不可篡改和不可伪造的去中心化共享总账，能够安全存储简单的、有先后关系的、能在系统内验证的数据。区块链可以看作是存储数字记录的数据库，数据库由网络节点共享，节点可以提交新的记录，区块链网络通过共识机制保证节点之间数据的一致性，记录一旦被输入就永远不会被更改或删除。

区块链的概念是中本聪（化名）在 2008 年发明比特币的时候，首次提出的。中本聪希望“允许利用网络支付直接从一方发送到另一方，而不通过金融机构”。中本聪提出了一个漂亮的解决方案：建立一个时间戳的、基于共识的、密码标记交易的分布式数据库，链接成无法改变的记录——区块链。比特币的所有活动都被记录在开放的互联网上的一个区块链数据库中，它完全暴露于政府、犯罪组织和黑客面前，但是比特币区块链从未被黑客入侵过。

虽然谈到区块链就一定会谈到比特币，但它们是两种独立的技术。有人将今天的区块链技术与 1992 年的互联网（万维网之前的互联网）的成熟度和创新潜力相提并论。各个行业已经认识到了区块链技术的潜力。自 2013 年以来，已将超过 10 亿美元的风险投资投入到 120 个区块链初创企业中。大型成熟公司，如洛克希德马丁公司，IBM 公司和高盛也开始考察各自部门潜在的区块链应用领域。

2.2 区块链在网络空间安全中的技术优势

区块链从实践上解决了数据科学中的一个具有挑战性的问题，即在一些节点不能被信任的不可靠网络上如何可靠地交换信息。区块链假定这些恶意节点将尝试造假，他们或者制造虚假的数据，或者操控从诚实节点得到的真实数据。区块链则利用消息传递技术和共识机制拒绝经验证为无效的虚假数据，并防止有效数据被偷偷修改或删除，有效确保数据的完整性。

区块链技术与传统的网络空间安全技术相比，具有三个显著的优势。

（1）区块链采用分布自治的数据管理结构，网络中的每个节点都天生具有安全防护能力，节点以自治的方式独立按照规则执行合约，对于恶意危害行为“步步为营、步步设防”，因此区块链可以运行在非安全的网络环境中，而且可以同时阻止外部黑客和内部人士的侵害。

（2）区块链采用共识安全机制，利用网络的总体力量积极抵御个别的恶意侵害行为，通过多数诚实节点达成的共识对抗少数恶意节点的攻击，网络规模越大反而安全性越高。恶意行为即使能够“单点突破”，也会在强大的网络共识机制作用下无形消融。

（3）区块链的安全机制具有扩展性，可以与其他安全技术有机结合，形成各个行业特点的、更灵活的安全机制。由于这些优势，区块链可以在开放式互联网上成功和安全地运行，为网络空间安全提供基础支撑。

3 区块链中的网络空间安全技术

区块链本身并不是一种全新的技术，它不仅继承了一些成熟的安全技术，还结合许多新兴安全技术，提供崭新的、独特的网络安全能力。

3.1 散列算法

区块链采用称为安全散列算法（SHA）或哈希的密码学技术。散列算法把任何数字信息（包括文本、图像、视频等）转换成具有规定长度的位串，比如通过 SHA-256 算法处理的数字信息将输出 256 位的字符串。安全散列算法有两个重要的特点。首先是原像不可逆。也就是说，知道输入值很容易通过散列算法计算出散列值，但知道散列值就没有办法计算出原来的输入值。其次在任何情况下一个输入的输出字符串都是唯一的。通过相同的散列算法处理同一条信息总是返回相同的结果，不同输入则一定不会产生相同的输出。更改输入的任何微小部分，散列值都将发生显著改变。因此，散列算法是验证电子数据完整性的有效工具，它甚至不必直接核对原来的数据就可以快速判断数据是否被改动。

3.2 区块链结构

如图 1 所示，区块链是由多个“区块”组成的链状数据库，区块则由一组记录构成，每个区块都包含与先前区块的加密链接，于是形成一串区块的链。当添加新的区块时，会在前一个块的顶部被“堆叠”。区块链的整体结构与一本书的页面相类似。区块像页面一样都有标题头和具体内容。每个区块的区块头包含几个信息，最重要的有三项：先前区块的散列值、表示块创建时间的时间戳、表示区块内容散列值的 Merkle 根节点散列值。

Merkle 散列树是一种密码学数据结构，将数据块的整体内容映射到单个散列值，它使用最少量的信息快速确认其内容的完整性。通过将每个区块与先前区块链接起来，区块链的内部一致性可以被验证而无需审核任何块的内容，就像在无需仔细阅读书籍就可以验证书中每一页是否存在一样。存储在每个区块中的信息可以是任何数字内容，包括简单文本、结构化消息、图像和视频。存储在区块链中的信息是永久受到防护的——永远不会被篡改的历史记录。

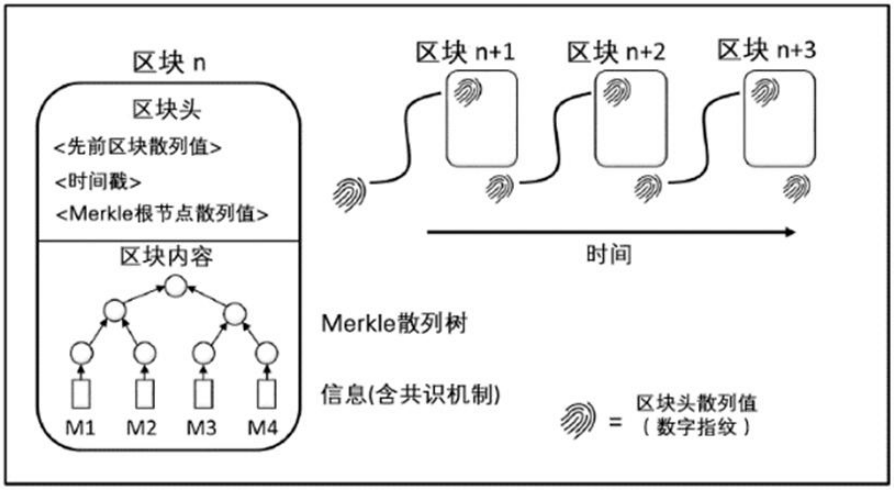

图 1：区块链的反向链式结构

3.3 共识机制

共识是一个过程，使得“一组分布式过程即使存在一些错误的过程，也能达成价值或行动方面的共同一致性”，这也被称为拜占庭将军问题。最着名的共识算法是实用拜占庭容错（PBFT）算法，被广泛用于安全关键系统，比如飞机上的四重冗余导航系统。在区块链网络中，共识被用来防止恶意节点偷偷地将虚假信息写入数据库。不同的区块链可能会使用不同的共识机制，包括各方之间的信任程度、利益的一致性，以及网络形状和同步等因素。在区块链网络上，共识机制可以联合数量占优的诚实节点来对抗少数的恶意节点，产生对恶意节点的不对称优势。因此，区块链网络规模越大越难以受到恶意的侵害。

3.4 区块链网络结构

从完全集中式结构到中心化结构，再到完全分布式结构，区块链可以采用各种网络架构，每一个网络架构都意味着对安全性和效率的某种权衡。在集中式网络中，所有外部节点都依赖于中心节点实现网络功能，如果中心节点受到危害，那么整个网络也将受到危害。而是完全分布式网络中的每个节点在功能上独立于任何其他节点，即使这些分散开来的某个节点受到危害，对整个网络的影响并不大。

3.5 访问权限控制

区块链的访问控制可以分为两类：需许可访问（permissioned）和无需许可访问（unpermissioned）。无需许可访问的（公共的）区块链不进行访问控制，任何人通过相应软件和连接入口，都可以在没有集中管控的情况下加入区块链网络并与区块链互动。相反，需许可访问的（私有的）区块链允许管理员控制网络节点、区块链的哪些部分可以被查看、哪些节点具有可以写入区块链，甚至规定哪些节点能参加共识团体。

根据区块链网络结构和访问权限控制的不同，已经演化出三种应用模式，即公共链、联盟链和私有链。公共链是完全分布化的，任何节点均可参与链上数据的读写、验证和共识过程。联盟链是多中心化的，用于多个实体构成的组织或联盟。私有链是完全中心化的，适用于特定机构的内部运行，访问控制权限完全由中心机构控制，可视需求有选择性地对外开放部分权限。

3.6 网络节点类型

网络节点既可以是区块链的普通用户，也可以是区块链的安全防护者。作为防护者的网络节点，可以通过参与共识机制来保护区块链的安全，尽管不是所有的节点都需要参与到共识的每一个方面(比如,由于访问权限的差异)。根据网络的用途不同，区块链网络中的节点类型也有所不同。根据其相对能力（例如处理、存储、通信等），区块链节点划分为三种类型，包括完整节点（full nodes）、部分节点（partial nodes）和简单节点（simple nodes）。

完整节点用作区块链网络的主干节点。

它们最重要的功能是构建和维护一个完整的、最新的区块链数据库副本。部分节点无需具备维护区块链数据库的完整副本的能力，保留仅包含每个区块头部形成的链。简单节点仅可以生成、传输和验证新记录，然而它在网络上的存在仍然可以在共识机制中发挥宝贵的作用。

4 区块链在网络空间安全领域中的应用

区块链技术在网络空间安全领域具有极大的发展潜力，从目前来看，至少在以下三个方面可以直接在网络空间中发挥安全防护作用。

4.1 保护网络数据的完整性

传统的网络空间安全主要采用边界防护的模式，以加密和信任为安全基础，但这两个技术已经被事实证明容易成为网络安全的薄弱环节。区块链则不同，它不依赖加密技术和信任机制，而是采用反向链接数据结构和共识机制来保护存储在区块链上的数据。

从本质上看，区块链不是构筑网络防御的安全边界，而是监视边界内的一切，并把虚假数据无情地“抛弃”掉。如果要攻击区块链网络上的数据，就必须对抗整个区块链网络，这样的代价非常大，往往超过了攻击本身的成本。

4.2 实现网络上的可靠通信

区块链技术可以在高度对抗的环境中提供可靠的通信。以比特币为例，比特币使用的P2P 消息传递技术，可在几秒钟内将每条消息传播到世界各地的每个活动节点。比特币网络上的每个节点都提供这项服务（包括智能手机）。如果地面、无线或卫星互联网服务被中断，则可以通过诸如高频无线电、传真甚至转录成条形码和手持的备用信道发送比特币消息。

对于区块链网络来说，由于没有“主要的”中心化节点可中断，所以即使大部分节点的连接被断开，区块链网络也可以持续运行。即使通信路径、单个节点或区块链本身遭受了恶意攻击，这些协议确保了经过验证的消息流可靠地传输到世界各地。

4.3 网上资产管理与溯源

利用区块链能够对有形资产和无形资产进行确权、授权和监控。对于网上的无形资产而言，利用区块链的时间戳技术和不可篡改等特点，可应用于知识产权保护、域名管理、积分管理等领域；对于有形资产而言，区块链就需要结合物联网的技术为资产标注唯一标识，对标识进行管理，形成对数字化的有形资产的安全可控的管理，可应用于房屋、车辆等实物资产使用权的发放和回收。

区块链还能够结合物联网技术，对供应链管理的资产转移创建永久记录，从而建立来源出处记录，为上下游不同行业之间的产品流动提供产品溯源等功能，提高产品使用中的透明度和安全性。

5 结论与建议

区块链颠覆了网络空间安全的许多传统假设和设计思路，为网络空间安全提供了一种崭新的安全防护模式和技术。首先，区块链是去信任的，能够在不可靠的网络空间中提供可信的系统运行环境。其次，区块链是透明安全的，它使用反向链接数据结构存储去中心化的数据，还为加入额外的安全协议提供了安全的基础。最后，区块链是可容错的，使用共识机制来联合诚实节点力量来对抗恶意节点。所有这些特性就为提高网络空间全提供一种思考网络系统和网络基本架构全新的思路。区块链技术仍在发展之中，仍有不少实际问题需要解决，我们应立足本国实际，抓紧研究区块链应用于网络空间安全领域的基本途径和方法，有效提高我国的网络空间安全防护水平。

参考文献

[1] 魏亮，魏薇．网络空间安全 [M]．北京：电子工业出版社，2016:2.

[2]Kevin Granville, “9 Recent Cyberattacks Against Big Businesses,” The New York Times, February 5, 2015, http://www.nytimes.com/interactive/2015/02/05/technology/recent-cyberattacks.html.

[3]Craig Timberg, “The Real Story of How the Internet Became so Vulnerable,” Washington Post, accessed March 23, 2016, http://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1/.

[4]Nancy Gibbs and Lev Grossman, “Here’s the Full Transcript of TIME’s Interview With Apple CEO Tim Cook,” Time, March 17, 2016, http://time.com/4261796/tim-cook-transcript/.

[5]Global Horizons: Final Report: United States Air Force Global Science and Technology Vision, AF/ST TR 13-01 (Chief Scientist, United States Air Force, 2013).

[6]Jennifer Valentino-DeVries and Danny Yadron, “Cataloging the World’s Cyberforces,” Wall Street Journal, October 12, 2015, sec. Tech, http://www.wsj.com/articles/cataloging-the-worlds-cyberforces-1444610710.

[7] 袁勇，王飞跃．区块链技术发展现状与展望．自动化学报，2016, 42(04): 81-494

[8]Antonopoulos, Antonopolis Testimony, sec. Standing Senate Committee on Banking, Trade and Commerce.

[9] “The Great Chain of Being Sure about Things,” The Economist, October 31, 2015, http://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable.

[10]Miguel Correia et al., “Byzantine Consensus in Asynchronous Message-Passing Systems: A Survey.,” International Journal of Critical Computer-Based Systems 2, no. 2 (2011): 141-61.

作者简介

刘永丹(1970-)，男，天津市蓟县人。博士学历。教授。研究方向为军事信息管理 / 军队信息化建设。

作者单位

国防大学政治学院军事信息管理系　上海市 200433