区块链与网络安全

安恒研究院

自从 2008 年 10 月《比特币白皮书》发表以来，区块链作为比特币的底层技术已成为炙手可热的技术新名词。国际上，以区块链为基础的各类数字资产已近千种，总市值约近 900 亿美元；在国内，短短几年，与区块链技术相关的创业公司已多达 300 多家。有研究者甚至宣称，“区块链技术有潜力为我们的经济和社会系统创造出新的更好的平台”。毫无疑问，区块链正处于其期望膨胀期的顶部。作为信息安全从业人员，不仅要十分重视区块链其自身的安全问题，还要关注如何利用区块链技术解决已有信息安全问题。

区块链的特点

区块链顾名思义就是将一系列数据区块通过某种方式链接在一起，并且这些数据区块共享于整个网络。区块链可以看成是一个分布式共享数据库，但又不同于传统的分布式共享数据库，其具有以下几个特性。

1. 数据完整性、防篡改性和不可伪造性

区块链中主要使用的密码技术有密码哈希函数和数字签名技术。密码哈希函数具有单向性、抗碰撞性以及伪随机性，而数字签名技术有不可伪造性。将前一区块的哈希值放于当前区块中，密码哈希函数的抗碰撞性和单向性保证了数据的完整性和防篡改性。在交易记录上运用数字签名技术，其不可伪造性又保证了交易记录的完整性、防篡改性和不可伪造性。这些特性使数据一旦被写入到区块中将不可修改，只能在后续区块中添加修改说明。

2. 匿名性

由于区块链的特性，它较适用于存储数据量少但价值高的数据。因为这些数据自身和元数据（如数字货币系统中的交易双方、时间等）的敏感性，区块链在设计时往往需要借助一些密码学工具隐藏数据中的具体字段。例如比特币中单个用户可以利用任意多个地址进行交易隐藏现实世界实体与交易双方的对应关系；在门罗币和零币中则分别使用环签名和零知识证明来保护交易中的金额信息；也有一些私有链（仅有少数指定者可以成为区块生成者）设置了精细的权限控制，能够为不同角色分别赋予交易跟踪、审计等功能。

3. 抗拒绝服务攻击性

去中心化也是区块链的主要特点之一，它无需中心化代理，实现点对点的直接交互，使高效率、大规模、无中心化代理的信息交互方式成为现实。区块链的运行取决于区块的产生是否正常，只要有区块继续产生，那么区块链就一直会运行下去。由于有众多的区块生成者，因此区块链不存在单点故障的风险，能够抵抗拒绝服务攻击。

4. 对智能合约的支持

与一般的分布式共享数据库不同，区块链不仅能存储数据，而且能存储可执行的代码。例如在以太坊中定义了一种基于堆栈的图灵完备的字节码，能够用来实现一些复杂的逻辑在适当的时候被矿工执行。有很多安全协议需要一个可信的第三方，而在对等网络中，这样的第三方是很难构造的。在区块链中，可以实现一些用于审计、公正、仲裁的智能合约，取代部分可信第三方的角色。

用区块链解决网络安全问题

区块链利用密码学等安全工具和方法，设计了一套与众不同的方案来存储和处理信息，因此很适合应用在高安全性要求和参与者相互不知道身份的网络环境中。例如，由于区块链的防篡改和抗拒绝服务等安全属性，美国五角大楼考虑将其作为国防

部信息系统的重要组成部分。

1. 重要数据的存储和共享

针对医疗行业的黑客攻击造成大量的医疗数据泄露。而医疗数据的特殊性使黑客有可能利用这些数据进行骚扰、勒索等行为，伤害患者权益。同时，传统存储方案无法为医疗数据提供防篡改保护，在一些场景中有着解释性弱的缺点。另外，越来越多的医院、药企和保险公司等领域，对医疗数据的需求逐渐增加。医疗数据中患者个人信息和其他医疗信息混杂在一起，又有可能使患者的个人隐私受到威胁。这是医疗大数据的困境，也是很多重要数据在存储和共享时的困境。数据既需要一定程度的隐私保护和验证，又需要在一定程度上开放。利用区块链，可以在细粒度地确保数据隐私的前提下，保证数据不被篡改。同时，区块链的特性使链上的其他机构能够在有权限的情况下灵活使用数据，为用户数据的流转提供方便。监管部门也可以通过区块链对链上数据的交易等操作进行更加精细的审计和管理。2017 年 1 月，IBM 已经宣布与美国食品与药品管理局（FDA）建立新的合作关系，研究区块链技术在保护医疗数据方面的应用。

2. 保护关键基础设施

互联网时代，大量应用程序的运行都离不开 DNS 服务。一旦 DNS 服务出现故障，就有可能导致大范围的服务瘫痪。2009 年 5 月 19 日，江苏、安徽、广西、海南、甘肃、浙江六省陆续出现大规模的网络故障。事件的起因是此前一天 DNS 服务提供商 DNSPod 遭到攻击后瘫痪，导致使用 DNSPod 服务的视频软件暴风影音无法解析软件官网，继而引发大量的 DNS 请求上一层 DNS 服务器，将上层服务器拖垮。从这一案例可以看出，目前互联网中的中心化基础设施不但会成为性能瓶颈，而且非常容易因为单点故障而瘫痪，继而波及基于这些基础设施构建的服务和应用程序，从而引发巨大的连锁反应，使应用程序和服务甚至其他基础设施失效。目前，已有一些运用区块链技术实现的关键基础设施。例如，在以太坊区块链上实现的分布式 DNS 系统 Nebulis。

3. 区块链社交网络

目前的社交网络大多是中心化结构，由用户创造内容，用户利用社交网络进行人际关系的沟通与维护、获取朋友动态、热点内容等信息；由社交网站设定规则、管理存储内容以及分发内容。由于用户之间的交互都是通过中心化的社交网站实现，使作为服务提供商的社交网站能够掌握用户的个人信息以及产生的数据，继而造成用户隐私泄露。同时，由社交网络管理用户也容易造成用户对网络管理者的不信任。利用区块链搭建的社交网络，由于区块链分布式运作的特点，用户对发布的内容、个人账户等数据有更多的控制权。区块链对用户信息和消息的严格加密则保障了用户的个人隐私。而社交网络中的发文、点赞、投票、浏览等操作都可以与构筑在区块链上的数字货币系统结合起来，构造出一个合适的激励机制，结合智能合约设计社交网络中的用户公约，使社交网络中的用户能够在数字货币的驱动下共同维护社交网络的正常运行。目前，已有多家公司正在尝试这方面的工作，如 Steemit、Synereo 和 Yours。

4. 智能合约实现网络众筹

智能合约是通过利用区块链去中心化、去信任化等特点实现数据的可编程，当一个预先编好的条件被触发时，智能合约便会执行相应的合约条款。智能合约的生命周期具有三个阶段：合约生成、合约发布、合约执行。在合约生成阶段，合约参与方需要相互协商制定合约文本并且由具备相关领域专业知识的专家和合约方进行协商制定生成合约代码，之后在虚拟机上运行，以保证合约文本与合约代码的一致性。合约发布与交易发布大体相同，合约制定之后，合约参与方将合约发布到 P2P 网络，网络中的节点将合约打包到区块链中，各节点进行相互转发并且定时更新，使所有节点对新发布的合约达成一致。合约执行期，即当触发条件达到时，合约交易自动执行。由区块链物联网公司 Slock.it 在

（下转 98 页）

短期技能培训。

网络空间安全一级学科的建设及人才培养

2015 年，国务院学位委员会和教育部批准设立网络空间安全一级学科，下设五个学科方向：安全基础、密码学及应用、系统安全、网络安全和应用安全。

目前，许多高校已经成立网络安全学院，制定人才培养方案，根据本校的特色和优势，设置相应的学科专业和方向，培养有特色的学生。如何保障网络安全是学科专业的鲜明特色，学科专业建设和人才培养必须围绕“网络安全”做文章，离开“安全”就失去设立网络空间安全学科的目的和意义。

在研究网络空间安全学科专业体系架构建设及人才培养方案时，一定要突出学科专业特色，明确学生应该学习掌握哪些学科专业知识和技术：例如将计算机硬件、计算机编程、软件开发技术、网络架构体系技术、无线有线通讯及无线网络技术、密码学、网络安全基础理论和网络安全法规等作为专业基础课。

从网络安全存在的主要问题及社会需求的角度出发，可以把以下 6 项技术作为学科专业和学生应学会并掌握的特色技术：第一，网络安全防护技术。包括网络实时预防技术，防火墙、网关、网闸、加密技术（数字加密、生物加密，如指纹、人脸、虹膜等）；第二，网络安全预警技术。包括网络实时监测技术，网络攻击响应技术，异常特征、异常动态、异常流量等识别及分析技术；第三，网络漏洞病毒等处置技术。包括检测发现漏洞技术，预防查杀木马等病毒技术，病毒、漏洞的特点分析及病毒库的建设技术等；第四，数据挖掘和溯源技术。包括数据挖掘技术，网络攻击溯源技术，发现、固定、获取证据技术；第五，电子数据取证和鉴定技术。包括电子数据的发现、恢复、复制、固定、保全、传送、保存、鉴定技术等。第六，内部网络系统安全管控技术。包括政府部门、事业单位、企业等内部网络系统的安全管控技术，网络安全问题的应急处置技术等。

如果这 6 项作为网络空间安全的特色技术能够成立，就可按此创建学科理论和体系架构，加强师资队伍建设，突出学科专业特色，并把这 6 项技术设置为专业骨干课，组织编写相应的学科专业特色教材，设置相应的实验实训课目。这样，学生就可以学到具有学科专业鲜明特点的知识、技术，学校的人才培养特色和质量都会提高。

公安技术一级学科及专业的建设及人才培养

1984 年，中国人民公安大学、国际政治学院及中国人民警官大学等设立计算机应用技术专业，并于 1998 年改为计算机科学与技术专业。2003 年，因为此专业不算公安类专业，毕业生在公安系统就业没有优惠政策，此专业被改为侦查学专业下的计算机犯罪侦查方向，工科学生被授予法学学位。

2009 年 5 月，考虑到全国网络警察队伍的扩大，

（上接 96 页）

以太坊公有链上发起的一个智能合约众筹项目 The DAO，在 28 天内筹集超过 1.5 亿美元，成为全球最大的区块链项目。

结语

区块链技术在多个主体之间、对等网络内部的数据交换方面给出崭新的方式。利用哈希函数、共识机制、数字签名等技术，不但能保护隐私，保障数据的完整和真实，同时对智能合约的支持也使区块链技术在一些场合中能够作为可信第三方提供服务。区块链带来的模式转变能够带来透明性和可审计性，充分地利用共享在线服务的同时减轻潜在的安全和隐私风险。区块链将被越来越多地作为一种行之有效工具来解决已有的信息安全问题。

（本栏责编：王丹娜）