区块链安全技术体系研究

武勇[1]，李斌[2]
（1. 国家信息安全工程技术研究中心，北京 100084；
2. 中国信息安全测评中心，北京 100085）

[摘要] 区块链是一种分布式的数据库，具有去中心化和去信任化的核心特征，近年来受到高度关注，得到了广泛应用。但作为一项新兴技术，区块链同时存在不可忽视的安全风险。本文从区块链关键技术出发，提出四层技术体系，逐层分析了区块链应用面临的挑战和安全风险，并形成通用的分层安全技术体系。该安全技术体系可用于指导区块链应用建设、保障区块链应用安全和促进安全技术的进一步发展。

[关键词] 区块链；安全风险；安全体系
[中图分类号] TP309 [文献标识码] A [文章编号] 1009-8054(2018)07-0044-09

2008 年，中本聪（Satoshi Nakamoto）设计了一种名为“比特币”的电子现金系统[1]，随后在 2009 年初搭建比特币系统。随着比特币和其他各种类似代币的蓬勃发展，这些电子货币的底层技术——区块链——在近几年内得到了高速的发展，逐渐成为信息技术领域的一项重磅技术。近年来，区块链相关研究呈现井喷的趋势，并在数字货币、金融交易及清算、公证、溯源和防伪等领域得到了大量的实践和应用[2-5]。全球很多国家也纷纷将区块链看作一项战略要地，通过制定政策、研制标准、发布白皮书、推进产业发展等措施来发展和应用区块链技术。

但是，区块链技术在技术高速发展且获得广泛应用的同时，也需要清醒地认识到由于其技术和应用上的特点，区块链应用实际上也存在很多安全风险。因此，研究区块链技术存在的安全风险，并以此为基础构建区块链安全技术体系，对于促进区块链技术发展和应用安全保障具有十分重要的意义。

1 区块链技术介绍

从概念上来说，区块链是一种去中心化基础架构与分布式计算范式[6]，是一种分布式、去中心化、去信任化的存储技术[7]，是一种按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构[8]。区块链技术具有去中心化、扩展性强、安全可靠等特点，在无需信任的分布式网络中实现了安全的点到点交易。

1.1 关键技术

区块链的关键技术主要包括链式结构、分布式存储、共识机制、密码算法和智能合约等。

链式结构是指区块链的逻辑组织结构。在区块链中，数据以电子记录的形式存储在一个一个“区块（block）”中，每一个区块记录下它在被创建期间发生的所有价值交换活动。同时，在每一个区块中，专门留出一个字段来存储前一个区块头部的哈希值，使得后一个区块能指向唯一的前一个区块。由此，从创世块（第一个区块）到当前区块前后顺序相连，形成了一条长链。顾名思义，区块链就是区块以链的方式组合在一起，形成一种区块链数据库。

分布式存储是指区块链数据的物理存储形式。和集中式系统不同，区块链是通过构建分布式的存储体系和开源协议，让网络中所有的区块链节点都参与数据的存储和验证。实际上，每个区块链节点都有各自独立的、完整的数据存储，从而极大地提高数据存储的可靠性。

共识机制是为了解决拜占庭将军问题[9]而设计的。所谓共识，是指多方参与的节点在预设规则下，通过多个节点交互对某些数据、行为或流程达成一致的过程。区块链在确定将由谁来构造有效的区块时，需要通过某种协商机制，让网络中所有节点能够达成一致的结论，即取得共识。当前，常见的共识机制包括 PoW、PoS、DPoS、PBFT[10] 等。

密码算法在区块链技术中处于基础性位置，通过使用适当的密码算法，区块链保证了数据和交易的安全性。区块链中主要的密码算法包括非对称密码算法、对称密码算法和哈希算法。这些密码算法主要提供数据加解密、签名验签、完整性验证、计算账号地址、保护用户隐私等安全能力。

智能合约的引入极大地拓展了区块链的应用前景。智能合约可以嵌入到区块链中永久保存。当满足条件时，这些智能合约将被自动执行，从而可以在没有第三方的情况下可靠地进行预定义的合同协议。从用户角度来看，智能合约是一个无人值守、分布式部署、结果不可撤回的应用程序，其部署可以大幅节省因集中部署和运营管理带来的成本。

1.2 技术层次体系

按照分层架构理论，区块链中各技术组件可按照层次分组，相邻层次的组件之间通过接口交互和支撑。目前已经提出了多种区块链的技术层次体系。

朱志文[11]提出区块链三层体系，即区块链从下往上可以分为协议层、扩展层和应用层。其中，协议层也可以细分分为存储层和网络层。协议层主要包括构建区块链的底层技术，包括对等网络通信、共识算法、密码算法和分布式数据存储等；扩展层则是连接协议层和应用层之间的桥梁，包括智能合约和数据交换共享服务等技术；应用层主要包括面向用户的区块链产品，包括钱包软件、交易网站和其他应用程序。

龚鸣[12]用六层结构来描述区块链的技术架构，这六层自下而上分别是数据层、网络层、共识层、激励层、合约层、应用层。其中，数据层主要包括数据区块的链式结构、密码算法和时间戳等技术；网络层主要包括分布式组网机制、数据传播机制和数据验证机制等；共识

层是指区块链中 PoW、PoS、DPoS 和 PBFT 等各类共识机制；激励层则将经济因素集成到区块链技术体系中来，主要包括经济激励的发行机制和分配机制；合约层主要封装各类脚本、算法和智能合约，支持区块链可编程特性；应用层是指面向用户的区块链的各种应用系统和场景。在这六层中，数据层、网络层、共识层是区块链技术体系必须的，而激励层、合约层、应用层不是必须的。

中国区块链技术和产业发展论坛 [13] 根据他们的研究，发布了区块链技术架构标准，将区块链技术按照基础层、核心层、服务层和用户层等四层架构进行组织。其中，基础层提供了区块链系统正常运行所需要的运行环境和基础组件，包括分布式存储、计算和对等网络（P2P）等；核心层包括共识机制、账本记录、时间戳服务和智能合约等区块链核心技术；服务层为应用提供可靠高效的区块链访问和监控功能，包括节点接入管理、账本管理等；用户层为用户提供区块链服务，提供应用业务交互和系统管理相关功能。

这些区块链层次体系是在区块链发展的不同时期提出来的，各有不同的特点，但也同时存在一定的局限性，如朱志文 [11] 提出的层次体系中，几乎将区块链中的所有核心技术基本都放到协议层中，使得该层次内容太多，比其他两层显得更为拥挤；而后两个层次体系中存在用户层，将业务功能和系统管理等纳入该层次中，而这些功能并非区块链技术的核心和特色功能。

2 安全风险分析

2.1 四层技术体系

分析区块链应用的结构，总是可以按照三个部分来理解：最上面一部分是各种应用系统，如交易、公证和溯源等；中间是区块链的各种核心技术，负责搭建区块链，并支持上面的应用系统运行；最下面是通用的网络和计算机系统。这三部分中，最上层和最下层本身和区块链技术无关。

为充分研究和体现区块链的技术特点，本文将重点放在区块链的核心技术组件及其相互支撑关系，而不考虑最上面的应用系统和最下面的通用网络系统。

考察区块链技术的当前发展和应用状况，参考上一节给出的三种不同的分层架构，本文按照四层架构来描述区块链核心功能组件，即从下到上依次是网络与存储层、数据与算法层、共识与合约层、应用支撑层。如图 1 所示。

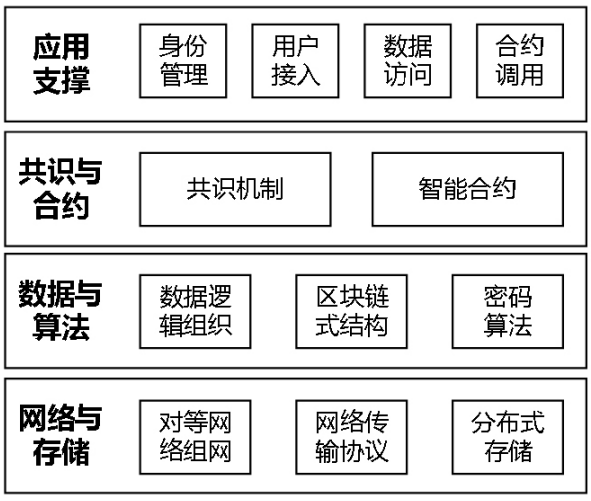

图 1 区块链层次体系

其中，网络与存储层为上层技术组件提供

节点组网和数据存储接口，主要包括对等（P2P）网络组网及优化、网络数据传输协议和分布式存储协议等技术；数据和算法层提供了区块链的数据逻辑组织和密码算法等基础性技术，包括区块数据逻辑组织、链式结构和基础密码算法等；共识与合约层则主要包括共识机制和智能合约这两项核心技术；而应用支撑层是为区块链应用系统的建立和运行而提供的一些支撑性接口和服务，主要包括身份管理、用户接入、数据访问和合约调用等。

可以看出，该四层机构将区块链的技术功能组件按照层次结构进行描述，下层为上层的功能实现提供了技术支撑。下面从各层的主要技术特点着手分析区块链应用面临的安全风险。

2.2 网络与存储层安全风险

网络与存储层面临的主要安全风险是区块链节点组网、数据传输以及存储时面临的保密性、完整性和网络可靠性方面的安全风险，包括：区块链数据在网络传输和存储时面临窃听、丢失、篡改等风险；区块链节点组网时邻居发现、连接可靠性和假冒节点攻击等风险。

如在以比特币和以太坊中为代表的大规模区块链应用中，各网络节点只需维护邻居节点的信息，并逐渐蔓延扩张到整个网络，以此保证整个网络正常运行。此时，如果恶意节点通过伪装，发布恶意数据，利用区块链节点对网络拓扑知识点有限性来发动 Sybil 攻击或 Eclipse 攻击，可以对区块链网络的完整性造成严重的破坏，造成隔离正常节点、劫持通信信息或控制其网络行为等后果。在 Ethan Heilman 等人[14]的研究基础上，2018 年 Yuval Marcus 等[15]对以太坊进行研究，发现只要两台普通机器就能成功地发起 Eclipse 攻击。

2.3 数据与算法层安全风险

数据与算法层面临的主要安全风险是使用低安全强度的密码算法、错误地实现密码算法、数据结构逻辑错误导致解析错误、交易数据树状组织不合理等。数据逻辑结构和密码算法如果没有安全的理论作为支撑，或在编码实现上存在错误使得区块链应用面临巨大的安全风险。

以密码算法为例，密码算法的安全性是区块链技术面临的最严重安全威胁之一。现有的各种区块链中，大都是采用 SHA256 和 RIMPED160 算法作为哈希算法、使用椭圆曲线密码算法作为非对称密码算法。从现有研究资料看，这些算法目前暂时没有发现有效的攻击方法。但是，随着密码学、计算技术和物理学的发展，这些算法在不久的将来可能会被破解，MD5 算法、SHA-1 算法的攻陷[16]就是前车之鉴。

同时，一个区块链应用系统是否安全，不仅仅取决于其使用了哪种密码算法，还和密码算法是否正确实现、采用的随机数是否真正随机、密钥是否被安全保管等问题密切相关。如果某个区块链应用中采用的密码算法程序本身存在漏洞或后门，这将为区块链应用系统带来致命的危害。如著名的 RSA 算法，曾经就被恶意埋入有缺陷的代码，从而降低了算法的安全强度。

2.4 共识与合约层安全风险

共识和合约层面临的安全风险是针对这两项核心技术的攻击，主要包括“51%”攻击、女巫攻击、双花攻击、DoS 攻击以及针对共识和智

能合约逻辑漏洞实施的攻击等。

共识机制是区块链得以成功的基础，如果因网络攻击使得网络节点不能取得共识，或共识机制的健壮性出现问题，那么区块链将变得不再安全。目前常用的 PoW、PoS、DPoS 以及 PBFT 等共识机制，在使用过程中都存在一定的安全风险。其中，PoW 共识机制面临的主要问题是 51% 攻击问题，即如果恶意组织掌握全网超过 51% 的算力就有能力篡改区块链数据，从而将破坏多数人的合法权益以获得自己的利益。51% 攻击在中本聪及很多安全专家一度被认为是难以达到的，然而随着矿池的出现和中心化趋势，51% 攻击发生的可能性将越来越大。

作为区块链的核心技术，智能合约极大地提升了其应用前景。但由于区块链具有不可更改和不可撤销的特点，如果智能合约代码中存在漏洞，这些漏洞将为区块链应用带来极大的安全隐患。Ivica Nikolic 等人 [17] 通过对近 100 万份智能合约进行研究，就发现其中相当多的智能合约存在漏洞。历史上，以太坊也曾因为智能合约安全问题而不得不出现了硬分叉，分叉的结果给以太坊社区带来了极大的争议和混乱，影响很大。

2.5 应用支撑层

应用支撑层面临的主要安全风险主要包括非法用户接入、数据非授权访问、弱口令、用户隐私窃取以及监管缺失等。

区块链应用中的隐私问题已经引起广泛的关注。由于区块链采取不同于传统信息系统的信息传递机制和共识机制，网络上任何一个区块链节点都可以获得链上的所有信息，包括用户地址、详细交易信息等隐私信息，这为区块链带来了严重的隐私保护难题。以比特币为例，其使用由匿名地址来代替用户的真实身份。但随着大数据的发展，通过交易数据挖掘分析以及整合真实世界的直接或间接的关联信息，完全有可能分析出一些地址所对应的用户真实身份，并和交易信息关联起来。Reid 等人 [18] 就展示通过数据挖掘技术，可以追踪到比特币大盗的真实身份。

此外，自 2014 年以来，通过利用弱口令和数据访问漏洞而发起的区块链攻击事件大量爆发。比特币交易所 Mt.Gox、Gatecoin 和 bitfinex 等均遭受过黑客攻击，导致出现用户帐号盗用、用户代币被偷等安全事件，为交易所和用户带来了巨大的损失，Mt.Gox 最终还因为损失太大而宣布倒闭。今年年初发生的 Binance 事件，黑客更是利用了社会工程学手段盗取了上万个用户帐号，并利用金融市场抛售拉空、投机套利的操作来获得巨大的利益。

3 区块链安全技术体系

区块链安全技术体系是指为保障区块链应用安全，在一定的原则指导下，将区块链中的各种安全技术按照其作用和相互间联系，以一定的结构方式组成的技术整体。

区块链安全技术体系的目的是，通过针对性地加强关键技术的安全设计和采取相关安全措施，提高区块链应用的安全运行能力，并使之能够防范和应对常见的安全风险。因此，本文在前面风险分析的基础上，也按照四层架构设计了一个通用的区块链安全技术体系，将区

块链相关的安全机制有机地部署在不同层次，并提出相应的安全要求和安全建议，以供区块链应用实现参考。安全技术体系如图 2 所示。

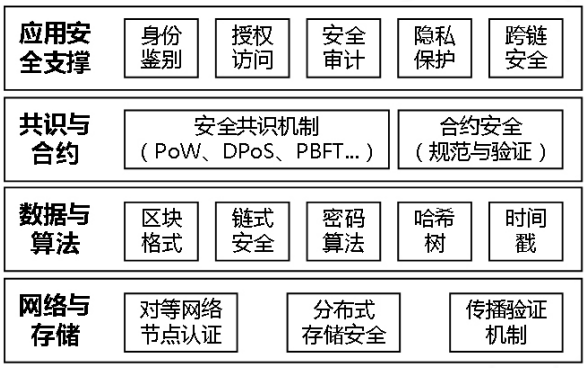

图 2 区块链安全技术体系

3.1 网络与存储层

在网络和存储层，安全技术体系主要针对该层存在的组网可靠性和数据传输方面的安全风险，通过安全设计来达到安全的区块链网络通信和可靠的分布式数据存储，主要包括：

1）构建安全和健壮的对等网络，防范网络瘫痪和被隔离攻击的风险。考虑到区块链采用 P2P 组网技术，因此，应在组网时采取合理的节点管理、资源索引、路由控制和对等网络协议等措施，建立可扩展、能自动组网、健壮的区块链节点网络，高效完成点对点网络通信，可靠地支撑上层功能。

2）构建安全的分布式存储系统，防范数据丢失、不一致，甚至被篡改的风险。应参考分布式数据库的安全功能设计分布式账本安全机制，提供高效、安全、稳定地提供数据写入及查询服务，确保区块和交易数据的可靠和一致性存储。

3）设计传播验证机制，防范区块和交易数据的泄漏、伪造和篡改风险。应在本层设计节点间通信认证机制，并加强节点间数据包的传播和验证，以增强节点间的可信鉴别、网络数据包校验和验证能力。

根据上述设计，区块链安全技术体系在网络与存储层主要的安全机制应包括对等网络安全组网、分布式存储安全和传播验证机制等安全机制等。

3.2 数据与算法层

针对数据和算法层带来的安全风险，区块链安全技术体系的主要目标是保护数据逻辑结构可靠性和可用性、保护数据签名和加密的正确性和抗攻击性，因此该安全技术体系主要从以下两个方面展开设计：

1）设计安全合理的区块数据格式和链式结构。合理的区块格式，包括定义区块头、区块、随机数、区块头哈希、交易数据等字段含义和大小，有助于在区块传播、验证效率和安全之间取得平衡。根据区块链应用的领域和关注点不同，可以设计不同的默克尔树、MPT 树结构，利用合适的树状形式和哈希算法、非对称密码算法来组织交易数据的存储，可以有效提高大量交易数据的验证和定位速度，同时也能在保证区块数据一致性的基础上，提高账本数据的完整性和不可篡改等安全保护能力。

2）设计和使用安全的密码算法和密码协议。密码学是区块链的安全基础。区块链中常用的密码算法包括哈希算法、非对称密码算法、对称密码算法等。因此，在区块链安全技术体系中，为应用选择使用合适安全强度的上述密码算法、

正确地实现这些密码算法以及加强密钥的安全管理是非常重要的，也是在实践中必须加以重点关注的。同时，时间戳的提供和验证机制，对于保证各节点之间的时间同步，确保区块计算和验证的有效性起到非常重要的作用。设计使用正确的时间戳并加以检验，可以有效地防范基于时间的攻击。

根据上述设计，区块链安全技术体系在数据与算法层主要的安全机制应包括区块格式、链式结构、密码算法、默克尔树和时间戳等。通过有效地实施这些安全机制，可保障区块链数据的可靠性、完整性和不可篡改性。

3.3 共识与合约层

共识机制和智能合约这两项技术在区块链技术框架中起到“灵魂”的作用，是区块链得以成功和发挥作用的关键。也正因为如此，近年来针对共识机制和智能合约的安全攻击也越来越多。因此，在共识和合约层，主要安全目标是保障两项关键技术安全可靠地发挥作用。区块链安全技术体系主要从共识机制和智能合约两个方面展开设计，并分别从原理设计和实现部署上确保这两项技术的安全。

1）安全共识。根据公有链、联盟链等不同应用场景设计合理和安全的共识机制，在分布式、高效和安全之间取得适当的妥协，并有效防范常见的共识攻击，如 51% 攻击和恶意代理人攻击。安全共识机制可以选择常规的或定制修改的 PoW、PoS、DPoS、PBFT 等，也可以设计可插拔机制，便于在具体应用场景中使用更为实用的共识机制。

2）安全合约。智能合约安全的目标是确保所编写的智能合约能够在充满不确定性的分布式环境下仍然能够正确、安全地运行。要达到此目的，应通过规范编码格式、设置正确的操作逻辑和采用形式化验证手段确保智能合约的安全性，严格防范出现交易顺序依赖、时间戳依赖、误操作异常、可重入攻击等漏洞。同时，还应加强合约安全监测等手段来保证及时发现和处置出现的问题，降低安全风险。

3.4 应用安全支撑层

应用支撑层是在传统的区块链之上，其本身为更好地发挥区块链的安全特性，并易于被区块链应用所使用，且避免安全与应用脱节而设计的。因此，区块链安全技术体系的主要目标是通过设计合理的安全接口，将安全技术体系的底下三层——即数据与算法层、网络与存储层、共识与合约层所提供的各种安全机制整合起来，并结合标识鉴别、访问控制和密码技术等通用安全技术，为应用系统提供安全的身份管理、用户接入、数据访问和合约调用等接口。

随着区块链的广泛应用，针对其应用安全支撑技术的研究和应用也越来越多，如利用区块链来实现身份鉴别，近年来已经有多种技术方案被提出和试用。又如隐私保护问题，由于区块链与传统信息系统的使用模式和架构不一样，很多传统的隐私保护方法在区块链中并不适用，需要根据区块链应用的实际情况研究和使用更适合的安全机制。目前在研究和应用领域比较活跃的安全机制包括：采用访问控制手段，如鉴别用户、限制用户接入；采用数据隔离手段，如将交易细节放到侧链、闪电网络或在线下执行，并不存储在公开的主链上；采用

数据变换手段；如通过数据加密、敏感数据脱敏、去标识化和同态加密等手段将重要数据进行变换；采用安全交易机制，如采用零知识证明、环签名等技术。

因此，结合区块链应用的安全需求，区块链安全技术体系在应用安全支撑层主要的安全机制应包括身份鉴别、授权访问、安全审计、隐私保护和跨链安全等。通过有效地实施这些安全机制，可以满足应用系统的保密性、完整性、可用性、真实性和不可否认性等安全需求。

4 结语

区块链是一项具有远大前景的技术，适应于在无需信任的去中心化网络环境中，用来实现可信的价值传递。区块链自诞生以来就受到了学术界和工业界的广泛关注，当前已经被应用在金融交易清算、公证、数字产权保护和物流溯源等领域。但是，区块链在应用过程中仍然面临一系列的安全挑战。本文针对区块链的技术特点，分析了其面临的主要安全风险，提出了一个通用的分层安全技术体系，可用于指导区块链应用系统建设，提高区块链应用的安全防护能力，并可促进区块链技术的进一步发展。

参考文献

[1] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[J]. Consulted, 2008.

[2] UK Government Chief Scientific Adviser. Distributed ledger technology: Beyond block chain[EB/OL]. (2018-04-29).https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf.

[3] Swan M. Blockchain: Blueprint for a New Economy[M]. O'Reilly Media, Inc. 2015.

[4] 乌镇智库 . 中国区块链产业发展白皮书 [EB/OL]. (2018-04-29).http://h5.iwuzhen.org/pdf/China-blockchain-201704.pdf.

[5] 蔡维德 , 郁莲 , 王荣 , 等 . 基于区块链的应用系统开发方法研究 [J]. 软件学报 , 2017, 28(6):1474-1487.

[6] 袁勇 , 王飞跃 . 区块链技术发展现状与展望 [J]. 自动化学报 , 2016, 42(4):481-494.

[7] 谢辉 , 王健 . 区块链技术及其应用研究 [J]. 信息网络安全 , 2016, (9):192-195.

[8] 中国区块链技术和产业发展论坛 . 中国区块链技术和应用发展白皮书 [M]. 北京：工业和信息化部 , 2016.

[9] Lamport L, Shostak R, Pease M. The Byzantine generals problem. ACM Trans. on Programming Languages and Systems (TOPLAS), 1982,4(3):382-401.

[10] Castro M, Liskov B. Practical Byzantine fault tolerance. In: Proc. of the USENIX Association. 1999. 173-186

[11] 朱志文 . Node.js 区块链开发 [M]. 北京：机械工业出版社 , 2017.

[12] 龚鸣 . 区块链社会 : 解码区块链全球应用与投资案例 [M]. 北京：中信出版集团 ,2016.

[13] 中国区块链技术和产业发展论坛 . 区块链 参考架构 [EB / OL].(2018-04-29). http://www.cbdforum.cn/index/dd/18.do.

[14] Ethan Heilman, Alison Kendler, et al. Eclipse Attacks on Bitcoin's Peer-to-Peer Network[C]. USENIX Security Symposium, 2015:129-144.

[15] Yuval Marcus, Ethan Heilman, Sharon Goldberg. Low-Resource Eclipse Attacks on Ethereum's Peer-to-Peer Network[EB/OL].(2018-04-29). http://www.cs.bu.edu/~goldbe/projects/eclipseEth.pdf.

[16] Stevens M, Bursztein E, Karpman P, et al. The First Collision for Full SHA-1[C]. In: Katz J., Shacham H. (eds) Advances in Cryptology – CRYPTO 2017. CRYPTO 2017. Lecture Notes in Computer Science, vol 10401. Springer, Cham.

[17] Ivica Nikolic, Aashish Kolluri, et al. Finding The Greedy, Prodigal, and Suicidal Contracts at Scale[J]. CoRR abs/1802.06038 (2018), https://arxiv.org/pdf/1802.06038.pdf.

[18] Reid F, Harrigan M.An Analysis of Anonymity in the Bitcoin System[C]. IEEE Third International Conference on Privacy, Security, Risk and Trust. IEEE, 2012:1318-1326.

作者简介

武勇，国家信息安全工程技术研究中心副研究员，博士，主要研究方向为网络与信息安全。

李斌，中国信息安全测评中心研究员，博士，主要研究方向为信息安全、风险评估。

Research on blockchain security technology architecture

WU Yong[1], LI Bin[2]

(1. National information security engineering center, Beijing 100084, China;
2. China information technology security evaluation center, Beijing 100085, China)

[Abstract] As a distributed database, blockchain is fully distributed, decentralized and de-trusted. It has been attracted by many researchers in recent years, and has also been widely used. However, as an emerging technology, there are a lot of challenges and security risks in the development of blockchain. After an introduction to the technology architecture we proposed here, we analyze the security risks faced by the blockchain application layer by layer. As a result, we put forward a universal layered security technology architecture. This architecture is useful to enhance the security of a blockchain application. At the same time, it can also promote the development of blockchain security technologies.

[Keywords] blockchain; security risk; security architecture