第5章

区块链安全与隐私

区块链技术为现代数字化世界提供了一种构建信任机制的分布式账本方案，然而由于其自身技术的不完善或在应用过程中的不恰当使用，使其存在着一些与传统技术不同的安全问题。首当其冲的就是数字货币领域，该领域作为区块链的核心应用，安全事故不断出现使得安全与隐私问题受到广泛关注，例如钱包客户端漏洞缺陷、交易所遭受的黑客攻击及智能合约漏洞等，这些问题已经造成了数以亿计的经济损失。

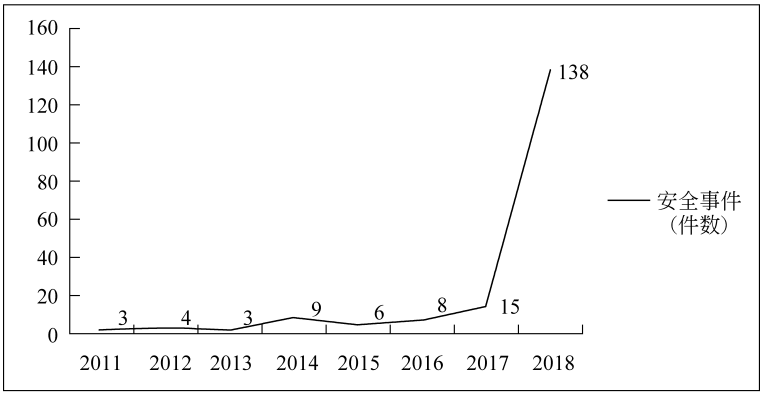
从本章开始，我们将会介绍区块链的安全与隐私问题及其相关技术。本章首先从总体层面来探讨有关区块链的安全目标，其次就存在于区块链各层级之间的主要安全问题做出介绍。在随后的章节中（第6～10章），将按照不同层级来详细分析每层中所存在的安全问题和相关的应对措施。

5.1 区块链安全与隐私威胁概述

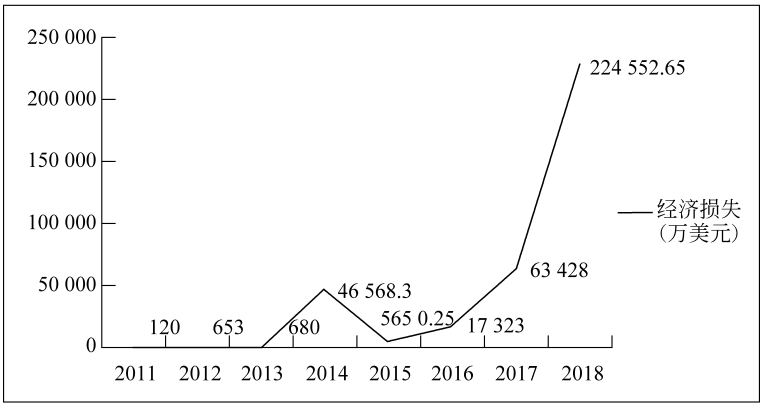
近年来，区块链的快速发展使其在各类场景中的应用越来越多，但应用中存在的安全问题也日渐凸显。例如，发生在区块链以太坊中的重大安全事件：2016年6月，黑客根据以太坊The DAO项目代码的编程模式，使项目的弱点完全可知并加以利用，盗取了所有的项目资金，造成了巨大的经济损失；2017年7月，攻击者利用与The DAO相似的攻击手段盗取了以太坊Parity钱包约3000万美元的以太币（ETH）；2018年1月，由于黑客的攻击造成Coincheck数字交易所上的NEM被盗取，经济损失超过5.2亿美元。另外，矿池也被攻击者利用来发起攻击，攻击者通过生成挖矿木马入侵受害者的计算机进行挖矿。直至2018年5月，挖矿木马入侵了数十万台主机进行挖矿获利千万美元。

如图5.1所示，据BCSEC调查数据显示，区块链相关的安全事件在2017年之后直线增长，截至2019年3月，由区块链安全漏洞引起的经济损失已经超过30亿美元，并且损失金额还在连年攀升。

本节以保密性、完整性、可用性、可控性和不可否认性为依据，将区块链相关的安全问题划分为数据安全和隐私泄露两方面，隐私泄露之所以单独作为一方面进行分析，主要在于区块链自身的特性在一定程度上已经保证了数据的完整性和不可否认性，因此其安全分析主要集中在保密性和可用性（可扩展性、交



(a) 区块链相关的安全事件统计



(b) 区块链安全造成的经济损失统计

图 5.1　区块链安全事件数量以及经济损失统计图

易吞吐量等)方面。

5.1.1　区块链数据安全威胁

区块链之所以能够在以数字货币为代表的应用领域中大放异彩,同时也能够得到其他应用领域的广泛关注,是由于区块链系统具有去中心化、可追溯、不可篡改、不可伪造、不可否认和可编程等特点。然而,区块链在安全和隐私方面的挑战仍然制约着区块链的快速发展。

首先,区块链是集信息安全与隐私保护于一体的新型技术,其相应的安全评估检测方法还处于发展过程中,这些技术(包括共识算法、激励机制、智能合约等)在某些关键环境下存在一定的安全隐患,并且已有的安全检测手段还无法完全应用到区块链中。例如,共识协议中的攻击问题:在 PoW 中存在的问题是集中 51%算力攻击的问题,即攻击者若获得了整个区块链网络的 51%算力,就有控制整个区块网络的能力,其中也包括篡改和伪造。在比特币应用中,上述提到的 51%的攻击问题带来的后果是攻击者可以实现双重支付(Double Spending),于是提出了 PoS 协议来替换 PoW 协议,上述协议的替换有效避免

了某种程度上 51%算力攻击的问题，然而新的问题会随之产生。现有的新的攻击问题有 Nothing at Stake，此问题会导致共识节点不计成本地对区块链进行分叉处理，这样会造成区块链网络中不断地产生很多分叉。漏洞检测是安全问题的一个重要方面，从漏洞检测的角度出发，区块链无法提供有效的代码漏洞检测。例如在以太坊中，虽然提供了一些模板和测试环境以方便开发者开发智能合约，但由于智能合约逻辑的复杂性和分布式运行的特性，使得智能合约在代码的编写和密码模块的利用上不可避免地让黑客有可乘之机。同时，网络架构的不一致性使得传统的入侵检测技术无法直接适用到区块链系统中，这也是导致区块链上各种安全问题无法解决的重要缘由之一。其次，量子计算机、人工智能、大数据分析等计算机技术的快速发展同样给区块链带来了安全威胁。尤其是量子计算机的出现会对区块链的安全性造成巨大冲击，量子计算机一旦产生，任意大整数的快速分解从理论上就变得极其容易，破解长度为 1024 位的非对称加密密钥只需要很短的时间，一些传统的计算性理论假设不再成立，例如基于数论的困难假设不再是密码学上的“困难”问题。2019 年 10 月 24 日，科技公司巨头谷歌的量子计算机研究团队在 *Nature* 发表论文，此论文正式向世界宣告量子计算机已被成功研发，该计算机可以有效解决当前计算机不能解决的难题，量子计算机只用 3 分 20 秒就可以完成当前第一超算需要计算 10 000 年的实验，这也表明基于传统非对称密码学的区块链技术在安全性上面临挑战。

此外，区块链的理论安全与实际应用安全之间还存在一些鸿沟。2014 年，Juan A. Garay、Aggelos Kiayias 和 Nikos Leonardos 3 位教授最先给出了有关比特币区块链的安全形式化分析和证明，列举了比特币有关的两个安全特性：公共前缀和链质量并通过协议分析得出比特币协议实现区块链的 3 个特性（活跃性、一致性和正确性）。虽然从理论上分析区块链的网络安全性比较高，但实际网络环境、用户自身安全意识和黑客主动攻击等方面的问题，仍然给区块链系统的应用带来了不可低估的安全威胁。鉴于区块链采用的网络结构是不同于传统的 P2P 结构，攻击者无法通过控制少部分节点的方式来实现对整个网络控制，但是由于实际网络部署时，各个节点之间配置的安全防护等级不同，导致攻击者可有针对性地从低安全防护等级的节点开始发起攻击，通过控制大多数节点阻碍区块链系统的正常运行。另一方面，用户在使用过程中对密钥的管理不严格，安全意识不足，或被钓鱼网站所诱骗，丢失自己的密钥，也会引发安全问题。以金融领域为例，由于区块链与金融紧密关联，相关的用户或者机构成为黑客的重点攻击目标，而一些传统用户应用层的攻击手段在区块链技术中依然可行，因此就其存在的安全问题，不论是用户自身引发的还是传统攻击手段引起的都不可忽视。

最后，匿名性、去中心化、防篡改性、自治化等特点虽然是区块链的技术标签，但与此同时也给区块链系统的安全监管带来了一系列难题。

（1）区块链的匿名性使得区块链网络系统中发生的漏洞利用等安全事件以及骗取数字货币等网络犯罪的溯源难度增加。当非授权用户利用区块链技术进行违法犯罪活动或者对系统实施攻击使得系统变得不安全时，系统很难追踪并从系统中剔除恶意用户和攻击者。例如勒索病毒，黑客利用操作系统漏洞将用户的文件进行加密处理，需要用户发送一定量的比特币来获取解密密钥。虽然比特币地址在用户交易的过程中是公开的，但其较高的匿名性使得无法链接到现实中的非法参与者。

(2) 区块链的去中心化特性导致攻击者可以在更多方面进行攻击,使得系统的安全监管的难度增大,基于区块链的分布式存储模式,数据存储在不同的节点而不是集中式的服务器,且用户的通信传输方式为点对点,不需要通过可信的集中服务器或平台,因此用户交易过程中很难获取监管数据,监管的技术接口也难以实现。

(3) 区块链的防篡改特性为恶意信息的传播提供庇护,使对数据内容的监管变得异常困难。具体地说,攻击者通过交易的方式向区块链中写入一些非法信息,利用区块链自身的同步机制实现非法信息的迅速传播,由于防篡改特性使这些非法信息难以被删除,加大了互联网监管的难度。

(4) 数据安全责任边界不清晰。在实际应用中,节点通常指的是区块链平台、应用系统、数据所有者等实体,区块链中的这些实体互不信任,这会导致在出现安全问题时,难以划清安全责任界限。

总而言之,区块链本身存在诸多亟须解决的安全问题,这些问题随着区块链应用技术的迅速发展变得更加突出。因此,确保区块链的安全性是当前区块链广泛应用面临的最棘手的问题之一。

5.1.2 区块链隐私泄露威胁

5.1.1 节主要从与区块链相关的一系列安全问题进行了阐述,与此同时,由于区块链在各个应用领域迅速的扩展延伸,使其在隐私泄露方面的问题也受到广泛关注。区块链技术之所以能够迅速发展并应用到相应的各领域,其优势在于数据的存储和处理不依赖于某个中心节点,从而避免了单点故障和权限滥用的恶意行为,是传统的中心化架构、集中式服务无法比拟的。然而,区块链中的数据需要分布式网络中的各个节点来共同维护,从而达到一致性共识,因此交易中的信息需要公开,让所有节点都能进行验证,这就使得区块链(主要指公有链、联盟链)上的公开信息毫无隐私可言。

1. 身份信息泄露

公有链没有准入机制,任何节点(包括攻击者节点)都可加入网络中进行数据维护,监听区块链网络节点之间传输的数据。因此,当攻击者想要推测出某个交易者的身份信息时,首先分析获取到的交易数据,其次通过给出的背景知识,将二者结合得到最终的交易参与者的真实身份,上述攻击可以成功的原因在于区块链上交易数据是可以关联的。通过交易的关联性关系,攻击者可以削弱区块链地址的匿名性,甚至暴露用户的真实身份。例如,Alice 在某个区块链交易平台上购买了一个比特币,它利用信用卡来进行支付,由于在美国 2000 美元以上的交易都需要实名,因此实名制使得攻击者可以通过交易的地址、金额和时间等相关数据从支付地址关联到实际支付人,从而达到获取交易者身份信息的目的。

数据挖掘技术为攻击者得到关联的交易地址提供了可能性。具体地,攻击者可以通过分析交易与交易之间的关系,得到某个地址的所有相关交易数据流。由于每笔交易都记录了所有的输入地址和输出地址的信息,通过对特定地址进行检索,就能够发现该地址的全部相关交易,只要任意一个地址对应的用户真实身份信息被暴露,其他所有和该地址

有关的地址都可能属于这个用户或相关用户，会致使更多的用户隐私数据泄露。此外，区块链服务提供商也有可能存在某些漏洞被攻击者利用，泄露用户隐私。如 2015 年，比特币论坛 Bitcointalk 就遭受网络攻击，被攻击者窃取了 49.9 万用户数据，包括用户名、密码、电子邮箱等。

数据的公开透明既是区块链技术的优势，也是区块链技术的劣势，它使得敏感信息得不到保护，通过从区块链网络中提取有价值的敏感数据，联合不同网络和平台下的用户数据，即使用户的交易费用通过比特币进行支付，也无法保证其隐私的安全性。具体地，通过利用区块链浏览器，与比特币相关的每笔交易信息都是公开可查询的，包括资金流向（即发送地址、接收地址）、交易金额、交易时间等。虽然用户使用的是匿名地址，无法直接利用交易地址查询到交易者真实的个人信息，但要查询到用户的真实信息还是有迹可循的。根据现有的研究表明，即使通过隐私保护的方法实现身份隐私，但是利用数据挖掘等手段对比特币交易信息统计分析，同时结合一些现实非比特币的交易记录，能够确认出 40％的比特币用户的真实信息。因此，简单地通过比特币的地址来实现用户交易的匿名性，这种匿名体制是不完善的，确切地说，是一种伪匿名性。

2. 交易数据泄露

大数据分析处理技术不断进步，基于大数据挖掘的分析技术可以将用户的真实身份和资金使用情况识别出来。《纽约时报》曾报道，根据用户的购物习惯、消费记录、出行数据等信息，可以准确地预测个人的隐私信息。例如，数据分析师可以通过用户的消费行为预测出某些女性购物者是否已经怀孕。一些看似无关紧要的数据可能揭示用户的敏感信息，而且一旦恶意用户出于经济利益等考虑去挖掘这类数据并进行非法利用，就很有可能损害其他合法用户的经济财产安全，甚至人身安全。

在区块链与其他具体应用相结合的情形中，会涉及大量高度隐私的数据。例如，在金融业务场景中，用户与银行之间的交易记录或者银行之间的相互交易记录都是极其敏感的数据，属于银行的核心数据，因此不论是用户还是银行，都不希望彼此之间的交易记录被其他非授权用户查看。此外，在医疗场景中，多个医院组成的联盟链可以有效促进数据的共享、有利于病情的诊断，但是个人病情同样属于极度隐私的数据，患者并不想将个人的医疗数据公开地放置在区块链环境中。由此可以看出，若想要区块链技术及其应用覆盖到其他的应用场景，隐私泄露应该是最先需要解决的问题。

区块链的多节点共同维护、公开透明等特性是把双刃剑，这项技术在带来安全性的同时，也造成了新的数据隐私性问题。第 4 章中的区块链经典理论——不可能三角，也即中心化、可扩展性和安全性三者之间的相互制约关系。同样，对于区块链的隐私性（安全性）和性能（可扩展性）之间的权衡也一直是实际应用中需要考虑的问题。为了做到安全的隐私保护，势必会影响系统的可扩展性，如何实现在保护数据隐私的同时依然能够支持不同节点针对数据进行安全、高效地验证是区块链领域中的热点研究方向，如何更进一步地保障区块链的隐私性就成为该领域的重要问题之一。

目前，从两方面考虑，既能保护隐私同时兼顾性能，有一种解决的方法就是提升硬件性能，例如，可以采用具有隐私保护功能的硬件设备 Intel SGX 同时保障效率。SGX 是由

英特尔公司开发的，旨在为商用计算机上进行的安全敏感计算提供完整性和机密性的指令集扩展，SGX 的核心技术是封装，即通过提供硬件安全的强制性保障将合法的运行软件封装在 Enclave 中，为软件的执行提供可信的环境，防止恶意者的攻击以及软件的越权访问，但此技术并不能对所有的攻击都能够识别和隔离，只能保证 Enclave 中运行数据的机密性和完整性。

通过密码协议来增强区块链的隐私性保护也是研究的热门方向，包括使用零知识证明、安全多方计算等技术来解决链上交易公开透明的问题。目前针对区块链隐私保护机制的研究按照层级来划分，主要包括网络层、数据层以及应用层 3 方面的隐私保护。

总体而言，区块链利用自身的优势为去中心化的分布式系统提供了强大的技术支撑，但是区块链本身会面临不同的安全问题和隐私威胁。为了满足实际应用的需求，需要识别这些安全问题，同时要引入有效的机制来避免安全问题的产生。

5.2 区块链安全目标

虽然区块链被证明了在满足一定的条件之后在理论上是安全的，这包括区块链所使用的密码学技术，但是在实现过程和应用过程中，由于开发者没有充分预估系统的使用环境，使得区块链系统遭受了各种攻击行为。区块链的安全性问题涵盖范围较广，从用户应用端到底层数据端都有安全问题存在。本节以区块链存在的安全问题为切入点，依次介绍区块链应用过程中包含的安全性问题。具体来说，区块链的安全目标是指利用一些现有的密码学技术手段和实施方法来保障区块链系统的应用安全，其中，应用安全主要涉及应用过程中的数据安全、共识安全、智能合约安全、内容安全、密钥安全、跨链交易安全、隐私保护以及具体的密码算法安全的设计和证明等，如图 5.2 所示。在上述的主要安全目标中，首先要实现的是数据安全，数据安全是其他方面各层级安全的基本前提。

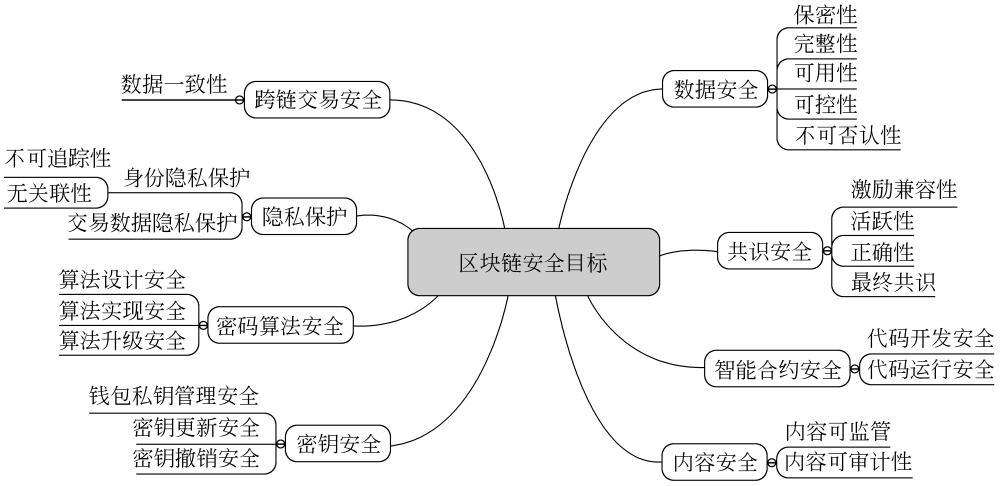


图 5.2 区块链的主要安全目标

5.2.1　数据安全

区块链实质上是一种去中心化的分布式存储系统，其保存有大量的与区块链相关的敏感数据，如用户的支付信息、交易过程、智能合约执行代码和具体的中间执行的状态等，如何保护敏感数据的隐私性是实现区块链安全的关键所在。下面基于信息安全方面的保密性、完整性、可用性、可控性和不可否认性 5 个特性定义区块链的数据安全。

1. 保密性

保密性是指避免合法用户或者实体的敏感数据泄露给非授权的或者恶意的参与者。在基于区块链的应用中，为了实现敏感数据的保密性，要求应用系统采用符合要求的、可靠的、具有安全性证明的身份认证算法、访问控制协议和安全审计机制。其中，身份认证算法是用来在计算机及网络环境中判断用户是否合法的一组认证规则，它是访问控制的基础。在传统的身份认证体系中最常用的方法是基于可信第三方的身份认证，主要是通过用户的口令或指纹等预存在平台的信息来确认用户身份。在区块链的身份认证中，每个区块或用户的加入方式和有效的身份鉴别认证方式都是确定的。例如，在公有链（如比特币中），身份认证是通过验证用户是否有合法的私钥（即口令）来验证用户身份的。为了实现身份认证又不破坏匿名性，学者们利用零知识证明方法提供相应的身份认证服务，被称为 ChainAchor 框架，此架构使得合法用户的身份可以有选择地打开，因为每个参与者都拥有多个有效交易身份。访问控制是一种按用户预设的身份来设定用户对某些信息项访问权限的技术。此技术是实现访问控制的一种最基本的方式，它允许授权用户按照权限级别来访问或使用系统的资源，任何非法用户对系统资源的访问都会被禁止。一般来说，通过对数据进行加密来实现访问控制，合法用户只有拥有与加密公钥相对应的解密私钥，才能满足访问权限，解密查看信息。对于公有链，其访问控制是通过私钥来实现的。用户可以任意加入公有链中查看数据、发送交易等操作，但在联盟链和私有链中，它有一套严格的准入机制，用户需要获得其他节点的同意才能有权限操作和访问链上的数据。

审计监管是指区块链能够对非授权的数据泄露事件进行监管，包括事件的监控、分析和追责等。它主要从法律层面保障区块链数据的保密性，确保非授权的数据泄露等不安全行为得到相应的惩罚，从管理角度来控制攻击者的恶意行为。

2. 完整性

完整性是指数据接收者得到的数据和数据发送者发送的数据是一致的，即在数据传输的过程中没有遭受恶意者的篡改。区块链利用冗余性较大的分布式数据库系统来保障链上数据的不可篡改性。区块链中的完整性主要指用户发布的交易信息、智能合约执行的中间状态不可篡改和不可伪造。在区块链中，任何已经确认的交易记录都不能被修改，已经发生的所有行为不可抵赖，例如，区块链系统中的攻击者若进行双重支付，则此行为无法抵赖。对于底层数据，数据完整性通常是基于相应的密码组件实现的，如数字签名、哈希函数等。其中，区块链中最为典型的哈希值体系结构是基于默克尔树的，使其能够维护数据完整性，同时验证数据的有效性。在共识层面上，数据存储的一致性是依靠各类共

识机制(如 PoW、PoS 等)实现的。

3. 可用性

可用性指合法用户可以对区块链系统中的数据随时地进行访问和使用。区块链系统的可用性首先应该具备抵抗单点故障和分布式容错的能力,使得系统在遭受各类攻击时仍然能够提供可靠的服务。同时,由于区块链网络主要是点对点的分布式结构,所以少部分的节点受到攻击或产生故障将不会对整个区块链系统的运行产生较大的影响,系统仍可以对外提供正常的服务。然而现有的一些攻击行为,例如自私挖矿,通过控制少部分节点来获取全网络超过 50%的资源,会影响区块链系统的可用性。此外,可用性还要求系统在遭受实际攻击时,能够在一定时间内完成修复和重构,保证系统的正常运行。其次,区块链系统的可用性还表现在能够为合法用户提供无差别服务,每个参与的节点都可以获得有效的、正确的数据,即使是新加入系统的节点也可获取相应的服务。

在限定时间内响应用户的访问数据请求是可用性非常重要的一方面,在区块链系统中有限时间内响应用户的访问数据请求的主要表现形式为可扩展性。可扩展性在区块链中要求系统具有低延时、高交易吞吐量等特性,考虑到区块链体系结构存在着不可能三角问题,为了使实现的系统具有更好的可扩展性,会在安全性、去中心化两个特性中牺牲某部分性能满足实际应用的需求。

4. 可控性

可控性指系统或数据在传输范围和存储空间的可控程度。对于区块链,可控性主要指区块链的数据在链上存储的可控安全程度。公有链中允许任何节点在任意时间都可加入,支持任意交易数据的发送,但是一定的匿名性使得非法的交易行为难以追踪。例如,暗网中有许多的用户利用比特币来进行黑市交易,甚至成为比特币的最大用户,这在一定程度上对区块链系统的可控性造成很大的冲击。因此,构建安全可控的联盟链更加符合数据安全的要求。此外,对于使用区块链技术的合法用户,可控性需要保证在不同个体之间,实现数字资产或数据在链上的安全控制权转移,防止非法用户对这些资产或数据的操作控制。

5. 不可否认性

不可否认性通常指用户不能否认自己发送信息的行为以及信息的内容,也称不可抵赖性,在此处是指用户无法否认在区块链系统中的操作行为。在区块链中,用户发送的数据都通过交易的形式被记录下来,一旦经过一定周期被确认后将无法修改。由于交易的产生与用户的地址唯一绑定,拥有该地址的用户无法否认其在区块链中所做出的操作行为。不可否认性要求在不同参与者之间,用户无法抵赖以自己身份参与所完成的操作,这需要与身份认证进行关联,同时系统支持安全审计功能,相关的审计日志需要被准确地记录下来。

5.2.2　共识安全

由于区块链网络中的节点包含个人计算机或移动客户端，与传统网络架构中的专用服务器相比，性能低、抗攻击能力差，所以这些节点很容易被攻击者或者恶意用户攻击。此外，在中心化架构中，管理者只需针对一台或者少数几台服务器进行重点保护，而在区块链网络，所有节点地位平等，很难对地理位置分散的众多节点采用相同的防护措施，这样攻击者可以选取安全保护较为薄弱的节点进行入侵，破坏区块链网络中数据的同步性。

共识机制用来保证区块链网络中的节点能够对某个提案达成一致，例如所有节点就某个区块可以加入区块链的问题，以此来确保区块链主链上数据的一致性，这是区块链的核心思想。区块链上的共识安全是实现数据安全的基石，起着重要的作用。保证区块链系统的最终共识、激励兼容性、活跃性以及正确性是实现共识机制的核心，也是衡量共识安全的重要属性。其中，满足最终共识是共识安全中需要保证的最基本特性。

最终共识是不同节点在共同约定的协议的保障下，整个系统对某些操作行为产生的结果的一致认同。在区块链系统中，满足最终共识要求在数据达成共识并存储到区块链后无法被更改。也就是说，所有节点的最终共识只有在主链上达成才能对各类攻击者行之有效，因为只有在主链上形成共识，攻击者就无法通过在分叉链上达成共识、抛弃主链来实施攻击。激励兼容性和活跃性主要是指在区块链网络中，要有足够多的节点持续地参与到区块链系统的维护过程中，这需要共识协议能够提供持续可靠的激励机制吸引节点参与。如果攻击者可以通过某种方式破坏共识协议的激励机制，这就会影响正常用户参与使用或维护区块链的积极性，从而在一定程度上降低区块链的活跃性。正确性要求共识协议能够抵抗双重支付攻击。虽然理论上需要达到 50％以上的算力才能控制区块链网络实现双重支付，但是在实际的网络环境中，攻击者通过使用一些如自私挖矿之类的攻击策略，在一定周期之后，可以将全网的算力往自己设定的这条主链上来运行，使得原始的这条链被废弃，已产生的交易转账信息也随之失效。造成双重支付攻击的策略有很多种，本书将在第 8 章中进一步描述。

5.2.3　智能合约安全

智能合约能够支持用户编写任意的代码逻辑，一旦部署之后，区块链网络中的任意节点都需要执行智能合约上的代码，且代码逻辑不可修改。当输入满足一定的条件后，合约就会自动运行程序，即使智能合约的发布者也无法阻碍程序的自动执行。正因如此，若存在漏洞问题无法通过传统补丁的方式去修改，只能重新部署合约，那么漏洞合约上涉及的金额也无法挽回。近年来，智能合约频繁出现漏洞，导致攻击案例层出不穷，给用户和社会带来了巨大的经济损失。

智能合约主要从软件代码层面来考虑其安全性。软件代码层面的安全由开发安全和运行安全两部分组成，同时，开发安全又包含逻辑安全和代码安全。逻辑安全即指开发人员首先应该在编写之前结合实际功能来设计符合逻辑的、简洁的、具有可行性的代码，因为代码出错的风险与复杂性是相关联的；其次，在代码编写的过程中要严格符合逻辑规范，避免在执行过程中出现规范错误导致异常退出的情况。代码安全即指开发人员在代

码的编写过程中需尽量使用安全且目前较为成熟的开发语言，并且需要确保符合规范，合约和函数可以进行模块化管理，并养成使用安全库的习惯。此外，开发人员要准确地掌握黑客常用的攻击手段，从而在代码的编写过程中尽量避免此类型的攻击，同时了解常见的智能合约漏洞，对编写的合约进行仔细地排查，保证编译后的代码不存在这些漏洞。

运行安全作为一种安全保护机制，它能够随时保持更新，是对智能合约在实际虚拟机平台或系统中运行的安全保护。运行安全的基础是保持更新，即当有新的漏洞被发现时，要及时检查部署智能合约是否受到影响。当用到的库或者工具有更新时，智能合约也要及时更新，并使用最新的安全技术。若智能合约的漏洞问题、甚至被攻击者攻击出现在执行过程中，运行安全的要求是不会对本地参与区块链的系统或设备造成影响，这就需要做到隔离运行，即智能合约并不运行在本地系统上，而是运行在系统的隔离环境中，如系统虚拟机等，这样在很大程度上避免了本地支持智能合约运行的系统遭受恶意者的攻击。例如，以太坊为了实现代码在隔离环境中运行，专门提供了虚拟机供合约代码运行。同时运行安全也要求即使智能合约调用了有漏洞的合约，也不会执行异常。为了实现这个目标，需要确保智能合约在开发中尽量保证模块化，即合约逻辑简单化、代码函数模块化，且需要降低模块之间的依赖性，高耦合低内聚。使得智能合约能够通过接口的方式进行安全调用，并且达到阻止异常结果通过合约调用技术方式扩散到整个区块链的目的，在一定程度上有效地确保了智能合约的安全性和可用性。良好的模块化能够降低智能合约的复杂性，使得智能合约的设计、调试和维护简单化。

5.2.4 内容安全

内容安全是对数据内容本身的规范性要求，它建立在数据安全的基础之上，主要描述的是存储在区块链分布式系统中的数据要达到法律法规的要求和符合用户道德规范的标准，阻止和避免不合要求的内容在网络中传播。那么要如何解决有关内容安全的问题呢？主要的解决方式是有效控制不良信息在区块链上的传播和加强对信息的管理，探索对链上违法信息审核与用户隐私保护需求间的平衡，明确区块链开发者、区块链平台运行者、区块链使用者等不同角色的安全责任。

针对区块链内容的攻击的主要形式包括恶意信息攻击和资源滥用攻击。其中，恶意信息攻击是影响区块链内容安全的主要攻击形式，它指的是攻击者刻意向区块链中写入恐怖信息、虚假信息等。这些恶意信息利用区块链数据传播速度快、达成共识后不可修改等特性，可以很快传播到全世界，造成极大的危害。区块链中的恶意信息使得区块链会被杀毒软件结束正常运行，或者引起政治敏感等问题。资源滥用攻击指的是节点之间恶意频繁交互使得区块的数据量大幅度不可控制地增长，导致普通节点由于存储不足无法容纳区块数据。这就致使可以维护区块链稳定运行以及达成主链数据共识的可靠节点逐渐减少，从而区块链掌握在少数有计算资源、存储资源的大公司手中，从资源的存储和掌握情况可以看出这与区块链的去中心化的特性不相符合。以以太坊的资源滥用攻击为例，2017 年 2 月，攻击者利用大数量级别的垃圾交易信息来攻击以太坊 Ropsten 的测试链，通过阻塞网络信道的方式导致区块链系统无法正常工作。

因此，内容安全可控是将区块链系统应用于各个场景的关键。内容安全也影响着政