2020

企业级区块链安全白皮书

北京航空航天大學 BEIHANG UNIVERSITY

中国移动 研究院 China Mobile CMRI

NSFOCUS

北京航空航天大學
BEIHANG UNIVERSITY

关于北京航空航天大学

自 1952 年 10 月建校以来，北京航空航天大学一直是国家重点建设的高校，2017 年北航入选国家“双一流”建设高校名单（A 类），学校突出人才培养中心地位，坚持“把一流学生培养成一流人才”的育人理念，在人才培养中创造知识，在创造知识中培育人才，为中国的航空航天事业和国家建设发展培养了一批领军人物和奠基人才。2017 年 8 月，北航网络空间安全学院正式成立。同年 9 月，北航获批由中央网信办、教育部共同授牌的“一流网络安全学院建设示范项目高校”，成为国内七所示范项目建设高校之一。北航网络空间安全学院在空天信息网络高速数据加密、卫星网络通信系统安全、移动互联网安全、区块链安全、大数据与云计算安全、工业互联网安全等研究领域形成了特色鲜明的研究方向。

中国移动 | 研究院
China Mobile | C M R I

关于中国移动研究院

中国移动研究院成立于 2001 年，是集团公司直属单位。研究院以做“中国移动技术创新的引擎”为愿景，落实国家创新驱动发展战略和公司“大连接”战略，致力于成为公司权威的战略智库，深入开展技术产业引领、现网运营与战略支撑、新型产品和重大平台研发，研究领域覆盖了无线、网络、人工智能、业务、安全、物联网、实验测试、用户与市场、战略研究等。研究院拥有高素质、专业化的干部队伍，高水平、国际化专家研发团队，目前有员工 1120 多人，平均年龄 34 岁，硕士以上超过 90%，拥有首席科学家 3 人和一大批国家级科技专项课题负责人和国际标准化组织领导人。研究院拥有国际一流的试验基地，总面积超过 1 万平方米，包括五个国家级工程实验室、两个国际组织全球测试认证基地，为行业提供了协同创新的平台。

NSFOCUS

关于绿盟科技

绿盟科技集团股份有限公司（以下简称绿盟科技），成立于 2000 年 4 月，总部位于北京。公司于 2014 年 1 月 29 日起在深圳证券交易所创业板上市，证券代码：300369。绿盟科技在国内设有 40 多个分支机构，为政府、运营商、金融、能源、互联网以及教育、医疗等行业用户，提供全线网络安全产品、全方位安全解决方案和体系化安全运营服务。公司在美国硅谷、日本东京、英国伦敦、新加坡设立海外子公司，深入开展全球业务，打造全球网络安全行业的中国品牌。

版权声明

目录

执行摘要 ····· 1
1. 区块链产业发展 ····· 3
1.1 区块链政策推进 ····· 4
1.2 区块链产业分类 ····· 4
1.3 区块链产业预测 ····· 5
2. 企业级区块链介绍 ····· 6
2.1 企业级区块链和联盟链的关系 ····· 7
2.2 企业级区块链的特点 ····· 7
2.3 企业级区块链的应用场景 ····· 8
2.3.1 去中心化金融 ····· 8
2.3.2 物联网应用 ····· 9
2.3.3 能源和工业互联网 ····· 10
2.3.4 司法存证 ····· 11
2.3.5 食品溯源 ····· 11
2.3.6 去中心化身份认证 ····· 12
2.4 企业级区块链的参考架构 ····· 12
2.5 主流企业级区块链平台 ····· 13
2.5.1 Hyperledger ····· 13
2.5.2 Quorum ····· 14
2.5.3 R3 Corda ····· 16
2.5.4 FISCO BCOS ····· 16
2.6 联盟链的关键技术 ····· 18
2.6.1 共识机制 ····· 18
2.6.2 智能合约 ····· 21
2.6.3 数据安全共享与计算 ····· 27
2.6.4 隐私保护 ····· 30
3. 企业级区块链面临的安全风险 ····· 33
3.1 基础层风险 ····· 34
3.2 核心层风险 ····· 34
3.3 服务层和用户层风险 ····· 35
3.4 跨层功能风险 ····· 35
4. 企业相关的区块链安全态势 ····· 36
4.1 区块链漏洞统计 ····· 37
4.2 公开的企业级区块链安全事件和安全研究 ····· 39

目录 CONTENTS

4.3 企业级区块链安全态势分析 40
5. 企业级区块链相关安全技术 41
5.1 密钥管理机制 42
5.2 参与者身份管理 42
5.3 监管 42
5.4 隐私保护 42
5.5 防双花 43
6. 企业级区块链安全治理 44
6.1 政策监管 45
6.2 数据治理 45
6.3 智能合约治理 46
7. 企业级区块链安全解决方案 48
7.1 基础层安全 49
7.1.1 容器安全 49
7.1.2 网络安全 50
7.1.3 密钥安全 50
7.1.4 终端安全 50
7.2 核心层安全 50
7.2.1 跨链安全 50
7.2.2 智能合约安全 51
7.2.3 隐私保护 52
7.2.4 数据治理 52
7.3 用户和服务层安全 52
7.3.1 Web 安全 52
7.3.2 业务安全 53
7.3.3 API 安全 53
7.3.4 认证和身份管理 53
7.4 全生命周期安全 54
7.4.1 开发交付 54
7.4.2 安全防护 54
7.4.3 异常检测 54
7.4.4 响应恢复 55
7.4.5 安全服务 55
8. 结语 57
参考文献 59

执行摘要

区块链（Blockchain）技术自 2008 年问世，至今已有 12 年之久，从最初的加密货币比特币（区块链 1.0），发展到当前火热的基于智能合约的去中心化应用（区块链 2.0），乃至现在各行各业在讨论各自垂直领域的泛区块链应用（区块链 3.0），发展受到监管和外部环境变化有起有伏，但总体方向是前进的。

可以预见，区块链应用借助其天然的数据不可篡改、去中心化、可取证可溯源等特性，必将超越最初金融经济领域的应用，会在政府交通、文化健康、数字金融、智能制造、供应链管理、数字身份等领域发挥更大的作用。区块链技术可构建去中心化的可信数据交换的业务模式，减少因缺乏信任而损失社会成本、经济成本和时间成本，提高多方参与的系统性运转效率。

2019 年 10 月，习总书记在中央政治局第十八次集体学习时强调，把区块链作为核心技术自主创新重要突破口，加快推动区块链技术和产业创新发展。习总书记的这番讲话，将区块链技术放到了新的战略高度，预计越来越多的企业将在其业务中使用区块链技术，与此同时，企业级区块链面临严峻的安全问题。借着这个契机，绿盟科技、北京航空航天大学、中国移动研究院联合推出《企业级区块链安全白皮书》，旨在对企业级的区块链的概念、架构、技术、安全等进行一个全面的介绍，使读者对企业级区块链相关的内容有一个较为深入的了解。

本白皮书的主要观点如下：

- 加快推动区块链技术和产业创新发展，探索“区块链 +”模式

2020 年 1 月，国务院办公厅发布《关于支持国家级新区深化改革创新加快推动高质量发展的指导意见》。该意见指出，加快推动区块链技术和产业创新发展，探索“区块链 +”模式，促进区块链和实体经济深度融合。

- 智能合约不是“完美合约”，安全问题需警惕

从区块链自身的漏洞和安全事件来看，企业级区块链应用还在早期，但随着区块链应用的普及，相关的公开漏洞会越来越多。可以预测大部分漏洞会来自智能合约，特别是不安全的函数、越界等常规安全问题。

- 区块链两大安全威胁：勒索病毒、挖矿木马

执行摘要

在与区块链相关的企业安全事件中，勒索软件和恶意挖矿是企业面临的两大安全威胁。匿名货币或加密货币变现的便利性，使得这类恶意攻击会持续一段时间。当然，货币的汇率变化，也会在一定程度上影响这类攻击的态势。

- 区块链步入监管时代

由于区块链存在不可删除、事后取证等特性，其合规性要求必然与其它信息服务不同。虽然我国区块链信息服务的监管尚处探索阶段，但国家互联网信息办公室先后发布了三期境内区块链信息服务名称及备案编号，预计后期会持续推进。

- 合规是区块链未来唯一出路

随着《网络安全法》等法律的颁布，个人数据的收集、管理、交换都受到了合规性的约束。无论区块链如何应用，都不应该触碰法律的红线。区块链离不开合规，如何能让区块链更加安全、规范是我们要做的事情。

- 区块链下一个风口：解决区块链上的隐私保护问题

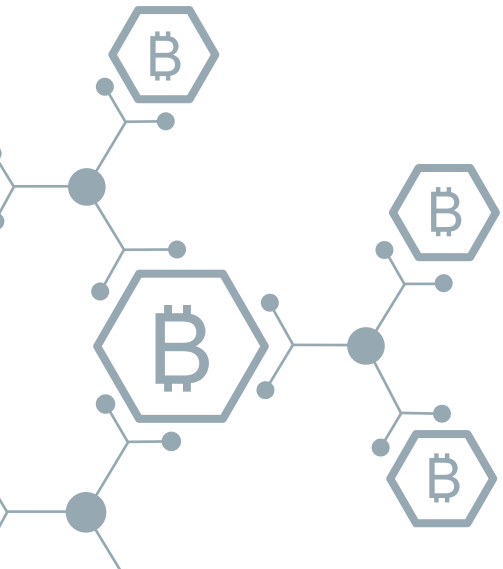
为了解决区块链上的隐私保护问题，近年来新技术、新机制不断涌现。其中新机制包括通道机制、私有交易、加密授权访问机制等；以及结合前沿密码理论的创新，包括零知识证明、环签名、安全多方计算等。

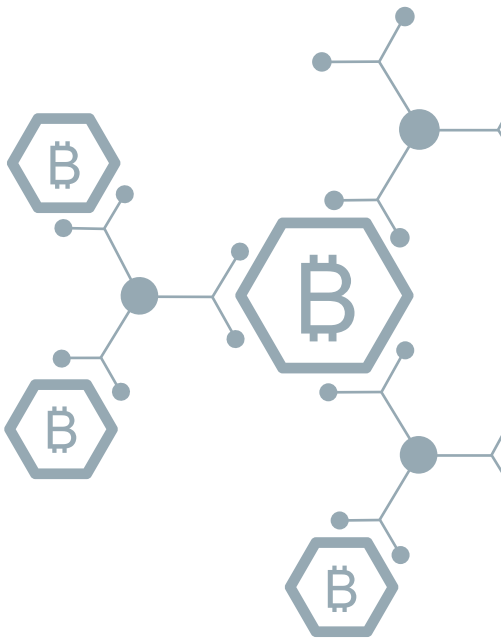
- 区块链，向“安全”而生方能终遇美好

安全厂商、高校与区块链服务商、用户应紧密合作，推动企业级区块链安全生态的构建。区块链的出现，大大提升了安全在企业中的地位。传统的“先推动业务的高速发展，再进行安全建设”模式将不再可行，安全成为区块链的刚性需求。

1

区块链产业发展





区块链技术 [1] 是利用块链式数据结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学方式保证数据传输和访问的安全、利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算范式。自区块链技术发布以来，区块链产业历经多次起伏，可预计未来几年内会加速发展。

1.1 区块链政策推进

2019 年 10 月，习总书记在中央政治局第十八次集体学习时强调，把区块链作为核心技术自主创新重要突破口，加快推动区块链技术和产业创新发展 [2] 。习总书记的这番讲话，将区块链技术放到了新的战略高度。从当前各大政府单位、主管机构和大企业 的反应来看，区块链相关的投资力度会变大。

同时，习总书记强调，要加强对区块链技术的引导和规范，加强对区块链安全风险的研究和分析，密切跟踪发展动态，积极探索发展规律。要探索建立适应区块链技术机制的安全保障体系，引导和推动区块链开发者、平台运营者加强行业自律、落实安全责任。要把依法治网落实到区块链管理中，推动区块链安全有序发展。可见区块链安全同样值得我们关注，保证区块链平台及应用的安全，也是推动区块链应用落地的重要因素。

2020 年 1 月 17 日，国务院办公厅发布关于支持国家级新区深化改革创新加快推动高质量发展的指导意见 [5] 。意见指出，加快推动区块链技术和产业创新发展，探索“区块链 +”模式，促进区块链和实体经济深度融合。各省市也对区块链非常重视，至少 22 个省份将区块链写入了政府工作报告中。以北京为例，北京的政府工作报告中提到，在科创方面，将强化对区块链的关键核心技术攻关；在营商方面，建立以区块链技术为支撑的政务信息资源共享和业务协同机制，开展“秒批”“无感审批”等智能场景应用，实现更多事项全程网办、1000 项事项移动端办理。

1.2 区块链产业分类

一般认为，区块链系统可分为公有链、联盟链和私有链，每种链技术有不同应用场景。

公有链中没有官方管理机构，也没有中心化服务器，各个节点可以自由加入和退出网络，运行时以扁平的拓扑结构互联互通，节点间基于共识机制开展工作。常见的公有链有比特币、以太坊、EOS 等，通常应用在加密货币等领域，这也是区块链产业最初兴起的领域。

私有链的各个节点的写入权限收归内部控制，而读取权限可视需求有选择性地对外开放。私有链仍然具备区块链多节点运行的通用结构，适用于特定机构的内部数据管理与审计。通常建立在特定机构内部，系统的运作规则根据该机构要求进行设定。可以认为私有链是一个健壮、可取证的内部分布式系统，可作为现有企业内部系统的去中心化的演进版本。

联盟链介于公有链和私有链之间，各个节点通常有与之对应的实体组织机构，通过授权后才能加入与退出网络。各组织机构组成利益相关的联盟，共同维护区块链的健康运转。常见的联盟链有 Hyperledger、Quorum、R3 Corda 等。联盟链继承了区块链固有的去中心化特性，又引入了有限中心化管理提升了整个系统的可运营性，可广泛应用于金融、物流、能源等企业级领域。

1.3 区块链产业预测

多家研究机构的研究表明，产业区块链在 2020 年可能迎来拐点。阿里巴巴达摩院发布的十大科技趋势 [3] 中预测提到，2020 年企业应用区块链技术的门槛将进一步降低，专为区块链设计的端、云、链各类固化核心算法的硬件芯片等也将应运而生，日活千万的区块链应用将走入大众。在腾讯研究院发布的《产业互联网 2019 回顾与 2020 展望报告》[4] 中，腾讯提及产业变革的 11 组关键词。其中包含“2020: 区块链与产业场景融合，有望大规模落地”。在这些报告的背后，蚂蚁金服、腾讯云、华为云等云服务商也不约而同地推出了各自的区块链即服务，帮助客户以较小的成本部署区块链应用，助力整个区块链产业的前进。IDC 预测，而在企业 IT 投入中，到 2023 年，中国企业将在区块链服务（咨询、实施、维护、支持等）上投入 27 亿美元，占企业管理服务支出的 29%。

Gartner 预测 [62]，到 2022 年，会有 10 亿人的信息存放在区块链上，尽管人们对此一无所知；到 2024 年，企业会使用区块链技术防护 30% 的敏感数据。此外，IDC 在 2020 年发布的《IDC FutureScape：2020 全球区块链市场预测——中国启示》[61] 报告中预测，到 2023 年，中国 40% 的一线金融机构将绕过 SWIFT 和中央银行基础设施，使用区块链网络处理点对点的跨境支付；到 2024 年，中国 85% 的集装箱运输将由区块链跟踪，其中的一半将使用区块链支持的跨境支付。

由 1.2 可知，上述预测中的金融、物流、身份认证等产业的区块链相关应用和基础架构大多是基于联盟链的，所以本文将主要围绕联盟链对企业级区块链应用进行介绍。

2

企业级区块链介绍

本章首先介绍企业级区块链的特点、应用场景和架构，然后列举了 4 个主流的企业级区块链系统，最后介绍了相关的关键技术。

2.1 企业级区块链和联盟链的关系

企业级区块链（Enterprise Blockchain）是指多个机构遵循统一的认证体系、共识机制、智能合约规范，将各自的同构或异构的区块链数据、系统和业务进行标准化对接，最终形成面向某领域的区块链应用。

企业级区块链是一种概念层面的术语，指定了其应用范围在企业级应用。但其必须使用某种区块链平台作为支撑技术。目前我们观察到大多数的企业级区块链采用了联盟链技术，所以本章以联盟链为基础进行介绍。本章及以下章节中，“联盟链”和“企业级区块链”可互换。

2.2 企业级区块链的特点

企业级区块链通常应用在多个机构间共享数据，或运行彼此认可的程序，所以与公有链存在大量无需注册的节点不同，企业级区块链的参与方是有限的、经过认证的；企业级区块链与私有链也不同，其节点是对等的，不存在单一的、拥有很高权限的管理方。

此外，企业级区块链是面向特定场景的特定应用，与公有链有很多差别，总体而言有如下特点：

1. **身份鉴别**。联盟链中的所有参与者都有可被唯一识别的身份。参与者只有有了唯一的身份，才能被确认权限。
2. **接入许可**。联盟链中的节点是许可制的。节点在满足一定的访问控制约束时，才能被接入联盟链的网络，所以联盟链也被认为是许可链（Permissioned Blockchain）。
3. **高吞吐**。在某些高频交易（如金融领域）应用中，联盟链需要较高的交易吞吐量，以支撑大规模的应用。
4. **低延迟**。在公有链，如比特币中，需要六个区块生成才能确认交易的时延就不满足很多联盟链应用的需要，这样的时延是无法满足快速交易的要求。联盟链通过身份鉴别和接入许可，假定了对等节点有一定的可信度，通过降低共识算法的强度来缩短达成共识的时间，从而具备较低的时延。

5. **机密和隐私性**。联盟链应提供确保业务交易的机密性和隐私性的能力。比如在供应链网络中，不同用户的价格有可能不同，如果每一个参与方都可以看到合约和交易的内容，那么则很难实现定价的差异化。所以，一些联盟链有通道（channel）的设计，为不同交易方提供对应的机密性和隐私保护。

2.3 企业级区块链的应用场景

如前所述，企业级区块链具有节点有限、认证、对等的特点，非常适合无中心、多方合作的企业级应用，应用场景广泛，本节选取一些典型场景进行介绍。

2.3.1 去中心化金融

去中心化金融 （DeFi） 是 2019 年区块链领域中最受关注的话题之一[12] 。与传统金融相比，去中心化金融通过区块链技术实现了去中介化，减少了中间人角色，从而降低了中间环节所带来的巨额成本。据 Consensys 报告，有 100 多个前沿的区块链项目在去中心化金融领域进行着开创性的工作。很多金融场景都可以将区块链技术与金融科技进行结合，比如，供应链金融、贸易金融（信用证、保函、福费廷、保理、票据）、征信、交易清算、积分共享、保险、证券等[13]。

2020 年 2 月 5 日，中国人民银行正式发布《金融分布式账本技术安全规范》（JR/T 0184—2020）[14] 。标准规定了金融分布式账本技术的安全体系，包括基础硬件、基础软件、密码算法、节点通信、账本数据、共识协议、智能合约、身份管理、隐私保护、监管支撑、运维要求和治理机制等方面。标准适用于在金融领域从事分布式账本系统建设或服务运营的机构。标准有助于金融机构按照合适的安全要求进行系统部署和维护，避免出现安全短板，为分布式账本技术大规模应用提供业务保障能力和信息安全风险约束能力，对产业应用形成良性的促进作用。

此外，去中心化的征信体系也是区块链在金融领域很好的企业级应用，多家征信机构可组成联盟链，将各自的征信信息彼此共享，很好的达到彼此信息互补的效果，且所有的信报都有据可查，值得信赖。这种有限信息共享的模式，一方面为金融机构提供了更全面的征信信息，有助于规避风险，提高风控水平，另一方面也利于中小企业降低融资成本，提升经济活力。

2.3.2 物联网应用

物联网应用具有海量设备，同时可能会对接支付系统，所以区块链在身份认证、原产地跟踪、数据存储等方面具有优势，物联网也经常被认为是区块链的一个典型应用场景。例如 Filament[15] 用区块链跟踪车的位置、保存交易信息等。

基于物联网设备的区块链应用目前还很不成熟，面临诸多挑战。例如，如果由物联网设备构建区块链，物联网终端算力和存储能力不足，无法支撑计算密集型和高能耗的工作量证明共识机制；此外，区块链交易频率容易受物联网规模制约。当然从长期看，物联网区块链应用可能会出现创新的设备和商业模式，但需要 5-10 年成熟。

而当前的物联网产业看，如果把区块链放于物联网应用的云端，而物联网设备不做改变，这种模式与普通区块链应用差别不大，但相对成熟。一个典型场景是供应链监控，可将所有的零件、零件变更上链，从而做到每项可回朔。例如沃尔玛通过区块链实现食品可溯源 [16]，提高供应链的透明度。

在国内，2019 年 6 月 28 日，在 MWC 2019 上海展期间，移远通信和广和通分别发布了集成摩联科技 BoAT SDK 5G 区块链模组，支持 5G 独立组网（SA）和非独立组网（NSA）两种模式，支持支持物联网设备的可信链上身份管理、数字签名和数据上链 [17]。10 月 25 日，海尔云裳物联与趣链科技联合成立的甘道智能，发布了首款自主研发区块链通信控制模组“物链 1 号”[18]，该模组除了具备物联网感知功能外，还集成了区块链操作系统。此外，该模组通过可信数据采集，保证了区块链最后一公里的可信。

前述三厂商的模组主要功能是通信，SDK 也好、区块链操作系统也罢，只是与云端区块链平台对接的客户端，数据还是存放在云端的联盟链中，如果攻击者通过修改硬件或底层操作系统的方式修改数据，容易造成局部数据错误。考虑到这种威胁，硬件提供商应通过可信（如 TEE）方式设计硬件模组，从而确保整个区块链应用的可信。

图 2.1 物链一号

2.3.3 能源和工业互联网

目前国内的能源企业都高度关注区块链技术及其落地的场景，国家电网成立了区块链公司，各省的研究院也在积极推进区块链在电网各个应用场景的落地。虽然这类区块链应用看似是在一个企业内部构建私有链，意义不大，但从实践上看，这类大国企的分公司和子部门间的数据仓库、IT 系统存在巨大的沟壑，如果要做统一的电费统计、电力交易、共享数据研究、电商财务等应用，其需要的治理数据的难度不亚于传统多个机构间的数据共享。通过构建基于联盟链的中间件，不同的分公司、子部门间可共享各自业务系统的数据，有助于打破传统的数据壁垒。

此外，工业互联网的核心是将工厂、客户、零部件供应商、经销商等主体的业务连接起来，区块链作为去中心化的数据存储和交易平台，天然地可以赋能工业互联网，保证多方进行可信的交易，打通工业生产的每个环节。

2.3.4 司法存证

随着信息化的发展，越来越多的证据将会以电子数据的形式出现，而与传统的实物类证据相比，电子证据的真实性、合法性和关联性的司法认定难度很大。由于区块链技术本身具有不可篡改、全程可追溯、多方参与等特性，与电子数据存证的需求天然契合，因此，区块链可以为整个链上电子数据的真实性提供可靠的保障，实现电子数据全链路可信、全节点见证、全流程留痕，有效解决诉讼中存证难、取证难、认证难等问题。

2020 年 1 月 18 日，全国高级法院院长会议在北京召开，会议指出要以建设“人民法院司法区块链统一平台”为重点，加快推进区块链技术攻关和应用场景落地，形成全国统一的人民法院区块链应用体系 [19]。

2018 年至今，北京互联网法院全面调研互联网审判模式的特点与需求，坚持中立、开放、安全、可控的建设理念，构建主动存证与跨链接入相结合的天平链电子证据存证平台 [20]，着力解决电子证据存证、上链证据在线勘验问题。“天平链”的设立，意味着北京互联网法院在区块链技术服务司法审判、与司法业务深度融合、提高审判质效中迈出了第一步，完成了区块链司法 1.0 的构建与应用。目前，“天平链”已完成跨链接入区块链节点 18 个，已完成版权、著作权、互联网金融等 9 类 25 个应用节点数据对接，上链电子数据超过 900 万条，跨链存证数据量已达上亿条。

2.3.5 食品溯源

国内外食品安全事故频发，食品安全是与我们每个人的生命安全都息息相关的问题。食品安全事件频繁发生的根本原因在于政府、企业、销售商和最终消费者之间的信息不透明、不对称。而且，全国乃至全球食品产业链，包括种植、生产、运输、存储、销售等环节都是采取不同的记账方式，标准化程度很低，这也就造成了食品的全球可追溯性非常差。

区块链溯源场景应用中，可以将商品从原料生产到销售的全过程信息流记录上链，并加盖时间戳，精确到一物一码。同时对数据进行加密存储，利用分布式账本，提高数据造假成本，保障数据真实。消费者可以查看到记录在链上的商品完整信息，解决信任问题。

针对原始数据的真实性问题，众安公司 [21] 在养鸡场大量铺设物联传感设备，并为每一只鸡都佩戴了物联网身份证——鸡牌。通过自动收集鸡的位置、运动数据以及养殖场的温度、空气湿度、污染物指

标、土壤指标等数据，并实时上传到区块链当中，确保数据在上链过程中不被人为篡改。

2.3.6 去中心化身份认证

传统的身份认证管理系统（IAM）是中心化的，权威机构 CA 为用户颁发证书，并撤销过期或不安全的证书。但这种 PKI 体系依赖于集中式的 CA，存在一定可用性的风险。此外，集中式 CA 也可能存在作恶的风险，是否信任 CA 颁发的证书也是一个存在的问题。

通过去区块链构建去中心化的身份认证系统，可将身份信息、证书信息和 CRL 放置于区块链的每个节点上，每个节点都可进行证书校验，并不需要依赖于某个集中 CA 的权威性；而且该过程不需要借助其他节点，也具有较好的实时性和可用性。此外，区块链的不可篡改特性，使得证书签发、撤销的记录都能被查询到，消除了 CA 作恶的风险。

当前，IBM 有 Verify Credentials 产品 [22]，但 Gartner 认为是概念验证阶段，成熟度还需要验证。

2.4 企业级区块链的参考架构

区块链作为多种支撑技术的组合，最终是一种层次化的架构。一些基于公有链开发的区块链新技术，随着时间迁移，也逐渐集成到联盟链和私有链系统中。因此，公有链、私有链和联盟链在技术栈上大体是一致的，但联盟链和私有链比公有链有更多控制和管理方面的组件，如认证和身份管理、监管和审计等。

中国区块链技术和产业发展论坛（CBD-Forum）在 2017 年给出的区块链参考架构 [6]，同样可以作为联盟链的参考架构，参见图 2.2 。

其中，基础层提供了区块链系统正常运行所需要的组件，包括存储、计算、P2P 对等网络等。

核心层是区块链的核心部分，包括共识机制、智能合约、密码学支持相关功能、账本记录等。

服务层通过调用核心层的功能组件，为用户层提供接入服务，包括接入管理、节点管理和账本应用。

用户层是提供给用户的服务功能，包括用户功能、业务功能和管理功能。

以上可以认为是通用的区块链架构，但联盟链为了达到可管理的目的，还应包含开发管理、运营、安全、监管和审计等方面，这些组件则融入到前述区块链技术栈的多个层面。例如，

开发功能提供了区块链开发所需的组件，包括 IDE、测试、构建等管理功能。

运营功能提供了区块链系统管理所需的组件，包括策略管理、异常和问题管理等功能。

安全功能用于用户和节点的认证，通信的加密，交易的加密，数据的访问控制等安全功能，包括认证和身份管理、授权和安全策略管理、隐私保护等组件。

实时监管和事后审计也是联盟链必不可少的，在应用中需要使其满足特定行业的监管需求。

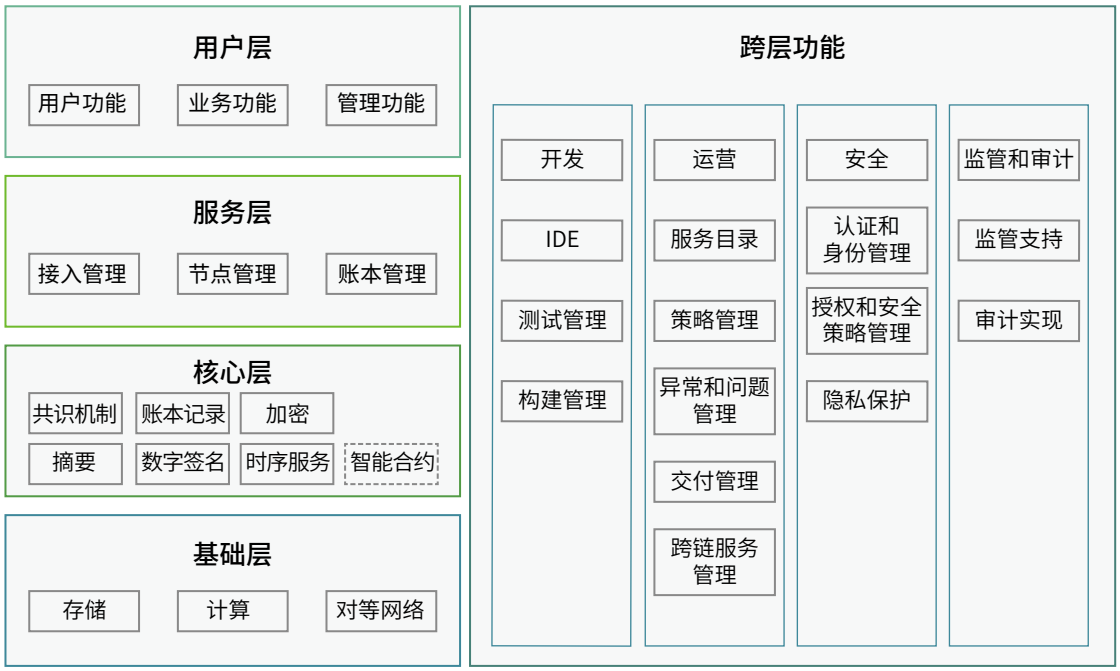


图 2.2 联盟链参考架构

2.5 主流企业级区块链平台

目前主流的企业级区块链平台有如 Hyperledger、Quorum、R3 Corda、FISCO BCOS 等，本节对上述平台做简要介绍。

2.5.1 Hyperledger

2015 年 12 月 Linux 基金会成立 Hyperledger project[7]。这个项目的目的是要共同建立并维系一个

跨产业的、开放的、分布式账本技术平台和标准，让任何数字化的价值交换，如房地产契约、能源交易、结婚证明等，都可以被透过具经济成本效益且安全的方式进行交易及追踪。该项目包括 Blockchain Explorer、Fabric、Sawtooth Lake 等多个项目。其中 Fabric 作为开发区块链应用或方案的基础，是 Hyperledger 最核心的项目。

Hyperledger Fabric 是一个开源的企业级许可分布式账本技术平台，专为在企业环境中使用而设计，具有高度模块化和可配置的架构，支持可插拔的共识、可插拔的身份管理协议（如 LDAP 或 OpenID Connect）、密钥管理协议和加密库；支持通用编程语言编写智能合约（如 Java、Go 和 Node.js），利用不需要原生加密货币的共识协议来激励昂贵的挖矿或推动智能合约执行。Fabric 平台也是许可的，许可区块链在一组已知的、已识别的且经常经过审查的参与者中操作区块链，参与者在产生一定程度信任的治理模型下运作。平台遵循执行 - 排序 - 验证架构，

这些差异化设计特性的结合使 Fabric 成为当今交易处理和交易确认延迟方面性能较好的平台之一，并且它实现了交易的隐私和保密以及智能合约（Fabric 称之为“链码”）。

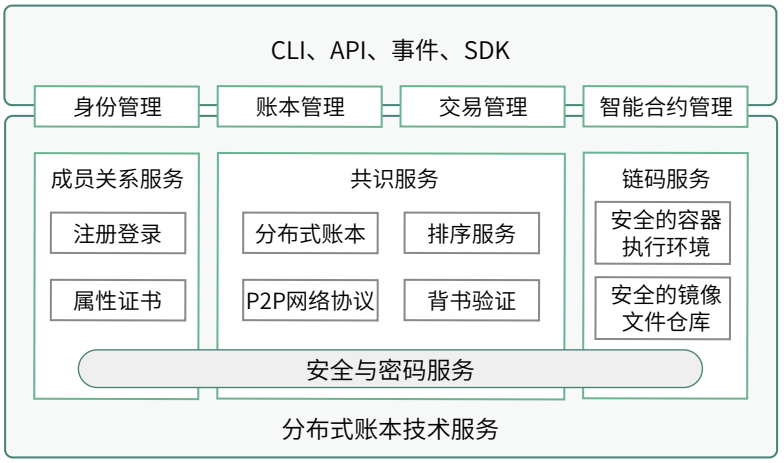


图 2.3 Hyperledger Fabric 架构图

2.5.2 Quorum

Quorum[8] 是一个由摩根大通推出的企业级分布式账本和智能合约平台，主要是为了解决区块链技术在金融及其他行业应用的特殊挑战而设计，适用于需要高速交易以及高吞吐量处理联盟间进行私有交

易的应用场景。Quorum 是基于以太坊分布式账本协议开发而成，因此被看作企业版的以太坊，相比于公有链以太坊，Quorum 提供了交易和合约的私有化功能，支持多种共识方式，提供网络与节点的权限管理功能，并且具有更高的性能，因而被认为是联盟链。

Quorum 的架构如图 2.4 所示，主要分为底层的区块链层和上层的业务逻辑层。

其中，区块链层主要包括三个组件：

Quorum Node：基于以太坊的 Quorum 节点，由于存储交易。

Constellation – Transaction Manager：用于交易的管理。

Constellation – Enclave：用于对交易信息进行加解密。

业务逻辑层使用区块链层提供的功能实现传统应用到区块链系统的移植，主要包括三个组件：

Smart Contracts：智能合约组件。

DApps：去中心化应用组件。

Legacy app integration：与已有非区块链应用集成的组件。

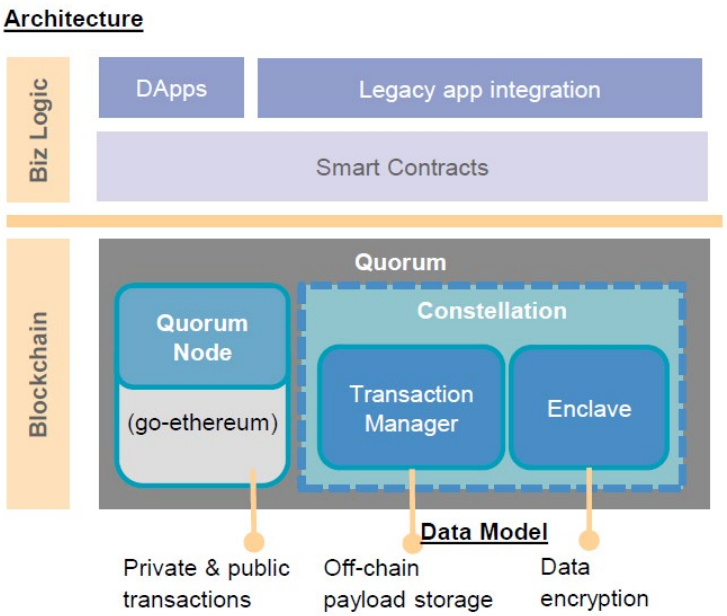


图 2.4 Quorum 架构图

2.5.3 R3 Corda

Corda[9] 是 R3 联盟推出的分布式账本平台。R3 联盟成立于 2014 年，目前已经有 300 多家联盟成员。最初的 R3 联盟成员由多家银行组成，目标是探索区块链技术在全球私有网络中实时执行金融交易的可能性。而现在的 R3 联盟，已经不止关注于金融场景，能源、医疗、供应链等各种能够应用区块链的场景亦有涉及。

Corda[10] 平台尤其适用于受监管的金融机构。它很大程度上是受到区块链系统的启发，但又摒弃了很多不适合金融场景的传统区块链设计选择。比如，与比特币、以太坊等典型区块链平台相比，Corda 舍弃了所有节点都要验证和记录每一笔交易的账本全网广播模式，仅仅要求每一笔交易的参与方对交易进行验证和记录，从而极大地提高了交易的吞吐能力；且解决了共享账本能否保证交易数据私密的争议，促进分布式账本技术在商业化应用落地。

Corda 提供了一个运行智能合约的框架，具备以下关键行为和特点：

- 通过基于现有合法框架并与现有和新兴法案兼容的方式，记录和管理
- 两个及以上可识别参与方的金融协议和其它共享数据的变化。
- 去中心化控制的公司间工作流设计；
- 在个人交易层面而非全局系统层面上，支持企业间达成共识；
- 支持纳入监管以及监督性质观察者节点；
- 仅在交易参与方之间验证交易的有效性；
- 支持多种共识机制；
- 记录自然语言法律文书与智能合约代码之间的显性关联；
- 使用符合产业标准的工具；
- 严格控制数据访问权，仅对有明确授权或逻辑上有权访问的用户开放。

2.5.4 FISCO BCOS

FISCO BCOS[11] 是由国内企业主导研发、对外开源、安全可控的企业级金融联盟链底层平台，由金

融区块链合作联盟（深圳）（简称：金链盟）成立的开源工作组协作打造，于 2017 年 12 月正式对外开源。

截止 2019 年 6 月，FISCO BCOS 开源生态圈已涵括 400 多家企业机构、逾 6000 名社区成员，并且仍在与日俱增中。基于 FISCO BCOS 搭建的应用有数百个，投产上线的有数十个，覆盖范围包括以交易清结算、供应链金融、数据存证、征信、场外市场等为代表的金融应用领域，以及司法仲裁、文化版权、娱乐游戏、社会管理、政务服务等其他行业应用领域，并且涌现出人民网人民版权平台、中国澳门智慧城市建设等重磅应用。

FISCO BCOS 分层架构设计如图 2.5 所示，共分为四层。

- 基础层提供基础工具和算法库。
- 核心层实现区块链内核逻辑以及网络共识算法等关键模块，包括链核心层与互联核心层。

链核心层实现区块链的链式数据结构、交易执行引擎和存储驱动。

互联核心层实现区块链的基础 P2P 网络通信、共识机制和区块同步机制。

- 管理层实现区块链的管理功能，包括参数配置、账本管理和 AMOP 等。
- 接口层面向区块链用户，提供多种协议的 RPC 接口、SDK 和交互式控制台。

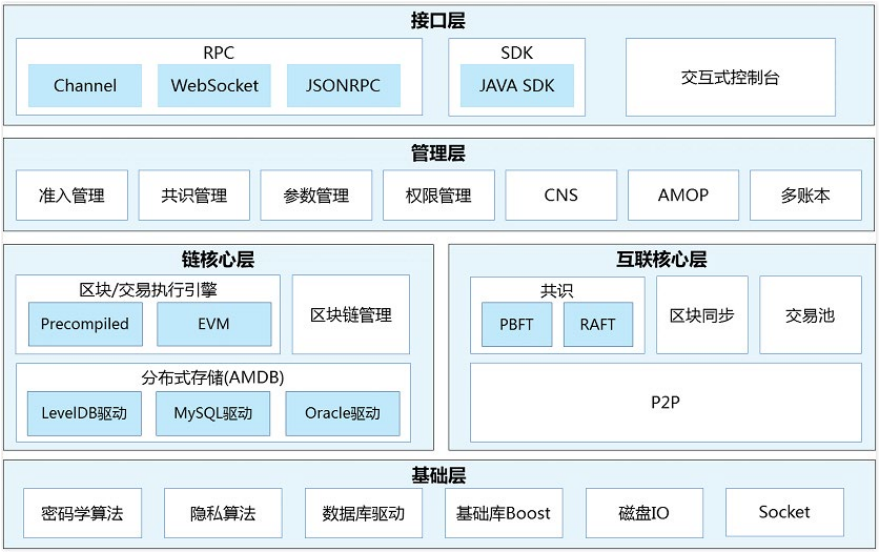


图 2.5 FISCO BCOS 架构图

2.6 联盟链的关键技术

联盟链的架构中包含了很多组件，大部分使用现有成熟的技术，如密码学算法、数据库、P2P 网络等，但也包含了支撑联盟链技术栈的关键技术，例如共识机制、智能合约，以及多种隐私保护技术，本节就上述关键技术做简要介绍。

2.6.1 共识机制

在分布式计算和多代理系统中，即便存在故障节点，最终也能达到全系统可靠性，就需要节点通过某种机制达成一致，该机制称为共识机制（Consensus）。我们整理了近年来区块链相关的共识机制，列举如下。

2.6.1.1 经典分布式共识

经典分布式共识机制是指在授权网络中，使得一组节点能够实现状态机复制的机制。它主要面向一些分布式数据库系统，像 Paxos 算法主要针对网络中可能出现的崩溃节点而设计，而 PBFT 则能够容忍一定的拜占庭错误节点。根据网络模型假设，可以将经典分布式共识机制分为以下三类：

1. 部分同步网络分布式一致算法，部分同步网络模型是经典分布式共识和区块链共识机制最常用的模型；
2. 异步网络分布式一致算法，异步网络模型也是共识研究中经常采用的模型，在完全异步网络中实现共识通常需要随机数发生器来完成；
3. 同步网络分布式一致算法，同步网络模型假设较强，通常无法直接在实际中使用。

2.6.1.2 授权共识机制

授权共识机制是指在授权网络中，节点首先经过身份认证加入网络中，然后在节点之间运行某种分布式一致性算法，实现状态机复制，对数据达成共识，进而生成和维护授权网络内部的区块链。授权共识机制产生的区块链不同于比特币之类的“公链”，节点只有在获得身份认可之后才能加入授权网络中，进入到授权网络内部，从而完成共识过程。

2.6.1.3 基于工作量证明的共识机制

工作量证明（Proof of Work, PoW）最早被用来防止垃圾邮件，由 Dwork 和 Naor[23] 在 1992 年提出。邮件在被发送之前，必须要求邮件发送方完成一定量的计算 , 如找到某个特定数学难题的解答。Back[24] 在 1997 年提出，并在 2002 年正式发表了 Hashcash，对工作量证明作出了改进，利用单向哈希函数实现工作量证明，即找到哈希函数原像才能完成工作量证明的过程。比特币的出现，将工作量证明运用到非授权网络的共识中，主要用来防止敌手制造假身份发动女巫攻击。

需要说的是 PoW 很好的解决了未知身份的主体间形成共识的问题，主要应用在公有链的场景下，但其缺点是通常会消耗大量的计算资源，联盟链中的节点是彼此认证的，所以一般不需要 PoW 机制。

2.6.1.4 基于权益证明的共识机制

为了解决工作量证明带来的巨大能源消耗问题，基于权益证明的共识机制（Proof of Stake, PoS）被提出。权益是指节点或用户拥有的资产，如代币等，根据用户拥有资产比例决定成为下一个区块生产者的概率，拥有资产比例越高，其成为生产者的概率就越大。

2.6.1.5 单一委员会的混合共识机制

混合共识机制的含义是将经典分布式共识机制与区块链共识机制相结合，即采用 PoW 或 PoS 的方式选举特定的委员会，在委员会内部运行经典分布式共识机制，生成区块。采用单一委员会的混合共识机制选举一个委员会负责全网所有交易的处理，而采用多委员会的混合共识机制选举多个并行运作的委员会，将全网划分为多个片区，分片处理网络中的交易。混合共识机制的一般过程如下：

1. 选举委员会成员。委员会成员通过 PoW 或 PoS 的方式选举，用来防止女巫攻击。采用 PoW 的选举方式需要设定一定的挖矿难度，保证每个时期找到 PoW 的节点数目替换掉委员会内部分节点。采用 PoS 的选举方式，需要在持币者中，根据持币者拥有币数量，随机选取一定数量节点作为委员会新成员。
2. 选举委员会领导者。委员会内部共识的运行需要领导者发起，并且采取一定的机制防止领导者不作为或者发生恶意行为。委员会领导者可以通过随机数或投票的方式选择。
3. 运行委员会内分布式一致性算法。委员会领导者在委员会内部对区块发起共识请求，一般可以

运行类似 PBFT 或其改进协议，实现委员会内部的拜占庭容错，达成分布式一致性共识，进而生成和维护区块链。

4. 广播区块。委员会成员将生成的区块广播至全网，使得网络中非委员会的节点和客户端收到新产生的区块，更新交易和区块链。

5. 重配置委员会。一个委员会工作的时间对应为一个时期，系统应当合理设置每个时期的时间长度，用来防止敌手腐化委员会成员。在一个时期过后，委员会开始重配置过程，按照一定的方式替换原本的委员会，然后新委员会接任下个时期的工作。委员会的更新方式一般有滑窗式、随机更新等方式，随机更新是指新找到被 PoW 或 PoS 算法选中的节点成为委员会新的成员，替换原委员会中的部分成员，进入新时期。

2.6.1.6 多委员会的混合共识机制

为了解决区块链处理交易的可扩展性，利用多个并行的委员会来处理网络中不同分片的交易的混合共识机制被提出，也被称为分片共识 (sharding consensus) 机制。

目前分片有以下几种含义：

1. 通信分片 (communication sharding)

通信分片是指将全网分为不同的片区，每个片区由一个对应的委员会处理，每个委员会内部成员大部分时间只需内部通信，每个片区内部的其他客户端、节点大部分时间可以通过与该分片内委员会通信获得目前区块链的状态。

2. 计算分片 (computation sharding)

计算分片是指每个分片委员会只负责处理其对应的交易，如根据交易的 ID 判断其对应的分片，交易 ID 最末位数字如果是 i，则由 i 号分片委员会处理该交易，对交易运行委员会内分布式一致性算法，验证该交易的合法性，决定该交易是否被添加到区块链中。

计算分片使不同的交易以并行的形式被不同的委员会处理，当网络中节点数量增多时，可以增加更多的委员会，这样不同的交易能够以并行的形式被不同的委员会同时处理，交易处理性能随着网络中节点数量的增多而增加，进而实现了交易处理的可扩展性。

3. 存储分片 (storage sharding)

存储分片是指不同分片委员会将处理后的交易分片存储，每个分片委员会只负责处理本分片对应的交易，将交易放到本分片专属的交易区块链上。交易区块链用于存储本分片产生的交易历史或当前分片的未花费交易池信息。存储分片将整个区块链系统的交易数据或未花费的交易输出 (unspent transaction output, UTXO) 数据分片存储，降低了节点的存储负担。

多委员会混合共识机制流程包括选举委员会成员、委员会成员分配、选举委员会领导者、运行委员会内分布式一致性算法、广播区块和重配置委员会等步骤。以上步骤与单一委员会混合共识机制相类似，但是存在三个关键区别：

① . 增添了委员会成员分配步骤，在选举委员会成员后，需要将新选举的委员会成员分配到不同委员会中，为了防止敌手在此过程中影响成员分配，需要设置合理的分配策略。

② . 在运行委员会内分布式一致性算法步骤中，需要考虑到跨片交易的处理，即当一个交易包含多个输入且其属于不同分片时，需要多个分片协作完成对该交易的处理，防止交易双花攻击。

③ . 在广播区块的步骤中，如果采用存储分片，那么可能每个分片各自生成和广播其区块链，不存在全局的区块链。

2.6.2 智能合约

“智能合约”的概念是由 Szabo[25] 在 1997 年提出来的，其主要描述了一种无需可信第三方即可自动执行的双方或多方协议。但由于当时并没有出现相应的实现方案，这一概念没有受到足够的重视，只能成为当时相关研究者心中的一种美好的幻想和愿望。

利用区块链技术，将有可能实现真正意义上的“智能合约”。

2.6.2.1 智能合约的发展

比特币系统提供了一种脚本语言系统，利用脚本语言，能够实现部分金融交易事务的自动化执行。有研究者利用脚本语言实现了零知识有条件支付（Zero-Knowledge Contingent Payment）的功能 [26]，以确保电子商品的公平交易。然而，比特币系统所提供的脚本语言，是一种非图灵完备的编程语言，其仅适用于简单的金融交易，而不能满足人们对复杂协议自动化执行的进一步需求。

企业级区块链介绍

2013 年，Buterin 等人 [27] [28] 在比特币系统的启发下提出了以太坊（Ethereum）系统，该系统引入了一种新的虚拟机结构，并且支持图灵完备的编程语言，旨在优化比特币系统中原生脚本编写过程中体现出来的复杂性，并使得智能合约的使用场景不再局限于金融交易事务。更具体地来说，该系统中的智能合约能够在理论上支持各种通用的计算机程序的执行。以太坊中底层的虚拟机（Ethereum Virtual Machine, EVM）执行与比特币系统类似的脚本语言（例如，OP_RETURN 等指令），其被称为 EVM bytecode。为了更方便地定义智能合约的运行规则，实际上还存在许多高级编程语言，可以通过编译器将高级语言代码转换为对应的 bytecode。开发者可以使用高级语言对合约内容进行设计，从而提高开发效率。

2016 年，R3 集团 [29] 提出了一种面向金融服务行业的分布式账本平台 Corda，以提升金融服务交易的处理速率，并且降低了交易确认延时。为保护智能合约内容的隐私性，摩根大通公司 [30] 通过在 Ethereum 系统的基础上引入 Private State Trie 以及 Manager 的方法，提出了一种支持私密合约执行的联盟链系统 Quorum，但其执行效率与 Ethereum 系统相仿。2018 年 6 月，Larimer 等人 [31] 主导的 EOS 系统主网正式上线，其采用了更加高速的共识算法，并声称支持智能合约的并行执行，这使得交易处理速度以及合约的执行效率有了进一步提高。

在当前流行的各种智能合约系统中，例如 Ethereum 和 IBM 开发的 Hyperledger[32] 等，智能合约大多被定义为一段部署在区块链上的可自动执行的计算机程序。用户通过向运行这个区块链系统的网络节点发送特定的交易信息，即可触发合约的执行。所有的交易信息都会被被记录在区块链上，从创世区块中的初始状态出发，利用区块链上的所有交易信息，即可推断出任意合约以及用户的账户状态。

正是由于区块链上信息的不可篡改等特性，智能合约执行结果的正确性才得到了保证，进而实现在无可信第三方的情况下多方合约内容的自动且正确的执行。支持智能合约功能的区块链系统的结构简图如图 2.6 所示 [33]。

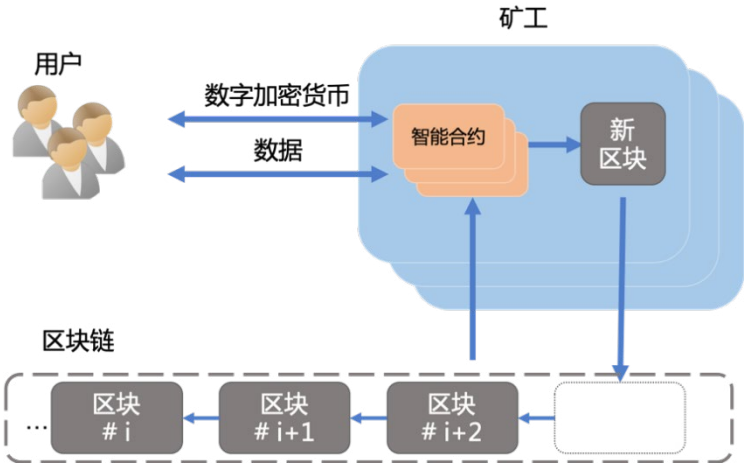


图 2.6 运行智能合约的区块链系统结构简图

2.6.2.2 智能合约安全问题

智能合约引发的安全问题已经成为区块链自身机制安全性的主要影响因素，现列出目前典型的智能合约安全问题。

首先是可重入漏洞（Reentrancy），这是智能合约中最严重的安全问题。若一个程序或子程序可以在任意时刻被中断然后操作系统调度执行另外一段代码，这段代码又调用了该子程序，则称其为可重入的。简单来说是一个函数在执行完成前又被调用了数次，发生意料不到的行为。正是这个问题，2016 年 Ethereum 上的区块链众筹项目 TheDAO[34] 便由于合约漏洞遭到黑客攻击，损失近 6000 万美元，导致了以太坊的硬分叉。此次事件正是结合了 Solidity 语言中 fallback 函数和无限次的递归调用，从而形成了闭环并转移出了大量资金。

其次是危险的 delegatecall 函数，该函数的原型为 address.delegatecall(bytes4(hash),arg)，其中第一个参数为调用函数名哈希值的前四个字节，第二个参数为传入该函数的参数。然而事实上为了灵活性也有一部分的开发人员会使用 msg.data 来直接作为参数，这也就意味着攻击者可以调用合约里的任意 public 属性函数，造成很大的危害。因为滥用 delegatecall 函数，2017 年 7 月和 11 月 Parity 多重签名钱包分别造成约 3000 万美元被盗和 50 万枚以太币被锁定。

然后是无 gas 发送问题，gas 是限制以太坊允许交易消耗的最大计算量的资源。如果在计算过程中

超过了 gas 限制，则会发生以下一系列事件：（1）引发 out of gas 异常而无法交易；（2）函数执行前的合约状态被恢复；（3）全部 gas 作为交易费用还给矿工，不再退还。同时 out of gas 也是未处理的异常（Mishandled Exceptions）安全问题中的一类，若是使用 send 函数转账时出现异常，如果不显式给出异常判定的代码，那么无法捕获异常，这是不安全且不符合逻辑的。有研究表明，大约有 28% 的合约没有去检查 send 函数调用返回值 [35]。

下面是与区块链机制本身相关的智能合约安全问题，如交易顺序依赖问题，一个区块内包含一个交易的集合，同属于一个区块内的交易执行顺序是不确定的，而这取决于矿工的交易选择标准，因此也就导致了区块的状态是不确定的。由此可见，打包在区块中的交易顺序与交易最终执行的顺序可能完全不同，更严重的是，恶意矿工可能会为了个人利益而故意延迟处理某个交易。如时间戳依赖问题，程序中经常会出现产生随机数的功能，而时间戳（Timestamp）能唯一地标识某一刻的时间，通常用来生成随机数，但这并不是安全的。时间戳是打包交易时候由矿工设置的，存在一定的人为操作因素在里面，矿工完全可以对时间戳做轻微的改动，因为这个时间大约能有 900 秒的范围波动。

目前的智能合约应用大多涉及金融交易，因此很容易被黑客和攻击者觊觎。进而，智能合约的编写要求相较于一般编程，对代码的安全性要求更高，这一事实增加了普通使用者自行编写合约的难度，进一步抑制了智能合约在法律、金融、公共服务等业务方面的普及。

2.6.2.3 智能合约的构建范式

为了减少合约编写过程中产生的错误，开发者们通常会参照一些合约构建范式。许多文献都从不同的角度对这些范式进行了归类和总结。

Atzei 等人 [35] [36] 对智能合约上可能受到攻击的脆弱点进行了总结，并针对这些点进行分类，以便在后续的开发或是研究过程中排查漏洞。如针对可重入漏洞，防御方法有三种：（1）不使用 call.value() 函数，而使用更安全的 transfer() 函数，避免执行多余代码；（2）确保在在完成所有内部程序之前不进行外部调用，这种做法被称为 checks-effects-interactions 模式；（3）引入互斥锁，即添加一个在代码执行过程中锁定合约的状态变量，从而来阻止可重入调用。如针对交易顺序依赖问题，可以在代码中设置判定条件，也可以进行代码的形式化验证（Formal Verification and Specification），从而保障交易在合理的环节以正确的逻辑呈现。

Bartoletti 等人 [37] 将智能合约的应用场景进行了分类，并给出了几种常用的合约范式，包括：代币

（Token）、认证（Authorization）、预言机（Oracle）、随机数（Randomness）、投票（Poll）、时间限制（Time constraint）、终止（Termination）、数学计算（Math）、分叉检查（Fork check）等。可以看出，以上的大部分范式都是针对合约构建过程中容易出错的部分提出的。

Solidity 语言的官方文档 [38] 中直接给出了一些关于智能合约编写的提示、要求以及一些被认为是没有漏洞的合约范式。这些官方文档是开发者入门的必读文档，其受到最多的开发者以及黑客人员的验证和审查，因此有理由相信文档中给出的合约是安全的。此外，ConsensysDiligence[39] 也给出了关于以太坊上智能合约编写最佳实践的文档，以供具有一定开发经验的 Solidity 合约开发者参考。

Wohrer 等人还 [40] [41] 从访问控制、认证、合约的生命周期、合约的维护以及合约的安全性等角度，根据目前已有的被广泛认为是安全的合约，分别给出了一些合约的范式。

2.6.2.4 智能合约安全性检验工具

在智能合约出现之前，就已经存在许多针对高级语言代码的安全性检测工具，这些高级语言同样是图灵完备的。因此，在基于图灵完备语言的智能合约出现之后，关于代码安全性检测的研究也扩展到了智能合约代码的领域。

Luu 等人 [42] 在 2016 年最先归纳了智能合约中可能产生的 4 种安全问题，即交易顺序依赖 (Transactions-Ordering Dependence, TOD)、时间戳依赖 (Timestamp Dependence)、未妥善处理的意外 (Mishandled Exceptions)、重入弱点 (Reentrancy Vulnerability)。针对上述安全漏洞，作者基于符号执行的检测方法，开发了检测工具 Oyente，其输入为合约对应的 EVM 字节码。相较于静态污点分析或数据流分析等检测方法，符号执行具有更高的准确性。虽然该方法对内存和时间的消耗较大，但智能合约的程序大多较为简短，因此，采用符号分析的方法对智能合约进行安全性分析是可行的。

Grossman 等人 [43] 专门针对以太坊中的重入攻击，提出了 Effective Callback Freedom 的概念，即要求 callback 函数的调用不会影响到原有程序的状态和行为。作者指出，这一概念可高效地用于检测以太坊中重入攻击，并给出了相应的在线检测器 ECFChecker。

Chen 等人 [47] 指出，智能合约设计不规范将会导致用户支付不必要的 gas 费用。通过对以太坊上的智能合约的总结和分析，作者列举出了 7 种 gas 消耗数量较大的合约模式，并将其进一步分为两种类型：无用代码类和循环类。同样利用符号执行的方法，作者开发了检测工具 Gasper，其输入为高级语

言 Solidity 编写的智能合约，能够检测并减少合约执行过程中不必要的 gas 花费。

Mueller[48] 借助符号执行 (symbolic execution) 后端 LASER-Ethereum[49]，结合可满足性理论 检验 (SMT solver) 和污点分析等，提出了合约分析工具 Mythril，其输入为合约对应的 EVM 字节码。截至当前 (2020 年 2 月)，Mythril 已经发展成为支持多种以太坊衍生平台上智能合约的安全分析工具，其能够用于分析多种常见的错误。

尽管符号执行在检测漏洞方面有强大的能力，但其不一定能够遍历程序中所有的路径，因此可能出现假阴性的结果。针对这一问题，Tsankov 等人 [44] 基于抽象释义 (abstract interpretation) 的方法，提出了分析工具 Securify，其可以保证遍历合约中所有可能的执行。其输入主要是 EVM 字节码 (也可以是 Solidity 语言) 以及由专用语言 (Domain Specific Language, DSL) 定义的安全模型，并通过反编译字节码、推测语义事实、检查安全模式等步骤，可以检测出合约是否满足安全模型中所描述的性质。

Kalra 等人 [50] 结合抽象释义、符号模型检查 (symbolic model checking) 以及约束霍恩字句 (constrained horn clauses, CHCs) 等方法，提出了 Zeus 工具。作者指出，利用该工具检测出现假阴性结果的可能性为 0，并且其有较低的假阳率，并且相较于 Oyente，具有更快的检测速度。Zeus 理论上能够接受各种高级语言编写而成的智能合约作为输入，因此还能够支持以太坊以外的平台，例如 Fabric 等。其首先将待检测合约转换成 IR，如 LLVM bitcode，再根据用户自定义的安全策略描述，采用静态分析的方法在 IR 中插入检测点，最后，其利用基于 CHCs 的验证工具验证合约的安全性。

Tikhomirov 等人 [45] 分析、总结了智能合约编程过程中可能出现的问题，包括 :1) 安全相关的问题；2) 功能相关的问题；3) 执行相关的问题；4) 开发相关的问题。作者在此基础上设计了静态分析工具 SmartCheck，其首先将 Solidity 代码转化成 XML 分析树作为 IR，再使用 XPath 对其进行安全性分析。

Torres 等人 [46] 针对智能合约中可能出现的多种整数漏洞，结合符号执行和污点分析的方法，给出了分析工具 Osiris。其能够接受 Solidity 或 EVM 字节码作为输入。相较于 Zeus，Osiris 能够检测出更多种类的漏洞，并且具有更低的假阳率。作者指出，Zeus 无法检测整数漏洞，因此其声称的零假阴率是不准确的。

Brent 等人 [51] 采用了逻辑驱动 (logic-driven) 的方法提出了分析框架 Vandal，其首先将输入的 EVM 字节码转化为逻辑关系，再利用逻辑驱动的方法验证该逻辑关系的正确性与安全性。使用该框架，用户可以更加便捷、容易地定义安全性分析的需求，这里的需求使用 Soufflé 语言 [51] 描述。作者还将该工具与前文中提到的 Oyente 和 Mythril 进行了性能方面的对比，结果表明，Vandal 和 Mythril 能够检测出比

Oyente 更多种类的漏洞，并且 Valdal 的计算效率相较其他两者更高。

Jiang 等人 [52] 提出了第一个基于模糊测试 (fuzzing) 方案的智能合约检测工具 ContractFuzzer，其利用智能合约的应用二进制接口 (Application Binary Interface, ABI) 生成模糊测试输入，并利用 EVM 对这些输入的执行结果进行安全性分析。测试结果表明，相较于 Oyente，ContractFuzzer 具有更低的假阳性，但某些漏洞检测结果具有更高的假阴性。

Dika[36] 对上述部分工具的效率、准确度以及所支持的漏洞类型等进行了详细的分析。Harz 等人 [54] 进一步对截至 2018 年已有的一些合约语言和验证工具进行了对比和分析。

2.6.3 数据安全共享与计算

原生的区块链系统解决了数据存储的不可篡改和不可伪造问题，但链上数据的安全共享与计算仍是一个开放的问题。本小节介绍联盟链三种主流的数据安全共享技术与机制。

2.6.3.1 私有交易与加密授权访问

私有交易与加密授权访问机制典型的应用代表是 Quorum 联盟链，它增加包括以下两种数据安全保护措施：

- 私有交易机制：在私有交易中，通过密码学技术来对私有交易数据加密，实现对相关的参与方可见而非相关方不可见；
- Constellation &Tessera 组件：Quorum 的两种独立的加密模块，分别使用 Haskell 和 Java 语言实现，它们的作用是利用 P2P 加密消息交换将私有数据定向传输到相关参与方。

Quorum 将交易类型分为公开交易 (Public Transactions) 和私有交易 (Private Transactions) 两类。前者应用在包括某些服务提供商的市场数据更新等公开场景；后者应用在企业间安全的交易活动。两种交易类型的主要区别在于数据内容是否被加密，私有的内容会被加密，只有具备解密能力的节点（相关参与者）才能获得具体的交易数据内容，而相关参与者范围可在交易的 privateFor 参数列表进行设定。区分 Quorum 在每笔交易是否哪一种类型，可通过签名中的一个特殊的 value 值进行判定：value 值为 27 或 28 时，表示这是一笔公开交易；当是 37 或者 38，则是一笔私密交易。

Constellation /Tessera 模块包括 Transaction Manager（交易管理器） 和 Enclave 两个子模块。

Transaction Manager 在私有交易中，Transaction Manager 会存储和管理私有交易的内容，并且与其他相关的 Transaction Manager 进行通信。同时利用 Enclave 来实现数据的加解密。Enclave 可实现高效并行的数据加密，公私钥对的生成和管理，安全隔离等功能。

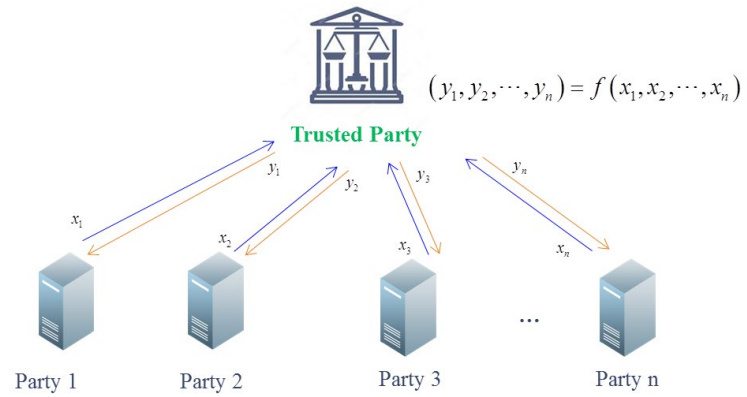
2.6.3.2 通道机制

通道 (Channel) 机制的作用非常类似于 Quorum 的私有交易机制，在联盟链 Hyperledger Fabric 平台中进行应用，它不同的交易组织建立独立的通道，实现不同组织之间的账本隔离。简单地说，对于同一个通道的交易、账本信息，只有相关组织的成员才可访问、接收和记录，非相关成员无法访问和查看。

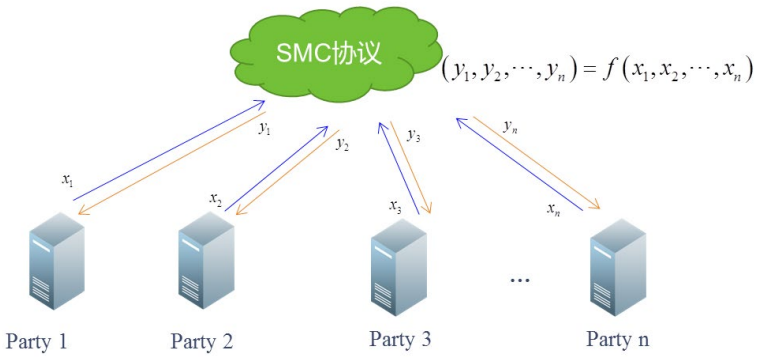
通道机制看作一个虚拟区块链网络，位于物理区块链网络之上，具有自己的访问规则。这些通道采用自己的交易订购机制，从而提供可扩展性，最终实现有效订购和大量数据的分区 [58]。Fabric 中的通道配置了一些访问策略，用于管理通道资源（链码、交易和账本状态）的访问权限，从而专门在通道内的节点中保护了信息的隐私性和保密性。Fabric 中的通道适用于以下情况：区块链网络参与者子组拥有大量共同交易（足以证明创建全新广播订购通道是合理的），并且不必依赖于该组以外实体所控制的状态，即可处理这些交易。同时，需考虑效率性能以及网络通道架构的可扩展性，交易率应该足够高并且业务合作伙伴建立的通道数量应该足够少。借助通道访问可配置性，可通过保护整个交易，不向该通道之外的其他各方显示，进而保护供应商及其每个合作伙伴的隐私。

2.6.3. 安全多方计算

安全多方计算（Secure Multi-party Computation，SMPC）无需引入可信任的第三方，即可解决一组互不信任的参与方之间保护隐私的协同计算问题。具体来说，SMPC 确保输入计算的正确性，同时不会泄露参与计算一方的输入值给其他方的成员。其可形式化描述为，n 个计算参与方分别持有数据 x_1，x_2，，x_n，协议的目的是利用各方的秘密数据计算一个预先达成的共识函数 y_1，y_2，，$y_n=(x_1，x_2，，x_n)$，此时任意一方可以得到对应的结果，但无法获得其他任何信息。图 2.7 给出了安全多方计算与传统分布式计算的模型框架图。



(a) 传统的多方输入计算模型



(b) 安全多方计算模型

图 2.7 安全多方计算与传统分布式计算的比较

SMPC 的“去中心化”以及计算过程的“分布式”，这与区块链的原生特性十分相近，因此区块链与 SMPC 技术结合具有天然的优势。一般来说，对于已有计算能力的区块链应用，如以太坊的智能合约，在链上计算过程中，其所有的数据都是公开透明的，因此会产生数据与隐私泄露问题，通过 SMPC，在链上实现两方或多方机构的数据共享与计算过程中，可确保敏感数据和隐私不被泄露。目前已经出现了一些实用的安全多方计算方案，国内外相关企业区块链在金融领域进行商业化应用。比如信用借贷场景，银行与信用机构进行协同计算，银行在获得用户正确的信用评分同时，保护贷款用户具体的各类征信内容不可见。

2.6.4 隐私保护

上一节介绍的私有交易与加密授权、通道机制和安全多方计算的三类数据安全共享技术，在对应的特定场景中同样实现了隐私保护。此外，对于区块链通用场景的隐私保护，目前主要采用混淆机制、环签名和零知识证明三类技术，下面对其分别进行介绍。

2.6.4.1 混淆机制

混淆机制（Mixing mechanism）用于实现的交易的匿名性，被广泛各种数字货币中，比如Blindcoin、达世币（Dash）和门罗币（Monero）等。

混淆机制的核心思想是在不影响区块链正常运行情况下，隐藏交易双方的交易过程的地址信息，使攻击者无法准确分析出地址之间的关联关系，将交易者的交易关系混淆在相互无关联的地址中，从而增加攻击者的分析正确交易信息的难度。混淆机制思想最初由 Chaum[58] 提出，经过发展已有多种方案，主要可分为两类：

中心化的混淆机制：该机制需要在交易双方之外引入第三方节点。原理如图 2.8 所示，首先，所有参与混淆的用户 s_1，s_2，，s_n 将资金发送给第三方节点 Mixer，第三方节点 Mixer 对收到的资金汇总后，进行一系列的重新分配，最终将指定金额的资金分别转发给相应的接收用户 r_1，r_2，，r_n。由于资金交易关系不是直接传递，而是经过第三方节点进行混淆，因此攻击者很难分析出交易双方的地址关系，从而保证资金流向的不可追踪性且实现用户隐私保护。此类方法的优点在于简单且容易部署，目前该机制已经发展一种服务，比如 BitLaundry、BitcoinFog、Blockchain.info 网站等，用户根据择不同的混淆服务提供商，需支付一定的服务费用。

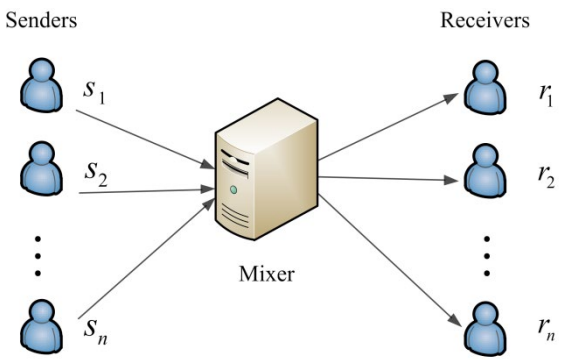


图 2.8 中心化的混淆机制原理

- 去中心化的混淆机制：中心化混淆机制由于依赖于第三方节点的处理，因此引入新的问题——无法保证第三方不会窃取混淆用户的交易隐私。去中心化的混淆机制克服这一缺陷，通过安全协议可以实现不需要第三方节点参与。最早的去中心化混淆方案是由 Gregory Maxwell[56] 在比特币论坛上提出，被称为 CoinJoin 方案。CoinJoin 方案主要思想是通过将同一个时间段的多笔交易合并成一笔交易，从而隐藏交易相关方具体的对应关系。比如在某一个时间段，有以下几笔资金的输入输出交易，$s_1 \rightarrow r_1$，$s_2 \rightarrow r_2$，，$s_n \rightarrow r_n$，通过 CoinJoin 方案后，可转变为一个交易 $\{s_1, s_2, , s_n\} \rightarrow \{r_1, r_2, , r_n\}$，由于交易输入和输出地址变成一个集合，因此攻击者无法确切地获得交易流向信息。为了保证交易是合法和不可篡改的，需要所有的输入方先后对联合交易进行签名。

2.6.4.2 环签名

环签名（Ring Signature）最早由 Rivest，Shamir 和 Tauman 三位密码学家于 2001 年首次提出 [57]，由于群成员的签名过程可连接为一个环形而得名。环签名同样可用于实现交易的匿名性，目前使用环签名方案的项目包括门罗币、布尔币、StealthCoin、XCurrency 等，以太坊平台也增加了一个类 CryptoNote 环签名。

环签名技术和一般数字签名过程一样，包括签名和验证步骤。但环签名特殊之处在于验证者验证签名消息时，只能确定签名者为“环”成员组的其中一个，但无法确定是哪一个，从而实现身份的隐藏与匿名性。假设一个“环”有 n 个成员，群组的第 s 个成员（签名者）准备对消息 m 进行环签名，具体过程描述如下：

- 签名：签名者用自己的私钥和环成员的公钥（不包括签名者自身的公钥）为消息 m 生成签名 a。
- 验证: 验证者根据环成员所有公钥（包括签名者公钥），对消息 m 和签名 a 进行验证: 若验证通过，证明签名为环中成员所签；否则签名无效，予以丢弃。

环签名在加密货币应用，使得交易具有良好匿名性和不可追踪。比如门罗币，环签名帮助它实现了交易的匿名性，攻击者无法通过区块链系统追查到交易过程确切的发送方，当其它节点对交易进行验证时，只能确定签名属于诸多公钥（用户）其中的一个，但无法定位到哪个公钥（用户）才是真正的发送方。

2.6.4.3 零知识证明

零知识证明（Zero-Knowledge Proof，ZKP）是一种密码学方法，可应用在身份认证、数据验证场景。ZKP 通过密码算法与协议的设计，可以使得证明者（Prover, P）可以使得验证者（Verifier, V）相信他们拥有某一个信息 X，但在此过程中没有泄露任何关于 X 的其他信息 [59]。ZKP 可以在区块链系统实现身份认证或交易验证过程中，确保交易双方的身份匿名化和隐私保护。在公有链和联盟链上均有所应用。在公有链应用中，主要包括 zk-SNARK 和 zk-STARK 两种协议。zk-SNARK（Zero-Knowledge Succinct Non-Interactive Argument of Knowledge）是一种证明简洁，可快速验证，且证明者 P 和验证者 V 之间几乎不进行任何交互的零知识证明协议。zk-SNARK 已经相对成熟并被较为广泛的使用，例如在 ZCash 货币的交易模型中，交易的发送地址和接收地址以及转账金额等关键性隐私信息是隐藏或加密的，但矿工通过 zk-SNARK 协议验证一笔交易是有效的。zk-STARK（Zero-Knowledge Succinct Transparent Argument of Knowledge）是 zk-SNARK 协议的改进版本，被认为是该技术的更快和更便捷的实现方式，它主要克服了 zk-SNARK 由于过分依赖于证明者和验证者之间的初始化可信设置可能引入的安全问题。然而，当前的 zk-STARK 协议方案仍然处于研究和发展阶段，有效性与可扩展性须待验证。

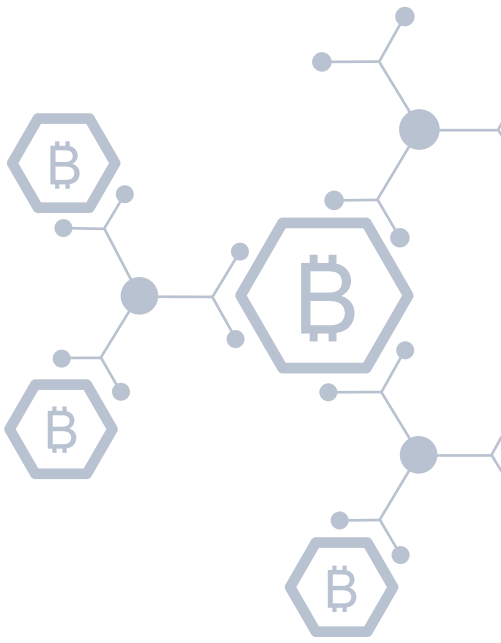
为了进一步增强 ZKP 隐私保护技术与区块链平台的结合，开发者设计了一种开源的智能合约的框架 Hawk，它使用与 zCash 相同的 zk-SNARK 协议（该库称为 libsnark）。通过该框架，非密码专业人员无需实现密码协议底层代码，可以轻松编写 Hawk 程序，通过引入 ZKP 实现验证身份、交易合法性的同时，确保身份信息与交易金额等敏感信息对外保密。

ZKP 技术在联盟链上也有诸多应用，比如 Hyperledger Fabric 1.2 版本后的身份混淆 (Identity Mixer)，它可实现交易的匿名性和非关联性 (Unlinkability)。其匿名性正是基于 ZKP 协议实现，它可以在不显示签名、选择的属性值本身（不泄露任何有关隐私信息）的同时，有效地证明拥有合法签名和相应的属性信息。

摩根和 Zcash 团队合作，在 Quorum 的 1.5 和 1.6 版本，引入 Zero-knowledge Security Layer（ZSL）模块。主要应用了 Zcash 的 zk-SNARKs 技术进一步增强隐私保护。它允许使用启用了 ZSL 的公共智能合同（Z-contract）发行数字资产。Quorum 的私人交易与 ZSL 的 Z-Contract 进行结合，允许由私人合约产生的义务通过 Z-Token 的屏蔽转移来解决，同时保持完全的隐私和机密性 [60]。

3

企业级区块链面临的安全风险



在本章中，我们以联盟链为主，分析了企业级区块链常见的安全风险[61]。

3.1 基础层风险

（1）存储计算设施是区块链系统和应用的载体，存在未授权访问等风险。

物理设备自身未及时修复的安全漏洞以及其所处的物理环境可能引入安全风险，如未经授权的设备访问和入侵，或者机房物理环境中存在的安全风险；虚拟化技术是云区块链服务的基础，存在资源滥用和越权访问风险：虚拟化技术（容器 / 虚拟机 / 虚拟网络）作为承载云区块链服务系统和应用的载体，根据平台管理功能动态创建和删除，由于资源的共用性，存在资源竞争、资源滥用、越权访问（如虚拟机逃逸、容器逃逸、VLAN 跨越）等风险。

（2）对等网络是区块链运行的关键，存在多方面的网络和通信安全风险。

区块链技术采用对等网络结构，联盟链节点成员实行准入机制，可能存在绕过准入审核机制或身份审查机制而引入恶意节点；同时，节点、网络等可能遭受攻击，如网络通信窃听、网络路由攻击、网络拒绝服务攻击等，典型的，联盟链还可能面临由于节点身份伪造造成的女巫攻击。

3.2 核心层风险

（1）共识机制算法设计不完善，可能导致信任体系崩溃。

共识机制是区块链各节点达成一致的算法，是区块链的核心能力。如果共识机制存在设计和实现缺陷，攻击者可发起共识攻击，削弱分散性、降低链上数据可信度。已出现的共识攻击有：51% 算力攻击、时间戳伪造攻击、贿赂攻击、自私挖矿、双花攻击等。

（2）密码算法面对算力增强和新计算模式挑战，未来面临多方面的破解风险。

区块链运用了大量的加密算法，包括哈希（摘要）算法、非对称算法等。哈希算法可能遭受哈希碰撞等攻击，导致身份冒用、虚假交易、共识机制失效等；非对称加密算法被攻击可能影响加密和数字签名过程，进而造成消息泄露、私钥泄露、身份伪造等。随着密码学技术发展和未来量子计算机等新技术的应用，目前广泛应用的加密算法被破解的风险将会更大。

（3）智能合约运行环境漏洞，可能影响合约的安全公正执行：智能合约运行的虚拟机及验证、控

制等机制可能存在安全漏洞，攻击者可能通过部署恶意智能合约代码，扰乱正常业务秩序，消耗网络、存储和计算资源，进而引发各类安全威胁。智能合约部署后难以更新的特点也让恶意智能合约的影响更持久。

智能合约代码实现若存在漏洞，可能导致业务欺诈等风险：智能合约语言及代码实现中可能存在安全漏洞和后门，如以太坊曾出现的交易顺序依赖、时间戳依赖、误操作异常、可重入攻击等漏洞，在调用执行合约时漏洞被利用，会影响合约处理逻辑的正确性和完备性，导致不可信的合约行为，造成财产损失。

（4）账本记录

账本记录公开易获取，如果账记录敏感信息，或账户与用户真实身份有关联，或区块链交易之间的关联性被用于推测敏感信息，都会发生用户隐私泄露风险。

3.3 服务层和用户层风险

（1）接入及节点管理机制不安全，可能造成未授权用户或恶意节点非法接入联盟链，造成联盟内数据的泄露等风险；一些联盟链追求性能，使用了弱化的共识机制并用可信节点作为整体信任的补充，非法节点接入更会影响共识结果，如 51% 攻击，账本篡改等。

（2）账本应用和业务功能逻辑设计和实现漏洞，可能影响业务安全运行。

应用安全依赖于业务逻辑、业务代码、测试程度等方面，主要风险有逻辑漏洞、木马攻击、后门等。

（3）用户和管理功能负责对区块链用户、平台用户及平台功能的管理，主要面临的风险包括身份伪造、权限设置不当、权限提升、操作不当等。

3.4 跨层功能风险

跨层功能包括开发、运营、安全、监管和审计，对区块链平台、服务、业务的正常运行至关重要，存在资源和业务生命周期管理手段不足等风险，传统的监控、运维、灾备等功能存在管理权限设置不合理、管理过程不可控等安全风险，此外跨链服务管理需考虑跨链数据泄露等风险。

4

企业相关的区块链安全态势

企业相关的区块链安全态势主要可以分为两个方面：企业级区块链安全态势，与区块链相关的企业安全态势。前者主要是指企业在部署区块链应用后的安全态势，后者企业虽然没有部署区块链应用，但其面临的安全威胁却与区块链有很大关系。

在企业级区块链安全态势方面，从行业发展来看，区块链前期主要是公有链，所以大部分公开的安全漏洞和安全事件均属于公有链。联盟链尚处于起步阶段，所以联盟链安全也主要处于早期探索阶段，公开的漏洞和安全事件非常少。当然，从技术角度，私有链、联盟链和公有链的体系和使用技术相似，所以在思考联盟链的安全实现时，分析通用区块链的公开漏洞，对提升联盟链的安全水平有很好的借鉴意义。此外，即便企业没有部署区块链应用，也应当对一些区块链相关的网络安全事件引起足够重视。

在本章后续部分，我们首先统计了区块链的漏洞，然后针对公开的企业级安全事件进行分析和研究，最后分析并总结了企业级的区块链安全态势。

4.1 区块链漏洞统计

如前所述，企业级的区块链应用漏洞还很少，如 NVD 漏洞库中与关键字“区块链（blockchain）”相关的 CVE 漏洞 408 条，且集中在 2018 年，绝大多数（401 条）是某实验室且全部在 2018 年，其中绝大多数是某实验室发现同类型的智能合约整数溢出高危安全漏洞，应为一类漏洞。此外，NVD 中，与 Hyperledger 相关的漏洞有一个 CVE-2018-3756，为 Hyperledger Iroha 中交易和区块签名认证绕过的漏洞；此外，Quorum、R3 Corda 和 FISCO BCOS 均没有公开的漏洞。

可见企业级区块链平台的漏洞还很少，而通用的区块链应用中，加密货币的安全漏洞却已屡见不鲜了，我们选取比特币和以太坊做简要分析。

比特币 WIKI 列出了所有公开的比特币漏洞 [66]，截止到 2020 年 2 月，共有 43 个，其中主要的漏洞类型如下：

表 4.1 比特币的相关漏洞统计

类型	数量
DoS	14
Fake Conf	8
Netsplit	5
Theft	4

类型	数量
Inflation	2
Deception	1
Exposure	4

此外，NVD 中 Ethereum 的漏洞多达 532 个，其中绝大多数是智能合约的漏洞（包括前面重复的 401 条），CVE Detail 网站中显示以太坊自身共 12 个漏洞 [1]，类型如下：

表 4.2 以太坊的相关漏洞统计

类型	数量
DoS	4
Bypass	8
Gain Information	5

CVE 的分类与比特币 WIKI 的不相同，但窃取数据和拒绝服务均在其中，其中两个系统漏洞数量最多的类型都是拒绝服务 DoS，即将某个节点瘫痪，从而影响共识达成。目标为双花的 Fake Conf 和 Netsplit 的数量紧随其后，其攻击的也是共识机制。

可见虽然区块链体系中，虽然区块链系统中共识层最难攻破，但其实现仍然可能出现欠考虑之处，攻击者还是可能会花很大精力去攻击共识层，因为一旦攻破，其获利巨大。这应引起区块链应用开发者的关注，虽然表现的是代码层的传统漏洞，但攻击者的目标却是新的共识机制。

[63] 分析了 Hyperledger Fabric 的安全性，指出了两个缺陷：一是背书节点的身份在给定通道上是全局可知的，可能会遭到拒绝服务攻击，造成交易受阻或网络降级；二是 Hyperledger 易受 wormhole 攻击，在通道中一个成员被攻陷后，会导致账本中的成员信息外泄。

需要说明的是，虽然 Hyperledger Fabric、Quorum、R3 Corda 和 FISCO BCOS 尚无公开的漏洞，这并不代表其运行时环境是安全的。例如 Hyperledger Fabric 使用 GO 和 JAVA 作为智能合约的运行时环境，那么这两类语言相关的漏洞，如 CVE-2016-3958，CVE-2017-10388[65]，可能被攻击者利用；此外 Hyperledger Fabric 使用 Docker 作为智能合约的隔离运行引擎，那么 Linux 内核漏洞和 Docker 的漏洞，如 Dirty COW(CVE-2016-5195)，都可能造成攻击逃逸。

1 https://www.cvedetails.com/vendor/17524/Ethereum.html

4.2 公开的企业级区块链安全事件和安全研究

Gartner 在 2018 年曾经预测，到 2020 年，至少一个灾难性的被发现漏洞会摧毁一个主要的区块链平台，导致巨大的金融损失 [67]。目前看相关的区块链安全事件主要集中在针对交易所的攻击，从而窃取加密货币。我们目前没有找到公开的企业级区块链相关的安全事件，但随着企业越来越多地使用联盟链等区块链技术应用于各种场景，相信在未来几年逐渐会出现相关的安全事件。

对于企业安全团队而言，攻击者利用区块链进行恶意攻击，破坏信息系统的完整性、可用性（或更具体的，通过加密货币牟利），这样的安全事件则更值得关注。

一旦被攻击，往往需要支付高额的赎金，而赎金往往是通过加密货币或匿名货币支付的。

一类安全事件是勒索软件（Ransomeware）引发的勒索事件，攻击者通常需要让受害者支付一定数量的加密货币作为赎金。近年的一些事件中，一些工厂和运营商，如本田、LG、台积电等，因为勒索软件造成可能会引起生产或服务中断等重大损失，2019 年相关的损失达到了 115 亿美元 [64]。如何构建纵深防护体系，做好事前灾备、事中检测响应、事后弹性恢复，是企业安全团队面临越来越重要的任务。

另一类安全事件是恶意挖矿（Cryptojacking），黑客通过在网站中植入恶意代码，使网站浏览者在不知情的情况下，无偿贡献自己的算力为攻击者挖矿，间接为其生产虚拟货币。它不仅会破坏 Web 服务完整性，而且会耗费大量电力资源和计算机资源，影响用户电脑的正常使用。2018 年“英国企业网络威胁”报告中显示，几乎全球半数企业都曾遭受过 Cryptojacking 攻击，总共有将近 5 万家网站都感染过挖矿劫持脚本。相比于勒索软件和其他恶意软件系列，Cryptojacking 拥有更低的操作难度系数和更高的投资回报比，它不需要侵入目标系统来建立命令和控制，受害者只是以被动的方式消耗自己的 CPU 周期和电力来进行与加密货币相关的哈希函数的计算。因其隐蔽性和获利便捷性，近些年来恶意挖矿已经成为最普遍的一种网络攻击方式。

在绿盟科技 2019 年的《物联网安全年报》[68] 中，我们公开了一个利用物联网设备等终端、面向门罗币挖矿的僵尸网络。据不完全统计，该僵尸网络控制的肉鸡数量上万台，单日最高活跃肉鸡数接近 600 台，在 2019 年 7 月份最为活跃，至今依然存在网络活动。

4.3 企业级区块链安全态势分析

从区块链自身的漏洞和安全事件来看，企业级区块链应用还在早期，但随着区块链应用的普及，相关的公开漏洞会越来越多。我们可以预测大部分漏洞会来自智能合约，特别是不安全的函数、越界等常规的安全问题，但也会有一些漏洞与业务相关，可能会造成业务中断或让攻击者获利。

在与区块链相关的企业安全事件方面，勒索软件和恶意挖矿是近年来企业面临的重大安全威胁，匿名货币或加密货币变现的便利性，使得这类恶意攻击会持续很长一段时间。当然，加密货币的汇率变化，也会在一定程度上影响这类攻击的态势。

中长期看，Gartner 认为，区块链会不断解决在可扩展性、可交互性的问题，在 2023 年左右在会显示其价值 [69]。随着企业部署区块链应用增加，针对企业级区块链的安全事件也可能在 2023 年后频发。及时构建面向区块链系统的态势感知能力，是准备部署或已经部署区块链的企业亟待解决的问题。

5

企业级区块链相关安全技术

区块链在设计中采用了分布式数据存储、共识机制、数字签名、加密算法等多种安全手段和技术，以保证数据的完整性、一致性和不可篡改。企业级区块链均为许可区块链，通过依赖参与者的身份以及联盟治理进行保护。本章以 Hyperledger Fabric 为例，介绍企业级区块链相关的安全技术。

5.1 密钥管理机制

密钥安全是联盟链安全的基础，安全的密钥管理机制涉及密钥的生成、分发、存储和找回等过程的安全机制。Hyperledger Fabric 提供 PKCS1.1（public-key Cryptography Standards）生成密钥，允许使用 HSM（硬件安全模块）保护并管理数字密钥，以实现强身份验证。Fabric 无密钥定期更换机制及找回机制。

5.2 参与者身份管理

Hyperledger Fabric 提供了一个成员身份服务，用于管理用户 ID 并认证网络上的所有参与者。访问控制列表可以通过授权特定的网络操作来提供额外的权限层。例如，可以允许特定的用户 ID 调用链码应用程序，但是不能部署新的链码。

5.3 监管

Hyperledger Fabric 支持参与者彼此了解对方以及所有的操作，无论是提交交易、修改网络配置还是部署智能合约都根据网络中已经确定的背书策略和相关交易类型被记录在区块链上。与完全匿名相比，可以很容易地识别犯罪方，并根据治理模式的条款进行处理。Fabric 利用密钥的层级可以给与审计员检查交易的审计权限，只将最相关的密钥披露给审计实体。

5.4 隐私保护

如前章所述，Hyperledger Fabric 通过通道、私有数据、加密链码等实现隐私保护。

1. 在每个通道的基础上使用一个不可篡改的账本，以及可以操作和修改资产当前状态（即更新键值对）的链码。账本存在于通道的范围内——它可以在整个网络中共享（假设每个参与者都在一个公共通道上操作）——或者它可以私有化，只包含一组特定的参与者。

2. 在后一种情况下，这些参与者将创建一个单独的通道，从而隔离他们的交易和账本。为了解决跨越透明度和隐私之间的差距，链码只可以安装于 Peer 节点上，需要访问执行读取和写入的资产状态（换句话说，如果一个链码不是安装在 Peer 节点上，它将无法正确地与账本链接）。当该通道上的一个组织子集需要对其交易数据保密时，将使用一个私有数据集将该数据隔离在一个私有数据库中，从逻辑上与通道账本分离，只有经过授权的组织子集才能访问该数据。
3. 为了进一步模糊数据，可以使用常见的加密算法（如 AES）对链码中的值进行加密（部分或全部），然后再将交易发送给排序服务并将区块添加到账本中。一旦加密数据被写入账本，就只能由拥有用于生成密码文本的相应密钥的用户解密。

5.5 防双花

Hyperledger Fabric 通过状态版本来防止双重支付，如果请求节点将背书过的具有相同状态依赖的交易提交给共识服务两次，共识服务会分配两个序列号给这两个交易并送达各个节点，节点在本地状态版本依赖验证时，先接受的交易由于已经提交，本地状态已经新增了一个版本，后来的相同交易由于依赖了一个过时的版本，无法通过状态版本依赖验证，会被作为非法交易被丢弃。

6

企业级区块链安全治理

6.1 政策监管

区块链产业经过多年发展，已经初具规模，而企业级的区块链应用还在探索阶段。可以将区块链的生态分成服务提供商、应用提供商和用户，那么区块链服务提供商提供区块链信息服务，由于区块链存在不可删除、事后取证等特性，其合规性要求必然与其他信息服务（如云服务）不同。虽然我国区块链信息服务的监管尚处探索阶段，但也在逐步明朗中。

2019 年 2 月 15 日，我国《区块链信息服务管理规定》正式实施。规定了须遵守规定的区块链信息服务的提供者包括主体、节点及组织等，监管执法主体是互联网信息办公室。规定提供者应建立健全用户注册、信息审核、信息记录备份、应急处置、安全防护等管理制度，区块链信息服务功能应不违反国家法律法规规定，且上线前需进行安全评估，需在规定时间内做备案、定期查验及编号标明，已备案主体后续将接受网信办及有关部门的监督和检查。使用者应进行真实身份信息认证。

国家互联网信息办公室先后发布三期境内区块链信息服务名称及备案编号，预计后期会持续推进。2019 年 3 月 30 日，国家网信办公开发布第一批共 18 个省的 197 个区块链信息服务名称及备案编号；2019 年 10 月 18 日，发布第二批 309 个境内区块链信息服务名称及编号；2020 年 4 月 24 日，发布第三批 224 个境内区块链信息服务名称及备案编号。

6.2 数据治理

随着《网络安全法》等法律的颁布，数据安全的重要性不断提升，特别是个人数据的收集、管理、交换都收到了合规性的约束。

其中，《网络安全法》第四十三条规定，个人发现网络运营者违反法律、行政法规的规定或双方约定收集、使用个人信息的，有权要求删除其个人信息，发现有错误的有权要求网络运营中更正。网络运营者应采取措施删除或更正”。

此外，网信办在 2019 年 5 月发布的《数据安全管理办法（征求意见稿）》的第二十一条规定“网络运营者收到有关个人信息查询、更正、删除以及用户注销账号请求时，应当在合理时间和代价范围内予以查询、更正、删除或注销账号”。

可见，上述法律法规都规定了作为网络服务运营者——区块链信息服务商——应提供数据删除的能力，而区块链的最大特点是数据不可删除，因而这同样是它最大的合规性风险。

尤其是恶意攻击者利用这一特性，将恐怖、反动信息上链，造成不良影响；或者将恶意代码、主控端地址上链，以达到持久化的目的。在这种场景中，数据治理就成为评价区块链系统的数据可运营性的重要指标。在传统公有链中，将错误、恶意的信息删除几乎是不可能的任务，唯一的意思例外是 DAO 事件中，以太坊通过硬分叉的方式避免了恶意的交易上链，但即便如此，仍然有政治的、非正常业务的数据存在在以太坊上。而在联盟链的场景下，相对来说，数据治理是可以实现的。原因是联盟链的节点数量有限，且经过彼此认证，除了线上的共识机制之外，容易通过线下传统的途径沟通协商，如果达成一致需要删除某个区块，则可将所有的节点（存储区块的节点，以及排序节点）上回退到历史上的相应层高即可。例如，在 Hyperledger Fabric 中，可以运行如下指令即可让当前 peer 节点回退到 blocknum 的区块，当然需要所有节点都运行该指令才能让 worldview 一致。

peer node rollback --blockNumber blocknum --channelID channelID

此外，基于 EOS 生态体系而开发的数字资产交易平台联盟链（USU）研发的镜像机制可以实现节点数据快速同步，可定期对本地账本制作镜像，实现便利的回滚机制，在统一共识下，可以指定镜像标签进行回滚。

从本质来看，区块链上操纵数据是可能的，但区块链系统节点越多，其代价越大，所以，在一般情况下攻击者无法作恶，但在必要情况下，用一定的代价（所有机构的沟通成本、系统可能的停机代价）获得数据治理的能力，也是一种技术和合规性之间的平衡。联盟链（USU）研发的镜像机制可以实现节点数据快速同步，可定期对本地账本制作镜像，实现便利的回滚机制，在统一共识下，可以指定镜像标签进行回滚。

6.3 智能合约治理

智能合约是所有背书节点都认可的可执行代码，一致的代码、相同的输入能够在全局范围内让所有的背书节点对交易的结果达成一致，节省了传统合约线下大量的核对、执行的人力、时间成本。

但从另一个角度也需要看到，智能合约是需要部署在所有背书节点上的，在一个去中心化的区块链系统上，即便是联盟链，也无法做到每个节点都能同时更新合约，所以这就给区块链应用带来了一个很大的安全风险：当智能合约出现了安全漏洞，其代码修复和合约更新的成本可能是极高的。

智能合约的安全问题非常重要，出现漏洞或错误后，无法像中心化系统那样通过关闭系统，集中升

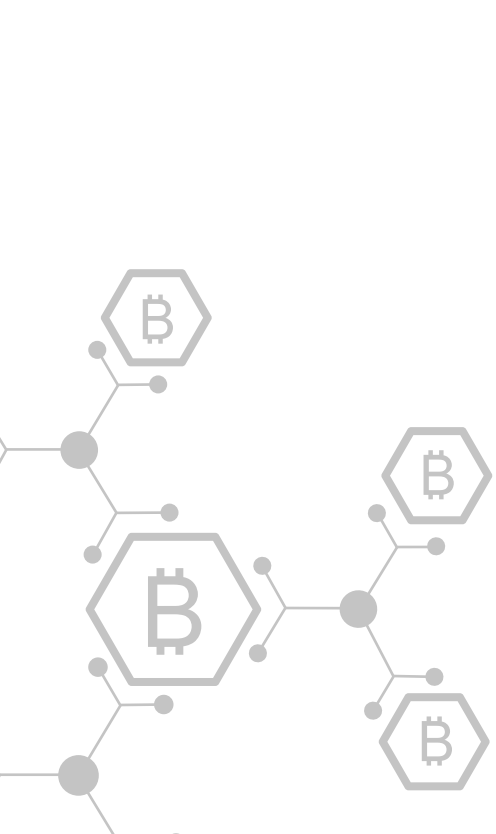
级的办法进行修复。而智能合约往往直接管理资金或重要的交易数据，一旦出现漏洞会直接导致经济损失，因此需要更强的安全措施。

目前在这方面的研究热点是把以往应用在芯片设计或者军事控制系统上的形式化验证的方法，应用到智能合约上，以数学证明的方式尽可能避免人为错误。例如，成都链安[1]研发的链码自动形式化验证工具，可有效检测 Hyperledger Fabric 链码常规安全漏洞，并向用户提供漏洞修复建议。

1 https://www.lianantech.com/

7

企业级区块链安全解决方案



为了应对企业级区块链面临的安全风险，我们提出了三层四阶段的企业级区块链安全解决方案，如图 7.1 所示。根据区块链的技术栈，可以将解决方案从纵向划分为基础层安全、核心层安全，以及用户和服务层安全；此外，根据安全防护的生命周期，可分为开发交付、安全防护、异常检测、响应恢复，以及全阶段的安全服务。

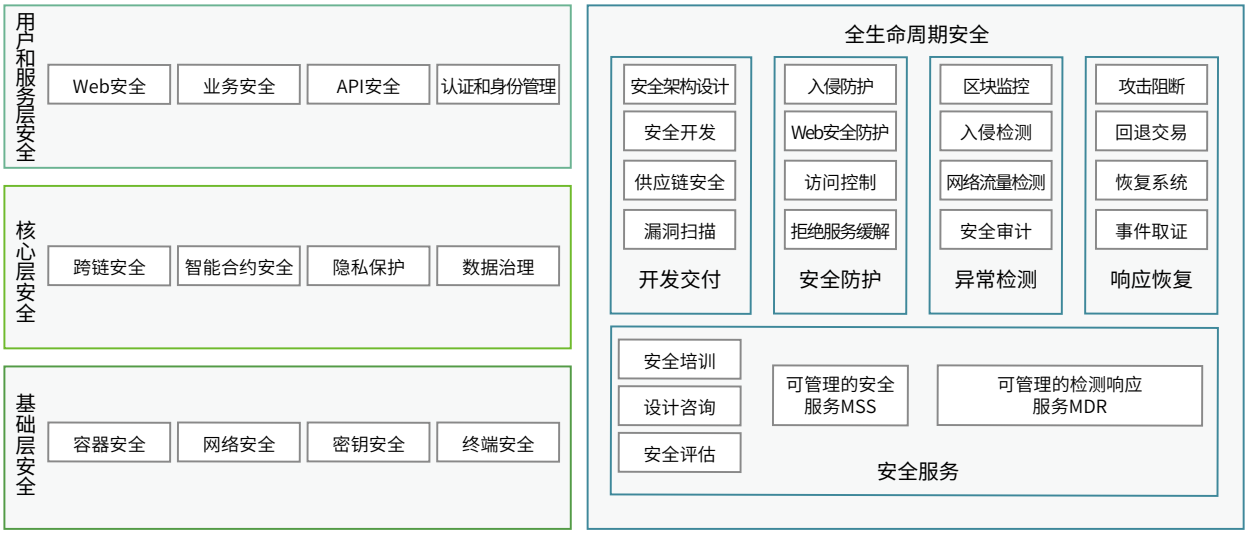


图 7.1 企业级区块链安全解决方案

7.1 基础层安全

基础层安全包括容器安全、网络安全、密钥安全和终端安全。

7.1.1 容器安全

容器（Container）技术通过共享主机操作系统内核，实现轻量的资源虚拟化和隔离，近年来在区块链、DevOps、微服务等领域有着广泛的应用。其中，Hyperledger Fabric 便是基于容器技术部署的，其智能合约运行在容器上，所以容器安全性决定了智能合约的运行时安全，甚至影响区块链节点的安全性。

容器安全涉及到容器镜像和仓库的安全评估、容器运行时异常（特别是容器逃逸）检测，以及微隔离、访问控制等。对于容器安全的防护可以参考《2018 绿盟科技容器安全技术报告》[70]。

7.1.2 网络安全

企业级区块链应用是典型的分布式部署的应用，通过计算机网络互联，所以同样面临各种传统的网络安全风险，需要应用传统的网络安全防护措施，包括安全域划分、访问控制、流量清洗、入侵检测、恶意代码防护、VPN 接入等。

此外，联盟链节点之间通过点对点网络互联，所以所部署的网络安全方案也需包含相应的 Overlay 网络支持。

7.1.3 密钥安全

企业级区块链中的密钥分配和管理非常重要，密钥的泄露不仅会导致隐私加密数据的泄露，攻击者更进一步还可以伪造虚假交易，对区块链系统的正常运转进行破坏。因此，需要对密钥进行安全存储，通常将其存储于密钥安全模块（HSM）中。

7.1.4 终端安全

终端安全主要包括区块链节点的安全防护，包括日常的清理工作，如操作系统安全配置与加固、可信计算栈、安装杀毒软件或 EDR 软件；运行时的监控，包括异常行为检测、内存监控、逃逸检测；以及发现恶意攻击时的响应处置。

7.2 核心层安全

核心层安全包括跨链安全、智能合约安全、隐私保护和数据治理。

7.2.1 跨链安全

多个企业级区块链应用交互时，不可避免地会使用到跨链技术。为了突破单链框架下的性能、容量、隔离性等多方面的瓶颈以及满足多集体的应用协同需求，以 Hyperledger Fabric 为代表的联盟链项目采用跨链技术来增强系统的可用性，跨链旨在多个区块链之间进行数据交换，但却存在公证人共谋、侧链验证主链交易、交易通道拒绝服务、长距离攻击、日蚀攻击、区块肿胀、跨链重放等需要解决的安全问题 [71] 。

因而，在设计侧链时应考虑上述可能的威胁，结合多种安全机制，例如 Interledger 最初采用了公证人机制的跨链技术路线 , 但考虑到公证人共谋的可能性 , 也在融入哈希锁定的理念。

Polkadot 引入了一种新的共享安全模型，让链与链之间进行交互的同时共享“池安全”，给双方提供相同的安全保证。

Cosmos 系统通过引入 Sovereign Zone 来管理其安全模型，为了防止恶意 Zone 进入 Cosmos Hub 攻击 Cosmos 网络以获取 Atom，每个被允许接入 Cosmos Hub 的 Zone 都需要拥有自己的一个安全去中心化网络。这样的机制使得 Cosmos 拥有更高的去中心化程度，有效地隔离了恶意攻击者并避免了因权限集中而引起的安全风险。

可以利用密钥管理机制，包括但不限于密钥的生成、分发、存储和找回等功能来实现强身份验证。Hyperledger Fabric 中通过引入参与者身份管理机制来管理并认证系统的所有参与者，其中就包含访问控制功能，通过给特定的参与者授权来进行相应的操作，赋予节点不同链以不同的权限，加强跨链数据的安全性，避免越权访问和重要数据的泄露。例如，如前文中提到的，可以允许特定的用户 ID 调用链码应用程序，但是不能部署新的链码。

设立确定性的检查点是应对长距离攻击比较好的方法之一。

此外要注意跨链时，需要考虑合规性要求，确定不同区块链的安全等级，以防止高安全等级链的数据流入低安全等级链。

7.2.2 智能合约安全

如前所述，大部分区块链相关的漏洞均为智能合约的漏洞，不安全的代码，或逻辑漏洞，都会给企业级区块链业务带来严重的安全风险。

因此，应严格按照安全设计规范进行智能合约的设计，在智能合约上线前需要对其进行安全审计，规避潜在的安全风险。智能合约安全审计需考虑业务逻辑缺陷、数据安全、条件竞争、外部调用错误处理等多方面的审计项。

此外，在安全审计阶段，也可采用形式化验证（Formal Verification）的技术，以验证智能合约的合法性。例如，Christian Reitwiessner 将形式化证明引擎 Why3 引入到了以太坊，允许计算机创建数学化证明断言（assertion），并检查智能合约行为是否满足断言 [72]。

7.2.3 隐私保护

在区块链应用中，需要对交易者的真实身份、ID 账号、IP 地址等进行身份隐私保护，可基于混淆机制实现，混淆多个交易输入输出的地址信息，在实现交易验证的同时实现交易内容与身份的不可关联。同时，可基于环签名的密码学方案实现，实现交易身份的匿名性与隐私保护。为了实现更高级别的隐私保护，可基于前沿的零知识证明技术，在无需透露相关交易方的隐私信息情况下保证交易的合法运行与验证。一般来说，三种相关技术的隐私保护能力越强，在区块链运行的时间开销也将越大，实际应用中需根据具体场景进行技术选取。

对于交易内容、账本数据的隐私保护，通过加密授权访问机制实现更细粒度的交易身份的数据访问控制；通过私有交易机制、通道机制实现联盟链不同组织的账本数据隔离，交易广播和验证的隔离。在智能合约执行两方或两方以上的计算任务时，可结合“去中心化”的安全多方计算技术，在获得可靠的计算结果同时，保证交易方的原始数据与隐私不会在计算过程暴露与泄露。

7.2.4 数据治理

数据治理要求区块链信息服务商能提供数据删除的能力。例如，可定期对本地账本制作镜像，实现便利的回滚机制，在统一共识下，可以指定镜像标签进行回滚。

7.3 用户和服务层安全

用户和服务层安全包括 Web 安全、业务安全、API 安全、认证和身份管理。

7.3.1 Web 安全

企业级区块链应用会包括面向用户的前端 Web 站点，所以需要考虑 Web 安全，对常见的各类 Web 攻击进行防护，如 SQL 注入、跨站脚本攻击、跨站请求伪造攻击等。

当前实现 Web 安全的手段主要包括部署在服务器端的 Web 应用防火墙和 RASP（Runtime Application Self-Protection）技术，以及部署在客户端浏览器策略的 CSP（Content Security Policy）技术等。

7.3.2 业务安全

不同行业所面临的业务风险不同，企业级区块链服务提供商应考虑业务场景相应的风险，构建业务风控系统，实现业务安全。

由于不同的区块链业务各不相同，所以很难有统一的业务安全机制。当然，通常有两种思路，第一种是对正常的业务进行画像，如业务正常范围、常见业务调用序列，当出现偏离基线较远的业务请求时，则需重点关注；另一种是分析恶意的业务特征，编写规则或训练生成模型参数。

7.3.3 API 安全

应用程序编程接口（API）的大量使用奠定了企业数字化转型的基础，在程序化驱动的区块链应用中也被广泛使用，例如 Hyperledger Fabric 可以通过 Docker 的 API 部署区块链节点，通过 Fabric peer 的 API 加载或运行 chaincode。

在区块链应用中，攻击者如果对 API 发动拒绝服务攻击，则会影响整个系统的可用性；如果窃取正常用户的访问凭证，就可以执行操作，进一步进行欺诈、盗窃或泄露隐私。

因而，需要事前对 API 设计进行安全评估，始终对 API 调用进行管理和监控，必须确保 API 不被滥用或非授权调用。

7.3.4 认证和身份管理

在企业级区块链应用中，每个背书节点、机构记账节点和机构管理节点都是经过认证中心 CA 认证的，正是预先的身份认证机制简化了区块链的共识机制，给高吞吐、低延时的应用提供了底层支撑。

近几年，数据泄露问题日益严峻，数据保护条例也更加完善，大量的数据泄露事件源于身份失窃。所以，近年来零信任的理念日渐深入人心，其原则是每一次操作都应得到授权，每次访问在未验证之前都是不可信的。所以，企业级区块链应用中，认证中心应管理好各参与方的身份，确认其对资源操作的权限；此外，应设计全局一致的访问资源策略，保证每次对区块链系统的访问、每次对链上数据的访问和操作，发起的主体都是经过认证和授权的。

7.4 全生命周期安全

横向来看，企业级区块链的整个生命周期都需要将安全考虑进来。在这里，从安全团队视角，我们分为交付、防护、检测、响应四个阶段，再加覆盖全生命周期的第三方安全服务。

7.4.1 开发交付

在安全团队视角，交付阶段主要是架构师团队、研发团队和测试团队参与，目标是交付安全的区块链系统。所以需要架构师团队研究区块链的特性和面临风险，设计安全的全栈企业级区块链平台、应用；研发团队应遵循安全编码的原则，编写安全健壮的代码，最大程度减少代码中的漏洞；测试团队遵循安全测试的原则，最大程度发现代码中的漏洞。

值得关注的是在代码中引入第三方库和开源软件时，应确保不存在安全漏洞，保证供应链的安全。

在部署区块链系统后，应持续地进行脆弱性评估，对区块链平台、智能合约、容器镜像等进行漏洞扫描，发现并及时修复漏洞。

7.4.2 安全防护

在部署完区块链业务系统后，应及时部署相应的安全防护机制，如入侵防护的 IPS 系统、Web 安全的 Web 应用防火墙、访问控制的网络防火墙、抗拒绝服务攻击的 ADS 系统等。这些机制可参见相应的产品介绍，本文不再赘述。

7.4.3 异常检测

在区块链系统运行时，按照纵深防护的理念，总是假定攻击者可能攻破前述的防护机制，那么就要依靠异常检测机制，及时发现异常行为，典型的检测机制包括区块监控、入侵检测、网络流量分析和安全审计等。

区块监控：在企业级区块链运行的过程中，区块监控系统必不可少，需要针对区块链的特性和业务的特性建立各项监控指标，及时发现异常交易值、分叉或其他异常行为。

入侵检测：需要对网络传输进行及时监控，在发现疑似攻击时发出告警。

网络流量分析：主要应用于网络流量（包括但不限于流、包载荷或文件）的行为分析，帮助企业发现可疑流量或网络访问。

安全审计：可对主体对资源的访问行为进行记录并核查，对网络行为进行安全审计，发现未授权的访问，或其他异常行为。

7.4.4 响应恢复

当发现异常行为后，需经过安全团队确认，及时进行事件响应。响应恢复阶段包括阻断攻击、回退交易、恢复系统和事件取证。

阻断攻击：在恶意攻击发生时，能够对攻击进行阻断，将受影响的主机进行必要的隔离，防止系统受到进一步损害。

回退交易：当恶意交易已经出现在区块链中时，按照合规性需要或业务需要，得到区块链业务参与各方的同意，将世界观和所有记账节点的账本回退到恶意交易发生之前的正常状态。

恢复系统：当系统因攻击而出故障时，能够对系统进行恢复，包括但不限于回退前述区块链交易。

事件取证：当出现安全事件时，需具备事件取证的能力，从而溯源出攻击者。

7.4.5 安全服务

事实上，企业级区块链系统使用了各种技术，因此其架构非常复杂，所以才有各大公有云平台的区块链即服务。要保证这样复杂的区块链系统的安全，可考虑在整个生命周期中引入第三方的安全服务。

在开发交付阶段，安全服务应包括从系统设计之处的安全咨询到开发阶段的安全培训，再到系统上线前的安全评估。

安全咨询：提供专业的安全咨询服务，包括但不限于不同共识机制的安全性建议、各类密码算法的安全性建议、隐私保护的安全性建议等。

安全培训：根据企业实际情况，提供体系化的培训服务，介绍区块链及区块链安全技术、区块链应用安全解决方案，通过详细的对区块链安全事件的解读，帮助企业安全人员了解和掌握区块链应用安全相关知识，并可应用于实践。尽可能的去避免安全开发生命周期中由于区块链安全知识的缺失导致的区块链安全事件。

安全评估：包括源代码审计、渗透测试等服务，及时发现代码、系统中存在的安全问题，防患于未然。

在安全防护阶段，安全厂商应提供可管理的安全服务（Managed Security Service，MSS），协助企业安全团队完成安全产品的上线、策略配置和事件管理等工作。

在异常检测和响应阶段，第三方安全服务提供商可提供可管理的检测和响应服务（Managed Detection and Response，MDR），提供定期或按需的安全检测，当发现恶意攻击时，协助企业安全团队进行响应的事件处置，最终解决安全问题。

8

结语

结语

区块链的出现，大大提升了安全在企业中的地位。传统的“先推动业务的高速发展，再进行安全建设”模式将不再可行，安全成为区块链的刚性需求。区块链对于安全的“容错性”是很低的。在公有链中，安全的缺失有可能导致币值归零，有可能导致链的分叉，有可能给相关方带来经济上的损失，也有可能导致交易所破产，等等，这样的事件已经屡见不鲜；而在联盟链中，虽然暂时还未见公开报道，但是安全的缺失有可能导致各个参与方写到链上的数据不再可信，有可能导致智能合约不按照预期执行，从而导致一个链的“崩塌”。虽然联盟链中的合法用户即便知道有安全漏洞，也未必会去利用，一方面有被溯源到的风险，另一方面，联盟链本就是为了业务存在的，看似也没有动力去做破坏联盟链的事情，但是，从风险的角度来讲，合法的用户有可能操作不当，企业中可能存在“内鬼”的蓄意破坏，最为值得关注的是，一个安全缺失的系统，有可能被攻击者入侵，有可能导致合法用户的私钥的泄露，从而攻击者可以进行一些破坏行为，这些都不是一个安全能力不足的区块链系统所能解决的。

因此，借由本白皮书，我们也想推动安全厂商、高校与区块链服务商、用户的紧密协作。安全不是一个人的事情，只有各方紧密的合作，才能推动企业级区块链安全生态的构建，从而更好地服务于企业级区块链的用户，真正实现企业级区块链的价值。

参考文献

[1] 中国区块链技术和应用发展白皮书（2016），工业和信息化部信息化和软件服务业司

[2] 习近平在中央政治局第十八次集体学习时强调，把区块链作为核心技术自主创新重要突破口，加快推动区块链技术和产业创新发展，http://xinhuanet.com/2019-10/25/c_1125153665.htm

[3] 蚂蚁金服蒋国飞：产业区块链开场，千万日活应用将出现，https://www.8btc.com/article/543896

[4] 产业研究：2020，区块链与产业场景融合，有望大规模落地，https://www.jinse.com/blockchain/577819.html

[5] 国务院：加快推动区块链技术和产业创新发展，https://www.8btc.com/article/548559

[6] 中国区块链技术和产业发展论坛标准，区块链参考架构

[7] Hyperledger project, https://www.hyperledger.org/

[8] Quorum, https://www.goquorum.com/

[9] Corda, https://www.corda.net/

[10] Corda 分布式账本平台：简介 , https://docs.corda.net/_static/corda-introductory-whitepaper-zhs.pdf

[11] FISCO BCOS, http://fisco-bcos.org/zh/

[12] 去中心化金融 （DeFi）已成主流趋势？看看这些杀手级产品也许你就明白了 , https://www.jinse.com/blockchain/351189.html

[13] 2018 年中国区块链产业白皮书，工业和信息化部信息中心

[14] 金融分布式账本技术安全规范，http://www.cfstc.org/bzgk/gk/view/bzxq.jsp?i_id=1855

[15] Filament, https://filament.com/

[16] 区块链 + 供应链！沃尔玛试点食品可追溯，https://www.walmartfoodsafetychina.com/fs%20spotlight/blockchain-and-supply-chain-food-traceability

[17] MWC 上海 | 移远通信宣布率先推出 5G 区块链模组，https://xueqiu.com/7083418776/130301313

[18] 趣链科技助力可信物联网生态区块链模组“物链 1 号”在杭发布，https://www.chainnews.com/articles/199417853863.htm

[19] 当区块链成为最火的司法科技，惠及民生有望，https://www.jinse.com/blockchain/577918.html

[20] 全国首例！北京互联网法院采用区块链智能合约技术实现执行“一键立案”，https://www.chinacourt.org/article/detail/2019/10/id/4594154.shtml

[21] 区块链在食品安全溯源中的应用 - 离实现还有多远，https://baijiahao.baidu.com/s?id=1603803154762304603&wfr=spider&for=pc

[22] IBM Verify Credentials: transforming digital identity into decentralized identity, https://www.ibm.com/blockchain/solutions/identity

[23] DWORK C, NAOR M. Pricing via Processing or Combatting Junk Mail[C/OL] //Advances in Cryptology - CRYPTO ’ 92, 12th Annual International Cryptology Conference, Santa Barbara, California, USA, August 16-20, 1992, Proceedings. 1992 : 139 – 147.

http://dx.doi.org/10.1007/3- 540- 48071- 4_10.

[24] BACK A. Hashcash: a denial of service counter-measure[EB/OL]. 2002. http://www.hashcash.org/papers/hashcash.pdf.

[25] Szabo, N.: Formalizing and securing relationships on public networks[EB/OL]. [2019-12-12] First Monday 2(9) (1997), http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/548.

[26] Banasik W, Dziembowski S, Malinowski D. Efficient zero-knowledge contingent payments in cryptocurrencies without scripts[C]//European Symposium on Research in Computer Security. Springer, Cham, 2016: 261-280.

[27] Buterin V. Ethereum: A next-generation smart contract and decentralized application platform [EB/OL], [2019-12-12]. http://ethereum.org/ethereum.html, 2017.

[28] Wood G. Ethereum: A secure decentralised generalised transaction ledger[J]. Ethereum project yellow paper, 2014, 151: 1-32.

[29] Brown R G, Carlyle J, Grigg I, et al. Corda: an introduction[J]. R3 CEV, August, 2016.

[30] Quorum [EB/OL]. [2019-12-12] https://github.com/jpmorganchase/quorum/wiki.

[31] Lee G, Lavin J, Larimer D, et al. EOS.IO Technical White Paper v2 [EB/OL]. [2019-12-12] https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md.

[32] Androulaki E, Barger A, Bortnikov V, et al. Hyperledger fabric: a distributed operating system for permissioned blockchains[C]//Proceedings of the Thirteenth EuroSys Conference. ACM, 2018: 30.

[33] Zheng Z, Xie S, Dai H N, et al. Blockchain challenges and opportunities: A survey[J]. International Journal of Web and Grid Services, 2016, 1: 1-25.

[34] David Siegel. Understanding The DAO Attack[DB/OL]. [2019-12-13] https://www.coindesk.com/understanding-dao-hack-journalists/.

[35] Atzei N, Bartoletti M, Cimoli T. A survey of attacks on ethereum smart contracts (sok)[M]//Principles of Security and Trust. Springer, Berlin, Heidelberg, 2017: 164-186.

[36] Dika A. Ethereum Smart Contracts: Security Vulnerabilities and Security Tools[D]. NTNU, 2017.

[37] Bartoletti M, Pompianu L. An empirical analysis of smart contracts: platforms, applications, and design patterns[C]// International conference on financial cryptography and data security. Springer, Cham, 2017: 494-509.

[38] Solidity Docs[EB/OL]. [2019-12-23] https://solidity.readthedocs.io/en/latest/solidity-by-example.html.

[39] ConsenSys Diligence. Ethereum smart contract security best practices[EB/OL]. https://consensys.github.io/smart-contract-best-practices/.

[40] Wohrer M, Zdun U. Design patterns for smart contracts in the ethereum ecosystem[C]//2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE, 2018: 1513-1520.

[41] Wohrer M, Zdun U. Smart contracts: security patterns in the ethereum ecosystem and solidity[C]//2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE). IEEE, 2018: 2-8.

[42] Luu L, Chu D H, Olickel H, et al. Making smart contracts smarter[C]//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2016: 254-269.

[43] Grossman S, Abraham I, Golan-Gueta G, et al. Online detection of effectively callback free objects with applications to smart contracts[J]. Proceedings of the ACM on Programming Languages, 2017, 2(POPL): 1-28.

[44] Tsankov P, Dan A, Cohen D D, et al. Securify: Practical Security Analysis of Smart Contracts[J]. arXiv preprint arXiv:1806.01143, 2018.

[45] Tikhomirov S, Voskresenskaya E, Ivanitskiy I, et al. SmartCheck: Static Analysis of Ethereum Smart Contracts[J]. 2018.

[46] Ferreira Torres C, Schütte J. Osiris: Hunting for Integer Bugs in Ethereum Smart Contracts[C]//34th Annual Computer Security Applications Conference (ACSAC’ 18), San Juan, Puerto Rico, USA, December 3-7, 2018. 2018.

[47] Chen T, Li X, Luo X, et al. Under-optimized smart contracts devour your money[C]//2017 IEEE 24th International Conference on Software Analysis, Evolution and Reengineering (SANER). IEEE, 2017: 442-446.

[48] Mueller B. Smashing ethereum smart contracts for fun and real profit[J]. HITB SECCONF Amsterdam, 2018.

[49] Bernhard Mueller. Laser-etherum:symbolic virtual machine for Ethereum[EB/OL], 2018. https://github.com/b-mueller/laser-ethereum.

[50] Kalra S, Goel S, Dhawan M, et al. ZEUS: Analyzing Safety of Smart Contracts[C]//NDSS. 2018: 1-12.

[51] Brent L, Jurisevic A, Kong M, et al. Vandal: A scalable security analysis framework for smart contracts[J]. arXiv preprint arXiv:1809.03981, 2018.

[52] Jiang B, Liu Y, Chan W K. Contractfuzzer: Fuzzing smart contracts for vulnerability detection[C]//Proceedings of the 33rd ACM/IEEE International Conference on Automated Software Engineering. 2018: 259-269

[53] Jordan H, Scholz B, Suboti P. Soufflé: On synthesis of program analyzers[C]//International Conference on Computer Aided Verification. Springer, Cham, 2016: 422-430.

[54] Harz D, Knottenbelt W. Towards safer smart contracts: A survey of languages and verification methods[J]. arXiv preprint arXiv:1809.09805, 2018.

[55] Chaum D L. Untraceable electronic mail, return addresses, and digital pseudonyms[J]. Communications of the ACM, 1981, 24(2): 84-90.

[56] Maxwell G. Coinjoin: Bitcoin privacy for the real world, 2013[J]. URI: https://bitcointalk. org/index. php.

[57] Rivest R L, Shamir A, Tauman Y. How to leak a secret[C]//International Conference on the Theory and Application of Cryptology

and Information Security. Springer, Berlin, Heidelberg, 2001: 552-565.

[58] 使用 Hyperledger Fabric 开展私密交易 . https://www.ibm.com/developerworks/cn/cloud/library/cl-blockchain-private-confidential-transactions-hyperledger-fabric-zero-knowledge-proof/index.html.

[59] Wikipedia，Zero-knowledge proof. https://en.wikipedia.org/wiki/Zero-knowledge_proof#cite_note-:0-1.

[60] Quorum - Enterprise Ethereum Client. http://docs.goquorum.com/en/latest/.

[61] ITU-T X.1401. Security threats to Distributed Ledger Technology

[62] IDC 发布 2020 年中国区块链市场十大预测——市场越发明朗，机遇可期，https://www.idc.com/getdoc.jsp?containerId=prCHC46045520

[63] Gartner，Predicts 2020: Blockchain Business

[64] Nitish A, Raghav G, Manas G.Vulnerabilities on Hyperledger Fabric[J]//Pervasive and Mobile Computing，2019

[65] 勒索软件的破坏成本预计到 2019 年将达到 115 亿美元，https://tutorials.hostucan.cn/ssl-network-crime

[66] Overview of hyperledger (blockchain technology) security design，http://www.antihackingonline.com/blockchain/overview-of-hyperledger-blockchain-technology-security-design/

[67] https://en.bitcoin.it/wiki/Common_Vulnerabilities_and_Exposures

[68] David Anthony Mahdi, Blockchain, Is This Stuff Secure? How CISOs Can Evaluate the Security Risks of Blockchain, Gartner Summit 2018

[69] 2019 物联网安全年报，绿盟科技博客，http://blog.nsfocus.net/2019-annual-iot-security-report/

[70] Gartner sees blockchain as top tech trend for 2020，https://www.ledgerinsights.com/bright-chinas-second-biggest-food-firm-launches-blockchain-platform/

[71] 2018 绿盟科技容器安全技术报告，https://www.nsfocus.com.cn/html/2018/101_0929/10.html

[72] 李芳 , 李卓然 , 赵赫 . 区块链跨链技术进展研究 [J]. 软件学报 , 2019, 30(6): 1649-1660

[73] Formal Verification for Solidity Contracts，https://forum.ethereum.org/discussion/3779/formal-verification-for-solidity-contracts

作者

北京航空航天大学 毛剑、张宗洋、关振宇、刘建伟、伍前红

中国移动研究院 何申、王珂、粟栗、杨波

绿　盟　科　技 刘文懋、张星、陈磊、刘永军

2020 企业级区块链安全白皮书

北京航空航天大学 BEIHANG UNIVERSITY

中国移动 China Mobile 研究院 CMRI

NSFOCUS

北京航空航天大学
官方微信

中国移动研究院
官方微信

绿盟科技
官方微信