CAICT 中国信通院

中国通信标准化协会
China Communications Standards Association

区块链安全白皮书

——技术应用篇

（2018 年）

中国信息通信研究院

中国通信标准化协会

2018年9月

版权声明

前　言

区块链已成为近年来技术创新的热点名词和市场追捧的热门对象。从最初应用于数字货币到如今在多领域的广泛应用，区块链作为一种全新的信息存储、传播和管理机制，实现了数据和价值的可靠转移。世界主要发达国家也纷纷加快该领域的技术研发、战略部署和推广应用。作为网络时代的新一轮变革力量，在与现有技术结合催生新业态新模式的同时，区块链技术发展和深入应用仍需要漫长的整合过程，其核心机制、应用场景中存在的潜在风险也给技术应用和现有网络安全监管政策带来新的挑战。因此，理性看待区块链的技术优势，强化应对潜在风险已成为保障区块链技术的健康、有序发展的当务之急。

中国信息通信研究院与中国通信标准化协会牵头，联合以下单位共同研究编制《区块链安全白皮书—技术应用篇（2018 版）》：中国移动通信集团公司信息安全管理与运行中心、中国移动通信集团公司研究院、国家计算机网络应急技术处理协调中心、科大国盾量子技术股份有限公司、中兴通讯股份有限公司、广州大学网络空间先进技术研究院、上海观安信息技术股份有限公司、平安科技有限公司、三六零科技有限公司、深圳市腾讯计算机系统有限公司安全管理部、北京京东尚科信息技术有限公司。本白皮书从网络安全的视

角，客观审视区块链技术发展和应用情况，分析探讨区块链技术应用分层架构、安全风险和应对框架，给出关于促进区块链技术安全应用的若干建议，希望与业界分享，切实提升区块链技术发展应用安全性。

目 录

一、从安全视角看区块链技术发展和应用态势 1
（一）全球情况总观..... 1
1、区块链技术生态基本成型，网络安全应用开始落地 1
2、区块链安全问题逐渐浮出水面，引发各界安全思考 5
3、 持续推进区块链安全标准化，助力技术安全发展 8
（二）我国发展应用..... 11
1、技术生态结构与国外基本一致，安全服务前景可期 ... 11
2、政策聚焦技术发展和应用落地，安全指导初见雏形 ... 13
3、加快布局区块链安全标准工作，强化技术风险防范 ... 15
（三）小结 16
二、区块链技术应用分层架构及安全风险分析 16
（一）区块链技术典型应用架构逐渐趋于共识..... 16
1、存储层[S]：存储上层应用所需及产生的数据文件 17
2、协议层[P]：构建分布式、去信任的共识网络 18
3、扩展层[E]：作为区块链应用方向延伸的支撑平台 19
4、应用层[A]：技术在各行业领域应用落地的直接体现 .. 19
（二）区块链技术典型应用架构对应的安全风险..... 20
1、存储层[S]：来源于环境的安全威胁 20
2、协议层[P]：核心机制的安全缺陷 21
3、扩展层[E]：成熟度不高的代码实现漏洞 22
4、应用层[A]：各类传统安全隐患集中显现 23

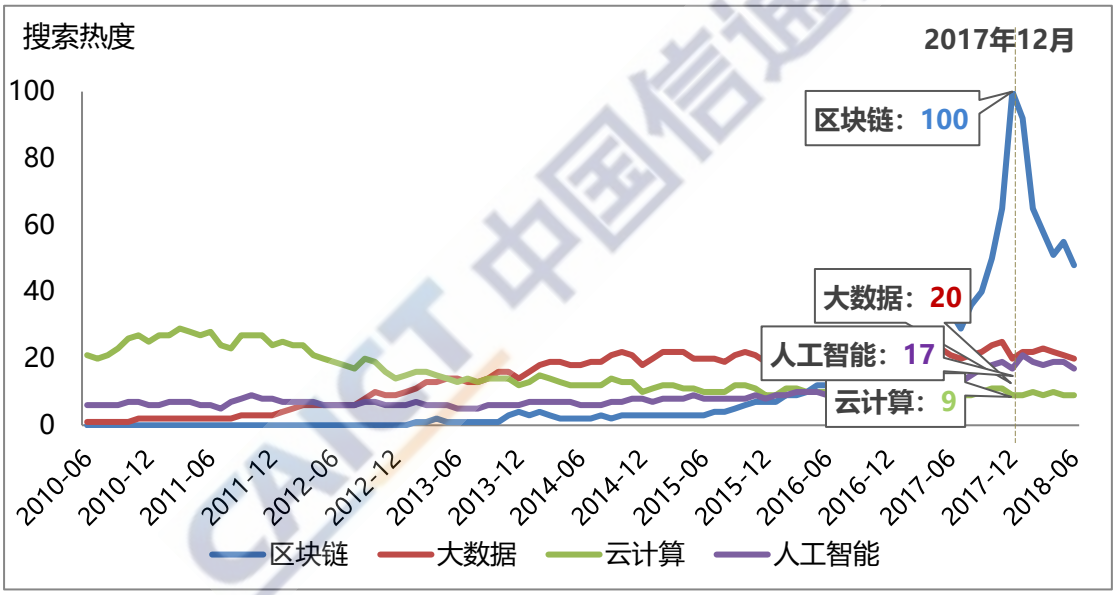
（三）区块链技术给安全监管带来的挑战..... 25
三、风险应对框架..... 27
四、促进区块链技术安全应用的建议..... 32
（一）强化应用领域引导，鼓励区块链自主可控开发..... 32
（二）创新监管手段，强化区块链平台和应用监管力度..... 33
（三）强化技术风险研究，夯实安全风险应对技术基础..... 34
（四）加强区块链网络犯罪风险防范，促进国际合作治理..... 34
附录 1 针对区块链技术核心机制的典型攻击..... 36
（一）以共识机制为目标的针对性攻击..... 36
（二）地址不具名机制对攻击者身份追溯的挑战..... 37
（三）分布式存储机制对攻击威胁面的扩大..... 37
（四）针对密码学机制固有安全风险的各类攻击..... 38
附录 2 国外区块链网络安全相关实践..... 40
附录 3 我国企业区块链网络安全相关实践..... 43
（一）中国移动研究院：基于区块链管理 PKI 数字证书..... 43
（二）360：EOSIO-BP 节点和钱包 APP 安全审核方案..... 45
（三）腾讯：区块链安全应用及应对实践..... 49
（四）平安科技：基于国产密码的自主可控联盟链实践..... 52
（五）观安：区块链移动用户数据资产安全管理实践..... 53
（六）京东：区块链防伪追溯平台..... 56
附录 4 区块链安全监管技术平台..... 58

一、从安全视角看区块链技术发展和应用态势

（一）全球情况总观

1、区块链技术生态基本成型，网络安全应用开始落地

区块链作为一种全新的信息存储、传播和管理机制，通过让用户共同参与数据的计算和存储，并互相验证数据的真实性，以“去中心”和“去信任”的方式实现数据和价值的可靠转移。近年来，区块链技术受到各界的广泛关注，搜索指数[1]持续上升，成为近年来炙手可热的新兴互联网技术之一，如图 1.1 所示。



数据来源：中国信通院整理自 2010-2018 年 Google 全球搜索趋势

图 1.1 2010—2018 年 Google 全球搜索趋势四类热点技术搜索指数对比

自 2008 年中本聪首次提出区块链概念以来，区块链技术架构经过十余年的发展已趋于成熟，因此，更多企业把发展重心放在**探索区块链在各行业领域的应用模式上**。据 Gartner 预测，到 2025 年，区块链技术将在以制造业为首的多个行业制造高达 1760 亿美元的商业

[1] 搜索指数：谷歌趋势（Google Trends）在给定时间段内的关键词搜索量统计，以百分制衡量关键词搜索热度

价值[2]。目前，区块链技术应用以金融领域为典型代表，向医疗健康、物流、工业互联网等经济社会诸多领域逐渐扩展延伸，得到了普遍的关注和全球性的探索，如图 1.2 所示。

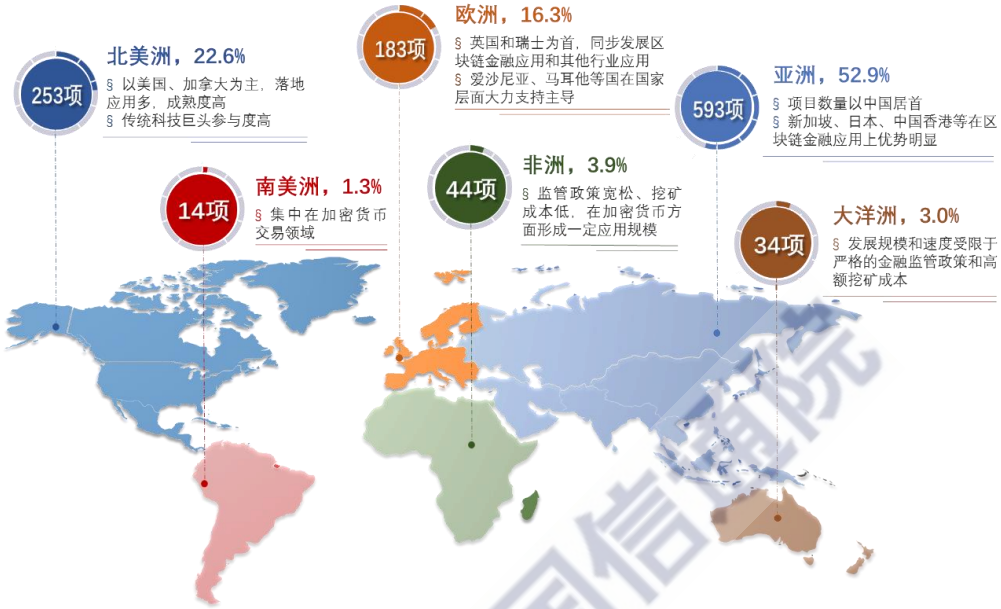


图 1.2 全球区块链技术发展应用情况

根据信通院对 1121 项全球范围内较活跃区块链项目的统计，从项目数量上看，**亚洲地区**以 593 项居首，其中，新加坡、日本、中国香港等国家和地区依托其传统金融优势，发展了一批成熟的区块链金融应用；**北美地区**的区块链项目以美国和加拿大为主，已有大量成熟高的项目和技术应用落地，其中不乏 IBM、Microsoft、Amazon 等科技巨头；**欧洲地区**以英国和瑞士为首，在发展区块链金融应用的同时，着重与传统行业结合，尤其是在爱沙尼亚、马耳他等国，在国家层面大力支持和主导，给区块链提供了大量的发展应用空间；**非洲地区**由于监管政策宽松、挖矿成本低等原因，虽然在区块链应用方面较为单一，基本集中在数字货币、交易所上，但也形成了一定的应用规模；

[2] 数据来源：Gartner ‘Forecast: Blockchain Business Value, Worldwide, 2017-2030'

大洋洲地区的区块链应用大多集中在澳大利亚和新西兰两国，但受限于当地严格的金融监管政策和高额的挖矿成本，发展规模和发展速度有限；**南美洲地区**的现有项目则主要活跃在加密货币交易领域。

从现有区块链相关项目、产品和服务内容上看，目前全球区块链技术的应用已初步形成了包含硬件和基础设施、底层技术、上层应用和安全服务在内的技术生态格局，如图 1.3 所示。

图 1.3 区块链技术生态格局

其中，**硬件和基础设施**主要为区块链运行提供矿机[3]等算力和硬件支持，包括矿机生产、矿池服务、矿机芯片生产，以及为区块链提供云基础设施等。**底层技术**一方面为各类区块链应用提供底层架构和开发平台等，起到类基础操作系统的作用，包括公有链、联盟链、私有链等；另一方面针对上层应用中的共通需求，提供分布式数据交易等区块链相关技术，旨在降低区块链应用开发门槛，加快应用落地进程。**上层应用**服务最终用户，形成不同行业和场景的应用解决方案。**安全服务**则为区块链提供代码审计、安全监测、安全管理等安全性增

[3] 目前，专业矿机多使用 ASIC 芯片，由矿机厂商设计架构，传统芯片厂商研发和代工生产

强服务。

众所周知，区块链分布式、点对点的通信具有易连接、大协作的特点，基于哈希加密的匿名性能够很好保护用户隐私和证明唯一性，依托公私钥的权限控制赋予数字资产丰富的管理权限。这些技术优势在为其发展应用提供大量创新空间的同时，也使得**区块链逐渐成为解决网络和数据安全存储、传播和管理问题的有效手段**，在攻击发现和防御、安全认证、安全域名、信任基础设施建立、安全通信和数据安全存储等方面得到了积极的探索，如图 1.4 所示。

图 1.4 区块链在网络安全领域的典型应用

例如，**在国家层面**，美国土安全部早在 2015 年已开展与 Factom[4] 等区块链企业的合作，支持区块链在身份管理、国土安全分析等领域的应用项目研发；俄罗斯联邦国防部于 2018 年在其军事技术加速器（the ERA）技术园区建设了区块链研究实验室，研究将区块链技术应用于识别网络攻击和保护关键基础设施等。**在产业层面**，LaunchKey[5]、Blockstack[6]、Guardtime[7]等企业均在各自领域推出了“区

[4] Factom，公证通，成立于 2015 年，德克萨斯州奥斯汀区块链公司，产品包括区块链数据保护工具、企业身份解决方案和分布式数据存储产品等

[5] Launchkey，去中心化认证平台

[6] Blockstack，总部位于旧金山，开发基于区块链技术的 DNS

[7] Guardtime，爱沙尼亚安全公司，开发基于区块链的安全解决方案

块链+网络安全”产品和解决方案。目前国际上区块链在网络安全领域的应用探索详见附录 2。

2、区块链安全问题逐渐浮出水面，引发各界安全思考

随着区块链技术在各行业领域的不断应用，一方面，其共识机制、私钥管理、智能合约等存在的**技术局限性和面临的安全问题逐渐显现**，区块链平台应用等安全事件层出不穷。例如，2018年3月，Binance 交易所遭到网络攻击，造成约4.2亿元的损失；2018年5月，EOS智能合约曝出严重安全漏洞，攻击者可利用漏洞控制和接管其上运行的所有节点等。据统计，2011年到2018年4月，全球范围内因区块链安全事件造成的损失高达28.64亿美元（约合人民币196.06亿元）[8]。另一方面，**区块链去中心、自治化的特点给现有网络和数据安全监管手段带来了新的挑战**（如GDPR[9]中关于数据主体、数据删除权的要求）。各类安全事件的频繁发生给区块链在新模式下的应用管理敲响了警钟，区块链安全问题也引发了政产学研等各界的广泛重视。全球主要国家和地区纷纷聚焦区块链安全，从政策引导、加强监管、技术应对等多方面开展应对，具体表现在：

英国：推动政产学研各界合作，提出“技术+法律”的区块链监管新模式

英国政府和央行一直积极响应区块链技术，希望凭借占领区块链技术发展先机，重夺其国际金融中心地位。早在2016年1月，英国政

[8] 数据来源：白帽汇

[9] GDPR：General Data Protection Regulation，通用数据保护条例

府科学办公室[10]就发布了《分布式记账技术：超越区块链》[11]研究报告，将发展区块链技术上升到英国国家战略高度，同时指出，区块链技术中存在的硬件漏洞和软件缺陷可能带来网络安全和保密风险。报告建议英国政府加强与学术界、产业界的合作，加快区块链标准制定，正视发展区块链技术面临的来自技术本身以及应用部署方面的双重问题，**以技术监管为核心，法律监管为辅助，双措并举打造区块链监管新模式。**2018年，英国政府宣布将启动新的加密货币研究工作，与金融市场行为监管局（FCA）和英格兰银行合作，探索比特币等加密货币带来的潜在风险。同时，英国企业也在积极探索区块链安全相关技术。英国最大的电信公司英国电信于2016年7月提交了“减轻区块链攻击”的专利申请，旨在建设能防止对区块链进行恶意攻击的安全系统。

美国：鼓励探索区块链在安全领域的应用，注重区块链安全风险技术应对

美国在监管方面多方听证、谨慎立法，对区块链技术发展保持着警惕而友好的态度。2018年，美国国会发布《2018年联合经济报告》，提出区块链技术可以作为**打击网络犯罪和保护国家经济和基础设施的潜在工具**，指出这一领域的应用应成为立法者和监管者的首要任务。美国国防高级研究计划局（DARPA）也正在大力投资区块链项目，旨在安全储存国防部内部高度机密项目数据。在区块链安全应对方面，2017年，美总统特朗普签署了一份7000亿美元的军费开支法案，其中

[10] 英国政府科学办公室：Government Office for Science，为英国总理和内阁成员提供建议，确保政府决策具有科学性和远见性。

[11] 《分布式记账技术：超越区块链》：《Distributed Ledger Technology：beyond block chain》，来自 https://www.gov.uk/government/publications/distributed-ledger-technology-blackett-review。

包括授权一项区块链安全性研究，呼吁“调查区块链技术和其他分布式数据库技术的潜在攻击和防御网络应用”，支持美国国土安全部（DHS）开展的**加密货币跟踪、取证和分析**工具开发项目。美国国家安全局（NSA）开发了名为MONKEYROCKET的比特币用户追踪和识别工具，通过与企业合作，从互联网的光纤连接中获取数据，监控通信内容并识别加密货币用户。除此之外，美国各大企业也积极投入提升区块链安全的技术研发中，埃森哲、Linux基金会、IBM等都在区块链硬件安全模块、区块链云环境安全等方面推出了各自的产品和解决方案（详见附录2）。根据IDC全球区块链支出半年度指南报告预测[12]，美国在区块链平台软件和安全软件方面的支出将成为服务类别以外最大的支出类别，是整体增长最快的类别之一。

欧洲：指出区块链监管机制不成熟，呼吁正视区块链安全风险

欧洲各国对待区块链和加密货币技术的态度不一，如法国政府对区块链技术表现出兴趣，但尚未在区块链领域实施重大举措，而瑞士、德国则积极发展区块链技术和应用，并先后开启区块链在本国的规范化应用进程。2016年3月，欧洲央行在《欧元体系的愿景——欧洲金融市场基础设施的未来》[13]报告中提出，欧洲央行正在探索如何使区块链技术为己所用。欧洲证券和市场管理局（ESMA）成立了“特殊小组”，进一步研究区块链技术，于2016年6月发布了一份关于应用于证券市场分布式记账技术的报告并指出，**现阶段区块链技术应用的数**

[12] IDC, Worldwide Semiannual Blockchain Spending Guide

[13] Eurosystem’s vision for the future of Europe’s financial market infrastructure

量和范围有限，监管机制并不成熟。

此外，新加坡、俄罗斯、加拿大等国也相继通过发布政策文件、成立区块链技术研究机构等不同举措，积极开展区块链技术研究，尤其是在金融等领域探索区块链应用新模式。随着区块链技术的不断发展和安全事件的频频发生，各国对区块链的态度也逐渐趋于理性，在鼓励技术创新和应用发展的同时，也在积极推动区块链安全风险、安全问题的发现和应对。

3、持续推进区块链安全标准化，助力技术安全发展

在区块链技术的发展过程中，区块链各技术分支和应用领域发展程度不均衡，缺乏统一的概念术语、架构及测评标准，技术和机制特性给法律和监管带来挑战等问题在不同程度上对技术的发展应用和产业化形成了阻碍。围绕技术架构规范、开发规范、身份认证等相关标准化、合规化问题，国际标准化组织和开源组织已开始启动区块链安全标准化工作，规范区块链技术应用发展。如图 1.5 所示。

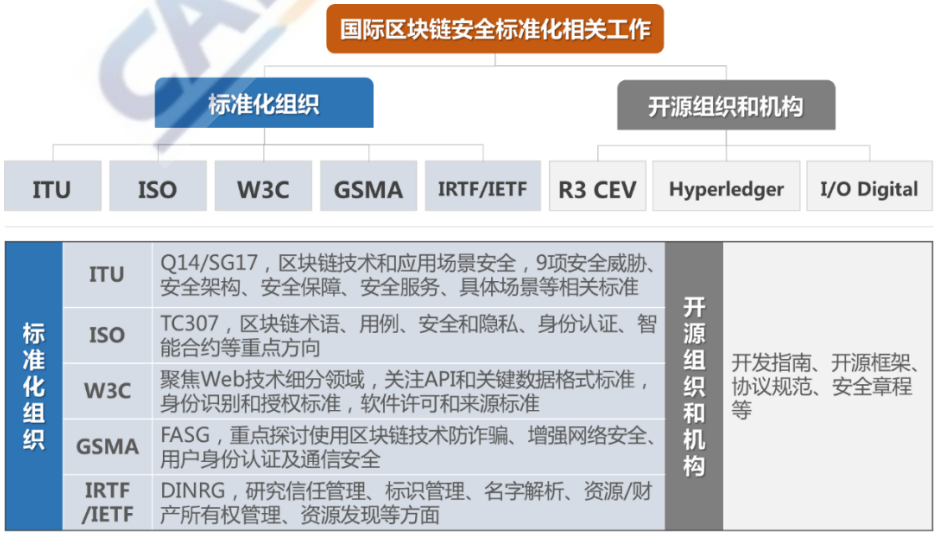


图 1.5 国际区块链安全标准化相关工作

如图所示，ITU、ISO、W3C、GSMA、IRTF/IETF 等国际标准化

组织已在区块链技术参考架构、智能合约安全等相关方面开展了大量的标准化工作，其中：

ITU：同步推进区块链技术安全和场景安全分析相关议题

ITU-T 在区块链安全议题上表现活跃，参与方众多，研究范围较广，推进路线明确。截至目前，ITU-T 成立了三个焦点组、一个问题小组，设立多个标准研究项目，围绕区块链整体发展、安全及物联网、下一代网络演进、数据管理应用等开展标准化工作。在安全方面，Q14/SG17 聚焦分布式记账技术安全问题，围绕基于区块链的应用和服务，识别安全问题和威胁，研究安全机制、协议和技术，研究个人信息保护、安全管理和互联互通安全，制定安全方案建议等。目前已开展了分布式记账技术的安全能力和威胁等 9 项区块链安全标准制定工作，分别围绕区块链技术的安全威胁、安全架构、安全保障、安全服务以及具体场景（如身份管理、在线投票、电子支付、软件分发）下的安全分析。

ISO：设立多个研究组和工作组，推进区块链安全标准研究

ISO 于 2016 年 9 月成立了区块链及电子化的分布式账本技术委员会 TC307，其下设立了多个研究组和工作组，开展区块链术语、用例、安全和隐私、身份认证、智能合约等重点方向的标准化研究工作。目前共有包括区块链和分布式账本技术参考架构（ISO/AWI 22739）、区块链和分布式账本技术安全风险和漏洞（ISO/AWI 23245 ）、区块链和分布式账本技术隐私和个人可识别信息(PII)保护概述（ISO/NP TR 2324）等在内的 8 项区块链安全标准研制中。

W3C：聚焦从细分技术层面创建安全规范的区块链标准

W3C 于 2016 年 7 月召开了区块链专题研讨会，探讨在 Web 中应用及支持分布式账本技术，明确提出区块链需要标准来消除冗余，同时促进竞争。W3C 提出了区块链的三大标准化工作目标：一是 API 和关键的数据格式标准，二是身份识别和授权标准，三是软件许可和来源标准；并呼吁创建区块链技术公共标准，为区块链安全发展和应用提供参考，其所成立的区块链社区组目前暂无成果报告输出。

GSMA：关注区块链技术在通信和安全领域应用

GSMA 于 2017 年 7 月份在 IG（Internet Group）中启动了区块链技术研究报告[14]，分析区块链技术特点、在运营商的应用场景、商业机会、投资分析和建议，其它工作组也在各自领域探讨区块链的应用。其中，FASG（Fraud and Security Group）重点探讨使用区块链技术防诈骗、增强网络安全、用户身份认证及通信安全。

IRTF/IETF：研究区块链安全和隐私保护技术方案

互联网架构委员会 IAB 下属的 IRTF 于 2016 年 9 月设立了 Blockchain, Distributed Data & Service Federation 研究项目，讨论数据分布式共享数据模型、通信协议、信息安全和隐私保护技术方案，并逐步推动制定流程、机制和协议标准，并于 2017 年 9 月更名为 DINRG（Decentralized Internet Infrastructure Research Group）工作组，研究内容为分布式基础设施服务中的关键问题（如信任管理、标识管理、名字解析、资源/财产所有权管理、资源发现等）。

[14] 报告名为 Blockchain: Opportunities for enhanced operators' propositions

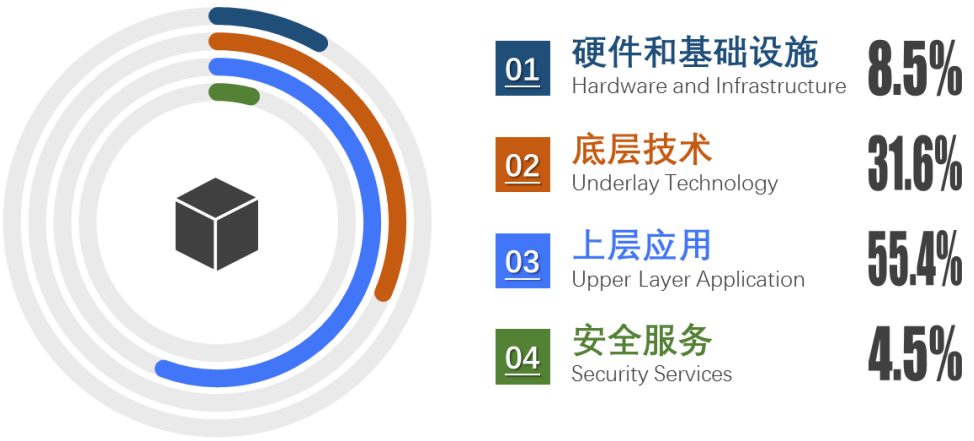
除国际标准化组织外，开源组织和联盟也对区块链开源框架、开发规范等作出了积极的探索。2018年5月，企业以太坊联盟（EEA）[15]发布了以太坊客户规范，旨在提高以太坊区块链应用程序的隐私性、可伸缩性和安全性。此外，以太坊、R3 CEV、Hyperledger-fabric等国际开源平台和联盟也相继发布了以太坊开发指南、fabric协议规范等，提出区块链开源框架、开发规范等，指导用户安全开发区块链相关程序，推动区块链技术安全发展和应用。

（二）我国发展应用

1、技术生态结构与国外基本一致，安全服务前景可期

相比于国外，我国在区块链技术发展、政策引导等方面的工作起步较晚，但近几年来，各行各业对区块链关注程度较高，在充分汲取国外发展经验的同时，积极开展自身领域与区块链技术结合的探索，区块链相关产业发展迅速。从数量上看，我国活跃的区块链项目众多，占亚洲地区总量的 85.5%，与全球各国相比也高居首位；从技术生态格局上看，在我国的区块链项目中，55.4%的项目聚焦探索区块链行业应用，其次是区块链底层技术项目占 31.6%，硬件和基础设施类项目占 8.5%，而安全服务类项目仅占 4.5%，总体看来，与全球技术生态格局基本一致，如图 1.6 所示。

[15] 企业以太坊联盟：2017 年 3 月，由摩根大通、微软、英特尔等 30 余家企业联合成立，旨在合作开发标准和技术来使企业更加容易使用以太坊区块链代码。



数据来源：中国信息通信研究院根据公开信息统计

图 1.6 我国区块链技术生态结构

尽管我国目前区块链企业数量众多，尤其是多数企业在行业应用方面积极布局，不断探索现有业务与区块链技术结合和应用模式，但其中不乏“区块链传销”、“山寨币”、“空气币”等行业骗局，以及虚假、夸大宣传区块链产品功能作用等行业乱象，从长期的市场规范化发展来看，相关问题亟待解决和优化。此外，由于目前我国区块链发展多集中于行业应用模式的探索，多数区块链技术开发者、平台运维者、用户等安全意识普遍不高，**区块链安全产品和服务的需求驱动尚不明显**；尤其是在中小企业、创业团队中，受人财物等资源的限制，开发和项目管理人员往往不具备专业的区块链安全知识，更鲜少设置专门的区块链安全管理和技术人员，专门从事安全开发控制、安全测试和安全管理相关工作，多种因素导致**我国区块链安全产品和服务市场尚未形成规模**。

随着近年来区块链平台、应用、智能合约安全事件频发，国内已有企业开始注意到区块链安全问题，一方面，传统安全企业、安全团队逐渐开始布局区块链安全，在智能合约漏洞挖掘、区块链产品代码

审计、业务安全监测等方面不断开展相关实践，致力于提升区块链产品应用安全水平和抗攻击能力；另一方面，部分企业和研究机构也在开始探索“区块链+网络安全”的应用模式，致力于发掘区块链技术在提升数据安全存储、认证安全性等方面的应用价值，详见附录 3。

2、政策聚焦技术发展和应用落地，安全指导初见雏形

近年来，我国在政策方面频频发力，在国家层面多次强调区块链技术应用价值，鼓励推动区块链技术发展和应用。2016 年 12 月发布的《“十三五”国家信息化规划》中，首次指出强化区块链等战略性前沿技术的基础研发和超前布局；2018 年 5 月，习近平总书记在两院院士大会上明确提出要加强“以人工智能、量子信息、移动通信、物联网、区块链为代表的新一代信息技术加速突破应用”。

随着区块链安全问题的逐渐显现，在推动技术发展和应用落地的同时，我国在政策制定中也开始注意到区块链安全问题，从区块链安全威胁描述、安全体系构建、安全应对建议等方面加强指导。2016 年 10 月，工信部信软司发布《中国区块链技术和应用发展白皮书》，明确指出了**区块链技术面临的安全挑战与应对策略**，针对当前区块链技术的安全特性和缺点，从物理安全、数据安全、应用系统安全、密钥安全、风控机制等五方面描绘了区块链安全体系的构建，如图 1.7 所示。

图 1.7 《中国区块链技术和应用发展白皮书》区块链安全体系

2018 年 5 月，工信部信息中心发布《中国区块链产业白皮书》，进一步分析了底层的代码安全性、密码算法安全性、共识机制安全性、智能合约安全性、数字钱包安全性等区块链面临的安全问题，梳理了通过技术手段、代码审计等方式提供安全服务的典型企业和实践，并针对性的提出了各项应对举措。

在地方性的政策层面，我国各地政府积极响应国家号召，高度重视区块链技术在本地的发展，积极推动应用落地，**对区块链安全的重视程度也不断提升，逐渐将区块链安全作为保障区块链发展不可或缺的重要元素强化引导**。2016 年 12 月，贵阳发布《贵阳区块链发展和应用》白皮书，提出通过区块链建立可信安全的数字经济，加强互联网治理，解决传统模式下数据与隐私保护难等问题。北京、深圳、上海、南京等市也相继出台政策，鼓励在金融领域开展对区块链等新兴技术的研究探索，如表 1.1 所示。

表1.1 我国地方性区块链安全相关政策

地区	政策文件	政策内容
北京	《北京市“十三五”时期金融业发展规划》	兼顾安全性的同时，鼓励发展区块链技术等互联网金融安全技术
深圳	《深圳市金融业发展“十三五”规划》	支持金融机构加强对区块链、数字货币等新兴技术的研究探索
贵阳	《贵阳区块链发展和应用》白皮书	通过区块链建立可信安全的数字经济，加强互联网治理等
南京	《南京市“十三五”金融业发展规划》	以区块链技术等为核心，推进金融科技在征信、授信等领域的广泛应用
上海	《互联网金融从业机构区块链技术应用自律规则》	注重创新与规范、安全的平衡，关注信息安全、防范系统风险等

3、加快布局区块链安全标准工作，强化技术风险防范

为防范区块链技术应用过程面临的一系列安全风险，引导规范区块链平台、系统等相关产品的开发和部署，我国在国家标准、行业标准、产业联盟标准等不同层面全面推进区块链安全标准化工作，致力于促进区块链技术的安全、有序和长效应用，如图 1.8 所示。

图 1.8 我国区块链安全标准化相关工作

目前，我国区块链安全标准化工作主要集中在安全体系架构、应用和平台安全要求等方面。其中，**在国家标准方面**，TC260[16]的 WG5[17]致力于规范基于区块链的审计信息基础设施的设计和建设，以应对审计

[16] TC260：全国信息安全标准化技术委员会
[17] WG5：信息安全评估工作组

记录篡改、敏感信息泄露等安全威胁；WG7[18]通过研究区块链应用安全管理的原则、角色、模型，提出区块链应用安全管理的内容，制定区块链应用安全管理基本控制措施；SWG-BDS[19]已启动区块链安全标准体系研究项目，并制定区块链风险模型，识别区块链关键资产和主要威胁，提出支持规划、设计和实施区块链安全的一致架构，并针对该架构的关键组件明确其具体的安全能力要求。**在通信行业标准方面**，区块链安全标准化工作主要由 CCSA TC8 WG4[20]负责推进，聚焦区块链安全，开展实施包括区块链开发平台网络与数据安全技术要求、区块链数字资产存储与交互防护技术规范等标准项目，以及基于区块链技术的数字证书管理技术研究、区块链平台安全机制与协议研究等研究项目。

（三）小结

总体来看，在经历了区块链技术的概念爆发期和炒作期之后，全球对区块链技术的关注程度仍然居高不下，世界各主要国家和地区竞相布局区块链发展和应用探索，区块链技术生态逐渐成型。在享受区块链释放的变革性技术红利的同时，其衍生的安全问题也在逐渐浮出水面。各国已开始在政策、标准、技术等不同层面寻求应对之策。

二、区块链技术应用分层架构及安全风险分析

（一）区块链技术典型应用架构逐渐趋于共识

随着区块链技术在各行业的不断探索，区块链技术应用模式日趋

[18] WG7：信息安全管理工作组

[19] SWG-BDS：大数据安全特别工作组

[20] CCSA TC8 WG4：中国通信标准化协会—网络与信息安全—安全基础组

成熟。如前所述，国际标准化组织、全球各主要国家、行业企业等都从各自的视角对区块链技术的应用架构进行了描述，尽管各方提出的技术架构并非完全一致，但总体看来，在区块链技术应用架构中应包含的关键层次和核心机制上已达到了高度的一致，如图 2.1 所示。

图 2.1 区块链技术典型应用架构

从技术架构设计的角度看，区块链技术典型应用架构呈四层的层次化划分，自下而上依次包含存储层、协议层、扩展层和应用层。其中：

1、存储层[S]：存储上层应用所需及产生的数据文件

区块链的底层数据存储较为灵活，多结合文件系统、关系数据库、键值数据库等存储方式，在各参与节点侧实现区块链中“区块+链”数据结构的存储和检索，如图 2.2 所示。

存储方式			典型应用例
区块数据存储	数据检索	其他运行数据	
关系数据库	关系数据库	文件系统	Ripple 币
文件系统	键值数据库		比特币、Hyperledger Fabric
键值数据库	键值数据库		以太坊

图 2.2 典型区块链底层数据存储方式

如依托键值数据库等非关系型数据库，实现区块链中“区块+链”的数据结构的存储和检索；或是采用传统文件系统存储区块数据，而只是在检索时使用“Key+Value”的键值数据库检索区块数据等。

2、协议层[P]：构建分布式、去信任的共识网络

协议层通常采用 P2P 网络组网，结合各类密码学安全机制和共识机制，为上层应用构建对等、安全、信任的网络和通信基础。**一是使用 P2P 技术构建对等的通信网络。**区别于传统 C/S 结构的服务型网络，区块链的每个参与者都将作为 P2P 网络的一个节点，可同时充当客户端和服务端的角色，参与到校验区块信息、广播交易、新节点识别等活动中。**二是依托非对称加密机制提供安全属性保障。**在区块链中，数据的加密解密、签名验签、认证校验等均以非对称加密机制实现，为数据的机密性、完整性、不可伪造性和隐私的保护提供不同程度的安全保障。**三是基于共识机制维持区块链有序运行。**通过共识机制，相互间未建立信任关系的区块链节点可共同对数据写入等行为进行验证，以大多数节点达成一致的信任构建方式，摆脱对传统中心化网络中信任中心的依赖。

3、扩展层[E]：作为区块链应用方向延伸的支撑平台

在区块链发展的初期，扩展层并非区块链技术架构中不可或缺的一部分。随着应用场景的持续延伸，区块链技术架构不断演变完善，扩展层的出现使得开发者可在上层应用和底层技术机制之间，以可执行代码的方式，为用户实现复杂业务流程的自动化；或是通过设置激励/惩罚机制，规范区块链节点贡献自身存储和计算资源，共同推动网络和业务的高效运行。目前，扩展层的实现主要以在以太坊之上开发和运行的智能合约为主，实现在各类交易场景中，交易双方或多方间协议在满足条件时的自动执行。值得注意的是，智能合约也在开始支撑 DApp[21]的开发和应用，探索新的去中心化的 App 开发、维护和运营模式。

4、应用层[A]：技术在各行业领域应用落地的直接体现

区块链以牺牲适量的计算力、带宽或存储资源换取安全性的机制，使其逐渐在金融、医疗、能源、通信等领域成为推动信任机制重塑，解决网络和数据安全存储、传播和管理问题的全新手段。应用层则是区块链技术在不同行业领域的各类应用场景和案例最直接体现，在支付结算、证券、票据、医疗健康、供应链等应用方向上通过 App、Web 平台等不同形式服务于最终用户。与区块链技术架构的其他层次相比，应用层最直观地体现了区块链技术的应用价值，因此，目前在国内外区块链技术生态中，对区块链技术应用方向的探索尤为活跃，覆盖加密货币、交易清算、能源交易、商品溯源等金融和实体领域应用。

[21] DApp： Decentralized App，基于智能合约，由参与者共同开发、维护、运营的去中心化应用

（二）区块链技术典型应用架构对应的安全风险

尽管区块链的防篡改、分布式存储、用户匿名等技术优势为其发展应用提供了大量的创新空间，但目前区块链技术在各领域的应用模式仍处于大量探索阶段，其深入应用仍需漫长的整合和发展过程。区块链技术本身仍存在一些内在安全风险，去中心化、自组织的颠覆性本质也可能在技术应用过程中引发一些不容忽视的安全问题，如图 2.3 所示。

图 2.3 区块链技术典型应用架构对应的安全风险

具体包括，

1、存储层[S]：来源于环境的安全威胁

如前所述，区块链存储层通常结合分布式数据库、关系/非关系型数据库、文件系统等存储形式，存储上层应用运行过程中产生的交易信息等各类数据。存储层可能存在的安全风险有**基础设施安全风险、网络攻击威胁、数据丢失和泄露**等，威胁区块链数据文件的可靠性、完整性及存储数据的安全性，具体包括以下三点。

■ **基础设施安全风险[S1]：**主要来自区块链存储设备自身以及所处环境的安全风险，如 LevelDB、Redis 等数据库中可能存在未及时修复的安全漏洞，导致未经授权的区块链存储设备访问和入侵，或者存放存储设备的物理运行、访问环境中存在的安全风险。

■ **网络攻击威胁[S2]：**包括 DDoS 攻击、利用设备软硬件漏洞进行的攻击、病毒木马攻击、DNS 污染、路由广播劫持等传统网络安全风险。

■ **数据丢失和泄露[S3]：**针对区块数据和数据文件的窃取、破坏，或因误操作、系统故障、管理不善等问题导致的数据丢失和泄露，线上和线下数据存储的一致性问题等。例如，EOS 的 IO 节点可通过原生插件，将不可逆的交易历史数据同步到外部数据库中，外联数据库数据为开发者和用户提供了便利的同时，也可能引发更多的数据丢失和泄露风险。

2、协议层[P]：核心机制的安全缺陷

协议层结合共识机制、P2P 网络、密码机制等，实现区块链用户网络的构建和安全机制的形成。该层安全风险主要由区块链技术核心机制中存在的潜在安全缺陷引发，包括来自**协议漏洞**、**流量攻击**以及**恶意节点**的威胁等。

■ **协议漏洞[P1]：**包括针对共识机制漏洞的算力攻击、分叉攻击、女巫攻击[22]，以及利用 P2P 协议缺陷的 DDoS 攻击手段等。例如，2016 年 8 月，全球最大的比特币交易所之一 Bitfinex 因多重签名漏洞导

[22] 详见附录 1：区块链技术核心机制的潜在安全风险

致 12 万个比特币（约 6800 万美元）的损失；自 2016 年起，Krypton 平台、Shift 平台等区块链平台持续受到 51%算力攻击等。区块链协议层**不安全的协议以及协议的不安全实现**，给攻击者提供了大量的可乘之机，不仅影响整个区块链系统的一致性，也可能违背区块链的防篡改性。

■ **流量攻击[P2]**：攻击者可通过 BGP 劫持、窃听、TCP Flood 攻击等多种手段，接管区块链网络中一个或多个节点的流量，达到迫使区块链网络分割、交易延迟、用户隔离、交易欺诈等攻击目的。尽管目前并未有此类攻击案例被披露，但相关攻击代码已在部分网络开发社区[23]上公开。

■ **恶意节点[P3]**：完全公开透明的区块链——公有链对加入其中的用户不设任何访问授权机制，恶意节点可在加入后刻意扰乱区块链运行秩序、破坏正常业务；而私有链、联盟链中尽管设置了不同等级的访问权限控制机制，也可能存在恶意节点通过仿冒、漏洞利用等手段非法获取或提升权限进而开展攻击，或节点间联合作恶的情况发生。

3、扩展层[E]：成熟度不高的代码实现漏洞

目前，在区块链扩展层较典型的实现是智能合约或称可编程合约，由于智能合约的应用起步较晚，大量开发人员尚缺乏对智能合约的安全编码能力，其风险主要来源于**代码实现中的安全漏洞**。

■ **合约开发漏洞[E1]**：合约处理逻辑的正确性、完备性是智能合约的基本要求，由于智能合约的开发者能力、安全编码水平良莠不齐，

[23] GitHub：Hijack-btc test code，https://github.com/nsg-ethz/hijack-btc

或是出于利益原因，智能合约的开发中可能存在安全漏洞和后门，导致在区块链钱包、众筹、代币发行等智能合约典型应用中，不安全的代码实现可能导致合约控制流劫持、未授权访问、拒绝服务等后果。2016 年 6 月，以太坊 The DAO 智能合约递归调用漏洞被利用，导致约 1.5 亿美元众筹资金被劫持；2017 年，BEC、SMT 等智能合约漏洞频发。2018 年 3 月，国外学者通过对近 100 万份智能合约进行每份 10 秒的粗略自动化分析后发现，其中有 34200 份存在易利用的安全缺陷，并通过对其中 3759 份智能合约的抽样调查，以高达 89%的概率确认了 3686 份智能合约中的漏洞存在[24]。

■ **合约运行安全[E2]：**作为区块链 2.0 的核心，智能合约运行环境的安全性是区块链安全的关键环节，目前，部分区块链项目会设计并使用自己的虚拟机环境，如以太坊的 EVM，而 HyperLedger Fabric 等则直接使用成熟的 Docker 等技术作为智能合约的处理环境，一旦在运行环境中存在虚拟机自身安全漏洞，或验证、控制等机制不完善等，攻击者可通过部署恶意智能合约代码，扰乱正常业务秩序，消耗整个系统中的网络、存储和计算资源，进而引发各类安全威胁。

4、应用层[A]：各类传统安全隐患集中显现

应用层直接面向用户，涉及不同行业领域的应用场景和用户交互，该层业务类别多样、交互频繁等特征也导致各类传统安全隐患集中，成为攻击者实施攻击、突破区块链系统的首选目标。应用层安全风险涉及**私钥管理安全、账户窃取、应用软件漏洞、DDoS 攻击、环境漏洞**

[24] 数据来源：Finding the greedy, prodigal, and suicidal contracts at scale

等。

■ **私钥管理安全[A1]：**私钥的安全性是区块链中信息不可伪造的前提[25]，区块链中用户负责生成并保管自己的私钥于本地，并可能根据使用需求在单点或多点进行私钥文件备份，该环节不安全的存储可导致私钥文件泄露或被窃取，威胁用户数字资产安全。

■ **账户窃取[A2]：**攻击者可利用病毒、木马、钓鱼等传统攻击手段窃取用户账号，进而利用合法用户账号登录系统进行一系列非法操作。2018 年 3 月 7 日，虚拟货币交易所币安的大量用户账户被窃取，攻击者利用被盗账户登录后，通过大量抛售等金融手段做高自己持有的虚拟货币种类价格，随后卖空离场实现获利。

■ **应用软件漏洞[A3]：**应用层的开源区块链软件中存在大量因开发问题而引发的输入验证、API 误用、内存管理等安全漏洞。根据 2016 年 10 月国家互联网应急中心发布的《开源软件源代码安全漏洞分析报告—区块链专题》报告[26]，在 25 款主流区块链开源软件中存在高危漏洞 746 个、中危漏洞 3497 个，可能导致系统运行异常、崩溃，或实现越权访问、窃取私密信息等。

■ **DDoS 攻击[A4]：**在区块链应用中，除对底层协议缺陷的 DDoS 攻击外，攻击者也可在应用层发起针对性的 DDoS 攻击，影响各类应用业务的可用性。根据云计算安全服务提供商 Incapsula 发布的 2017 年第四季度 DDoS 威胁报告[27]，应用层 DDoS 攻击数量较前一季度成倍

[25] 详见附录 1：区块链技术核心机制的潜在安全风险

[26] http://if.cert.org.cn/res/web_file/bug_analyze_report.pdf

[27] Global DDoS Threat Landscape Q4 2017, https://www.incapsula.com/collateral/2017-q4-ddos-threat-landscape.pdf

增长，且针对加密货币行业的攻击数量持续增长，占所有攻击数量的3.7%。

■ **环境漏洞[A5]：**区块链应用所在服务器上的恶意软件、系统的安全漏洞、配置不当的安全管理策略等都可能成为攻击者攻破区块链应用的脆弱点。在 2011 年比特币交易所 Mt.Gox 被攻击、2017 年热钱包应用 Gatecoin 被盗等事件中，攻击者都是通过攻击区块链应用或数据所在服务器，间接盗取账户资产获利。

（三）区块链技术给安全监管带来的挑战

如前所述，除区块链技术架构本身存在的安全风险之外，其去中心、自治化、难更改、强匿名等特点也给现有网络和数据安全监管手段带来了不少挑战，具体表现在：

一是隐匿性强，增加了网络安全事件和网络犯罪的追踪溯源难度。区块链中用户账户由随机数字、字母和用户公钥生成，不直接包含网络地址、设备地址等信息，更不关联手机号、住址等与用户真实身份强相关的各类信息。区块链难以追溯的特性在一方面导致了对恶意网络行为、攻击事件等追溯更加困难；另一方面，也助长了不法分子网络犯罪的气焰，勒索病毒、暗网交易等往往利用基于区块链技术的加密货币收取赎金、实施结算以逃避溯源。根据澳大利亚研究小组[28]于 2018 年发布的一份比特币交易报告显示，使用比特币进行结算的违法交易规模已达到 720 亿美元/年。此外，基于区块链的隐匿性较强的即时通信工具也可成为不法分子用以通联交互的工具，为用户提供

[28] 由来自悉尼大学、悉尼科技大学和里加斯德哥尔摩经济学院的几位经济和金融领域专家组成

身份隐藏、通信内容加密等功能，难以实施有效监管手段。

二是无中心化特性导致威胁面扩大，技术接口难以实施。区块链中开源的共享协议可使数据在所有用户侧同步记录和存储，对攻击者来说，能够在更多的位置获取数据副本，分析区块链应用、用户、网络结构等有用信息；但对监管方来说，在区块链模式下，区块中的数据采用分布式方式存储在用户节点，而不再集中化存储，用户的通信数据也通过点对点的方式进行传输，无需经过集中的服务器或平台，导致监管数据的采集和获取困难，监管技术接口难以实施。

三是防篡改特性为有害信息形成天然技术庇护，给信息内容管理带来挑战。区块链中数据写入时，需要大部分节点通过共识机制进行裁决，决定是否同意写入，并设置了时间戳机制记录写入时间，以实现禁止对历史记录的修改。因此，一旦暴恐、色情等有害信息被写入区块链中，不但可利用其同步机制快速扩散，也难以进行修改、删除。尽管理论上可采取攻击手段制造硬分叉、回滚等，但实施代价高、难度大，给信息内容管理带来新的挑战。在 2018 年 3 月，德国研究人员就曾在比特币区块链中发现超过 274 份儿童色情网站的链接和图片，经查证，为恶意用户通过将有害信息编码为比特币交易信息，注入区块链中的行为。

四是数据安全责任边界模糊，可能违背数据跨境、数据可删除等监管要求。区块链能作为各类应用的底层技术，实现上层应用间的交互操作，如医疗、金融、通信等行业的数据都通过区块链公司提供的技术平台存储在用户侧，其应用过程中涉及到区块链平台、应用、数

据所有者等多方主体，易导致安全责任界限的模糊。此外，区块链可在所有用户侧创建和维护完整的数据库，一旦有新的数据写入，所有用户侧可同时更新，因此，一旦涉及到境外节点加入，这种天然自组织性将使得自发、频繁的跨境数据流动成为必然。另外，欧盟 GDPR 中关于数据纠正、删除等权利的规定也似乎与区块链防篡改的技术核心格格不入。

三、风险应对框架

区块链技术的安全应用需综合考虑其技术架构本身，以及应用在不同场景中可能面临的各类安全风险。基于区块链技术的系统应用普遍拥有较高的复杂度，需要根据存储层、协议层、扩展层、应用层等不同层面的风险来源和成因，从编码、部署、管理等环节实施针对性的应对措施以降低风险，如图 3.1 所示。

			应对措施									
			安全开发	代码审计	安全评估和测试	安全配置	输入校验	加密存储/传输	节点/数据安全验证	身份认证和权限管理	流量清洗	必要的安全防护产品/服务
安全风险	存储层[S]	S1.基础设施安全风险			● Δ	● Δ		● Δ				● Δ
		S2.网络攻击威胁									● Δ	● Δ
		S3.数据丢失和泄露				● Δ		● Δ				● Δ
	协议层[P]	P1.协议漏洞	●	●	● Δ		●					
		P2.流量攻击						● Δ		● Δ	Δ	Δ
		P3.恶意节点				● Δ		● Δ	● Δ	● Δ		● Δ
	扩展层[E]	E1.合约开发漏洞	●	●	●	●	●					
		E2.合约运行安全			● Δ	● Δ		● Δ		● Δ		
	应用层[A]	A1.私钥管理安全				● ◎ Δ		● ◎ Δ				
		A2.账户窃取								● Δ		● ◎ Δ
		A3.应用软件漏洞	●	●	● Δ		●					● ◎ Δ
		A4.DDoS 攻击					●				● Δ	● ◎ Δ
		A5.环境漏洞			● Δ	● ◎ Δ	●	● ◎ Δ				● ◎ Δ

图例：● 区块链开发者◎区块链用户 Δ 区块链平台运行者

图 3.1 区块链风险应对框架

其中，

■ **安全开发：**区块链技术在比特币中的成功实践表明，严谨的技术规范是技术健康有序应用的重要前提，包括**区块链应用开发者、智能合约开发者、区块链平台开发者等**在内的各类区块链开发者，都应实施规范的开发流程，使用规范的开发和编译工具，预留充分的上线试运营周期等，降低编码过程中引入安全风险的几率。

■ **代码审计:**近年来屡屡发生的交易所被攻击、虚拟货币被盗窃等事件中，有大量事件是由于代码层面的安全问题所引发，而区块链开源的特性也使得攻击者可以便捷地获得代码，通过分析代码的逻辑缺陷找到攻击突破口。因此，区块链开发者应在产品上线发布前，采用自动化或人工的方式，对代码架构、逻辑流程、关键功能模块开展足够的静态代码分析、交互式代码审计等源代码安全检查工作，以检查代码中的安全缺陷和安全隐患。

■ **安全评估和测试：**通过对区块链技术架构、应用场景、攻击模式等开展针对性的安全评估和测试，及时识别运行环境、基础设施、核心协议、智能合约以及应用软件等各层面存在的安全漏洞，发现和和采取措施应对安全风险；对算力的集中度、节点的分散度以及基础设施的可靠性和安全性进行评估。一方面，区块链开发者可借助贯穿开发生命周期的安全评估和测试，在相关产品投入市场前及时降低产品安全隐患；另一方面，区块链平台、系统的运行维护者也可在产品运行过程中定期或不定期地开展安全评估和测试，及时发现和解决安全问题。

■ **安全配置**:在区块链技术应用过程中，软件、硬件、协议、系统等层面不安全的配置也可能成为引入安全风险的原因，如开放了不必要的系统服务访问、设置了不当的权限管理原则等。为此，区块链平台、系统的运行维护者需要实施安全的配置以限制脆弱性的暴露，从各方面缩小攻击面，包括关闭和限制不必要的服务和端口，对系统资源、用户权限等采用“最小特权原则”管理，合理部署智能合约外部调用接口安全参数，为私钥文件配置硬件冷备份，尽量引入无关联利益关系的实体以降低节点间联合作恶的可能性等。

■ **输入校验：**实施输入校验的目的是从入口侧降低输入数据对业务逻辑的影响，包括对区块链交易平台 Web 端、智能合约输入变量等参数的合理妥善校验。鉴于输入数据与业务逻辑之间曲折复杂的关联关系，尽管输入校验无法完全解决 DDoS 攻击、利用漏洞的攻击等安全问题，但区块链开发者仍应对区块链应用层、扩展层、协议层等不同层面的输入进行合法性校验，以降低恶意代码执行和逻辑错误风险。

■ **加密存储/传输**:一方面，私钥的安全管理是所有非对称加密系统中安全保障的重要环节，区块链中也不例外。与明文存储的私钥相比，采取加密存储的方式可大大降低私钥信息泄露的可能性；亦可将加密存储应用于重要配置文件、核心数据库记录中，以减少各类数据泄露风险。另一方面，在协议层、扩展层等层面可通过部署 TLS 等可靠的加密传输，在一定程度上防止恶意节点攻击、流量窃取或劫持，以及针对合约运行安全的攻击方式等。

■ **节点/数据安全验证：**区块链中，各节点根据共识机制共同维

护网络和相关业务的有序进行，试图向区块链中植入恶意节点也成为攻击者控制区块链，窃取经济利益和实施破坏的主要手段，因此，针对区块链网络中的未授权节点或恶意节点实施必要的节点/数据安全验证，可有效减弱因恶意节点带来的安全隐患。

■ **身份认证和权限管理**:与节点/数据安全验证类似，必要的身份认证和权限管理也是对区块链用户、节点和操作进行安全控制的有效手段，以应对协议层可能出现的未授权节点、流量攻击，以及因验证控制机制不完善引发的智能合约运行安全问题等。

■ **流量清洗：**主要针对存储层、协议层、应用层等不同层面可能面对的流量攻击威胁，尤其是 DoS、DDoS 攻击威胁，通过对流量的实时监控，及时识别和剥离隐藏在网络流量中的异常攻击流量，可以服务、产品或内嵌安全功能的模式按需在区块链应用场景中部署。

■ **必要的安全防护产品/服务**:防火墙、入侵检测、WAF、安全审计等传统安全的部署尽管未必能解决所有层面的安全问题，但能从各自的角度实施针对性的防护，持续监测发现异常交易、异常节点行为、安全漏洞等，对各类安全事件进行及时处理响应，给区块链系统、平台等带来整体安全性的提升，间接提高攻击者发起攻击的成本和被发现的可能性。任何技术的安全的落地应用，都离不开必要的安全防护产品或服务的有效部署，区块链也不例外。

四、促进区块链技术安全应用的建议

区块链技术正日益成为金融支付、供应链管理、公共服务等领域创新的重要驱动力量，其技术带来的巨大变革不容忽视，技术和应用场景中的潜在安全风险也在逐渐显现。我国在着力把握技术发展先机的同时，也需正视风险，从发展引导、强化监管、风险研判、国际合作等多角度积极应对，有效防范化解新技术安全风险，切实保障区块链技术的健康、有序发展。

（一）强化应用领域引导，鼓励区块链自主可控开发

一是加强对区块链应用领域的正确引导。政府部门应加强对区块链技术发展、应用领域的正确引导，如鼓励“区块链+网络安全”应用模式的探索，以应用试点等模式，推动区块链技术在提升认证安全性、保障关键信息基础设施安全、强化数据存储安全等方面的应用落地；在金融、物联网、工业等领域，在安全风险相对可控的前提下鼓励区块链解决方案的开发和探索；在公共服务、大众媒体等领域，应对利用区块链传播有害信息、恶意代码等风险加强警惕，探索对链上违法信息审核与用户隐私保护需求间的平衡。**二是强化推动区块链安全产品和服务市场发展。**鼓励网络安全企业、区块链相关企业等重视区块链技术安全问题，推动智能合约漏洞挖掘、区块链产品代码审计、业务安全监测等相关安全产品和服务的开发应用，提升区块链产品应用安全水平和抗攻击能力，不断优化区块链技术生态结构；**三是鼓励自主可控的区块链平台和应用开发。**当前，区块链的核心技术机制中仍存在很大的完善空间，且比特币、以太坊等主流的区块链技术平台

均发源于国外。因此，应鼓励区块链开发者进行自主可控的平台和应用开发；鼓励国内重点企业、科研机构、高校等加强合作，加快对共识机制、可编程合约、分布式存储、数字签名等核心关键技术的攻关；逐步推行区块链中加密算法的国产化替代；形成具有我国自主产权的技术成果，打造更加符合国家安全要求的自主可控的区块链平台，为众多应用的发展与落地保驾护航。

（二）创新监管手段，强化区块链平台和应用监管力度

一是探索创新性的区块链监管手段。探索“沙盒监管”、“穿透监管”等区块链监管模式，监管机构可为特定区块链产品、服务和应用模式的测试创新构造“安全沙盒空间”，在满足企业在真实场景中测试其产品方案需求的同时，严防风险外溢；或在区块链节点中设置一个或多个监管机构节点的方式，使监管方可全面及时获取区块链业务流程、用户关系、信息流向等监管信息，以“穿透式”的方式深入区块链业务核心实施监管。**二是加强区块链平台和应用的监管力度。**对于区块链行业应用平台，推动建立行业监管、安全监管等的跨部门备案制度；明确区块链开发者、区块链用户、区块链平台运行者等不同角色的安全责任；推动国内区块链应用平台的用户实名注册；探索对拟采取区块链技术存储的业务和用户数据实行数据安全分类分级、风险评估制度；强化区块链平台、应用等安全评估评测要求，提升对平台和应用的管控程度。**三是打造区块链安全监测和监管平台技术实力。**建设区块链安全监测和监管技术平台，识别区块链平台应用，全面掌握区块链相关安全漏洞、攻击事件和安全威胁发展态势，探索对重大

异常、安全事件的溯源追踪手段，技管结合，打造区块链安全监管硬实力（详见附录 4）。

（三）强化技术风险研究，夯实安全风险应对技术基础

一是针对区块链安全风险开展持续性、常态性研究。深入研究区块链技术架构中各层独有安全风险、跨不同层次的接口安全风险等，根据区块链技术发展变化情况，持续开展区块链技术和应用安全风险研判，对区块链核心机制潜在风险、常换时新的攻击威胁，非法组织、犯罪分子等利用区块链的模式等进行跟踪评估，加强对区块链安全风险的认识。**二是集中力量攻关区块链风险应对技术。**针对区块链存储层、协议层、扩展层、应用层等各层安全风险，研究部署覆盖编码、部署、管理等环节的风险应对措施；如探索对浏览器历史记录、设备 MAC 地址等的多维信息分析技术，实现区块链行为取证分析和用户身份追溯，发展加密环境下有害信息发现、协议逆向分析等风险应对技术等。

（四）加强区块链网络犯罪风险防范，促进国际合作治理

为应对利用区块链开展网络犯罪的全球化趋势，需要：**一是积极凝聚国际共识，深化全球监管合作。**以构建网络空间命运共同体为目标，积极推动区块链违法犯罪在定罪标准、管辖协调、情报共享以及司法协助等方面的国际共识与合作。**二是探寻跨国治理有效手段，**提升对区块链违法犯罪行为的及时预警、证据留存、犯罪追溯等领域的跨国实操水平，在一定范围内加强各国区块链应用数据的开放共享程

度，以充分利用大数据分析等技术手段，对区块链应用中的用户通信行为和内容进行挖掘分析，及时发现可疑行为。针对利用区块链应用进行网络犯罪的涉案人员，在必要时候，可采取网络技术侦查等特殊手段进一步深入调查，实现对用户身份、通信行为和内容的追溯排查。

附录 1 针对区块链技术核心机制的典型攻击

（一）以共识机制为目标的针对性攻击

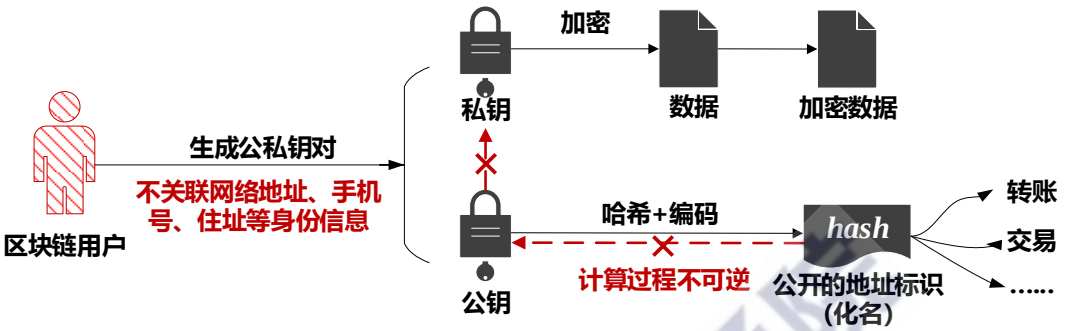
共识机制是维持区块链系统有序运行的基础，相互间未建立信任关系的区块链节点通过共识机制，共同验证写入新区块中的信息的正确性。区块链中使用的共识机制有很多，包括 PoW（Proof of Work，工作量证明机制）、PoS（Proof of Stake，权益证明机制）、BFT（Byzantine Fault Tolerance，拜占庭容错机制）等。目前，PoW、PoS 和 DPoS（Delegated Proof of Stake，委托权益证明）机制已经过大规模长时间的实践检验，发展较为成熟。但在区块链共识机制的长期发展应用中，也衍生出了算力攻击、分叉攻击、女巫攻击等大量**针对性的攻击手段，造成链上记录被篡改**等后果，如表附 1-1 所示：

表附 1-1 以区块链共识机制为目标的典型攻击

攻击类型	攻击对象	攻击手段	影响
分叉攻击	PoW PoS	一个或多个节点通过控制全网特定百分比以上算力/数字资产，利用这些算力/数字资产隐秘计算新区块（攻击区块），构造区块链分叉，并在攻击区块达到一定长度之后向所有节点释放，迫使节点放弃原区块	篡改分叉后攻击者账户数据，实现双重支付，可导致链上记录回滚（可达数月）
女巫攻击	PoW PoS DPoS	攻击者生成大量攻击节点并尽可能多的将攻击节点植入网络中，在攻击期间，这些被称为女巫节点的攻击节点将只传播攻击者的块，导致攻击者算力无限接近于 1	实现攻击者对区块链网络的高度控制权
贿赂攻击	PoS	攻击者购买商品或者服务，商户开始等待区块链网络确认交易，此时攻击者开始在网络中首次宣称，对目前相对最长的不包含本次交易的主链进行奖励。当主链足够长时，攻击者开始放出更大的奖励，奖励那些在包含此次交易的链中挖矿的矿工。六次确认达成后，放弃奖励。货物到手，同时放弃攻击者选中的链条。	以小于货物或者服务费用的成本获利
预计算攻击	PoS	将某一时间段内计算出的新区块扣留不公开，等到挖到第二块新区块后同时公布	攻击者所在分叉成为最长链

（二）地址不具名机制对攻击者身份追溯的挑战

区块链中使用非对称加密方法，除了可以让用户使用自己的私钥对写入数据进行加密外，还会对用户的公钥进行哈希运算，生成特定格式的字符串作为公开的用户地址以标识用户，如图附 1-1 所示。



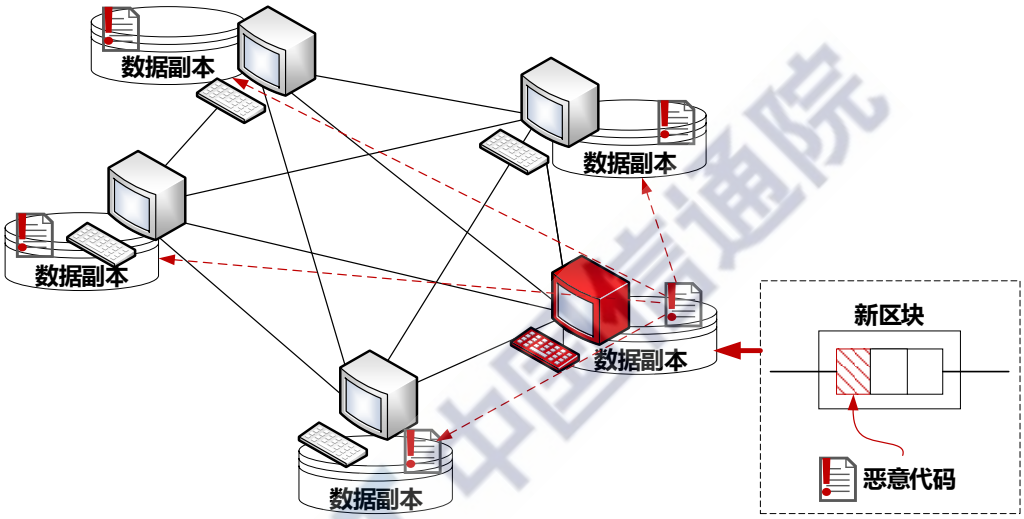
图附 1-1 区块链中不具名的地址生成机制

通过此种方法生成的地址标识将被作为用户的“化名”，用户可利用一个或多个“化名”在区块链应用中开展各类转账、交易等活动。在大多数情况下，“化名”的生成只需要几串随机的数字、字母和用户公钥，不包含网络地址、手机号、住址等与用户真实身份相关联的信息。因此，尽管这种“化名”或者说不具名的机制能够在一定程度上保护用户的隐私，但也导致恶意行为难以追溯到人，造成**网络安全溯源环节中从网络身份到社会身份的脱节**。

（三）分布式存储机制对攻击威胁面的扩大

区块链通过构建开源的共享协议，实现数据在所有用户侧的同步记录和存储。与传统中心式数据库在一个或几个中心集中存储数据的方式不同，在区块链系统中，所有用户侧均有可能存放完整的数据拷贝，因此，单个或多个节点被攻击均不会对全网数据造成毁灭性的影响，提高了存储的可容错性。但是这种分布式的存储机制也在一定程

度上扩大了安全威胁面：**一是攻击者可以在更多的位置获取数据副本，**分析区块链应用、用户、网络结构等有用信息；**二是全网的安全性升级将耗费更多时间和资源，**导致一旦发生有效的攻击，对区块链系统的影响将更具持续性；**三是恶意节点可在新区块中嵌入病毒、木马等恶意代码，**利用分布式机制自发向全网传播，伺机发起网络攻击。如图附 1-2 所示：



图附 1-2 区块链分布式存储机制可能扩大安全威胁面

（四）针对密码学机制固有安全风险的各类攻击

非对称算法、哈希函数等密码学机制在区块链中的应用解决了消息防篡改、隐私信息保护等问题，但这些密码学机制的固有安全风险仍未在区块链系统中得到解决，仍将面临由私钥管理、后门漏洞等引发的各类攻击。**一是通过窃取私钥威胁用户数字资产安全。**私钥的安全性是区块链中信息不可伪造的前提，在区块链中，私钥由用户自行生成并负责保管，一旦私钥丢失，用户不仅无法对数据进行任何操作，也无法使用和找回其所拥有的数字资产，造成无法挽回的损失。**二是 ECC、RSA 等复杂加密算法本身以及在算法的工程实现过程中都可能**

存在后门和安全漏洞，进而危及整个区块链系统和其上承载的各种应用的安全性。**三是**随着**量子计算技术的飞速发展，**大量子比特数的量子计算机、量子芯片、量子计算服务系统等相继问世，可在秒级时间内破解非对称密码算法中的大数因子分解问题（破解 1024 位密钥的 RSA 算法只需数秒），也成为区块链技术面临的典型攻击手段之一。

附录 2 国外区块链网络安全相关实践

方向	细分领域	详细信息	代表性企业/项目
区块链 安全问题应对	基础设施安全	“安全区块链云环境”服务，帮助企业测试和运行需要处理私人或敏感的数据的区块链项目	IBM
	攻击应对	在区块链中创建某种“交易配置文件”，监控特定区块链上的交易，检测包括 51%攻击、Sybil 攻击等恶意攻击	英国电信
	业务追溯	通过对区块链上的数字货币进行追踪和分析，来打击网络违法犯罪行为	Chainalysis
	项目安全管理	审计和合规解决方案	Gecko Governance
		区块链项目的自我监督和管理	Ventureum
	代码安全	智能合约的代码安全审计	EOSCANADA
		通过深度规范技术进行代码安全验证和审计，包括区块链智能合约、协议、算法、钱包 APP 等代码的渗透性测试和安全验证	CertiK

方向	细分领域	详细信息	代表性企业/项目
区块链 网络安全应用	攻击发现 和防御	开发可用于验证国土安全部在美国南部边境所部署各类安全设备采集数据的区块链技术方案，确保采集数据完整，识别篡改行为	DHS+Factom
		建设区块链研究实验室，以确定区块链技术是否可用于识别网络攻击，并保护关键基础设施	俄罗斯研究机构 ERA
		为数据或系统的状态创建时间戳哈希，根时间戳哈希对状态持续监测，以发现文件、系统或程序是否受到未授权访问，目前已在英国核电站、防洪系统等国家关键基础设施应用	Guardtime
		构建分布式网络，在受到攻击时可连接到附近的保护池，并将贷款分流到其他节点和网站	Gladius
	安全认证	构建防篡改的区块链技术平台，通过设备网络大规模分发私人数据和身份验证，通过安全认证保护边缘设备	Xage
		基于区块链技术，将物联网设备唯一身份签名到物理项目，以确认设备身份的真实性	英国马恩岛政府
	安全域名	将域名基础设施建立在区块链之上，建立域名哈希映射，在每个网络节点处进行域名注册、转移等操作，存储域名所有人的公私钥对并记录解析后的域名，分散了原本集中的域名服务，由于不存在可被黑客攻击或修改的中央记录，也防止了域名劫持、缓存投毒等传统攻击	Blockstack
		使用 Ethereum 区块链和 IPFS 注册和解析域名	Nebulis

方向	细分领域	详细信息	代表性企业/项目
区块链 网络安全应用	信任基础设施建立	基于区块链的PKI，将区块链作为域名和公钥的分布式账本，实现公共和可审计的PKI	CertCoin
		使用区块链来存储颁发和吊销证书的散列	Pomcor
	安全通信	将物联网传感器数据直接编码到区块链中，为分散交互和交换提供安全的基础	Startup Filament
		使用区块链保护在聊天、短信应用和社交媒体中交换的私人信息，将用户元数据随机保存在分类账中	Obsidian
		使用区块链创建安全且无法通过外部攻击的消息服务	DARPA
	数据安全存储	将患者身份特征、疾病情况、治疗方案等医疗数据哈希后存储在区块链中，使用多签名技术制定访问规则，用户只有在被授权情况下，才能创建、共享和更新病例，在保障数据安全的同时，提高医疗行业效率和透明度	Gem
		基于区块链，依赖硬件安全模块（HSM）保护用户数据安全	埃森哲
			HyperLedger
		基于区块链，提供可审计、合规的数据完整性保障服务	爱立信+GE

附录 3 我国企业区块链网络安全相关实践

（一）中国移动研究院：基于区块链管理 PKI 数字证书

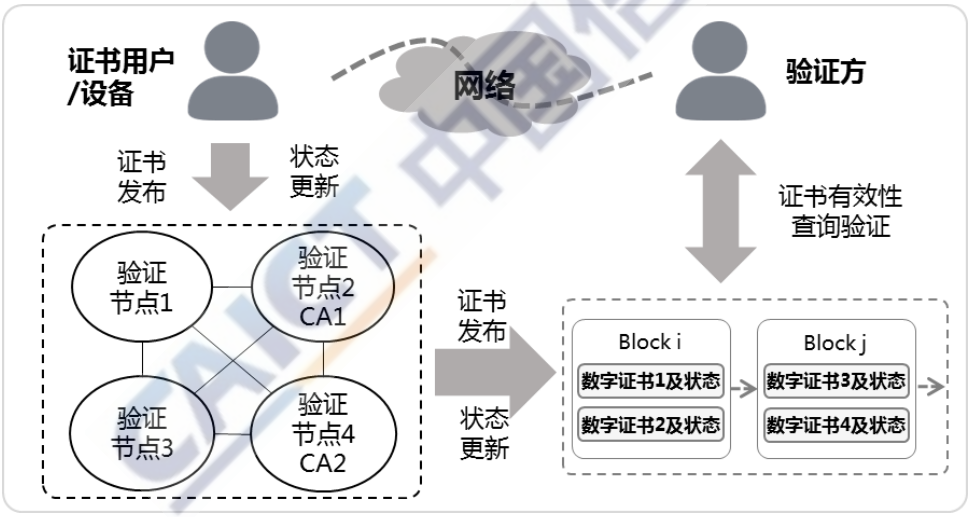
传统 PKI 技术中，CA 中心（Certificate Authority，证书认证机构）是信任的起点，只有信任某个 CA，才信任该 CA 签发的数字证书。但在具体应用中，处于核心的 CA 极易遭受攻击，一旦被控制，CA 根证书以及该 CA 已经签发的证书都不再可信，目前已经发生多起 CA 被攻击导致证书不可信的安全事件，荷兰 CA 机构 DigiNotor 曾因遭受此类攻击导致破产。此外，用户在配置和使用证书时，需要首先向 CA 中心申请证书，CA 中心签发证书后，用户需要将签发的证书配置或安装至目标设备或服务器中。在移动通信网、物联网、车联网等场景中，由于涉及数量巨大的网络设备和终端设备，由于私钥和证书的个体差异，导致批量配置设备证书效率较低。最后，用户证书只能由所属 CA 的根证书进行验证，不同 CA 之间不能相互验证。

在区块链中，一旦数据通过共识之后记录到区块链中，那么数据就被所有参与方认可。若将通过共识的数字证书记录到区块链中，那么这些数字证书就可以被区块链所有参与方认可。区块链没有中心化的信任节点，区块链数据也以分布式的方式存储于多个节点之中，破坏任意节点均不会导致区块链数据丢失，区块链可以解决传统 PKI 技术单点失败问题。

区块链没有中心化信任节点，因此可以实现证书用户自行生成证书，区块链节点按照规则判断证书是否真实，将真实有效的证书记录到区块链当中，这样可以提升证书批量配置的效率。特别的，如果参

与共识的节点仅限于传统 CA 机构，那么就在多个 CA 机构之间建立起信任关系，可以解决多 CA 互信难的问题。

基于上述特点，基于区块链的 PKI 数字证书管理系统可以确保记录到其中的数字证书的安全可信。在该系统中，证书用户可自行生成一份数字证书，将数字证书提交给区块链系统进行验证和共识，通过验证和共识之后，该数字证书及其状态就记录到区块链系统中。在证书使用过程中，以 TLS、IPSec 等安全协议为例，证书用户需要将证书提交给认证方，认证方接收到证书后，通过区块链系统检查证书的正确性和有效性，如图附 3-1 所示。



图附 3-1 基于区块链的 PKI 数字证书管理系统

基于区块链的 PKI 数字证书管理系统可以用于 4G 小基站（又称为 HeNB，Home evolved Node B，家庭演进基站，简称家庭基站）场景。4G 小基站是一种利用小型化、低功率蜂窝技术，通过固网宽带接入到移动核心网，为用户提供包括传统蜂窝移动通信基础业务在内的固定移动融合业务。HeNB 与安全网关之间采用数字证书进行设备双

向认证。因此，4G 小基站在入网提供蜂窝移动通信服务之前，需要向 CA 申请并配置数字证书。传统方式需要大量人工参与证书申请和配置，效率和安全性较低。

采用基于区块链的 PKI 数字证书管理系统，工厂在制造小基站设备时产生公私钥对以及自签名数字证书，通过厂商节点在区块链 PKI 数字证书管理系统中发布证书，区块链节点依据共识机制形成共识，将经过共识的证书记录到区块链中，即可完成证书的配置。该流程将传统方式中“设备商申请证书——CA 签发证书——设备商下载证书—设备商配置证书”的过程，简化为“设备产生和配置证书——设备商发布证书”，可有效提高证书配置效率和安全性。

（二）360：EOSIO-BP 节点和钱包 APP 安全审核方案

- EOSIO-BP 节点安全

EOSIO 是类似操作系统的区块链体系架构平台，旨在实现去中心化分布式应用的性能扩展，提供帐户、权限验证、数据存储和异步通信，实现跨 CPU 核心和集群的应用程序调度，每秒可以支持数百万个交易，同时普通用户无需支付使用费用。在 EOS 生态中，区块由 21 名生产者（即 EOSIO-BP 节点）轮流产生。

按 EOSIO 目前的设计，每半秒一个节点出 6 个块，每个块会容纳成百上千个交易，这样的高并发设计对集群架构和安全策略构成了一个挑战：如何尽量减少各个区块的同步时间，在保障出块节点安全的情况下尽量加速区块的同步；同时，为用户提供高效的合约调用服务，针对恶意流量要能进行针对性识别，不同场景使用不同的安全防

护策略。

360 的 EOSIO-BP 节点安全方案将出块节点放在 P2P 和 HTTP 节点集群后以保障出块节点的安全。在出块节点的前端，严格限制访问策略，只有信任的节点才可以接入到出块节点。在出块节点的后端，部署专门的安全管理堡垒机，对出块节点的私钥进行管理。依托 360 安全大脑的积累，分别在物理安全、平台安全、网络安全、系统安全、应用安全和数据安全六方面进行防御部署，并将安全设备以及日志等信息发送到 EOS 超级节点智能感知系统，如图附 3-2 所示。

图附 3-2 “安全大脑”组成

依托安全大脑分布式智能系统，针对 EOS 超级节点的功能和架构，360 量身定做了 EOS 超级节点智能感知系统，该系统作为 360 安全大脑数据采集的重要环节，将与云端的 360 安全大脑进行联动，用人工智能的方法进行分析和计算，来实时感知网络安全运行状况和安全态势，预测可能要发生的攻击，监测和发现正在发生的攻击，发现攻击后就自动响应，协同分布在网络中的网络安全设备和软件对攻击进行处置，支撑应急指挥。

- **钱包 APP 安全审核方案**

随着各种数字货币的诞生，为了方便用户记录地址和私钥，官方

会同时发布全节点钱包，例如 Bitcoin Core、Parity 钱包，同时也有一些第三方公司为了进一步提高用户体验，相继开发了如比特派、imToken、AToken、币信、币包等钱包 APP，它们并不同步所有的区块数据，因此称其为轻钱包，这两种数字钱包都属于热钱包。冷钱包也称为硬件钱包，常见的冷钱包有库神钱包、Ledger Nano S、Trezor 等，由于私钥不接触网络，相对安全性也较高。不过由于业务场景的快速迭代以及推广需求，无论热钱包还是冷钱包都会有一些的安全隐患会被忽视。

基于我们对当前数字钱包 APP 的安全现状分析，360 可对热钱包的 App 端和服务端进行安全审核，App 端安全审核范围如图附 3-3：

图附 3-3 APP 端安全审核覆盖范围

其中运行环境安全检测包括：手机系统漏洞扫描、Root 环境检测、APP 完整性检测、网络代理检测、网络安全检测；协议交互安全检测包括：新用户注册安全、创建交易安全、交易签名安全、交易完毕确认、余额查询安全；数据存储安全检测包括：助记词创建安全、助记词存储安全、私钥生成安全、私钥储存安全、本地存储数据敏感性检测；功能设计安全检测包括：导入钱包功能安全、交易密码安全、用户输入安全、转账地址安全检测、助记词，私钥网络储存安全、https

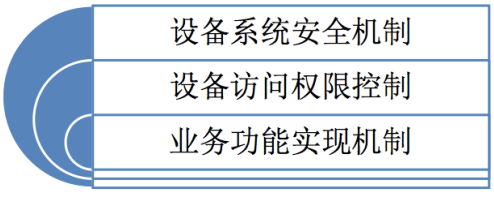
通信中的证书校验。

而服务端作为区块链数字钱包的中心化对象，显然已是黑客十分青睐的攻击目标，安全是其健壮运行的核心基石。基于对当前数字钱包服务端的安全现状分析，可将相关审计点归纳总结如图附 3-4。

图附 3-4 APP 端安全审核覆盖范围

其中，域名 DNS 安全检测包括域名注册商安全检测评估、域名记录安全检测、DNS 服务安全检测、TLD/gTLD 安全检测、全网多节点 DNS 解析监测、证书安全；主机实例安全检测包括：口令安全、系统安全、访问控制、日志审计、冗余安全、云 IAM 授权检测；服务端应用安全检测包括：代码安全、服务应用安全、环境隔离、云存储。

针对冷钱包目前是使用趋势，实际上是将密钥保存在了硬件芯片当中，但依然会存在诸多安全风险，冷钱包安全审核方案如图附 3-5 所示。



图附 3-5 冷钱包安全审核覆盖范围

其中，设备系统安全机制包括：硬件钱包是否存在联网控制、硬件钱包系统安全检测、硬件钱包系统漏洞更新机制、设备丢失锁定方

案；设备访问权限控制包括：是否允许用户对设备进行连接调试、是否允许用户对设备存储区进行读写、是否允许用户对设备内存进行转储分析、是否采用加密芯片；业务功能实现机制包括：设备使用密码设置、创建钱包助记词安全、交易过程安全、数据存储安全、系统完整性安全。

（三）腾讯：区块链安全应用及应对实践

- **“守护者计划[29]”—区块链安全威胁全面感知**

近年来，移动互联网高速发展，基于公有链上的加密数字货币概念逐渐被公众认知接受。由于网络黑产犯罪的趋利性，目前涉及区块链的黑产主要集中在以公有链为主的数字货币及其算力等衍生方面，围绕着公有链及加密数字货币的网络攻击和安全风险逐渐显现。

因为公有链加密数字货币在非法交易中的广泛应用，“挖矿”也成为热门行业。黑产人员采取网络手段，非法控制他人计算机系统，为其“挖矿”牟利。

根据腾讯守护者计划的安全态势感知，挖矿木马、勒索病毒、漏洞攻击等安全威胁持续上升，位于用户前端的病毒、木马的活跃量，在 2018 年呈现明显回升趋势。黑产利用病毒、木马感染形成僵尸网络挖矿，获取暴利已成为一大趋势。

1、蠕虫病毒控制计算机挖矿

目前，国内已发现利用与 Wannacry 勒索病毒相同的“永恒之蓝”漏洞制作传播挖矿木马的黑客行为。**2018 年 5 月，腾讯守护者计划**

[29] 腾讯于 2016 年 4 月推出的打击电信网络违法犯罪的联合公益平台

协助广东警方打掉该挖矿木马黑产团伙。

2、病毒、木马感染形成僵尸网络挖矿

根据腾讯统计，现已发现的挖矿类僵尸网络超过 20 个，规模较大的有 PhotoMiner、Myking、WannaMiner、JBossMiner、NrsMiner 等。这些僵尸网络感染的用户量级均在百万以上。

在我国，存在黑产团伙利用在热门游戏外挂、盗版视频软件和网吧渠道植入木马来“挖矿”的情况。**2018 年 4 月，腾讯守护者计划协助国内警方破获利用“tlminer”等近百款木马，非法控制 389 万台计算机，用僵尸网络集群算力进行“挖矿”牟利的系列案件，刑事打掉一个公司通过运营开放式木马平台、公开招募代理进行木马投毒实施挖矿，非法获利过千万元的黑产团伙。**

- **抗篡改的司法联盟链**

在司法存证安全领域存在公正与记录的流程长，证据鉴定慢，记录可能存在造假风险等问题。同时传统的存证记录保全过程中，客户的维权成本较高。区块链所具备的防篡改、不可伪造、多方参与、线上操作等特性可以在真实业务场景中，有效地帮助客户解决公证、信息记录与业务流程长，单据繁多和信息作伪与易篡改的问题。2018 年 4 月，腾讯携手慧狮利用 BaaS 平台搭建司法联盟链，帮助司法鉴定、公证、仲裁、审计等权威机构，记录和存证各项法律文件。既提高了共识效率，也确保了共识内容的可信度；解决了传统流程公信力不足、流程复杂、信息不对称、传递效率低的痛点。

- **供应链金融安全**

在供应链金融安全领域，腾讯推出微企链，通过腾讯区块链技术及运营资源，连接核心企业资产端及金融机构资金端，可以帮助提升资金配置效率、提升流动性支持小微企业供应链，进而降低社会融资成本，支持实体经济。与此同时，以源自核心企业的应收账款为底层资产，通过腾讯区块链实现债权凭证的流转，又可以保证相关信息不可篡改、不可重复融资，可被追溯，链上安全可信。

- **数字资产**

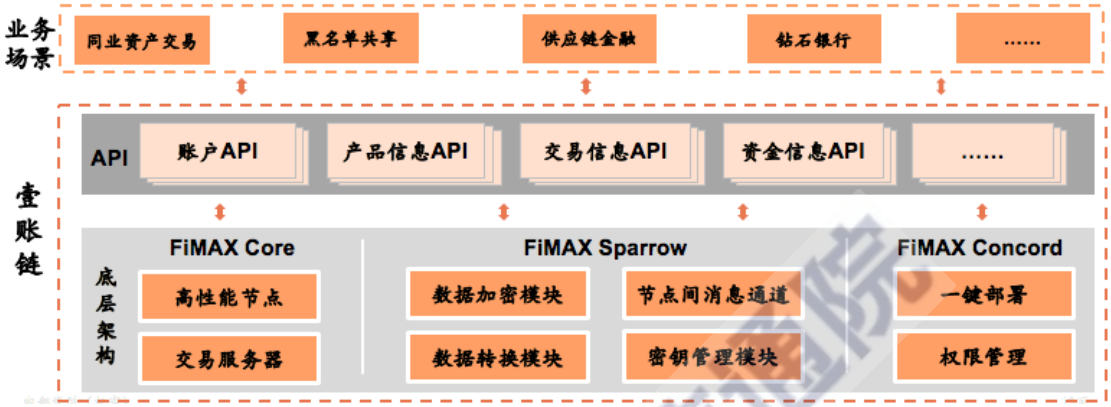
微黄金是腾讯在做区块链项目时实验的第一个内部落地的商业场景。银行、腾讯等多组织参加到微黄金产品中来，用多个节点一起参加记帐。这其中，由腾讯来供给联盟链的底层技能支持以及交易信息的安全性、可追溯性。2018 年 5 月 24 日，由腾讯与深圳市国家税务局（以下简称“深圳市国税局”）联合建立的“智税”创新实验室正式成立。同时还发布了基于腾讯区块链的数字发票解决方案。该方案是目前全国首个基于区块链的发票应用研究成果。在该方案上，企业方可以在区块链上实现发票申领和报税，用户则可以实现链上报销和收款。

- **推动构建区块链行业安全生态**

2018 年 6 月 21 日，由中国技术市场协会、腾讯安全、知道创宇、中国区块链应用研究中心、网络安全企业、区块链相关机构及媒体等二十余家机构单位联合发起“中国区块链安全联盟”，联盟成立后将建立区块链生态良性发展长效机制，着重打击一切假借区块链名义进行变相传销、诈骗等敛财行为，加速构建区块链行业安全生态。

（四）平安科技：基于国产密码的自主可控联盟链实践

平安集团壹账链 BaaS 平台基于平安区块链团队自主研发的 FiMAX 框架，应用隐私保护技术和高效率高性能底层技术等，旨在解决效率低、隐私保护差以及部署管理难等问题，如图附 3-6 所示。



图附 3-6 壹账链 BaaS 平台结构

FiMAX 高性能架构单节点在 2.2Ghz 的 8 核 CPU 条件下，可支持 4000-5000 笔每秒的交易吞吐量。通过增加算力和多链分片，可达 10 万+笔 / 秒，使区块链在供应链金融的运用中，在普通硬件配置下也可实现高性能吞吐量，多方并发高频交易无性能障碍。

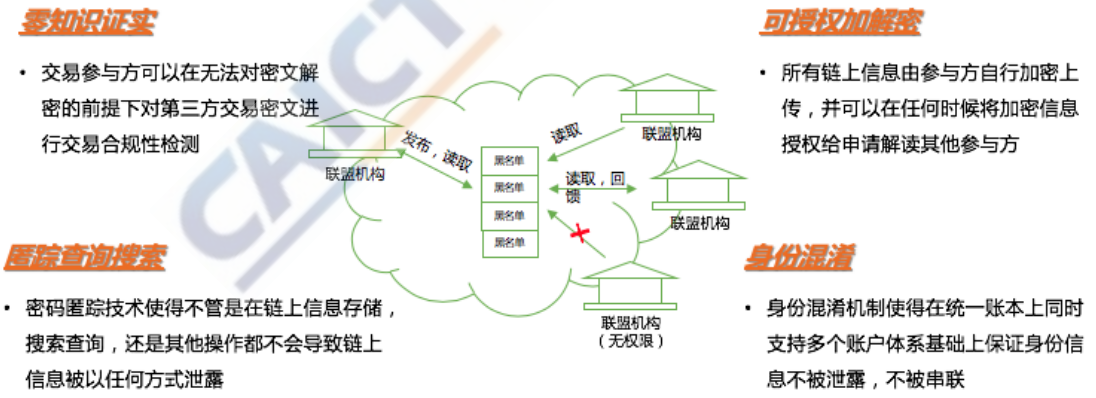
其中，FiMAX Core 集成自主产权的国密加速系统 GCCA，根据国密算法以及 x86 指令特点进行深度优化，提升国密效能。FiMAX Sparrow 区块链中间件是自主研发的隐私保护系统，能提供完整的隐私保护，并有效解决链上多方的数据隐私保护及数据验证核心痛点。

- 提供多种零知识协议的隐私安全中间件系统，交易参与方可以在无法对密文解密的前提下，对第三方交易密文进行交易合规性检测；
- 区块链加密信息的可授权式加解密方案，所有链上信息由参

与方自行加密上传，并可以在任何时候将加密信息授权给申请解读其他参与方；

- 采用包括字母公私钥体系在内的多重密码协议达到身份混淆效果，目的是让参与机构达到保护自身交易信息，使得在统一账本上同时支持多个账户体系基础上，保证身份信息不被披露，不被串联。在强监管模式下，字母公私钥体系中的证书可由监管统一颁发使（只有）监管机构完全掌握身份信息，在保证身份混淆的效果的同时，满足强监管模式下的监管看穿要求；
- 匿踪查询搜索技术使得不管是在链上信息存储，搜索查询，还是其他操作都不会导致链上信息被泄露。

平台数据隐私安全保障机制如图附 3-7 所示。

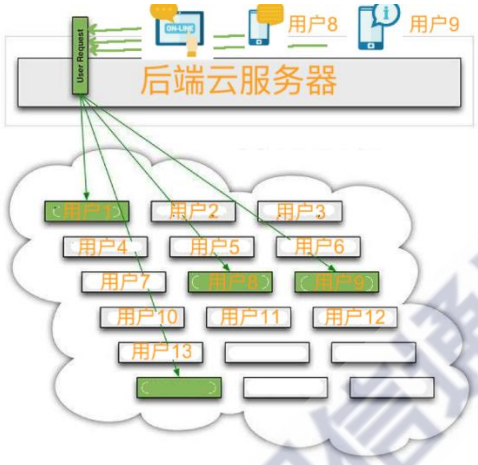


图附 3-7 壹账链 BaaS 平台数据隐私安全保证

（五）观安：区块链移动用户数据资产安全管理实践

由于手机客户端掌握在手机用户的手里，运营商不能完全控制，可在后端搭建联盟链服务，提供给所有成员（手机用户及企业用户）使用，每个用户对应一个专属的服务空间（服务节点），如图所示，

每个服务空间对应区块链上的一个节点，把每个移动用户纳入到联盟链中，利用区块链多方签名、不可篡改的特点，使得数据转移、存储及转让通过云端的区块链结点进行，在用户友好的情况下，得到多方共识，降低减少操作难度，如图附 3-8 所示。



图附 3-8 区块链数据资产安全管理部署

基于如图所示的联盟链服务，可为保护用户敏感数据应用、用户虚拟身份认证和保护 Web 主机安全提供底层基础架构保证。主要包括以下四个方面：

- **用区块链解决敏感数据的保护**

一是用户重要数据/文件一旦上链，就无法篡改，后续的每一次改动都会有不可磨灭的记录；二是区块链结合访问控制和加解密等技术，可以做到数据向指定人员开放相关的权限，以及在某段时效内具备相关权限；三是指定人员每一次提出的数据访问请求均可被记录在区块链上，因此，对人员的访问行为可以全程追溯。同时通过智能合约，可实现特定用户的数据查阅或者审批权限的收回和终止；四是避免 / 缓解 DDoS 攻击，去中心化的系统允许用户出租自己的额外带宽，

并将带宽访问权限“提交”到服务端的区块链分布式节点，当网站遭受 DDoS 攻击时，网站可以利用这些出租带宽来缓解 DDoS 攻击。

- **区块链虚拟认证**

一是通过区块链共享云盘，实现用户个人数据安全存储和可追溯，共享数据通过类似云盘的方式存储，所有用户的个人数据、文件等都可以存储到专属的云服务器帐号上，同时采用区块链加密方式（如非对称加密），用户通过 APP 查看入口和专属的私钥查看数据和文件，任何数据和文件的查看、移动都会记录进入区块链账本，方便用户对其数据和文件进行管理的监控。二是客户端节点身份真实性追溯。可在区块链平台上建立一个身份映射信息，以用户号码等为基础，追溯第三方平台的用户名和移动号码的关联，从而最终能追溯到实名人。三是确权的数据传输。用户之间可以自动组合成为子链，互相为对方记账，形成不可篡改的账本，互为证明，保护用户隐私。任意用户之间的数据传输，都可以选择见证人／见证节点，以保障传输的重要信息安全可靠。

- **区块链用于文件系统完整性保护**

一是主机系统文件的完善性保护。将区块链用于检测 Web 主机操作系统、数据库、关键应用中的关键数据是否被恶意篡改，定期地依据区块链保存的摘要和当前摘要进行比对，以判定是否发生篡改。二是对客户端文件系统的完善性保护。保护过程与主机系统保护相似，包括摘要生成、时间戳植入、签名认证、摘要上链、摘要对比、系统恢复预警等。

- **区块链用于解决日志安全**

主要包括 App 应用日志系统安全和 Web 服务器日志系统安全，由于日志数据属于高频数据，需要频繁地存储，对系统性能压力非常大，区块链的分布式特性可以通过增加区块链节点的方式实现负载均衡。在 App 日志安全方面，数据后台可通过采集策略以加密的方式 log 到区块链系统，日志数据通过后续的分析系统可以进行用户行为统计分析和系统级故障分析。在服务器日志数据管理方面，可结合大数据分析区块链日志系统中的数据，先从百万数量级的访问 IP 中挖掘可疑的 IP，再分析可疑 IP 的访问行为并挖掘安全风险，在兼顾效率同时保证日志数据的安全性。

（六）京东：区块链防伪追溯平台

结合物联网和区块链技术，记录商品从原材料采购到售后的全生命周期闭环中每个环节的重要数据，结合大数据处理能力，与监管部门、第三方机构和品牌商等联合打造防伪和全链条闭环大数据分析相结合的防伪追溯开放平台。平台基于区块链技术，与联盟链成员共同维护安全透明的追溯信息，建立科技互信机制，保证数据的不可篡改性和隐私保护性，做到真正的防伪和全流程追溯，主要功能包括：

- **物联网解决方案**

按照统一的编码机制，为每件商品的最小包装赋予唯一的身份标识，实现消费者线上验真伪。

- **跨主体信息采集**

将商品生产、加工、包装、出厂等信息，结合京东仓储出入库、

订单、物流等信息，实现商品全程品质信息可追溯。

- **营销增值**

以防伪追溯作为切入点，连接用户，为品牌商聚集消费用户，通过一系列营销宣传和促销活动，扩大商品销量。

- **数据服务**

多项专业报表，为品牌商梳理数据报表，全方位反应商品的防伪溯源状况，量化追溯带来的收益。

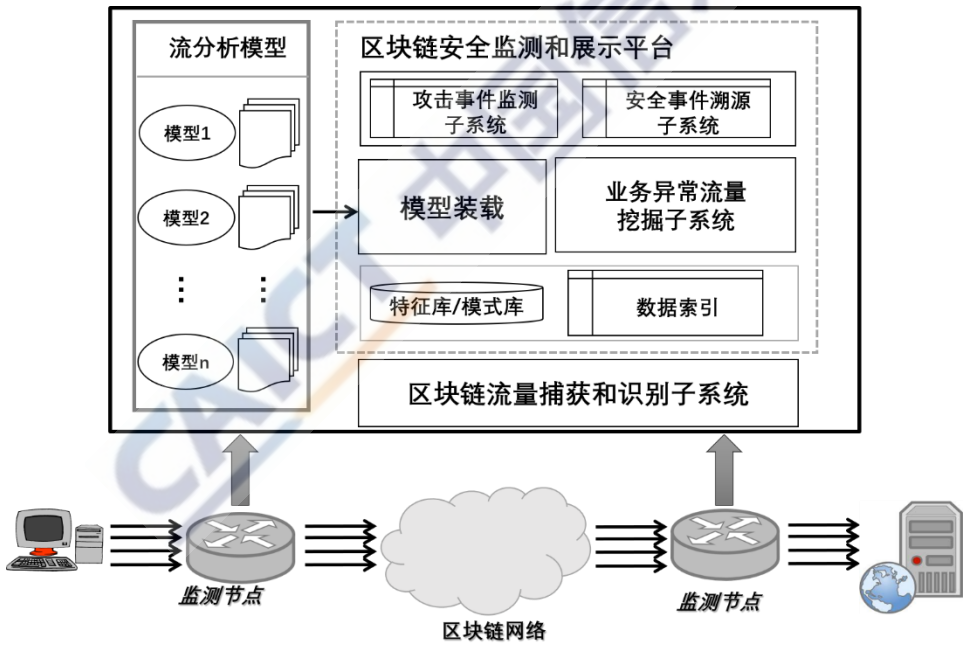
- **区块链联盟链技术服务**

借助智臻链区块链服务平台，组建防伪追溯联盟链，共建共享可信安全数据环境。

在与外部合作方面，一是与政府合作，包括与工信部消费品工业司开展合作，共同推进乳制品追溯体系建设；与商务部签署战略合作协议，防伪追溯写入战略合作事项；与北京商务委开展战略合作共建重要产品追溯体系。二是组建社会联盟，形成合力，包括联合商务部、农业部、工信部、国家质检总局成立京东品质溯源防伪联盟；联合跨国品牌、海关商检成立跨境溯源联盟；与沃尔玛、IBM、清华大学成立首个安全食品区块链溯源联盟，共建食品安全。

附录 4 区块链安全监管技术平台

当前区块链网络在节点和内容管控、异常业务监测和预警、智能合约安全检测和防护等方面仍存在诸多问题，特别是比特币等数字货币由于其匿名特性成为各种网络犯罪资金的主要载体，在许多非法网站上，甚至成为唯一支付手段，给国家的网络安全监管和安全防护带来了巨大的挑战。区块链安全监管技术平台旨在识别区块链平台应用，全面掌握区块链相关安全漏洞、攻击事件和安全威胁发展态势，探索对重大异常、安全事件的溯源追踪手段，技管结合，打造区块链安全监管硬实力，平台架构如图附 4-1 所示。



图附 4-1 区块链安全监管技术平台

平台主要包括流量捕获和识别子系统、业务异常流量挖掘子系统、攻击事件监测子系统和安全事件溯源子系统，具体功能详述如下：

- **基于网络流量识别区块链平台和应用**

通过深入分析比特币、以太坊等区块链平台的通信协议、网络结

构和计算模型等，抽取区块链分布式网络的通信机理、监测方法特征，在国内互联网关键节点和部位部署区块链大规模流量监测系统，采取基于机器学习、模式识别等流分析的方法识别区块链网络通信协议和应用，实现面向大规模高速网络流量的区块链平台和应用识别。

- **区块链漏洞和攻击事件监测**

监测和挖掘区块链典型应用、平台、智能合约等安全漏洞，提取典型应用攻击事件的异常行为模式和特征，提取可供利用和扩充的区块链安全监测规则，基于 DDoS 攻击、病毒、木马等攻击特征，开展区块链钱包、矿机、交易所、区块链 app、智能合约等漏洞和攻击事件的监测，实现面向区块链的重大安全事件的可视化展示。

- **区块链典型业务异常发现和处置**

面向区块链业务异常监测和防护的需求，结合区块链分布式架构分析，挖掘区块链网络业务异常行为监管方法，结合 IP 地址备案、域名备案等管理手段，实现区块链异常业务画像，基于区块链网络异常流量识别区块链网络恶意节点、发现异常业务行为（如异常交易、勒索赎金、传播非法内容等），以支持区块链网络中恶意节点发现和处置、业务异常监控等。

- **重大异常、安全事件的溯源追踪**

针对重要领域、关键位置的区块链网络、业务系统所面临的重大异常、安全事件的溯源追踪需求，通过区块链底层网络节点跟踪监测、基于大规模流量分析区块链网络节点通联关系、用户关系测绘等手段，以基于启发式方法的区块链网络业务图分析、基于图挖掘算法的用户

族谱分析等方法，突破区块链业务图构建与攻击路线还原技术，支撑对区块链网络恶意行为、重大安全事件的溯源追踪。

- **区块链威胁情报发布**

结合系统检测发现的漏洞、非法行为模式、黑地址等，以及公开发布的区块链安全事件、漏洞、预警等情报信息，集中形成区块链威胁情报，同时对系统的威胁监测、溯源等相关功能形成正向反馈和指导。另外，针对区块链网络的重要安全事件、漏洞以及重要研究进展等不定期发布区块链相关安全报告。

中国信息通信研究院

地址：北京市海淀区花园北路 52 号

邮政编码：100191

联系电话：010-62304839

传真：010-62304980

网址：www.caict.ac.cn

中国通信标准化协会

地址：北京市海淀区花园北路 52 号

邮政编码：100191

联系电话：010-62302734

传真：010-62301849

网址：www.ccsa.org.cn