CAICT 中国信通院

区块链安全能力测评与分析报告

（2021 年）

中国信息通信研究院安全研究所

2021 年 3 月

版权声明

前　言

区块链技术的集成应用逐渐成为新的技术革新和产业变革的重要驱动力量。世界各主要国家纷纷加快区块链相关技术战略部署、研发应用和落地推广，探索区块链在各行业领域的应用模式，抢占技术发展先机。近年来，在区块链应用落地探索过程中，基础能力不足和安全风险涌现两大障碍逐渐凸显。为进一步推动区块链业务主流化进程，以微软、IBM、亚马逊等行业巨头为代表纷纷投身区块链基础设施能力建设，各国政府也不断完善区块链及基础设施的建设和安全监管相关政策。在区块链生态系统中，区块链基础设施作为对上承载各类区块链应用、对下衔接网络基础设施的核心枢纽，保障其安全已成为确保区块链生态安全的重中之重。一旦其遭受漏洞利用及 DDoS 攻击等攻击威胁，将对其上的区块链应用、用户数据乃至整个区块链生态带来极大的安全影响。在此背景下，2020 年 11 月-2021 年 1 月期间，中国信息通信研究院安全研究所主办了首轮区块链基础设施安全能力测评工作，切实排查区块链基础设施安全风险，旨在提升区块链基础设施乃至区块链生态的安全水平，保障区块链安全、有序、高质量发展。

本报告综合分析了首轮区块链基础设施安全能力测评情况，形成了区块链基础设施十大安全隐患及十大必知必会，对 2021-2023 年间区块链基础设施安全新方向进行了展望，提出了未来发展建议。希望通过与业界共享，共同夯实区块链安全基础设施，为区块链技

术在建设新型基础设施、发展数字经济等方面发挥积极重要作用奠定扎实的安全保障。

目 录

图 目 录

表 目 录

一、区块链安全发展现状

凭借其抗篡改、透明化、分布式的安全特性，区块链技术已成为全球科技和经济发展新热点，世界各主要国家纷纷加快区块链相关技术的战略部署、研发应用和落地推广。据统计，2020 年全球共发生其区块链融资事件 626 起，中国有 99 起融资事件[1]，平均融资金额为 1.05 亿元，同比增加 8.23%。从细分领域统计，2010-2020 期间我国融资事件集中于区块链应用层和数字货币方向，但区块链基础技术领域的融资金额占据首位，高达 698.55 亿元，可见资本市场对基础技术的重视度[2]。

随着区块链应用在国计民生多领域落地探索，为上层区块链应用提供存储、传输、计算、开发和测试等资源能力的**区块链基础设施，其发展已成为推动区块链业务主流化的决胜关键所在**。区块链基础设施通过建立区块链底层架构和平台，为区块链技术、产业和应用落地提供区块链底层核心能力、资源和服务，可有力清扫区块链落地进程中必须解决的区块链底层性能不足和开发技术门槛过高等障碍，逐步成为区块链竞争新热点领域。

在政府层面，以欧盟为代表已启动区块链基础设施建设部署。2018 年，21 个欧盟成员国合作建立欧洲区块链服务基础设施(EBSI，European Blockchain Services Infrastructure)，旨在使用区块链技术提供整个欧盟范围的跨境公共服务基础设施。2020 年 2 月，EBSI 已推出首个比利时节点。2020 年 8 月，欧盟委员会宣布将在沙箱中

[1] 数字来源：《全球区块链产业发展月报（2020 年 12 月）》，01 区块链，零壹智库

[2] 数字来源：《2020 区块链产业投融资报告》，陀螺研究院、IT 桔子联合撰写，星球日报、碳链价值、深圳市信息服务业区块链协会、链证经济联合发布

对 EBSI 架构中的区块链和数字资产用例进行测试。

在行业层面，多样化区块链基础设施能力正加快建设。区块链即服务(BaaS，Blockchain as a Service)作为一类特殊的基于云平台的区块链基础设施，其所提供的资源丰富、弹性按需分配的底层技术特性使其受到了科技巨头、云厂商、区块链初创企业的高度关注和大力推动，微软、IBM、甲骨文、思科、亚马逊、SAP、阿里、百度、华为、腾讯等国内外诸多行业巨头和区块链领头企业均已推出区块链即服务平台，促进区块链基础设施成为公共信任基础设施。据 Zion Market Research 预测，2024 年全球区块链即服务市场价值将达 305.9 亿美元。2018 年，瑞士邮政和瑞士电信宣布合作建设“100％瑞士”国家级区块链网络基础设施，为瑞士公民和企业提供区块链基础设施和区块链即服务等区块链基础性服务。2019 年，国家信息中心、中国移动、中国银联等机构正式发布并启动区块链服务网络（Blockchain-based Service Network，BSN）公测，以全国性区块链服务基础设施平台形式为开发者提供公共区块链资源环境。

区块链发展的同时也面临着新的风险挑战和不确定因素，相关安全事件不断涌现，加强安全能力建设已迫在眉睫。习近平总书记在 2019 年主持中共中央政治局第十八次集体学习时强调，“要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。”区块链基础设施作为对上承载各类区块链应用、对下衔接网络基础设施的核心枢纽，针对区块链基础设施的安全攻击将对其上承载的各类区块链应用、用

户数据等带来极大的安全影响。在此情况下，开展区块链基础设施安全测评可实质性排查其安全风险、提升其安全水平，对推动其上区块链生态安全、健康、有序发展具有重要意义。

2020 年 11 月起，中国信息通信研究院安全研究所依托行业标准《区块链基础设施安全防护要求》《区块链基础设施安全防护检测要求》，公开征集公有链、联盟链和私有链[3]项目，开展了首轮区块链基础设施安全测评。通过综合分析测评结果，形成了区块链基础设施十大安全隐患及十大必知必会，并对未来 3 年区块链安全新方向进行了展望，旨在与业界共同筑建安全扎实的区块链基础设施，助力区块链行业提升整体安全水平。

二、区块链基础设施安全能力综合分析

此轮安全测评共涉及区块链系统账户权限管理、数据及个人隐私、密码机制、共识机制、智能合约、安全运维 6 大领域，各领域整体测评情况分析如下:

（一）具备基础权限管理功能，网络控制能力有限

参评项目根据不同的链类型，可**提供相应的基础性权限管理功能**。无论是公有链或许可链均支持身份鉴权、双向认证管理、认证信息复杂性管理、账户权限管理、账户信息传输机密性和完整性保护；许可链项目还普遍支持身份标识唯一性管理、账户冻结与恢复功能、区块读写权限管理、智能合约权限管理。

参评项目在**默认账户管理、账户新鲜度管理、终端访问权限管理**

[3] 本报告中统称联盟链和私有链为许可链。

方面的表现待强化，约 18%-25%的参评项目未能通过相关测试。约半数的参评项目**缺少完善的数据流访问管理**，存在 DDoS 等资源攻击风险，如 62%的项目不会根据报文类型和地址对节点可接收报文进行过滤；50%的项目不会根据会话状态信息，或基于应用协议和应用内容对进出节点的数据流进行控制。权限管理领域整体表现分析见图 1。

数据来源：中国信息通信研究院

图 1 权限管理能力分析

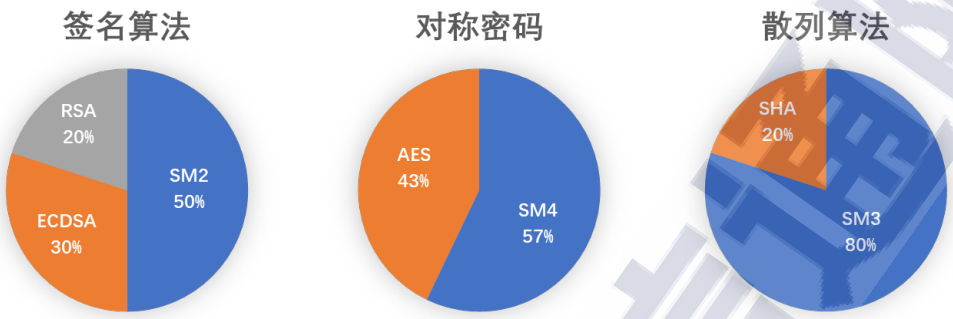
（二）采集用户信息类型简单，隐私保护能力单一

参评项目采集的用户信息包括邮箱、手机号、地理位置、登录时间、交易时间点等，但 80%的项目**对用户隐私保护仍停留在对隐私数据提供访问管理这种单一保护方式，**未对隐私用户信息进行模糊处理或其他额外保护，难以抵抗内部恶意使用和外部隐私攻击。一方面，管理人员可通过后台获得用户隐私信息，甚至在未经用户允许的情况下进行二次分析获取用户画像；另一方面，攻击者一旦获得用户的身份信息即可获取用户隐私信息。

（三）密码算法国产化程度高，密钥存在安全漏洞

参评项目主要采用 SM2 签名算法、ECDSA 签名算法、RSA 签名算法、SM4 对称加密算法、AES 对称加密算法、SM3 摘要算法、SHA256 摘要算法等密码算法，算法使用比例如图 2 所示。整体可见，**国密算**

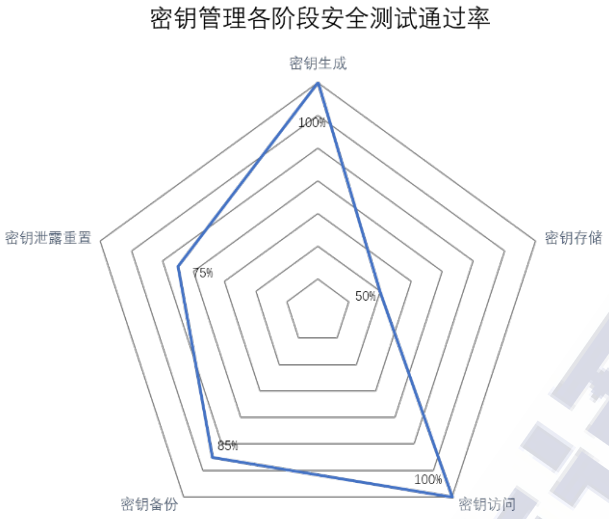
法的应用比例较高，75%的参评项目均使用了至少一种 SM 系列国密算法，38%的参评项目采用了国产 SM2、SM3、SM4 算法分别用于签名、摘要和加密过程。



数据来源：中国信息通信研究院

图 2 密码算法使用比例分析

参评项目对密钥全生命周期安全管理能力参差不齐，尤其**在密钥存储、备份、泄露与重置方面有待增强**，如图 3 所示。在密钥生成方面，所有项目密钥生成所使用的随机数均可通过随机性测试；在密钥存储方面，实测中仍发现了密钥明文存储情况，仅半数的项目提供专用设备用于存储私钥；在密钥访问方面，所有参评项目均对密钥的访问设置了访问控制，使用口令、USB 认证等方式方可访问主密钥和主密钥种子；在密钥备份方面，85%以上的项目采用安全服务器或第三方托管的方式对密钥进行必要的备份；在密钥泄露与重置方面，75%的参评项目可以在疑似密钥泄露的情况下，通过注销 CA、冻结账户等方式终止使用旧密钥，但对密钥重置仍采用手动维护为主，效率有待提高。



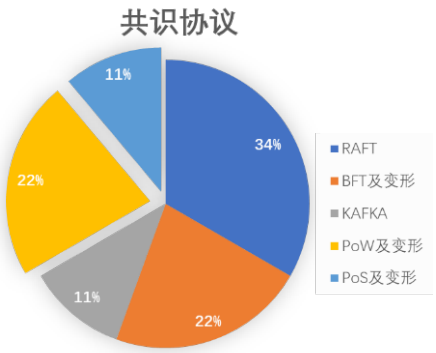
数据来源：中国信息通信研究院

图 3 密钥全生命周期安全性分析

（四）共识机制类型繁多，安全性能缺乏清晰验证

参评项目使用的共识机制类型各异。非竞争类的共识机制包括 BFT[4]及其变形协议、RAFT、Kafka，竞争类的共识机制包括 PoW[5]、PoS[6]及两种协议的变形，如图 4 所示。在所有的协议中 RAFT 使用比例最高，而**采用自研共识机制的比例达 25%**。考虑到共识机制类型繁杂且专业性较强，用户对项目共识机制安全性的了解更多依赖于项目方的说明与论证。而据测评发现，**仅半数的项目以文档形式提供对共识协议的机制及安全性论证**。共识机制安全性的不清晰可能会导致与用户就安全要求产生矛盾，甚至对系统内部恶意节点防护的缺失。

[4] BFT: Byzantine Fault Tolerance，拜占庭容错
[5] PoW: Proof of Work，工作量证明
[6] PoS: Proof of Stake，股权证明



数据来源：中国信息通信研究院

图 4 共识协议应用情况分析

（五）智能合约安全投入大，缺少第三方审计支持

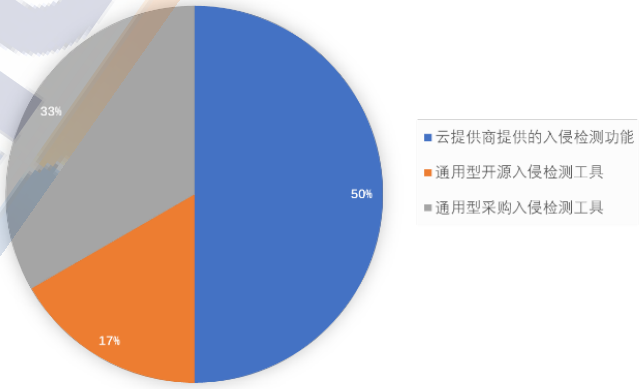
智能合约安全漏洞作为近年来区块链安全事件重要诱因之一，一直是区块链项目安全防护的重点。此次测评也验证了参评项目普遍对智能合约安全投入较多，**专业化安全检测机制基本完备**。许可链基本都具备对智能合约的安全检查机制，可以对用户上传的智能合约进行基础性安全检测及代码审计，并向相关情况告知用户。但**第三方智能合约代码审计的支持率不高**，随着区块链系统的壮大，代码审计的专业性及效率将面临挑战。

（六）系统安全运维专业化、精细化程度有待提升

参评项目初步具备了资源滥用攻击的应对功能，但水平待提升。**一方面，项目测试环境在大规模请求下的稳健性表现不佳**。测试环境正常运行时，测评节点 CPU 占用率在 0.2%-5.1%不等。在突发 10000 个区块获取请求后，CPU 占用率上升到 2.4%-20.6%，增长率最低为 47%，最高可达 5300%。**另一方面，参评项目的资源监测和告警能力测评灵敏度不高**。75%的参评项目具备对链节点资源的监控功能，如节点运行时间、响应时长、区块高度、节点间连接情况等。其余 25%

的项目不具备资源监控功能，故无法通过资源使用情况分析进一步提供对 DDoS、算力攻击等网络攻击行为的检测分析。但在 10000 个区块获取请求测试中，参评项目均未发出资源告警信息，参评项目对异常资源使用的告警敏感度待加强。

在入侵检测能力实测环节，仅有 12%的参评项目测试环境对测试漏洞提出了告警，其余项目未能成功检测出特定的测试漏洞。这主要是因为参评项目**对区块链特有漏洞的检测能力和入侵规则定期更新能力匮乏**。一方面，区块链漏洞检测覆盖率较低。参评项目入侵检测功能主要依赖于云环境等基础资源提供商提供的入侵检测功能、通用型商业化检测工具和通用型开源入侵检测工具（如图 5 所示），未采购区块链特有的入侵检测模块，且仅有 25%参评项目漏洞库参考了区块链漏洞库或区块链社区发布的漏洞信息。另一方面，缺少检测规则定期更新机制。只有半数的项目维护相关入侵防范机制的升级和更新，其中仅有 1 个平台的漏洞库及时更新了参评当月最新的区块链漏洞，对通用系统或区块链最新漏洞的检测能力有限。



数据来源：中国信息通信研究院

图 5 入侵检测功能类型分析

三、区块链基础设施十大安全隐患

通过综合评估，根据本轮测评中安全风险的检出比例和严重程度，区块链基础设施十大安全隐患涉及 2 项权限管理，2 项密钥安全，1 项隐私保护，1 项智能合约安全，4 项安全运维，相关信息见表 1。

表 1 区块链基础设施十大安全隐患列表

排名	内容	检出比例	严重度	攻击能力	领域
1	区块链特有入侵行为检测缺失	75%	☆☆☆	长期	安全运维
2	密钥明文存储	25%	☆☆☆	长期	密钥安全
3	单一外部隔离防护引入横向移动风险	85%	☆☆	未来	安全运维
4	智能合约代码审计覆盖面不全	100%公有链 33%许可链	☆☆	长期	智能合约安全
5	资源滥用攻击防范检测能力不足	25%-62%	☆☆	长期	安全运维
6	隐私数据未模糊化处理	80%	☆	长期	隐私保护
7	公有链账户可用性管理不完善	100%公有链	☆☆	长期	权限管理
8	密码更新管理缺失下的默认账户风险	18%	☆☆	长期	权限管理
9	测试环境迁移不完备	100%	☆	未来	安全运维
10	密钥存储存在敏感字段	38%	☆	长期	密钥安全

数据来源：中国信息通信研究院

（一）Top 1-区块链特有入侵检测能力弱，传统入侵检测是目前主流

75%的参评项目通过部署采购的或开源的通用型入侵检测工具，提供对 Windows/Linux 等操作系统的恶意代码检测及其他传统网络入侵检测能力。其采用的漏洞库则参考入侵检测工具提供商、云服务提供商等发布的漏洞库，这些漏洞库针对传统网络或云环境下的安全漏洞，但无法提供针对区块链的特有漏洞扫描检测。其余 25%的参评平台额外采用了国家区块链漏洞子库或区块链社区官方发布的漏洞

库对传统漏洞库形成补充，但其中**仅有 1 个平台**的漏洞库及时更新了参评当月最新的区块链漏洞，具备区块链特有漏洞的定期更新能力。实际上，区块链安全漏洞频出，国家区块链漏洞子库自 2020 年 7 月-12 月已收录 116 个漏洞，某区块链漏洞平台[7]在 2020 年 12 月 23-31 日即发布区块链高危漏洞 11 个。**如若区块链平台不能及时更新区块链专有漏洞，攻击者可利用近期发布甚至未及时修复的历史漏洞渗透区块链平台**，造成平台数据丢失、用户经济损失等。

（二）Top 2-密钥明文存储威胁不容小觑，或引发跨平台风险传播

在此轮检测中，25%的参评区块链项目存在密钥明文存储现象。经调研得知，尽管参评平台可通过软加密、硬加密等方式提供密钥保护能力，但为了满足平台客户便捷式使用要求，平台会牺牲高安全要求，采用密钥明文存储方式作为默认模式，仅在用户高要求环境下提供软加密、硬加密等密钥保护措施。实际上，因密钥明文存储导致的账户泄密、恶意盗用转卖等安全事件屡见不鲜，区块链平台自带的生产、经济等属性更易受到攻击者关注。**攻击者可利用明文存储的密钥，渗透区块链平台，甚至跨平台系统造成大规模风险传播，**造成用户和平台损失。

（三）Top 3-区块链核心运行环境多采用外部隔离，存在横向渗透风险

85%以上参评项目的区块链核心运行环境仅采用外部隔离功能以

[7] 去中心化漏洞悬赏平台，https://dvpnet.io/home

提供入侵防范能力，即通过将区块链的运行环境隔离在内网环境中，在外侧对区块链核心运行环境进行恶意代码、入侵检测等防护能力，而在核心运行环境内部（如核心节点处）不再提供安全入侵能力。然而，单纯采用“**隔离即安全**”**的区块链核心系统将受到内部横向攻击威胁**。一旦恶意攻击突破外部隔离机制，则可利用内部防护缺失这一漏洞，以被攻陷的设备为跳板，在区块链核心运行环境肆意横向移动，造成更大范围更快速度的节点沦陷，加大安全防控难度。

（四）Top 4-智能合约代码审计覆盖有限，第三方审计服务支持率低

所有参评的公有链项目均不为用户上传的智能合约提供代码审计功能，仅由用户自行判断上传和调用的智能合约代码安全性。参评许可链项目虽均提供智能合约代码审计，其中仅 67%的许可链项目提供第三方智能合约代码审计功能，其余许可链项目则通过人工检测等方式提供内部代码检测。近年来，受智能合约专业门槛较高且尚未形成安全规范等客观影响，智能合约代码漏洞一直是公有链和许可链安全事件重要诱因之一。未来随着区块链系统不断扩张，智能合约的生命周期管理越发复杂，**如果区块链系统不提供智能合约代码审计或仅依赖于内部人工审计方式，区块链系统将面临审计人才短缺、人力成本较高、代码审计效率低下等问题**，智能合约极易成为重要风险点。

（五）Top 5-系统访问控制和资源监控能力不足，面临资源滥用威胁

25%的参评项目在实测中未限制访问终端的地址范围，62%的参评

项目中节点可接收到目标地址中不包含自身地址的报文，且 50%的参评项目不限制单个用户或进程对系统资源的最大使用量。**如此不完备的网络和设备访问控制机制为恶意终端进入系统并进一步开展 DDoS 等大规模攻击提供可乘之机。**一旦系统遭受大规模资源滥用攻击，有 25%的参评项目无法提供对节点的资源监控功能，相应影响对 DDoS 等资源滥用攻击的检测能力，**难以及时告警并排查风险**。

（六）Top 6-个人隐私数据未模糊化处理，引入个人隐私暴露风险点

约 90%的参评项目采集了手机、邮箱地址、地理位置、登录时间等个人隐私数据，其中 80%的项目虽通过账户验证对个人隐私数据进行访问控制，但未对个人隐私数据进行模糊化处理，即只需通过账户验证便可访问用户的所有隐私信息。对于这些未模糊化处理个人隐私数据的区块链平台，**一旦账户信息被泄露，攻击者**进入用户账户后，**无需进行多重认证，即可获取明文存储的所有隐私数据。管理人员**也可在未经用户允许的情况下，通过后台**获得甚至分析用户隐私信息**，存在用户隐私数据滥用风险。

（七）Top 7-公有链账户可用性管理机制不完善，用户独立承担风险

所有的参评公有链项目均不提供对可疑、高危账户的权限冻结措施，仅由用户独立为自身密钥及账户的安全性负责。相比之下，所有的许可链参评项目均可通过证书冻结、注销等方式终止疑似泄密账户的权限，为用户账户及时提供系统层面安全防护，与用户共同保障账

户安全。实际上，与许可链相比，公有链公开化的特性加剧了入侵风险，在此情况下，**由防护能力有限的用户独立承担账户防护责任，将引入防护空白期**，带来极大的安全隐患。例如一旦用户账户受到攻击，出现账户行为异常或用户密钥泄露，公有链用户将无法从系统处获得账户冻结等保护，在用户发现异常并更新密钥的过程中，**攻击者可利用此段防护空白期窃取账户数据或资产**。

（八）Top 8-密码更新管理缺失，默认账户将成为攻击突破口

18%的参评项目中检测出 admin 类默认账户，兼之相关项目未设置密钥周期性更新机制，默认账户尤其是具有管理者权限的 admin 默认账户极易成为攻击者入侵的重要突破口。据统计，在企业遭遇远程暴破并被投放勒索病毒的案例中，因默认账户被入侵的事故就占据了 8 成[8]。在账户数量不断增多的区块链系统中，**如果允许默认账户的存在且账户密码不要求及时更新，**仅靠人工进行默认账户管理，极有可能出现默认账户使用默认密码或弱密码的情况，**为攻击者利用默认账户非法获取权限提供便捷入口**。

（九）Top 9-测试环境安全配置不及实际环境，环境迁移或引入风险

几乎所有参评项目都存在测试环境在传输机密性保护、身份认证、入侵检测或其他领域的安全配置低于生产环境的现象。以安全传输协议为例，75%的测试环境中采用 tcp、http 等弱加密安全协议，在迁

[8] 来源：火绒安全实验室

移到实际环境后则改用 https、TLS 等安全传输方式。在环境迁移过程中，可能存在**测试环境的弱安全保护机制未完全迁移带来的安全短板**。

（十）Top 10-密钥存储存在敏感字段，为密钥窃取攻击提供切入口

38%的参评项目中检测出“PRIVATE KEY”等密钥相关敏感词，测评人员可借助敏感词所在位置查找到密钥存储相关信息。**未经混淆的密钥敏感词同时也为攻击者精准获取密钥存储信息提供入口，**提高密钥攻击的成功率和效率。攻击者可借此捕获加密存储甚至明文存储的密钥，进而获取用户信息或进入系统进行渗透。

四、区块链基础设施十大必知必会

针对区块链基础设施安全测评中出现安全风险和安全保障缺失情况，根据重要性排名，对区块链基础设施平台提出十大必知必会安全操作，如表 2 所示。

表 2 区块链基础设施十大必知必会列表

排名	主要安全操作	目标	相关风险	领域
1	区块链恶意代码检测机制	当前专业化恶意代码检测能力弱，未能定期更新	Risk Top 1	安全运维
2	细粒度数据流访问控制	提升节点资源消耗攻击防范检测能力	Risk Top 3	权限管理
3	复合应用第三方审计与内部审计	提高审计效率，降低系统安全风险	Risk Top 1-10	安全运维
4	节点资源监控分析与权限管理	实现对可疑节点和疑似攻击的告警处置	Risk Top 5	安全运维
5	隐私数据多重保护	降低内部恶意人员和外部攻击者获取隐私数据风险	Risk Top 6	隐私保护
6	第三方核心密钥托管	降低对存储密钥的盗取风险	Risk Top 2，10	密钥安全
7	为高级别账户提供智能合约权限管理能力	控制联盟链中智能合约相关的恶意代码影响范围	Risk Top 4	智能合约

8	规范密钥更新周期	减少密钥泄露风险	Risk Top 8	密钥安全
9	扩展第三方安全支持能力	提高安全管理效率，打造开放式安全生态	Risk Top 1-10	安全运维
10	消除系统敏感字段	降低攻击者通过敏感词捕获密钥的风险	Risk Top 10	密钥安全

数据来源：中国信息通信研究院

（一）Top 1-部署专业性全面化的区块链恶意代码检测机制

公有链、联盟链及私有链项目均应部署**专业的区块链恶意代码检测工具**，支持对上传的智能合约进行形式化验证、与漏洞库里的漏洞进行自动匹配分析等功能。漏洞库应多方位参考国家级区块链漏洞库、区块链官方社区与区块链安全社区发布的漏洞信息，并**定期进行更新**。

（二）Top 2-对进出节点数据流提供细粒度访问控制

联盟链可**采用黑白名单、网络隔离、报文筛选、端口限制等方式**，基于进出节点数据包的类型、源地址、目的地址、协议内容等，对数据流进行细粒度监测和控制。节点细粒度访问控制机制将更有**针对性地避免对节点的资源消耗攻击**，降低因网络中可用节点减少带来的全网 51%攻击、日蚀攻击等攻击风险。

（三）Top 3-结合第三方审计与内部审计排查系统安全风险

此轮测评所有参评项目均提供内部安全审计，但仅有 1 家参评项目提供了第三方源码审计报告。一旦区块链源码或核心机制存在的漏洞被利用，分布式、抗篡改的区块链系统将面临攻击范围大、系统难恢复的后果。因此建议**在公有链和许可链各版本上线等关键时期前**进行第三方审计，通过采用**专业第三方审计与内部审计双重保障**的方式，

对智能合约、共识机制等区块链特有技术模块实现区块链专业审计能力复用，最大程度地提高审计效率，降低系统安全风险。

（四）Top 4-基于节点资源监控分析功能加强权限灵活管理

联盟链应具备**对节点资源使用情况的监控和分析功能**，包括对节点运行时间、响应时长、网络连接情况、资源消耗情况、节点区块链高度等情况的监控，并基于资源使用情况分析实现对可疑节点和疑似攻击的告警。区块链即服务平台或联盟链底层平台还应在**系统层面支持对可疑节点和账户的权限变更，**如通过 CA 吊销数字证书、取消相关账户权限，或为管理者提供可快速变更可疑账户权限的智能合约，实现异常账户冻结、节点禁入、资源使用量限制等操作。

（五）Top 5-采用隐私数据多重保护技术实现内外双重防护

在现有隐私数据访问控制的基础上，一方面使用**隐私数据库**存储隐私数据，为内部访问提供安全保护，另一方面对**隐私数据进行模糊化处理**，要求用户通过多重安全验证后方可访问隐私数据。通过采用如上多重保护技术确保内部恶意人员和外部攻击者无法直接获取隐私数据。

（六）Top 6-拓展第三方核心密钥托管以降低密钥盗取风险

目前 85%以上的参评项目已为主密钥和密钥种子提供了备份，但仅有半数的项目**采用加密机等专用设备机制保护密钥**。基于核心密钥

安全的重要性，应进一步**增加对主密钥和密钥种子的第三方托管业务**。在颁发核心密钥时，对私钥进行拆分加密，并分别交由可信的第三方机构、银行等进行托管，以保证任意一个机构都无法独立盗取私钥进行签名交易。

（七）Top 7-强化联盟链智能合约权限管理以控制攻击影响

在联盟链中建议为 admin 等高级别管理账户增加与智能合约生命周期相关的控制权限。一旦运行环境中智能合约漏洞被恶意调用，**高级别账户可以紧急进行升级或销毁操作**，有效控制智能合约相关的恶意代码影响范围。

（八）Top 8-规范密钥更新周期以减少密钥泄露风险

加强账户新鲜度管理，尤其是对 admin、test 等高权限、高安全、高危账户的密钥管理，**根据不同的账户安全级别设置相应的密钥更新周期，**定期进行密码更新，降低密钥泄露风险。

（九）Top 9-提升第三方安全支持能力打造开放式安全生态

目前仅有少数项目可支持多种第三方安全能力，如 2/3 参评项目支持第三方智能合约审计，仅有 1 个参评项目提供了支持第三方密码服务的证明材料。在安全能力服务化趋势推动下，在区块链项目中尤其是在区块链即服务项目中**扩展支持第三方密码服务、智能合约审计、恶意代码检测机制等多种安全能力，**对单一项目而言可提高系统安全管理效率和灵活性，降低供应链风险，对区块链行业而言可推动区块

链安全市场向专业化、开放化、服务化方向蓬勃发展，助力打造健康安全的区块链生态环境。

（十）Top 10-通过加密混淆等方式消除系统敏感字段

通过对“ PRIVATE KEY ”“ PRI_KEY ”“ PRIVATE ”“ KEY ”等诸多敏感词进行加密或混淆操作，消除敏感词检出风险，降低攻击者通过敏感词采集密钥相关信息甚至捕获密钥的可能。

五、区块链基础设施安全新方向展望

在区块链基础设施加速建设的同时，也带来了区块链基础设施安全市场精细化发展需求。预计 2021 年-2023 年间区块链安全领域将涌现两类新兴安全方向，分别从广度和深度提供区块链专业化安全能力。

（一）方向 1-区块链安全即服务 Blockchain Security as a Service

随着区块链应用对专业化区块链基础设施需求提高，公共型区块链基础设施平台已成为近年来一大发展热点。由于其上承载的业务将不限于特定的客户，区块链应用、技术模块、用户数据的类型和数量愈发繁杂，对基础设施平台的安全能力提出了更高要求。在此情况下，**区块链安全即服务作为区块链安全产品迈向服务化细分化的产物**，有望成为未来三年内新生市场方向，既为区块链基础设施方提供更高水平、低成本的安全保障，也为区块链安全市场成长注入强心针，催生更加精细的安全产品服务。

区块链安全即服务的发展需要区块链基础设施平台方、区块链安

全提供方、研究测评机构等多方共同发力。**一是提升区块链基础设施平台开放性**，平台方提供密钥、审计、攻击检测等第三方安全服务接口，为用户提供多样化选择可能。**二是提高区块链安全即服务规范性，**平台方明确安全服务需求，与区块链安全服务提供商共同加快安全服务技术、评估等标准研制，落实相关技术指标、接口要求等，提高安全服务适配性。**三是加快区块链安全即服务的评估，**研究测评机构将开放性纳入区块链基础设施平台评估指标，同时加快对区块链安全即服务相关测评，为用户选择提供可信参考。

（二）方向 2-区块链安全容器 Blockchain Security Container

在区块链基础设施尤其是不同区块链即服务平台上，存在多种不可控制的服务对象共同使用平台资源，进行联盟创建与维护、智能合约创建与调用、资源占用与释放等操作。其中可能存在恶意节点上传恶意代码、资源滥用等行为，如若不能尽快被发现或被控制在特定范围内，将有可能辐射影响基础设施平台上其他用户或系统。在此情况下，**区块链安全容器有望为区块链打造隔离化安全运行环境，填补当前区块链专业化入侵防护产品缺失**。

区块链安全容器需要区块链基础设施提供方、区块链安全厂商与云安全厂商合力打造，最大程度**发挥安全容器标准化、可移植、灵活性、可控制的优势**。区块链安全容器中应集成有标准化的安全能力供用户直接使用，且即使用户在不同环境下部署也可保持容器一致性，避免环境迁移带来的影响。区块链安全容器还具备可控制优势，限制

不同应用程序可占用的最大资源，有效避免恶意智能合约、恶意节点等的攻击危害。此外，安全容器可提供隔离化特性，不同容器中应用程序可完全分隔与隔离，将单个容器中的漏洞影响控制在一定范围内。

六、区块链基础设施未来发展建议

安全可靠的区块链基础设施奠定区块链应用平稳落地的基石。但当前区块链基础设施自身存在的技术风险、不完善的安全标准、缺失的风险应对手段、不完备的安全生态均为其平稳建设运行提出了挑战，亟需政产学研合力，从政府监管、行业标准、评估评测、安全生态多角度积极应对。

一是强化区块链基础设施安全监管力度。政府机构尽快把区块链基础设施作为重点应用基础设施纳入安全监管范畴，明确区块链基础设施中不同角色的安全责任，引导和推动区块链基础设施运营者落实“安全三同步”主体责任。

二是加快区块链基础设施安全标准规范出台。推动出台区块链基础设施安全防护要求、安全部署指南、安全评估评测规范等相关安全标准，鼓励企业积极参与标准的研制与试点工作，以标准规范指导区块链基础设施安全建设部署。

三是开展区块链基础设施安全评估评测。通过政府引导、行业自律的方式，开展区块链基础设施安全合规测试验证，切实排查安全隐患问题，指导区块链安全应对措施手段部署。

四是鼓励区块链基础设施安全生态发展。鼓励区块链企业、网络安全企业、区块链安全企业多方联手，推动智能合约漏洞挖掘、代码

审计、安全监测、入侵检测等安全产品服务化细分化专业化发展，规范相关接口，加大对第三方安全服务的支持，打造开放式区块链基础设施安全生态。

附录：首轮区块链基础设施安全能力测评概述

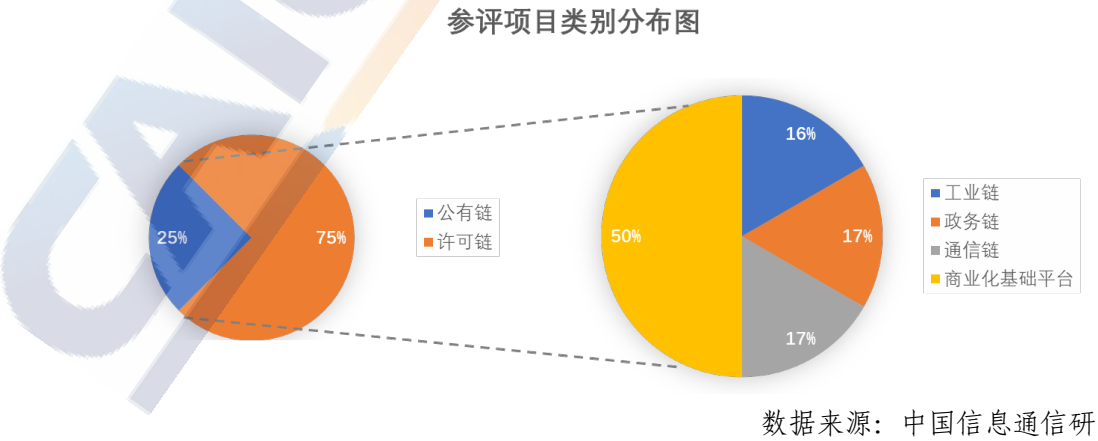
首轮区块链基础设施安全测评由中国信息通信研究院安全研究所牵头，联合上海玄猫信息科技有限公司，对公开征集的区块链项目开展基础设施安全能力测评。此轮测评共涉及区块链系统账户权限管理、数据及个人隐私、密码机制、共识机制、智能合约、安全运维 6 大领域共 108 项分级别的安全性能指标，如表 3 所示。

表 3 首轮区块链基础设施安全测评指标分布表

	二级指标数	三级指标数
账户权限	16 项	12 项
隐私保护	3 项	2 项
密码机制	11 项	1 项
共识机制	6 项	1 项
智能合约	4 项	2 项
安全运维	33 项	17 项
总　　计	108 项	

数据来源：中国信息通信研究院

首轮测评自 2020 年 11 月 19 日起公开征集参评企业。参评企业分布于北京、上海、江苏、浙江、山东、福建、陕西、广东多个省市，其中 25%的参评项目为公有链平台，其余 75%为许可链平台，涉及区块链商业区块链基础设施服务平台、运营商区块链服务、工业区块链服务平台、政务区块链服务平台多种类型，如图 6 所示。



数据来源：中国信息通信研究院

图 6 首轮区块链基础设施安全能力测评参评情况分析

自 2020 年 11 月 26 日正式启动测评后，中国信通院安全测评团队通过调研问卷、技术访谈、工具实测、排查后复测四个步骤，对参评项目基础设施安全能力进行有效检测，流程如图 7 所示。在测评中，团队发现了区块链病毒库缺失、密钥明文存储、恶意终端入侵风险、默认账户未清除等多项安全隐患，并协助参评企业及时完成复测验证，有效排除安全风险。

数据来源：中国信息通信研究院

图 7 首轮区块链基础设施安全能力测评时间轴

中国信息通信研究院 安全研究所

地址：北京市海淀区花园北路 52 号

邮政编码：100191

联系电话：010-62308680

传真：010-62300264

网址：www.caict.ac.cn