成都链安
BEOSIN

年度报告

成都链安科技有限公司

2020年区块链生态安全态势年度报告

目录

Contents

第一章 2020 年区块链生态安全态势概览

1.1 区块链行业整体发展态势

1.2 区块链安全挑战依然严峻

1.3 区块链监管进程亟待推进

第二章 2020 年区块链安全事件全画像

2.1 区块链安全解决方案

2.2 总体安全态势复盘

2.3 安全风险不容忽视

第三章 2020 年区块链典型安全事件盘点

3.1 交易所方面典型安全事件

3.2 DeFi 方面典型安全事件

3.3 诈骗跑路/加密骗局方面典型安全事件

3.4 勒索软件/挖矿木马方面典型安全事件

3.5 暗网方面典型安全事件

3.6 其他方面典型安全事件

第四章 安全风险分析及应对策略

4.1 网络安全

4.2 密码安全

4.3 共识机制安全

4.4 智能合约安全

4.5 应用生态安全

第五章 区块链生态安全发展的对策及建议

5.1 加大区块链安全技术的研究和攻关

5.2 推动区块链安全标准和规范建设

5.3 促成区块链监管和合规体系搭建

参考文献

免责声明

关于我们

第一章 2020 年区块链生态安全态势概览

1.1 区块链行业整体发展态势

2020 年，新冠肺炎疫情突如其来，席卷全球，对原本固已形成的社会秩序和经济秩序造成巨大的冲击。如何在疫情时期提升现行实体经济的运作效率，并进一步促成数字经济发展，区块链凭借其去中心化、开放性、机制透明等天然特性，在全球经济复苏和产业结构升级中发挥了巨大的优势。

从政策环境上来看，各国政府对区块链的重视程度进一步提升。美国方面，2020 年 10 月，白宫发布了《关键与新兴技术国家战略》（National Strategy for Critical and Emerging Technology），首次将区块链核心技术组成部分——分布式账本技术提升到国家战略高度；欧盟方面，2020 年 9 月，欧盟委员会发布了一份全新的数字金融一揽子计划，详细涵盖了数字金融战略、虚拟资产立法建议等方面；我国方面，2020 年 4 月，国家发改委明确将区块链纳入“新基建”范畴，各地方政府纷纷制定区块链行业发展规划及相关政策。根据公开数据统计，2020 年我国国家部委、各地方政府发布与区块链相关的政策、法规、方案文件共计 217 份，显示出我国区块链发展环境得到空前政策助推。

从产业赋能上来看，得益于区块链政策环境的态势利好，“区块链+产业”发展进程进入快车道，垂直行业的各类落地应用项目不断涌现。我国方面，在国家政

策、基础技术推动和下游应用领域需求不断增加的促进下，我国“区块链+产业”的市场规模正在不断拓展，涵盖了包括金融、政务、物流、文娱、社交、社会公共服务等多个垂直领域。根据公开数据统计，2020 年我国区块链落地应用项目总计达 194 个，同比增加 102.8%。区块链行业正阔步迈向“区块链+产业”3.0 时代。

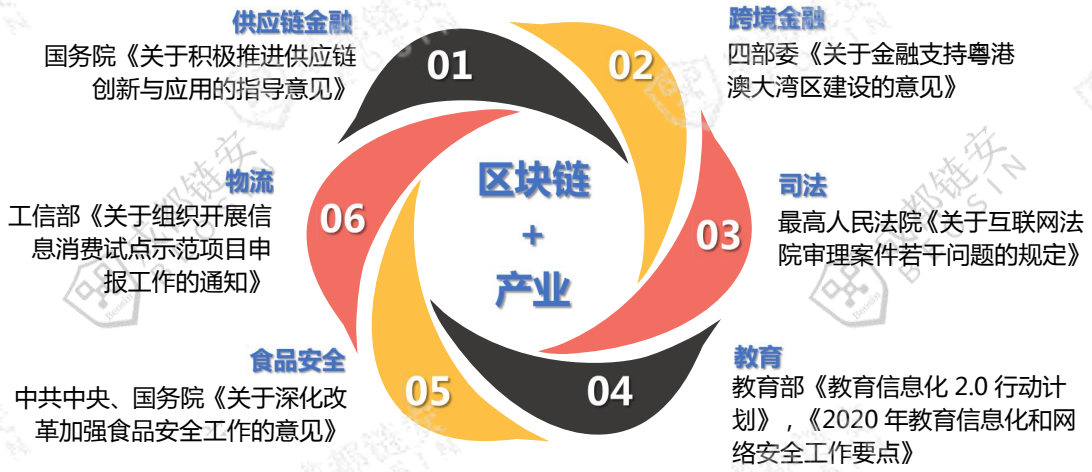


图 1：我国部分“区块链+产业”结合政策

从年度热点上来看，诸如跨链项目 Polkadot、分布式存储项目 Filecoin、比特币减半、以太坊 2.0、虚拟资产市值暴涨等事件备受瞩目，但 2020 年最具创新性和热度的领域无疑当属 DeFi（去中心化金融）。根据 DeFi Market Cap 数据显示，2020 年 4 月，DeFi 代币总市值约为 10 亿美元；6 月，总市值约为 60 亿美元；8 月，总市值破 100 亿美元；而在 2020 年年末，DeFi 代币总市值为 210 亿美元。DeFi 热度由此可见一斑。

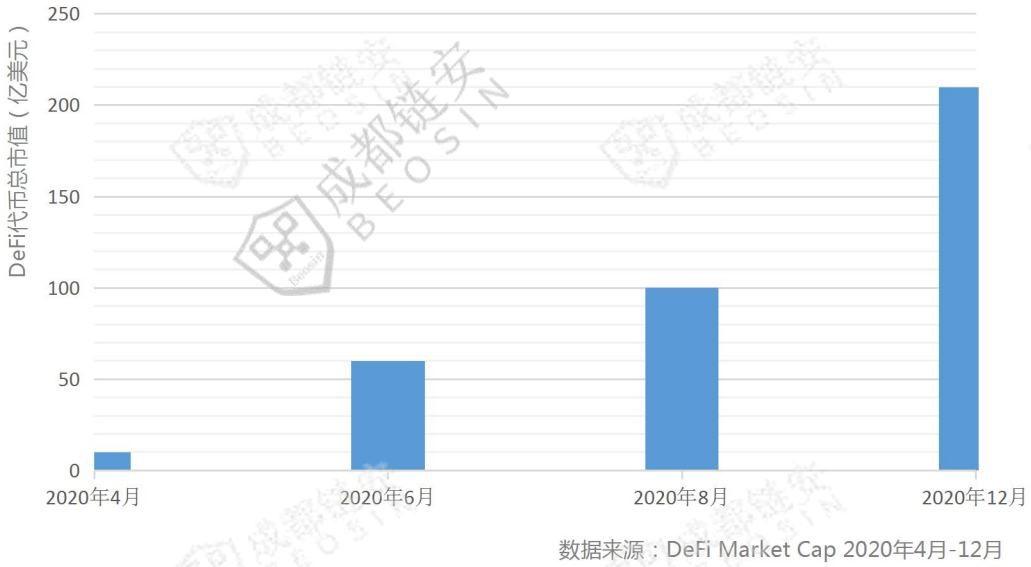


图 2：2020 年 4 月-12 月 DeFi 代币总市值

1.2 区块链安全挑战依然严峻

2020 年区块链行业正在加速演进，方兴未已；但伴随着整体发展态势如火如荼的同时，区块链生态所面临的安全挑战依然严峻。根据成都链安【链必安-区块链安全态势感知平台（Beosin-Eagle Eye）】所监测到的数据统计：2020 年，整个区块链生态造成的经济损失已超 38 万个 BTC，以币价 31600 美元来计算，总计损失约达 121 亿美元。

值得注意的是，据成都链安（Beosin）安全团队历年数据统计，2018 年区块链生态经济损失超 20 亿美元，2019 年区块链生态经济损失超 60 亿美元，而 2020 年区块链生态经济损失，甚至远超于前两年总和，呈“急剧爆发式”增长。

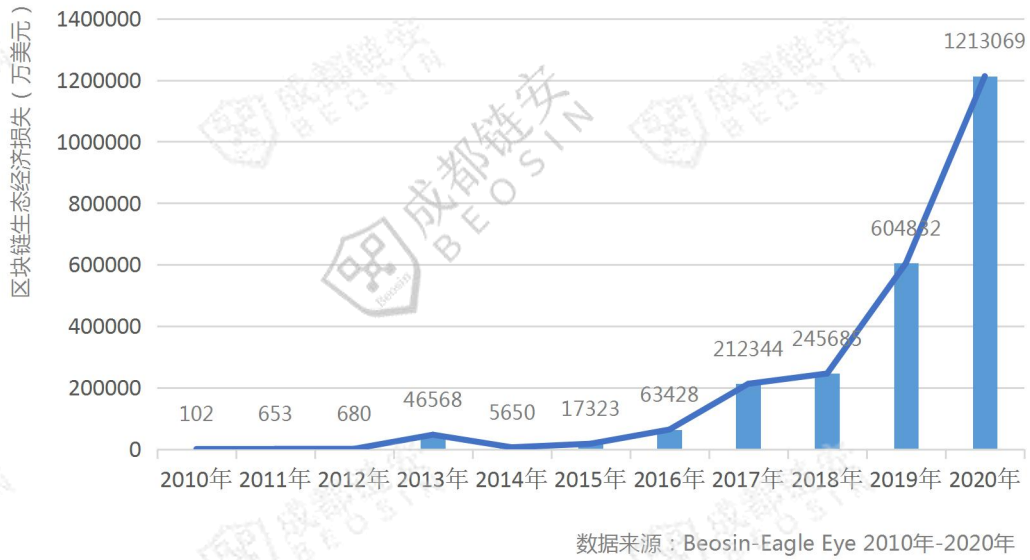


图 3：2010 年-2020 年区块链生态经济损失

经济损失方面，2010 年-2020 年呈整体逐步上升趋势。需要关注的是，自 2016 年以来，损失金额走势持续大幅走高；2020 年甚至出现了愈演愈烈的增长趋势。区块链生态安全现状令人堪忧，需要从业者清楚地意识到，达摩利斯之剑高悬。区块链行业蓬勃生命力的背后，无时无刻不面临着如影随形的安全风险。

背后原因方面，自 2016 年以来，区块链生态经济损失逐年增多，源于近几年来区块链行业进入到一个高速发展的阶段，伴随着区块链底层技术逐步走向成熟，区块链应用价值愈加获得认可，区块链生态所承载的经济效益逐年提升，随之而来的安全风险也愈发严峻。2020 年新冠肺炎疫情的冲击下，全球经济数字化转型步伐加快，以比特币为代表的虚拟资产普及程度提升且总市值不断突破历史新高，黑客与不法分子的犯罪行为随之更加猖獗。

反映问题方面，其一，整个区块链生态当下仍缺乏普适的安全标准和安全规范，行业乱象难以得到有效遏制；其二，区块底层技术在应用层、合约层、网络层、共识层分别仍然存在着各种不容忽视的安全风险；其三，区块链生态的安全监管进程亟待推进，如何实现高效可行的安全监管，是整个行业需要重点攻坚的难题所在。

1.3 区块链监管进程亟待推进

区块链安全现状所曝出的多方面安全风险，诸如各大交易所被盗事件频繁发生、智能合约漏洞凸显、利用虚拟资产进行非法犯罪、趋于活跃的暗网地下交易、日益突出的 DeFi 安全问题等等，都从根本上要求推动区块链监管进程建设迫在眉睫。

从技术特性上来看，区块链技术本身是一把“双刃剑”，其去中心化、难篡改、匿名等“基因特性”在推动新一轮技术变革和产业创新的同时，也为目前的安全监管工作带来严峻的挑战。其中，“去中心化”特性造成了监管主体不明确，监管范围模糊等客观问题难以避免；“难篡改”特性一定程度上增加了监管规则制定和执行的困难；“匿名”特性难以追踪，不法分子则很可能将区块链技术作为从事犯罪活动的新型手段。

从监管对象上来看，面对不同的监管主体，管理方式和监管手段也存在着显著的差异。其中，业务应用的监管主要针对需求方，目的在于为区块链需求方合规合

法地开展业务创造先行条件；技术的监管主要针对技术提供方，在鼓励技术发展的同时亦需兼顾技术风险的的法律责任；市场主体的监管则主要针对区块链服务的参与主体，旨在达到明确责任主体，推动行业有规可循，稳健发展。

从相关法规上来看，区块链监管进程亟待推进业已成为世界各国及从业者的普遍共识。2019 年 6 月，FATF（Financial Action Task Force）对于评估各国是否已采取必要行动来部署虚拟资产的相关监管标准达成一致，其发布的 INR15 规定各国及 VASP 必须在 2020 年 6月之前，开始执行 FATF 的监管要求。根据公开数据统计，2020 年已有多个国家相继发布了有关虚拟资产方面的政策法规，国际虚拟资产监管趋于合规化。

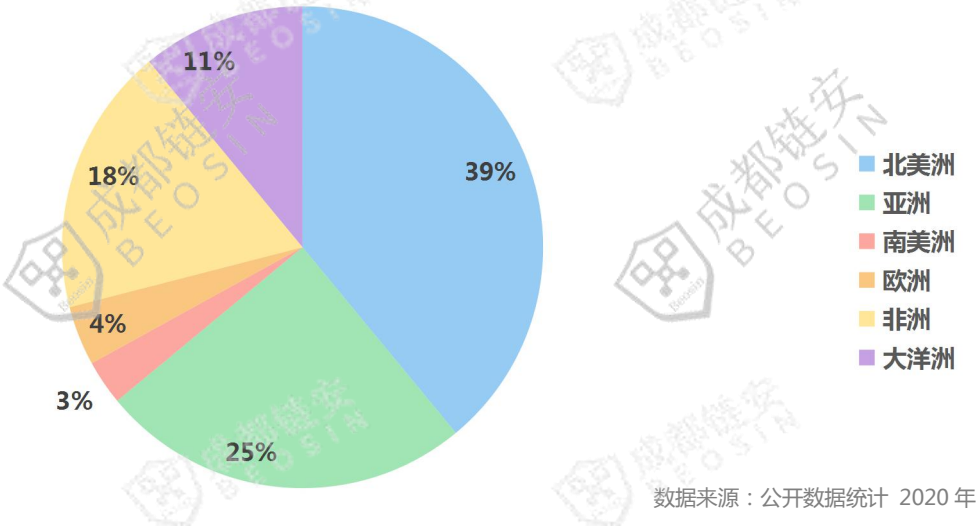


图 3：2020 年各洲发布有关虚拟资产政策法规占比

第二章 2020 年区块链安全事件全画像

2.1 区块链安全解决方案

基于 2020 年区块链生态的整体安全态势，如何针对当下区块链生态所面临的技术风险及监管风险两大层面，立足于区块链系统及应用的安全研发、安全运行、安全监管等场景，实现全流程闭环管理，并打造覆盖全生命周期的一站式区块链安全解决方案，是行而有效的关键措施。

总的来说，一站式区块链安全解决方案通过对区块链安全技术的研发及迭代，在积累海量区块链安全攻防实战的基础上，以“安全产品”和“安全服务”的形式为整个区块链生态提供全方位的安全支持，涵盖安全审计、安全检测、态势感知、渗透测试、安全防护、威胁情报、安全咨询、应急响应等方面，为区块链生态的安全发展实现保驾护航。

2.2 总体安全态势复盘

截至 2020 年 12 月 31 日，成都链安（Beosin）安全团队根据【链必安-区块链安全态势感知平台（Beosin-Eagle Eye）】监测到的数据统计梳理，2020 年区块链生态整体安全态势极为严峻，全球范围内所造成的经济损失已超 121 亿美元，涉案金额远超于前两年总和。2020 年已成为区块链生态安全领域的第一大

灾年。

2.2.1 安全事件高发

据不完全统计，放眼整个区块链生态，2020 年所发生的相关典型安全事件数量已超 270 起，相比于 2019 年，增长率达 54%。从数量走向上来看，全年安全事件呈爬坡式上升的趋势。其中，安全事件数量峰点在 9 月。值得关注的是，8 月、9 月、12 月安全事件均突破“30 起”关口，原因在于 8 月、9 月 DeFi 热潮以及 12 月以比特币、以太坊为代表的虚拟资产币价暴涨。

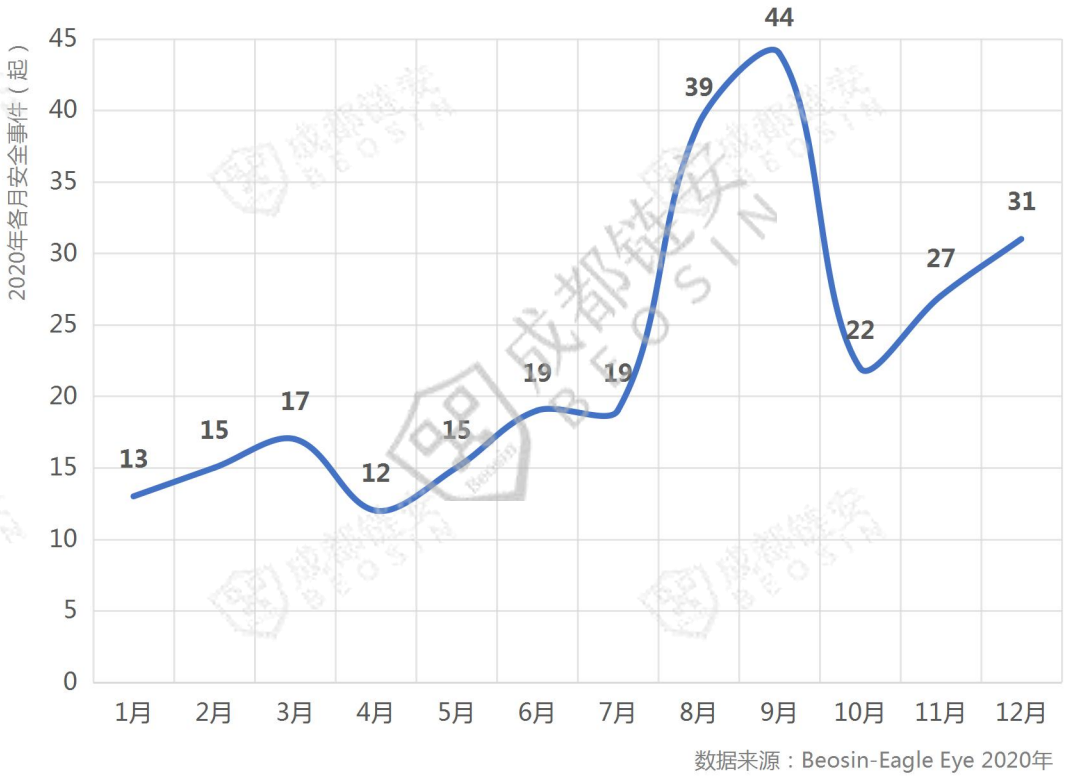


图 4：2020 年各月安全事件数量

2.2.2 经济损失严重

据不完全统计，2020 年整个区块链生态所造成的经济损失已超 121 亿美元，所暴露出的安全现状及潜藏的安全风险亟需从业者加强重视。从损失走向上来看，全年经济损失整体上呈现波动分布、单点爆发的趋势。值得关注的是，11 月经济损失“爆发式”升高，原因在于 11 月交易所方面涉案金额巨大。

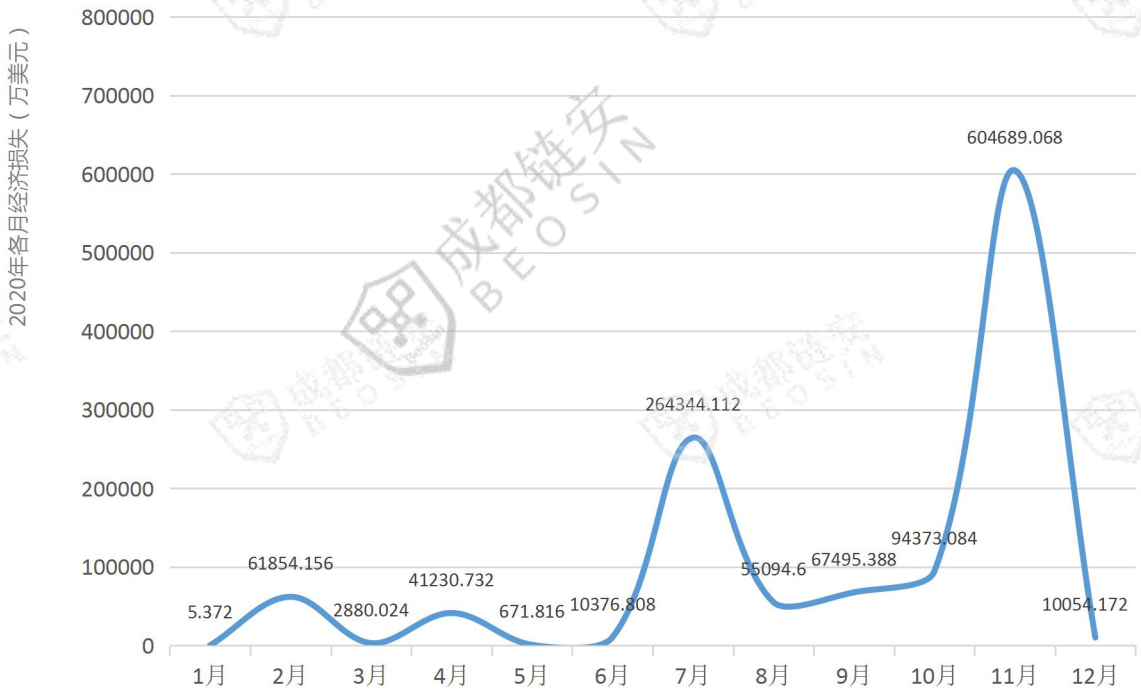
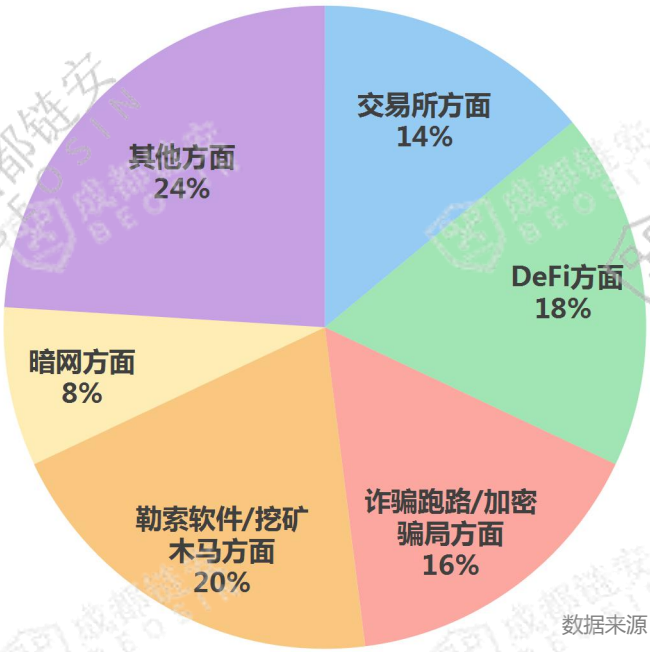


图 5：2020 年各月经济损失金额

2.2.3 分布类型多样

总的来看，2020 年区块链生态所造成的经济损失主要分布在以下几个方面：交

易所方面、DeFi 方面、诈骗跑路/加密骗局方面、勒索软件/挖矿木马方面、暗网方面、其他方面。其中，值得关注的是，勒索软件/挖矿木马方面、其他方面所发生的典型安全事件数量占比较高。



数据来源：Beosin-Eagle Eye 2020 年

图 6：2020 年典型安全事件数量占比

2.3 安全风险不容忽视

随着 2020 年区块链行业迎来新的发展时期，区块链作为“新基建”的重要组成部分，与实体经济和数字经济加速融合，稳步推进，区块链应用价值得到进一步凸显。与此同时，各类安全风险也伴随着区块链技术的大规模应用不断升级。总的来说，结合近年来区块链生态安全事件呈现画像，区块链行业主要的安全风险存在于技术层面和监管层面。

2.3.1 技术层面

区块链技术层面所面临的安全风险不仅存在区块链平台特性所带来的相关安全问题，也存在传统网络安全风险。主要包括：区块链底层平台、区块链中间协议层、区块链应用服务层。

2.3.1.1 区块链底层平台

区块链底层平台作为对上承载各类区块链应用、对下衔接网络底层平台的核心枢纽，为区块链应用落地提供了必需的存储、传输、计算、开发和测试等底层核心能力、资源和服务。因此，区块链底层平台的安全能力是确保区块链安全发展的关键所在。

2.3.1.2 区块链中间协议层

区块链中间协议层的安全风险，主要存在于智能合约及其共识机制，其主要面临成熟度不高的代码实现带来的安全风险。如利用智能合约逻辑、开发中存在的安全漏洞和后门，或智能合约运行环境中的虚拟机自身安全漏洞，或不完善的访问验证、控制等机制，攻击者可部署恶意智能合约代码以实施逃逸漏洞攻击、逻辑漏洞攻击、堆栈溢出漏洞攻击、资源滥用漏洞攻击等，实现不符合智能合约约定的操作。

2.3.1.3 区块链应用服务层

区块链应用服务层同样存在诸多安全风险。在应用服务层开发过程中存在的代码漏洞问题，尤其在第三方平台介入的应用场景下，更容易出现越权漏洞风险。钓鱼攻击、中间人攻击、木马劫持等传统网络攻击手段也会对上层区块链应用构成威胁。

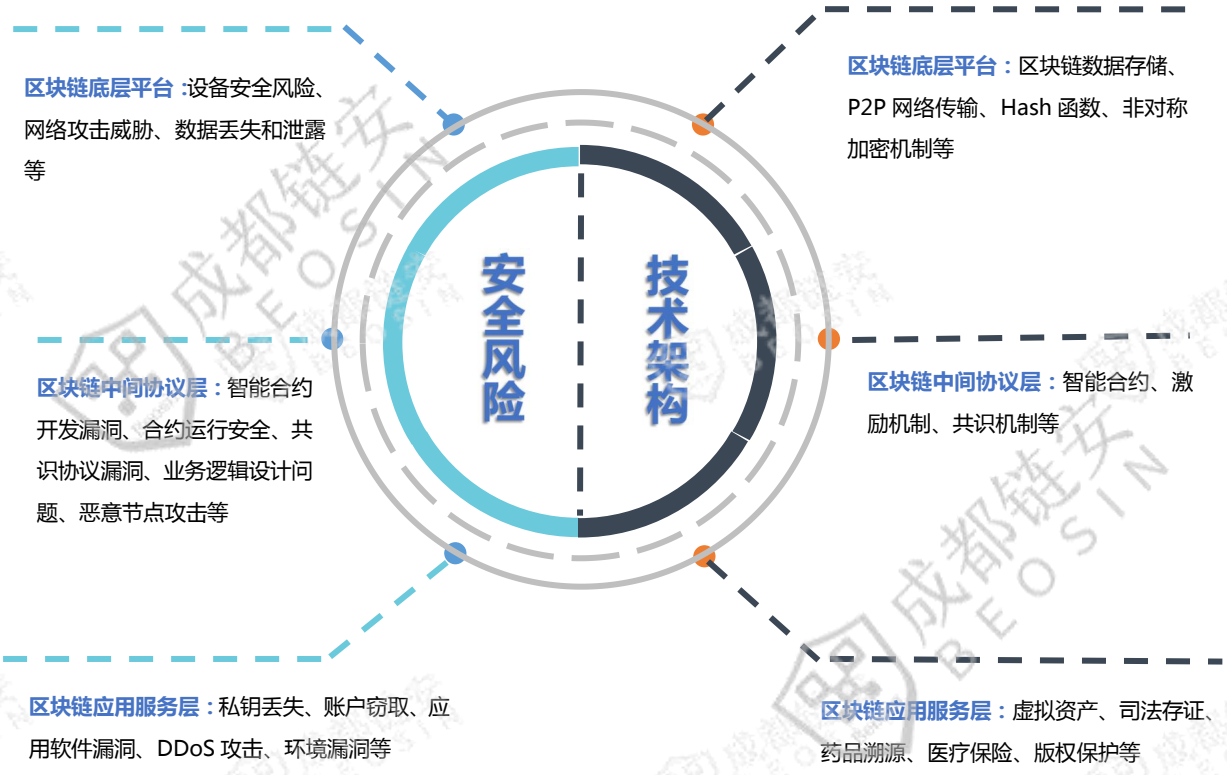


图 7：区块链行业技术架构及主要安全风险

2.3.2 监管层面

除区块链技术架构本身所存在的安全风险之外，其诸如去中心化、难篡改、匿名等“基因特性”也为区块链安全监管层面带来了不容忽视的挑战。具体表现为三个方面。一是区块链技术无国界限制，区块链网络节点可存在多个国家，链上产生的异常行为追踪，引发管辖权限困境、责任认定困境等问题。二是区块链的强隐秘性，无疑增加了安全事件和犯罪行为的追踪溯源难度。三是区块链的防篡改性，为有害信息、犯罪行为等形成天然庇护，向行业安全监管提出挑战。

第三章 2020 年区块链典型安全事件盘点

面对 2020 年区块链生态极为严峻的安全现状，成都链安（Beosin）安全团队通过梳理整年监测到的数据信息，细分为六大方面回顾 2020 年区块链生态各领域所发生的典型安全事件，以此复盘 2020 年区块链生态整体安全态势，以作警钟长鸣。

3.1 交易所方面典型安全事件

交易所是距离用户资产最近的地方，用于海量资产的管理存储及撮合交易，因此一直以来也是黑客首当其冲的攻击目标。作为区块链生态极其重要的一环，交易所的安全问题直接决定了整个行业的发展态势。

3.1.1 安全事件概览

▶Altsbit 交易所遭攻击后关闭

2 月 5 日，意大利交易所 Altsbit 存放热钱包私钥的服务器被入侵，导致损失了 6.929 个 BTC、23 个 ETH，以及其他数量的虚拟资产，随后交易所宣布于 5 月 8 日关闭。

▶VBITEX 交易所被入侵

2 月 17 日，VBITEX 交易所发布公告称被黑客入侵，导致平台数据被恶意篡改、虚拟资产被盗。

▶Coinhako 交易所遭攻击后限制用户取款

新加坡交易所 Coinhako 在遭受攻击后限制用户取款，Coinhako 发言人实施账户限制是防止“未经授权的交易”。

▶OKEx、Bitfinex 相继遭 DDoS 攻击

OKEx、Bitfinex 等交易所相继遭 DDoS 攻击，纷纷出现宕机等情况，OKEx 宣称遭到至少 600G 流量 DDoS。

▶Bisq 交易所被盗

4 月 9 日，虚拟资产交易所 Bisq 被盗，攻击者利用 Bisq 交易协议中的一个缺陷，针对单笔交易来窃取交易资金，造成 7 名受害者共损失 3 个 BTC 和 4000 个 XMR。

▶币安交易所遭攻击导致合约页面大范围卡顿

4 月 29 日，币安交易所遭到攻击并导致合约页面大范围卡顿，甚至打不开页面。

▶Youbi 交易所遭 DDoS 攻击

5 月 6 日，自 Youbi 交易所开启平台币认购后，连续 3 天遭遇大流量 DDoS 攻击，造成服务器短时间无法访问。

▶Upbit 交易所被盗资产发生大规模转移

5 月 14 日，Upbit 交易所被盗资产发生大规模转移。黑客团伙将赃款通过多层中间地址层层转移，切分转移后使用大量充币地址将赃款转入多个交易所。

▶UEX 交易所遭黑客攻击

5 月 27 日，UEX 交易所在 20：00 正式开启交易对后，平台遭遇黑客入侵和攻击，用增发的 UEX 对盘面进行不计成本地砸盘。

▶LMEX 联交所遭黑客入侵

5 月 27 日，LMEX 联交所在社群发布关于交易所运营调整通知称：平台遭黑客入侵被盗损失了 15 万个 USDT，致使平台资不抵债。

▶Cashaa 交易所被盗

7 月 12 日，英国 Cashaa 表示，黑客从其中一个钱包中窃取了超过 336 个 BTC。

▶ETERBASE 部分热钱包被盗

9 月 8 日，欧洲虚拟资产交易所 ETERBASE 遭遇黑客攻击，导致部分热钱包被盗，包括 BTC、ETH 及 ERC-20 代币、XRP、TRX、XTZ 和 ALGO，损失逾 500 万美元资产。

▶Deribit 遭遇 DDoS 攻击

9 月 22 日，加密衍生品交易所 Deribit 发推称凌晨遭遇 DDoS 攻击，使得平台服务器难以访问。

▶KuCoin 交易所遭黑客攻击

9 月 26 日，KuCoin 库币交易所遭到黑客攻击，大量 ETH 和 ERC20 代币被转移，其中包括 11486 个 ETH、19788586 个 USDT、525405 个 GLA 等。此后，该黑客跑路资金遭到各个大交易所联合封堵。

▶Bitbay 交易所再次突然宕机

10 月 13 日，爱沙尼亚交易所 Bitbay 在 0 时 28 分左右突然宕机，后于 2 时 10 分左右恢复。这是该交易所今年第二次突然宕机，3 月份曾出现过一次长达 18 小时的宕机。

▶Liquid 交易所数据泄露

11 月 13 日，虚拟资产交易所 Liquid 发布通知称，发生了一起数据泄漏安全事件。

▶Bitcoin.org 遭到 DDoS 攻击

12 月 19 日，Bitcoin.org 遭到 DDoS 攻击，导致该网站瘫痪。

▶Exmo 交易所发生重大安全漏洞

12 月 21 日，英国虚拟资产交易所 Exmo 发生重大安全漏洞，导致平台已冻结

所有提款。根据 The Block 研究分析师说法，Exmo 或损失了 1050 万美元的资金。

▶Livecoin 遭到所谓的“精心计划的攻击”

12 月 24 日，俄罗斯虚拟资产交易所 Livecoin 遭到了所谓的“精心计划的攻击”。该交易所失去了对所有服务器、后端和节点的控制权，并恳请用户停止存款、交易或与该交易所进行互动。

3.1.2 安全建议

- 交易所应建立完善的安全风控应急预案，以及时响应并处置各类黑客攻击事件的发生。
- 交易所应建立全面的安全防护机制，加固平台自身安全架构，并适时对平台进行来自第三方安全公司的整体安全测试。
- 加强对内部员工和用户的安全意识普及，避免出现监守自盗的情况。

3.2 DeFi 方面典型安全事件

根据 DeFiPulse 数据统计，DeFi 生态在 2020 一年间锁仓价值由年初的 6.6 亿美元上升至年末的 143 亿美元，实现年内累计涨幅近 2000%的飞速增长。由于 DeFi 热潮的兴起，该领域也自然成为了 2020 年黑客“大展拳脚”的重点对象。

3.2.1 安全事件概览

▶bZx 遭遇两次闪电贷攻击

2 月 15 日，DeFi 贷款协议 bZx 遭受攻击，攻击者同时跨多个协议完成了一笔闪电贷杠杆套利交易，导致价值 35 万美元的 ETH 被盗。2 月 18 日，bZx 再次遭受闪电贷攻击，攻击者通过控制预言机价格获利 2388 个 ETH，约 64.4 万美元。

▶Curve V4 流动性不充足进行超大额的兑换

2 月 28 日，一名用户在 Curve V4 流动性不充足的前提下进行了超大额的兑换，虽然团队发现了该事件，并立即进行了补救，但这名用户最终还是损失了 14 万美元的资产。

▶MakerDAO 清算机制异常

3 月 12 日，由于以太坊币价暴跌，MakerDAO 的大量抵押债仓跌破清算门槛，引发了清算程序执行。原本应该参与到清算过程中的清算机器人（Keeperbot）因设置了较低的 gas 值，导致出价受阻，一位清算人在没有竞争者的情况下，以 0DAI 的出价赢得了拍卖。

▶Synthetix 公开合约漏洞

Defi 项目 Synthetix 公开了一个合约漏洞，不过该合约尚未启用因此未产生损失。该漏洞存在于 Synthetix 合约的清算接口。在正常情况下用户质押 ETH 而

获得 SETH，在抵押期过后进行资产清算，调用清算接口返还 SETH 获得 ETH；然而该漏洞可导致任意用户都可以直接 Burn 掉其他用户抵押的 SETH 进而获得 ETH。

▶Uniswap 的 ERC777 重入风险

4 月 18 日，黑客利用 DeFi 平台 Uniswap 和 ERC777 标准的兼容性问题缺陷，对 Uniswap 实施了重入攻击。黑客在交易 ETH-imBTC 时，利用 ERC777 标准中进行转账的 tokensToSend 回调函数实现了重入攻击，总获利 34 万美元。

▶DeFi 平台 Lendf.Me 遭受重入漏洞攻击

4 月 19 日，以太坊 DeFi 平台 Lendf.Me 遭受重入漏洞攻击，损失约 2500 万美元。

▶DeFi 项目 Hegic 代码出现漏洞

4 月 27 日，DeFi 项目 Hegic 代码出现漏洞导致用户资产被用户永久锁定。在该项目上线几小时后，其代码中的一个错误锁定了该平台智能合约价值 2.8 万美元的用户资金，由于该漏洞将资金锁定在了过期合约中，使其无法被访问。

▶Bancor 新合约出现安全漏洞

6 月 18 日，由于新的 Bancor Network 合约上未经验证的 safeTransferFrom () 函数，用户资金即将被耗尽。

▶Balancer 流动性池两次遭黑客闪电贷攻击

6 月 29 日，知名 DeFi 平台 Balancer 流动性池遭黑客闪电贷攻击，损失 50 万美元。Balancer 上遭遇损失的为 STA 和 STONK 两个代币池，目前这两个代币池的流动性已枯竭。6 月 30 日，黑客再次利用 dYdX 的闪电贷攻击了 Balancer 部分流动性矿池中的 COMP 交易对，将池子中未领取的 COMP 奖励抽走，获利 10.8 个 ETH，约合 2408 美元。

▶VETHer (VETH)遭黑客攻击

7 月 1 日，VETH 在去中心化交易所 Uniswap 遭遇黑客攻击。黑客仅使用 0.9 个 ETH 就盗走了 919299 个 VETH，价值约为 90 万美元。

▶Opyn 看跌期权被外部参与者恶意利用

8 月 5 日，链上期权平台 Opyn 披露其以太坊看跌期权被外部参与者恶意利用。Opyn 指出，除以太坊看跌期权外的所有其他 Opyn 合约均不受此漏洞的影响。攻击者双重利用 oToken 并窃取了看跌期权卖方的抵押资产。

▶DeFi 项目 YAM 合约存在漏洞

8 月 13 日，知名以太坊 DeFi 项目 YAM 官方表明发现合约中存在漏洞，24 小时内价格暴跌 99%，导致了治理合约被“永久破坏”，价值 75 万美元的 Curve 代币被锁定而无法使用。

▶DeFi 项目 YFValue 在 YFV 质押池中发现漏洞

8 月 25 日，DeFi 项目 YFValue（YFV）官方称，团队在 YFV 质押池中发现一个漏洞，恶意参与者借此漏洞对质押中的 YFV 计时器单独重置，1.7 亿美元资金存在被锁定风险。

▶Degen.Money 利用双重授权漏洞获取用户资金

DeFi 流动性挖矿项目 Degen.Money 利用双重授权漏洞（Double Approval Exploit）来获取用户资金。

▶SushiSwap 仿盘智能合约均存在漏洞

SushiSwap 仿盘 YUNo Finance（YUNO）与 KIMCHI.finance（KIMCHI）智能合约均存在漏洞。智能合约拥有者可以利用漏洞，无限制地增发项目对应的代币数目，继而导致通胀并最终崩溃。

▶BaconSwap 和 shroom.finance 均存在时间锁定漏洞

9 月 3 日，以太坊研发者 Philippe Castonguay 称 DeFi 项目 BaconSwap 和 shroom.finance 均存在时间锁定漏洞，将允许项目所有者在没有时间锁定的情况下无限增发代币。

▶EOS 项目 EMD 跑路

9 月 9 日，EOS 项目 EMD 疑似跑路。项目合约 emeraldmine1 向某账号转移 78 万个 USDT、49 万个 EOS 及 5.6 万个 DFS。

▶DeFi 流动性挖矿项目“珊瑚”遭攻击

9 月 10 日，EOS 生态 DeFi 流动性挖矿项目“珊瑚”的 wRAM 遭到黑客攻击，损失逾 12 万个 EOS。

▶YFI 仿盘 rebase 机制漏洞获利

YFI 仿盘 Soft Yearn 的一名用户因 rebase 机制漏洞用 200 美元获得了 25 万美元的回报。

▶Soda Finance 存在智能合约安全漏洞

9 月 21 日，Soda Finance 被爆出存在智能合约安全漏洞。该漏洞允许任意外部调用者通过调用智能合约函数，无视受害用户债务中的代币数目，强行结算受害用户的债务，并将通过结算操作所得的收益转入到自己的收款地址，最终项目损失约 105 万人民币。

▶GemSwap 遭到项目拥有者后门攻击

9 月 26 日，DeFi 项目 GemSwap 遭到项目拥有者的后门攻击。项目拥有者通过调用后门函数 emergencyWithdraw ()将所有的流动性证明取出并转移至自己拥有的账户中，最终项目损失约 850 万人民币。

▶Eminence（EMN）遭遇闪电贷攻击

9 月 29 日，yearn.finance 创始人 Andre Cronje 刚推出的游戏项目 Eminence（EMN）遭遇闪电贷攻击，黑客将 800 万美元的资金返还给了 yearn 部署者合

约。

▶DeFi Saver 交易所漏洞致 31 万 DAI 被盗

10 月 8 日，去中心化钱包 imToken 表示，用户报告称 31 万个 DAI 被盗，这与 DeFi Saver Exchange 漏洞有关。

▶以太坊项目 WLEO 合约遭黑客攻击

10 月 11 日，以太坊项目 WLEO 合约遭到黑客攻击，导致价值 4.2 万美元的资金被盗。黑客通过向自己铸造 WLEO，并将其换成 ETH，从去中心化交易所 Uniswap 的池中窃取了 ETH。

▶Harvest.finance 遭闪电贷攻击

10 月 26 日，DeFi 挖矿项目 Harvest.finance 被使用闪电贷功能实现了巨额套利。Harvest 官方解释称，这次套利攻击起源于一笔巨额闪电贷，并通过多次操纵 Curve y Pool 的价格，以套取 fUSDT、fUSDC 的价差进而获利。

▶黑客利用 Axion Staking 合约的 unstake 函数设法铸币

11 月 2 日，黑客利用 Axion Staking 合约的 unstake 函数设法铸造了约 800 亿个 AXN 代币。黑客随后将 AXN 代币在 Uniswap 交易所中兑换以太币，重复此过程，直到 Uniswap 中 ETH-AXN 交易对的以太币被耗尽，同时 AXN 代币价格降至 0。该攻击是内部操作造成的，该内部操作通过在部署代码时，对项目依赖的 OpenZeppelin 依赖项注入恶意代码，最终损失约 330 万人民币。

▶SharkTron 匿名开发者跑路

11 月 10 日，基于 Tron 区块链 DeFi 项目、JustSwap 白名单项目 SharkTron 的匿名开发者 Daniel Wood 跑路，推特用户报告称损失了 3.66 亿至 4 亿个 TRX，价值约 1000 万美元。

▶Akropolis 合约遭多次连续重入攻击

11 月 13 日，黑客利用 Akropolis 项目存在的存储资产校验缺陷，向合约发起连续多次的重入攻击，致使 Akropolis 合约在没有新资产注入的情况下，凭空增发了大量的 pooltokens，进而再利用这些 pooltokens 从 YCurve 和 sUSD 池子中提取 DAI，最终导致项目合约损失了 203 万个 DAI。

▶Value DeFi 协议遭闪电贷攻击

11 月 15 日，Value DeFi 协议遭到了闪电贷攻击。攻击者从 Aave 协议借了 80000 个 ETH，执行了一次闪电贷攻击，在 DAI 和 USDC 之间进行套利。攻击者在利用 740 万美元 DAI 后，向 Value DeFi 退还了 200 万美元，保留了 540 万美元，净损失达 600 万美元。

▶Cheese Bank 遭攻击损失 330 万美元

11 月 16 日，基于以太坊的去中心化自治数字银行平台 Cheese Bank 因黑客攻击遭受了 330 万美元的损失。黑客通过利用基于自动做市商（AMM）的预言机在 dYdX、Uniswap 等平台上进行了一系列恶意借贷操作，共导致价值超 330

万美元的损失。

▶OUSD 遭闪电贷+重入攻击

11 月 17 日，DeFi 协议 Origin Protocol 稳定币 OUSD 遭到攻击，攻击者利用 dYdX 的闪电贷进行重入攻击，造成价值 770 万美元的 ETH 和 DAI 的损失。

▶Pickle Finance 未经审核的合约漏洞被利用

11 月 22 日，DeFi 项目 Pickle Finance 因被黑客攻击未经审核新创建的智能合约漏洞，损失近 2000 万美元的 DAI。

▶Compound 喂价错误致 9000 万美元资产遭清算

11 月 26 日，Compound9000 万美元资产遭清算。Debank 创始人 hongbo 表示，Compound 巨额清算事件其实是因预言机数据源 Coinbase Pro 的 DAI 价格剧烈波动而导致，通过操控预言机所依赖的信息源可以实现短时间的价格操纵，以误导链上价格。

▶Sushi Swap 遭到流动性提供者攻击

11 月 30 日，以太坊 AMM 代币兑换协议 Sushi Swap 遭到流动性提供者攻击，损失约 1.5 万美元。

▶Compounder.Finance 项目智能合约发生数笔大量代币交易

12 月 1 日，Compounder.Finance 项目智能合约发生数笔大量代币的交易。经

过仔细验证得知这些交易为内部操作，项目拥有者将大量数额代币转移到自己的账户中。经统计，最终共损失价值约 7610 万人民币的代币。

▶DeFi 保险协议 Nexus Mutual 创始人个人地址被攻击

12 月 14 日，DeFi 保险协议 Nexus Mutual 表示，其创始人 Hugh Karp 的个人地址被一位平台用户攻击，被盗 37 万个 NXM，损失超过 800 万美元。官方表示这是一次具有针对性的攻击，只有 Karp 的地址受到影响，Nexus Mutual 或其他成员没有后续风险。

▶Warp Finance 遭遇闪电贷攻击

12 月 18 日，流动性 LP 代币抵押借贷 DeFi 协议 Warp Finance 遭遇闪电贷攻击，约 800 万美元被盗。据称，闪电贷攻击者最多可盗走价值 770 万美元的稳定币，不过 Warp Finance 团队已拟定计划来追回仍在抵押金库中的价值约 550 万美元的稳定币。

▶Cover 合约漏洞遭黑客攻击

由于奖励合同中的一个漏洞，Cover Protocol 损失了 300 万美元。此外，已有攻击者利用 Cover 合约共增发了约 1 万个 COVER，并且已将其换成了 WBTC 和 DAI 等资产。

3.2.2 安全建议

- 项目上线前，DeFi 项目方应做好前置预防工作，寻求第三方安全公司进行严格的安全审计，排查已知的各类安全漏洞。
- 项目上线后，DeFi 项目方应联合第三方安全公司，引入一整套态势感知、威胁情报、安全响应等全生命周期的安全解决方案，完善安全防护机制。
- 作为用户，在选择项目时，应留意该项目是否经过第三方安全公司的安全审计，是否具备权威的安全审计报告，切不可掉以轻心。

3.3 诈骗跑路/加密骗局方面典型安全事件

随着区块链价值愈发得到认可，虚拟资产普及程度亦愈发得到扩散，不少投机者及诈骗者开始利用大众对于区块链和虚拟资产的知识盲区炮制骗局，加之波及人数多、遍布区域广、涉案金额高等原因推波助澜，进而导致该领域安全事件高发，经济损失严重。

3.3.1 安全事件概览

▶比特币虚假二维码骗局

3 月 29 日，有网站声称免费将用户的比特币地址映射成二维码，便于用户收钱转账；生成的二维码实则为黑客地址，该黑客地址已有超过 0.6 个 BTC 的转入。

▶雪碧交易所开盘即归零

3 月 12 日，雪碧交易所上线空气币 PETH，开盘即归零。所有受害者皆为前期

私募受害者，额度在 80 个 USDT 到 1000 个 USDT 不等，约为 228 人。初步估计涉及金额约 40 万人民币，有大学生不幸涉及其中。

▶区块链资金盘硅谷区块鸡疑似跑崩盘路

3 月 30 日，硅谷区块鸡是典型的虚拟宠物类资金盘，类似于区块猫，区块狗，低价买入宠物，一段时间后高价卖出。此类加密骗局实则为击鼓传花类资金盘，直到无人接盘，即是项目崩盘的时刻。

▶EOS 生态资金盘跑路

4 月 19 日，运营超过一年半的 EOS 生态资金盘项目跑路，其充币地址 w.io 频繁向其他地址转账，露出转移资产套现的意图。链上数据追踪显示，EOS 生态的资金最终汇集到 4 个主要的 EOS 地址，总计超过 2000 万 EOS，涉及金额超 3.6 亿元。

▶Telegram 搬砖套利骗局

Telegram 搬砖套利骗局仍在流行。近期多名用户被骗超过 900 个 ETH。尽管无论是 Huobi 方面还是 imtoken 钱包方都曾发表过官方声明，然而此类骗局还是时常有用户上当受骗。

▶虚假 imtoken 官方电报群

钓鱼账号创建的虚假 imtoken 官方电报群充当官方技术人员的身份，引导搬砖套利。被骗用户在指定网站输入私钥进行所谓的交易回滚操作，遭到二次诈骗，

被骗用户资金已经部分流入交易所。

▶冒充 Voice 官方账号诱骗用户充值的骗局

EOS 主网上存在冒充 Voice 官方账号诱骗用户充值的骗局，目前两个骗局的充币地址月超过 9000 个 EOS。

▶骗子冒充波场创始人孙宇晨

骗子冒充波场创始人孙宇晨，使用伪造的孙宇晨的视频诱导受害者进行“现场”通话。他们邀请受害者与孙宇晨一起“现场”Skype 通话，企图从毫无戒心的受害者那里窃取钱财。

▶百慕大交易所涉嫌大量侵吞用户资金

6 月 11 日，用户爆料称百慕大交易所涉嫌大量侵吞用户资金，疑似已携款跑路。

▶Twitter 诸多账号被黑客攻击并发布钓鱼信息

7 月 16 日，包括比尔·盖茨，奥巴马，埃隆·马斯克，苹果官方账号等在内的诸多 Twitter 账号被黑客攻击并发布比特币钓鱼信息。经查询黑客留在推特上的地址发现，该地址目前已经收到了 12.86 个 BTC。

▶某 YouTube 频道遭到黑客攻击

8 月 5 日，拥有 26.2 万名订阅用户的 YouTube 频道遭到黑客攻击，频道名称被改为 NASA News，并开始直播关于 SpaceX CEO 埃隆·马斯克赠送比特币的虚

假消息。约两个小时内，非法获利 4000 美元。

▶Uniswap 出现 SRM 假币

8 月 7 日，Uniswap 出现 SRM 假币，已有用户被骗。Serum 发布推特提醒用户提高警惕，在除 FTX 和 BitMax 平台以外的其他交易平台（如 Uniswap 等）出现的 SRM，均为假冒。

▶Bantiample 团队砸盘套现跑路

9 月 19 日 ,币安智能链上的项目 Bantiample 团队已砸盘套现 3000 个 BNB 跑路，团队的主要开发者已经删除 Telegram 账号，项目代币 BMAP 单日跌幅超过 90%。

▶以太坊挖矿项目 LV Finance 跑路

9 月 20 日，以太坊挖矿项目 LV Finance 疑似跑路，不到一个小时已有 400 万被转走，该项目通过伪造虚假审计网站并提供虚假审计信息诱骗投资者进行投资，待一段时间后资金池内金额足够大时进行跑路。

▶SushiSwap 仿盘项目 GemSwap 跑路

9 月 26 日，名为 GemSwap 的 SushiSwap 仿盘项目被曝跑路，LP 被卷走。查询发现，该项目在 15 点左右发布推特，自曝其遭受了“whatitdobb”开发者的攻击。据了解，该项目早些时候完成了流动性迁移，但发起攻击的开发者在迁移之前就获得了相关许可，能够将流动池中的代币取走。

▶大富翁项目砸盘 90%跑路

12 月 1 日，大富翁项目私自篡改合约转移用户资产，抽取超 1 亿 GOLD 代币后，砸盘 90%跑路。

▶比特币广告方案骗局

12 月 16 日，一个欺诈性的比特币广告方案通过未经授权的名人图片吸引了数千名受害者，该骗局已被追查到来自俄罗斯。

▶OneCoin 虚拟资产庞氏骗局

12 月 14 日，阿根廷科尔多瓦市检察院起诉了涉及 OneCoin 虚拟资产庞氏骗局案件的 12 名诈骗者。据报道，OneCoin 庞氏骗局使相关投资者在从 2014 年 4 月至 2018 年 3 月期间因投资该项目遭受了共 44 亿美元的财务损失。

3.3.2 安全建议

- 作为用户和投资者，应提高警惕，谨慎甄别投资产品和投资项目，不盲从，不跟风。
- 加强自身安全意识和防骗意识，谨慎分辨网络上的有关消息，切莫掉进圈套。
- 行业各方从业者应积极配合相关部门，推动整个区块链生态安全监管的进程建设。

3.4 勒索软件/挖矿木马方面典型安全事件

近年来，勒索软件/挖矿木马方面发生的安全事件呈爆发态势；该类型安全事件的发生通常会造成全球性的波及，攻击目标也逐渐从个人转向金融机构、跨国企业，甚至是政府网站。勒索软件方面，黑客一般会通过钓鱼攻击、病毒软件、漏洞攻击锁定受害人的网络设备或加密重要文件，以此勒索指定虚拟资产；而挖矿木马方面，则会利用挖矿木马和蠕虫来完成大量计算以获取虚拟资产，在计算过程中，计算机大量的 CPU、GPU 资源被占用，将导致计算机变得异常卡慢，干扰正常系统运行。

3.4.1 安全事件概览

▶Grubman Shire Meiselas & Sacks 受到 REvil 勒索软件攻击

Grubman Shire Meiselas & Sacks 已受到 REvil（Sodinokibi）勒索软件的攻击，攻击者威胁要分 9 次发布高达 756 GB 的被盗数据。被盗数据包括保密合同、电话号码、电子邮件地址、个人通信、保密协议等。

▶Fresenius 集团遭 Snake 勒索软件攻击

5 月 5 日，欧洲最大私人医院的德国 Fresenius 集团遭 Snake 勒索软件攻击，Snake 在加密计算机文件之后要求限期支付比特币形式的赎金，否则会将公司内部文件发布到网上。

▶Ghost 博客平台服务器被黑客攻击

5 月 6 日，Ghost 博客平台服务器被黑客攻击。黑客利用 CVE-2020-11651（身份验证绕过）和 CVE-2020-11652（目录遍历）来控制其 Salt 主服务器并安装了虚拟资产挖掘软件。

▶H2Miner 黑产团伙入侵企业主机进行挖矿

H2Miner 黑产团伙利用 SaltStack 远程命令执行漏洞入侵企业主机进行挖矿。截止 5 月 6 日，H2Miner 黑产团伙通过控制服务器进行门罗币挖矿已非法获利超 370 万元人民币。

▶Souleman 矿工利用永恒之蓝漏洞攻击企业

Souleman 矿工利用永恒之蓝漏洞攻击企业并下载由 XMRig 编译的门罗币挖矿程序，该团伙已通过挖矿和剪切板劫持数字交易获利超过 27 万元人民币。

▶英国肯特郡公司 KCS 遭勒索攻击

英国肯特郡公司 KCS 遭勒索攻击，黑客要求 80 万英镑赎金，否则将在暗网上泄露该公司的数据。KCS 方面表示，该公司并没有支付赎金，也没有涉及纳税人的个人数据被盗。

▶诈骗者利用 SIM 欺骗攻击窃取比特币

6 月 2 日，Reddit 用户 Gandeloft 称在 HodlHodl 平台上进行的 P2P 比特币交易出现了问题。诈骗者利用 SIM 欺骗攻击窃取比特币，虽然用户并没有在

Revolut 上看到这笔钱，但骗子成功向受害者施压，让他从第三方托管中释放了比特币。

▶勒索软件 NetWalker 攻击三所美国大学

勒索软件 NetWalker 攻击三所美国大学，并窃取了这些学校的敏感数据，包括学生姓名、社会安全号码和财务信息。NetWalker 威胁这些学校支付比特币赎金，若不支付赎金，将在一周内泄露这些数据。

▶Kingminer 僵尸网络黑客攻击微软 SQL server 数据库

英国网络安全公司 Sophos 指出 Kingminer 僵尸网络背后的黑客于 6 月 8 日至 12 日期间攻击微软的 SQL server 数据库，并安装了加密矿机程序 XMRig，以挖掘门罗币。

▶饮料巨头 Lion 遭遇两次勒索软件袭击

澳大利亚饮料巨头 Lion 在不到一周内遭遇了两次勒索软件的袭击，据称 Lion 被勒索软件袭击破坏了其 IT 基础设施。勒索软件组织 REvil 最初要求以门罗币支付 80 万美元的赎金；如果 Lion 未能在 6 月 19 日之前汇出这笔款项，该组织将把赎金翻倍至 160 万美元。

▶恶意 Docker 镜像隐藏虚拟资产挖矿代码

黑客利用恶意 Docker 镜像隐藏虚拟资产挖矿代码，以开采门罗币。

▶新型恶意软件 Lucifer

安全公司 Unit 42 的研究人员发现一种新的恶意软件 Lucifer，该软件是某种旧的虚拟资产勒索软件的变种。新的变体可用于恶意虚拟资产挖矿以及进行 DDoS 攻击。

▶加州一医学院遭遇黑客袭击

6 月 30 日，加州一医学院遭遇黑客袭击，研究人员无法访问网络上的加密数据。该校已向黑客的钱包中转移了 116.4 个 BTC，以换取解锁加密数据的工具，并归还他们获得的数据。

▶国内大量企业遭遇亡命徒（Outlaw）僵尸网络攻击

腾讯安全威胁情报中心检测到国内大量企业遭遇亡命徒（Outlaw）僵尸网络攻击。亡命徒（Outlaw）僵尸网络已造成国内约 2 万台 Linux 服务器感染，影响上万家企业。其主要特征为通过 SSH 爆破攻击目标系统，同时传播基于 Perl 的 Shellbot 和门罗币挖矿木马。

▶Garmin 受到 WastedLocke 勒索软件攻击

黑客要求 Garmin 支付 1000 万美元赎金以恢复 Garmin 系统。Garmin 内部员工证实，Garmin 受到了名为 WastedLocke 的勒索软件的攻击。这是一款新的勒索软件，由恶意软件开发团队 Evil Corp 运营。

▶佳能 Canon 遭到 Maze 团伙勒索软件攻击

跨国公司佳能（Canon）的电子邮件、存储服务和其美国网站遭到了 Maze 团伙的勒索软件攻击。Maze 要求佳能支付虚拟资产赎金，否则将泄露其照片和数据。

▶Brown-Forman Corp 遭到勒索软件犯罪团伙 REvil 袭击

勒索软件犯罪团伙 REvil 声称已成功袭击了美国葡萄酒和烈酒巨头 Brown-Forman Corp。该公司拒绝支付 REvil 要求的门罗币赎金。作为回应，黑客在其暗网官方博客以大约 150 万美元的价格出售被盗数据。

▶阿根廷官方移民局遭遇 Netwalker 勒索软件攻击

阿根廷官方移民局 Dirección Nacional de Migraciones 遭遇 Netwalker 勒索软件攻击，暂时停止了出入该国的边境。黑客要求赎金 400 万美元。阿根廷政府拒绝与黑客谈判，也不会支付赎金。

▶智利三大银行之一 Banco Estado 受到 REvil 勒索软件网络攻击

据悉，智利三大银行之一的 Banco Estado 银行不得不关闭其全国性业务，原因是受到了 REvil 勒索软件的网络攻击。REvil 以拍卖在攻击中窃取的数据而闻名，并经常要求使用门罗币支付赎金。

▶巴基斯坦电力生产商 K-Electric 遭遇勒索软件攻击

巴基斯坦最大的电力生产商 K-Electric 遭遇勒索软件攻击，黑客索要约 770 万美元的比特币赎金。

▶数据中心和托管巨头 Equinix 遭到 Netwalker 勒索软件攻击

数据中心和托管巨头 Equinix 遭到了 Netwalker 勒索软件攻击，威胁参与者要求 450 万美元购买一个解密器，以防止泄露被盗数据。

▶意大利跨国能源巨头 Enel Group 遭遇勒索软件攻击

意大利跨国能源巨头 Enel Group 遭遇勒索软件攻击，其计算机网络感染了名为 NetWalker 的 Windows 勒索软件。据悉，NetWalker 黑客公布了大约 5TB 被盗数据的截图，并威胁 Enel Group 支付 1234 个 BTC（约合 1680 万美元）作为赎金。

▶以色列无线芯片和摄像头传感器制造商遭勒索软件攻击

9 月 7 日，黑客向以色列纳斯达克上市无线芯片和摄像头传感器制造商 Tower Semiconductor Ltd（TSEM）进行勒索软件攻击，并索要数十万美元比特币赎金。为了安全起见，TSEM 关闭了一些正在运行的服务器，并暂停了部分工厂的生产。

▶芬兰数万名患者机密就医记录遭到黑客攻击

10 月 28 日，芬兰数万名接受心理治疗的患者的机密就医记录遭到黑客攻击，其中一些被泄露到网上。许多患者收到了要求支付 200 欧元比特币的电子邮件，称如不交付赎金，他们与治疗师讨论的内容将被公之于众。

▶保险公司 Shirbit 遭遇黑客组织 Black Shadow 网络攻击

12 月 3 日，黑客组织 Black Shadow 对保险公司 Shirbit 进行网络攻击，该组织在其电报频道上发布消息称，Shirbit 需向其比特币钱包发送 50 个 BTC，否则将泄漏并出售 Shirbit 的客户和员工的私人信息。

▶富士康遭到勒索软件 Doppel Paymer 攻击

富士康 CTBG MX 生产设施遭到勒索软件 Doppel Paymer 的攻击。在勒索信中，黑客索要了 1804.0955 个 BTC 作为赎金，并声称已加密了约 1200 台服务器。

3.4.2 安全建议

- 应避免使用弱口令密码，同一个密码不能重复使用。
- 日常工作中应加强安全防护，不要轻信或下载来源不明的链接或文件，谨慎打开来历不明的邮件或网址。
- 联合全球力量，严厉打击勒索软件/挖矿木马，推动行业安全监管进程建设。

3.5 暗网方面典型安全事件

2020 年暗网方面依然是网络犯罪活动频发的不法之地，暗网中充斥的军火、毒品、色情、信息贩卖、人口走私等非法活动在无形中威胁着国际社会的稳定与安全；通常，犯罪分子为逃避有关部门的监管和追踪，基于虚拟资产的匿名特性，多会选择以比特币、莱特币等作为交易媒介。

3.5.1 安全事件概览

▶Email.it 数据被挂暗网

4 月 9 日，电子邮件服务提供商 Email.it 遭黑客入侵，60 万用户数据被挂暗网。

▶Facebook 账户信息在暗网出售

4 月 23 日，2.67 亿个 Facebook 账户信息在暗网以 600 美元的售价出售，账户信息包括姓名、邮箱地址、电话、社会身份、性别等。

▶慧影医疗公司数据在暗网出售

4 月 29 日，一名黑客将慧影医疗公司的新冠肺炎检测技术和数据在暗网上以 4 个 BTC 的价格进行出售。

▶俄罗斯车主数据暴露在暗网上

匿名黑客获取了超过 1.29 亿俄罗斯车主的数据，并将其暴露在暗网上以获取比特币。泄露的信息包括数百万俄罗斯汽车司机的全名、地址、护照号码和其他数据。

▶安徽一男子于暗网出售公民身份信息

安徽一男子利用比特币于暗网出售公民身份信息，被判处侵犯公民个人信息罪，获刑三年，并处罚金三万元。其在暗网上出售公民手持身份证照片等个人信息，

累计数量达 20 万余条。

▶黑客组织 REvil 在暗网上发起拍卖信息

黑客组织 REvil 已在暗网上发起了其从 Fraser Wheeler&Courtney 和 Vierra Magen Marcus 两家美国律师事务盗取的敏感数据的拍卖信息。拍卖的信息包括客户信息、公司内部文件、电子信函、专利协议、商业计划和项目，以及尚未申请专利的新技术。

▶加密毒品帝国在暗网上非法交易

6 月 8 日，英国莱斯特刑事法院下令从一名英国人手中没收 180 多万英镑（约合 229 万美元），此人在自家阁楼上经营着一个价值数十亿英镑的加密毒品帝国，并在暗网上利用比特币进行非法交易。

▶Aleksei Burkov 被指控经营 Cardplanet 暗网

6 月 26 日，俄罗斯黑客 Aleksei Burkov 被美国法院判处 9 年监禁。Aleksei Burkov 被指控经营一家名为 Cardplanet 的暗网，该网站售有多国公民的信用卡信息。

▶暗网毒贩被指控试图炸弹袭击竞争对手

7 月 13 日，暗网毒贩 William Burgamy 和内布拉斯加药剂师 Hyrum Wilson 被指控试图炸弹袭击竞争对手，两人已对美国联邦指控认罪。

▶两名意大利青年被捕

两名意大利 17 岁青年因于暗网支付比特币观看儿童性虐待、酷刑和谋杀相关直播视频被捕。

▶28 万个 Instacart 账户在暗网出售

据称，近 28 万个 Instacart 账户在暗网出售。Instacart 通过应用程序为客户提供杂货配送服务。被非法出售数据包含客户名、信用卡号和数字、订单历史记录等。

▶114 万俄罗斯人的护照数据在暗网出售

114 万俄罗斯人的护照数据在暗网的地下商店出售。据悉，此前在宪法改革公投中，这些俄罗斯公民通过区块链平台投票，但他们的数据在互联网上遭到了泄露。

▶暗网市场 Empire Market 骗取资金后关闭运营

8 月 30 日，著名暗网市场 Empire Market 已关闭运营，退出时该网站共骗取了 130 万用户的约 2638 个 BTC，价值近 3000 万美元。

3.5.2 安全建议

- 作为用户，应正确使用互联网，规范网络道德。
- 作为网络安全公司，需加强暗网治理有关技术，协助相关部门参与到打击暗网和黑灰产业链的专项行动中。

- 加强国际合作，提升全球治理和管理暗网的整体实力。

3.6 其他方面典型安全事件

其他方面，诸如信息泄露、隐私保护、私钥窃取、非法洗钱、恐怖融资等各领域所发生的安全事件在 2020 年依然不容忽视。同时，随着区块链技术与多个产业领域实现大规模融合及应用，未来各类型的安全事件将呈高发态势，值得重点关注，需及时搭建起具备针对性的安全防御机制。

3.6.1 安全事件概览

▶SIM 卡被黑导致被盗

2 月 22 日，Bitcoin Builder 创始人、Mt.Gox 第二大债权人 Josh Jones 的 SIM 卡被黑，导致价值 45000000 美元的虚拟资产被盗。

▶Trident Crypto Fund 被攻击致数据泄露

3 月 5 日，加密基金 Trident Crypto Fund 遭黑客攻击，26.6 万名用户数据被泄露。

▶稳定币网络 PegNet 遭到 51%攻击

稳定币网络 PegNet 遭到了 51%攻击，四名攻击者合计占有了高达 70%的哈希率，在提交了虚假的价格数据后，将自己钱包中的余额由 11 美元变更为 670 万

美元。

▶Zcash 元数据可能存在隐私性漏洞

Zcash 元数据可能存在隐私性漏洞，使得攻击者可能利用该协议而使用其中某些程序。该漏洞暂未对区块链构成威胁。

▶黑客疑似侵入俄罗斯外交部官方 Twitter

7 月 2 日，黑客疑似侵入了俄罗斯外交部的官方 Twitter 账户。黑客通过该账户发帖出售某失窃支付数据库，要价 66 个 BTC。该数据库据称包含 2020 年 6 月俄罗斯联邦公共服务门户网站的游客支付详情。

▶Ravencoin（RVN）区块链存在漏洞

7 月 3 日，CryptoScope 团队发现 Ravencoin（RVN）区块链存在漏洞，经过 RVN 首席开发团队确认后已发布了紧急更新。据悉，该漏洞可生成额外的 RVN，但是不会影响或控制已经存在的 RVN 资产。

▶黑客团伙 Keeper 建立互连网络

一个名为“Keeper”的黑客团伙建立了一个互连网络，从 570 多个电子商务网站窃取信用卡数据。自 2017 年以来，该组织通过在暗网出售信用卡信息而获得了超过 700 万美元的虚拟资产。

▶虚拟资产挖矿组织 BitClub Network 电信欺诈

7 月 10 日，根据美国新泽西州联邦检察局发布的公告显示，程序员 Silviu Catalin Balaci 承认参与建立了虚拟资产挖矿组织 BitClub Network，并进行电信欺诈，出售未经注册的证券。

▶多个推特账号被黑

7 月 16 日，多位名人政要以及一些公司的推特账号被黑客袭击，这些推特账户都发布了相关的虚拟资产钓鱼骗局信息。不过，这些钓鱼信息在发布几分钟后就被删除。

▶CWT 被劫持并同意支付比特币

8 月 1 日，美国第五大旅游公司 CWT 同意向劫持其计算机系统的黑客支付价值 450 万美元的比特币。

▶黑客从 CryptoTrader.Tax 窃取用户数据

8 月 24 日，黑客从 CryptoTrader.Tax 中窃取了 1000 多个用户的数据。CryptoTrader.Tax 是一款用来计算和归档虚拟资产交易税的在线服务。

▶硬件钱包制造商 Ledger 遭网络钓鱼攻击

硬件钱包制造商 Ledger 遭受了网络钓鱼攻击。一些用户收到了带有钓鱼软件的电子邮件，导致资金损失。据报道，此次黑客攻击可能与该公司在 2020 年 7 月的用户数据泄露事件有关。

▶Axion Network 合约出现铸造漏洞

11 月 2 日，仅上线后几小时，Axion Network 合约中出现了铸造漏洞，已有 50 万美元被盗。他们甚至建议用户避免立即购买 AXN 代币，并远离网络的仪表板。

▶Grin 网站遭受 51%攻击

11 月 9 日，Grin 网站遭受 51%攻击。一个未知实体控制了超过 57%的网络算力。根据 Grin 网站的说法，该团队建议人们等待“关于支付最终性（Finality）的额外确认”。

▶Aeternity（AE）遭到黑客 51%攻击

12 月 9 日，Aeternity（AE）遭到了黑客 51%攻击。据 Aeternity 社区核心成员披露，此次 51%攻击造成的损失超过 3900 个 AE 代币，官方团队正在解决问题，此次受损的主要是交易所和矿池。

▶Voyager Digital 遭遇网络攻击

12 月 29 日，虚拟资产经纪商 Voyager Digital 遭遇网络攻击，交易系统受损，被迫下线，并告知客户其域名系统（DNS）服务器遭到破坏，但此后已经恢复。

3.6.2 安全建议

- 行业各方从业者在关注热点领域安全事件的同时，也需兼顾其他方面的安全

风险。

- 在夯实传统安全、网络安全的基础上，积极应对区块链生态各领域的安全挑战。
- 加强对区块链安全技术的投入与研究，建立覆盖区块链生态全生命周期的安全解决方案。

第四章 安全风险分析及应对策略

不难看出，区块链基于其天然的“基因特性”在价值安全转移、数据安全存储、信息安全防护等方面具备显著的优势。作为多种技术整合的一种全新的数据记录、存储和表达的方式，区块链技术能够在不可信的竞争环境中低成本建立信任机制，同时又具备一系列加密算法和数字签名等方式以确保交易安全，并形成一种随时间戳排序的链式结构来保证数据不被篡改。可尽管如此，区块链既是坚韧的安全捍卫者，同时也是脆弱的被攻击对象。通过 2020 年区块链生态典型安全事件的复盘，可以发现，当下区块链生态依然面临着巨大的安全威胁。

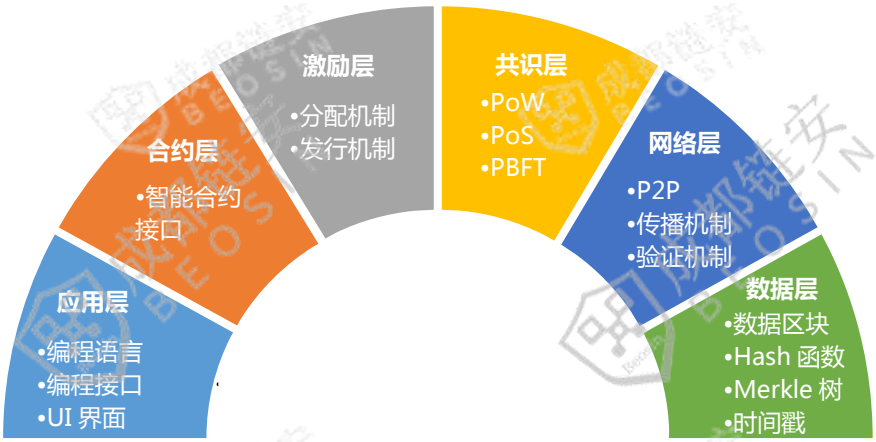


图 8：区块链底层架构

4.1 网络安全

4.1.1 攻击方式

4.1.1.1 DDoS 攻击

传统的 DDoS 攻击分为两步：第一步利用病毒、木马、缓冲区溢出等攻击手段入侵大量主机，形成僵尸网络；第二步通过僵尸网络发起 DDoS 攻击。不同于传统的中心化系统，针对区块链系统的 DDoS 攻击可以分为主动攻击和被动攻击。

4.1.1.2 日食攻击

日食攻击是通过其他节点实施的网络层面攻击，这种攻击目的是阻止最新的区块链信息进入到被攻击的节点，从而隔离节点。其攻击手段为：囤积和占用受害者的点对点连接时隙，将该节点保留在一个隔离的网络中，达到隔离节点的目的。

4.1.1.3 女巫攻击

在 P2P 网络中，特别是公链网络，由于节点随时加入退出等原因，为了维持网络稳定，同一份数据通常需要备份到多个分布式节点上，被称为数据冗余机制。女巫攻击是攻击数据冗余机制的一种有效手段。

4.1.2 应对策略

4.1.2.1 加强 DDoS 防御能力

应对 DDoS 攻击是一个系统工程，想仅仅依靠某种系统或产品防住 DDoS 是不现实的。通过适当的措施或办法，诸如安装专业抗 DDoS 防火墙、部署 CDN 等方式，在一定程度上加大了攻击者的攻击成本，可做到有效的安全防御。

4.1.2.2 加强节点准入机制

区块链网络用户应能通过标识建立唯一的、可验证的数字身份；合理设置对等网络节点的连接数目、连接时长、地址列表大小等。提供区块链服务的平台应具备基本的网络边界防护、网络入侵检测与病毒防御机制。

4.1.2.3 加强转发验证机制

区块链网络应具备针对恶意节点检测和防御机制，能够及时检测出网络中的恶意节点，并进行针对性处理。针对恶意交易/区块，各节点应有合理的交易/区块转发验证机制，对不良的交易/区块不做转发。

4.2 密码安全

4.2.1 攻击方式

4.2.1.1 穷举攻击

此类攻击主要作用于散列函数中，且几乎所有散列函数或多或少都受此类攻击方式影响，而且其影响程度与函数本身无关，而是与生成的 hash 长度有关，主要是一个概率论的问题。

4.2.1.2 碰撞攻击

此类攻击同样主要作用于散列函数中，其攻击原理是通过寻找算法的弱点，瓦解其强抗碰撞性这一特性，使得散列函数原本要在相当长一段时间才能寻找到两个值不同 hash 相同的值的特性被弱化，攻击者能在较短的时间寻找到值不同但 hash 相同的两个值。

4.2.1.3 量子计算攻击

量子计算对于密码算法存在潜在威胁。目前量子计算技术正在飞速发展，该技术走向成熟将对当今密码算法造成极大影响。因此，在量子计算技术完全成熟之前，必须有能够对抗量子计算的新型密码体制出现，否则一切运用现有密码体制的事物都将失去原有的安全性。在未来，尤其是与密码体制紧密相关的区块链技术，更需要具备抗量子计算的密码体制来保证其安全性。

4.2.2 应对策略

4.2.2.1 使用多种方式存储保障私钥安全

私钥管理的安全是区块链密码体制安全的前提，目前主流的方式是通过软硬件钱包的方式进行管理，或者由用户自行保管。一旦私钥丢失，用户不仅无法对数据进行任何操作，也无法使用或找回其所拥有的虚拟资产。因此，加强私钥安全管理是最为直接和高效的应对策略，目前来说针对私钥安全的存储方式一般分为硬件存储、软件存储和分割存储三种。

4.2.2.2 使用 PKI 数字证书管理及 CA 认证

PKI（Public Key Infrastructure）是一种遵循标准的利用公钥加密技术为电子商务的开展提供一套安全基础平台的技术和规范。通过第三方的可信任机构——认证中心 CA（Certificate Authority），把用户的公钥和用户的其他标识信息捆绑在一起，以在网络中验证用户的身份。基于 PKI 结构结合数字证书，通过加密需要传输的数字信息，保证数据与信息的真实性、完整性，是当下较为通用的应对策略。

4.3 共识机制安全

4.3.1 攻击方式

4.3.1.1 双花攻击

简言之，双花攻击指的是同一资产被花费了多次。在区块链网络中，每个用户的每一次交易都可以对应一个网络请求。而区块链整个系统会进行对此请求的验证，其中包括检查其资产的有效性、是否已经使用已花费的资产来进行交易。再经过全网节点的检验后，广播这个成功验证的账本。由于区块链系统分布式的特性，在交易过程中存在的延时性不可避免，这即导致了“双花（Double Spending）”此类攻击方式得以实现。

4.3.1.2 51%攻击

在 PoW 共识算法中，系统同时允许存在多条分叉链，在 PoW 的设计理念中有一个最长有效原理：“无论在什么时候，最长的链会被认为是拥有最多工作的主链”。51%攻击是指在攻击者拥有超过整个网络一半算力的情况下，就有能力推翻原有确认过的交易，重新计算已经确认过的区块，使区块产生分叉，完成双花并获取利益。

4.3.1.3 重放攻击

重放攻击又称重播攻击、回放攻击，是指攻击者发送一个目的主机已接收过的数据包，来达到欺骗系统的目的。在区块链技术中，重放攻击是指“一条链上的交易在另一条链上也往往是合法的”。这种攻击一旦发生，就会产生类似于双花攻

击的效果；同一笔资产转给了同一个人两次，就会导致在不需要付款人参与的情况下多一次支付。

4.3.2 应对策略

4.3.2.1 合理界定共识算法的安全范围

共识算法的安全更多是在确保安全和攻破安全防御所付出的代价之间找到一个平衡点，判断共识算法是否安全应立足于具体的应用场景以及该链所处的状态。例如，采用 PoW 共识算法的比特币系统，其虽然有遭受 51%攻击的可能，但要构建一次超过全网一半算力的攻击需要付出极大的代价，而该代价远远大于收益。因此，可以认为，采用 PoW 共识算法的比特币系统是安全的。

4.3.2.2 根据业务场景选择多种或可切换的共识算法

不同的共识算法有不同的侧重和工作效率，评价一种共识算法的整体性能一般采用四个维度：安全性、扩展性、性能效率、资源消耗。因此，面对不同的应用场景须选用不同的共识算法。为了保证安全性，也可以在全网采用多种共识算法，通过多级共识来确认交易。

4.4 智能合约安全

4.4.1 攻击方式

4.4.1.1 面向智能合约安全漏洞

由于智能合约本质上是部署和运行在区块链上的程序，在没有标准的合约模板或编写规范的情况下，很难要求开发人员写出最佳实践的代码，一些逻辑不严谨的代码会造成智能合约设计和实现上出现很多意想不到的安全漏洞，而往往这些漏洞会成为黑客发起攻击的“后门”，使区块链生态蒙受巨大经济损失。

经成都链安（Beosin）安全团队梳理和总结，2020 年“智能合约安全”的典型安全事件较为集中在各类 DeFi 项目中爆发，其中主要涉及到的安全问题包括：闪电贷攻击、业务逻辑缺陷、外部合约交互缺陷、项目方后门等等。

4.4.1.2 面向虚拟机安全漏洞

目前，大多数智能合约语言属于虚拟机语言，由其实现的智能合约需要运行在特定的语言虚拟机，例如以太坊上的由 Solidity 语言编写的智能合约需要运行在 EVM 上。虚拟机本身的安全性一方面可以保证智能合约运行结果的正确性，另一方面也可以防止运行其上的智能合约免受其他恶意合约的攻击。考虑到一个区块链系统的大量节点往往部署同样版本或类似实现的虚拟机上，单个虚拟机的安全漏洞很可能影响到整个系统。

4.4.2 应对策略

4.4.2.1 重视智能合约的安全审计

智能合约往往被用来管理大量的用户资产和有价凭证，然而大多数区块链项目为了增加可信度和透明性，对其项目代码进行开源管理，这样使得项目更易受到攻击。智能合约开发者在实现业务功能之外，额外学习大量的安全编码规范和已有漏洞问题等成本过高，因此接受来自第三方安全公司针对智能合约开展的安全审计工作，是有效规避智能合约安全漏洞潜在风险的有效措施。

4.4.2.2 采用形式化验证技术

形式化验证的含义是根据某个或某些形式化规范或属性，使用数学的方法证明其正确性或非正确性。形式化验证是一个系统性的过程，将使用数学推理、定理证明、模型检测来验证设计意图（用户功能需求）在实现（智能合约）中是否得以正确贯彻。将形式化验证这一技术运用于智能合约的安全审计，是一种非常可靠且准确的智能合约安全审计策略。

4.4.2.3 加强虚拟机安全漏洞防范

在设计和实现智能合约语言虚拟机时，加强虚拟机相关安全漏洞的防范，主要可以从四个方面进行考虑：保证目标语言和源语言的语义的一致性；结合区块链的

机制设计防范拒绝服务攻击；在虚拟机设计和开发中着重关注虚拟机逃逸漏洞；对多个智能合约运行环境进行强隔离。

4.5 应用生态安全

4.5.1 攻击方式

4.5.1.1 面向公有链平台

公有链是指任何人、任何节点都能够参与，无任何访问限制的区块链，如比特币、以太坊、EOS 等。由于公有链的开源性质，导致公有链安全性较低，受攻击面较大，包括在节点通信、区块处理、交易逻辑、数据存储及共识机制等各个层面，容易受到威胁。

4.5.1.2 面向联盟链平台

联盟链是由符合某种条件的成员组成联盟来管理的区块链，只有经过许可的可信节点才能参与该联盟链的记账，其它用户仅有部分权限，如 IBM Hyperledger Fabric 2.0、蚂蚁链开放联盟链、腾讯区块链等。由于联盟链有接入权限管控的限制，安全性相较于公有链有些许提升，但依然存在某些和公有链类似的安全风险点，如链上数据异常、节点异常、加密通信的安全性，以及联盟链特有的认证授权策略及账户授权机制的风险等。

4.5.1.3 面向数字钱包

区块链的数字钱包指的是存储区块链资产的地址和私钥文件。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或多或少存在一些安全隐患容易被忽视，主要的安全问题体现在数字钱包 APP 重打包、交易密码未检测弱口令、核心代码未加固、未检测到系统运行环境、操作存在截屏及录屏记录等方面。

4.5.1.4 面向 DAPP 项目

无论是在“Web+智能合约”或是“移动 APP+智能合约”的去中心化应用系统 DAPP 项目中，均存在着各种各样的安全威胁，其中 Web 端安全风险包括错误的安全配置、文件泄露、缓冲区溢出等方面；移动 APP 端包括 APP 组件配置错误、APP 加解密算法机制风险、钓鱼劫持风险等方面。

4.5.1.5 面向虚拟资产犯罪活动

随着虚拟资产体量逐步增大，加之虚拟资产犯罪活动门槛较低，利用虚拟资产进行非法洗钱、诈骗、非法交易、恐怖融资、病毒勒索等犯罪行为愈演愈烈。与此同时，虚拟资产犯罪活动所造成的影响极其恶劣，不仅会在全球范围内引发惨重损失，还将严重破坏和扰乱世界经济秩序和金融市场的稳定运转。

4.5.2 应对策略

4.5.2.1 重视链平台的安全审计

链平台是区块链的底层系统，负责支撑各类区块链应用的运行环境，是区块链生态中的核心与基石。在经历了新的区块链分化之后，公有链和联盟链两种应用方向正在快速发展。在链平台项目进行上线运行之前，与第三方安全公司进行针对链平台的代码安全测试，可有效保障链平台节点通信、存储、共识和权限管理等各个层面的安全性。

4.5.2.2 加强数字钱包及 DAPP 项目的安全防护

基于底层链平台，各类诸如数字钱包及 DAPP 项目等区块链应用也应运而生。作为与海量资产息息相关的关键对象，各类区块链应用的安全更需要行业各方从业者引起重视。通过全面模拟黑客攻击场景，对数字钱包和 DAPP 项目等区块链应用进行全封闭式（黑盒）或者半开放式（灰盒）测试，可提高区块链应用的整体安全防护水平。

4.5.2.3 建立整体虚拟资产风控体系和监管方案

针对各类虚拟资产犯罪活动，建立整体虚拟资产风控体系和监管方案是极为高效

的应对策略。通过对链上海量交易信息进行深入分析，利用丰富的实体地址库和机器学习异常行为建模技术，打造 KYT（Know Your Transactions）及持续性风险评估的能力，并进一步开展追踪溯源、调查取证、实时自动告警、风险态势呈现等相关工作的推进。

4.5.2.4 构建各方从业者广泛参与的安全生态

伴随着区块链技术的赋能场景已广泛应用于各个领域的实体经济和数字经济的发展当中，区块链应用生态的发展形势欣欣向荣。在积极探索产业区块链的解决方案的同时，区块链行业与相关垂直行业亦需通力合作，共同推动区块链技术在安全生态的有序发展。

第五章 区块链生态安全发展的对策及建议

在区块链技术与实体经济、数字经济加速融合，“区块链+产业”发展愈加成熟和规范的同时，也需要尤其注意到进入 2020 年，区块链生态各领域安全事件频频发生，区块链生态所造成的经济损失愈演愈烈。

2020 年 12 月，习近平总书记在中央政治局第二十六次集体学习时强调要“统筹发展和安全，筑牢国家安全屏障”，这一重要指示精神贯彻到区块链行业同样适用。如何在发展中保安全、在安全中促发展，兼顾区块链生态当下最为急迫的两项任务，值得从业者思考和实践。为此，成都链安（Beosin）安全团队提出如下对策及建议。

5.1 加大区块链安全技术的研究和攻关

面对现有的区块链生态安全现状，尽管 2020 年区块链技术正在加速演进和趋于完善，但立足于长远的发展目光来看，层出不穷的区块链安全事件的高发态势对诸如共识机制、隐私保护、非对称加密、分布式存储、点对点传输等区块链安全技术提出考验。

由此，加大区块链安全技术研究和难点攻关投入，抢占技术高地，针对区块链技术性能瓶颈与系统安全性的平衡、隐私保护以及数据信息的安全防护和追踪溯源

等方面，应积极开展研发和创新工作，以满足区块链生态各领域的安全需求。同时，积极关注区块链行业的前沿方向，将安全技术转为安全生产力，并持续打造出更具价值和前瞻性的安全解决方案。

5.2 推动区块链安全标准和规范建设

伴随着区块链行业政策环境的态势利好且趋于积极稳定，日益完善的区块链安全标准和规范建设无疑将加速外界对区块链整个行业的正确认知，以更快更好地促进“区块链+产业”的高速发展。蛮荒的行业乱象正在成为历史，但未来依然需要大力推动区块链安全标准和规范建设。

根据公开数据统计，截至 2020 年 12 月，由国家标准化管理委员会牵头的《信息技术区块链和分布式账本技术参考架构》、《信息技术区块链和分布式记账技术智能合约实施规范》、《信息技术区块链和分布式记账技术存证应用指南》，以及由全国信息安全标准化技术委员会(SAC/TC260)提出的《信息安全技术 区块链信息服务安全规范》和《区块链服务安全技术要求》的国家标准正在起草中。另外，已发布 3 项行业标准、5 项地方标准、34 项团体标准。

级别	牵头单位	标准名称	标准号
行业标准	中国人民银行	金融分布式账本技术安全规范	JR/T 0184-2020
	中国人民银行	区块链技术金融应用评估规则	JR/T 0193-2020
	工业和信息化部	区块链技术架构安全要求	YD/T 3747-2020
地方标准	贵州省	基于区块链的精准扶贫实施指南	DB52/T 1469-2019
	贵州省	基于区块链的数据资产交易实施指南	DB52/T 1468-2019
	贵州省	区块链系统测评和选型规范	DB52/T 1467-2019

	贵州省	区块链应用指南	DB52/T 1466-2019
	山东省	基于区块链技术的疫情防控信息服务平台建设指南	DB37/T 3909-2020

图 9：2020 年我国已发布的行业标准及地方标准

具体而言，区块链安全标准和规范建设的推进工作，有利于支撑各类区块链应用的底层平台的开发、运行、维护和管理，规范和引导区块链相关技术和相关软件的开发。同时，加快制定具备我国特色的区块链相关安全标准和规范，搭建起我国“自主创新、自主可控”的区块链安全技术和保障体系，以此保障区块链生态健康发展和持续创新。

5.3 促成区块链监管和合规体系搭建

在监管和合规方面，区块链行业的相关体系的完善和搭建工作仍然任重道远，亟需相关部门的介入和行业从业者的有效推动。区块链行业当前发展态势整体向好，未来发展潜力也前景可期，但也要清醒地认识到，乱象丛生的安全现状与多方位的安全挑战，迫切要求加强区块链的安全监管和合规。

在促成区块链监管和合规体系的搭建方面，需推动监管模式的创新，明确区块链服务主体责任，积极探索在区块链系统中增加的监管节点的可行性，推动建设跨部门监管的长效机制，开展区块链安全监管、安全评测、安全标准等相关工作，为行业发展提供安全、有序的内部环境。

参考文献

1. 《成都链安区块链生态介绍》，成都链安科技有限公司。
2. 《盘点 | 成都链安安全月报（2020 年 1 月-12 月）》，成都链安科技有限公司。
3. 《2019 年区块链安全事件总结，全球损失超 60 亿美元》，成都链安科技有限公司。
4. 《Beosin（成都链安）年报 | 2018 年区块链安全事件及损失盘点》，成都链安科技有限公司。
5. 《区块链智能合约安全漏洞解析》，杨霞，郭文生，高子扬，岳亮亮。
6. 《区块链安全探索与实践报告》，杨霞。
7. 《区块链生态安全挑战及解决方案研究》，杨霞。
8. 《区块链白皮书（2020 年）》，中国信息通信研究。
9. 《区块链安全白皮书（1.0 版）》，可信区块链推进计划。
10. 《2020 年全球区块链发展趋势报告》，FISCO 金链盟，金融科技·微洞察。
11. 《2020 开放金融发展报告》，Odaily 星球日报。
12. 《区块链技术安全威胁分析》，孙国梓，王纪涛，谷宇。

免责声明

《2020 年区块链生态安全态势年度报告》版权为成都链安科技有限公司独家所有，包括本报告的所有数据、表格及文字内容。其中，部分图表在标注有数据来源的情况下，版权归属原公司。

未经成都链安科技有限公司的审核、确认及书面授权，本报告不得以任何方式提供给其他单位或个人。如有侵权行为的个人、法人或其它组织，必须立即停止侵权并对其因侵权造成的一切后果承担全部责任和相应赔偿，否则我们将依据相关法律、法规追究其经济和法律责任。

本报告基于我们对区块链行业的理解，以及【链必安-区块链安全态势感知平台（Beosin-Eagle Eye）】的数据支持。但由于区块链技术“匿名性”这一天然特性，我们在此并不能保证所有数据的绝对准确，也不能对其中的错误、疏漏、或使用本报告引起的损失承担责任。

由于时间紧迫，编者水平与资料有限，本报告中若有疏漏和不足之处，欢迎大家批评指正。

数据支持：成都链安（Beosin）安全团队

编写人员：张成锐

关于我们

成都链安科技有限公司，全球领先的区块链安全公司，致力于区块链安全生态建设，总部位于四川成都。团队核心成员是由从事信息安全长达 20 多年的海内外知名高校教授、博士后、博士以及曾任职于阿里、华为、360 等知名企业的网络安全精英组成。

公司已获前海母基金、联想创投、复星高科、成创投、分布式资本等知名机构的多轮投资。作为工信部“网络安全技术应用试点示范项目”、中国信通院区块链安全检测的主要技术合作单位、CNVD 国家区块链安全漏洞平台的主要技术支持单位、国家互联网应急中心的“区块链安全技术检测中心”的主要技术合作单位、成都区块链安全工程技术研究中心的依托单位，四川省区块链行业协会“蜀信链”安全检测和准入测试的支撑单位、成都高新区区块链公共技术平台；并作为中国信通院可信区块链联盟理事单位和安全组副组长、全国信息安全标准化技术委员会成员单位、北京金融科技产业联盟会员单位、四川省区块链协会理事单位、四川省互联网行业联合会副会长单位，公司参与了多项国家级区块链安全标准和白皮书的撰写。

以网络安全、形式化验证、人工智能和大数据分析四大技术为核心，打造了面向区块链全生态安全的自主可控的【链必安（Beosin）一站式区块链安全服务平台】，包含【六大核心安全产品】和【八大明星安全服务】，为区块链企业提供

安全审计、虚拟资产追溯与 AML 反洗钱、安全防护、威胁情报、安全咨询和应急等全方位的安全服务与支持，实现区块链系统“研发→运行→监管”全生命周期的安全解决方案。

以用户需求为根本，致力于搭建起我国“自主创新、自主可控”的区块链安全技术和保障体系，申请软件发明专利和著作权近 20 项。公司已与工信部、中国信通院、网信办、公安等监管机构，以及包括蚂蚁链、腾讯区块链、长虹、泰豪、微众银行、万向区块链、布比等国内外 100 多家区块链头部企业建立了深度合作关系；并为全球 1000 多份智能合约、50 多个区块链平台和落地应用系统、近 100 家数字金融企业提供安全审计与防御部署服务。

公司荣获 2020 金熊猫全球区块链创新创业大赛一等奖、2018 全国首届中小微企业“SaaS”应用创新创业大赛冠军、2020 首届人民网内容科技创新创业大赛全国总决赛“创业人气奖”、2020 成都市新经济“双百工程”重点培育企业、2018&2019 工信部赛迪研究院“中国区块链企业百强榜”、2019 中国区块链安全领军企业、2019 区块链安全服务机构、2019 区块链技术突破奖、2019&2020 中国区块链技术创新典型企业、2019 最佳区块链数据安全团队、2019 产业区块链安全卫士、2018 最专业安全服务机构等诸多荣誉。

成都链安以“让区块链生态更安全”为使命，以“成为全球第一的区块链安全公司”为愿景，不断打造区块链安全监管技术和安全保障体系，为区块链生态的安全发展保驾护航。

电话：028-83262585

邮箱：market@lianantech.com

网址：https://www.lianantech.com

公众号

客服