2022

区块链技术与金融应用安全白皮书

/ 易 / 于 / 链 / 接 / 共 / 赢 / 未 / 来 /

/ 易 / 于 / 链 / 接 · 共 / 赢 / 未 / 来 /

关注浙商银行微讯公众号

浙商银行 CZBANK

浙江大学 ZHEJIANG UNIVERSITY

编委会

主　　编（按姓氏笔画排序）
任　奎　杨国正

编制单位　浙商银行股份有限公司
浙江大学

编写成员（按姓氏笔画排序）
刘　健　张文翰　张秉晟　陈嘉俊　黄　蓉　臧　铖

设　　计　汪　忆

版权声明

目 录

前言

近年来，我国数字经济发展迅速、成效显著，以区块链为代表的新兴数字技术日益融入经济社会发展各领域全过程，实现了数字技术与实体经济的深度融合，推动了数字经济的高质量发展。

区块链技术作为“新基建”基础设施之一，已在金融经济、社会民生、政务治理、商业贸易等重点领域进行了广泛应用。这些应用领域对网络安全、风险管理的高要求、高标准使得区块链技术的安全性与区块链应用的隐私性成为了各方关注的焦点。尽管区块链技术本身具有去中心化、分布式存储、防篡改、可追溯等特性使其安全性远高于传统网络体系，但区块链技术在应用过程中仍会存在一些安全风险。

本白皮书聚焦于分析区块链技术体系安全问题以及区块链在金融重点领域应用中的安全问题，并针对各个安全问题提出了风险应对框架，使读者对区块链技术与应用潜在的安全问题及其应对方式有清晰的认知。最后，本白皮书对我国区块链安全的发展进行了展望，期望能够从加强自主可控、深化标准建设、打造基础设施、强化技术融合等方面进一步提升区块链技术与应用的安全性，推动我国区块链产业安全、健康发展。

1 chapter one 区块链技术与应用

一 国内政策框架

- “十三五”以来，新一代信息技术的高速发展推动了数字经济与实体经济的深度融合，为我国全面开启数字经济新时代奠定了坚实基础；“十四五”规划更是进一步明确提出要加快数字化发展、建设数字中国。建设数字经济、以数字化转型整体驱动生产方式、生活方式和治理方式变革已成为了我国国家战略。

- 随着经济社会全面数字化转型的推进，区块链技术被逐步应用于金融经济、政务治理、社会民生等各方各面，区块链的应用场景也越来越丰富。区块链不可篡改、可追溯、多中心化等特点使得区块链成为了新一代的信任传递工具。但是区块链技术发展至今，其技术本身的内部、外部仍存在一些安全风险。因此，在应用区块链技术的同时，大量机构与高校针对区块链的技术与应用安全展开了大量探索，各监管部门从顶层设计出发也出台了一系列与区块链网络安全相关的政策、标准。部分重要政策汇总如表 1-1。

表 1-1 区块链安全相关重要政策汇总

发布时间	发布单位	政策或标准	主要内容
2016 年 11 月 7 日	全国人大	《中华人民共和国网络安全法》	《网络安全法》是网络安全领域的“根本大法”，对网络安全支持与促进、网络运行安全、网络信息安全、监测预警与应急处置等做了规定，确立了网络安全的基本法律遵循。
2019 年 10 月 26 日	全国人大	《中华人民共和国密码法》	《密码法》的推出是为了规范密码应用和管理，促进密码事业发展，保障网络与信息安全，维护国家安全和社会公共利益，保护公民、法人和其他组织的合法权益，而加密技术是区块链的关键技术，《密码法》对于区块链技术与应用安全规范发展具有重大意义。
2019 年 1 月 10 日	国家互联网信息办公室	《区块链信息服务管理规定》	《区块链信息服务管理规定》旨在明确区块链信息服务提供者的信息安全管理责任，规范和促进区块链技术及相关服务健康发展，规避区块链信息服务安全风险，为区块链信息服务的提供、使用、管理等提供有效的法律依据。
2020 年 8 月 31 日	工业和信息化部	《区块链技术架构安全要求》	《区块链技术架构安全要求》面向区块链平台，规定了区块链技术架构应满足的安全要求，包括共识机制安全、智能合约安全、账本安全等，为区块链系统的设计开发提供参考。
2020 年 2 月 5 日	中国人民银行	《金融分布式账本技术安全规范》	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。
征求意见稿，尚未正式发布	全国信息安全标准化技术委员会	《信息安全技术 区块链信息服务安全规范》	标准规定了区块链信息服务的安全要求，包括安全技术要求和安全保障要求，以及相应的测试评估方法。

二 区块链安全机制

- 众所周知，区块链具有天然的高安全性，其安全机制主要包括共识机制、加密算法、隐私保护、多级签名等。

1. 共识机制

区块链作为一种去中心化的分布式系统，需要通过节点之间的底层共识协议来保证其账本的数据一致性，因此共识机制是区块链技术的基础，是区块链核心价值的体现。一般来讲，我们将区块链分为许可链（联盟链、私有连）和非许可链（公有链），由于实际应用场景和系统架构不同，不同种类的链所使用的共识算法也不同。常见的共识机制包括：工作量证明 /POW（Proof of Work）、权益证明 /POS（Proof of Stake）、股份授权证明 /DPOS（Delegated Proof-of-Stake）、拜占庭容错（PBFT/RBFT）、类 BFT 共识协议、RAFT 共识协议等。

2. 加密算法

为了实现区块链系统整体的安全性和可靠性，区块链引入了包括哈希算法、数字签名、密钥协商、对称加密的综合加密机制。

- **杂凑算法**

哈希是一种散列函数，把任意长度的输入原文通过哈希算法，变换成固定长度的输出 (哈希值)，哈希值的空间通常远小于输入原文的空间，哈希函数具有不可逆性，根据哈希值无法反推输入原文的内容，保障原文的安全及隐私。在区块链平台中交易的信息摘要、合约地址、用户地址、账本指纹等都运用了哈希算法，实现了账本数据的快速验证与查找、隐私保护以及数字签名的高效性。

- **数字签名**

在区块链中，交易发起方对交易内容进行数字签名，发送给区块链节点，

区块链节点接受交易后验证发起方身份及签名是否对应，保证交易内容不篡改及可定向追溯。

- **基于非对称的密钥协商**

  密钥协商是指两个或多个实体在不可信环境下通过非对称加密算法交换双方公钥，安全地协商出一个只有双方可知的密钥的协议。在区块链节点组网的过程中，需要各区块链节点之间通过密钥协商构建一种支持快速加解密的对称密钥，用于后续节点之间的数据加密及信息交换。

- **基于对称的数据加密**

  通信双方基于非对称的密钥协商得到一个对称密钥后，再基于对称加密算法对数据进行快速加密，使得通信双方之间数据不能被窃听，保证区块链节点之间信道的通信安全。

目前国外主流开源区块链平台（包括以太坊、IBM HyperLedger Fabric 等）使用的是 RSA 和 ECC 等算法。为满足我国金融安全和监管要求，国内区块链平台应支持国家密码管理局所公布的 SM2、SM3 等国密算法。经过国密算法改造之后，原有 ECC 椭圆曲线算法、SHA2 算法可替代为 SM2 非对称算法、SM3 杂凑算法，交易数据的哈希通过 SM3 算法生成，签名验签涉及的公私钥对通过 SM2 算法实现，保持对底层透明，提升系统安全性和合规性。

3. 隐私保护

区块链公有链的匿名性很好地保护了用户的隐私，但在联盟链的模式下，交易数据在所有节点进行共识，数据被完整的保存在每个节点，虽然通过密码学机制进行了相应的数据加密，但随着量子计算的不断发展，数据被破解的概率也会随之上升。针对该种情况，可通过采用合约访问控制、分区共识、隐私交易三种机制提供隐私保护。

- **合约访问控制**

  在智能合约编码阶段定制合约方法的访问权限，通过合约设置用户公钥操作权限，在查询时验证查询方公钥，保证区块链数据持有方才具有查询权限，实现业务数据的隐私保护。

- **分区共识**

  通过设计分片机制实现区块链网络内部交易的分区共识，每个分片通过业务的交易共识、分发以及存储的逻辑级别隔离实现业务级别的隐私保护。

- **隐私交易**

  支持交易粒度的隐私保护，发送交易时指定该笔交易的相关方，该交易明细只在相关方存储，隐私交易的哈希在全网共识后存储，既保证了隐私数据的有效隔离，又可验证该隐私交易的真实性。

4. 多级签名

通过叠加客户在交易平台采用的 Ukey 或文件证书的数字签名、应用服务器采用的 CA 机构颁发的数字证书的数字签名、应用服务器采用的区块链平台颁发的公私钥的数字签名以及区块链节点间的非对称密钥数字签名，构建从交易指令到区块链记账的全过程数字签名证据链，形成端到端的验证体系，确保用户通过应用平台访问区块链系统过程中的可追溯性。

三 区块链应用概况

- 区块链作为新一代价值传递工具，在各行各业落地了大量应用，从早期的存证溯源场景，到现阶段全面拓展至金融、政务、医疗、司法存证、产品溯源等场景，区块链有效解决了信任问题，实现了价值的自由传递。

1. 区块链基础应用

- 区块链的上层场景应用大多以区块链底层技术平台为基础。早期区块链技术平台大多基于 Fabric、以太坊等国外开源平台进行改造。随着国产自主可控意识的觉醒，我国互联网企业等科技公司、银行等金融机构自主研发了一批优秀的区块链底层技术平台。部分典型区块链底层技术平台汇总如表 1-2。

表 1-2 典型区块链底层技术平台

机构名称	区块链底层技术平台介绍	是否国产自主可控
工商银行	2018 年 10 月，工商银行正式发布具有自主知识产权的企业级区块链技术平台“工银玺链”，以“自主研发 + 合作共建”的模式联合打造开放协同、安全稳定、智慧高效的“区块链 +”基础设施，促进“区块链 +”模式的融合创新发展。（来源：《中国金融家》采访：《工银科技李六旬：为智慧银行、数字中国提供技术支撑》）	是
浙商银行	2017 年 7 月，浙商银行推出了自主研发的、符合金融特性的区块链技术平台，并率先完成平台的国密适配与共识算法改造，以“科技 + 金融 + 行业 + 客户”的综合金融服务方案在产业链进行应用，有效推动产业链数字化转型和高质量发展。（来源：浙商银行官网）	是
微众银行	微众银行于 2016 年 5 月发起成立金链盟，推出安全可控的企业级金融联盟链底层平台 FISCO BCOS，并于 2017 年正式对外开源。FISCO BCOS 汇聚了数千企业及机构、上万开发者参与共建，已经发展成为最大最活跃的国产开源联盟链生态圈。（来源：金链盟官网）	是
杭州趣链科技有限公司	2016 年 10 月，趣链科技发布了国产自主可控的区块链底层技术平台 Hyperchain，可面向企业、政府机构和产业联盟的区块链技术需求，提供企业级的区块链网络解决方案。（来源：趣链科技官网）	是
国网区块链科技公司	国网链是国网区块链科技公司在国家电网公司的统一指导下建设的行业级能源区块链公共服务平台，面向国家电网公司直属单位、20 多家省公司以及上下游企业来共同提供服务，实现与政府、高校、科研院所等单位互联互通，构建“共建、共享、共赢”协作模式。（来源：电网头条微信公众号）	是

2. 区块链金融应用

- 金融是区块链应用场景中探索最多的领域，在供应链金融、贸易融资、跨境金融、信用证 / 福费廷、资金监管等细分金融场景都有具体的应用落地，以银行等金融机构为应用重点，互联网企业等科技公司参与共建。

（1）供应链金融领域的典型案例如表 1-3 所示：

表 1-3 区块链供应链金融典型应用案例

机构名称	落地平台名称	应用情况
浙商银行	浙商银行应收款链平台	浙商银行应收款链平台于 2017 年 8 月推出，为业内首创基于区块链的供应链金融平台。企业可将账面的应收账款转化为电子支付结算和融资工具，轻松盘活流动资产，加快资金周转，减少融资成本，帮助企业降本增效。（来源：浙商银行官网）
	仓单通	仓单通平台基于应收款链平台打造，于 2018 年推出，是浙商银行运用区块链技术开发的，集仓单签发、转让、质押、融资、交易、清算、提单等功能于一体的综合性在线业务平台。（来源：浙商银行官网）
	浙商银行 BaaS 平台	浙商银行 BaaS 平台于 2020 年 9 月推出，为区块链应用开发、快速落地到运维管理提供了一站式的区块链技术服务，面向生态合作伙伴提供快速接入、高效管理的区块链服务能力，提升各类场景落地效率。（来源：浙商银行官网）

平安银行	SAS 区块链平台	SAS 区块链平台由平安银行于 2017 年底推出，采用区块链技术实现精准溯源，与人行中登网直连，避免应收账款重复抵押，对接外部资金实现应收账款资产的快速变现、流转，能有效解决传统应收账款融资痛点，缓释业务风险。（来源：《平安银行：区块链加持下的 SAS 平台怎么玩？》）
建设银行	基于区块链的再保理业务平台	建设银行于 2019 年 12 月上线基于区块链的再保理业务平台，为提高保理业务操作效率、降低风险，构建再保理业务下多方参与的生态圈。（来源：《中国建设银行推出区块链再保理业务》）
中企云链	中企云链	中企云链平台是多家大型国企倾力打造的基于互联网的供应链金融服务平台，旨在充分发挥大型国企在产业链中的核心作用，全方位服务于产业链上每一个经济体，建立和谐、健康、良性的产业生态圈。（来源：中企云链官网）
山东高速	高金云信平台	高金云信平台是山东高速集团内部供应链金融平台，将集团内部沉淀的应收应付账款转换为区块链应收款，帮助集团及权属各单位开拓创新业务、增收增效、减少外部融资依赖，主动化解风险，全面降低总体融资成本。（来源：山东高速集团官网）

（2）贸易融资领域的典型案例如表 1-4 所示：

表 1-4 区块链贸易融资典型应用案例

机构名称	落地平台名称	应用情况
中国人民银行数字货币研究所	中国人民银行贸易金融区块链平台	中国人民银行贸易金融区块链平台于 2018 年 9 月 4 日正式上线，创建了基于区块链技术的开放、可信、安全、标准、合规、高效、公益、共享的贸易金融资产登记、托管、交易和流转平台。同时赋能中小企业，服务实体经济，降低企业融资成本，提高融资效率，积极探索基于区块链的创新性贸易金融产品形态、金融监管政策，以贸易融资推动深港合作和粤港澳大湾区发展，为推动数字经济的全球化发展奠定基础。（来源：“中国人民银行贸易金融区块链平台”百度百科）

（3）跨境金融领域的典型案例如表 1-5 所示：

表 1-5 区块链跨境金融典型应用案例

机构名称	落地平台名称	应用情况
国家外汇管理局	国家外汇管理局跨境金融区块链服务平台	跨境金融区块链服务平台由国家外汇管理局发起，于 2019 年 3 月 22 日开始试运行，针对出口应收账款融资、企业跨境信用信息授权查证和进口货到付款这三个场景展开服务，对跨境融资业务六成优化再造，提升跨境金融业务效率，已有 170 余家法人银行加入该平台。（来源：《中国银行业区块链应用与探索报告 2020》）
招商银行	区块链跨境创新支付平台	区块链跨境创新支付平台由招商银行于 2017 年推出，通过组建总行与境外子公司永隆银行间的联盟链，实现报文的实时同步与资金快速清结算，实现快捷便利的跨境支付，一笔直联支付的报文可在数秒内完成交互。（来源：《招商银行完成国内首单区块链跨境支付业务》）

（4）信用证 / 福费廷领域的典型案例如表 1-6 所示：

表 1-6 区块链信用证 / 福费廷典型应用案例

机构名称	落地平台名称	应用情况
中信银行	全功能区块链 福费廷交易平台	全功能区块链福费廷交易平台 (BCFT) 由中信银行主导，中国银行、民生银行、光大银行、平安银行等参与研发，于 2018 年 9 月 30 日上线，服务于福费廷业务预询价、资产发布后询价、资金报价等场景，解决了传统福费廷业务协议线下双边签订过于繁琐的痛点，已成为国内最大的福费廷交易平台之一。来源：（《中国银行业区块链应用与探索报告 2020》）

（5）资金监管领域的典型案例如如表 1-7 所示：

表 1-7 区块链资金监管典型应用案例

机构名称	落地平台名称	应用情况
工商银行	雄安工程 建设资金管理	于 2020 年推出，为雄安新区首个财政建设资金管理区块链信息系统，成功完成了建设者工资和供应商材料款的穿透式支付，有效避免资金截流、挪用、拖欠等问题，保障建设者的合法权益。（来源：中国雄安官网）

3. 区块链其他垂直领域应用

- 除金融业务之外，互联网企业等科技公司基于区块链技术在政务、医疗、司法存证、产品溯源等领域作了大量的应用。

（1）政务领域的典型案例如表 1-8 所示：

表 1-8 政务领域区块链典型应用案例

机构名称	落地平台名称	应用情况
成都高新区政府	成都高新区基于区块链的线上授权办事服务	2021 年 4 月底，成都高新区网络理政办依托微信统一政务服务平台“高新服务”，上线区块链授权办事应用，基于趣链科技区块链平台打造。（来源：趣链科技微信公众号）
徐州市文化广电和旅游局	徐州文广旅安全生产监管平台	徐州文广旅安全生产监管平台利用区块链技术实现安全生产监管现状的同步共享、监管过程的可控可追溯以及责任的明确划分，保证安全生产监管的高效、透明和可信。（来源：2021 全球区块链创新应用示范案例集）
浙江省财政厅	浙江区块链 电子票据平台	蚂蚁与浙江省财政厅共同搭建浙江区块链电子票据平台，于 2019 年 6 月上线使用。区块链电子票据平台已与浙江医保、商保完成对接，从而实现票据理赔全链路打通，原先理赔时效从天的维度提升到小时级。（来源：蚂蚁集团官网）
深圳市税务局	区块链电子发票平台	2018 年 8 月，深圳市税务局与腾讯联合推出区块链电子发票平台，实现了线上直接申领与开具发票，无须专用硬件及为购票往返税务局，推动了深圳税收管理服务的质量和效率双提升。（来源：腾讯区块链微信公众号）

（2）医疗领域的典型案例如表 1-9 所示：

表 1-9 医疗领域区块链典型应用案例

机构名称	落地平台名称	应用情况
山东省医疗保障局 武汉市中心医院	鲁医链区块链 医疗健康服务平台	工商银行承建山东省医保区块链平台，利用区块链技术将电子处方、药品配送、支付交易等信息上链存储，解决了纸质处方难保存、疫情期间零接触就诊、失能人员和慢病患者就医困难、线上问诊缺少监管流程等痛点。（来源：2021 全球区块链创新应用示范案例集）
武汉市中心医院	区块链医疗 健康服务平台	蚂蚁利用区块链技术帮助武汉市中心医院打造“未来医院”，利用区块链医疗健康服务平台打通医院开具处方、药师审方、药品配送、药品支付、流程监管等多个环节，保障患者多渠道购药的安全。（来源：蚂蚁集团官网）
上海信医 科技有限公司	基于区块链的中药 处方流转及监管平台	基于区块链的中药代煎业务流转及监管平台为每一个中药处方打上独一无二的“身份证”，清楚的记录处方流转过程中的各个环节，保障中药饮片安全、有效、可追溯，有利于保证药品质量，保障用药安全，推动中药饮片流转监管的模式创新。（来源：2021 全球区块链创新应用示范案例集）

（3）司法领域的典型案例如表 1-10 所示：

表 1-10 司法领域区块链典型应用案例

机构名称	落地平台名称	应用情况
百度	百度超级链 电子签约平台	百度超级链电子签约平台采用区块链 + 可信时间戳 + 数字证书相结合的方式，在可靠电子签名基础上完成合同的签署，并通过百度超级链上链存证，为用户提供有效、可靠、低成本、易维权、有司法公信力的电子签约服务。（来源：百度超级链官网）
深圳法大大 网络科技有限公司	法大大实槌可信 电子证据平台	法大大实槌可信电子证据平台基于法大大的诉源治理区块链电子证据固化技术，实现让公证处 / 司法鉴定中心通过技术系统在线对客户系统的电子数据进行实时证并实时出证；结合实槌中后端的类案系统和执行服务，实现互联网业务的快速争议处置。（来源：法大大官网）
上海新虹桥公证处	“采虹印”公证服务平台	2020 年 5 月 30 日，趣链科技与上海新虹桥公证处联合发布了一站式电子证据存取证平台“采虹印”，面向政府监管、司法机构等相关部门以及 B 端商业机构，提供基于区块链的在线取证、存证、固证的全流程电子证据服务。（来源：趣链科技官网）
杭州互联网法院	杭州互联网法院 司法区块链	2018 年 09 月 18 日，杭州互联网法院宣布司法区块链正式上线运行，成为全国首家应用区块链技术定纷止争的法院。司法区块链拥有公证处、司法鉴定中心、CA、法院等重要区块链节点，让电子数据的生成、存储、传播、和使用的全流程可信。（来源：杭州互联网法院官网）

（4）产品溯源领域的典型案例如表 1-11 所示：

表 1-11 产品溯源领域区块链典型应用案例

机构名称	落地平台名称	应用情况
天猫	天猫国际全球溯源计划	2017 年 5 月 , 天猫国际跨境进口商品溯源利用区块链技术、药监码技术及大数据跟踪进口商品全链路信息，为跨境进口商品打上“身份证”。消费者可快速获知产品的生产、包装、发货等信息。（来源：蚂蚁集团官网）
浙江省市场监管局	浙冷链	法 2020 年 6 月 , 浙江省市场监管局借助蚂蚁区块链和阿里云技术建立“浙冷链”，实现从供应链首站到消费环节产品最小包装的闭环追溯管理，进一步健全了食品安全追溯体系，强化疫情防控。（来源：蚂蚁集团官网）
京东	智臻链防伪追溯平台	智臻链防伪追溯平台记录商品从原产地到消费者全生命周期每个环节的重要数据，通过物联网和区块链技术，建立科技互信机制，保障数据的不可篡改和隐私保护性，为企业提供产品流通数据的全流程追溯能力。（来源：京东官网）
浪潮集团	质量链	质量链通过汇集质量管理、政府监管、企业运营、第三方服务以及互联网舆情等数据形成数据湖，以数据为支撑采用“平台 + 生态”的发展理念提供一体化质量品牌服务，并形成了机构制定标准、第三方提供检测、企业加强赋码、百姓主动扫码、数据反馈企业的“多方共治一体化”闭环运行模式，为高质量发展和品牌提升提供新动能，助力国家“质量强国”战略实施。（来源：浪潮集团官网）
沃尔玛	沃尔玛中国区块链可追溯平台	2019 年 6 月 25 日，沃尔玛中国区块链可追溯平台正式启动。顾客通过扫描商品上的二维码，可以了解到商品供应源头及沃尔玛接收的地理位置信息、物流过程时间、产品检测报告等链上信息。（来源：《沃尔玛中国上线区块链可追溯平台》）

2 chapter two 区块链安全态势

- 区块链安全问题可以分为区块链体系安全问题与区块链在应用中的安全问题。区块链体系安全问题包括区块链在共识、密码、加密算法、网络等协议层上的安全问题，以及在智能合约、跨链、链上链下协同、客户端上的扩展层安全问题；区块链应用安全问题包括区块链应用在内容、治理、数据融合、数据隐私、实名认证、数字孪生、预言机上的安全问题（如图 2-1 所示）。

图 2-1 区块链安全态势概览

一 区块链体系安全问题

1. 底层代码安全

- 底层代码作为区块链运行的根基，是保证区块链系统安全运行的基础。在区块链技术高速发展的过程中，针对底层代码漏洞的区块链应用攻击事件频发，造成了极大的经济损失，引发了公众对区块链安全性的质疑和对其发展前景的忧虑。因此，研发针对区块链底层代码的评估机制以保障区块链安全迫在眉睫。

- 目前实现区块链的编程语言主要包括 Solidity、Serpent、LLL 等图灵完备语言和 Go、Java 等高级编写语言，严重依赖于国外的开源项目。与此同时，随着对区块链密码协议的安全性要求越来越高，对密码协议的安全验证分析要求也越来越高。代码级的密码协议成为了一个新兴的研究方向，国外的代码级的密码协议安全验证分析的研究发展迅速，而国内仍以常用的安全验证分析为主，在代码级上分析密码协议实际执行是否安全的相关研究则少之又少。因此，完备的代码评估体系亟需被构建，以保障区块链应用安全。

- 除此之外，在现有的区块链底层代码体系中，区块链应用极易受到智能合约代码漏洞安全问题的影响，受到代码攻击的威胁。2019 年，通过对 Dogecoin、Ripple、Litecoin、Dash、Ethereum-Wallet 等区块链领域知名开源软件的扫描和人工审计，在代码层发现高危漏洞 746 个，中危漏洞 3497 个，对区块链安全有着极大的威胁。在语言安全、代码静态分析等方面，智能合约的代码安全问题也层出不穷，对其使用者造成了严重的困扰，在某种程度上限制了区块链的广泛发展。

- 在数据层以及应用层，底层代码安全问题也时有发生，造成严重的数据隐私泄露，破坏数据的保密性与完整性，对组织管理上的人员安全造成威胁。因此要重新构建完备、安全的区块链底层代码评估体系，从根本上解决代码安全问题。

2. 加密算法安全

- 虽然我国对区块链的起步研究并不迟于其它国家，但其中的应用研究高于基础研究，尤其是在一些关键的例如加密算法等技术上，严重依赖于外部开源项目。

- 加密算法处于区块链技术体系中的核心地位，得到了广泛的应用，是区块链技术的根基。随着《网络安全法》、《密码法》等法规的颁布，密码安全已上升至国家战略层面。因此，摆脱当前对国外技术的过度依赖，扭转区块链发展的被动局面，实现自主可控，构建先进、安全、可控的国产密码，并形成以国产密码为基础的网络空间安全体系已经刻不容缓。

- 目前国内各区块链底层技术平台都在尝试应用国密算法，但在融合的过程中仍然存在一些问题，比如对于 SSL 等上层的协议涉及较少，区块链相关硬件设施（如硬件钱包、国产密码机、云服务密码机等）很少采用国密标准进行设计，与国产芯片、操作系统及软件适配度不高等。同时，国密中并没有针对零知识证明、多方安全计算等热门密码学协议的标准，因此相关协议很难国密化。

- 除此之外，从先前大量的研究工作中能够发现，区块链在开发过程中面临着恶意后门漏洞嵌入的风险，尤其是第三方开发的数字钱包普遍存在着被植入后门的隐患。这些后门可以绕过所有的黑盒测试，不借助额外的信道，将支付密钥等用户秘密信息通过正常交易数据中的数字签名泄露给攻击者。因此，需要从区块链体系架构上重新设计，从根上解决软件后门问题。

3. 网络协议安全

- P2P 网络是在区块链网络层中频繁使用的一种架构。在 P2P 网络中，所有网络节点都是一个计算机系统，由互联网相互连接，信息可以由各个节点直接共享，而不需要中心服务器。换句话说，P2P 网络中的每个计算机系统既是服务器，又是客户端，节点与节点之间是对等的，与互联网中常使用的客户端 - 服务器架构存在根本性的差异。P2P 网络作为一种分布式应用架构，构成了区块链系统去中心化的基石。然而，P2P 网络“每个节点都是对等的”特性更多体现在通信上，在其他环节，每个节点还是会发挥着其他不一样的功能。比如有些节点主要承担计算能力，而有些节点承担的是存储功能，可以存储完整的块链式数据。

- 对于恶意用户而言，P2P 网络的这种特性可以被利用来从网络通信层对区块链系统发起 DDoS 攻击、日蚀攻击等各种攻击，严重威胁了区块链系统的安全性，对区块链系统造成了巨大的破坏。

- 对单个节点的 DDoS 攻击可以让其处理的信息超出最大承受度，而在接下来的时间里不能再去处理新的区块和交易信息。

- 日蚀攻击通过占据和积累受害者节点周围的点对点连接空隙，将这个节点阻绝在一个闭塞的网络中，使其不能和其他网络通信。这种攻击是从网络层面对区块链系统发起的一种攻击，目的是让最近更新的区块链信息不能流通到受害者节点，从而破坏区块链的安全性。日蚀攻击除了利用垄断所有连接来阻断一个或多个网络节点的手段之外，还包括 BGP 劫持等路由攻击手段。恶意用户使用 BGP 劫持让整个网络划分为至少两个独立的网络，这些网络之间不相交，且无法通信。在攻击期间，对应的区块链会分裂为至少两条并行的链；在攻击完成后，这些并行的链会重新调整合并为一条链，选取最长的链作为主链，比主链短的链都会失效，使得失效链上的交易和奖励都无效，从而恶意增加区块链网络的交易成本。

4. 共识协议安全

- 在区块链中，共识协议是其核心内容之一，因此，共识协议同时决定了区块链系统的性能及安全性。

- 区块链中使用的共识协议有很多，包括诸如 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。当前共识协议面临的主要威胁有：

- **拜占庭攻击**

  攻击者使用一定手段让超过一定比例的节点合谋，以达成非法共识。

- **双花攻击**

  攻击者通过控制算力或恶意利用共识协议延迟导致同一笔区块链资产被多次使用。

- **女巫攻击**

  攻击者通利用 P2P 网络的分布式特性，将一个节点伪装成多个节点，并将这多个伪装节点广播到整个网络中，从而影响网络中的正常节点。

- **预测攻击**

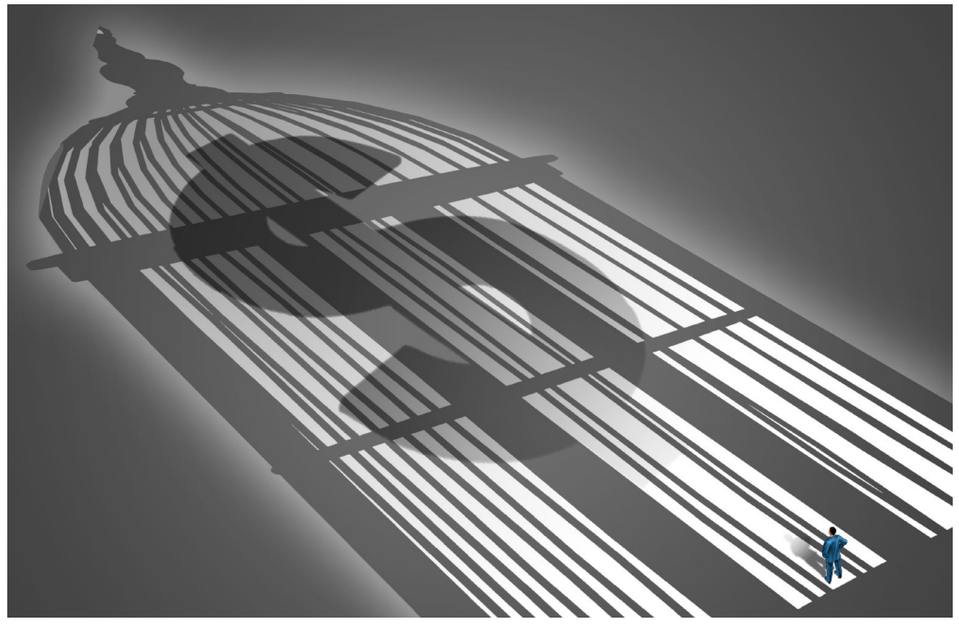
  攻击者利用共识机制的漏洞预测打包节点，进而发起具有针对性的恶意攻击。

- **重放攻击**

  攻击者发送一个目的主机已接收过的数据包，以达到欺骗系统的目的。此类攻击发生后可以产生与双花攻击类似的效果。

- **贿赂攻击**

  恶意节点通过协议之外的贿赂来收购算力，从而达到攻击区块链系统的目的。



5. 密码协议安全

- 密码算法与密码协议支撑了区块链安全体系，密码协议的安全决定了区块链的安全。

- 区块链技术中应用的核心密码算法主要有数字签名与杂凑函数，另外还采用了非对称加密体系来实现匿名，并利用公钥来代替用户的真实身份。但是由于区块链具有链上交易公开透明的特点，导致匿名的安全性并不够高，在交易的过程中仍会泄露信息。攻击者仍能够通过交易信息来追踪分析、推测用户的真实身份。

- 区块链中的密码协议大多依赖随机数这一不可或缺的参数，安全的随机数生成机制是密码算法安全的重要支撑。但由于真性随机数的生成较为困难，在大多数密码协议的开发过程中，常常使用伪随机数生成器来生成能够达到安全标准的一些随机数。但这也留下了一些安全漏洞。当生成的随机数安全性不达标时，可能会导致严重的安全事故。区块链中具有广泛的随机数生成需求，如果选取的伪随机数生成器存在后门，造成的损失是不可挽回的。

- NSA 曾在 NIST 的随机数生成器中写入了带后门的 Dual_EC_DRBG，在 RSA 算法的实现过程中埋下了一个漏洞，使其能够轻松破解加密信息；区块浏览器 blockchain.info 也曾被曝没有正确生成随机数，导致私钥暴露，进而引发了严重的安全问题；交易所 Bitfinex 也被攻击者利用了其系统中存在的多重签名缺陷，遭受了约 6800 万美元的损失；Krypton 平台遭受的 51% 算力攻击也是一种在密码协议层面的攻击。

- 综上，采取更加安全的密码协议，尽可能地避免交易过程中信息泄露问题，是区块链发展过程中的重中之重。

6. 智能合约安全

- 近年来，随着去中心化应用（Decentralized Application，DApp）的推广，由智能合约主导的新型区块链平台与应用以及其中涉及的数字资产出现了指数级别的增长。但在运营的过程中，智能合约频频出现的漏洞与频发的安全问题严重影响了整个区块链上的经济生长态势。

- 智能合约的低运行成本、低干预风险等优势使其成为了区块链的重要组成部分，在区块链数字经济中得到了大规模的应用。一但智能合约的设计存在问题，就容易被攻击者加以恶意利用，将会带来巨大的损失。

- 例如以太坊基于智能合约的著名众筹项目 Dao，在 2016 年被不法者利用重入攻击（Reentrancy）引发了以太坊硬分叉（hard fork）和以太坊社区的分裂。此外，基于例如整数溢出等其他智能合约漏洞的攻击也呈现出逐年递增的态势。

- 相比于传统软件，智能合约的安全问题更加棘手，现实情况也更加严峻。智能合约中出现频率最高的 10 类安全问题分别为：代码重入、访问控制、整数溢出、未严格判断不安全函数调用返回值、拒绝服务、可预测的随机处理、竞争条件 / 非法预先交易、时间戳依赖、短地址攻击以及其他未知漏洞类。

- 除此之外，智能合约在本身的设计上也存在着如下缺陷：

  （1）智能合约秉承“代码即规则”的理念，一旦被部署便无法修改，其不可篡改的特性促成了它的高可信度，但也为它埋下了一个安全隐患。任何人都可以对已上线的合约中的安全漏洞发起攻击，即使有恶意交易被记录下来，也无法将其从区块链上剔除。

  （2）智能合约常常是公开透明的，许多项目会将代码开源来博得用户的信任度，但这也大大降低了黑客的攻击成本。

（3）智能合约的起步时间较晚，发展时间不足，本身就存在很多短板，并且专业技术人员的匮乏也使得其存在许多的人为漏洞。

（4）当前还没有足够成熟的漏洞挖掘自动化工具来验证智能合约的代码是否安全，主要还是依靠经验专家进行代码审计，或者寄托于专业开发者的技术水平，这已经无法满足当前功能逐渐复杂的交易需求，并且在日益壮大的智能合约规模与漏洞挖掘难度显著提升的新形势下，高效地进行漏洞分析与发现成为了一个亟待解决的问题。

（5）一旦智能合约被攻击者攻破，将会严重损害合约的经济价值，降低公众对项目的信任。回滚交易的唯一方法是执行硬分叉，但这又在一定程度上冲击了区块链系统的去中心化理念。

7. 链上链下协同安全

- 可扩展性是区块链大规模应用的一个瓶颈。链下支付通道网络作为解决该问题的关键方案之一，可以在遵守现有区块链共识协议的基础上，极大提升区块链交易的可扩展性。以往的区块链交易需要在链上进行清算，经过全网的节点认证。而支付通道网络与此不同，它包含多个支付通道，通过支付通道可以将交易转移到链下，经过用户支付的双方验证。这样一来，用户可以在链下完成大量的交易，只需要在链上确认部分关键的交易。这部分交易可以避开区块链的共识协议， 因此效率会大大提高。

- 闪电网络首先需要寻找一条连接交易双方的支付路径。假如付款方想转账给收款方，闪电网络提供一个连接双方的支付路径，这条路径的两头分别是收款方和付款方，不仅如此，路径中包含的多个支付通道的余额需要满足交易的条件。

- 由于支付路径上的中间节点会收取一定比例的交易费用，保证交易费率低至关重要。闪电网络是一种链下扩容方案，是在主链之外建立的第二层的

交易网络。为了保证闪电网络中交易的匿名性高于一般的链上交易，寻找路径时首先应当保证一次多跳支付的付款方和收款方不泄漏给其他节点，其次应当保证支付路径中包含的节点不被付款方和收款方以外的节点获取。同时，一次多跳支付的支付金额不能被透漏给支付路径以外的节点，每个支付通道的余额信息不应该被通道持有者以外的用户获取。

- 由于支付隐私受到闪电网络的保证，用户禁止公布每个支付通道的余额信息，能公布的只有通道的存款交易、结算交易等信息。每个用户都要维护一个支付通道信息的网络拓扑，这个网络拓扑是为了用户在支付时能够找到一条支付路径。用户在收集其他支付通道信息的同时，也在广播自己的支付通道信息。当用户想要付款的时候，先通过网络拓扑找到一条连通的支付路径，并且询问支付路径上的中间节点，确保这些支付通道的余额足够。因此，攻击者可以伪装成付款方通过广播消息去获得支付通道的余额信息，这样就破坏了闪电网络的隐私性。并且，用户维护的网络拓扑结构并不是实时更新的，处于滞后的状态，很可能导致寻找到的支付路径走不通或处于不可用的状态。这样一来，还需要重新路由，导致闪电网络的效率低下。

8. 跨链安全

- 随着各大行业各个领域都在不断开展对区块链领域的应用试水，在可见的未来，很快会出现多种行业联盟链并存的局面，多链协同、跨链交互、信息共享是各领域单链落地后的必然趋势。

- 不同的区块链底层往往会采用不同的数据存储结构、加密算法、共识机制，这将导致跨链交易中异构链交接与交易合法性证明存在困难；不同来源的数据在跨链系统中还会涉及到信息传递路由与与数据安全的问题。此外，不同链中的用户身份确认机制也存在着一定的可靠性问题与隐私泄露风险，对于链间访问权限控制也是一个极大的挑战。因此，实现异构区块链的快速接入、对跨链交易进行可靠传递和可信验证、对跨链交易数据进行隐私保护对于跨链应用至关重要。

- 2021 年，区块链业界发生了多起针对跨链安全的重大攻击事件，引起了严重的安全事故：THORChain 在 6 月 29 日和 7 月 16 日分别遭受了两次恶意攻击，损失总计超过 2500 万美元；跨链项目 Chainswap 合约在 7 月 3 日和 7 月 11 日遭到两次攻击，攻击部位主要位于跨链桥的智能合约部分，总共损失大约为 480 万美元；7 月 12 日，跨链项目 Anyswap 新推出的 V3 跨链流动性池遭到黑客攻击，总计损失超过 787 万美元。

- 综合分析这些攻击者的进攻方向，可以得到漏洞主要存在于跨链交易中的身份认证和交易确认过程中。并且，由于跨链平台的特殊性，在一个项目受到攻击时，往往还会牵连同平台上的其它项目。

9. 客户端安全

- 匿名性是区块链交易的一个重要特性，账号地址之间的价值流动是区块链交易的本质，但是通过账号地址并不能确认账户拥有者的真实身份。交易时只需要验证交易发起者账户对应私钥的有效签名，而不需要知道私钥持有者的身份信息。因此，只要攻击者截取了账户私钥就可以盗窃账户，并且无法追踪到攻击者的真实身份；链上的交易一旦完成，将无法逆转，被盗窃的账户也就无法找回了。存储私钥的工具称为区块链钱包，如今钱包被盗窃的现象在各种公链中十分频繁，给用户造成了巨大的损失，因此如何保证区块链钱包安全是区块链客户端安全面临的一个重大挑战。

- 区块链钱包在生成，存储以及使用期间都可能遭到攻击。在钱包生成阶段，攻击者通过分析分层确定性钱包中的随机数之间的关联性，可以推导出钱包的私钥。如果攻击者掌握了分层确定性钱包的父私钥，那么可以直接得到与父私钥关联的子私钥。钱包存储是通过交易所的保管完成的，因此攻击者常常攻击交易所来获取钱包盗窃资产。在使用阶段，由于个人原因，用户常常重复使用相同的随机数来生成椭圆曲线数字签名，这带来了安全隐患，攻击者可以分析椭圆曲线数字签名来反向推导出私钥。

二 金融应用安全问题

1. 内容安全

- 区块链上的内容安全问题随着区块链应用的扩张而逐渐凸显，区块链的匿名性为用户提供隐私安全保障的同时，也使得攻击者更容易利用这一特点来进行有害信息的传播，区块链不可篡改、公开透明等特性也为网络黑客留下了可进攻的一个缺口。目前，全球主要国家在推进发展区块链基础建设的同时，都开始加快在区块链内容监管方面的政策与法律框架规划和制定。

- 2019 年初，中央网信办委托浙江大学团队建设境内区块链应用的链上监管系统，首次引入了“以链治链”的监管技术思路，并率先开展了技术实践、探索了“以链治链”的技术可行性，即将应用链数据接入监管链，采用区块链技术实现应用链信息服务的监管，完成分布式和多层次的信息监测和管控。该系统计划在全国范围内选择 50 个区块链信息服务开展试点接入工作。

- “以链治链”技术思路的合理性已被充分证明，但在分层多级监管、危害内容治理等多个方向上还存在大量理论和技术问题，总结如下。

（1）大规模并发式监管存在较高的效率问题。由于区块链中采用了加密机制来维护用户的匿名身份与数据隐私，但一些不法分子也可以藉由区块链的这种特性来逃避监管，因此关于区块链的安全合规检查一直无法高效开展。

（2）区块链数据难以进行快速修正。由于区块链具有不可篡改的特性，即使监管方发现了区块链中的合约漏洞、非法数据等恶意行为发布的错误信息，也无法及时进行修正。

（3）跨链监管难以实现。随着区块链应用落地的部署逐渐加快，不同职责的监管部门需要在区块链上开展合作。在一些跨链事务中，监管机构常常需

要整合多元被监管方的数据进行交叉比对与综合分析。但数据不统一、跨链信息资源互操作性差等问题将导致“数据孤岛”。除此之外，由于信息互通困难，跨部门协作的监管指令难以高效传递，监管责任人也难以落实，使得跨领域跨链数据的协同监管十分困难。

虽然当前的区块链内容监管建设取得了一定的成绩，但在实现跨链监管、协同监管、隐私计算和自动化监管等方面，面临的问题仍亟待解决和突破。

2. 治理安全

- 区块链治理是区块链安全和可持续性生态建设的重要基石。在区块链基础建设高速发展的同时，区块链技术和产业仍然存在着的性能瓶颈和安全隐患区块链治理问题已经成为各机构关注的重点。
- 现阶段，大部分联盟链应用中的资源分配、决策治理是由一个权威机构以中心化的形式进行的，这与区块链的分布式核心思想相违背。去中心化是区块链安全中亘古不变的核心价值与中心思想，因此在区块链的每一个环节与各个管理过程中都应该尽可能避免中心化的出现，从而规避中心化带来的安全风险。目前中心化的区块链资源分配和治理方式阻碍了决策的公平性和透明性。
- 分布式的治理决策机制可以实现资源的分配和有效治理，使区块链监管治理更加透明化，同时也面临着两大核心挑战：

  （1）如何有效引入主动干预机制。设计一个基于陷门的可主动干预公链共识协议，使得当权者可以绕过工作量证明机制，不再需要投入大量的工作量即可发布区块。

  （2）如何有效引入区块链审查机制。设计一个基于权益的自纠错分布式区块链审查机制，尽可能地避免由于区块链的不可篡改性，使得账本中的错误无法修改的问题。

- 解决区块链治理与决策中面临的挑战是构建分布式的区块链资源分配与决策治理框架的关键所在。

3. 数据融合

- 机器学习和人工智能技术高度依赖模型、算法，更依赖于通过海量数据进行模型训练，从而不断改进，单单依靠某一机构所掌握的数据，无法实现技术的快速突破。但是由于竞争关系、安全问题、审批流程等因素，数据的流通存在着难以打破的壁垒，形成所谓的“数据孤岛”。联邦学习旨在帮助多个机构进行协同建模，进而打破数据孤岛，实现数据的互联互通。
- 联邦学习的概念最早于 2016 年由 Google 公司提出，用于解决 Android 手机终端用户在本地更新模型方面的问题，其研究成果已在 GBoard 输入法中针对联想词和智能提示等功能进行了应用实践。与集中式学习相比，联邦学习更强调个人对数据的控制权，即“数据不离域”，故该方法对于医疗、金融、交通等领域下的机器学习任务尤为适用。一方面 , 此类场景下的数据往往包含大量个人敏感信息，且受政策与法律的制约不可传播与共享；另一方面，联邦学习能够很好的避免大数据传输下的带宽占用。因此，联邦学习能够有效的促进跨地区、跨行业、跨部门的数据共享互通，并且保障数据所有者、使用者各方面的各自利益分配，提升整体制造全过程的紧密性、完整性和有效性，从而促进工业大数据的共享开放、融合创新以及价值再造。
- 各国在联邦学习领域都进行了相关布局。美国宾夕法尼亚大学与英特尔正

在推进面向医学影像的联邦学习平台，旨在建立通用的高效的医疗模型，全球已有 19 所医学科研机构加入，英特尔为该平台的效率和可靠性提供技术支持。欧盟成立 MELLODDY 组织，致力于通过联合建模的方法提高药品研发的效率，MELLODDY 的 10 个医药合作伙伴正在贡献数十亿组数据、几百个 TB 的标记着分子信息的图片。欧盟同时发起了 FeatureCloud 项目，旨在建立一个联合建模平台，使全欧洲国家共享医疗数据。瑞士再保险公司与微众银行签署战略合作协议，致力探索联合建模在保险行业风险管理中的应用，以促进该行业的数据共享，提高数据利用率。

- 区块链作为一个去中心化、数据加密、不可篡改的分布式共享数据库，可以为联邦学习的数据交换提供数据保密性从而对用户隐私进行保障，保证各参与方之间的数据安全，也可以保证多参与方提供数据进行模型训练的数据一致性。区块链的价值驱动激励机制也能够增加各参与方之间提供数据、更新网络模型参数的积极性。

4. 数据隐私

- 区块链中的数据隐私是多维度的，它不仅包括用户的交易隐私、身份隐私，还包括了从中分析得到的用户行为画像。交易隐私主要包括关于此次交易的相关账户、账户余额、资金流向、交易详情等；身份隐私主要包括区块链用户在现实生活中的自然人身份以及交易偏好等。由于区块链数据存在公开透明、无法篡改、可追溯等特性，攻击者能够轻而易举地通过一些关联性的区块链地址来对多个交易进行融合分析，得出交易的时间、地点、场景等数据，进而总结出用户的行为模式，获取到关于用户的隐私数据，进而从中牟利。

- 当前区块链面临的主要数据隐私泄露威胁有：

（1）特殊交易被跟踪

攻击者可以通过跟踪区块链中的一些特殊交易来对用户进行身份标记，进而将这些交易的用户类别抽取出来，缩小攻击范围，确定攻击目标。

（2）交易规律被探查

攻击者针对某个特定的攻击目标，去搜寻更多有关交易，从中进行数据分析，规律整理，进而获取该用户在区块链交易中留下的隐私数据。

（3）真实身份被顶替

攻击者利用获取到的隐私数据，结合聚类分析和时间分析，将假名映射到用户真实身份，顶替用户进行非法交易，侵害用户的合法权益，为自身牟利。

5. 实名认证

- 区块链保护用户的交易隐私和身份隐私，它的匿名性和隐私性在保护用户数据隐私的同时也带来了风险，主要包括以下三个方面：

（1）在项目价值方面，区块链的匿名性使得批量虚假注册层出不穷，项目可能存在大量虚假用户，降低了项目的价值，最后整个项目会因为缺乏价值而逐渐消失。

（2）在监管方面，匿名性使得区块链上的数字资产难以被统一监管，伴随着区块链的蓬勃发展，实名认证已经成为了对区块链进行监管的必由之路。

（3）在个人资产方面，由于区块链技术未来会被用来承载实体世界的财产，实体世界的财产权利必将收到法律的约束和规范，同理也受到法律的保护。如果没有实名认证，个人的资产难以保证不受到他人的侵犯，个人也不能合规地对接实体世界的资产。

- 因此，实名认证是保障区块链应用价值的基本手段，区块链应用通过实名认证接纳真实用户、拒绝虚假用户，避免了虚假数据的产生，大幅提升了区块链上项目的价值。此外，实名认证也是对区块链进行监管、保护个人实体和数字资产的重要措施。

- 由于实名认证关乎用户的个人私密数据安全，考虑到用户个人实名信息的敏感性，部分用户对实名认证仍有抵触心理，实名认证的发展任重而道远。此外，传统实名认证系统对用户私密数据的保存缺乏透明性，易导致用户私密数据泄露。因此，设计一个可以保护用户隐私的实名认证方案至关重要。

6. 数字孪生

- 数字孪生是一种超越现实的概念，指充分使用物理模型、传感器、系统历史运行数据进行过程仿真，在虚拟的电子空间实现对现实实体的映射。使用数字孪生技术可以更好地展现对应实体的全生命周期过程，使得建立的模型更接近实际情况，帮助人们更好地认识现实中实际运行的系统。

- 数字孪生作为一个极为复杂的数字映射系统，涉及到多种技术，也存在着部分安全问题。

（1）网络安全

数字孪生涉及到原有系统的基础设备大多是长期运行在封闭系统环境下的简单设备。数字孪生的应用使得这些设备有联网的需求，而这些设备缺少有效的安全措施，极易遭受网络攻击。一个系统的安全程度取决于最薄弱的环节，数字孪生技术系统较为复杂，综合了硬件传感器和仿真软件，任何一个环节被忽视安全漏洞都可能导致整个系统级别的安全问题。因此，从小型嵌入式传感器到中心服务器，必须保证硬件不被侵入成为后门。网络安全问题涉及到系统中使用的交换机、路由器等硬件，以及配套的网络设置，防火墙等所有软件。

（2）数据安全

数字孪生技术高度依赖各个传感器的实时数据，这些数据大多是机密数据，有着极高的商业价值；数字孪生体作为一个实时同步的动态模型，也是有着高商业价值的机密数据，因此必须限制其访问权限，防止隐私数据外泄。

（3）认证安全

数字孪生需要海量的传感器数据达成同步状态，并根据其状态实时调整运行策略。数字孪生体从所有的传感器获取数据，使得认证安全显得极为重

要。攻击者可以伪造错误的数据，恶意欺骗数字孪生系统，使得物理实体和数字虚体之间无法达成同步，甚至导致数字孪生体反映出了错误的结果，带来错误的判断和调整决策。

- 数字孪生技术有不可限量的发展空间和潜力，在很多领域已经落地实现并展现了其巨大的应用价值，但是与之相随的安全问题仍然是重大的挑战。

7. 预言机安全

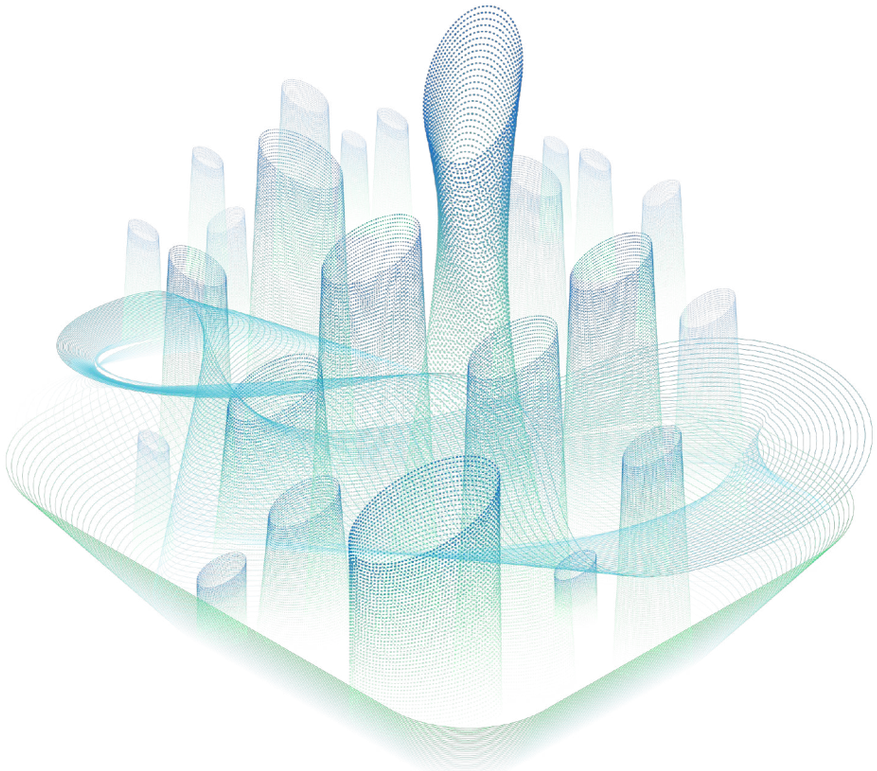
- 预言机是连通区块链与互联网以及其它区块链网络等现实世界保持数据、信息沟通的“桥梁”，是连接两个不同世界的“中间件”。预言机从现实世界中搬运知识，转换成为区块链可读可用的数据，提供给智能合约，智能合约判断现实世界中的事件是否发生，从而裁定是否执行代码。这种方式保证了区块链的可信赖性和透明性；但是，如果输入的数据是错误的，就会给链上用户带来巨大的损失。

- 预言机安全事件已发生过多次。例如 DeFi 衍生品平台 SyntheTIx 曾在 2019 年 6 月遭遇过重大的预言机问题。SyntheTIx 预言机负责给它的智能合约提供上游价格源数据，6 月 25 日，它引入了错误价格数据，该数据报告的 KRW（韩元）价格是实际价格的 1000 多倍。这一错误数据被一个交易机器人发现后迅速套利，借此获取了超过 10 亿美元的利益。最后 SyntheTIx 跟该交易机器人的所有者协商解决，在支付一定的漏洞赏金之后，将其恢复。在这个过程中，值得警惕的是，缺乏有效性验证的中心化预言机在数据正确性、稳定性方面存在极大的安全隐患。

- 非中心化预言机中也存在着例如女巫攻击等安全问题。女巫攻击会通过控制预言机池，提供错误数据，影响最终答案。为减少操作成本，女巫攻击者还会采用镜像，这些恶意预言机会在链下共享数据，假装有独立数据源，

这样结果是减少了数据源的分散化，降低了安全性。此外，预言机节点中也可能会存在“搭便车问题”，即某些节点为了节约成本而抄袭其它节点数据的情况，这亦会降低数据源的分散程度，不利于安全。

- 开拓区块链新领域，链上、链下的数据交换势在必行，预言机的作用大有可观，但是现阶段的预言机还很难及时应对和抵御黑客的攻击。因此，只有解决了核心的安全问题，预言机才有具有可信度。



3 chapter three 区块链安全风险应对框架

- 区块链安全风险应对框架可分为体系安全问题应对框架与应用安全应用框架。具体应对方式如图 3-1 所示。

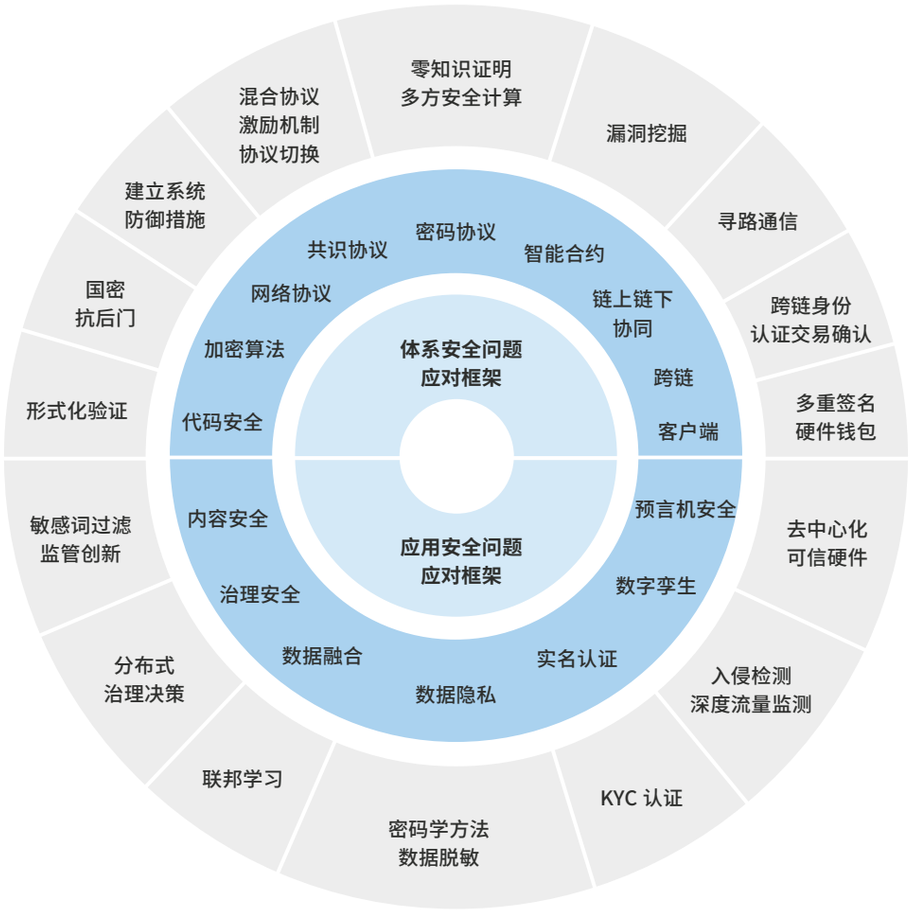


图 3-1 区块链安全风险应对框架

一 区块链体系安全问题应对框架

1. 代码安全 - 形式化

- 随着区块链技术的广泛应用，构建完备的代码安全评估体系迫在眉睫。针对目前底层代码安全存在的问题，可以从以下几个方面入手：

（1）加快研究形式化建模和验证技术，加强形式化验证技术在区块链底层代码中的研究力度。现有的形式化验证和程序分析工具多是针对已知漏洞的检测和验证，未来的研究需更加关注现有的智能合约的反模式，构造动态检测的程序分析工具，同时大力研究形式化验证理论基础，建立形式化验证的标准。

（2）构建代码级的密码协议安全验证分析方案，推动国内代码级密码协议安全验证方向的发展，加强实验研究，达到国际领先水平。

（3）大力研究针对于智能合约的沙盒环境，建立适用于多样、复杂场景的沙盒环境检测技术，提供更加丰富的方案，保障智能合约的安全性和可信性，推动区块链技术的发展。

- 其中，形式化验证是保障区块链底层代码安全的重要方案与发展方向。将形式化方法应用于智能合约，可以使得合约的生成和执行有规范性约束，保障了智能合约的生产过程和执行效力。通过形式化语言，将合约中的概念、判断、推理转化成智能合约模型，消除自然语言的歧义性、不通用性，进而采用形式化工具对智能合约建模、分析和验证，进行一致性测试。

- 综上，从以上三个方面出发，加强底层代码安全问题的研究，从多个角度来思考问题，建立健全代码评估体系，才能从根本上解决代码安全问题。

2. 加密算法安全 - 国密、抗后门

- 国密算法的应用与创新随着区块链底层技术的加速研发被真正的提上日程，加强国产密码算法方面的自主创新研究与开发已经迫在眉睫。对于国密算法体系当前的问题，可以从以下几个方面着手改进：

  （1）加快推进区块链中的加密算法更新，使用国密算法替代国外开源算法，并加大关于国密算法在区块链底层技术中的应用研究力度，增加实验、实践，并进行标准化工作，制定相关的技术说明书与应用指南。

  （2）进一步开展国产密码新算法的研究，包括零知识证明、多方安全计算、签名、共识等更为丰富的方案并制定相应的标准说明，不断壮大国密算法体系。

  （3）开展关于可信硬件方面的密码学处理模块的研究，加大硬件系统对区块链的支撑力度，扩展区块链在物联网、工业互联网等领域的集成应用，加速推动多领域协同创新。

  （4）深度促进区块链中加密算法研究的国际性合作，在合作中结合现有高效安全的密码技术，发挥自身的原始创新能力，努力提升自主密码算法的可靠性，并扩大其影响力，推进国产密码的国际化应用。

- 此外，关于区块链中的抗软件后门方法，可以利用反向防火墙技术来解决植入后门的签名算法中，平均两次就能泄露信息的隐蔽信道问题。反向防火墙指的是在交易信息上链之前，区块链节点对交易信息进行过滤、清洗，来消除这个隐蔽信道。

《专题 | 国产密码体系在区块链中的应用与挑战》北京大学信息科学技术学院教授、区块链研究中心主任陈钟，北京大学软件工程国家工程中心 副研究员 关志，刊登于《中国信息安全》杂志 2019 年第 11 期。
链接：专题 | 国产密码体系在区块链中的应用与挑战 (gdinsa.org)

3. 网络协议安全

- 区块链中的网络攻击主要是依靠区块链中存在问题的机制以及网络中固有的安全问题来达到将受害节点隔离的目的，从而使受害节点遭受各种损失。因此，我们需要针对网络层攻击建立更加系统的防御措施，这样才能更好地预防区块链网络层中的 0Day 攻击，建立一个更加可靠的通信环境。

- 比如日蚀攻击主要通过操纵受害节点对连接节点的选择来实施攻击。而 1 个节点选择 peer 时，该节点会从自己的 new 表（包含了从 peer 学到的节点信息）以及自己的 tied 表（节点曾经连接过的节点信息）中进行选择，日蚀攻击的攻击者正是通过填满这 2 张表达到操纵受害节点选择 peer 的目的。因此在日蚀攻击被披露以后，区块链社区迅速地禁止了对远程节点的 new 表和 tied 表的直接访问，这样攻击者几乎不可能同时填满这 2 张表（最多填满 new 表，且十分困难）。通过这个措施以及其他的一些补丁使得日蚀攻击的难度增大。

- 区块链网络中的 BGP 劫持攻击主要通过虚假的 BGP 通知来转移传递给受害节点的网络信息，从而达到将受害节点隔离的目的。因此可以通过中继网络来解决 BGP 劫持。SABRE 其核心思想是通过在网络中选取安全的位置来放置区块链网络的中继节点，并确保中继节点之间以及外部节点与中继节点之间的连接安全性。当区块链网络中的节点与 SABRE 的中继节点建立连接时，SABRE 就能依靠自己的网络安全性来保证与 SABRE 连接的节点不会被 BGP 劫持所隔离。并且通过中继网络主要是大量通信，而不是大量计算这个特征，采用可编程交换机（P4）实现大部分的逻辑，对 DDoS 攻击也有一定的抵御能力。但是这个中继网络的设计同时也在一定程度上违背了区块链系统去中心化的特征，使得攻击者目标更加集中。

4. 共识协议安全

- 针对共识协议安全问题，可以从三个方面来进行研究和解决，一是融合不同机制的优点进行互补，设计更安全的新共识机制；二是与激励机制进行配合，提高节点作恶成本，从而提高共识协议的安全性；三是根据业务场景选择多种或可切换的共识算法。

（1）混合协议

区块链存在“三元悖论”——安全性、扩展性和去中心化三者不可兼得，只能依靠牺牲一方的效果来满足另外两方的需求。不同的共识算法有不同的侧重和工作效率，所以单一的共识算法很难满足复杂业务场景的安全要求。以此为切入点，混合共识机制可以把两种或多种共识机制运用在同一区块链的底层架构中。合理运用混合共识，可以弥补单一共识机制带来的效率低下、失去安全防护或牺牲中心化程度的缺陷。

（2）激励机制

共识协议规定了节点为维护区块链账本安全性、一致性和活性而必须遵守的行为规范和行动次序；激励机制则规定了在共识过程中为鼓励节点验证区块链账本数据而发行的经济权益，通常包括发行机制、分配机制、交易费定价机制。共识协议通过与奖惩激励机制的配合，利用经济平衡的手段，鼓励节点参与到维护区块链系统安全运行中来，防止对总帐本进行篡改、为节点长期维持区块链网络运行提供动力，从而提高了共识协议的安全性。

（3）协议切换

共识协议种类繁杂，无论使用何种共识协议，想要完全解决存在的安全威胁是非常困难的。共识协议安全更多的是在确保安全和攻破安全防御所付出的代价之间找一个平衡点，判断共识协议是否安全应该立足于具体的应用场景。因此，区块链应用可以结合业务需求与应用场景，利用可插拔共识机制技术，实现多场景下共识机制的自由切换，从而采取适当的共识机制来避免攻击者利用共识机制的漏洞破坏区块链网络。

5. 密码协议 - 零知识证明、多方安全计算

- 近年来，多方安全计算技术作为一种新型隐私计算密码协议，能够在不泄露各方原始数据信息的前提下完成多方数据跨主体的共同计算，提供了区块链分布式数据计算过程中隐私保护的新思路，对加速区块链技术在各个领域的应用落地起到了重要作用。为进一步加深多方安全计算在区块链中的应用，可以从构造前摄性安全 MPC 通用可重组模型和群体可验证 MPC 安全模型、构造前摄性安全 MPC 协议和群体可验证 MPC 协议、构造基于硬件加速的高并发式 MPC 协议，并从构建恶意敌手编译器等方法着手，大力推动多方安全计算与区块链的产业结合，提高区块链中多方安全计算的安全性、可验证性、高效性和可用性。

- 零知识证明技术能够在不泄露信息的前提下对用户身份、交易信息等进行验证，为区块链中的信息交互提供了更加安全的隐藏手段。零知识证明分为交互式与非交互式，基础的交互式零知识证明通过证明者与验证者进行交互，回答验证者的提问，来证明自己；非交互式零知识证明避免了交互过程，以减少串通的可能性，使证明更具有可信度。

6. 智能合约安全 - 漏洞挖掘

- 形式化验证、模糊测试、符号执行和污点分析等方法是当前主流的智能合约漏洞挖掘手段。

- 形式化验证是将智能合约内容通过逻辑语言进行建模，利用严谨的数学推理来检查智能合约中是否存在漏洞。与传统的穷举测试法相比，基于数学的形式化智能合约模型，在推理证明的过程中能够有效涵盖穷举漏洞，在一定范围内完全覆盖代码行为，将可能性遗漏减小到最低，弥补了原有审计工作的局限性。因此，形式化验证方法已经在各大安全领域展开了初步应用，并取得了良好成效。

- 模糊测试需要生成大量随机非预期数据来作为输入，观察智能合约在运行过程中是否会发生异常，并跟踪检测异常发生的位置与条件。根据故障检测结果，对输入数据进行微调，继续新一轮的运行与监测，尽可能多的触发智能合约的状态空间，并利用有限状态机来分析每一笔交易的状态，从而合理规避潜在的漏洞与安全风险。其主要特点就是简单、高效，并且在具有低误报率的同时还能够有利于检测出合约中更深层的漏洞。

- 符号执行指的是对合约执行过程中可能产生的不确定值的变量均采用符号来表示，在程序执行过程中逐条解释路径中的各条指令，根据语义更新执行状态，在路径分叉出进行分路，判断每一条路径是否存在漏洞，最后能够将每一条路径都遍历检测一遍。

- 污点分析是针对污点变量的一种数据流分析技术。它识别并标记智能合约中产生污点信息之处，再按照传播规则对该点数据进行前后双向依赖分析，得到关于污点数据的依赖关系指令集，最后检测程序的关键点是否遭受污点信息的侵蚀。

- 未来，还可以从扩展形式化验证的应用范围、提取重点路径缩减路径空间、动态符号执行辅助的模糊测试技术等方向着手对漏洞挖掘方法进行改进。

- 与此同时，针对智能合约安全问题，还应该从安全开发、合约测试、合约审计这三个角度采取措施，完善智能合约漏洞库，建立漏洞挖掘工具效率评价体系，并将不同的检测方法进行组合，进一步提高与完善漏洞挖掘的准确性、效率和自动化程度，满足未来与日俱增的大规模智能合约复杂漏洞挖掘需求。

7. 链上链下协同安全

- 支付通道信息分为两个部分，一部分是静态信息，即两个节点之间是否存在支付通道；另一部分是动态信息，比如节点的状态（是否在线），通道余额等。支付通道寻路时基于这两种信息完成寻路。

- 第一个在实际应用中使用的寻路方案通过定义支付通道网络寻路的寻路目标在一定程度上提高了寻路效率问题，但是在最后选择路径时，所计算路径上的节点需要将支付通道信息发布给付款方，这样恶意用户可以伪装成付款方获取多个支付通道上的余额信息，这并没有达到保护通道余额隐私的目标。针对这一问题，可以将交易金额分解成多个网络中预设的单元，类似于计算机网络中的分组交换网络。这样闪电网络种每一个交易中的每个单元可能通过不同的路径传输到收款方处。然而，这样的闪电网络依然存在缺陷。首先，需要对已有的支付通道网络协议进行较大的更改；其次，在多跳支付过程中，可以通过 HTLC 来保证资金安全；最后，没有解决用户在整个支付过程中的隐私保护问题，中间用户可以监听各个交易，从而获取付款方和收款方的支付隐私。恶意用户可以获取某次交易的付款方、收款方、以及交易金额等信息。

- 为了达到隐私保护目标，其基本思想是将整个网络划分为多个子集，每个子集包含一个地标节点。在寻路的初始阶段，每个子集以地标节点作为根节点，生成一棵生成树，每个包含在相应子集的节点都拥有一个在对应生成树的匿名地址。当新用户想要加入整个网络时，它根据自己目前已经建立通道的节点就近选择子集，并将该节点设置为自己的父亲节点。当用户需要完成从付款方到收款方的多跳支付时，付款方可基于收款方的匿名地址找到具有足够余额的支付路径并完成转账。为了保证付款方找到的路径所包含的通道余额充足，在寻路探测阶段需要将余额锁定。由于在寻路过程中用户需要发送探测消息寻路，并依赖分布式广度优先算法计算路径，因此寻路通信开销会很大，而且寻路时间较长。

8. 跨链安全 - 跨链身份认证、交易确认

- 解决跨链安全问题、制定跨链安全规范与准则，需要针对异构区块链间跨链业务完整生命周期所涉及的节点 / 网关准入、身份认证、跨链消息隐私、通信传输、交易确认等安全问题打造基于国密算法的跨链安全保障体系，采用多种安全防范策略，保障跨链系统的高度可靠性。

  （1）中继链节点准入及外部访问权限控制机制。针对跨链身份认证，可以利用分布式 CA 证书体系来对当前节点进行身份认证，再结合基于国密 SM2 算法的数字签名验证技术，并利用共识机制对中继链上的申请节点提案进行投票，实现中继链上的节点准入机制。提案通过后，新节点可获得证书，并同步其它节点的数据，实现对需要接入中继链的跨链网关和业务系统的访问权限控制。

  （2）跨链交易隐私和传输安全机制。针对跨链交易数据隐私安全问题，科研利用国密体系中的对称加密 SM4 算法来实现跨链体系中的端到端加密，实现跨链密文传输，保障跨链交易隐私数据的安全传输。除此之外，针对跨链交易过程中数据传输的网络通信安全问题，可以同时结合国密体系中基于密钥协商的算法 SM2-2 和对称加密 SM4 来作为加密传输体系，来有效隔绝非法窃听的第三方盗取消息。

  （3）异构跨链交易高效可信验证机制。利用基于中继链的高效可插拔验证引擎实现基于动态注入的验证规则，对相应应用链提交的跨链证明进行验证。结合智能合约，针对不同链上的不同规则与不同需求，动态建立并部署相应的验证规则并支持规则的升级与更改，实现区块链上交易的全生命周期管理，实现统一、高效、可信的交易在线验证确认机制。

9. 客户端安全

- 目前已有诸多区块链钱包管理方案被提出，主要包括在线钱包、离线钱包、气隙钱包和钱包托管等方案，上述方案虽然在一定程度上提升钱包使用的便利性和安全性，但都存在将钱包存储在单个位置、无法有效地抵抗单点攻击的问题。

- 为了应对单点攻击引发的安全性问题，可以将有效签名扩展为多个参与者合作生成，联合控制区块链钱包。这种联合控制机制可以通过多重签名 (Multi-signature) 来实现，包括 (t，n) 多重签名、(t，n) 门限签名等方案。(t，n) 多重签名方案在一次交易中，将对应的公钥与 n 个特殊地址相关联，设定一个方案阈值 t，只有当参与交易签名的用户满足这个阈值时，此次交易才被判定为有效。该方案使得只有满足阈值的攻击者进行签名，攻击才能成功，大大增加了欺诈交易的成本，提升了钱包的安全性。但是，多重签名方案中特殊地址 n 的值受到限制，并且在修改时要求公开企业的访问控制策略，这导致修改的难度很大，个人用户的匿名性也随之遭到严重的侵害，交易费用也会增加。(t，n) 门限签名与 (t，n) 多重签名不同的是，(t，n) 门限签名将账户的密钥分成 n 个部分，将每个部分分别交给不同的参与者来保管，从而实现对账户的联合控制。交易时，如果有达到阈值 t 的用户合作产生签名，那么该签名有效。这个方案可以很好地保护用户的匿名性，在产生签名的过程中不会泄漏个人的身份信息。由于多位参与者合作只产生一个签名，与 (t，n) 多重签名相比，交易的费用大幅降低，这有利与对区块链钱包进行更好地联合控制。由于 ECDSA 签名在区块链钱包中使用得最多，所以区块链上的门限签名多为对应的门限 ECDSA。

- 另一种保证区块链客户端安全的方案是硬件钱包。硬件钱包由一种硬件设备来实现，私钥被储存在实体设备的受保护区域中。硬件钱包像是生活中的纸质钱包，但是具有更为强大的功能，尤其体现在收付款上。由于硬件钱包的漏洞较少、应对攻击者与病毒的能力较强，截至目前，硬件钱包还

未发生过大规模安全事件。基于上述优点，硬件钱包逐渐成为公链开发者的首要选择。硬件钱包中存储了一个公钥和一个私钥，即所谓的密钥对。密钥对的拥有者即是钱包中资产的拥有者，没有了密钥对，也就没有了资产，密钥对和资产在某种意义上是划等号的。所以，如何安全有效保存用户的密钥成为了一个需要重点解决的问题。由于硬件设备中存放了钱包的私钥，而且在设备中可以完成签名，保证了私钥被限制在 PC 端。从这个方面来看，硬件钱包的安全性是毋庸置疑的。

二 金融应用安全问题应对框架

1. 内容安全

- 建立基于国产自主可控区块链平台的区块链应用监管系统，实现监管分级模型与评价体系的建设，形成区块链信息安全或监管标准，助力境内区块链行业的可持续发展，针对区块链的内容监管需求，大力推进区块链监管架构创新、区块链监管技术创新，需要利用以下几点关键技术：

（1）层次化跨链监管技术

针对目前区块链监管中存在的监管内容复杂、范围广、难以下探等问题，提出层次化的三层监管架构：主监管链、从监管链和业务链。结合中继链来维护骨干网的高效安全运行，承载多种异构跨链信息；采取直连跨链模式，使得平行链网关能够一对一直连通信；实现异构数据可信协同，促进异构业务链与监管链之间达成数据共识，实现不同链之间的监管信息能够做到互联互通。

（2）基于智能合约的跨监管机构协同技术

结合区块链智能合约技术来促监管指令高效路由，促进主从监管链之间的监管规则的高效下发与上传；同时实现监管指令智能协调，完善跨链合约的调用，促进跨机构监管自动化；建立监管权限访问控制体系，健全智能合约之间的权限控制，做到统一管理与多链协同。最终实现不同监管部门之间的信息畅通、统一管理，监管指令的高效下达，对不同监管机构的管理级别、监管权限进行管理。

（3）基于多重签名技术的分布式联盟自治框架

多重签名可以理解为对一个重要标的的多个签名，针对当下对监管的高安全、可审计的要求，通过多重签名技术可以有效提高裁决效率，同时保证其有效性。

（4）面向大规模监管的区块链核心技术

针对复杂监管网络，提出高鲁棒性高性能共识机制，研究复杂监管网络下的交易快速验证机制，针对数据流式指定动态分发策略；针对监管友好的异构大规模分层组网机制，研究大规模节点网络动态转发模型与异构多类型节点动态组织策略；针对基于监管链数据的混合高效存储模型，设计多级缓存机制，实现监管数据的高效存取，设计链上非结构化大文件存储模型，实现 PB 级监管链大文件数据的可信存储、安全共享与高效查询。

（5）监管友好的新型账本结构

针对隐私保护的交易模式，研究在监管权限管理机制下的隐私数据监管方法，以及在监管规则下的合规性内容监管。建立多级角色监管权限管理机制，保证授权与鉴权的一致性并保障其效率；研究高效可靠隐私数据监管技术，研究可追溯可还原的数据屏蔽方法，实现安全、有效、合规的可信审查。

（6）敏感词过滤技术

在区块链中实现基于确定有穷自动机（Deterministic Finite Automaton）算法的敏感数据过滤，从而有效监督、限制敏感词上链的行为，提升应急处置效率，保障区块链业务安全运行。

2. 治理安全

- 要解决区块链资源分配与治理中心化、存在着单点失败风险的问题，实现区块链治理决策的“透明化”，可以从分布式区块链资源分配与决策治理框架等方向重点突破，开展理论与实践研究，构建分布式的治理决策机制，完善公平的资源分配和有效决策治理，实现区块链风控智能化、监管精准化、治理透明化，支撑区块链生态的长期平稳发展。

（1）构建可证明安全的分布式区块链资源分配与决策治理框架。分布式区块链资源分配与决策治理中的核心问题是区块链上的用户的可验证投票问题，可以通过可验证 MPC 来解决，即将区块链中的权益持有者进行角色划分，引入专家支持方案，构建一个包括选民、专家和选举委员会的三方交互式治理框架。其中选民是指一组拥有固定数目权益数量的权益持有者，而专家则是一类特殊的投票者，他们在某个领域拥有专业知识和专长。在基于权益的投票机制中，选民和专家需对任何一项区块链中的提案进行投票表决，保证区块链社区中所有的用户都拥有参与区块链决策过程的权力。普通用户的投票权益可以合法授权给可信专家，由其进行代理投票。在此过程中，无法判断用户是作为选民亲自进行投票还是将权益授信给了专家，因此用户的隐私能够获得一定程度的保护。该方案可以有效解决区块链中关于软件更新等操作引起的硬分叉问题，保障区块链生态的长期稳定发展。

（2）搭建基于陷门的可主动干预机制与自纠错分布式治理框架。引入基于陷门的可主动干预公链共识协议，结合一类新的证明者 - 验证者协议 PoWorK，验证者无法辨别证明者投入的计算量或者是否拥有陷门。引入基于权益的自纠错分布式区块链审查机制，结合 Ouroboros 和 Algorand，通过构造门限可验证伪随机函数 VRF 来实现审计委员会的遴选，并进行审查，并进一步结合如 Redactable Blockchain 等可修订（或可重写）区块链技术，对审查有问题的区块进行自纠错。

3. 数据融合

- 尽管联邦学习使用户拥有了个人数据的控制权，但并不能完全防御潜在的隐私攻击。比如对于结构简单的机器学习模型 , 采用动态分析或计算记录间的相似度等方法便可推测出训练数据中个体的敏感信息。全球范围内对数据隐私的重视加剧了数据孤岛的产生，欧盟出台了首个关于数据隐私保护的法案《通用数据保护条例》（General Data Protection Regulation, GDPR），明确了对数据隐私保护的若干规定。我国在 2017 年起实施的《中华人民共和国网络安全法》和《中华人民共和国民法总则》中也指出“网络运营者不得泄露、篡改、毁坏其收集的个人信息，并且与第三方进行数据交易时需确保拟定的合同明确约定拟交易数据的范围和数据保护义务。”这意味着对于用户数据的收集必须公开、透明，企业、机构之间在没有用户授权的情况下不能交换数据。这成为联邦学习进一步推广的巨大挑战，如何在保证数据隐私的前提下进行联邦学习也成为国内外学术界、工业界广泛关注的课题。

- 另外，联邦学习也为 AI 模型的安全性带来了新的挑战，在联邦学习中，攻击者可以更轻松的实施毒化攻击。毒化攻击是指攻击者通过攻击训练集来误导学习过程的攻击方法。由于机器学习的主要学习内容来自训练集，因此，即使训练集只有一小部分遭受毒化攻击，仍会使得学习的效果大幅下降。如何抵御毒化攻击是对抗性环境下安全的联邦学习的重要研究领域。在联邦学习中，攻击者能够通过更改训局部模型的方式来改变全局模型的行为，

即为模型添加后门。该攻击可以在攻击者选择的输入上改变模型的行为而不影响其在其他任务上的精度。该攻击迄今为止没有得到很好的解决。

- 在实际应用中，因为孤岛数据具有不同的分布特点，所以联邦学习也可分为横向联邦学习（参与者的数据服从水平分布）和纵向联邦学习（参与者的数据服从垂直分布）。

- 在横向联邦学习中，每个参与者都拥有完整的特征空间，因此每个参与者可以在本地独立的训练模型。横向联邦学习的过程中，各个参与者在获得中心节点的副本后独立训练，并将训练后更新的模型参数上传至中心节点；中心节点将所有上传的参数整合至中心模型，并再次将模型分发出去；如此迭代，直至中心模型收敛。横向联邦学习能够让各节点的数据保留在本地，以降低带宽占用和隐私泄露的风险。在海内外专家的广泛关注下，横向联邦学习的安全隐私问题已基本解决。比如参与者上传的模型参数会泄漏它本地的信息，通常的做法是用安全合并的方法对新的模型参数进行保护，即参与者在本地用一次性密码本的方法对梯度进行加密，所有参与者两两协调生成一次性密码，合并后的一次性密码会自然消除，另外中心节点生成的中心模型也会泄漏参与者的信息，这一问题通常通过差分隐私来解决。

- 相比之下，纵向联邦学习受到的关注相对较少。现有纵向联邦学习隐私保护的解决方案是通过密码学技术（同态加密或多方安全计算）达到数据可用不可见的目的。Facebook 人工智能团队正在开发名为 CrypTen 的开源项目，这是一个基于 PyTorch 并且提供隐私保护的机器学习框架，可以在加密数据上完成联合建模。TFEncrypted 是另一个提供隐私保护的联合建模框架，它基于 TensorFlow 并且集成了多方安全计算等密码学技术。国内企业也开始了在该方向上的投入，微众银行提出 FATE 联合建模框架，可以让企业和机构在保护数据安全和数据隐私的前提下进行 AI 协作。蚂蚁金服也推出了摩斯安全计算平台能够在本地数据不泄露、原始数据不出域的前提下，通过密码学算法，分布式执行既定逻辑的运算并获得预期结果，从而完成数据合作。然而上述方法引入大量的带宽和计算开销，无法在实际应用中广泛部署。

4. 数据隐私 - 密码学、数据脱敏

- 区块链中防止隐私数据泄露的手段主要有现代密码学方法和数据脱敏。

- 现代密码学方法即利用哈希算法与加密解密算法对数据、用户身份、传输信道等进行加密保护，保障相关数据的隐私安全。

- 数据脱敏技术也叫数据的去隐私化，指的是通过给定的脱敏规则和策略，将一些区块链上的用户敏感信息数据进行转换或者修改，从而达到保护数据隐私的目的的一种技术手段。脱敏后的数据可以安全便捷的在开发、测试、外包或者其它非生产环境中进行使用，能够有效防止敏感数据直接暴露于不可信的区块链网络环境中。基于区块链的数据脱敏技术能保证数据私密性，为隐私保护下的数据开放提供了解决方案。

- 数据脱敏技术主要包括了以下几点主要方法。数据替换，使用固定的虚构值来替换真实值；数据无效化，对数据进行截断、隐藏等方式，剥离它的实际价值；数据随机化，使用随机数据代替真实值，能够模拟样本的真实性；数据偏移和取整，通过随机位移来改变数据，保持了数据的范围真实性，同时也对区块链大数据应用具有重大价值；数据掩码屏蔽，掩码隐蔽主要针对区块链中的账户类数据信息，通常做法是将账户的中间部分进行掩盖；数据灵活编码，通常根据区块链中数据保护的具体情况来利用一些特殊的编码规则。

5. 实名认证

- 区块链系统身份认证包括实名认证和可控匿名认证，主要采用的方法为 KYC(Know Your Customer) 认证方案。
- 身份认证是指在区块链系统中用于确认交易者身份的过程，实名认证要求在用户身份标识的建立和认证过程中直接或间接地确定交易者的真实身份。进一步的，区块链还可以做到可控匿名认证，即在用户身份标识的建立和认证过程中，除监管方以外的参与者不允许直接或间接确定交易者的真实身份。在必要时，监管方可复原出匿名化后交易方的真实身份。
- KYC 认证是一种被当前区块链项目普遍采用的实名认证机制。为了实现用户的准入控制并满足交易监管要求，Fabric、Corda、趣链区块链平台、微众银行 FISCO BCOS 等区块链项目都采用了 KYC 认证，在身份管理中采用基于数字证书的实名认证。它们在系统中部署公钥基础结构 (Public Key Infrastructure, 简称 PKI) 和证书认证中心 (Certificates Authority, 简称 CA) 来管理身份，用户基于非对称密码算法通过 CA 生成和管理数字身份，用户实名认证获得数字证书身份标识的过程主要如下：

（1）用户发送实名注册信息给 CA 申请数字证书；

（2）CA 核实用户实名信息，如果有误，则终止申请过程；

（3）CA 基于用户实名信息为用户生成公私钥并签发实名数字证书，确保数字证书与用户身份的一一绑定；

（4）CA 将生成的数字证书和私钥发送给用户；

（5）在区块链交易过程中用户使用数字证书作为身份标识符，通过私钥签名实现身份认证，身份管理的全周期过程中用户都是实名的。

基于数字证书的实名认证方案适用于中心化系统中账本保密的应用场景。

KYC 认证一般验证的三要素是姓名、身份证和手机验证，目前的 KYC 实名认证机制已经被广泛用于预防洗钱、身份盗窃、金融诈骗等犯罪行为。

6. 数字孪生

- 目前有很多成熟的网络安全解决方案，可以为数字孪生提供安全保证。例如入侵检测系统（IDS）可以检测和拦截来自外部的恶意请求和连接，防止包含病毒代码的片段进入系统，同时实现接入设备的管控，限制陌生设备的一切行为，要求设备必须经过认证；在网关部署的深度流量检测（DPI）可以审查系统所有内部外部信息交换，识别并拦截包含敏感信息的流量，防止机密数据外泄，同时检查从外界进入系统内部的流量信息，精准识别出恶意流量并拦截。
- 数字孪生对数据可信度和计算基础设施可信性都具有很高的要求，而区块链技术结构包含一整套行动协议与思维模式，通过链上参与方公认的规则、协议、流程和方法，能够使区块链系统的计算运行顺利进行，解决数据的可信度问题，为数字孪生构造一个可信的计算平台。物联网设备从物理世界收集数据并传输到电子空间，可以使用区块链技术进行保护。通过保证源认证和数据传输机制，利用区块链的密码学特性，使得数据孪生系统收集到的数据真实可信、不可篡改且可溯源，进而阻止恶意篡改和干扰基础设施影响正常计算结果。区块链系统采用通证（Token）的形式管理有价值的事物，通过 Token 实现资产上链，实现物理实体与数字体之间的一对一关系，可以防止有价值的实体经过数字化后被无限复制。

7. 预言机安全

- 预言机的最终目标是给区块链输送持续安全可靠的外部数据，因此保障预言机安全对维护区块链安全具有重大意义。去中心化是解决预言机安全问题的一种重要方法。中心化预言机往往面临着单点失败、数据泄露、数据被篡改等安全问题，将预言机进行离散化是保障预言机安全的重要举措。

- 去中心化包括外部数据源的去中心化和预言机节点的去中心化。预言机可以通过从多种渠道收集数据，来避免因单一数据源出错、停机或被黑客占领而导致的安全问题。预言机本身也需采取多节点汇总合约的方法，来防止部分预言机存在错误，从而得出更可靠的响应。除此之外，可以使用基于门限签名的分布式协议来防止节点“搭便车问题”的发生。

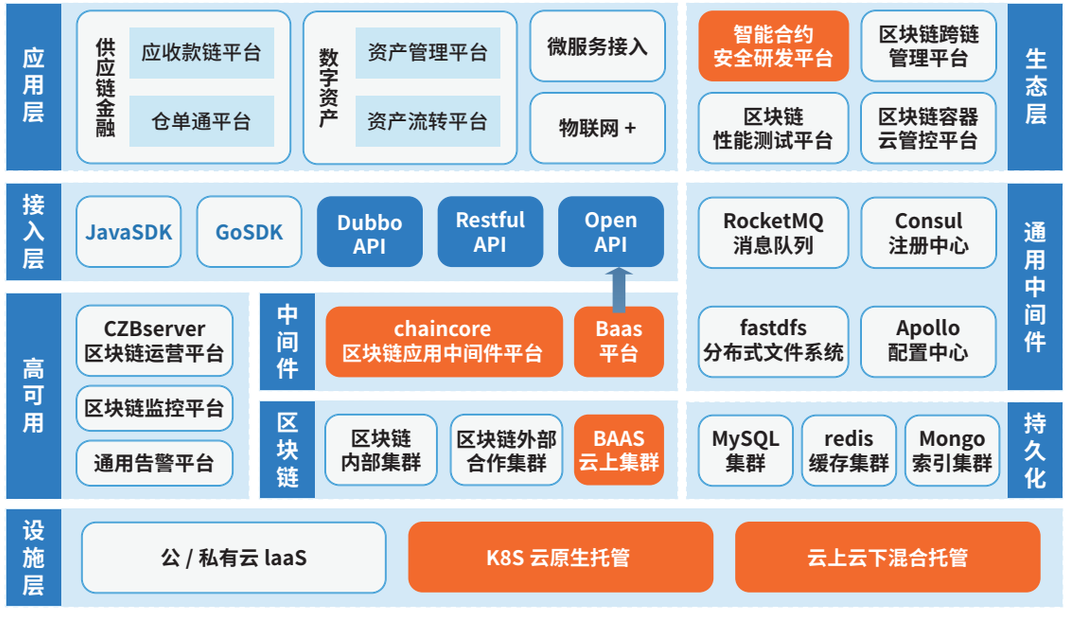
- 仅仅依靠去中心化的方式，还无法实现全面的预言机安全，为进一步提高可信度，还需要考虑更多其它的安全性措施。例如使用可信硬件为高质量的预言机提供信用背书；对源数据进行数字签名，防止恶意篡改，提升预言机抗干扰能力；对数据预留处理机制，对齐时间戳，保证数据合法可靠；监控预言机的行为，并统计其可用性与正确性，得出准确率与响应时间，并计算节点犯错成本，为节点做出声誉评判标准，来合理规划各节点的信息权重；形成举报机制，对揭发恶意节点的节点进行一定的奖励；对高价值交易的响应进行审计，形成验证机制、异常报警机制，拦截黑客对数据的恶意篡改，削弱套利空间；加强对预言机的针对性测试，提高预言机的抗攻击能力等。

三 区块链安全问题应对实践

- 浙商银行自 2017 年首先将区块链技术应用于银行核心业务以来，先后推出了区块链技术平台、区块链 BaaS 平台、区块链供应链金融服务等一系列区块链技术产品与应用服务，一直以来都面对着区块链技术与应用安全问题的挑战。在实际应用过程中，浙商银行通过在区块链技术平台安全性、可用性、可靠性研究中的持续投入，保障了浙商银行区块链相关应用的金融级高安全性。

- 浙商银行区块链技术平台是浙商银行自主研发的、符合金融特性的区块链基础设施，浙商银行区块链技术平台通过国密算法改造与共识协议创新保障了底层协议的高安全性，同时通过引入智能合约安全研发平台，在最大程度上杜绝了智能合约漏洞导致的安全问题。此外，平台还引入了分区管理、隐私交易、多级签名、弹性共识、合约权限管控、多城多园区区块链节点灾备机制等技术特性，应对了区块链平台可能面对的各方面技术与安全风险，保障了上层应用金融级的高可用性与高安全性。

- 基于区块链技术平台，浙商银行构建了一套完整的区块链架构，以云平台为基础计算设施，以数据库集群为存储资源，支持区块链节点集群以及 BaaS 平台与中间件平台，辅以运管平台、监控平台与告警平台保障区块链系统的易运维、事件可感知，通过消息队列等通用中间件提升区块链系统的可用性，区块链系统通过 API 或 SDK 与上层应用对接，最终加入跨链平台、智能合约安全研发平台、性能测试平台与容器云管控平台构造完整的区块链技术与应用生态。



4 chapter four 区块链安全展望

一 加强自主可控

- “自主可控”指关键技术依靠自身研发设计，全面掌握核心技术，实现信息系统从硬件到软件的自主研发、使用、升级、维护的全程可控，保障核心技术、关键步骤、重要硬件的国产化。自主可控是保障网络安全、信息安全的前提。当前国际环境日益复杂，不稳定性、不确定性明显增强，近几年来对我国或我国企业的技术封锁、商务制裁事件频发，不能实现自主可控就意味着大量信息系统将受制于他国，导致我国信息安全难以治理，无法对技术进行自由地使用、升级、维护，甚至可能存在将对信息安全产生重大威胁的恶意后门。反之，在技术自主可控的条件下，关键技术国产化使得我国信息安全整体在掌控之中，相关技术可以自由进行相关研发、使用、升级、维护，不再受制于人。

- 对于区块链技术而言，评估其是否自主可控的要求主要包含以下几点：

（1）知识产权自主可控

在当前的国际竞争格局下，知识产权自主可控格外重要，只有掌握了自主可控的区块链技术知识产权，才能保障区块链在数字经济、数字金融等关键领域的应用安全，建立全球性的竞争优势。当然，除了所有知识产权从研发开始便掌握在自己手中之外，买断国外区块链厂商的区块链知识产权

也是自主可控的一种方式，而只购买自主权不充分的国外区块链知识产权授权则不属于自主可控的范畴。

（2）技术能力自主可控

技术能力自主可控要求企业、机构拥有真正掌握区块链平台核心技术的科技队伍。自主可控离不开关键核心技术的研发、迭代与创新，拥有技术能力自主可控的科技团队才能够持续创新，持续攻坚核心关键技术；才能拥有区块链技术长期发展的能力，在大环境变化、技术发生变革时能够快速反应，进行针对性的改造创新。技术能力自主可控是打造国产自主可控的区块链技术发展模式、打造自主可控的区块链技术生态的前提。

（3）部署环境自主可控

部署环境自主可控要求区块链平台在国产软硬件环境中进行部署使用，要求区块链平台可以与国产芯片、国产服务器、国产云平台、国产操作系统、国产数据库等全套国产化体系全面适配。随着我国国产软硬件的高速发展，在实现部署环境自主可控制后，区块链技术可完成从研发、应用、软件到硬件的全栈国产化体系，构建完整的国产自主可控技术生态圈。

二 深化标准化建设

- 区块链已成为我国国家战略的重要组成部分，区块链安全也成为了网络安全、信息安全体系中重要的一环，相关顶层设计与标准化体系成为了保障区块链安全标准化发展的重中之重。

- 在顶层设计方面，《网络安全法》作为网络安全与信息安全领域的“根本大法”，同样也适用于区块链安全。在区块链安全标准化体系的建设方面，目前主要有中国人民银行于 2020 年 2 月 5 日发布的《金融分布式账本技术安全规范》(JR/T 0184 2020) 金融行业标准，并有《信息技术区块链和分布式记账技术存证应用指南》、《信息技术区块链和分布式记账技术智能合约实施规范》等国家标准正在制定中。2020 年 4 月 13 日，工业和信息化部发布了《全国区块链和分布式记账技术标准化技术委员会组建公示》，正式成立全国区块链和分布式记账技术标准化技术委员，并由该技术委员会承担起体系化推进区块链标准制定工作的具体任务。

- 2019 年 1 月 10 日，国家互联网信息办公室发布《区块链信息服务管理规定》，要求区块链信息服务提供者应当在其对外提供服务的互联网站、应用程序等显著位置标明其备案编号，并由国家互联网信息办公室依法依规组织开展备案审核工作。截止 2021 年 06 月 18 日，共有五批共 1238 个境内区块链信息服务通过备案，标志着我国已将区块链信息服务纳入到了规范化的监管体系中。

- 随着区块链的创新应用和深入发展，区块链安全的政策、标准、规则及机制等方面需要持续推进、加快制定，除了国家的顶层设计以及监管机构的规范化监管，区块链行业企业、科研机构也需要积极参与各项国家标准、行业标准、国际标准的制定，加快相关标准化体系的建设。

三 打造产业示范区块链基础设施

- 在建设数字中国的大背景下，建设数字经济、推动数字化改革已经成为了国家战略。区块链技术作为重要的数字化技术之一，在各产业数字化转型、数字化改革的过程中起到了非常重要的作用。因此，在各行业打造一批重点产业示范区块链基础设施项目显得格外重要，可以在标准化产业区块链应用规范的同时，简化产业链企业使用区块链、接入区块链基础设施的流程，迅速推进区块链在各行业的应用，同时以统一的接口规范、数据规范、智能合约规范、管理规范等保障产业链区块链的整体应用安全与技术安全，以区块链技术推动各行各业的产业链数字化升级，为经济社会全面数字化发展做出重要贡献。

- 在数字资产交易领域，以北京国际大数据交易所为例，利用区块链、隐私交易、联邦计算等技术推动数据要素高效流转、深度挖掘数据价值、探索数据交易新模式；在供应链金融领域，以上海票据交易所供应链票据平台为例，在区块链中签发供应链票据并在链上流转、融资，拓宽产业链企业融资渠道，同时与各类供应链金融平台对接，打造供应链金融领域标杆平台。同样的，在知识产权交易、碳交易、司法存证等领域，都可以推进打造产业垂直领域一体化区块链基础设施，引导区块链在各行业产业的应用方向。

四 加强多学科交叉融合

- 在新基建的大背景下，区块链技术作为信息基础设施，与物联网、云计算、大数据、人工智能、5G 等其他新兴技术的融合交叉将为各项技术的发展与应用提供广阔的空间，以区块链技术为信任基础设施，以物联网为数据采集工具，以云计算为硬件资源支撑，以 5G 为网络传输工具，以大数据、人工智能为判断决策大脑，各类技术的融合创新将激发技术发展的潜力，为进一步推出全国范围内安全可信的数字社会基础设施打下坚实的技术基础，推进数字经济与数字社会的发展。

- 同时，加强区块链技术与跨链技术、多方安全计算技术、联邦计算技术、可信硬件等扩展技术的结合应用，深化技术与实际业务场景的结合，持续探索区块链技术基础研究突破的可能性。