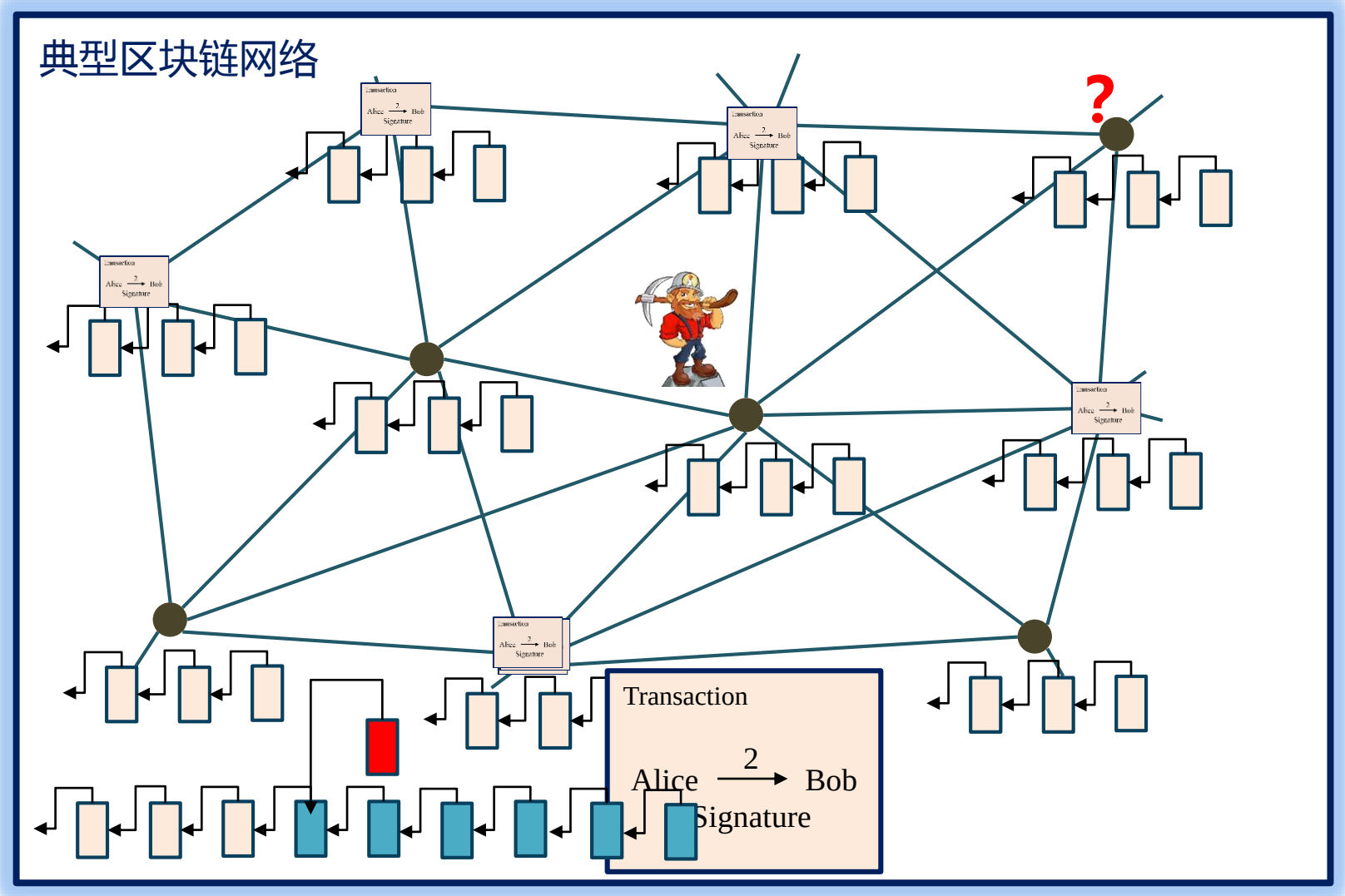
区块链安全与标准化

伍前红
北京航空航天大学
2018年10月28日

主要汇报内容

1. 区块链工作原理与概述
2. 国内外应用与政策现状
3. 区块链安全风险与挑战
4. 区块链的安全参考架构
5. 区块链安全的发展趋势

1.1区块链工作原理



比特币网络中每个节点均保存完整数据

交易地址为公钥，支付方使用私钥签名

交易单广播到网络中，但不一定所有节点收到

节点验证交易合法性：签名、余额

矿工计算Hash，获得挖矿奖励和交易费奖励

矿工将合法交易记录在新区块上，广播到网络

节点只接受最早生成到最长链且合法的区块

交易所在区块后生成6个新区块则认为支付成功

若全网算力51%以上诚实，则比特币安全稳定

1.2 区块链的定义

目前为止，区块链还没有一个统一的定义，不同的组织或者机构根据自己的理解与需求给出不同的定义。以下列出几个标准组织给出的定义。

美国国家标准技术研究所（NIST）：区块链是带加密签名交易的分布式数字账本，其中账本以块的形式组成。 在验证并进行共识决策之后，每个合法的块都以密码学方式链接到前一个块（使其防篡改）。随着新块的添加，旧块将变得难以修改。新块利用网络复制至账本，并使用已建立的规则自动解决冲突问题。

澳大利亚标准局：区块链是一个以公共和安全的方式记录和验证交易信息的数字平台。这种基于密码学的分布式解决方案能够重新定义交易和众多不同行业的信任基础，将消除交易对第三方“中间商”的需求。

中国工信部：一种在对等网络环境下，通过透明和可信规则，构建不可伪造、不可篡改和可追溯的块链式数据结构，实现和管理事务处理的模式。需注意的是，在本定义中事务处理包括但不限于可信数据产生、存取和使用。

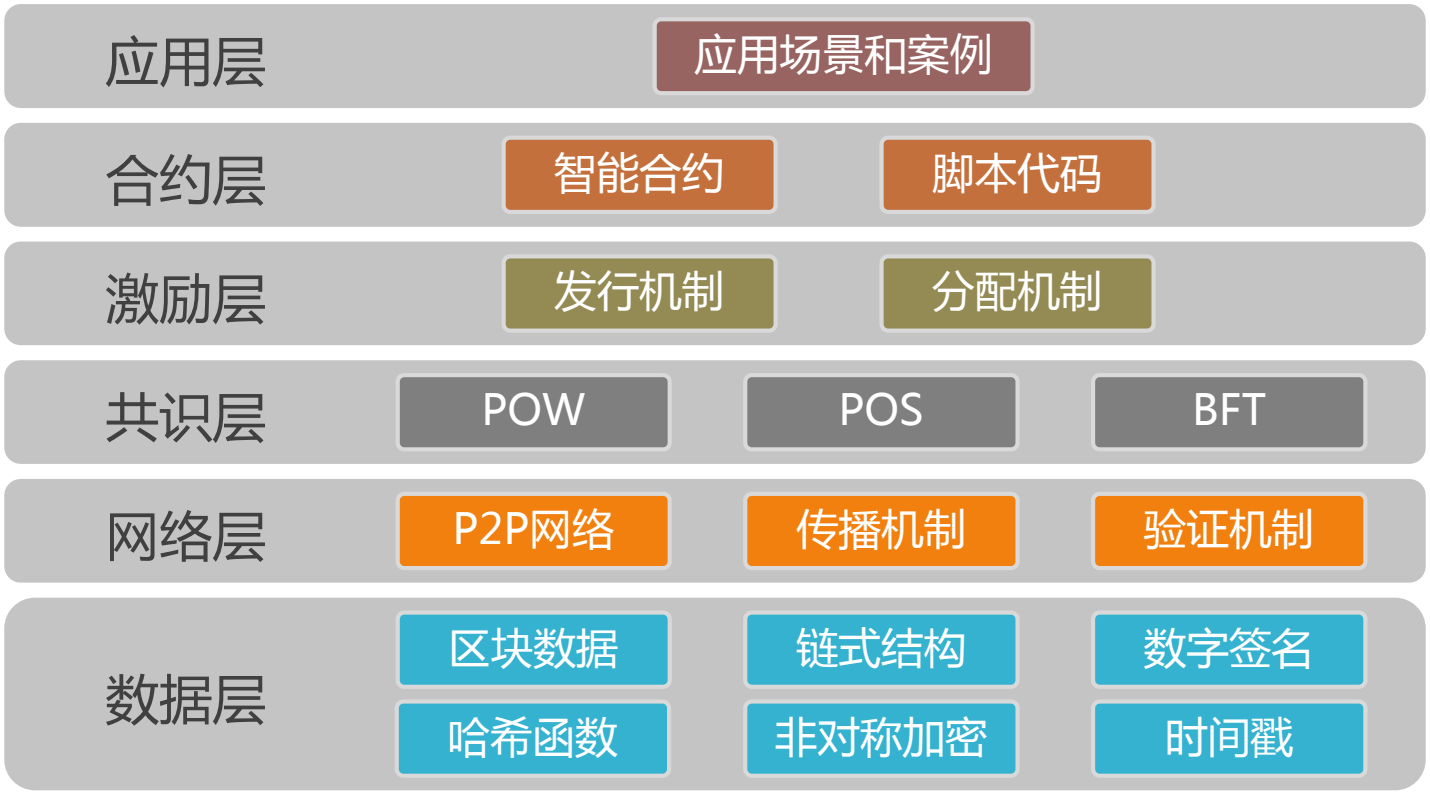
我们采用工信部给出的区块链定义。

1.3 区块链的技术特征

区块链技术作为一种分布式数据存储、点对点传输、共识机制、加密算法等技术的新型集成应用，具有去中心化、开放性、防篡改、匿名性、可追溯等特点。

1.4 区块链的体系架构

从最早应用区块链的比特币到引入智能合约的以太坊，再到应用广泛的联盟链Hyperledger Fabric，区块链经历了1.0时代，2.0时代和3.0时代。尽管具体实现上各有不同，但在整体体系架构上存在着诸多共性。区块链系统整体上可划分为成数据层、网络层、共识层、激励层、合约层和应用层六个层次。



1.4 区块链关键技术

根据区块链体系架构中自下到上的结构顺序，区块链关键技术主要包括底层网络技术、密码学算法、分布式账本、共识机制和智能合约。

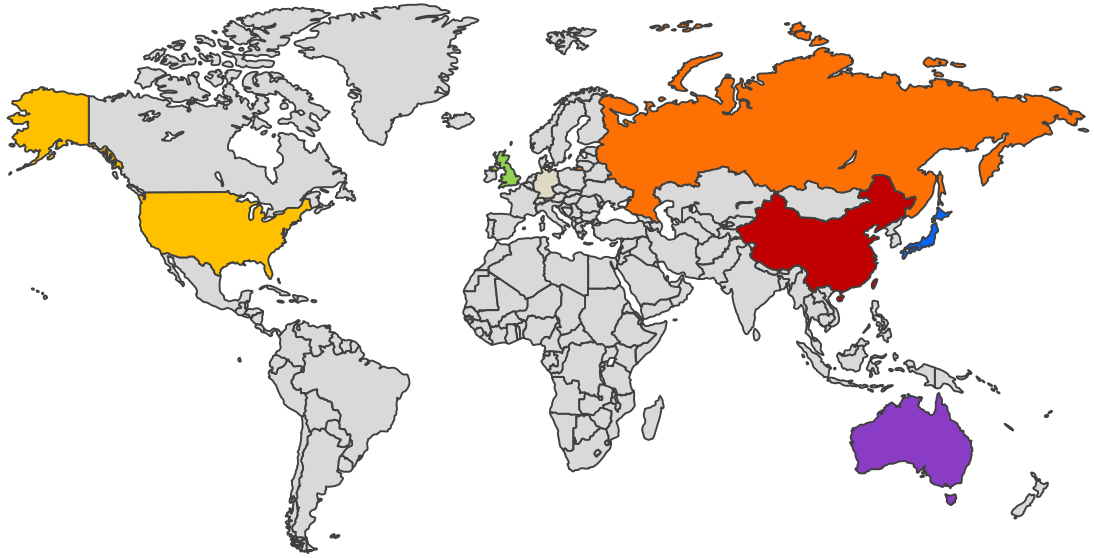
- 区块链底层网络技术：区块链底层网络技术包括P2P网络、网络路由和分布式存储。
- 区块链中的密码学算法：区块链中主要用到hash函数、数字签名、非对称加密等密码学算法。
- 分布式账本：区块链账本使用块链式数据结构、Merkle 树、有向循环图DAG等数据结构来形成数据记录格式，从而进一步形成数据块链。
- 共识机制：区块链主流的共识算法有：工作量证明（PoW）、权益证明（PoS）及委托权益证明（DPoS）、拜占庭共识（BFT、PBFT、SBFT、VBFT）等。
- 智能合约：是一种旨在以信息化方式传播、验证或执行合同的计算机协议。智能合约允许在没有第三方的情况下进行可信交易，这些交易可追踪且不可逆转。该概念于1994年由Nick Szabo首次提出，区块链的出现，赋予了智能合约可靠执行的环境。

主要汇报内容

1. 区块链工作原理与概述
2. 国内外应用与政策现状
3. 区块链安全风险与挑战
4. 区块链的安全参考架构
5. 区块链安全的发展趋势

2.1 区块链国内外政策现状

目前关于区块链及安全的政策，主要集中在数字货币的发行机制监管上，而对于区块链技术应用项目的政策目前多以宏观为主。



中国

- 2016年12月，《“十三五”国家信息化规划》首次纳入区块链技术
- 2017年5月，工信部发布中国首个区块链标准《区块链参考架构》
- 2017年10月，国务院提出要研究利用区块链等新兴技术建立基于供应链的信用评价机制
- 2018年5月，工信部发布《2018年中国区块链产业白皮书》
- 2018年10月，中央网信办发布《区块链信息服务管理规定（征求意见稿）》

美国

2016年，美国证券交易所批准在区块链上进行公司股票交易
2018年，美国指出：未注册的ICO违法，并否认曾批准和将批准ICO

俄罗斯

2017年，俄罗斯向普京提交《区块链技术发展路线图》

英国

2017年英国政府监管机构金融行为监管局（FCA）颁发电子货币许可证

日本

2018年，日本最大的银行宣布计划推出“超大规模”的区块链支付网络

澳大利亚

2017年，澳大利亚国家标准局发布了国际区观念标准开发路线图

2.1 区块链国内外政策现状

详细的国内外法律法规及政策汇总

附表： 国内外法律法规及政策汇总

B.1.1 中国大陆

时间	
2013 年 12 月 3 日	中国人民银行、监督管理委员会（银发[
2017 年 9 月 4 日	中国人民信息化、保险的公

B.1.2 中国香港

时间	
2017 年 9 月 5 日	香港证监的声明》
2018 年 3 月 20 日	香港政府切监察本
2018 年 3 月 20 日	香港金融拟商品的

B.1..3 中国澳门

时间	
2018 年 4 月 19 日	澳门金融

B.1.8 德国

时间	
2018 年	德国指导

B.1.9 澳大利亚

时间	
2018 年	澳大澳大(Aust 专项

B.1.10 美国

2018 年 7 月 2 日	菲律宾规将开

B.1.16 俄罗斯

时间	
2018 年 4 月 16 日	俄罗斯门槛设
2018 年 4 月 25 日	俄罗斯

B.1.17 英国

时间	
2018 年 3 月 16 日	Coinba 可证
2018 年 4 月 6 日	FCA 警
2018 年 5 月 26 日	英国金融市场行为监管局对 24 家涉及加密货币的企业开展调查
2018 年 7 月 4 日	英国金融行为管理局更新全球金融技术监管沙盒项目

根据英国媒体 CityWire 的报道，英国金融监管机构-英国金融行为管理局正在审查 24 家加密货币公司，并针对一些未经授权的企业获得进行调查，以确定他们是否需要经过英国金融行为管理局的授权，才能进行一些活动。

据英国金融行为管理局（FCA）公告消息，其宣布了最新进入全球金融技术监管沙盒的 29 个项目。29 个项目中主要包括通过智能合约来提高债务融资效率的 Capexmove 公司、基于区块链发行股票和数字货币的 Fineqia 公司、利用区块链搭建融资平台的 Globacap 公司等。

B.1.18 加拿大

时间	政策/指导建议名称	重点内容
2018 年 4 月 20 日	加拿大税务局警告数字货币用户 4 月 30 日前必须缴税	据 CBC 消息，根据加拿大税务法，税收法适用于数字货币交易，使用数字货币不会免除消费者的税收义务。会计师 McCann 说：“无论您的收益是什么，4 月 30 日前必须对其进行申报纳税。如今全世界的税务机关都知道加密货币在 2017 年获得巨额收益了。在加拿大，不进行税务申报的后果在加拿大是十分严重的。”
2018 年 6 月 7 日	加拿大证券监管机构 CSA：加拿大人使用加密资产交易平台进行投资时要谨慎	据 newswire 消息，加拿大证券监管机构 CSA 提醒当地民众在通过交易平台购买加密资产时要谨慎。尽管平台可能自称为“交易所”，但并不意味着它符合证券监管体系规定。CSA 明确表示：目前在加拿大没有得到官方认可的加密资产交易平台或被授权的市场或交易商而运作的相关机构。CSA 是加拿大各省和地区证券监管机构的理事会，负责协调和统一加拿大资本市场的监管。

B.1.19 法国

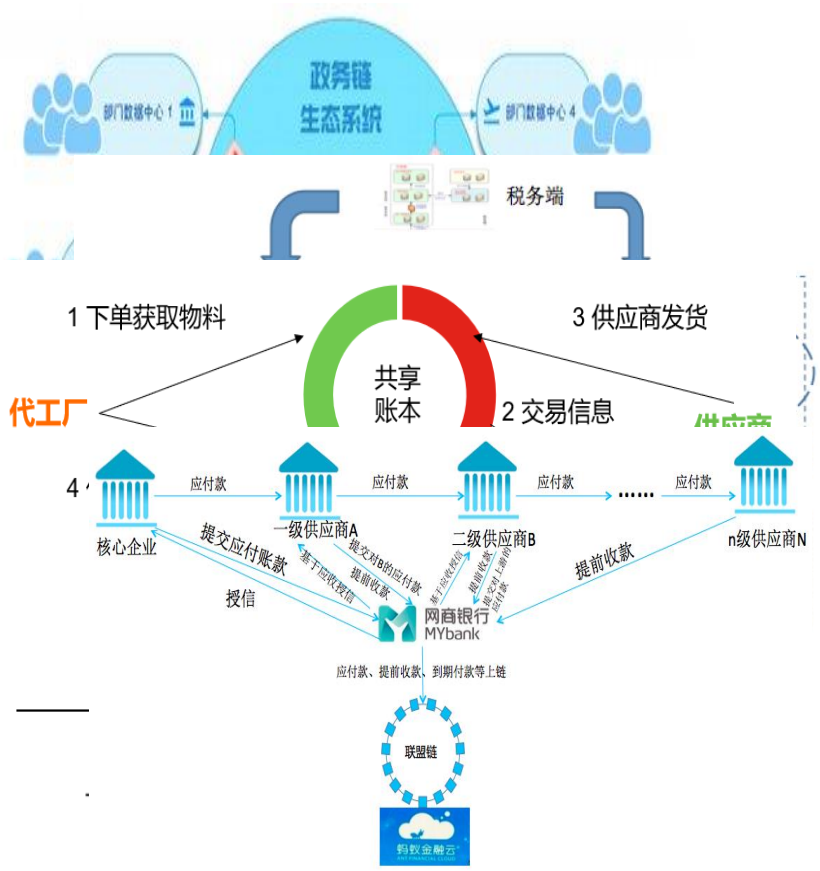
时间	政策/指导建议名称	重点内容
2018 年 3 月 16日	法国AMF将数家加密资产投资网站列入未授权网站清单	法国金融市场监管局（AMF）于周四宣布，它已将15个加密资产投资网站列入未授权网站清单。AMF宣称，任何在法国直接宣传可能有金融回报、或涉及中介的类似经济效益的各类资产投资都必须经AMF事先审批，如果没获得AMF注册登记号，不能在法国直接销售报价。

2.2 区块链应用典型案例

区块链在金融、电子政务、公共服务、食品药品监管追溯、供应链金融等领域已有典型应用

区块链
安全应用案例

- 基于区块链技术的数字票据平台
- 区块链电子政务服务平台
- “互联网+“的电子发票生态平台
- 基于区块链技术的药品追溯机制
- 基于区块链的交易业务供应链
- 基于区块链的供应链金融系统



2.3 区块链国内外应用现状

随着区块链技术发展逐步成熟，区块链应用已经从数字货币逐渐延伸到金融领域，并开始与实体经济产业深度融合。

国内区块链应用发展现状

金融领域	目前国内区块链在金融领域的应用探索主要集中在供应链金融、贸易金融、征信、交易清算、积分共享等场景。
实体经济产业	在政府公共管理与政务服务、物品追溯、交通物流等实体经济领域，也进行了针对区块链应用的探索与尝试。

国外区块链应用发展现状

金融领域	目前国外区块链在金融领域的应用主要集中在数字货币、交易与清算、证券交易等场景。
实体经济产业	在实体领域的应用主要集中在能源、保险、物流、公共事务、医疗卫生以及娱乐等方面。

2.3 区块链国内外应用发展存在的问题

技术局限性

主要表现是性能效率问题。系统吞吐量相对较低，数据处理和存储能力取决于单节点能力，尚难以支撑高频、高数据业务应用

面临安全挑战

由于设计、实现或实施方面的缺陷，区块链系统同样会面临外部或者内部的攻击风险

业务模式改变困难

对于长期习惯于中心化信息处理模式的各界而言，接受区块链这一去中心化的信息技术解决方案，需要一个不断了解与理念转变的过程。区块链的大规模落地与应用，需要大量应用实例，尤其是成熟实例的验证与支持

相关政策法规缺失

目前国内外还没有出台一份完整的标准化规则或者政策来管理监督区块链的使用，区块链标准的研制工作都还刚刚起步

主要汇报内容

1. 区块链工作原理与概述
2. 国内外应用与政策现状
3. 区块链安全风险与挑战
4. 区块链的安全参考架构
5. 区块链安全的发展趋势

3.1 区块链应用的安全现状

区块链作为分布式数据存储、点对点传输、共识机制、密码算法等技术的集成，近年来成为许多国际组织及国家政府的研究热点，其应用已延伸到数字资产交易、征信服务以及供应链溯源等多个领域，但同时也面临着更严峻的安全威胁、风险和挑战。

1. 区块链系统的安全威胁

- 共识机制威胁—51%攻击等
- 密钥安全威胁
- 面临外部或内部的攻击威胁：DoS攻击、女巫攻击、长程攻击等

2. 区块链系统的安全风险

- 设计、实现或实施存在的数据一致性风险：分叉攻击、长链攻击等
- 算法安全、协议安全、使用安全和系统安全等方面的安全漏铜
- 区块链资产或价值的被盗、遗失风险

3. 区块链应用的安全挑战

- 区块链中数据的安全和用户的隐私保护
- 智能合约的安全执行成为一个具有挑战性的问题
- 在金融服务、物联网、基础设施等领域的应用能够实现审计与监管

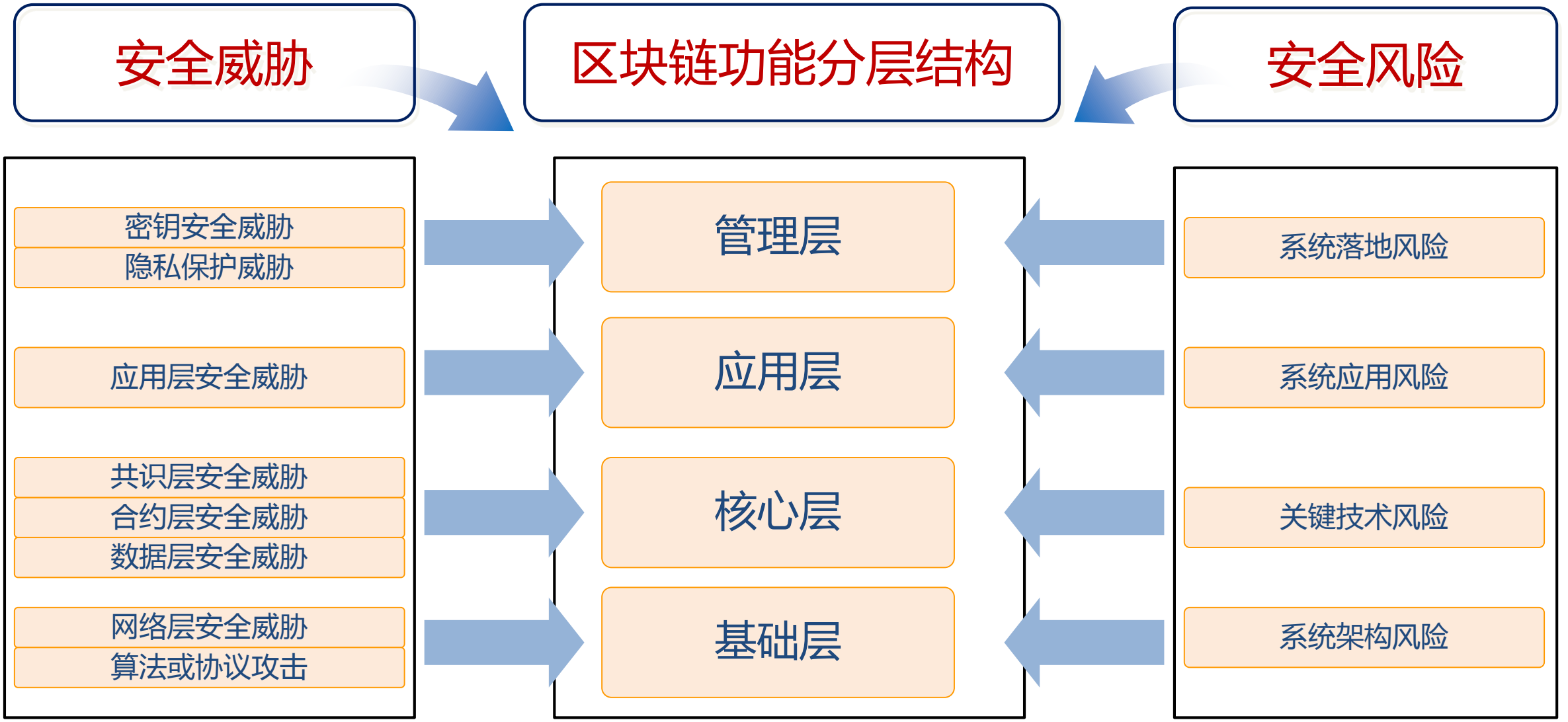
Coin-check新经币被盗

日本交易所Coincheck5.3亿美元数字货币失窃，成为史上最大数字货币被盗案

The DAO事件

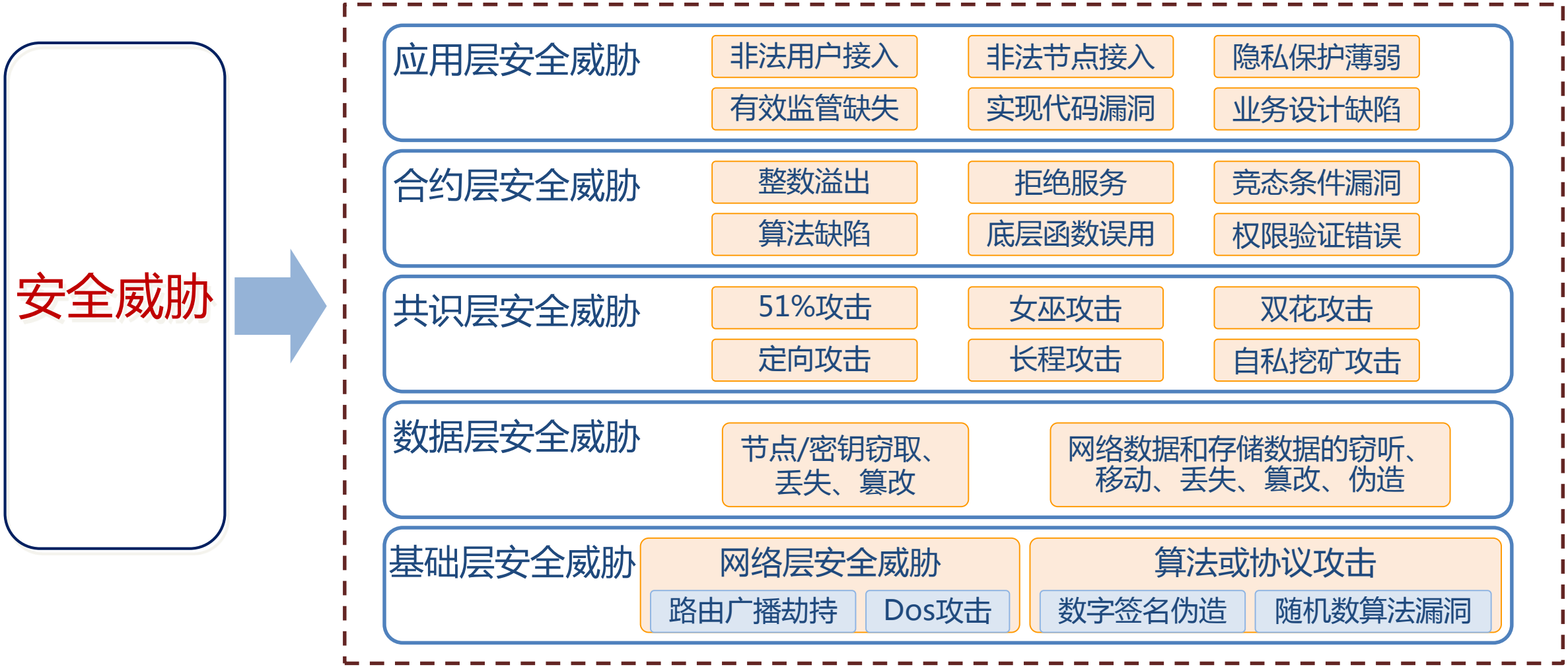
智能合约最大众筹项目The DAO受到攻击，损失超过6000万美元以太币

3.2 区块链面临的威胁与风险



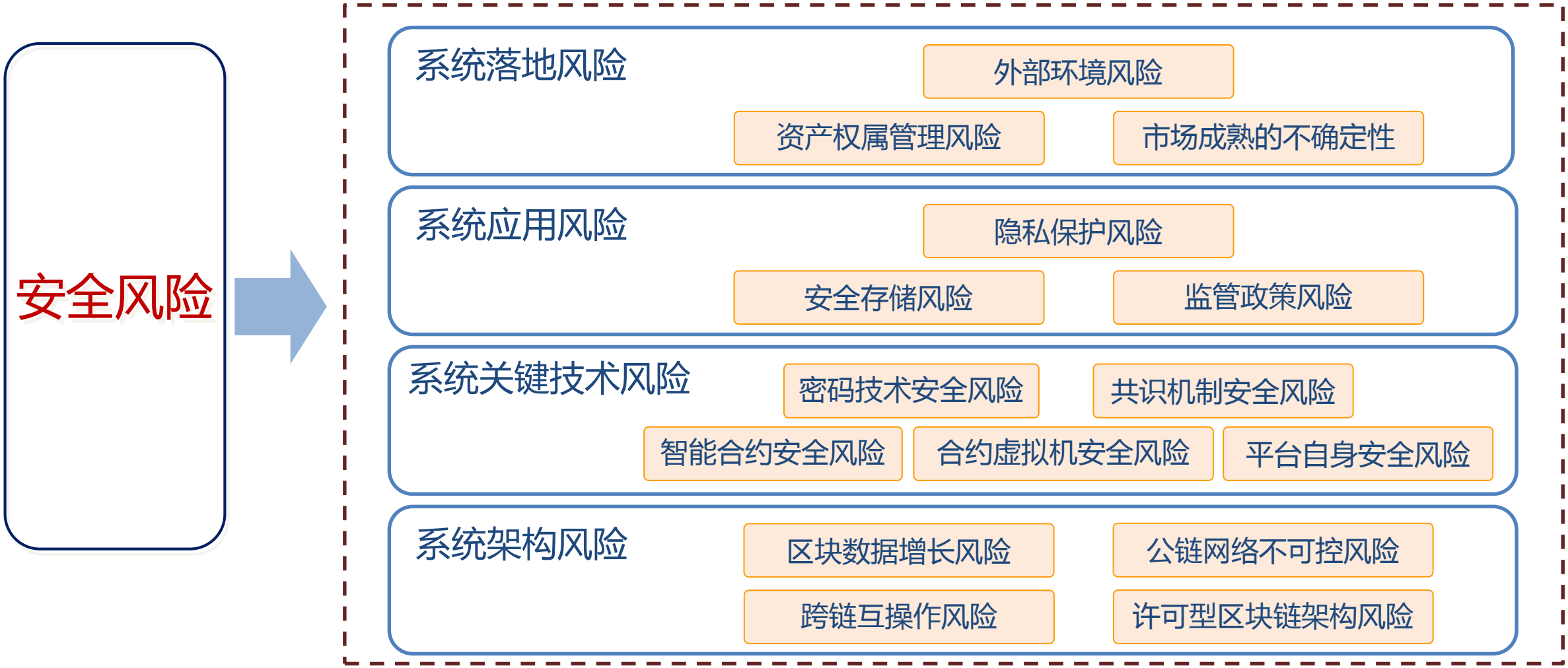
3.3 区块链面临的威胁与风险

具体的安全威胁内容：



3.3 区块链面临的威胁与风险

具体的安全风险内容：



3.4 区块链主要安全需求

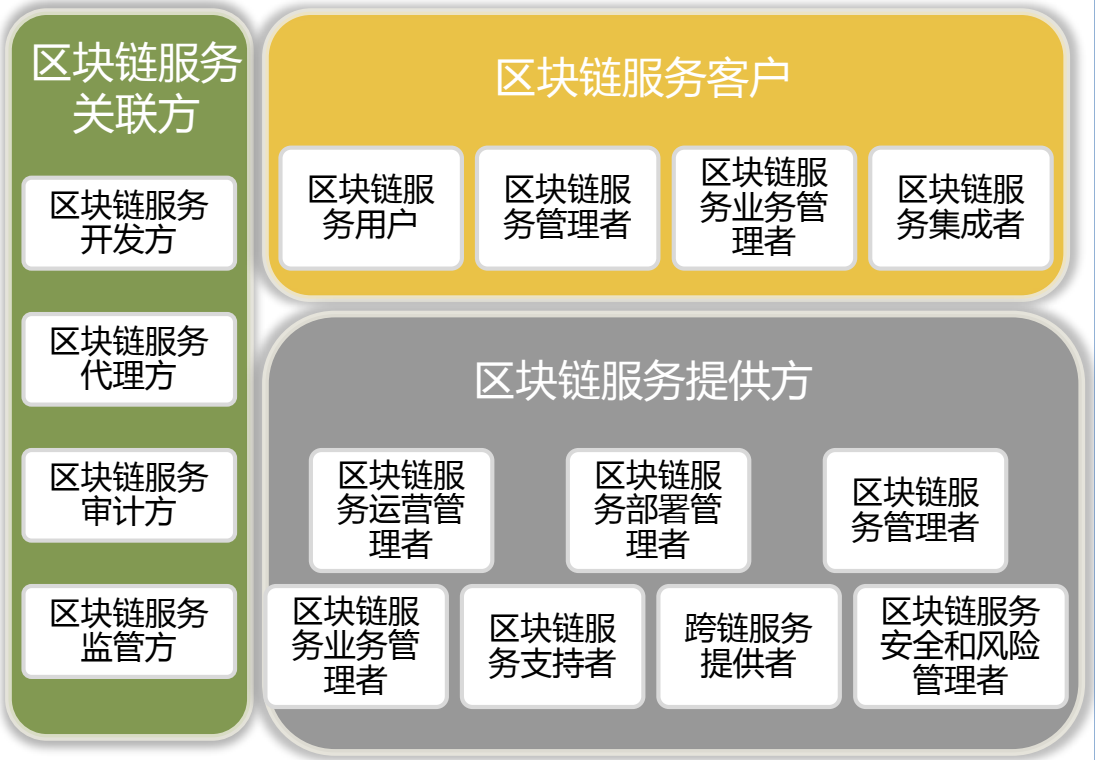
主要汇报内容

1. 区块链工作原理与概述
2. 国内外应用与政策现状
3. 区块链安全风险与挑战
4. 区块链的安全参考架构
5. 区块链安全的发展趋势

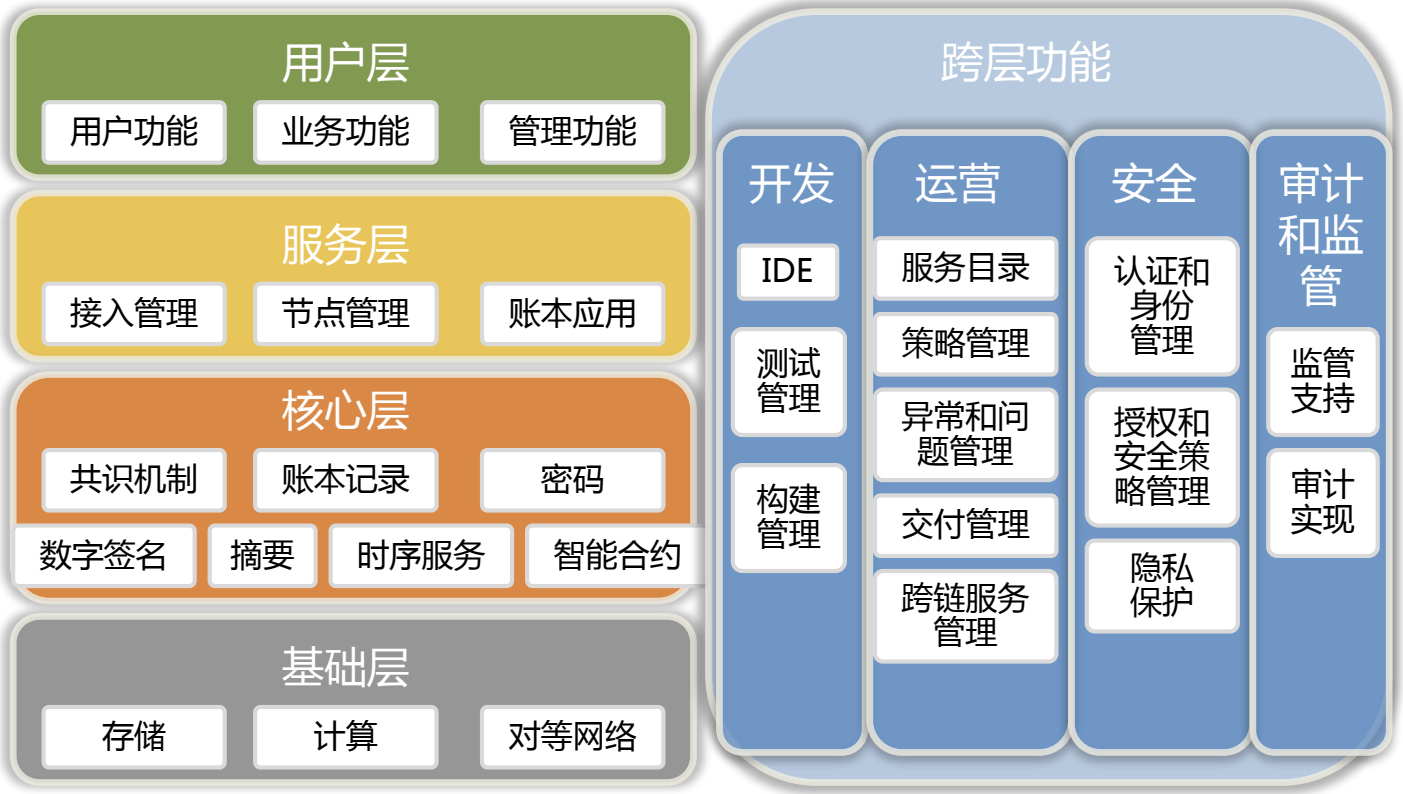
4.1 区块链 参考架构

目前，区块链还没有标准的体系架构。对于区块链系统，广泛统一认知的是工信部《区块链 参考架构》标准中规定的区块链架构，具体分为用户视图的区块链参考架构和功能视图的区块链参考架构。

1. 用户视图的区块链参考架构

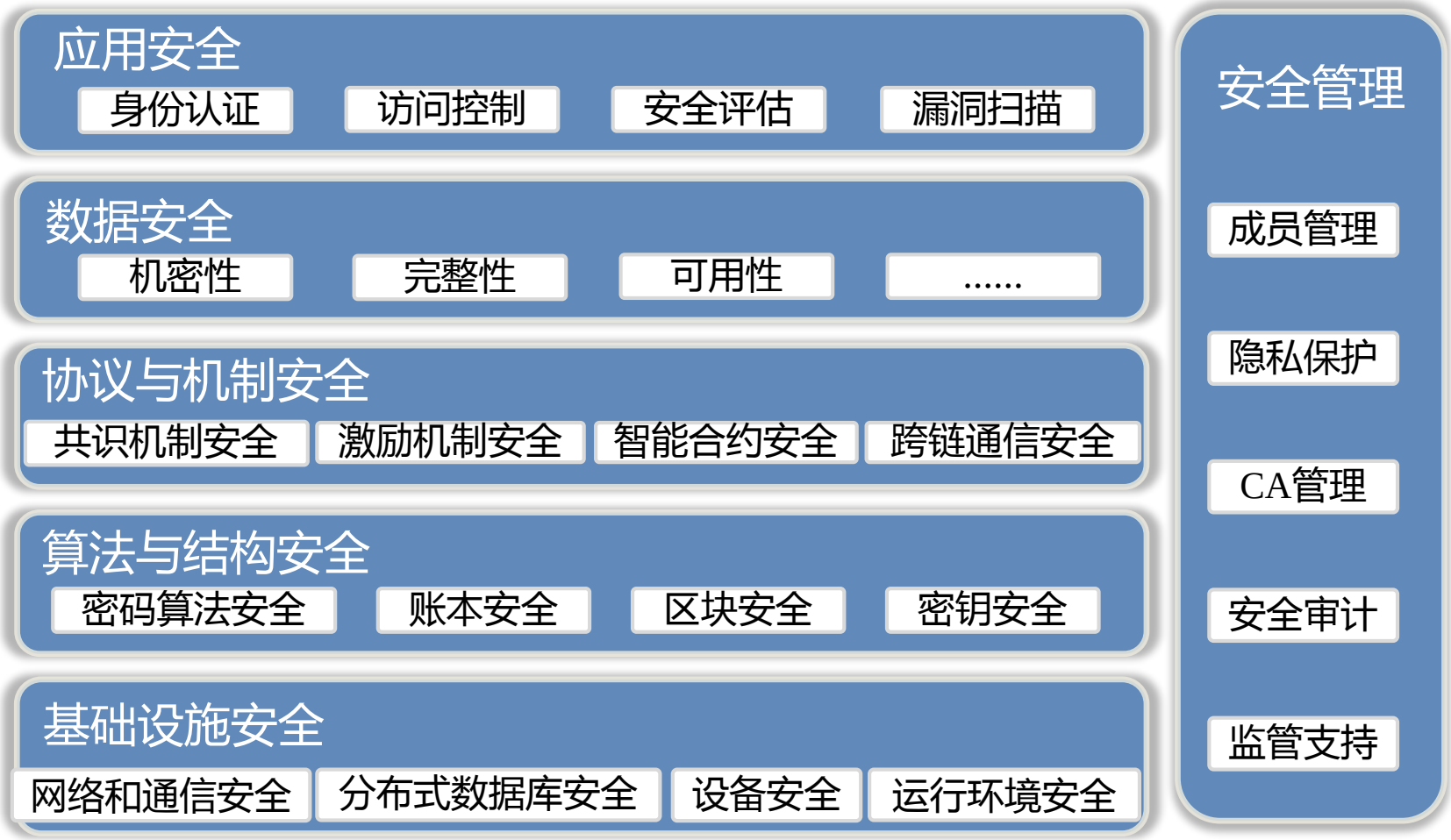


2. 功能视图的区块链参考架构

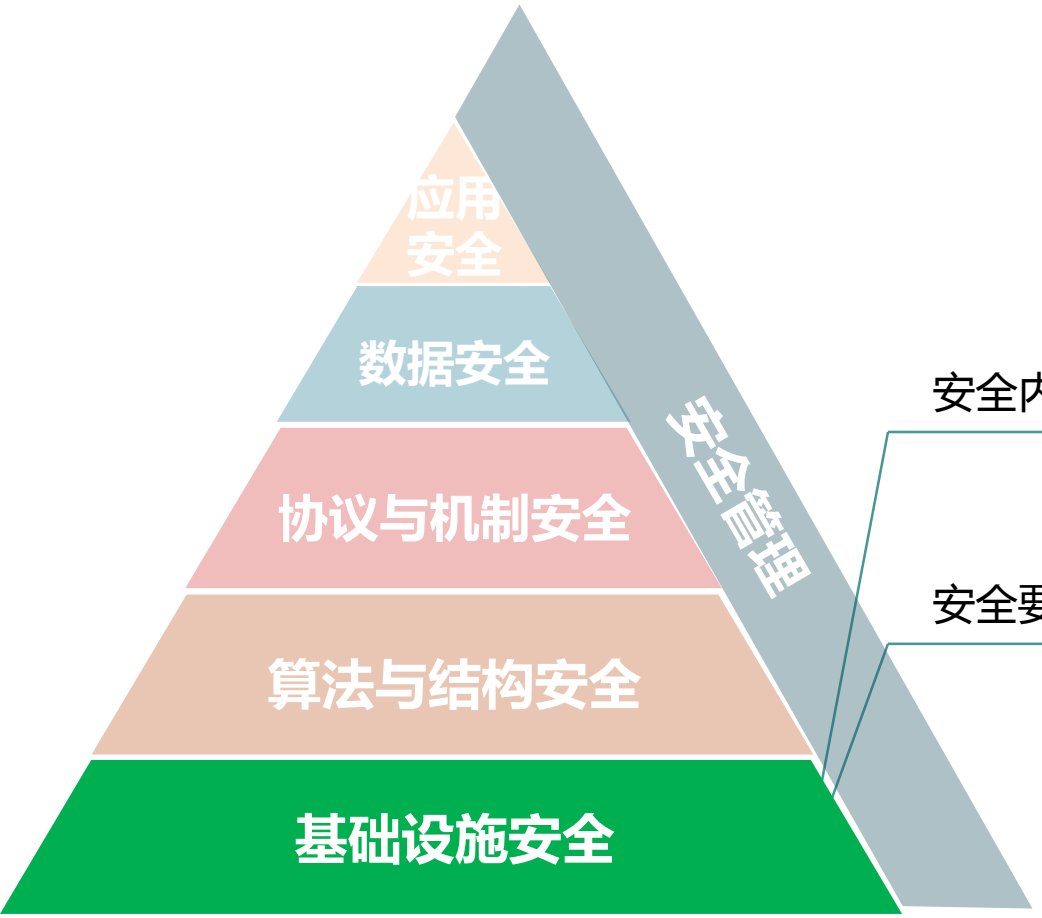


4.2 区块链安全参考架构

在工信部提出的区块链标准《区块链 参考架构》基础上，结合区块链面临的安全威胁、风险与区块链安全需求，提出区块链安全参考架构。



4.3 区块链信息基础设施安全分析



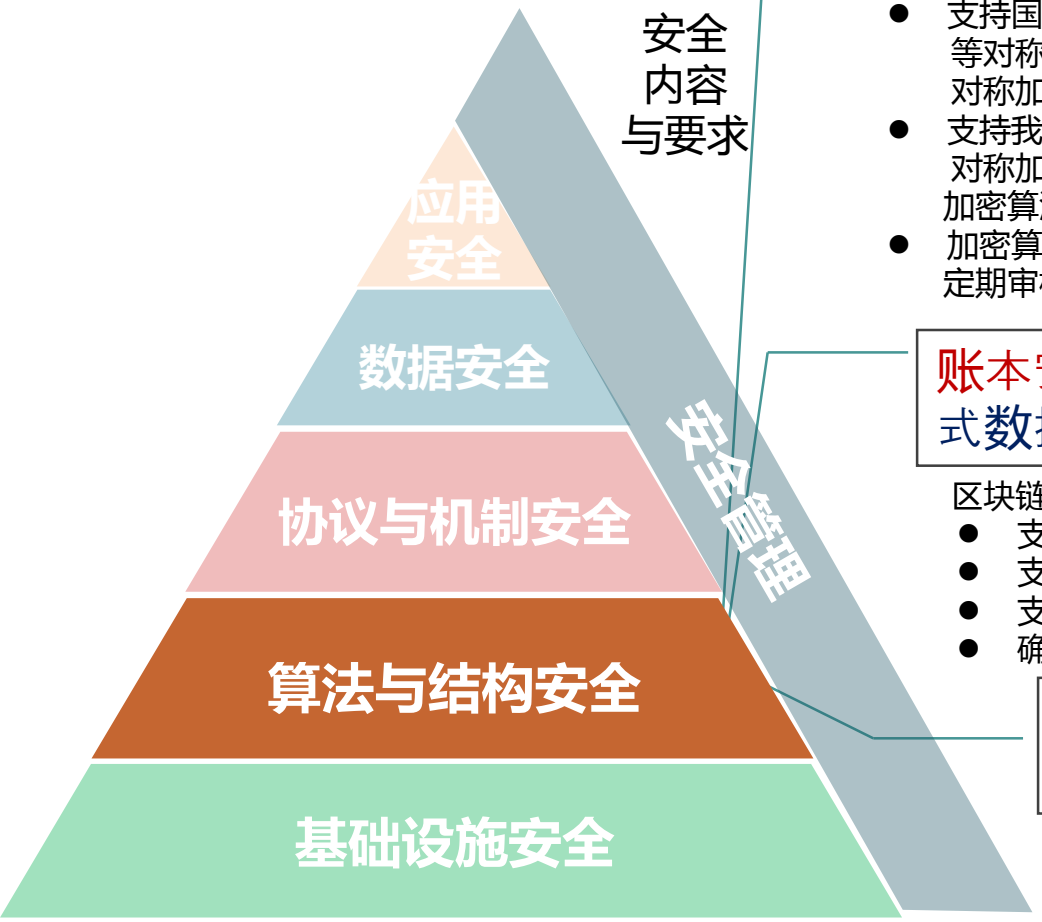
安全内容

基础设施安全包括网络和通信安全、分布式数据库安全、设备安全和运行环境安全。

安全要求

其安全标准对应并达到：
GB/T20270-2006的《信息安全技术 网络基础安全技术要求》、
GB/T20271-2006的《信息安全技术 信息系统通用安全技术要求》、
GB/T20272-2006的《信息安全技术 操作系统安全技术要求》、
GB/T20273-2006的《信息安全技术 数据库管理系统安全技术要求》、
GB/T22240-2008的《信息安全技术 信息系统安全等级保护实施指南》

4.4 区块链数据结构与算法安全分析



密码算法安全：主要涉及加密、签名、哈希函数、密码协议的使用安全

加密宜具备以下安全功能：
- 支持国际主流加密算法，如 AES256 等对称加密算法和 RSA、ECC 等非对称加密算法；
- 支持我国商密算法，如 SM4、SM7 等对称加密算法和 SM2、SM9等非对称加密算法；
- 加密算法应具备抵御破解的能力，宜定期审核加密算法的安全性

签名宜具备以下安全功能：
- 支持国际主流的数字签名算法，如 RSA、ECC 等；
- 支持我国商密的数字签名算法，如 SM2 等；
- 数字签名算法应具备抵御破解的能力，宜定期审核数字签名算法中使用

哈希函数宜具备以下安全功能：
- 支持国际主流散列算法，如 SHA256等；
- 支持我国商密算法，如SM3等；
- 散列算法应具备抵御破解的能力，宜定期审核散列算法的安全性，必要时采用更高破解计算复杂性的散列算法。

账本安全：账本是区块链中分布式数据的存储介质

区块链账本的使用宜具备以下安全功能：
- 支持持久化存储账本记录；
- 支持多节点拥有完整的数据记录；
- 支持向获得授权者提供真实的数据记录；
- 确保有相同账本记录的各节点的数据一致性。

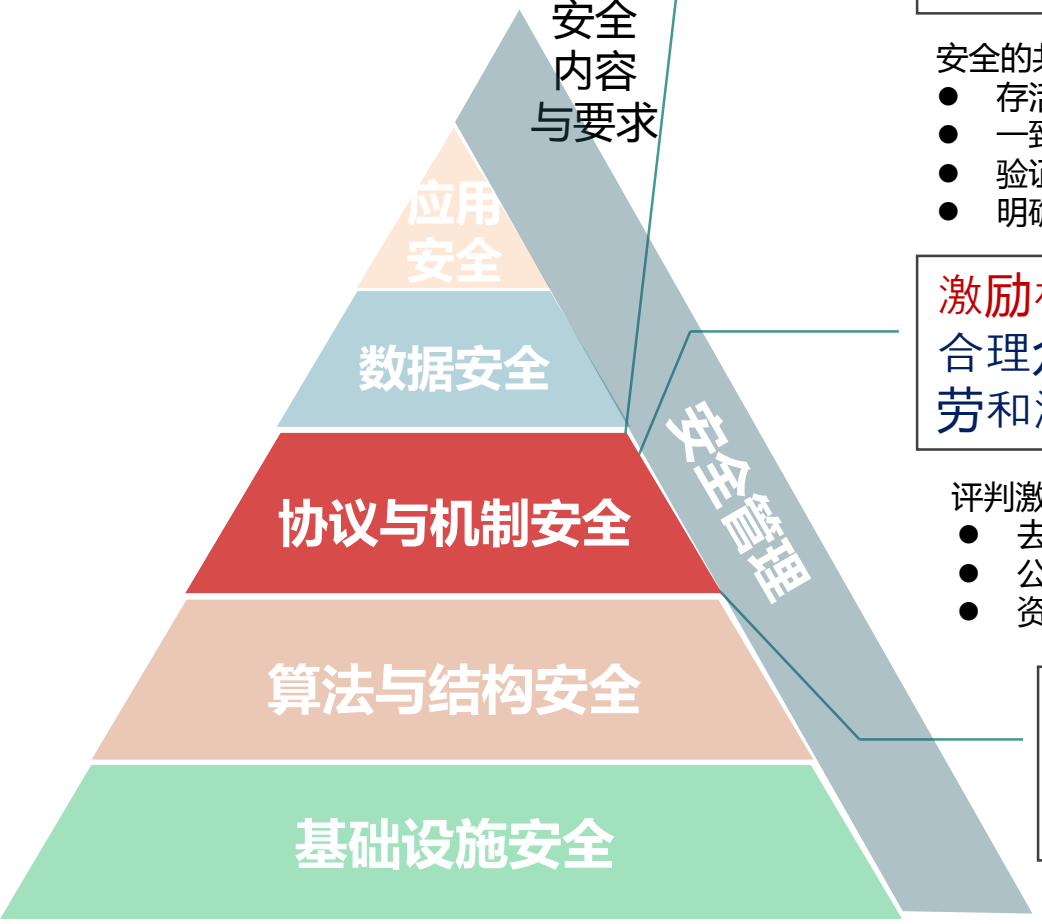
区块安全：区块是区块链的基础单元

区块链中的区块宜具备以下安全功能：
- 通过健壮的激励机制形成区块；
- 防止矿池合谋的51%攻击；
- 区块的设计需在提高效率的同时考虑安全。

密钥安全：区块链私钥的安全，需要综合签名算法、随机数选择、关键信息保护、密钥生命周期安全等各方面给出要求建议

密钥的使用宜具备以下安全功能：
● 密钥生成和导入；● 密钥存储；● 密钥导出/分发/交换；● 密钥更新 ● 密钥清除

4.5 区块链协议与机制安全



共识机制安全：共识算法是区块链体系的核心，共识机制安全需求随应用场景的需求而变化

安全的共识机制需具备如下特点：

- 存活性：来自于正确运行节点的请求最终能够被系统接收并处理；
- 一致性：诚实的节点会对相同的请求做出明确且一致的判断；
- 验证的概然性与统一性：验证规则必须满足概然性与统一性，保证每一参与节点的独立判断能力
- 明确的应用范围：共识方案的发布需伴随清晰的应用场景和规模参数

激励机制安全：设计激励相容的合理众包机制，作为参与者的酬劳和激励

评判激励机制的标准可以有以下几个维度：

- 去中心性；
- 公平性；
- 资源投入成本。

跨链通信安全：跨链通信把区块链从分散的孤岛中拯救出来，是区块链向外拓展和连接的桥梁

跨链技术的实施需具备如下安全特点：

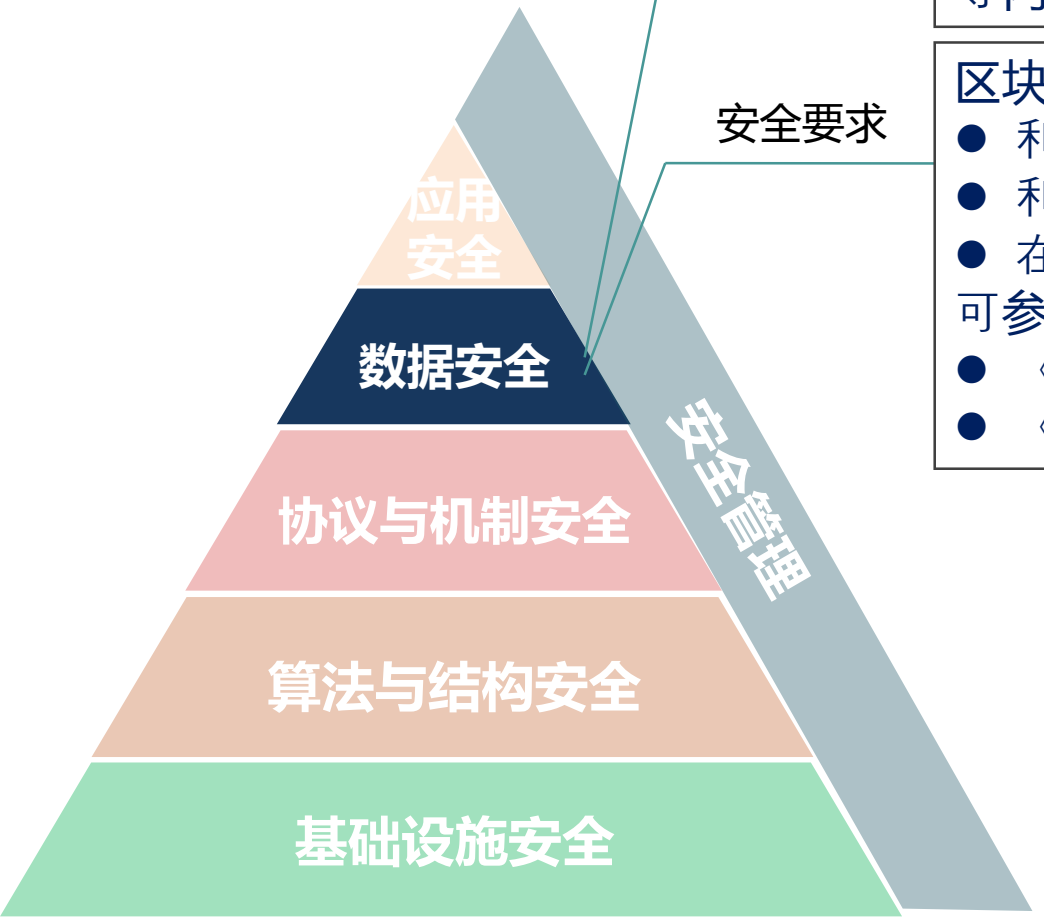
- 保持分布式网络里节点之间连接状态的强健性；
- 抵御跨链之间发起的DoS攻击；
- 防止母链出现分叉；
- 解决网络拓扑结构中链与链连接处的安全问题。

智能合约安全：主要由智能合约来实现区块链核心业务逻辑

评判智能合约的安全可以有以下几个维度：

- 代码安全；
- 运行机制安全；
- 业务逻辑安全；
- 用户使用安全。

4.6 区块链数据安全



安全内容

区块链上的数据安全包括数据完整性、数据机密性和数据访问控制等内容。

安全要求

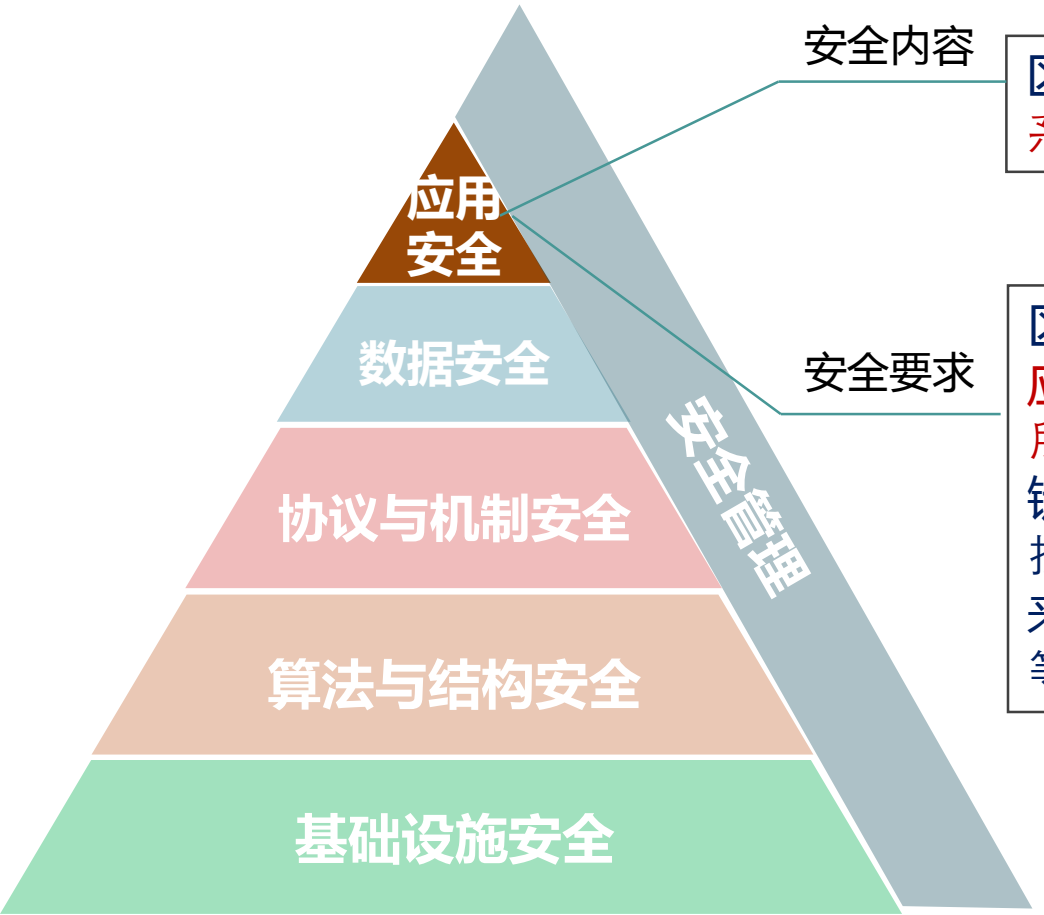
区块链的数据安全应用总结为以下方面：

- 利用高冗余的数据库保障信息的数据完整性
- 利用密码学的相关原理进行数据验证，保证不可篡改
- 在权限管理方面运用多私钥规则进行访问权限控制

可参考正在制定的相关密码标准：

- 《信息安全技术 大数据安全管理指南》
- 《信息安全技术 个人信息安全规范》

4.7 区块链应用安全



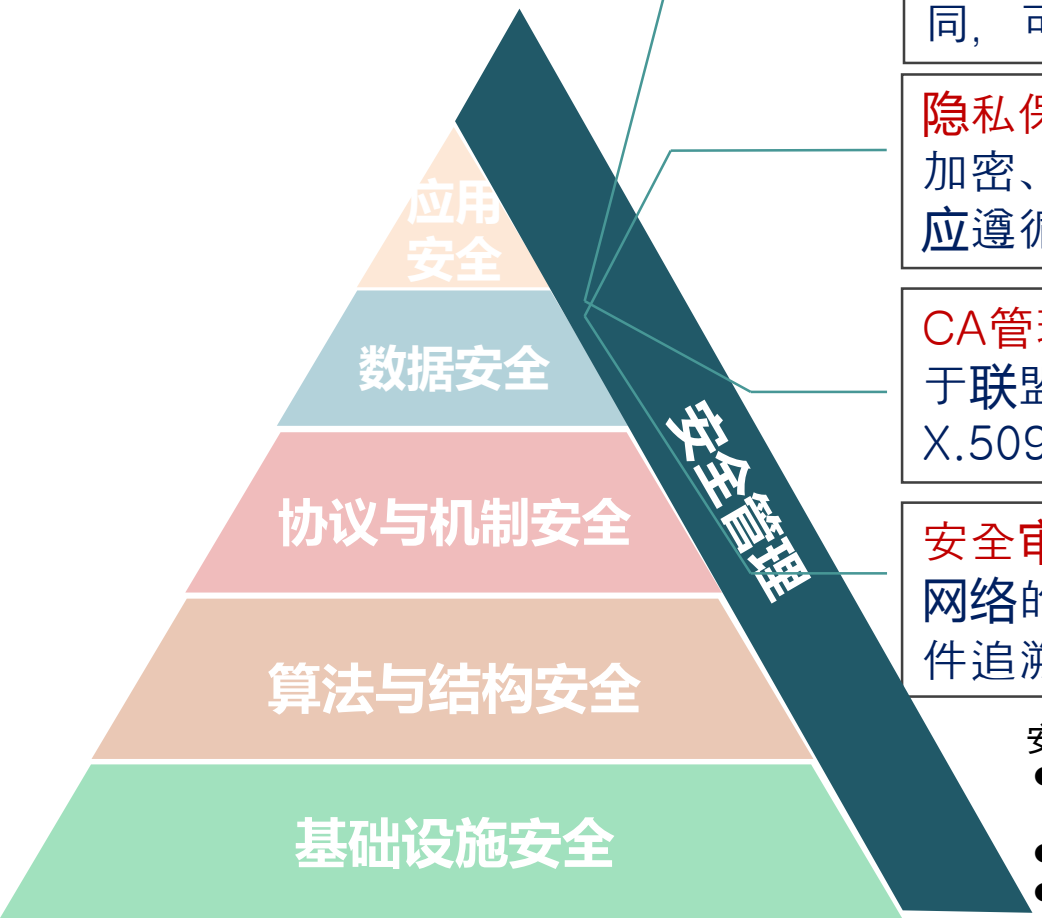
安全内容

区块链的应用安全可以进一步细分为身份认证安全、访问控制安全、系统安全评估和系统漏洞扫描。

安全要求

区块链应用也是一种信息系统，与传统信息系统不同的是，区块链应用系统由不同的节点组成，不同的节点隶属于不同的机构来运维，所有应用数据承载于这种分布式结构的区块链系统之上。因此区块链应用系统在建设时也需要根据区块链应用上所承载的应用数据，按照《GB 17859-1999 计算机信息系统安全保护等级划分准则》来确定区块链应用的安全等级。同时，需要根据区块链应用的安全等级来建设区块链运维系统。

4.8 区块链安全管理



安全内容与要求

成员管理：成员管理主要指成员的身份管理，通常使用一次一签、数字证书、匿名证书、群签名等方式来完成不同场景下的身份管理。根据应用环境的不同，可以选取合适的身份管理机制。

隐私保护：区块链隐私保护机制主要包括：账本隔离、链外存储、账本数据加密、身份混淆、同态加密、安全多方计算等。在选择使用各类安全技术时，应遵循“大胆尝试，谨慎评估”的原则，对其安全性作充分的分析和测试。

CA管理：数字证书目前主要应用于联盟链场景。数字证书应符合X.509标准，支持国密算法。

CA管理的实施需具备如下安全功能：

- 用户注册和权限配置；
- 证书申请、产生、更新、注销、查询统计；
- 系统配置管理；
- 接口层。

安全审计：主要用于实现区块链网络的审计内控、责任鉴定和事件追溯

安全审计的具体要求包括：

- 对区块链活动的事前、事中、事后三个阶段进行审计；
- 实现区块链网络与其他系统的对接与交互；
- 保存与审计活动相关的数据和证据。

监管支持：主要用于对区块链服务的环境、系统、可用性、系统运维、所支持业务的合规性监管

安全监管的具体要求包括：

- 仅监管者可以查看链上所有用户的交易信息和跟踪用户状态；
- 提供监管者密钥的安全保存机制，防止密钥泄露导致链上信息泄露；

主要汇报内容

1. 区块链工作原理与概述
2. 国内外应用与政策现状
3. 区块链安全风险与挑战
4. 区块链的安全参考架构
5. 区块链安全的发展趋势

5.1 区块链安全国外标准化趋势

ITU：国际电联电信标准化部门 (ITU-T) 在区块链议题上表现活跃，参与方众多，研究范围较广，有专门组织方式，推进路线明确。截至目前，ITU-T成立三个焦点组、一个问题小组和多个项目，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。

IEEE：电气与电子工程师协会（ IEEE ）目前已启动供应链技术与实施、区块链在物联网领域的应用框架、基于电力基础设施的传导式能源系统的互操作性指南等项目，并正在筹备IEEE 分布式账本技术在农业领域的应用框架、区块链数据格式规范等项目。

W3C、GSMA、IRTF/IETF：万维网联盟（W3C）、GSM协会（GSMA）与互联网架构委员会IAB下属的IRTF/IETF也分别成立区块链社区组并开展区块链标准的研究工作。

5.1 区块链安全国外标准化趋势

ISO：国际标准化组织（ISO）正在制定8项关键区块链标准。2017年下半年以来，ISO/TC 307加快推动基础类、智能合约、安全隐私、身份认证、互操作等方向的重点标准研制工作。目前，术语和概念、参考架构、分类和本体等8项国际标准已完成立项，进入研制阶段。

序号	英文名称	中文名称
1	ISO/AWI 22739 Blockchain and distributed ledger technologies–Terminology and concepts	区块链和分布式记账技术——术语和概念
2	ISO/NP TR 23244 Blockchain and distributed ledger technologies — Overview of privacy and personally identifiable information (PII) protection	区块链和分布式记账技术——隐私和个人可识别信息(PII)保护概述
3	ISO/NP TR 23245 Blockchain and distributed ledger technologies — Security risks and vulnerabilities	区块链和分布式记账技术——安全风险和漏洞
4	ISO/NP TR 23246 Blockchain and distributed ledger technologies — Overview of identity	区块链和分布式记账技术——身份概览
5	ISO/AWI 23257 Blockchain and distributed ledger technologies — Reference architecture	区块链和分布式记账技术——参考架构
6	ISO/AWI TS 23258 Blockchain and distributed ledger technologies — Taxonomy and Ontology	区块链和分布式记账技术——分类和本体
7	ISO/AWI TS 23259 Blockchain and distributed ledger technologies — Legally binding smart contracts	区块链和分布式记账技术——合规性智能合约
8	ISO/NP TR Blockchain and distributed ledger technologies — Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems	区块链和分布式记账技术——区块链和分布式记账技术系统中智能合约的交互概述

5.2 区块链安全国内标准化趋势

工信部：2016年10月，工信部发布《中国区块链技术和应用发展白皮书》，
2017年5月，中国区块链技术和产业发展论坛发布国内首个区块链标准《区块链 参考架构》标准，
2018年1月，中国区块链技术和产业发展论坛发布《区块链 数据格式规范》标准。

全国信息安全标准化技术委员会：全国信息安全标准化技术委员会大数据安全标准特别工作组将进一步开展区块链安全风险、区块链安全体系框架、区块链安全管理等相关标准化研究。

CCSA：中国通信标准化协会（CCSA）已陆续开展区块链相关课题的研究，TC1正开展“区块链技术研究”研究项目、“区块链总体技术要求”、“区块链通用测评指标和测试方法”标准项目、TC11开展了“基于区块链技术的数据处理平台”研究项目，TC8开展了“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”标准项目，“基于区块链技术的PKI系统研究”研究项目。

团体标准：中国区块链技术和产业发展论坛、数据中心联盟可信区块链工作组与中国区块链生态联盟等组织分别设立标准工作组，积极开展区块链和分布式记账技术领域的标准化工作。

5.3 区块链安全标准化一点思考

区块链安全标准化需求分析

目前，国内外标准化组织的区块链研究处于起步阶段，基于区块链的整体架构已经初步成型，但在区块链安全方面，还缺乏系统性的安全模型指导，为保证区块链应用的落地，促进区块链的健康发展，推动其大规模推广和应用，十分有必要开展区块链安全体系架构的标准化工作。

区块链安全标准化建议

在区块链安全参考架构基础上，结合现有基础设施技术标准，可以进一步研究《区块链通信安全标准》、《区块链的共识机制标准》、《区块链密码技术应用指南》、《区块链的账本存储安全标准》、《区块链的智能合约标准》、《区块链的账本结构标准》等多项标准来对区块链的发展进行安全规划。同时，需要分析已有基础设施标准是否适用于区块链技术规范。

敬请批评指正

谢 谢！