topnetwork现阶段，虽然区块链的行业生态已初步成形，但区块链技术仍面临诸多技术瓶颈，具体表现在体系架构、共识机制、互操作性、系统安全等多个方面。因此，必须对区块链关键技术给予高度重视，并集多方力量突破技术瓶颈，从而为区块链应用的全方面落地扫清障碍。2.1共识机制共识机制是区块链系统能够稳定、可靠运行的核心关键技术。不同于传统的中心化系统，区块链系统中所有网络节点是自由参与、自主维护的，不存在一个可信的中心节点承担网络维护、数据存储等任务。因此，如何使众多地理位置分散、信任关系薄弱的区块链节点维持一致性的可信数据副本，并实现系统稳定运行，是区块链共识机制必须解决的难题。共识机制的主要功能是解决两个基本问题：（1）谁有权写入数据。区块链系统中，每一个骨干网络节点都将各自独立维护一份区块链账本（即区块链系统中的数据库）。为了避免不同的区块链账本出现数据混乱的问题，必须要设计公平的挑选机制，每次只挑选一个网络节点负责写入数据；（2）其他人如何同步数据。当被挑选的网络节点写入数据后，其他网络节点必须能够准确及时的同步这些数据。为了避免网络中出现伪造、篡改新增数据的情况，必须设计可靠的验证机制，使所有网络节点能够快速验证接收到的数据是由被挑选的网络节点写入的数据。一旦解决这两个问题，区块链分布式网络中的节点就可以自发的建立一致性的可信数据副本。首先，每隔一定时间，经过共识机制挑选的节点将挑选待入库的交易，构造最小的区块链数据存储结构“区块”，然后将区块数据广播到区块链网络。其次，全网所有节点将对接收到的区块数据进行检测，根据共识机制判断区块数据是否是由合法的授权节点发布。如果区块数据满足共识机制和其他格式需求，将会被节点追加在各自维护的区块链账本中，完成一次数据同步。通过重复这两项过程，区块链账本就可以稳定、可靠的实现更新和同步，避免数据混乱、数据伪造等问题。共识机制是区块链的核心技术，与区块链系统的安全性、可扩展性、性能效率、资源消耗密切相关。迄今为止，研究者已经在共识相关领域做了大量研究工作，提出了众多不同的共识机制。从如何选取记账节点的角度，现有的区块链共识机制可以分为选举类、证明类、随机类、联盟类和混合类共5种类型：选举类共识是指矿工节点在每一轮共识过程中通过“投票选举”的方式选出当前轮次的记账节点，首先获得半数以上选票的矿工节点将会获得记账权。例如PBFT、Paxos和Raft等。PBFT共识机制效率高，支持秒级出块，而且支持强监管节点参与，具备权限分级能力，在安全性、一致性、可用性方面有较强优势。然而，在PBFT系统，一旦有1/3或以上记账人停止工作，系统将无法提供服务，当有1/3或以上记账人联合作恶，且其他所有的记账人被恰好分割为两个网络孤岛时，恶意记账人可以使系统出现分叉。证明类共识被称为“Proof of X”类共识，即矿工节点在每一轮共识过程中必须证明自己具有某种特定的能力，证明方式通常是竞争性地完成某项难以解决但易于验证的任务，在竞争中胜出的矿工节点将获得记账权。例如PoW和PoS共识算法等。PoW（工作量证明机制）的核心思想是通过分布式节点的算力竞争来保证数据的一致性和共识的安全性。PoS（权益证明机制）的目的是解决PoW中资源浪费的问题。PoS是由具有

最高权益的节点获得新区块的记账权和收益奖励，不需要进行大量的算力竞赛。PoS一定程度上解决了PoW算力浪费的问题，但是PoS共识机制导致拥有权益的参与者可以持币获得利息，容易产生垄断。随机类共识是指矿工节点根据某种随机方式直接确定每一轮的记账节点，例如Algorand和PoET共识算法等。Algorand共识是为了解决PoW共识协议存在的算力浪费、扩展性弱、易分叉、确认时间长等不足。Algorand共识的优点包括：能耗低，不管系统中有多用户，大约每1500名用户中只有1名会被系统随机挑中执行长达几秒钟的计算；民主化，不会出现类似比特币区块链系统的“矿工”群体；出现分叉的概率低于10-18。联盟类共识是指矿工节点基于某种特定方式首先选举出一组代表节点，而后由代表节点以轮流或者选举的方式依次取得记账权。这是一种以“代议制”为特点的共识算法，例如DPoS等。DPoS不仅能够很好地解决PoW浪费能源和联合挖矿对系统的去中心化构成威胁的问题，也能够弥补PoS中拥有记账权益的参与者未必希望参与记账的缺点。混合类共识是指矿工节点采取多种共识算法的混合体来选择记账节点，例如PoW+PoS混合共识、DPoS+BFT共识等。通过结合多种共识算法，能够取长补短，解决单一共识机制存在的能源消耗与安全风险问题。当前现有的共识机制很难做到性能和扩展性的平衡。比特币、以太坊等公有链使用的共识机制（如PoW，PoS等）虽然支持大规模节点网络，但共识性能较低，如比特币的TPS（每秒处理的交易数）大约只有7。而以Fabric为首的联盟链共识机制（如PBFT等）虽然有较高的TPS，如PBFT的TPS能达到1000，但这些共识算法的扩展性较差，只支持小规模的网络，当节点数量过多时共识机制就会崩溃，且很多联盟链共识算法的共识节点是预置的，不支持节点的动态加入与退出。目前区块链系统的共识效率仍是区块链技术的瓶颈之一，在一定程度上限制着区块链技术的发展和相关应用的落地。未来区块链共识算法的研究方向将主要侧重于共识机制的性能提升、扩展性提升、安全性提升和新型区块链架构下的共识创新。2.2互操作性区块链技术已经渗透至金融、供应链等不同的行业与场景，有效打破了同一场景下不同参与方间的价值孤岛。但现阶段价值难以在不同行业、不同场景之间流动。这使得不同区块链的参与方成为了一个个封闭的小团体，这显然不利于价值的社会化流通。因而，实现区块链的互操作性势在必行。目前，区块链的互操作性主要通过跨链技术实现。依据具体的技术路线，跨链技术可分为公证人技术、侧链技术、原子交换技术以及分布式私钥控制技术四类。（1）公证人技术在公证人技术中，交易参与方事先选择一组可信的公证人，以确保交易的有效执行。由Ripple公司提出的InterLedger协议，是公证人技术的一个典型案例。InterLedger实现了跨区块链转账，在A链发送方在向B链接收方转账前，需找到一组连接者(Connectors)，由连接者逐跳地把资金发送至接收方。各连接者需指定一组公证人(notaries)，由公证人监督这一组交易的有效性。公证人技术的主要问题在于需要信任特定的公证人群体，这违背了区块链去中心化的设计初衷，并引入一定的安全性隐患。（2）侧链技术借助侧链技术，一条区块链可以读取并验证其他区块链的事件和状态。目前，侧链技术可分为一对一侧链和星形侧链两大类。一对一侧链技术包括以btcRelay、RSK为代表的新型区块链。此类区块链能够和一条已有的区块链（如比特币）交互，主要目的是实现已有区块链的功能拓展。而

星形侧链技术主要包括以Polkadot、Cosmos为代表的跨链基础设施，其通过构建一条新区块链连接多条其他区块链，进而形成一个星形拓扑结构，实现不同区块链间的价值与信息流通。（3）原子交换原子交换的基本思想是，当位于两条链上的双方互换资产时，交易双方通过智能合约等技术，维护一个相互制约的触发器(trigger)以保证资产交换的原子性。即A与B之间的资产交换或者同时发生，或者同时不发生，而不会发生A向B转账完成，而B未向A转账的情况。此类跨链方案的典型案例是Blocknet。在原子交换的基础上，Blocknet增加了订单匹配、交易撮合等功能，以实现去中心化跨链货币兑换。然而，原子交换技术的应用范围较为狭窄，仅限于跨链转账领域，无法满足其他跨链需求。（4）分布式私钥控制技术分布式私钥控制技术旨在通过分布式私钥生成与控制技术，将各种数字资产映射到一条新的区块链上，从而在同一条区块链上实现不同数字资产的自由交换。Fusion是分布式私钥控制技术的代表性项目。其核心思想将各条区块链上的数字资产映射到Fusion构建的公共区块链上。简单来说，就像不同区块链用户将数字资产存入“银行”，银行内的数字资产可以进行自由的流通与兑换，并实时更新用户账户余额，用户从“银行”提款时以最后的账户余额为准。分布式私钥控制技术与原子交换技术类似，仅能完成跨链资产转移，尚不能进行更复杂的跨链互操作。如果后续无法对其功能完成进一步的拓展，那么分布式私钥控制技术的应用范围将远达不到预期的效果。可以看到，已有区块链互操作性方案存在明显不足。首先，应用范围窄。例如，BTC Relay只能完成比特币到以太坊的单向操作，而InterLedger和Fusion等仅能完成跨链转账，无法进行其他类型的操作。其次，兼容性差。例如，Cosmos等系统仅支持结构相同区块链的互联互通。总之，现有各种跨链与互操作性方案仍处在起步阶段，距离实际应用还有很长一段距离。针对此类问题进行优化，也是区块链互操作性的未来演进方向。此外，区块链的互操作性研究直接关系到区块链通信的接口标准。然而，目前最具影响力的跨链方案均由国外的企业和研究机构提出。相关实体在设计跨链方案时，首先考虑的将是自身经济利益。因此，我国应尽快推动区块链互操作性研究，积极参与跨链标准的制定，从而为国内的区块链产业争取更多话语权。2.3安全性目前，区块链技术已在金融、政务甚至国防领域获得初步应用。这些场景对安全性的要求极高，然而很多区块链均发生过严重的安全问题。截至2018年4月，区块链已发生超过200起重大安全事件，造成的经济损失已超过36亿美元。因此，对区块链安全性的研究势在必行。现阶段，业界侧重于从不同角度提出针对区块链系统的攻防措施，进而对区块链安全性进行全方位探索。研究表明，任何违反区块链安全性的行为，都可以归结为从算法安全、协议安全、实现安全、使用安全和系统安全等五个层面进行的破坏、更改和泄露。（1）算法安全算法安全通常是指密码算法安全，既包括用于检验交易的哈希算法、签名算法，也包括用于某些智能合约中的复杂密码算法。一般来说多数区块链中使用的通用标准密码算法在目前是安全的，但是这些算法从间接和未来看也存在安全隐患。首先从间接来看，SHA256算法对应的ASIC矿机以及矿池的出现，打破了原有“一CPU一票”的理念，使得全网节点减少，权力日趋集中，51%攻击难度变小，对应的区块链系统受到安全性威胁。其次从未来发展看，随着量子计算的兴起，实用的密码体制均存在被

攻破的威胁。此外，对于新型密码，由于其没有经过足够的时间检验和充分的攻防考验，其在实际应用中更容易成为短板。比如麻省理工学院发现新兴区块链IOTA的哈希算法中存在致命漏洞，使得IOTA团队紧急更换算法。某些未经检验的随机数生成器也可能存在漏洞，利用生日攻击会产生相同随机数，进而威胁区块链安全。为了防止ASIC过度使用造成区块链中心化问题，设计不利于并行计算的哈希算法势在必行。目前，莱特币的scrypt算法和暗黑币X11算法均从增加内存消耗方面提高了ASIC开发难度。为防范量子计算威胁，传统密码算法需要尽早替换为抗量子密码算法，目前业界已提出了基于格上困难问题的密码算法和基于纠错码的密码算法等。为了防范不成熟密码造成的安全漏洞，必须对于未经验证的密码算法谨慎使用。另外随机数生成器也必须从伪随机向真随机过渡，如采用基于混沌的随机数发生器129J和基于量子的随机数发生器等。（2）协议安全协议是通信双方为了实现通信而设计的约定或通话规则，包括网络层面的通信协议和上层的区块链共识协议。协议安全在网络层面表现为P2P协议设计安全。攻击者利用网络协议漏洞可以进行日蚀攻击(Eclipse Attack)和路由攻击(Routing Attack)。攻击者利用网络节点的连接数限制可以用日蚀攻击将节点从主网中隔离，而路由攻击则是通过控制路由基础设施将区块链网络分区而进行的攻击。攻击者还可以发起DDoS攻击，目前对于DDoS攻击只能依靠收取交易费和浪费算力来控制。协议安全在区块链共识层面表现为共识协议安全。首先各类共识协议均有容错能力限制，如PoW存在51%算力攻击，PoS存在51%币天攻击，而DPoS还存在着中心化风险。其次，共识协议容易受到外部攻击影响。例如，针对PoW共识已出现了自私挖矿(Selfish Mining)和顽固挖矿(Stubborn Minging)等多种攻击。自私挖矿可以使攻击者获得多出自身算力占比的收益；而顽固挖矿是对自私挖矿的拓展，可以使攻击者收益率比自私挖矿提高13.94%。PoS共识则存在“无利害关系(Nothing at Stake)”问题，即区块链发生分叉时，矿工可能会在多个分叉上同时下注，以谋取不当利益。针对协议安全性问题，为防止网络层面的攻击，需要开发者谨慎选择区块链的网络协议。而为了防止区块链共识层面的攻击，则需设计适当的激励与惩罚措施，从而降低攻击者获得的收益。（3）实现安全在区块链系统的实现过程中，程序员可能会有意或无意留下漏洞，从而导致区块链的安全性受到损害。具体表现在以下两个方面。首先，众多区块链引入了图灵完备的智能合约机制。用户可以利用智能合约编写自动化程序，完成资产分配等操作。然而，在编写智能合约时很可能会引入安全性漏洞。例如，某些合约可能会错误地把资产发送到不受控的地址，或者资产无限期锁死，导致全网可用代币减少等。其次，区块链的底层源码也可能存在整数溢出漏洞、短地址漏洞和公开函数漏洞等各种漏洞。例如，比特币0.3.11之前版本可以违规生成大量比特币，而以太坊的短地址漏洞可以使交易者从交易所违规获得256倍甚至更多的利益。针对智能合约等程序在实现上的安全问题，业界已提出一系列的形式化验证和安全测试技术，从而在产品上线之前发现其可能存在的漏洞。此外，诸多区块链的产品开发者已开始定期进行代码审计，包括交易安全审查和访问控制审查等，从而争取在攻击者发现漏洞之前修复安全问题。（4）使用安全在区块链中，“使用安全”特指用户私钥的安全。私钥代表了用户的资产所有权，是资产

安全的前提。然而在传统的区块链中，私钥均由用户自己生产并保管，没有第三方的参与，所以私钥一旦丢失或被盗，用户就会遭受资产损失。在现实使用中，某些交易平台会代替用户管理私钥，但是很多平台往往采用联网的“热钱包”管理私钥，一旦“热钱包”被黑客破解，用户的资产就会被盗取。此外，由于没有完善的风险隔离措施和人员监督机制，导致部分拥有权限的员工利用监管机会盗取信息或代币。针对使用安全性问题，用户需要更加谨慎保管私钥，尽量使用与网络隔离的冷钱包存储私钥。而交易平台需严格进行权限管理，谨慎开放服务器端口，定期进行安全监测，建立完善的应急处理措施。（5）系统安全系统安全是一个整体性概念，它受到各级安全因素的共同影响。攻击者可以综合运用网络攻击手段，对算法漏洞、协议漏洞、使用漏洞、实现漏洞、系统漏洞等各个方面综合利用，从而达成攻击目的。另外社会工程学攻击的引入也使区块链变得更加脆弱。为此，业界需还要关注用户自身系统安全性，包括定期更新补丁、启用设备防火墙、禁用路由器中不必要的组件等。区块链技术已开始获得广泛应用。然而，现有区块链的安全问题曾出不穷，因此必须对安全性问题高度重视。目前对区块链安全性的研究主要从“攻”与“防”两个角度进行。业界分别从从算法、协议、实现、使用和系统等五个层面发现安全隐患，并提出弥补措施。然而，现阶段并从根本上解决安全问题。因此在未来，必须从区块链体系架构进行创新，从本质上找到单一漏洞影响系统安全的原因，得到应对区块链安全问题的有效机制。2.4隐私保护随着区块链技术不断发展和广泛应用，其面临的隐私泄露问题越来越突出，必须得到研究人员和工业界开发人员的充分重视。相对于传统的中心化存储架构，区块链机制不依赖特定中心节点处理和存储数据，因此能够避免集中式服务器单点崩溃和数据泄露的风险。但是为了在分布式系统中的各节点之间达成共识，区块链中所有的交易记录必须公开给所有节点，这将显著增加隐私泄露的风险。然而，区块链本身分布式的特点与传统IT架构存在显著区别，很多传统的隐私保护方案在区块链应用中不适用，因此分析区块链隐私泄露缺陷、研究针对性的隐私保护方法具有重要意义。根据保护隐私的对象分类，主要可以分为3类：网络层隐私保护、交易层隐私保护和应用层的隐私保护。网络层的隐私保护，涵盖数据在网络中传输的过程，包括区块链节点设置模式、节点通信机制、数据传输的协议机制等；交易层的隐私保护，包含区块链中数据产生、验证、存储和使用的整个过程，交易层隐私保护的侧重点是满足区块链基本共识机制和数据存储不变的条件下，尽可能隐藏数据信息和数据背后的知识，防止攻击者通过分析区块数据提取用户画像；应用层的隐私保护场景，包含区块链数据被外部应用使用的过程等，区块链被外部使用的过程存在泄露交易隐私和身份隐私的威胁，因此，应用层隐私保护的侧重点包括提升用户的安全意识、提高区块链服务商的安全防护水平，例如合理的公私钥保存、构建无漏洞的区块链服务等。目前的公有链项目中，各参与方都能够获得完整数据备份，所有数据对于参与方来讲是透明的，任何人都可以在链上查询到上链数据。比特币项目只是通过隔断交易地址和地址持有人真实身份的关联，达到匿名效果，攻击者能够看到每一笔转账记录的发送方和接受方的地址，但无法对应到现实世界中的具体某个人。尽管如此，攻击者仍可以通过多个层面的攻击达到窃取隐私的目的，例如网络层、交易层和应用层

发动不同形式的攻击。对于联盟链而言，带有CA性质的监管角色虽然可以保证接入节点的可信，但如果区块链要承载更多的业务，比如实际场景中登记实名资产、通过智能合约实现具体借款合同的同时保证验证节点在不知晓具体合同信息的情况下如何执行合同等等，基于密码学、零知识证明等技术的研究正在不断推进，只有不断完善区块链技术本身的多层面隐私保护机制，才能让区块链实际赋能传统行业，发挥其既定的优势。2.5可监管性当前以数字货币比特币概念股为首的各类区块链应用发展迅速，与此同时，区块链中潜在的监管问题也逐渐显现。一方面，区块链数字货币为洗钱、勒索病毒等犯罪活动提供了一条安全稳定的资金渠道，促进了地下黑市的运行。以比特币为例，著名的勒索病毒WannaCry通过比特币来实现对用户资产的勒索，地下黑市网站“丝绸之路”利用比特币进行非法买卖，很快受到了地下人群的追捧。另一方面，区块链数字货币使跨国境的资金转移变得更为简单，将有可能损害各国的金融主权，影响金融市场的稳定。与此同时，由于区块链去中心化、不可篡改等特性，使得区块链常被用于敏感信息的存储与传播。有些人将敏感有害信息保存在比特币和以太坊区块链的交易中，而这些信息并不能从区块链中删除。同时，由于区块链的匿名性，监管方也不能通过这些敏感信息和涉及违法犯罪的交易的发送方地址找到发送方的真实身份。此类事件严重危害国家安全和稳定，给网络监管机构带来了极大的挑战和威胁。当前对公有链的监管刚刚处于起步阶段，研究方向不全面，研究技术也不成熟。然而，对公有链的监管需求又是十分必要且紧急的。因此，监管成为了公有链领域急需解决的问题，也成为了当前公有链项目落地的最大挑战。联盟链由于其自身特点，使得联盟链能够很好的支持对节点和链上数据的监管。因此，如何设计监管友好的联盟链基础架构，在保护隐私的前提下实现监管功能，是联盟链监管中需要研究的主要问题。任何技术的发展都离不开对技术本身的监管，我们需要加强对区块链监管的研究，只有这样才能够保证区块链行业的健康和可持续发展。新闻排行榜1全球各国区块链、数字货币等政策汇总2斯坦福大学终身教授张首晟：区块链最核心的理念，必然是「 In Math We Trust 」3人民日报：让行业协会走上前台比特中国4洪门发布洪币白皮书首发价格1美元，谁敢砸盘？5区块链热潮下，BAT也坐不住了 百度上线首个区块链应用“莱茨狗”6习主席首提“区块链”，蕴含“区块链强国”战略7中共中央关于制定国民经济和社会发展第十四个五年规划和二〇三五年远景目标的建议8区块链为什么上升为国家战略技术的原因解析9区块链在国家治理与公共事务中的现实应用102019年是区块链行业跌宕起伏的一年山寨币