区块链关键技术研究进展

CCF 区块链专业委员会

斯雪明[1]　孙　毅[2]　祝烈煌[3]　朱建明[4]
高　胜[4]　陈　福[4]　董学文[5]

[1]复旦大学，上海
[2]中国科学院计算技术研究所，北京
[3]北京理工大学，北京
[4]中央财经大学，北京
[5]西安电子科技大学，西安

摘　要

区块链是一种由多方共同维护，使用密码学保证传输和访问安全，能够实现数据一致存储、难以篡改、防止抵赖的记账技术，也称为分布式账本技术。近年来，区块链技术的发展对社会产生了重要的影响。本文介绍近年来区块链关键技术的发展现状和研究进展。首先从共识机制、互操作性、安全性、隐私保护和可监管性等方面介绍了区块链技术的现状和面临的挑战。然后重点从跨链通信技术、区块链智能合约、区块链安全性、区块链监管与隐私保护、区块链技术应用等方面分析当前国内外研究现状，并指出了相关技术的发展趋势和展望。作为金融科技的重要技术、数字经济的重要基础，区块链技术在未来将发挥重要的作用。

关键词：区块链，智能合约，数字货币，安全，监管

Abstract

Blockchain is a kind of accounting technology that is maintained by many parties and uses cryptography to ensure transmission and access security. It can realize consistent data storage, difficult to tamper with and prevent repudiation. It is also called distributed ledger technology. In recent years, the development of blockchain technology has had an important impact on society. This paper introduces the development status and research progress of key technologies of blockchain in recent years. Firstly, the status quo and challenges of blockchain technology are introduced from the aspects of consensus mechanism, interoperability, security, privacy protection and maintainability. Then it focuses on the current research status at home and abroad from the aspects of cross-chain communication technology, blockchain intelligent contract, blockchain security, blockchain supervision and privacy protection, blockchain technology application, etc., and points out the development trend of related technologies. As an important technology of financial technology and an important foundation of the digital economy, blockchain technology will play an important role in the future.

Keywords: Blockchain, Smart contracts, Digital currency, Security, Regulation

1 引言

2008 年 10 月，中本聪（Satoshi Nakamoto）在论文《比特币：一种点对点式的电子现金系统》（Bitcoin：A Peer-to-Peer Electronic Cash System）中基于区块链技术描述了一种称为比特币（Bitcoin）的电子现金系统。2009 年 1 月，比特币系统正式运行，产生了第一个比特币。十年来，比特币给整个社会带来了巨大的影响。与此同时，区块链技术也从发行比特币到应用于社会的许多领域，为解决现实问题提供了一种新的选择，被称为“创造信任的机器”、“将颠覆互联网的新技术”。2019 年 6 月，Facebook 加密货币项目 Libra 白皮书正式公布，引起世界各国的高度关注，再一次将数字货币与区块链技术推向一个新的阶段。

区块链是一种由多方共同维护，使用密码学保证传输和访问安全，能够实现数据一致存储、难以篡改、防止抵赖的记账技术，也称为分布式账本技术。区块链技术为进一步解决互联网中的信任问题、安全问题和效率问题，提供了新的解决方案，也为金融等行业的发展带来了新的机遇和挑战。为应对区块链技术所带来的机遇和挑战，产业界和学术界纷纷开展了区块链技术应用探索和理论研究，为深入推进区块链技术与实际业务的融合提供了强大的动力。同时，近年来，区块链技术发展与政策监管相向而行的趋势愈发明显，也为区块链技术与金融等行业的深入融合提供了重要的推动力。

本文介绍近年来区块链关键技术的发展现状和研究进展。重点从可扩展性、跨链通信技术、区块链智能合约、区块链安全性、区块链监管与隐私保护、区块链技术应用等方面分析当前国内外研究现状，并指出了相关技术的发展趋势和展望。

2 区块链关键技术及其面临的挑战

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地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 BTC Relay、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，业界还需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层出不穷，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，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，监管成为公有链领域急需解决的问题，也成为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地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。

3　核心技术研究进展

针对当前区块链技术发展面临的问题，本节可扩展性、从跨链通信技术、区块链智能合约优化、区块链安全性、区块链监管与隐私保护、区块链技术应用等六个方面分析当前国内外研究进展。

3.1　可扩展性

可扩展性[1]是指区块链系统处理交易以及适应交易增长而扩展的能力。现有提升区块链可扩展性方法主要可分为：高效共识算法、分片技术、链上扩容、链下扩容等。其中高效共识机制已经 2.1 节进行了介绍，这里重点从分片技术、链上扩容、链下扩容等部分介绍区块链可扩展性研究进展。

3.1.1　分片技术

2016 年，Luu 等[2]最先将数据库中分片技术引入区块链中，提出了一种面向公有链的安全分片协议 Elastico，可提供近似线性的扩展性，同时容忍 1/4 恶意节点。具体地，Elastico 首先使用 PoW 方式生成节点身份，然后根据节点身份中后几个比特位将区块链节点划分到不同分片中，同一分片中节点身份后几个比特位相同。为保证每个分片中至少

有一定数量节点同时减少广播消息数量，Elastico 建立分片目录，由其管理每个分片；若每个分片节点数量满足要求则将节点身份广播给全网节点。最后，每个分片内部独立运行 BFT 共识算法，并将各自产生的区块头发送给裁决分片，由其验证所有签名并产生全局区块广播给每个分片。可见，随着网络节点数量不断增多，Elastico 可实现区块链吞吐量近似线性增加。

2017 年，基于分片技术的公有链 Zilliqa 被提出[4]。首先，Zilliqa 采用 Elastico 中验证节点分片方法，即同样采用 PoW 选出验证节点，并根据哈希后几位比特进行分片，增强分片中验证节点可靠性，以抵御女巫攻击。为确定每个分片节点数量，实验发现当每个分片节点数量大于 600 时，出现 1/3 坏节点的概率抵御百万分之一。为此，Zilliqa 按照 600 个一组将验证节点分配到每个分片。然后，在片内进行 BFT 共识。考虑到 PBFT 在节点数量较多时性能较差，Zilliqa 采用多重签名算法优化 PBFT 共识算法，从而降低通信复杂度。

2018 年，Kokoris-Kogias 等[5]指出 Elastico 存在节点数量较少的分片具有高损害概率，分片划分不具有强抗预测性，不能保障跨分片交易的原子性，验证节点频繁切换分片带来性能下降等问题。为此，利用分片技术提出了第一个可与中心化支付系统（如 Visa）竞争，具有横向扩展交易处理能力的区块链 OmniLedger。具体地，OmniLedger 通过一条身份链将生成的验证者身份分配给不同分片。为保证验证者选择过程是可扩展和强抗预测性，OmniLedger 使用公共随机协议或加密抽签协议选择验证者分组，并利用 RandHound 协议安全地将验证者分组分配到不同的分片上。其次，为了保障跨分片交易的原子性，OmniLedger 提出一种拜占庭分片原子提交协议 Atomix，保证每个交易被完全提交或最终取消，实现跨分片交易的一致性，从而阻止双重支付或资金永久锁定问题。最后，OmniLedger 利用状态区块汇总一个周期内所有分片状态，为验证者较少存储和启动开销，同时利用信任但检查方式实现小额支付的实时性。

随后，Zamani 等[6]指出 OmniLedger 同 Elastico 一样只能容忍 1/4 恶意节点，并且只有当恶意节点数低于 1/8 时，才可达到低于 10 秒延时。其次，共识过程中节点之间通信复杂度较高，并且需要一个可信初始化过程来产生随机参数。此外，容易遭受利用 Atomix 锁定任意交易恶意用户的 DoS 攻击。为此，提出了一种抵御拜占庭的公有链 RapidChain，提升 Elastico、OmniLedger 等区块链的安全性和可扩展性。具体地，RapidChain 包含启动、共识、重配置等阶段，其中启动阶段主要利用选举协议从网络节点中选出根群组，用来产生建立分片的随机比特。共识阶段主要采用实用同步化拜占庭共识算法[14]，实现片内容忍 1/2 恶意节点，总体容忍 1/3 恶意节点。重配置阶段主要利用 Cuckoo 规则[15]保障新节点加入分片后不影响所有分片 1/2 拜占庭容忍。

2018 年，Vitalik 提出了一种基于双层设计的以太坊分片方案[3]。具体地，以太坊区块链被分为主链和分片链，其中主链通过验证管理合约（Validator Manager Contract，VMC）来管理分片链，分片链采用 PoS 共识机制打包交易数据生成验证块，通过这些验证块最终生成主链上的区块。每笔交易都独立运行在其中一个分片，验证节点只校验所在分片的交易。为保证验证选择过程是强抗预测性，VMC 采用随机抽样方式将验证节点

分配到分片链上，同时校验所有分片提交的验证块头，并将校验通过的验证块头哈希记录到链上。此外，VMC 采用 UTXO 模型和收据树实现跨片通信。

3.1.2　链上扩容

链上扩容通过改变区块链底层结构，如增加区块大小、缩短出块时间等，提升区块链可扩展性。现有研究一部分研究高效的共识机制，如 Bitcoin-NG，PBFT 等，通过缩短出块时间来提升区块链可扩展性。一部分研究通过增加区块容量，涉及 BIP-102、BIP-103、BIP-104、BIP-106、BIP-107。2016 年 2 月达成的香港共识指出，比特币核心将在隔离见证之后通过硬分叉将区块扩容到 2M。然而，该共识并没有被实施。2016 年 10 月，比特大陆投资的新矿池 ViaBTC 提出 Bitcoin Unlimited 中，区块容量上限不再是固定值，而可以由矿工投票改变。然而，最后由于技术原因导致 Bitcoin Unlimited 以失败告终。2017 年 5 月达成的纽约共识指出，将准备实施 SegWit2X 扩容方案，即 SegWit 软分叉和 2M 扩容硬分叉。然而，该共识最终也以失败告终。2017 年 8 月，BCH 在比特币区块高度 478558 执行硬分叉，删除了隔离见证，将区块扩容到 8MB，期望通过该链上扩容解决比特币系统中区块拥堵和手续费高等问题。在此之后，BCH 通过硬分叉的方式进行了 4 次升级。

3.1.3　链下扩容

链下扩容是将交易转移到链下完成，链上只作为交易记录或仲裁平台。通过将区块链从结算平台变为清算平台，从而降低区块链的交易数量，提升区块链的交易能力，主要包括隔离见证、状态通道、侧链等方案。

2015 年，Poon 等[16]首次提出闪电网络的概念，通过在链下建立交易的微支付通道，将比特币网络中的小额交易带离。在闪电网络中，主要包括序列到期可撤销合约（Revocable Sequence Maturity Contract，RSMC）和哈希时间锁定合约（Hashed Timelock Contract，HTLC）两个协议。RSMC 机制通过设置时间锁和引入惩罚机制来实现支付通道的双向支付，而 HTLC 则是利用条件支付的方法，实现不同节点跨通道支付问题。闪电网络的具体流程大致分为起始阶段、交易阶段和结束阶段。交易双方在起始阶段创建交易通道并将各自的押金放入创建的资金池中，广播彼此的初始状态；交易阶段通过更新每一轮的承诺来进行交易；交易完成后，交易双方广播承诺，通道关闭。为保证支付通道双向支付，RSMC 利用时间锁机制来延迟通道中交易一方取回资产的时间，同时通过惩罚机制来保证通道双方的承诺是最新的状态。若交易一方存在虚假交易，另一方可以通过时间锁的延迟内发现，并将通道内的资产收回，以对虚假交易的惩罚。然而，为解决闪电网络效率及可用性不足等问题，Raiden 网络[17]的支付通道中的惩罚交易是基于交易双方对交易轮数的签名，这使得支付通道不再受限于比特币系统脚本的限制，有效地避免了因高频交易的持续发生而带来交易代价越来越大的问题。Miller 等[18]定义了一种新的支付通道 Sprites，解决了用户如果跨链不成功，所要消耗的时间过大的问题。Sprites 利用以太坊平台中的智能合约，设计基于哈希原象的管理合约，使用户可以通过调用合

约的状态获取交易是否成功的信息，从而减少了时间成本。为了保证交易通道的可持久性，Decker 等[19]提出的 Duplex 利用比特币系统中的时间锁机制设计了无效树的结构来保证通道的可持久性，同时保证客户间安全及时的交易。Khalil 等[20]提出的 Revive 通过交易通道所有者的偏好，允许交易通道中的任意一组用户安全地重新平衡他们的交易通道，保证支付网络的可持久化。

Poon 等[21]提出的 Plasma 是基于以太坊网络，通过建立侧链机制来尽可能地减少在根链上的交易量，从而降低根链的交易负荷的侧链技术。Plasma 区块链为树状结构，有多个分支，每个分支为一条子链，一般子区块的区块头哈希值存储在根链中，其目的是用来对区块的有效性进行验证。为了防止子链和根链之间交流发生欺诈，Plasma 设计了欺诈证明（Fraud proofs）机制，主要由根链负责保证网络环境的安全和对欺诈行为的处理。每个子链可以有自己的欺诈证明，可以构建在不同的共识算法之上。当发生欺诈行为时，用户可以将欺诈证明提交到根链来保证用户的权益不受伤害。MapReduce 作为跨多个数据库组织和计算数据的分布式运算规则，被应用于 Plasma 中。在 MapReduce 机制中，将每个子链看作是一个数据库，实现了数据的快速处理。最后，Plasma 这种通过树状结构创建多条子链来减轻主链的工作方式，使主链可以每秒处理更多的事务，提高以太坊网络的整体性能。

3.2 跨链通信技术

区块链跨链技术的研究可以追溯到 2012 年，Ripple 发布 Interledger 协议（ILP）首次提出了跨区块链的互操作方案；2014 年 Blockstream 推出 Sidechain，提出了双向锚定的侧链技术方案，该技术方案直至今天都是研究的重点；2015 年提出闪电网络的设计思路，开创了使用哈希锁定技术进行跨链的技术路线；2017 年 Fusion 正式启动，提出了分布式私钥控制技术方案。区块链跨链技术经过不断的发展创新，大致可以分为四类：公证人技术、侧链技术、哈希锁技术以及分布式私钥控制技术。

3.2.1 公证人技术

公证人技术是指利用可信的公证人保证交易执行的原子性从而完成跨链交易的技术，这种技术的主要代表是 Ripple 实验室提出来的 Interledger 协议（ILP）。

（1）Ripple

Ripple 是世界上第一个开放支付系统，也是第一个利用区块链技术实现跨系统转账的技术，其本质是一个开源、分布式的支付协议，其主要应用领域是跨境转账。现在银行的跨境转账、清算等操作依赖于 SWIFT 网络，存在手续费高、效率较低等问题。通过 Ripple 协议实现跨境转账，将大大降低所需的手续费，统计 Ripple 网络事实清算将大大提高交易处理效率。Ripple 设计了 Interledger Protocol（ILP）实现跨链交易：利用多跳连接者连接跨链交易的发送者和接收者，通过发送者、多跳连接者与接收者之间的一组交易达到目的交易需要实现的效果，同时通过公证人保证这一组交易

执行的原子性。

Ripple 早在 2012 年就成立了，其提供了三种解决方案：协助银行处理全球支付的 xCurrent、为支付服务商提供流动性的 xRapid 以、协助普通公司接入瑞波网进行支付的 xVia。2014 年开始，Fidor 银行、Cross River 银行、CBW 银行等金融机构接入 Ripple 协议。现在 Ripple 生态已较为成熟了，越来越多的金融机构与 Ripple 保持合作关系，但是由于 Ripple 主要解决跨境转账的问题，而且 ILP 需要公证人，Ripple 在跨链通信上没有更多的进展。

（2）PalletOne

PalletOne 是一个区块链跨链平台，其目标不仅仅是设计跨链协议、实现价值流通的公链跨链载体，还包括实现处理高并发、构建高性能的“超级公链”、实现区块链网络价值最大化。PalletOne 架构包括：对接底层区块链的适配器、使用 DAG 的分布式存储、负责网络安全型的陪审团及调停中介、通证抽象层、保证合约安全稳定运行的虚拟机层以及为软件开发者提供的 SDK，PalletOne 要实现的是一个完整的跨链生态。PalletOne 跨链通过一个轻量型，与区块链分离的高阶合约执行层实现，具体交易通过陪审团的多签名执行，陪审团相当于跨链交易的公证人。

PalletOne 项目概念诞生于 2017 年 9 月，2018 年 5 月发布项目白皮书以及黄皮书。根据团队的 Git 更新以及公布的开发进度，2018 年 9 月底，PalletOne 完成了 BTC 和 ETH 适配器的开发，实现了 BTC 与 ETH 基于 PalletOne 的跨链交换，目前在还不断对适配器进行更新、完善。根据官网显示的开发团队计划，2018 年第四季度将上线测试网络，2019 年第二季度将上线主网。

3.2.2　侧链技术

侧链技术根据其实现方式和主要用途可以分为狭义和广义两类。狭义上的侧链技术指以 BTC Relay、Sidechain、Drivechain 以及 RSK 为代表的以锚定某种原链（主要是比特币区块链）为基础的新型区块链。广义上的侧链技术还包括以 Polkadot、Cosmos 为代表的跨链基础设施，其主要目的是解决现有区块链可拓展性问题、延伸性问题以及互操作性问题。

（1）BTC Relay

2016 年 ConsenSys 团队推出的 BTC Relay 使用以太坊智能合约以一种去中心化的方式连接了现在受众最广的两条区块链——比特币区块链和以太坊区块链，实现了以太坊用户在以太坊区块链上验证比特币交易。BTC Relay 利用 Relayers 提供的比特币区块头建立起一个轻量版的比特币“区块链”，从而实现对比特币网络活动的验证。

BTC Relay 自推出就获得了广泛的认可，被认为是第一种跨区块链通信的产品，同时也被寄托了帮助完善以太坊基础设施，帮助以太坊完成更大的创新的愿望。2017 年一家建立在以太坊上的去中心平台 EtherEx 与 BTC Relay 合作，将 BTC 交易引入 EtherEx，探索对不在以太坊上的加密货币的处理。

由于该项目实现的仅仅是以太坊区块链和比特币区块链之间单方向的跨链操作，应

用范围较为狭窄，同时 Relayer 提交区块头需要支付一定的手续费，Relayer 活跃度不够高，该项目没有被广泛接受。根据 BTC Relay 官网上的信息，现在已经没有活跃的 Relayer 在工作了，同步的最后一个比特币区块高度是 501329，该区块打包的时间是 2017 年 12 月份，也就是说 BTC Relay 主网有快一年的时间没有工作了。目前该项目没有其他更新的有价值的消息。

（2）Liquid

Liquid 是 Blockstream 推出的锚定在比特币区块链上的一条侧链，其目标是帮助交易所、经纪商以及金融机构等组织快速且安全地转移大量比特币，提高资金使用效率以及市场流动性。Liquid 作为比特币区块链的侧链通过 Sidechain 双向锚定技术锚定在比特币区块链上从而实现与比特币区块链的互操作。Liquid 区块链底层采用利用强联盟改进的区块链，利用强联盟充当主链与侧链之间的协议适配者以提供更有效率的跨链。

人们对 Liquid 存在不同看法：不看好 Liquid 的人们认为强联盟区块链是对比特币区块链的一种破坏，多重签名技术存在的缺陷会带来安全隐患，同时他们还认为双向锚定技术会导致区块链的独立安全性受影响；信任 Liquid 的人们则认为由 23 家交易所组成的联盟是值得信任的，高效的交易可以最大限度地减少利差，增加流动性。

Blockstream2016 年公布 Liquid。经过近两年的开发研究与内测，Blockstream 在 2017 年 5 月举行的 Consensus 2017 大会上进行了展示，Liquid 区块链进入公测阶段。2018 年 9 月 27 日，Liquid 区块链正式上线，参加上线的成员有数字货币行业内 23 家最大的公司。

（3）RSK

RSK 是一个通过双向锚定技术锚定在比特币区块链上的一个开源智能合约平台，其目标是将智能合约以可操作的形式带入比特币系统，实现即时支付以及高扩展性，从而为比特币生态系统增加价值和功能。由于比特币系统目前不支持验证外部 SPV，比特币区块链与根链无法实现完全可信和无需第三方的双向锚定，因此 RSK 引入了一个由多个半可信第三方组成的联邦，由联邦成员共同决定比特币的锁定与释放。具体的锚定方案是：根链侧使用 Sidechain 的锚定方案，比特币区块链侧使用 Drivichain 锚定与联邦投票结合的方案。RSK 通过联合挖矿保证网络算力从而保证系统的安全性。

由于 RSK 不是比特币区块链的竞争链而是锚定在比特币区块链上完善比特币区块链生态系统的侧链，它争取到了比特币社区以及矿工的支持。据统计，RSK 测试网络发布是 50% 的比特币矿工表示愿意进行联合挖矿支持 RSK，但是目前 RSK 主网上进行维护的矿工远达不到这个比例。对于普通用户而言，RSK 的提出将实现快速支付并为比特币增加新功能，提高使用体验。

早在 2015 年 RSK Lab 就提出了 RSK。2016 年 RSK 智能合约测试网络 Turmeric 正式上线，此时大多数矿工对 RSK 的联合挖矿表示支持。2017 年底 RSK 主网正式上线，2018 年 1 月 4 日，RSK 挖出了初始区块。目前 RSK 主网上有超过 88 万个区块，共有 16 个节点进行挖矿和网络维护，平均 33S 出一个区块。虽然目前 RSK 主网节点较少，打包的交易也较少，但是可以说是侧链技术一次较为成功的尝试，公司目前也在积极的开发

配套的钱包工具。

（4）Cosmos

与其他跨链项目不同，Cosmos 不是某一条区块链的侧链，而是一种支持跨链交易的网络架构，其目标不是解决某一区块链存在的问题，而是解决数字货币于区块链系统长久存在的互通性、扩展性以及可升级性等问题。Cosmos 网络涵盖多条基于 Tendermint Core 运行的独立区块链，这些独立区块链被称作“Zone”。Cosmos 上的第一个空间叫作“Cosmos Hub”。Cosmos Hub 及各个 Zone 可以通过区块链间通信（IBC）协议进行沟通，可以说 Cosmos 使用 IBC 协议实现了区块链中继功能，具体来说 IBC 协议允许区块链读取和验证其他区块链中的交易。

Cosmos 目标长远、愿景庞大，为了保证构建的网络足够安全，提供的服务足够优质，开发团队在软件迭代时都进行了彻底的迭代测试。2017 年 10 月 Cosmos 公共测试网络 gaia-1 发布，在该测试网上用户可以在 Hub 上发送和接受代币；2018 年 1 月 gaia-2 发布，该测试网实现了动态节点发现功能；2018 年 4 月至 8 月，每个月都进行了一些更新从而不断完善测试网络功能，同时启动对应的新测试网络，当前测试网络版本是 gaia-8001，SDK 版本是 v0. 24. 1，如图 1 所示。

图 1　Cosmos 测试网信息

据了解 Cosmos 主网发布前需要实现的 7 个主要功能：手续费、协议内权益罚没、多签名功能、ABCI（Application Blockchain Interface）更新、Gas 定价以及治理 v2，大部分已经实现了，但是 Cosmos 主网具体上线时间还是不能确定。

（5）Polkadot

Polkadot 也是一种支持跨链交易的网络结构，其目标是重构区块链架构，将区块链共识的规范性和有效性分开，从根本上解决区块链系统存在的扩展性及伸缩性问题。Polkadot 与 Cosmos 不同的是，Cosmos 网络是必须给予 Tendermint 的同构系统，而 Polkadot 预计构建成异构的多链系统。Polkadot 由一个中继链以及若干平行链做成，同时根据节点在网络中承担的功能将网络节点分成了四种角色，分别是：收集者、渔夫、提名者以及验证者。其中，验证者负责网络维护的主要工作，其他角色协助、监督验证者工作，具体的相互关系见图 2。四种角色协同工作维护网络，可以实现安全有效的跨链交易。

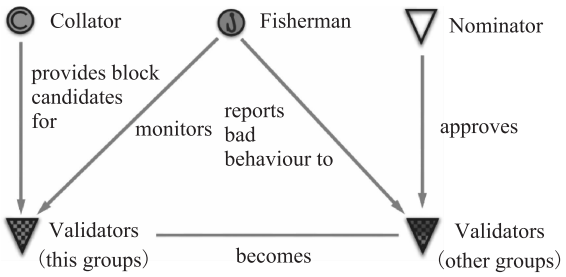


图 2 Polkadot 角色交互

为了更好地构建 Polkadot 生态系统，开发团队在开发过程中抽象出了 Substrate 框架，使用该框架可以方便地构建一条可直接接入 Polkadot 的平行链，当然该框架也可以用于独立区块链的开发。Substrate 框架的已经实现了共识机制、出块投票逻辑、P2P 网络、Wasm 虚拟机、智能合约原生执行等功能，目前已经有其他团队基于 Substrate 构建区块链，例如国内的 ChinaX。

Polkadot 的进度比 Cosmos 稍慢一步，目前处于 PoC-3 阶段，其第一个概念证明已经可以验证区块并实现状态转换，同时还实现了通过测试网发送 Dot 代币等功能。Polkadot 团队计划于 2019 年第三季度发布主网。

3.2.3 哈希锁技术

哈希锁技术的基本思想是交易双方维护一个设定相互操作的触发器（trigger）以保证双方操作的原子性，其典型代表就是闪电网络（Lightning network）以及雷电网络（Raiden Network），这两者都是状态通道技术的典型应用。

（1）闪电网络

闪电网络是状态通道的典型应用，是一个通过智能合约实现即时、高容量支付的分布式网络。其目的是实现安全的链下交易，但是其核心技术——哈希锁定技术使得它可以进行原子级的跨链交换。但是为了运行原子级的跨链交换，需要进行跨链交换的两条区块链上均支持闪电网络。交换双方在两条区块链上都开通闪电支付通道，形成环路通道；交换双方使用哈希时间锁定契约（HTLC）实现原子交换，具体来说就是交换双方将交换资产暂存至临时账户，通过相同的哈希原象以及设定的时间差达到两笔“付款”交易要么同时发生要么均不发生的效果。当然，并不是所有的跨链交换都需要建立新的通道，也可以通过已有的中间人通道来实现。

闪电网络最初并不是用来进行跨链通信的，但是由于其技术特性，可以很好地适用于跨链交易。2017 年 11 月，闪电网络实验室完成了比特币到莱特币的跨链交换，证实了闪电网络原子级跨链交易的能力。2018 年年初，BitUN 正式上线，它定义了闪电网络 2.0，构建了一个数字货币清算网络，试图实现更高效、安全的跨链资产管理。

（2）雷电网络

雷电网络与闪电网络一样，也是状态通道的应用，只不过闪电网络是针对比特币的，而雷电网络是以太坊上的链下扩容方案。其目的是利用链下状态网络对以太坊的交易能

力进行扩展。其基本原理与闪电网络类似，但是具体实现上有所差别：雷电网络的支付通道由智能合约控制而非多签名地址、雷电网络使用智能合约可以实现更多复杂的交换条件。

2017 年雷电网络团队在以太坊测试网络上发布一个早期版本后由发布了一款简洁版的测试版本——μRaiden（微雷电）。2017 年 11 月底，μRaiden 正式在以太坊主链上线，可以支持每秒 100 万笔交易。2018 年 3 月 Liquidity. Network 正式加入了雷电网络，其作为最新的以太坊项目，试图将交易从世界上第二大的最有价值的区块链转移到支付渠道上，从而允许网络可以支持被更多地采用和使用。此外，雷电网络还与 Share & Change，Smart Mesh，Grid + ，Tobalaba 等公司建立了合作关系，将在多个领域探索应用。

（3）Blocknet

Blocknet 是提供分布式应用程序和智能合约的链间基础设施，其目的是实现不同区块链之间的通信，让不同区块链用户之间的互操作及相应服务成为可能，简单来说，Blocknet 致力于构建“区块链互联网”。为了实现这个目标，Blocknet 设计了相应的分布式网络架构以及协议，Blocknet 包含三个核心组件：Xbridge——链间网络覆盖层、Xname——区块链路由、Xchat——P2P 数据传输；实现货币化的链间服务则需要三项核心基础设施服务：服务查找、链间消息传输以及分散交换。基础设施服务是核心组件的编排，如下图所示。

Blocknet 早在 2014 年就被提了出来，当时想实现的是一种虚拟货币为另一种虚拟货币提供服务，其在原子交换的基础上，增加了订单匹配、交易撮合等功能，实现去中心化跨链货币兑换。在经过功能拓展后，可用于跨链购买服务等。但是进度缓慢，最近透露的信息比较少。

3.2.4　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，其主要代表包括 Fusion 以及万维链。

（1）Fusion

Fusion 是一个加密金融层级的应用，其目的是构建一套区块链基础设施平台运行加密金融应用，在该平台上将通过智能合约自由的互相作用实现价值互操作，从而达到“银行”的效果。其核心技术是分布式签名技术，通过该技术用户可以将其拥有的各种数字资产映射到 Fusion 构建的公共区块链上，映射了诸多数字资产的 Fusion 公共区块链可以自由的进行不同数字资产的交换，并在用户申请提现时给予相应的支持。简单来说，就像不同区块链用户将不同数字资产存入“银行”，“银行”内的数字资产自由流通影响用户账户余额，用户从“银行”提款时以最后的账户余额为准。

Fusion 项目 2017 年开始启动，预计在 2019 年实现平台的建设。根据开发团队的规划，2018 年前三个季度应该完成合规划工作、核心团队建设、核心协议开发、智能浏览器以及核心钱包开发并完成协议安全性和效率的不断提升。按照计划团队应该在 2018 年

第二季度就上线了测试链和主链，但是现在查阅不到更多的相关内容，还需要继续跟踪。

（2）万维链

万维链时资产跨链、隐私保护以及智能合约三大特性结合的数字资产基础设施平台，其目的与 Fusion 类似：以去中心化的方式完成不同区块链网络的链接和价值交换，建立一个分布式的未来“银行”。其终极目标是建立一个分布式的数字资产金融基础设施。万维链通过分布式的方式完成不同区块链账本的链接及价值交换。它提出通用的跨链协议以及记录跨链交易、链内交易的分布式账本。公有链、私有链、联盟链均可以低成本地接入万维链，实现不同区块链账本的连接及资产的跨账本转移。任何机构和个人都可以再万维链中开设自己的业务窗口、提供基于数字资产的存贷、兑换、支付、结算等服务。通过万维链提供的基于区块链的基础设施的保障，更多人能够享受更加丰富的基于数字资产的金融服务。

万维链项目启动于 2016 年，同年进行了概念证明，2017 年 9 余额完成了 ICO。2017 年 11 月，万维链发布 Alpha 测试网，并在社区公开召集志愿者参与测试，此时已完成了交易隐私保护的核心开发工作，还进行了部分共识算法及钱包的开发；同年 12 月发布万维链 Bate 测试网。2018 年 1 月，万维链主网 1.0 宣布正式上线，该版本的万维链包含了以太坊的智能合约机制和 Monero 式的隐私交易功能；2018 年 7 月，万维链 2.0 对接以太坊宣布正式上线，该版本的万维链实现了跨链功能，开发团队还将进一步完善以实现良好的跨链生态。2018 年 9 月发布万维链 3.0 Aloha 测试网络，同年 10 月发布万维链 3.0beta 测试网络，开发团队表示最终实现万维链 3.0 将打破以太坊系列项目与比特币网络项目之间的壁垒，具体情况还需要继续跟进。

3.2.5 跨链技术比较

公证人技术的主要问题在于需要信任特定的公证人群体，这违背了区块链的设计初衷，而信任问题也将带来一系列的安全问题。这可能就是除了单独使用公证人技术的跨链项目较少的原因。但是公证人技术作为技术点被运用在各种跨链交易方案中，例如在属于侧链技术的 Rootstock（RSK）项目中，由于使用联合挖矿，前期 RSK 区块链的算力很有可能会低于比特币全网算力的一半，为了防止其他算力对 RSK 区块链的 51% 攻击，RSK 区块链的区块打包借助公证人技术。

锚定某一特定区块链的侧链技术均是通过 SPV 证明验证跨链交易的有效性，理论上支持所有区块链的跨链交换以及跨链资产转移，但是需要为每一条主链、侧链的组合设计实现中继，实现复杂且难度巨大，可拓展性较差。不锚定特定区块链的侧链技术则是基于侧链技术的理念建立跨链基础设施，可以解决狭义侧链技术存在的诸多问题，但是实现复杂，目前没有真正上线的项目可以参考。

哈希锁技术是保证跨链交易原子性的理想方案，但是仅使用哈希锁技术的跨链方案应用范围较为狭窄仅限于跨链转账领域，无法满足其他的跨链需求。与公证人技术一样，哈希锁技术也可以被用在其他跨链方案中以保证跨链交易的原子性。

分布式私钥控制技术提出的将不同区块链的资产映射到同一条区块链上后实现的多

币种智能合约，目前实现的与哈希锁技术一样，还只是单纯地进行资产交换的交易出发，还不能完成更加复杂的跨链互操作。如果后续无法进一步增强多币种智能合约的设计，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。表 1 为当前主要跨链技术的比较。

表 1　跨链技术比较

	公证人技术	侧链技术	哈希锁技术	分布式私钥控制技术
互操作性	所有	使用了中继的区块链	交叉依赖	所有
信任模型	多数公证人诚实	链不会失败或收到 51% 攻击	链不会失败或收到 51% 攻击	链不会失败或收到 51% 攻击
实现难度	中等	难	容易	难

3.3　区块链智能合约

智能合约是运行于区块链上，并通过交易触发执行的程序。智能合约研究主要包括合约编码、合约性能、合约安全性以及合约隐私问题。

3.3.1　智能合约性能与安全

Loi Luu[32]等研究了在类似于加密货币的分布式网络中运行基于以太坊智能合约的安全性问题，通过理解底层架构的平台的分布式语义方面存在细微的差距提出增强以太坊操作语义的方法，列举以太坊智能合约运行过程中的可能出现的漏洞，构建了名为 Oyente 的执行工具来发现潜在的安全漏洞。Stefano Bistarelli[33]等人通过收集了大量使用 Solidity 语言编写的验证智能合约，并分析了他们的代码；对 Solidity 编译器进行了类似的研究以确定操作码在实践中所发挥的重要作用。Atzei，Bartoletti 和 Cimoli 提供了对以太坊智能合约的攻击调查[34]，他们定义了可能导致不同漏洞的常见编程错误，并对其进行分类。这项研究工作为程序员提供了有用的指导，以避免由于程序员由于缺乏对区块链的了解而导致的安全问题。Delmolino 等人提出了按部就班编写智能合约的步骤[35]。Anderson[36]等人提供 2015 年 8 月至 2016 年 4 月以太坊区块链交易的定量分析。他们的调查侧重于智能合约，特别关注僵尸合同。他们对合同执行安全分析，以检查未受保护的命令（如 SUICIDE）的使用情况，同时还检查了协议代码中的相似之处，分析了智能合约代码部分相似的原因。Maurice Herlihy 在[37]文中探讨了由于并发控制等因素引起的智能合约的问题，Bhargavan 等人[38]利用形式方法来分析和验证智能合同的正确性，而 Bigi 等人[39]则更进一步，将形式方法与博弈论技术相结合来验证智能合同。在文献［40］中，作者做出了系统的映射研究；从技术角度收集所有与智能合同相关的研究，得出未来的研究方向。由于区块链的不变性，智能合同在部署到区块链后不能更改或终止，为了解决这一问题，Marino 等人[41]提出了一套允许更改或终止智能合同的标准。当前的智能合同是基于程序语言，如 Solidity。在过程语言中，代码是作为一系列步骤来执行的，因此，程序员必须指定应该做什么以及如何做。这使得用这些语言写智能合同的任务既

麻烦又容易出错。为了解决这个问题，Idelberger 等人[42]建议使用基于逻辑的语言，而不是过程语言。一些智能合同需要来自区块链以外的信息，问题是不能保证外部来源提供的信息是可信的。为了解决这个问题，F. Zhang 等人[43]构建了一个 Town crier 解决方案，作为外部和智能合同之间的可信第三方，为智能合同提供经过认证的传送数据。

3.3.2 智能合约的优化

针对智能合约存在的隐私、安全、性能以及统一标准等问题，随着区块链技术的研究进展和突破，国内越来越多的学者也在关注着智能合约的优化研究。如王璞巍等人[44]通过对现有智能合约的实现进行分析和对比，提出了一种面向合同的智能合约的形式化定义方法，并且给出了参考实现。在构建智能合约的研究中文献［45］使用领域特定语言（DSL）和区块链技术构建去中心化的点对点分布式模型，实现智能合约的可编程性和执行环境的可信性。在区块链技术应用中，文献［46］实现了 Fabric 的跨境汇款追踪平台，并详细给出了其智能合约的主体结构以及方法级权限控制，是技术与应用的真正结合。为提高智能合约的鲁棒性以及抗击打能力，文献［47］通过提出基于安全多方计算（SMPC）的智能合约框架、面向线性秘密共享的公平 SMPC 算法设计、以及非阻塞信息传递接口技术明确定义了基于多方计算的智能合约模型，通过规范基于 SMPC 的智能合约执行流程、语言结构，增强了智能合约的安全执行。针对市面上的智能合约大多是面向开发者且过分依赖开发平台以及开发技术的不友好问题，文献［48］开发了通过安卓端即可接入合约网络的智能合约平台。为便于档案数据的记录和有效保存，使得档案数据不被篡改，文献［49］通过智能合约和数字签名技术实现了数字档案馆的身份认证和档案所有权的确定来实现基于区块链的档案数据保护与共享方法。文献［50］通过定义新的操作码表示字节压缩，进行部署后有效地节省智能合约的存储空间。为了保障智能合约的隐私性，文献［51］中，引入盲签名技术和改进 PBFT 算法来提高智能合约的隐私保护。对于智能合约的管理和查找，文献［52］引入代码分类思想来对智能合约进行分类管理并在此基础上提出基于语义嵌入模型与交易信息的智能合约自动分类系统。针对区块链性能的研究，以及区块链的吞吐量的研究，文献［53］提出了以太坊平台上基于智能合约的可信存证系统，提高了数据存储的安全性和效率，保障数据不被篡改和丢失。

总体来看，有关智能合约的研究还处于起步阶段，特别是智能合约的优化方面，还没有形成有效的方法。

3.4 区块链安全性保障

国际上，NEC 欧洲实验室、美国康奈尔大学、罗马尼亚巴比什-波雅依大学、德国明斯特大学、美国波士顿大学、以色列希伯来大学、美国麻省理工学院、新加坡国立大学、澳大利亚纽卡索大学、美国普林斯顿大学、西班牙巴塞罗那自治大学、英国爱丁堡大学等团队在区块链安全性方面进行了一定的研究。这些学者主要关注于数据安全、网络安

全、共识安全、智能合约安全等角度研究区块链技术的安全性和稳定性。在国内，区块链安全的工作主要体现在区块链相关标准研制工作，推出了一系列相关标准。区块链标准化能打通应用通道，防范应用风险，提升应用效果，对于解决区块链安全发展问题、推进区块链安全应用起到重要作用。我国相关标准化组织、联盟协会、研究机构等已将区块链标准化提上议事日程，开展了组织建设、标准预研等一系列工作，并取得了一定进展。

3.4.1　数据安全方面

区块链的数据存储结构决定了区块链难以篡改的特性，同时也从客观上增加了有害信息上链的风险，以及敏感数据上链后的隐私保护问题。

（1）有害信息上链问题

区块链数据的难以篡改特性使得区块链上的数据难以通过传统的方式进行修改和删除，增加了有害信息上链的监管难度，为信息管理提出新的挑战。因此，一旦暴恐、色情等有害信息被写入区块链中，不但可利用其同步机制快速扩散，也难以进行修改、删除。尽管理论上可采取攻击手段制造硬分叉、回滚等，但实施代价高、难度大，给信息内容管理带来新的挑战。在 2018 年 3 月，德国研究人员就曾在比特币区块链中发现超过 274 份儿童色情网站的链接和图片，经查证，为恶意用户通过将有害信息编码为比特币交易信息，注入区块链中的行为。

对于公有链，例如比特币区块链，应对策略主要是通过 Reid、Meiklejohn 等学者提出的比特币地址之间的关联关系追踪有害信息的来源。对于联盟链或私有链，应对策略主要是增加审核机制，探索对链上违法信息审核与用户隐私保护需求间的平衡。

（2）隐私数据保护问题

区块链中开源的共享协议可使数据在所有用户侧同步记录和存储，对攻击者来说，能够在更多的位置获取数据副本，分析区块链应用、用户、网络结构等有用信息。例如区块链的典型应用之一比特币，其每一笔交易都会公开记录在区块链账本上，任何人都可以查阅。Reid、Meiklejohn 等学者研究发现历史交易中输入地址、输出地址和找零地址之间的关联关系可以推测比特币用户之间的关联关系。区块链的应用尤其是金融行业对隐私保护会更加注重。隐私问题成为区块链应用落地的主要保障之一。

隐私数据链外存储，可以公开的部分数据存放在分布式账本上。根据不同隐私需求的数据分别存放在不同的分布式账本上。隐私数据加密保护，只有相关方才能够解密查看。使用群签名对身份匿名，将区块链上交易用户的身份隐匿起来。

3.4.2　网络安全

（1）P2P 网络安全漏洞

P2P 网络为对等网络环境中的节点提供一种分布式、自组织的连接模式，缺少身份认证、数据验证、网络安全管理等机制。攻击者可以自由发布非法内容，传播蠕虫、木马、病毒，甚至实施分布式拒绝服务攻击（DDoS）、路由攻击等，具有不易检测、传播

迅速等特点。Donet 等学者研究指出，弱连接和不正确的协议将会增加 IP 网络中的传播延迟，并致使某些系统中的区块链分叉。尽管区块链是一个完全分散的系统，但在实际中很难建立均匀的节点间连接。Gervais 等学者的研究结果表明，攻击者通过控制多个区块链节点阻止矿工挖矿，从而获取更多收益。

P2P 网络的安全漏洞是一个系统工程，而且 DDoS 等网络攻击越来越智能化，从而导致网络安全漏洞引发的攻击难于应对。可以通过安装专门的抵御 DDoS 防火墙等安全设备来增加攻击者的攻击成本，从而降低此类攻击发生的概率。

（2）节点的网络拓扑

节点的网络拓扑结构会为攻击者寻找攻击目标并实施攻击创造便利。攻击者可以采用主动式注入报文或者被动式监听路由间传输的数据包来监测网络拓扑结构，很容易获得目标节点的路由信息并控制其邻居节点，进而实施攻击。Francisco 等学者研究发现“日蚀攻击”就是攻击者利用节点间的拓扑关系实现网络隔离的一种典型攻击方式。其基本思想是攻击者通过网络拓扑控制目标节点的数据传入传出节点，限制目标节点与外界的数据交互，甚至将目标节点与区块链主网络隔离，使目标节点仅能接收到攻击者传输的消息，导致目标节点保存的区块链视图与主网区块链视图不一致，破坏局部的一致性。“日蚀攻击”可作为其他攻击的基础。当网络出现阶段性区块链分叉竞赛时，攻击者利用日蚀攻击迫使目标节点将计算资源浪费在无效的区块链上。攻击者还可以针对算力优势节点实施“日蚀攻击”，实现算力的分离，影响挖矿奖励的分配，降低网络中的有效算力，进一步降低自私挖矿和双重支付等攻击的难度。

区块链网络用户通过建立唯一标识的、可验证的数字身份，合理设置对等网络节点的链接数目、连接时长、地址列表大小、更新频率、更新机制、链接选择机制、异常检测机制等。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。

3.4.3 共识安全

共识机制就是区块链交易达到分布式共识的算法，它用来使得区块链达到一致的状态，它实现了驻留在网络的每个节点上的许多副本。共识机制应该将一个状态与其余状态分开，以便该状态可被整个网络所接受。共识机制是保障区块链系统不断运行并不断发展的关键。良好的共识机制有助于提高区块链系统的性能效率，提供强有力的安全性保障，支持功能复杂的应用场景，促进区块链技术的拓展与延伸，各种典型的区块链共识机制对比如表 2 所示。

表 2 典型的区块链共识机制对比表

共识机制	能耗	出块时间	安全性	一致性	去中心化程度	应用场景
PoW	巨大	长	面临 51% 算力攻击	易分叉，没有最终性	完全	公有链无信任环境
PoS	低	较短	解决了 51% 算力攻击。中间步骤较多，易产生安全漏洞	易分叉，没有最终性	完全	公有链无信任环境

（续）

共识机制	能耗	出块时间	安全性	一致性	去中心化程度	应用场景
DPoS	低	秒级	解决了51%算力攻击。中间步骤较多，易产生安全漏洞	没有最终性	部分	公有链无信任环境
PBFT	较低	较慢	安全性较低，只能容忍1/3的恶意节点	具有最终性，不会分叉	低	联盟链、私有链可信任环境
类BFT	较低	快	安全性较低，只能容忍1/3的恶意节点	具有最终性，不会分叉	低	联盟链、私有链可信任环境
SCP	较低	快	渐进式安全，参数可根据实际情况调整以抵御拥有强大算力的对手	具有最终性，不会分叉	低	私有链完全信任环境

（1）双重花费攻击

2012年，Ghassan等学者提出双重花费攻击，它是针对比特币系统的一种特有攻击。该攻击分为两种类型：

第一种攻击：攻击者使用一笔金额，同时和多个对象进行交易。若这些交易对象在这笔交易未被记录进合法区块链的情况下，完成了交易，则攻击者达到了双重消费甚至多重消费的目的。尽管在攻击者发起的多笔交易中，最终只会有一笔交易认定为合法并记录入区块链中，但交易对象完成了交易（如已经把攻击者购买的货物发给攻击者），攻击者已经从这次攻击中受益。

第二种攻击：攻击者利用自身的算力发起双重花费攻击。攻击者利用同一笔金额，同时和两个交易对象进行交易，如交易A和交易B。其中一笔交易A被确认记录进区块链，使得交易A完成。由于攻击者拥有强大的算力，他将交易B记录在私人区块链里，并挖出一条比合法连更长的链，促使交易B也得到了确认，并完成交易B。

在双重花费攻击中，第二种类型攻击的危害性更大。这是由于，对于第一种类型攻击，交易者只需要在交易得到确认6次以上，再完成交易就可以避免；对于第二种攻击，由于攻击者将“非法”交易加入私人区块链，并且最终这条链被认定为合法，相当于更改了区块链中的这笔交易（将交易A更改为交易B），这种对区块链数据进行篡改的行为严重影响了区块链的完整性。

（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。”中本聪在发明比特币时就提及了51%攻击。51%攻击是指在攻击者拥有超过整个网络一半能力的情况下，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，完成双花并获得利益。攻击者实施51%算力攻击的动机：一是可以完成对自己交易的双花，骗取交易接收方的利益；二是可以控制最长链的生成过程，从而获得区块奖励。51%算力攻击曾一度被认为是难以达到的。然而随着矿池的出现，一个名为GHash. IO的矿池就曾经在2014年6月拥有全网51%的算力；因此51%算力攻击的威胁始终存在，

并且是可能发生的。

（3）自私采矿攻击

Eyal 和 Sirer 学者认为如果存在一群自私的矿工（矿池），采用自私的采矿战略并获得成功，就可能会使诚实矿工的工作无效。这种自私采矿攻击表现为：一个恶意的采矿池决定不发布它发现的块，进而创建一个分叉，因此网络中就存在由诚实矿工维护的公共链和恶意采矿池的私人分叉，恶意采矿池在此私人分叉下继续进行挖掘，当私人分叉比公共链长的时候，恶意采矿池就发布该私人分叉，由于该分叉是当前网络中最长的链，因此会被诚实的矿工认定为合法链，所以原公共链及其包含的诚实数据将被丢弃。研究结果表明，一般情况下恶意采矿池采用自私采矿策略将获得更多的收益。

（4）扣块攻击

Courtois 和 Bahack 学者通过实际的实例分析，发现恶意矿工也可以从“扣块攻击”中获利。在扣块攻击中，某些已加入联合采矿池的恶意成员不布任何挖到的区块，从而降低了采矿池的收益，浪费了其他成员提供的算力。这种攻击也被称为“破坏（Sabotage）”攻击，通常恶意矿工不会有任何收益，但“扣块攻击”的主要危害是浪费矿池算力资源，减少矿池收入。

从上面的分析可以看出，“扣块攻击”会使矿工和采矿池都受不同程度的损失，相对于矿工很低的成本，采矿池的损失则比较大。从利益方面考虑，发起“扣块攻击”多为互相竞争的采矿池，一般矿工则较少。尽管“扣块攻击”理论上成立，但是实际上实施该攻击却很难。这是因为“扣块攻击”的代价非常大，这一点与比特币的 51% 攻击相似，即发起该攻击必要的基础是需要掌握巨大的算力，所以基本上“扣块攻击”在现实中极少发生。

（5）贿赂攻击

Chepurnoy 学者提出攻击者可以通过高额奖励的方式鼓励矿工在包含攻击者发起的交易链上进行挖矿。首先，攻击者购买某个商品或服务，商户开始等待网络确认这笔交易；若此时攻击者开始在网络中首次宣称，对目前相对最长的不包含这次交易的主链进行奖励；当主链足够长时，攻击者开始放出更大的奖励，奖励那些在包含此次交易的链条中挖矿的矿工；当六次确认达成后，放弃奖励；最后当奖励到手时，放弃攻击者选中的链条。因此，只要此次贿赂攻击的成本小于奖励或者服务费用，此次攻击就是成功的。值得注意的是该攻击对 PoW 机制基本无效，因为在 PoW 机制中，贿赂攻击就需要贿赂大多数矿工，因此成本极高，难以实现。

3.4.4 智能合约安全

智能合约是合约层的核心，是一种可自动执行的数字化协议，包含相关代码和数据集，部署在区块链上，也是可按照预设合约条款自动执行的计算机程序。智能合约最早由学者 Nick Szabo 提出，后经以太坊重新定义，并建立完整的开发架构。智能合约大多数操作的对象为数字资产，因此智能合约具有高风险性。本部分从编写安全和运行安全两部分进行安全问题和解决方案。

（1）编写安全

侧重智能合约的文本安全和代码安全两方面。文本安全是实现智能合约稳定运行的第一步。智能合约开发人员在编写智能合约之前，需要根据实际功能设计完善的合约文本，避免由合约文本错误导致智能合约执行异常甚至出现死锁等情况。代码安全要求智能合约开发人员使用安全成熟的语言，严格按照合约文本进行编写，确保合约代码与合约文本的一致性，且代码编译后没有漏洞。

（2）运行安全

涉及智能合约在实际运行过程中的安全保护机制，是智能合约在不可信的区块链环境中安全运行的重要目标。运行安全指智能合约在执行过程中一旦出现漏洞甚至被攻击，不会对节点本地系统设备造成影响，也不会使调用该合约的其他合约或程序执行异常，包括模块化和隔离运行两方面。模块化要求智能合约标准化管理，具有高内聚低耦合的特点，可移植，可通过接口实现智能合约的安全调用。遭受攻击后的异常结果并不会通过合约调用的方式继续蔓延，保证了智能合约的可用性。隔离运行要求智能合约在虚拟机等隔离环境中运行，不能直接运行在参与区块链的节点本地系统上，防止运行智能合约的本地操作系统遭受攻击。

（3）虚拟机的安全漏洞

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中，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，单个虚拟机漏洞的影响很可能影响到整个系统。

3.4.5　安全相关标准

在密码算法和签名标准方面，我国研究基础较好，据赛迪区块链研究院统计，截至2018 年 6 月底，我国已出台包括 SM2 椭圆密码算法、SM3 杂凑算法、SM9 标识密码算法在内的 19 项密码算法和数字签名方案、PKI 组件最小互操作规范、电子签名格式规范等 20 项签名方案。在底层框架技术标准研制方面，相关工作已经有序展开，目前在区块链基础标准、可信和互操作标准、过程和方法标准等方面有一些初步成果，如 2017 年 5 月，中国电子技术标准化研究院发布区块链标准《区块链和分布式账本技术参考架构》，对区块链的概念、主要参与者、核心功能组件等进行了详细规定。2017 年 12 月，中国区块链生态联盟发布了《中国区块链生态联盟团体标准管理办法（试行）》。2018 年 3 月，工业和信息化部宣布筹建全国区块链和分布式记账技术标准化技术委员会。2018 年 4 月，中国区块链生态联盟宣布成立《区块链平台一般技术要求（暂定名）》和《区块链企业服务能力一般要求（暂定名）》标准起草工作组，推动标准研制工作，这些标准中均有对区块链安全的描述。2018 年 4 月，全国信息安全标准化技术委员会开展了对《区块链安全技术标准研究》项目立项评审工作。据赛迪区块链研究院统计，截至 2018 年 6 月，有 20 多项底层平台测评标准处于在研状态。

3.5 区块链监管与隐私保护

3.5.1 区块链监管

国内外，对区块链可监管性的研究主要基于对公有链的监管，主要针对以比特币、以太坊等为首的数字货币。数字货币作为区块链中最典型的应用，有着较大的市场价值和潜力。因此，对数字货币的监管引起了国内外政府机构和研究人员的广泛关注。本部分从政策角度和技术角度进行分析国际上区块链监管的现状。

（1）政策角度

对于以比特币为代表的匿名数字货币，很多国家都制定了较为严厉的禁令，防止相关的违法活动的发生。2015 年美国商品交易期货委员会并没有承认比特币等数字加密货币的货币地位，而是将它们定义为商品。日本、加拿大等国家将一些比特币交易活动定为非法。2016 年美国区块链公司 R3 发起了同名区块链联盟，包括高盛、汇丰等 80 多家银行、金融机构和监管机构加入其中。R3 最新的研究报告指出金融机构需要的是一个自主可控的系统，要在保障交易隐私的基础上对监管可见。2018 年欧盟计划发布区块链技术标准和众筹法规等特定草案，建立区块链技术的共同标准。

2019 年 1 月 10 日，国家互联网信息办公室发布了《区块链信息服务管理规定》，要求区块链信息服务提供者事前设立监管平台；事中及时发现问题源、处理违法违规信息、控制事态发展、消除不良影响；事后根据监管体系追溯违法来源。由于比特币、以太坊等公有链自组织、跨国界等特点，使得很难从法律层面对这些公有链进行监管。

（2）技术角度

对于区块链技术各国都以规范和监管为主。国外的研究人员对以比特币为首的数字货币的匿名性和区块链隐私保护展开研究，取得了许多研究成果。这些研究为实现区块链监管提供了一些技术上的指导和支持。公有链的账号匿名性使得人人都能生成大量的账号地址，而这些地址的生成并不需要提供和个人信息相关的内容。然而，卢森堡大学等高校的研究人员指出，攻击者可以利用网络上公开的背景知识，或对比特币网络层的交易传播信息进行监听，可以找到地址背后的用户身份及其对应的 IP 地址。伦敦大学学院的研究人员提出了基于匿名数字货币 Zcash 的启发式聚类方法，并以 Shadow Broker 为例，介绍了如何利用上述技术，结合网络上的公开信息，实现对 Zcash 中违法犯罪行为的监管。英国、新加坡、日本和加拿大推广监管沙盒，将区块链风险防控在一定的范围内。

3.5.2 区块链隐私保护

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。

（1）网络层的隐私保护机制

通过分析网络层的报文数据和攻击手段，可以得出攻击者主要是通过监听网络层信息来搜集交易隐私和身份隐私。因此，网络层防御机制的重点是增加攻击者搜集网络层数据的难度，让攻击者不能从网络层中提取到有用的信息，现有的防御机制可以分为3类：

1）限制网络接入。对区块链中的节点进行授权控制，没有得到授权的节点无法接入网络，不能获得交易信息和区块信息，这将从根本上增加网络层攻击的难度。但是，这种方法需要修改区块链的本身运行机制，目前主要运用在私有链或者联盟链的架构中，例如超级账本联盟链的架构就是需要CA认证的节点接入机制，而公有链中，如以太坊和比特币等知名区块链项目，不适合做身份认证形式的网络限制。

2）恶意节点的检测和屏蔽。限制接入的方式不适合在公有链系统中，那么在公有链架构中，不能直接限制节点接入网络，但是可以采取检测采样的机制，发现恶意节点并加入黑名单，阻止恶意节点继续搜集敏感信息。研究人员曾提出一种基于行为模式聚类的恶意节点检测方法，能够快速定位恶意节点，消除恶意节点带来的隐私泄露隐患。

3）数据混淆。为了阻止攻击者通过发现网络拓扑获得身份隐私信息，一些研究人员提出可以将区块链运行在具有隐私保护特性的网络上，保证攻击者很难发现发送者的真实IP，从而无法从网络层面分析用户的行为和地理位置。

（2）交易层面的隐私保护机制

通过分析交易层的攻击方法，可以得到攻击者主要是通过分析公开的区块链交易数据获得隐私信息。因此，交易层保护机制的侧重点是在满足区块链正常运行的基础上，防止恶意节点获得准确的交易数据，或者限制其无法在少量的数据中分析得到有价值的信息。目前，学术界研究人员已经提出多种交易层的隐私保护方案，此处，我们将不同的保护机制按照分布式数据库隐私保护的分类方法进行3种主要的分类：

1）数据存储失真。在数据存储时，通过将交易内容的部分数据进行混淆，使攻击者无法获得准确的数据，增加分析难度。这种方案的难点混淆方法的效率，必须保证在不破坏交易结果的条件下，防止攻击者发现不同地址之间的交易关系。

2）数据加密。通过将交易信息加密，使攻击者无法获得具体的交易信息，从而无法开展分析。这种方案的难点在于实现加密的同时，必须保证原有的验证机制不受影响，例如加密数据在链上存储时如何保证双方的交易信息能够被矿工或其他人员确认并验证有效性。

3）限制发布。通过发布少量或者不发布交易数据，减少攻击者能够获取到的信息数

量，从而增加攻击难度，本方法难度在于如何保证在限制发布的同时，保证数据本身的完整性和一致性不被破坏。

（3）应用层面的隐私保护机制

通过分析应用层面的攻击方法，可知看出攻击者主要是利用用户不规范的操作和区块链服务商的漏洞搜集交易隐私和身份隐私。因此应用层防御机制的重点是从用户的角度提升保护能力。用户可以采用的防御方法通常有两种：

1）区块链应用中引入隐私保护方案。比特币是区块链技术在数字货币领域的第一个应用，在隐私保护方面存在明显缺陷。攻击者可以从交易和网络两个层面分析用户身份。在这种背景下，出现了许多隐私保护效果更好的货币，例如零币（Zcash）等。Zcash 是目前隐私保护效果最好的数字货币，通过采用 zk-SNARKs（简洁的非互动性零知识证明）技术，能够在满足验证和共识机制的条件下隐藏区块链交易的发送方、收款方乃至交易的金额，其设计中有不同级别的隐匿方案，最高级别的方案既可以保证收款方身份不可见，也可以保证接收方身份的不可信，同时隐藏交互的金额。新型的数字货币采用密码学技术保护交易数据，相对比特币能够更好地保护用户的身份隐私和交易隐私。

2）使用具有隐私保护机制的区块链程序。不同的区块链程序在隐私保护方面具有不同的特点，需要采用针对性的保护方法。以比特币为例，冷钱包通过将秘钥离线保存，能够有效防止黑客攻击，但是有可能出现存储介质丢失和被盗带来的安全风险，隐私保护的关键是保护存储介质的安全性，可以采用多重备份、加密存储等机制保护存储介质的安全。同时，需要提高用户对应用层面安全操作的意识，例如不随意授权、离线保存、不随意暴露私钥等，应用程序也应该做到不收集用户隐私信息。

3.6 区块链技术应用

区块链技术的应用主要表现在金融行业、供应链管理、物联网、版权保护、医疗行业等。区块链技术应用国际研究现状呈现出以传统大公司为主，初创企业为辅的趋势，大公司布局整个生态链及基础平台，其在物联网、供应链、版权保护、医疗等多个行业都有涉及，而小公司注重某个行业的具体应用，以不同角度切入区块链领域。传统企业与初创型企业双向发力，不断促进区块链在行业内的广泛普及和加速融合。

3.6.1 金融行业

在金融领域，区块链已应用于股权众筹、P2P 网络借贷和互联网保险等商业模式。证券和银行业务也是区块链的重要应用领域，传统证券交易需要经过中央结算机构、银行、证券公司和交易所等中心机构的多重协调，而利用区块链自动化智能合约和可编程的特点，能够极大地降低成本和提高效率，避免烦琐的中心化清算交割过程，实现方便快捷的金融产品交易。为了促进区块链技术及其应用的发展，各种类型的区块链产业联盟出现。其中最有影响力的是 R3 区块链联盟，其汇集了 40 多家世界领先的金融机构，包括美国银行、花旗银行、摩根士丹利投资公司、德意志银行和 Barclays 银行[61]。

Barclays 银行和一家以色列公司完成了世界上第一笔基于区块链的交易，这笔交易保证了从爱尔兰公司 Ornua 出口到塞舌尔贸易公司的价值约 10 万美元的奶酪和黄油产品。这笔交易是在 Barclays 银行合作公司 Wave 设立的一个平台上完成的。使用区块链技术，一笔交易的处理时间可以从 7 ~ 10 天降低到 4 小时。

瑞士联合银行（United Bank of Switzerland，UBS）还计划建立一个使用分布式账本的贸易金融系统，可以简化全球进出口贸易。在当前的大型交易中，当产品仍在运输的过程中时，买方银行可以使用信用来排查卖方的信用风险。区块链技术可以将这一过程编程到智能合约当中，降低信用处理时间，降低操作风险。

3.6.2　供应链管理

供应链由多个节点构成，其运行过程中，不同节点间需要进行大量信息交互。供应链运行过程中产生的数据零散地保存在各节点的私有系统内，无法保证数据公开透明，这会导致多方面问题：①节点信息无法实现共享，导致上游节点维持过多库存以应对下游节点需求，使生产、库存管理和营销风险大幅增加，反之则可能导致供应商风险增大；②信息流动不畅导致供应链上的各节点无法第一时间掌握相关情况，从而影响供应链效率；③当供应链各节点出现纠纷时，生产信息的低可追溯性将导致调查追责过程遇到的困难大大增加；④中小物流企业面临的融资难问题。

区块链能使供应链上的信息保持互通，各成员节点能第一时间掌握相关情况，由此提升供应链管理的整体效率。同时，各节点能获取准确的交易信息，所有成员节点都是供应链上全部信息的所有者，在此基础上开展生产活动，可降低供应商风险，提升供应链稳定性。区块链的可追溯、不可篡改性，不仅保证数据准确，还能保证交易可溯源。区块链可解决信息不对称问题，完善信用评价体系，助力中小物流企业走出融资难困境[57]。

在各国政府及相关企业的推动下，不少区块链在物流供应链领域的应用项目得以开展。IBM 采用区块链技术来追踪卡车位置跟货物来源可提高运输过的程透明度，通过 IBM 区块链技术和 IBM Watson 来追踪卡车及其货物的来源和位置，IBM 区块链技术解决方案记录了处理货物的交易和信息，物联网传感器将跟踪货物的行程，以及卡车上可用的空间，并将这些数据记录在所有相关方面的区块上。该区块链技术解决方案与 IBM Watson 物联网系统集成，以检查天气和温度等因素，从而估算行程和估计交货时间[59]。

由阿里巴巴、IBM 等来自全球 9 个核心国家的核心研发团队率先提出了区块链即服务（Blockchain-As-A-Service）的设想和理念，旗下产品唯链致力于货运资产追踪管理，其提供的物流行业解决方案利用区块链技术和 IoT 技术，在物流关键环节中，由各个参与方采集关键数据并在唯链雷神区块链上存证。该方案支持将物资管理的维度精确到每一件货品，记录每一件货品的信息和流转过程，为新型的物流、商业模式提供了可能。此外，根据区块链上的存证信息，还能够提供各种数字化增值服务[73]。

雀巢联合区块链平台 OpenSC，开展新区块链供应链追踪试点，雀巢将与区块链平台 OpenSC 合作，共同开发分布式分类账系统。该项目首先将追踪新西兰农场运往中东雀巢

公司的牛奶，然后扩大到美洲棕榈油生产。收集价值链上每个步骤的数据记录在开放平台，为消费者提供可独立核实的数据，推动市场透明化。同时，该机制将提高食品安全性并改善质量控制[75]。

3.6.3 物联网

许多国际知名公司如 IBM 已经在物联网领域投入了海量资源，区块链技术被用来解决其中一些核心问题。传统的中心化机制对于潜在数量在百亿级的物联网设备而言是低效甚至不可用的。在解决节点间信任问题方面，中心化的解决方案并不现实。区块链技术提供了一种无需依赖某个单个节点的情况下创建共识网络的解决方案。基于区块链的物联网应用，每个物联网设备都能够自我管理，无需人工维护。只要物联网设备还存在，整个网络的生命周期就可以很长，并且运行开销可以明显降低。例如智能家居，所有智能家居的联网设备都能够自动地和其他设备或外界进行活动，只能电报能够通过调节用电量和使用频率来控制电费等[57]。

国内众多企业开展了物联网和区块链融合的行业应用，比如在渔业、食品溯源、能源等领域，表明区块链作为物联网应用的基础技术已经广受认可。如在渔业领域，庆渔堂公司采用物联网和区块链技术帮助农民进行水质监控，降低种养过程中的风险，提高生产效率，实现农业科技授信贷款、农业科技保险、供应链溯源、农产品溯源及品牌营销等。在食品安全溯源领域，食品安全区块链实验室 Akte 致力于打造基于物联网和区块链技术的食品防伪溯源生态，通过打通物联网智能终端的信息采集与区块链的数据链路，保障食品可溯源和信息真实可信。

腾讯基于 TBaaS 基础平台已经在物联网领域率先提出多个应用案例，比如智能制造，智能电网等方面。针对智能制造行业的痛点问题，区块链与物联网结合，使得智能设备以更加安全可靠的形式进行管理，并实现物联网的高级目标，即支付与费用的结算，形成价值流通的网络。

3.6.4 版权保护

以“视觉中国”为主的网络版权侵权事件引起了公众的关注，网络版权保护成为大家关注的重点。网络媒体、自媒体数量每天产生海量的内容，那么，原创者如何保护自己的版权，如何证明作品是自己的，并且如何授权其他人合法使用自己的作品，这都是难以解决的问题[63]。

从目前来看，网络版权保护中最大的难点就在于用户取证困难、取证成本高，且取证周期长，这也正是阻碍网络版权保护发展的痛点之一。基于这些网络维权中常见的问题，华智博通就设计推出了自主研发的网络维权工具“版权宝”。基于比原链开发在原创新闻的自证（原创上链）和侵权证据的获取（证据上链）两个业务流程中使用了区块链技术，保证用户在网络侵权行为发生之时及时取证、固证，解决取证难、取证贵、取证周期长的难题。

微软与国际知名咨询机构安永联合推出保护版权的区块链工具，即利用区块链技术

为作者、软件开发人员和其他创意制作人收取版税，该项目旨在简化目前追踪和收取版税的流程。数字版权和版税交易的规模、复杂性和数量，使得这成为区块链技术的完美应用场景。区块链可以处理数字版权所有者和许可证颁发者之间的每一份具有特殊性的合同，可以通过可扩展、高效的方式为参与者提供查账系统[71]。

3.6.5　医疗行业

目前医疗数据领域数据收集无统一标准，无法形成患者完整画像。网络安全压力大，获取信息成本降低。数据分类模糊，缺乏价值数据等级。医疗数据行业完全能够利用区块链技术的优点，把不准确和存在差异影响的医疗数据记录上链[78]。

2017 年 4 月左右，IBM 推出了自己的区块链即服务 BaaS，该项目关注医疗等方面。2019 年 1 月，IBM 宣布一项与 Aetna、Anthem、HCSC（Health Care Service Corporation）和 PNC Bank 的新合作，通过使用区块链技术设计和构建网络，提高医疗保健行业的透明度和互操作性[79]。这项合作的目的是创建一个具有包容性的区块链网络，使医疗生态系统中的大部分成员都能够在一个高度安全的共享环境中受益[80]。

2018 年 8 月 17 日，阿里健康与常州市合作“医联体 + 区块链”试点项目。该项目是国内首个基于医疗场景的落地应用，运用区块链技术，应用于常州市医联体底层技术架构体系中，并已实现当地部分医疗机构之间安全、可控的数据互联互通，用低成本、高安全的方式，解决长期困扰医疗机构的“信息孤岛”和数据安全问题[84-85]。目前该项目已经取得了一定成效，以分级诊疗就医为例，居民在就近卫生院体检，通过在区块链上的体检报告分析，筛查出心脑血管慢性病高危患者，5% 左右的需要转诊患者可以由社区医生通过区块链实现病例向上级医院的授权和流转，上级医院的医生在被授权后能够迅速了解病人的过往病史和体检信息，病人无需做不必要的二次基础性检查，提升效率，降低成本。

4　发展趋势与展望

区块链目前已经应用到多个领域，用来解决一些实际问题，保证上链数据的防篡改、可追溯。但是区块链本身存在的一些问题仍需考虑，例如：性能瓶颈、数据存储、资源消耗等问题。针对不同的应用场景，需设计不同的区块链架构和业务模式来满足当前场景的需求，助力区块链在各个垂直行业发挥作用。

4.1　可扩展性

尽管当前国内外研究在区块链可扩展性方面做了大量努力，但现有各种性能优化方案在提升区块链性能方面都有一定的局限性，使得区块链大规模商业应用存在较大距离。

（1）软硬件一体化区块链可扩展架构有待研究。现有研究大多从数据结构、传输协

议、共识层、应用层等方面提升区块链可扩展性，大多是软件系统架构层面研究。构建软硬件一体化系统架构，从软硬件协同创新方面提升区块链可扩展有待研究。

（2）分片技术的实际规模化应用有待提高。分片技术使得随着网络规模化增长，区块链处理越来越多的交易将成为可能。理论上，分片技术可以实现区块链系统处理能力的规模化扩展，是提高区块链可扩展性的重要方向。然而，现有网络分片、交易分片、状态分片等分片技术总体上仍然处于初级发展阶段，存在安全性、数据有效性和可用性问题。例如，网络分片使得单个分片算力低于整个网络算力，容易遭受双重支付或女巫攻击；针对 UTXO 数据模型，交易分片容易引起跨片通信，极端情况下，单个分片内所有交易都是跨片交易，从而使得系统整体性能低于分片前；状态分片因验证节点存储部分状态容易导致数据有效性和可用性问题。针对这些问题，现有研究在这些方面提出了一些解决方案，但在分片规模量化、片内通信复杂度、跨分片通信原子性及性能方面离规模化应用仍存在一定距离，需要进一步深入研究。

（3）链上扩容和链下扩容协同有待深入。链上扩容和链下扩容各自存在一定的局限性。链上扩容通过改变区块链底层结构使得单位时间的区块容纳更多交易。然而，容易加剧区块链中心化、安全攻击等风险风险；而链下扩容无需改变区块链底层结构，通过将链下结算与链上清算隔离开，在保证安全性和一定程度去中心化同时，有效提高区块链扩展性。然而，面临通道路由、节点离线及保证金锁定等问题。针对不同额度的交易需求，链上扩容和链下扩容协同对去中心化程度、安全性、可扩展性的影响需要进一步研究。

4.2 跨链通信技术

未来跨链技术研究的发展具有如下趋势：

（1）跨链将成为不可阻挡的潮流。这可以类比互联网的发展历程。信息交互的迫切需求将各独立的局域网连接成一个覆盖全球的国际互联网——Internet。与之类似，价值互联的迫切需求将会促使当下由不同区块链构成的“价值联盟内流通”转变为“社会化流通”。

（2）同构跨链呼之欲出。底层架构一致的区块链间进行跨链通信，相对异构跨链而言是较为简单的。现阶段的 Cosmos 主要关注同构跨链通信，目前，Cosmos Hub 已经开始了初步的公测，而多个 Cosmos Zone 也处在开发过程中。预计在不久之后，就会建成一个初步可用的跨链系统。虽然同构跨链在兼容性等方面存在很大的局限性，但是，相关工作也可以视作跨链技术的重要进展。

（3）异构跨链必将实现。比特币和以太坊是目前极具影响力的两条区块链，前者是出现最早、市值最高的区块链；而后者已经集成了由世界各地开发人员提供的上千种应用。一种跨链方案如果希望获得全球范围的认可，则必须兼容这两类不同的区块链。因此相信在同构跨链实现之后，将会有更多的研究投入到异构跨链中，进而打通不同的价值流通体系，更好地服务经济社会。

4.3　区块链智能合约

在智能合约方面，未来重点研究以下几个方面：

（1）智能合约性能优化

目前智能合约的运算能力较为有限，难以满足大规模复杂计算的要求，第二层扩展解决方案（Layer2）将大多数“昂贵”的工作转移到链下，使得区块链开发者能够在图灵完备的可编程区块链上对可扩展性、去中心化和费用三者之间做出权衡，如其四种主要形态中的状态通道允许将区块链上的交易、操作、运行在链外进行管理并在链外操作完成基础上进行多重签名，将最终状态上链。通过对 Layer2 的持续研究和改进，是提高区块链及其智能合约性能的有效方法。

（2）部署跨链智能合约

跨链及其衍生的侧链仍然是区块链技术发展的重要环节。跨链能够实现链与链之间的相互通信与价值流转。为了实现更好的跨链通信，需要制定高可用、高性能、支持可扩展的跨链合约。

（3）智能合约安全性

根据猎豹科技整理的区块链安全事件统计数据，从 2011 年到 2018 年间，智能合约安全事件只占 6.67%。这个占比数字相对区块链安全事件来说不算太高，但是其造成的经济损失却高达 12.4 美元。其中著名的有 The DAO 安全漏洞、parity 多签名钱包两次安全漏洞、BEC 被盗事件等。智能合约在安全上应减少漏洞，在重入攻击、权限控制、整型溢出、时间戳依赖、短地址攻击等方面提高制定合约的安全性。

（4）智能合约隐私性

目前智能合约上各用户只是存在理论上的匿名，尽管用户名等其他身份信息通过转化为地址标识在区块链网络间进行传输，真实信息无法被获知，但是，一旦网络用户与现实世界的事务发生关联，地址标识就成为网络代号，任何与用户相关的信息和行为都会关联到这个账户，如果对账户进行画像，依然会泄露用户信息。且目前智能合约隐私保护是基于非对称密码学原理，现有的技术手段难以直接去通过计算方式来攻克。但是随着量子密码学的发展，非对称密码的破解存在可能。应提高对智能合约的隐私性与其风险应对措施研究的关注。

（5）智能合约与应用领域相结合

区块链与智能合约技术的落地具有巨大的商业价值，如何优化智能合约使其与新兴领域如物联网相结合具有重大意义，物联网具有多节点，高并发等特性，会产生大量数据，会给传统的中心化网络数据存储带来严重的负担，与区块链技术相结合有助于减轻中心化节点的负担。智能合约在物联网与区块链技术结合中实现物联网流程的自动化，保证效率节约成本。

（6）智能合约法律问题

智能合约在实际应用中可能会出现难以追责等法律问题，让智能合约具有实际意义

上的法律效率也是制定智能合约首先需要考虑的前提。为充分保障智能合约的法律效率，在制定合约时应充分考虑实际应用过程中的法律法规。

（7）智能合约更加智能化

目前大多数人考虑智能合约的智能特性，未来随着深度学习、语义识别等人工智能技术的发展，需要制定更加智能的智能合约，让智能合约具备自主感知、自主学习、自主推理等能力，实现智能合约真正的智能化。

4.4 区块链安全性保障

区块链安全性保障方面的研究，主要体现在以下三个方面：

（1）去中心化、安全性和可扩展性三者兼顾的问题

PoW 是最早应用在区块链上的共识机制，一直存在效率低、能耗高等问题。低能耗的 PoS 共识方案面临易分叉的安全问题。有相对完善证明体系的 BFT 协议不支持大规模节点扩展，网络开销较大。分片技术提高系统效率的同时也造成安全性弱的问题。利用可信硬件实现共识会有后门风险。如何兼顾去中心化、安全性和可扩展性是区块链共识机制发展要解决的重要问题。

（2）区块链互联

为了丰富区块链的功能、完善区块链生态、实现区块链价值最大化，区块链与外部数字世界、物理世界和异构区块链之间的互联将成为未来发展趋势。在实现区块链互联的过程中会面临诸多安全问题，也将成为未来区块链安全方向的研究重点。

（3）系统级安全体系

区块链的发展还需要建立系统级安全体系，从整体上提升区块链的安全性，推动区块链安全标准化，为区块链开发和使用提供设计、管理和使用指南。加快制定区块链相关安全规范和标准，提升区块链安全监控能力，以保障区块链产业健康发展和持续创新。

4.5 区块链监管与隐私保护

区块链监管的研究重点是：

（1）公有链匿名监管技术有待深入：虽然很多研究人员在通过对比特币、以太坊等公有链通过账号分析等方法，希望能找到某个公有链账号背后的所有者，但当前的研究还处于初级阶段，并没有很好的方法能够解决这一问题。

（2）联盟链隐私保护与监管并存技术有待提高：当前的联盟链架构中并未设计专门的监管节点，从架构层面无法做到在保护区块链成员和数据隐私的前提下，满足监管方的监管需求。监管与隐私之间平衡需要进一步研究。

（3）内容监管有待研究：公有链现有的研究大多只针对区块链的地址匿名性，在内容监管等领域还缺乏足够的研究。虽然联盟链和公有链相比，更加容易监管，但联盟链同样具有不可篡改性等特点，一旦有敏感信息上链，则无法对链上数据进行回滚操作。

在隐私保护方面，隐私保护的重要性持续提升，主要研究：

（1）按需配置的网络层安全防护机制：针对联盟链和私有链，采用合适的访问控制策略防止恶意节点接入和监听网络，从根本上增强网络层的保护能力。此外，联盟链或者私有链与传统中心化架构有很多相似之处，可以采用传统中心化架构中成熟的安全措施。针对公有链网络，重点研究异常节点检测的方法，及早发现和屏蔽恶意节点。此外，需要研究在效率、性能、易用性方面更好的匿名通信机制，替代现有的 Tor 等匿名通信方案。

（2）基于密码学算法的交易层隐私保护机制：随着数据分析技术的发展，传统的混币机制保护隐私的效果将逐渐降低。有必要研究采用密码学算法保证混币的安全性。例如零知识证明机制，同态加密机制。基于加密的保护方案应该充分考虑区块链服务器在计算性能和存储性能上的缺陷，设计通用性更高的加密方法。

（3）安全密钥技术：在应用层，除了提升用户安全意识，增强区块链服务商安全能力以外，重点是要研究钱包的密钥保护技术，开发使用方便、安全可靠的钱包程序。钱包秘钥直接关系到账户安全，可以研究无密钥的密码算法和代码混淆技术，防止恶意用户通过反汇编等方法提取秘钥信息，可以研究基于口令、硬件以及生物特征等多因素认证机制，增强私钥的安全性。

4.6 区块链技术应用

在区块链应用方面，除了金融行业、供应链管理、物联网、版权保护、医疗行业等方面，应用的领域在不断扩展，应用的层次不断加深。

效率是制约区块链技术应用的重要因素，在很大程度上限制了区块链在金融系统的高频交易中的应用。提升区块链效率是未来区块链技术在金融行业以及各个相关行业的目标和发展趋势。并且，区块链该如何监管也是未来需要解决的问题。此外，区块链技术在应用到金融行业时，其安全性还需要使用权威标准进行测试[91][93]。

随着区块链技术水平的不断提高，区块链将广泛应用于教育、慈善、农产品溯源等，区块链技术的广泛应用会给社会生活带来更大的变化。

5 结束语

相对于传统的分布式数据库，区块链主要的技术优势包括：一是从集中式存储账本演进到分布式共享账本。区块链打破了原有的集中式记账，变成“全网共享”的分布式账本，参与记账的各方之间通过同步协调机制，保证数据的一致性，提升了支付清结算效率。二是解决传统中心化的信任机制问题。网络中没有中心节点，所有节点都是平等的，通过点对点传输协议达成整体共识。三是数据安全且难以篡改。每个区块的数据都会通过非对称密码算法加密，并分布式同步到所有节点，确保任一节点停止工作都不影响系统的整体运作。四是以智能合约方式驱动业务应用。系统由代码组成的智能合约自

动运行，无需人工干预。

当前全球区块链技术创新日趋活跃，世界各国高度重视并超前布局，国际组织、科技巨头、初创企业正积极探索区块链与垂直领域的融合创新，落地场景从金融领域向实体经济逐步延伸。尽管行业生态初步成形，但由于行业偏重于应用创新，底层平台缺乏自主研发能力，相应匹配法律法规尚待完善。现阶段，需要积极开展重点领域试点应用和示范推广，集多方力量突破技术瓶颈，加强政策制定和监管合规研究，为区块链产业提供良性发展空间。

参考文献

[1] Croman K, Decker C, Eyal I, et al. On scaling decentralized blockchains[A]. Proc. 3rd Workshop on Bitcoin and Blockchain Research[C]. 2016.

[2] Luu L, Narayanan V, Zheng C, et al. A Secure Sharding Protocol For Open Blockchains[A]. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security[C]. Vienna, Austria: ACM, 2016: 17-30. 2978389.

[3] Buterin V. On sharding blockchains[EB/OL]. https://github. com/ethereum/sharding/blob/develop/docs/doc. md.

[4] Team T Z. The ZILLIQA Technical Whitepaper[EB/OL]. https://docs. zilliqa. com/whitepaper. pdf.

[5] E K K, P J, L G, et al. OmniLedger: A Secure, Scale-Out, Decentralized Ledger via Sharding[A]. 2018 IEEE Symposium on Security and Privacy (SP)[C]. 2018: 583-598.

[6] Zamani M, Movahedi M, Raykova M. RapidChain: Scaling Blockchain via Full Sharding[A]. Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security[C]. Toronto, Canada: ACM, 2018: 931-948. 3243853.

[7] Bano S, Al-Bassam M, Danezis G. The road to scalable blockchain designs[J]. USENIX; login: magazine, 2017.

[8] 曾帅，袁勇，倪晓春. 面向比特币的区块链扩容：关键技术，制约因素与衍生问题[J]. 自动化学报，2019，45(6)：1015-1030.

[9] Sompolinsky Y, Zohar A. Secure High-Rate Transaction Processing in Bitcoin[A]. International Conference on Financial Cryptography and Data Security[C]. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015: 507-527.

[10] Sapirshtein A, Sompolinsky Y, Zohar A. Optimal Selfish Mining Strategies in Bitcoin[A]. 2017. International Conference on Financial Cryptography and Data Security[C]. International Conference on Financial Cryptography and Data Security.

[11] 潘晨，刘志强，刘振. 区块链可扩展性研究：问题与方法[J]. 计算机研究与发展，2018，55(10)：2099-2110.

[12] Wiki B. Transaction malleability[EB/OL]. http://en. bitcoin. it/wiki/Transaction_Malleability.

[13] Andrychowicz M, Dziembowski S, Malinowski D, et al. On the Malleability of Bitcoin Transactions[A]. 2015. International Conference on Financial Cryptography and Data Security[C]. International Conference on Financial Cryptography and Data Security.

[14] Ren L, Nayak K, Abraham I, et al. Practical Synchronous Byzantine Consensus[EB/OL]. https://www.cs.umd.edu/kartik/papers/10_syncsmr.pdf.

[15] Sen S, Freedman M J. Commensal cuckoo: secure group partitioning for large-scale services[J]. SIGOPS Oper. Syst. Rev., 2012, 46(1): 33-39. 2146389.

[16] Poon J, Dryja T. The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments[EB/OL]. https://lightning.network/lightning-network-paper.pdf.

[17] Foundation R. Raiden network whitepaper[EB/OL]. https://raiden.network/.

[18] Miller A, Bentov I, Bakshi S, et al. Sprites and State Channels: Payment Networks that Go Faster than Lightning[A]. Proc. of the 23rd International Conference Financial Cryptography and Data Security[C]. 2019.

[19] Decker C, Wattenhofer R. A Fast and Scalable Payment Network with Bitcoin Duplex Micropayment Channels[A]. 2015: 3-18.

[20] Khalil R, Gervais A. Revive: Rebalancing Off-Blockchain Payment Networks[A]. Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security[C]. 2017: 439-453.

[21] Poon J, Buterin V. Plasma: Scalable Autonomous Smart Contracts[EB/OL]. https://plasma.io/plasma.pdf.

[22] 房卫东，张武雄，潘涛. 区块链的网络安全：威胁与对策 [J]. 信息安全学报，2017，3（2）.

[23] 韩璇，袁勇，王飞跃. 区块链安全问题：研究现状与展望 [J]. 自动化学报，2019，45（01）：208-227.

[24] 可信区块链推进计划. 区块链安全白皮书（1.0 版）[J]. 研究报告，2019，http://www.trustedblockchain.cn/schedule/detail/2992.

[25] 中国通信标准化协会. 区块链安全白皮书——技术应用篇 [J]. 研究报告，2019，http://www.caict.ac.cn/kxyj/qwfb/bps/201809/P020180919411826104153.pdf.

[26] 祝烈煌，高峰，沈蒙. 区块链隐私保护研究综述 [J]. 计算机研究与发展，2017，54（10），2170-2186.

[27] 房卫东，张武雄，潘涛. 区块链的网络安全：威胁与对策 [J]. 信息安全学报，2017，3（2）.

[28] 韩璇，袁勇，王飞跃. 区块链安全问题：研究现状与展望 [J]. 自动化学报，2019，45（01）：208-227.

[29] 可信区块链推进计划. 区块链安全白皮书（1.0 版）[J]. 研究报告，2019，http://www.trustedblockchain.cn/schedule/detail/2992.

[30] 中国通信标准化协会. 区块链安全白皮书——技术应用篇 [J]. 研究报告，2019，http://www.caict.ac.cn/kxyj/qwfb/bps/201809/P020180919411826104153.pdf.

[31] 数据缔造者. 盘点各国区块链监管政策 [J]. 研究报告，2019，http://www.sohu.com/a/253116037_774878.

[32] LUU L, CHU D-H, OLICKEL H, et al. Making smart contracts smarter[C]. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2016: 254-269.

[33] Stefano Bistarelli, Gianmarco Mazzante, Matteo Micheletti, Leonardo Mostarda, Francesco Tiezzi: Analysis of Ethereum Smart Contracts and Opcodes[J]. AINA 2019: 546-558.

[34] Atzei, N, Bartoletti, M, Cimoli, T. A survey of attacks on ethereum smart contracts (SoK)[R]. Principles of Security and Trust, Springer, Heidelberg, 2017: 164-186.

[35] Delmolino, K, Arnett, M, Kosba, A, Miller, A, Shi, E. Step by step towards creating a safe smart contract: lessons and insights from a cryptocurrency lab[C]. Financial Cryptography and Data Security:

FC 2016 International Workshops, BITCOIN, VOTING, and WAHC, 2016.

[36] Anderson, L, Holz, R, Ponomarev, A, Rimba, P, Weber, I. New kids on the block: an analysis of modern blockchains,2016.

[37] Herlihy M. Blockchains and the future of distributed computing[J]. PODC,2017.

[38] K Bhargavan, A Delignat-Lavaud, C Fournet, A Gollamudi, G Gonthier, N Kobeissi, N Kulatova, A Rastogi, T Sibut-Pinote, N Swamy, et al. Formal verification of smart contracts: Short paper[C]. Proceedings of the 2016 ACM Workshop on Programming Languages and Analysis for Security, 2016, 91-96.

[39] G Bigi, A Bracciali, G Meacci, E Tuosto, Validation of decentralised smart contracts through game theory and formal methods, Programming Languages with Applications to Biology and Security[M]. Springer, 2015, 142-161.

[40] ALHARBY M, VAN MOORSEL A. Blockchain-based smart contracts: a systematic mapping study[J]. arXiv preprint arXiv: 1710.06372, 2017.

[41] B Marino, A Juels. Setting standards for altering and undoing smart contracts, in International Symposium on Rules and Rule Markup Languages for the Semantic Web[M]. Springer, 2016, 151-166.

[42] F Idelberger, G Governatori, R Riveret,G Sartor, Evaluation of logic-based smart contracts for blockchain systems, in International Symposium on Rules and Rule Markup Languages for the Semantic Web[M]. Springer, 2016, 167-183.

[43] F Zhang, E Cecchetti, K Croman, A Juels, E Shi, Town crier: An authenticated data feed for smart contracts, in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security[C]. ACM. 2016.

[44] 王璞巍，杨航天，孟佶，陈晋川，杜小勇. 智能合约的形式化定义及参考实现 [J]. 软件学报，2019，30 (9). http://www.jos.org.cn/1000-9825/5773.htm.

[45] 朱忠宁. 基于 DSL 和区块链技术的可编程智能合约设计与实现 [D]. 广州：华南理工大学，2017.

[46] 朱涛，姚翔，许玉壮，周钰. 基于 Fabric 的跨境汇款追踪平台实现 [J]. 信息安全学报，2018，3 (03)：50-61.

[47] 朱岩，宋晓旭，薛显斌，秦博涵，刘国伟. 基于安全多方计算的区块链智能合约执行系统 [J]. 密码学报，2019，6 (2)：246-257.

[48] 朱翀. 基于安卓的智能合约平台的设计与实现 [D]. 北京：北京邮电大学，2018.

[49] 谭海波，周桐，赵赫，赵哲，王卫东，张中贤，盛念祖，李晓风. 基于区块链的档案数据保护与共享方法 [J]. 软件学报，2019，30 (9). http://www.jos.org.cn/1000-9825/5770.htm.

[50] 王守道，蒋玉明，胡大裟. 基于区块链的智能合约压缩存储方法 [J]. 现代计算机 (专业版)，2019 (09)：42-46.

[51] 杨茜. 基于区块链的智能合约研究与实现 [D]. 四川：西南科技大学，2018.

[52] 黄步添，刘琦，何钦铭，刘振广，陈建海. 基于语义嵌入模型与交易信息的智能合约自动分类系统 [J]. 自动化学报，2017，43 (09)：1532-1543.

[53] 曹迪迪，陈伟. 基于智能合约的以太坊可信存证机制 [J]. 计算机应用，2019，39 (04)：1073-1080.

[54] A Kosba, A Miller, E Shi, Z Wen, C Papamanthou. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts[J]. IEEE, 2016.

[55] M Vukolić. Rethinking permissioned blockchains[J]. ACM, 2017.

[56] 田雪晴，张晓玉，雷珂. 区块链技术在国际金融与贸易上的应用和影响［J］. 时代金融，2019（16）：81-83.

[57] 饶东宁，王军星，蒋志华，等. 区块链技术在物流供应链领域应用综述［J］. 软件导刊，2018，17（9）：1-3，8. DOI：10. 11907/rjdk. 181186.

[58] 卿苏德. 区块链在物联网中的应用［J］. 智能物联技术，2019，51（3）：1-8.

[59] IBM 采用区块链技术来追踪卡车位置跟货物来源可提高运输过的程透明度［OL］. http://www. elecfans. com/blockchain/773296. html.

[60] 区块链技术企业 TBSx3 与港口物流企业合作打击假药供应链［OL］. http://www. aijinrong. cc/caijing/qukuailian/398198. html.

[61] Guo Y，Liang C. Blockchain application and outlook in the banking industry［J］. Financial Innovation，2016，2(1)：24.

[62] 谭征. 区块链视角下物流供应链重构研究［J］. 商业经济研究，2019，(5)：83-86.

[63] 刘睿智，赵守香，张铎. 区块链技术对物流供应链的重塑［J］. 中国储运，2019，(5)：124-128.

[64] 林洧. 区块链视角下数字版权保护路径探究［J］. 图书情报导刊，2019，4（3）：46-51.

[65] 夏朝羡. 区块链技术视角下网络版权保护问题研究［J］. 电子知识产权，2018，(11)：109-116.

[66] 邱安邦. 区块链技术应用于数字版权保护的优势分析［J］. 梧州学院学报，2019，29（1）：50-55.

[67] 陈亮，李峰，夏征义，等. 区块链：物联网应用进展研究［J］. 物联网技术，2018，8（5）：100-103，106. DOI：10. 16667/j. issn. 2095-1302. 2018. 05. 033.

[68] 金凯，杨睿哲，杨兆鑫，等. 区块链在供应链管理上的应用［J］. 情报工程，2018，4（3）：29-38. DOI：10. 3772/j. issn. 2095-915x. 2018. 03. 005.

[69] 王红. 基于区块链的物流服务供应链应用模式研究［J］. 商业经济研究，2019，(7)：84-86.

[70] 网络版权保护“挂上”区块链，未来可期［OL］. https://www. 8btc. com/article/408001.

[71] 微软牵手安永推出版权保护区块链工具，Quorum 真的能带来新生？［OL］. https://www. 8btc. com/article/224379.

[72] 物联网 + 区块链：下一个增长引擎？［OL］. https://www. 8btc. com/article/356310.

[73] 唯链落地！首个物流供应链项目已签订正式商业合约［OL］. http://www. chinaz. com/news/2016/0913/580705. shtml.

[74] Kuo T T，Kim H E，Ohno-Machado L. Blockchain distributed ledger technologies for biomedical and health care applications［J］. Journal of the American Medical Informatics Association，2017，24(6)：1211-1220.

[75] 雀巢联合区块链平台 OpenSC，开展新区块链供应链追踪试点［OL］. https://www. 8btc. com/article/439137.

[76] 法链与初版联手，探索我国版权保护新路径［OL］. https://www. 8btc. com/article/130432.

[77] 以区块链技术重塑数字版权保护，解决版权三大痛点［OL］. https://www. sohu. com/a/235904446_460230.

[78] 向菲，张柏林，范伯男. 区块链技术在国外医疗卫生领域中的应用［J］. 中华医学图书情报杂志，2018，27（08）：31-37.

[79] Linn L A，Koo M B. Blockchain for health data and its potential use in health it and health care related research［C］. ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg，Maryland，United States：ONC/NIST. 2016：1-10.

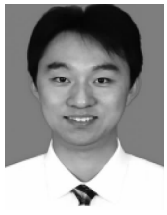
[80] Angraal S，Krumholz H M，Schulz W L. Blockchain technology：applications in health care［J］.

Circulation: Cardiovascular quality and outcomes, 2017, 10(9): e003800.
[81] 韩秋明，王革. 区块链技术国外研究述评［J］. 科技进步与对策，2018，35（02）：154-160.
[82] 黄征，李祥学，来学嘉，陈克非. 区块链技术及其应用［J］. 信息安全研究，2017，3（03）：237-245.
[83] 袁勇，王飞跃. 区块链技术发展现状与展望［J］. 自动化学报，2016，42（04）：481-494.
[84] 吴珊，张元友，邢文圣. 区块链技术在医疗健康领域的应用与展望［J］. 电子技术与软件工程，2019（10）：172.
[85] 赵延红，原宝华，梁军. 区块链技术在医疗领域中的应用探讨［J］. 中国医学教育技术，2018，32（01）：1-7.
[86] 中国区块链生态联盟、青岛市崂山区人民政府、赛迪（青岛）区块链研究院. 2018—2019 年中国区块链发展年度报告（上）［N］. 中国计算机报，2019-06-03（008）.
[87] 中国区块链生态联盟、青岛市崂山区人民政府、赛迪（青岛）区块链研究院. 2018—2019 年中国区块链发展年度报告（下）［N］. 中国计算机报，2019-06-17（008）.
[88] 李伟，夏明月，华梦莲. 区块链技术：金融领域的变革与伦理挑战［J］. 上海立信会计金融学院学报，2019（03）：17-29.
[89] 张雅茹，陈颖，程楣，简李文. 区块链技术在金融领域的应用前景研究［J］. 现代商业，2019（14）：127-128.
[90] 游丽. 金融领域中区块链技术的应用及发展趋势［J］. 金融经济，2019（10）：124-125.
[91] 王艳. 区块链技术在金融业的应用及其发展建议［J］. 海南金融，2016（12）：37-39 +49.
[92] Nguyen Q K. Blockchain- a financial technology for future sustainable development［C］. 2016 3rd International Conference on Green Technology and Sustainable Development (GTSD). IEEE, 2016: 51-54.
[93] Paech P. The governance of blockchain financial networks[J]. The Modern Law Review, 2017, 80(6): 1073-1110.
[94] Stagnaro C. White paper: Innovative blockchain uses in health care[J]. Freed Associates, 2017.

作者简介

斯雪明 现任复旦大学教授，中国计算机学会区块链专委会主任，福州市区块链首席专家，中原工学院前沿信息技术研究院院长。专业方向为密码学、数据科学、计算机体系结构、网络与信息系统安全、区块链。

孙 毅 中科院计算所研究员、博导，区块链实验室主任，中科计算海南区块链创新研究院院长，中国计算机学会区块链专委会副主任，首届中国区块链技术大会程序委员会主席，入选中科院 50 人卓越青年科学家计划。



祝烈煌 北京理工大学教授，博导，CCF 区块链专委秘书长。入选教育部新世纪优秀人才，中国通信学会网络与信息安全杰出人才。研究方向区块链安全监管与隐私保护。主持科技部重点研发计划课题、国家自然科学基金重点、科技委创新特区基金等国家级、省部级项目 20 余项。

朱建明 中央财经大学信息学院教授，CCF 理事、区块链专业委员会常务委员。从事金融信息安全、电子商务安全、区块链技术等方面的教学和科研工作。现主持国家重点研发计划项目 1 项、国家自然科学基金重点项目 1 项，主持完成国家自然科学基金项目 4 项。

高 胜 中央财经大学信息学院副教授，CCF 区块链专业委员会委员。主要从事数据安全与隐私保护、区块链技术及应用等研究。已在 IEEE TISF，TSC，中国科学等国内外著名期刊和国际会议上发表论文 30 余篇，参编著作 4 部，授权国家技术发明专利 6 项。

陈 福 中央财经大学信息学院教授，CCF 高级会员、互联网专委委员、服务计算专委委员。“新世纪优秀人才支持计划”入选者；主持和参加多项国家自然科学基金等课题；三项国家发明专利；出版三本著作，发表多篇学术论文。

董学文 西安电子科技大学副教授，IEEE/ACM/YOCSEF 会员。主要从事网络与信息安全等领域的研究工作，出版专著与教材 2 部，先后主持参与了国家/陕西省重点研发计划项目、国家自然基金重点/面上项目等，结合研究工作在《INFOCOM》《IEEE Trans. on Vehicular Technology》《Computers & Security》《软件学报》等国内外重要学术期刊会议上发表了二十多篇论文。