区块链技术研究综述：原理、进展与应用

曾诗钦[1]，霍如[2,3]，黄韬[1,3]，刘江[1,3]，汪硕[1,3]，冯伟[4]

（1. 北京邮电大学网络与交换国家重点实验室，北京 100876；2. 北京工业大学北京未来网络科技高精尖创新中心，北京 100124；
3. 网络通信与安全紫金山实验室，江苏 南京 211111；4. 工业和信息化部信息化和软件服务业司，北京 100846）

摘 要：区块链是一种分布式账本技术，依靠智能合约等逻辑控制功能演变为完整的存储系统。其分类方式、服务模式和应用需求的变化导致核心技术形态的多样性发展。为了完整地认知区块链生态系统，设计了一个层次化的区块链技术体系结构，进一步深入剖析区块链每层结构的基本原理、技术关联以及研究进展，系统归纳典型区块链项目的技术选型和特点，最后给出智慧城市、工业互联网等区块链前沿应用方向，提出区块链技术挑战与研究展望。

关键词：区块链；加密货币；去中心化；层次化技术体系结构；技术多样性；工业区块链

中图分类号：TP393

文献标识码：A

doi: 10.11959/j.issn.1000−436x.2020027

Survey of blockchain: principle, progress and application

ZENG Shiqin[1], HUO Ru[2,3], HUANG Tao[1,3], LIU Jiang[1,3], WANG Shuo[1,3], FENG Wei[4]

1. State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China
2. Beijing Advanced Innovation Center for Future Internet Technology, Beijing University of Technology, Beijing 100124, China
3. Purple Mountain Laboratories, Nanjing 211111, China
4. Department of Information Technology Application and Software Services, Beijing 100846, China

Abstract: Blockchain is a kind of distributed ledger technology that upgrades to a complete storage system by adding logic control functions such as intelligent contracts. With the changes of its classification, service mode and application requirements, the core technology forms of Blockchain show diversified development. In order to understand the Blockchain ecosystem thoroughly, a hierarchical technology architecture of Blockchain was proposed. Furthermore, each layer of blockchain was analyzed from the perspectives of basic principle, related technologies and research progress in-depth. Moreover, the technology selections and characteristics of typical Blockchain projects were summarized systematically. Finally, some application directions of blockchain frontiers, technology challenges and research prospects including Smart Cities and Industrial Internet were given.

Key words: blockchain, cryptocurrency, decentralization, hierarchical technology architecture, technology diversity, industrial blockchain

1 引言

2008 年，中本聪提出了去中心化加密货币——比特币（bitcoin）的设计构想。2009 年，比特币系统开始运行，标志着比特币的正式诞生。2010—2015 年，比特币逐渐进入大众视野。2016—2018 年，随着各国陆续对比特币进行公开表态以及世界主流经济的不确定性增强，比特币的受

收稿日期：2019–10–08；**修回日期**：2019–12–12

通信作者：霍如，huoru@bjut.edu.cn

基金项目：国家高技术研究发展计划（“863”计划）基金资助项目（No.2015AA015702）；未来网络操作系统发展战略研究基金资助项目（No.2019-XY-5）

Foundation Items: The National High Technology Research and Development Program of China (863 Program) (No.2015AA015702), The Development Strategy Research of Future Network Operating System (No.2019-XY-5)

关注程度激增，需求量迅速扩大。事实上，比特币是区块链技术最成功的应用场景之一。伴随着以太坊（ethereum）等开源区块链平台的诞生以及大量去中心化应用（DApp, decentralized application）的落地，区块链技术在更多的行业中得到了应用。

由于具备过程可信和去中心化两大特点，区块链能够在多利益主体参与的场景下以低成本的方式构建信任基础，旨在重塑社会信用体系。近两年来区块链发展迅速，人们开始尝试将其应用于金融、教育、医疗、物流等领域。但是，资源浪费、运行低效等问题制约着区块链的发展，这些因素造成区块链分类方式、服务模式和应用需求发生快速变化，进一步导致核心技术朝多样化方向发展，因此有必要采取通用的结构分析区块链项目的技术路线和特点，以梳理和明确区块链的研究方向。

区块链涵盖多种技术，相关概念易混淆，且应用场景繁多，为此，已有相关综述主要从技术体系结构、技术挑战和应用场景等角度来梳理区块链的最新进展、技术差异和联系，总结技术形态和应用价值。袁勇等[1]给出了区块链基本模型，以比特币为例将非许可链分为数据层、网络层、共识层、激励层、合约层和应用层；邵奇峰等[2]结合开源项目细节，对比了多种企业级区块链（许可链）的技术特点；Yang 等[3]总结了基于区块链的网络服务架构的特点、挑战和发展趋势；韩璇等[4]系统性归纳了区块链安全问题的研究现状；Ali 等[5]总结了区块链在物联网方面的应用研究进展、趋势。上述文献虽然归纳得较为完整，但是都没有从许可链与非许可链共性技术的角度进行通用的层次结构分析，没有体现出区块链技术与组网路由、数据结构、同步机制等已有技术的关联性，且缺少对区块链项目的差异分析。本文则对有关概念进行区分，探讨了通用的层次化技术结构及其与已有技术的关联性，并针对该结构横向分析相关学术研究进展；根据分层结构对比部分区块链项目的技术选型；最后以智慧城市场景、边缘计算和人工智能技术为代表介绍区块链应用研究现状，给出区块链技术挑战与研究展望。

2　相关概念

随着区块链技术的深入研究，不断衍生出了很多相关的术语，例如“中心化”“去中心化”“公链”“联盟链”等。为了全面地了解区块链技术，并对区块链技术涉及的关键术语有系统的认知，本节将给出区块链及其相关概念的定义，以及它们的联系，更好地区分易使人混淆的术语。

2.1　中心化与去中心化

中心化（centralization）与去中心化（decentralization）最早用来描述社会治理权力的分布特征。从区块链应用角度出发，中心化是指以单个组织为枢纽构建信任关系的场景特点。例如，电子支付场景下用户必须通过银行的信息系统完成身份验证、信用审查和交易追溯等；电子商务场景下对端身份的验证必须依靠权威机构下发的数字证书完成。相反，去中心化是指不依靠单一组织进行信任构建的场景特点，该场景下每个组织的重要性基本相同。

2.2　加密货币

加密货币（cryptocurrency）是一类数字货币（digital currency）技术，它利用多种密码学方法处理货币数据，保证用户的匿名性、价值的有效性；利用可信设施发放和核对货币数据，保证货币数量的可控性、资产记录的可审核性，从而使货币数据成为具备流通属性的价值交换媒介，同时保护使用者的隐私。

加密货币的概念起源于一种基于盲签名（blind signature）的匿名交易技术[6]，最早的加密货币交易模型“electronic cash”[7]如图 1 所示。

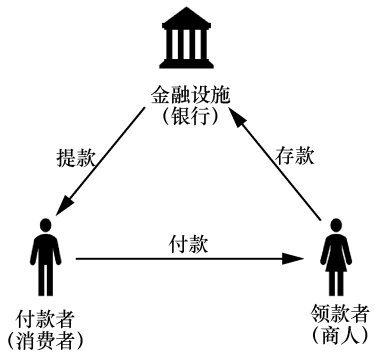


图 1　“electronic cash”交易模型

交易开始前，付款者使用银行账户兑换加密货币，然后将货币数据发送给领款者，领款者向银行发起核对请求，若该数据为银行签发的合法货币数据，那么银行将向领款者账户记入等额数值。通过盲签名技术，银行完成对货币数据的认证，而无法获得发放货币与接收货币之间的关联，从而保证了价值的有效性、用户的匿名性；银行天然具有发放

币种、账户记录的能力，因此保证了货币数量的可控性与资产记录的可审核性。

最早的加密货币构想将银行作为构建信任的基础，呈现中心化特点。此后，加密货币朝着去中心化方向发展，并试图用工作量证明（PoW, poof of work）[8]或其改进方法定义价值。比特币在此基础上，采用新型分布式账本技术保证被所有节点维护的数据不可篡改，从而成功构建信任基础，成为真正意义上的去中心化加密货币。区块链从去中心化加密货币发展而来，随着区块链的进一步发展，去中心化加密货币已经成为区块链的主要应用之一。

2.3 区块链及工作流程

一般认为，区块链是一种融合多种现有技术的新型分布式计算和存储范式。它利用分布式共识算法生成和更新数据，并利用对等网络进行节点间的数据传输，结合密码学原理和时间戳等技术的分布式账本保证存储数据的不可篡改，利用自动化脚本代码或智能合约实现上层应用逻辑。如果说传统数据库实现数据的单方维护，那么区块链则实现多方维护相同数据，保证数据的安全性和业务的公平性。区块链的工作流程主要包含生成区块、共识验证、账本维护 3 个步骤。

1) 生成区块。区块链节点收集广播在网络中的交易——需要记录的数据条目，然后将这些交易打包成区块——具有特定结构的数据集。

2) 共识验证。节点将区块广播至网络中，全网节点接收大量区块后进行顺序的共识和内容的验证，形成账本——具有特定结构的区块集。

3) 账本维护。节点长期存储验证通过的账本数据并提供回溯检验等功能，为上层应用提供账本访问接口。

2.4 区块链类型

根据不同场景下的信任构建方式，可将区块链分为 2 类：非许可链（permissionless blockchain）和许可链（permissioned blockchain）。

非许可链也称为公链（public blockchain），是一种完全开放的区块链，即任何人都可以加入网络并参与完整的共识记账过程，彼此之间不需要信任。公链以消耗算力等方式建立全网节点的信任关系，具备完全去中心化特点的同时也带来资源浪费、效率低下等问题。公链多应用于比特币等去监管、匿名化、自由的加密货币场景。

许可链是一种半开放式的区块链，只有指定的成员可以加入网络，且每个成员的参与权各有不同。许可链往往通过颁发身份证书的方式事先建立信任关系，具备部分去中心化特点，相比于非许可链拥有更高的效率。进一步，许可链分为联盟链（consortium blockchain）和私链（fully private blockchain）。联盟链由多个机构组成的联盟构建，账本的生成、共识、维护分别由联盟指定的成员参与完成。在结合区块链与其他技术进行场景创新时，公链的完全开放与去中心化特性并非必需，其低效率更无法满足需求，因此联盟链在某些场景中成为实适用性更强的区块链选型。私链相较联盟链而言中心化程度更高，其数据的产生、共识、维护过程完全由单个组织掌握，被该组织指定的成员仅具有账本的读取权限。

3 区块链体系结构

根据区块链发展现状，本节将归纳区块链的通用层次技术结构、基本原理和研究进展。

现有项目的技术选型多数由比特币演变而来，所以区块链主要基于对等网络通信，拥有新型的基础数据结构，通过全网节点共识实现公共账本数据的统一。但是区块链也存在效率低、功耗大和可扩展性差等问题，因此人们进一步以共识算法、处理模型、交易模式创新为切入点进行技术方案改进，并在此基础上丰富了逻辑控制功能和区块链应用功能，使其成为一种新型计算模式。本文给出如图 2 所示的区块链通用层次化技术结构，自下而上分别为网络层、数据层、共识层、控制层和应用层。其中，网络层是区块链信息交互的基础，承载节点间的共识过程和数据传输，主要包括建立在基础网络之上的对等网络及其安全机制；数据层包括区块链基本数据结构及其原理；共识层保证节点数据的一致性，封装各类共识算法和驱动节点共识行为的奖惩机制；控制层包括沙盒环境、自动化脚本、智能合约和权限管理等，提供区块链可编程特性，实现对区块数据、业务数据、组织结构的控制；应用层包括区块链的相关应用场景和实践案例，通过调用控制合约提供的接口进行数据交互，由于该层次不涉及区块链原理，因此在第 5 节中单独介绍。

3.1 网络层

网络层关注区块链网络的基础通信方式——

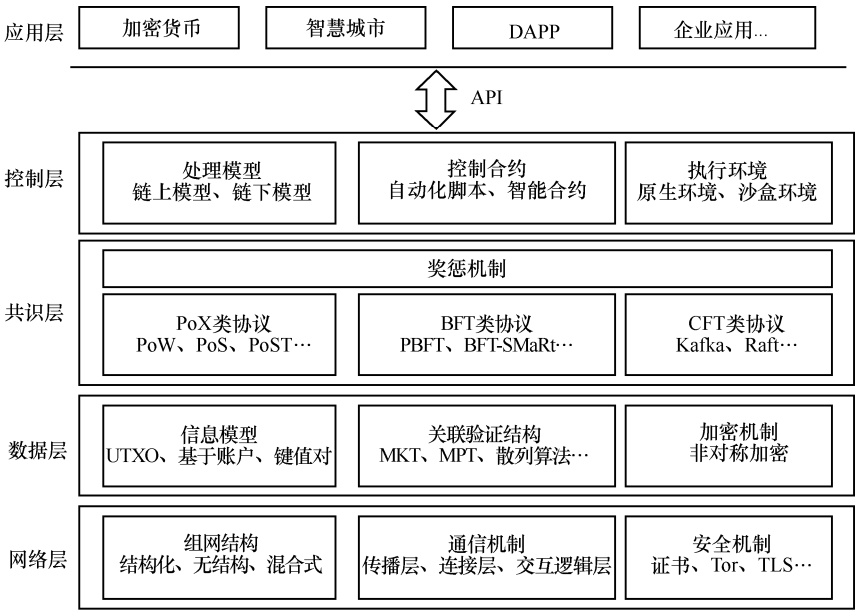


图 2　区块链层次化技术结构

对等（P2P, peer-to-peer）网络。对等网络是区别于“客户端/服务器”服务模式的计算机通信与存储架构，网络中每个节点既是数据的提供者也是数据的使用者，节点间通过直接交换实现计算机资源与信息的共享，因此每个节点地位均等。区块链网络层由组网结构、通信机制、安全机制组成。其中组网结构描述节点间的路由和拓扑关系，通信机制用于实现节点间的信息交互，安全机制涵盖对端安全和传输安全。

1) 组网结构

对等网络的体系架构可分为无结构对等网络、结构化对等网络和混合式对等网络[9]，根据节点的逻辑拓扑关系，区块链网络的组网结构也可以划分为上述 3 种，如图 3 所示。

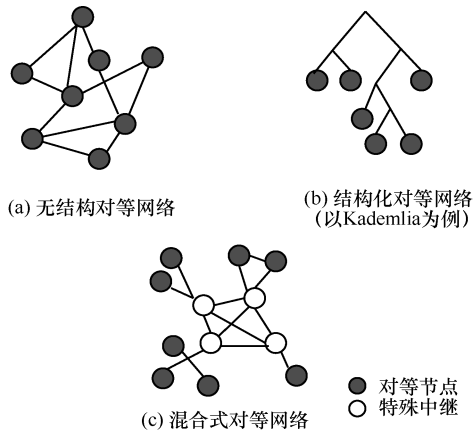


图 3　区块链组网结构

无结构对等网络是指网络中不存在特殊中继节点、节点路由表的生成无确定规律、网络拓扑呈现随机图状的一类对等网络。该类网络结构松散，设计简洁，具有良好的容错性和匿名性，但由于采用洪泛机制作为信息传播方式，其可扩展性较差。典型的协议有 Gnutella 等。

结构化对等网络是指网络中不存在特殊中继节点、节点间根据特定算法生成路由表、网络拓扑具有严格规律的一类对等网络。该类网络实现复杂但可扩展性良好，通过结构化寻址可以精确定位节点从而实现多样化功能。常见的结构化网络以 DHT（distributed hash table）网络为主，典型的算法有 Chord、Kademlia 等。

混合式对等网络是指节点通过分布式中继节点实现全网消息路由的一类对等网络。每个中继节点维护部分网络节点地址、文件索引等工作，共同实现数据中继的功能。典型的协议有 Kazza 等。

2) 通信机制

通信机制是指区块链网络中各节点间的对等通信协议，建立在 TCP/UDP 之上，位于计算机网络协议栈的应用层，如图 4 所示。该机制承载对等网络的具体交互逻辑，例如节点握手、心跳检测、交易和区块传播等。由于包含的协议功能不同（例如基础链接与扩展交互），本文将通信机制细分为 3 个层次：传播层、连接层和交互逻辑层。

传播层实现对等节点间数据的基本传输，包括

2 种数据传播方式：单点传播和多点传播。单点传播是指数据在 2 个已知节点间直接进行传输而不经过其他节点转发的传播方式；多点传播是指接收数据的节点通过广播向邻近节点进行数据转发的传播方式，区块链网络普遍基于 Gossip 协议[10]实现洪泛传播。连接层用于获取节点信息，监测和改变节点间连通状态，确保节点间链路的可用性（availability）。具体而言，连接层协议帮助新加入节点获取路由表数据，通过定时心跳监测为节点保持稳定连接，在邻居节点失效等情况下为节点关闭连接等。交互逻辑层是区块链网络的核心，从主要流程上看，该层协议承载对等节点间账本数据的同步、交易和区块数据的传输、数据校验结果的反馈等信息交互逻辑，除此之外，还为节点选举、共识算法实施等复杂操作和扩展应用提供消息通路。

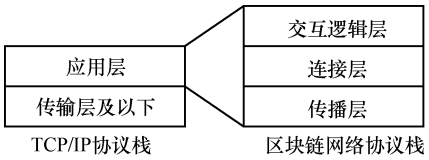


图 4 区块链网络通信机制

3) 安全机制

安全是每个系统必须具备的要素，以比特币为代表的非许可链利用其数据层和共识层的机制，依靠消耗算力的方式保证数据的一致性和有效性，没有考虑数据传输过程的安全性，反而将其建立在不可信的透明 P2P 网络上。随着隐私保护需求的提出，非许可链也采用了一些网络匿名通信方法，例如匿名网络 Tor（the onion router）通过沿路径的层层数据加密机制来保护对端身份。许可链对成员的可信程度有更高的要求，在网络层面采取适当的安全机制，主要包括身份安全和传输安全两方面。身份安全是许可链的主要安全需求，保证端到端的可信，一般采用数字签名技术实现，对节点的全生命周期（例如节点交互、投票、同步等）进行签名，从而实现许可链的准入许可。传输安全防止数据在传输过程中遭到篡改或监听，常采用基于 TLS 的点对点传输和基于 Hash 算法的数据验证技术。

4) 研究现状

目前，区块链网络层研究主要集中在 3 个方向：测量优化、匿名分析与隐私保护、安全防护。

随着近年来区块链网络的爆炸式发展以及开源特点，学术界开始关注大型公有链项目的网络状况，监测并研究它们的特点，研究对象主要为比特币网络。Decker 等[11]设计和实现测量工具，分析传播时延数据、协议数据和地址数据，建模分析影响比特币网络性能的网络层因素，基于此提出各自的优化方法。Fadhil 等[12]提出基于事件仿真的比特币网络仿真模型，利用真实测量数据验证模型的有效性，最后提出优化机制 BCBSN，旨在设立超级节点降低网络波动。Kaneko 等[13]将区块链节点分为共识节点和验证节点，其中共识节点采用无结构组网方式，验证节点采用结构化组网方式，利用不同组网方式的优点实现网络负载的均衡。

匿名性是加密货币的重要特性之一，但从网络层视角看，区块链的匿名性并不能有效保证，因为攻击者可以利用监听并追踪 IP 地址的方式推测出交易之间、交易与公钥地址之间的关系，通过匿名隐私研究可以主动发掘安全隐患，规避潜在危害。Koshy 等[14]提出识别比特币地址和 IP 地址之间映射关系的启发式算法，学习了近 1 000 对可能的映射关系。Biryukov 等[15]通过监测比特币网络的地址传播信息来标识节点身份，进而提出一种客户端去匿名化方法。Venkatakrishnan 等[16-17]从网络拓扑、传播层协议和作恶模型 3 个方面对比特币网络进行建模，通过理论分析和仿真实验证明了比特币网络协议在树形组网结构下仅具备弱匿名性，在此基础上提出 Dandelion 网络策略以较低的网络开销优化匿名性，随后又提出 Dandelion++原理，以最优信息理论保证来抵抗大规模去匿名攻击。

区块链重点关注其数据层和共识层面机制，并基于普通网络构建开放的互联环境，该方式极易遭受攻击。为提高区块链网络的安全性，学术界展开研究并给出了相应的解决方案。Heilman 等[18]对比特币和以太坊网络实施日蚀攻击（eclipse attack）——通过屏蔽正确节点从而完全控制特定节点的信息来源，证实了该攻击的可行性。Apostolaki 等[19]提出针对比特币网络的 BGP（border gateway protocal）劫持攻击，通过操纵自治域间路由或拦截域间流量来制造节点通信阻塞，表明针对关键数据的沿路攻击可以大大降低区块传播性能。

3.2 数据层

区块链中的“块”和“链”都是用来描述其数据结构特征的词汇，可见数据层是区块链技术体系的核心。区块链数据层定义了各节点中数据的联系和组织方式，利用多种算法和机制保证数据的强关

联性和验证的高效性，从而使区块链具备实用的数据防篡改特性。除此之外，区块链网络中每个节点存储完整数据的行为增加了信息泄露的风险，隐私保护便成为迫切需求，而数据层通过非对称加密等密码学原理实现了承载应用信息的匿名保护，促进区块链应用普及和生态构建。因此，从不同应用信息的承载方式出发，考虑数据关联性、验证高效性和信息匿名性需求，可将数据层关键技术分为信息模型、关联验证结构和加密机制 3 类。

1) 信息模型

区块链承载了不同应用的数据（例如支付记录、审计数据、供应链信息等），而信息模型则是指节点记录应用信息的逻辑结构，主要包括 UTXO（unspent transaction output）、基于账户和键值对模型 3 种。需要说明的是，在大部分区块链网络中，每个用户均被分配了交易地址，该地址由一对公私钥生成，使用地址标识用户并通过数字签名的方式检验交易的有效性。

UTXO 是比特币交易中的核心概念，逐渐演变为区块链在金融领域应用的主要信息模型，如图 5 所示。每笔交易（Tx）由输入数据（Input）和输出数据（Output）组成，输出数据为交易金额（Num）和用户公钥地址（Adr），而输入数据为上一笔交易输出数据的指针（Pointer），直到该比特币的初始交易由区块链网络向节点发放。

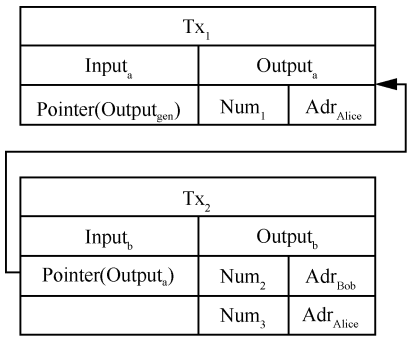


图 5　UTXO 信息模型

基于账户的信息模型以键值对的形式存储数据，维护着账户当前的有效余额，通过执行交易来不断更新账户数据。相比于 UTXO，基于账户的信息模型与银行的储蓄账户类似，更直观和高效。

不管是 UTXO 还是基于账户的信息模型，都建立在更为通用的键值对模型上，因此为了适应更广泛的应用场景，键值对模型可直接用于存储业务数据，表现为表单或集合形式。该模型利于数据的存取并支持更复杂的业务逻辑，但是也存在复杂度高的问题。

2) 关联验证结构

区块链之所以具备防篡改特性，得益于链状数据结构的强关联性。该结构确定了数据之间的绑定关系，当某个数据被篡改时，该关系将会遭到破坏。由于伪造这种关系的代价是极高的，相反检验该关系的工作量很小，因此篡改成功率被降至极低。链状结构的基本数据单位是“区块（block）”，基本内容如图 6 所示。

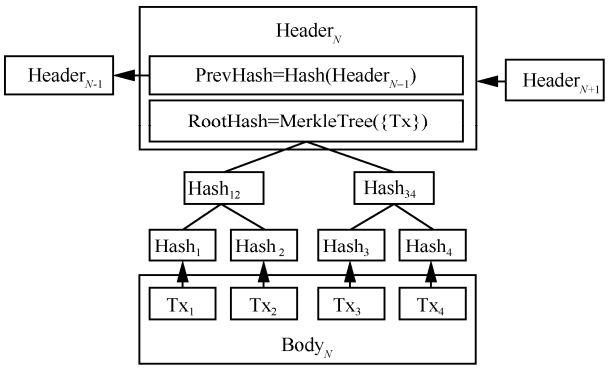


图 6　基本区块结构

区块由区块头（Header）和区块体（Body）两部分组成，区块体包含一定数量的交易集合；区块头通过前继散列（PrevHash）维持与上一区块的关联从而形成链状结构，通过 MKT（MerkleTree）生成的根散列（RootHash）快速验证区块体交易集合的完整性。因此散列算法和 MKT 是关联验证结构的关键，以下将对此展开介绍。

散列（Hash）算法也称为散列函数，它实现了明文到密文的不可逆映射；同时，散列算法可以将任意长度的输入经过变化得到固定长度的输出；最后，即使元数据有细微差距，变化后的输出也会产生显著不同。利用散列算法的单向、定长和差异放大的特征，节点通过比对当前区块头的前继散列即可确定上一区块内容的正确性，使区块的链状结构得以维系。区块链中常用的散列算法包括 SHA256 等。

MKT 包括根散列、散列分支和交易数据。MKT 首先对交易进行散列运算，再对这些散列值进行分组散列，最后逐级递归直至根散列。MKT 带来诸多好处：一方面，对根散列的完整性确定即间接地实现交易的完整性确认，提升高效性；另一方面，根据交易的散列路径（例如 Tx_1：$Hash_2$、$Hash_{34}$）可降低验证某交易存在性的复杂度，若交易总数为

N，那么 MKT 可将复杂度由 N 降为 lb$N$。除此之外，还有其他数据结构与其配合使用，例如以太坊通过 MPT（Merkle Patricia tree）——PatriciaTrie 和 MerkleTree 混合结构，高效验证其基于账户的信息模型数据。

此外，区块头中还可根据不同项目需求灵活添加其他信息，例如添加时间戳为区块链加入时间维度，形成时序记录；添加记账节点标识，以维护成块节点的权益；添加交易数量，进一步提高区块体数据的安全性。

3) 加密机制

由上述加密货币原理可知，经比特币演变的区块链技术具备与生俱来的匿名性，通过非对称加密等技术既保证了用户的隐私又检验了用户身份。非对称加密技术是指加密者和解密者利用 2 个不同秘钥完成加解密，且秘钥之间不能相互推导的加密机制。常用的非对称加密算法包括 RSA、Elgamal、背包算法、Rabin、D-H、ECC（椭圆曲线加密算法）等。对应图 5，Alice 向 Bob 发起交易 Tx_2，Alice 使用 Bob 的公钥对交易签名，仅当 Bob 使用私钥验证该数字签名时，才有权利创建另一笔交易，使自身拥有的币生效。该机制将公钥作为基础标识用户，使用户身份不可读，一定程度上保护了隐私。

4) 研究现状

数据层面的研究方向集中在高效验证、匿名分析、隐私保护 3 个方面。

高效验证的学术问题源于验证数据结构（ADS, authenticated data structure），即利用特定数据结构快速验证数据的完整性，实际上 MKT 也是其中的一种。为了适应区块链数据的动态性（dynamical）并保持良好性能，学术界展开了研究。Reyzin 等[20]基于 AVL 树形结构提出 AVL+，并通过平衡验证路径、缺省堆栈交易集等机制，简化轻量级节点的区块头验证过程。Zhang 等[21]提出 GEM2-tree 结构，并对其进行优化提出 GEM2∗-tree 结构，通过分解单树结构、动态调整节点计算速度、扩展数据索引等机制降低以太坊节点计算开销。

区块数据直接承载业务信息，因此区块数据的匿名关联性分析更为直接。Reid 等[22]将区块数据建模为事务网络和用户网络，利用多交易数据的用户指向性分析成功降低网络复杂度。Meiklejohn 等[23]利用启发式聚类方法分析交易数据的流动特性并对用户进行分组，通过与这些服务的互动来识别主要机构的比特币地址。Awan 等[24]使用优势集（dominant set）方法对区块链交易进行自动分类，从而提高分析准确率。

隐私保护方面，Saxena 等[25]提出复合签名技术削弱数据的关联性，基于双线性映射中的 Diffie-Hellman 假设保证计算困难性，从而保护用户隐私。Miers 等[26]和 Sasson 等[27]提出 Zerocoin 和 Zerocash，在不添加可信方的情况下断开交易间的联系，最早利用零知识证明（zero-knowledge proof）技术隐藏交易的输入、输出和金额信息，提高比特币的匿名性。非对称加密是区块链数据安全的核心，但在量子计算面前却显得“捉襟见肘”，为此 Yin 等[28]利用盆景树模型（bonsai tree）改进晶格签名技术（lattice-based signature），以保证公私钥的随机性和安全性，使反量子加密技术适用于区块链用户地址的生成。

3.3 共识层

区块链网络中每个节点必须维护完全相同的账本数据，然而各节点产生数据的时间不同、获取数据的来源未知，存在节点故意广播错误数据的可能性，这将导致女巫攻击[29]、双花攻击[30]等安全风险；除此之外，节点故障、网络拥塞带来的数据异常也无法预测。因此，如何在不可信的环境下实现账本数据的全网统一是共识层解决的关键问题。实际上，上述错误是拜占庭将军问题（the Byzantine generals problem）[31]在区块链中的具体表现，即拜占庭错误——相互独立的组件可以做出任意或恶意的行为，并可能与其他错误组件产生协作，此类错误在可信分布式计算领域被广泛研究。

状态机复制（state-machine replication）是解决分布式系统容错问题的常用理论。其基本思想为：任何计算都表示为状态机，通过接收消息来更改其状态。假设一组副本以相同的初始状态开始，并且能够就一组公共消息的顺序达成一致，那么它们可以独立进行状态的演化计算，从而正确维护各自副本之间的一致性。同样，区块链也使用状态机复制理论解决拜占庭容错问题，如果把每个节点的数据视为账本数据的副本，那么节点接收到的交易、区块即为引起副本状态变化的消息。状态机复制理论实现和维持副本的一致性主要包含 2 个要素：正确执行计算逻辑的确定性状态机和传播相同序列消息的共识协议。其中，共识协议是影响容错效果、吞吐量和复杂度的关键，不同安全性、可扩展性要

求的系统需要的共识协议各有不同。学术界普遍根据通信模型和容错类型对共识协议进行区分[32]，因此严格地说，区块链使用的共识协议需要解决的是部分同步（partial synchrony）模型[33]下的拜占庭容错问题。

区块链网络中主要包含 PoX（poof of X）[34]、BFT（byzantine-fault tolerant）和 CFT（crash-fault tolerant）类基础共识协议。PoX 类协议是以 PoW（proof of work）为代表的基于奖惩机制驱动的新型共识协议，为了适应数据吞吐量、资源利用率和安全性的需求，人们又提出 PoS（proof of stake）、PoST（proof of space-time）等改进协议。它们的基本特点在于设计证明依据，使诚实节点可以证明其合法性，从而实现拜占庭容错。BFT 类协议是指解决拜占庭容错问题的传统共识协议及其改良协议，包括 PBFT、BFT-SMaRt、Tendermint 等。CFT 类协议用于实现崩溃容错，通过身份证明等手段规避节点作恶的情况，仅考虑节点或网络的崩溃（crash）故障，主要包括 Raft、Paxos、Kafka 等协议。

非许可链和许可链的开放程度和容错需求存在差异，共识层面技术在两者之间产生了较大区别。具体而言，非许可链完全开放，需要抵御严重的拜占庭风险，多采用 PoX、BFT 类协议并配合奖惩机制实现共识。许可链拥有准入机制，网络中节点身份可知，一定程度降低了拜占庭风险，因此可采用 BFT 类协议、CFT 类协议构建相同的信任模型[35]。

限于篇幅原因，本节仅以 PoW、PBFT、Raft 为切入进行 3 类协议的分析。

1) PoX 类协议

PoW 也称为 Nakamoto 协议，是比特币及其衍生项目使用的核心共识协议，如图 7 所示。

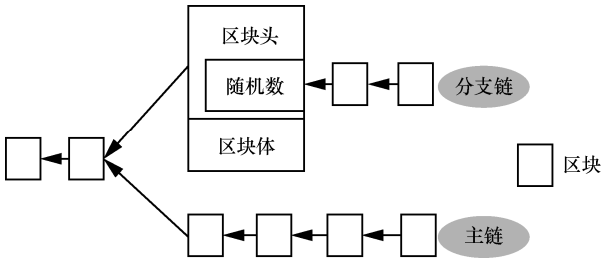


图 7　PoW 协议示意

该协议在区块链头结构中加入随机数 Nonce，并设计证明依据：为生成新区块，节点必须计算出合适的 Nonce 值，使新生成的区块头经过双重 SHA256 运算后小于特定阈值。该协议的整体流程为：全网节点分别计算证明依据，成功求解的节点确定合法区块并广播，其余节点对合法区块头进行验证，若验证无误则与本地区块形成链状结构并转发，最终达到全网共识。PoW 是随机性协议，任何节点都有可能求出依据，合法区块的不唯一将导致生成分支链，此时节点根据“最长链原则”选择一定时间内生成的最长链作为主链而抛弃其余分支链，从而使各节点数据最终收敛。

PoW 协议采用随机性算力选举机制，实现拜占庭容错的关键在于记账权的争夺，目前寻找证明依据的方法只有暴力搜索，其速度完全取决于计算芯片的性能，因此当诚实节点数量过半，即“诚实算力”过半时，PoW 便能使合法分支链保持最快的增长速度，也即保证主链一直是合法的。PoW 是一种依靠饱和算力竞争纠正拜占庭错误的共识协议，关注区块产生、传播过程中的拜占庭容错，在保证防止双花攻击的同时也存在资源浪费、可扩展性差等问题。

2) BFT 类协议

PBFT 是 BFT 经典共识协议，其主要流程如图 8 所示。PBFT 将节点分为主节点和副节点，其中主节点负责将交易打包成区块，副节点参与验证和转发，假设作恶节点数量为 f。PBFT 共识主要分为预准备、准备和接受 3 个阶段，主节点首先收集交易后排序并提出合法区块提案；其余节点先验证提案的合法性，然后根据区块内交易顺序依次执行并将结果摘要组播；各节点收到 $2f$ 个与自身相同的摘要后便组播接受投票；当节点收到超过 $2f$+1 个投票时便存储区块及其产生的新状态[36]。

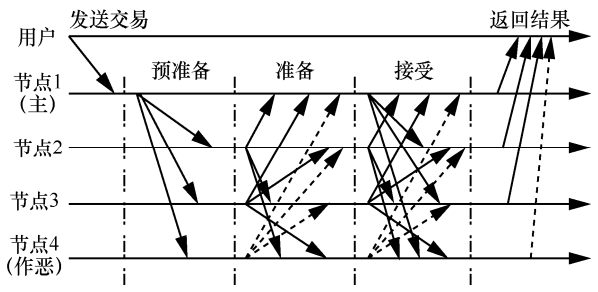


图 8　PBFT 协议示意

PBFT 协议解决消息传播过程的拜占庭容错，由于算法复杂度为 $O(n^2)$且存在确定性的主节点选举规则，PBFT 仅适用于节点数量少的小型许可链系统。

3) CFT 类协议

Raft[37]是典型的崩溃容错共识协议，以可用性强著称。Raft 将节点分为跟随节点、候选节点和领导节点，领导节点负责将交易打包成区块，追随节点响应领导节点的同步指令，候选节点完成领导节点的选举工作。当网络运行稳定时，只存在领导节点和追随节点，领导节点向追随节点推送区块数据从而实现同步。节点均设置生存时间决定角色变化周期，领导节点的心跳信息不断重置追随节点的生存时间，当领导节点发生崩溃时，追随节点自动转化为候选节点并进入选举流程，实现网络自恢复。

Raft 协议实现崩溃容错的关键在于领导节点的自选举机制，部分许可链选择降低可信需求，将拜占庭容错转换为崩溃容错，从而提升共识速度。

4) 奖惩机制

奖惩机制包括激励机制与惩罚策略，其中激励机制是为了弥补节点算力消耗、平衡协议运行收益比的措施，当节点能够在共识过程中获得收益时才会进行记账权的争夺，因此激励机制利用经济效益驱动各共识协议可持续运行。激励机制一般基于价值均衡理论设计，具有代表性的机制包括 PPLNS、PPS 等。为了实现收益最大化，节点可能采用不诚实的运行策略（如扣块攻击、自私挖矿等），损害了诚实节点的利益，惩罚策略基于博弈论等理论对节点进行惩罚，从而纠正不端节点的行为，维护共识可持续性。

5) 研究现状

随着可扩展性和性能需求的多样化发展，除了传统的 BFT、CFT 协议和 PoX 协议衍生研究，还产生了混合型协议（Hybrid）——主要为 PoX 类协议混合以及 PoX-BFT 协议混合。因此本节从 PoX 类、BFT 类以及 Hybrid 类协议归纳共识层研究进展。

如前文所述，PoX 类协议的基本特点在于设计证明依据，使诚实节点可以证明其合法性，从而实现拜占庭容错。uPoW[38]通过计算有意义的正交向量问题证明节点合法性，使算力不被浪费。PoI（proof-of-importance）[39]利用图论原理为每个节点赋予重要性权重，权重越高的节点将越有可能算出区块。PoS（poof-of-stake）为节点定义“币龄”，拥有更高币龄的节点将被分配更多的股份（stake），而股份被作为证明依据用于成块节点的选举。Ouroboros[40]通过引入多方掷币协议增大了选举随机性，引入近乎纳什均衡的激励机制进一步提高 PoS 的安全性。PoRep（proof-of-replication）[41]应用于去中心化存储网络，利用证明依据作为贡献存储空间的奖励，促进存储资源再利用。

BFT 协议有较长的发展史，在区块链研究中被赋予了新的活力。SCP[42]和 Ripple[43]基于联邦拜占庭共识[44]——存在交集的多池（确定规模的联邦）共识，分别允许节点自主选择或与指定的节点构成共识联邦，通过联邦交集达成全网共识。Tendermint[45]使用 Gossip 通信协议基本实现异步拜占庭共识，不仅简化了流程而且提高了可用性。HotStuff[46]将 BFT 与链式结构数据相结合，使主节点能够以实际网络时延及 $O(n)$通信复杂度推动协议达成一致。LibraBFT[47]在 HotStuff 的基础上加入奖惩机制及节点替换机制，从而优化了性能。

Hybrid 类协议是研究趋势之一。PoA[48]利用 PoW 产生空区块头，利用 PoS 决定由哪些节点进行记账和背书，其奖励由背书节点和出块节点共享。PeerCensus[49]由节点团体进行拜占庭协议实现共识，而节点必须基于比特币网络，通过 PoW 产出区块后才能获得投票权力。ByzCoin[50]利用 PoW 的算力特性构建动态成员关系，并引入联合签名方案来减小 PBFT 的轮次通信开销，提高交易吞吐量，降低确认时延。Casper[51]则通过 PoS 的股份决定节点构成团体并进行 BFT 共识，且节点可投票数取决于股份。

3.4 控制层

区块链节点基于对等通信网络与基础数据结构进行区块交互，通过共识协议实现数据一致，从而形成了全网统一的账本。控制层是各类应用与账本产生交互的中枢，如果将账本比作数据库，那么控制层提供了数据库模型，以及相应封装、操作的方法。具体而言，控制层由处理模型、控制合约和执行环境组成。处理模型从区块链系统的角度分析和描述业务/交易处理方式的差异。控制合约将业务逻辑转化为交易、区块、账本的具体操作。执行环境为节点封装通用的运行资源，使区块链具备稳定的可移植性。

1) 处理模型

账本用于存储全部或部分业务数据，那么依据该数据的分布特征可将处理模型分为链上（on-chain）和链下（off-chain）2 种。

链上模型是指业务数据完全存储在账本中，业

务逻辑通过账本的直接存取实现数据交互。该模型的信任基础建立在强关联性的账本结构中，不仅实现防篡改而且简化了上层控制逻辑，但是过量的资源消耗与庞大的数据增长使系统的可扩展性达到瓶颈，因此该模型适用于数据量小、安全性强、去中心化和透明程度高的业务。

链下模型是指业务数据部分或完全存储在账本之外，只在账本中存储指针以及其他证明业务数据存在性、真实性和有效性的数据。该模型以“最小化信任成本”为准则，将信任基础建立在账本与链下数据的证明机制中，降低账本构建成本。由于与公开的账本解耦，该模型具有良好的隐私性和可拓展性，适用于去中心化程度低、隐私性强、吞吐量大的业务。

2) 控制合约

区块链中控制合约经历了 2 个发展阶段，首先是以比特币为代表的非图灵完备的自动化脚本，用于锁定和解锁基于 UTXO 信息模型的交易，与强关联账本共同克服了双花等问题，使交易数据具备流通价值。其次是以以太坊为代表的图灵完备的智能合约，智能合约是一种基于账本数据自动执行的数字化合同，由开发者根据需求预先定义，是上层应用将业务逻辑编译为节点和账本操作集合的关键。智能合约通过允许相互不信任的参与者在没有可信第三方的情况下就复杂合同的执行结果达成协议，使合约具备可编程性，实现业务逻辑的灵活定义并扩展区块链的使用。

3) 执行环境

执行环境是指执行控制合约所需要的条件，主要分为原生环境和沙盒环境。原生环境是指合约与节点系统紧耦合，经过源码编译后直接执行，该方式下合约能经历完善的静态分析，提高安全性。沙盒环境为节点运行提供必要的虚拟环境，包括网络通信、数据存储以及图灵完备的计算/控制环境等，在虚拟机中运行的合约更新方便、灵活性强，其产生的漏洞也可能造成损失。

4) 研究现状

控制层的研究方向主要集中在可扩展性优化与安全防护 2 个方面。

侧链（side-chain）在比特币主链外构建新的分类资产链，并使比特币和其他分类资产在多个区块链之间转移，从而分散了单一链的负荷。Tschorsch 等[52]利用 Two-way Peg 机制实现交互式跨链资产转换，防止该过程中出现双花。Kiayias 等[53]利用 NIPoPoW 机制实现非交互式的跨链工作证明，并降低了跨链带来的区块冗余。分片（sharding）是指不同节点子集处理区块链的不同部分，从而减少每个节点的负载。ELASTICO[54]将交易集划分为不同分片，每个分片由不同的节点集合进行并行验证。OmniLedger[55]在前者的基础上优化节点随机选择及跨切片事务提交协议，从而提高了切片共识的安全性与正确性。区别于 OmniLedger，PolyShard[56]利用拉格朗日多项式编码分片为分片交互过程加入计算冗余，同时实现了可扩展性优化与安全保障。上述研究可视为链上处理模型在加密货币场景下的可扩展性优化方案。实际上，链下处理模型本身就是一种扩展性优化思路，闪电网络[57]通过状态通道对交易最终结果进行链上确认，从而在交易过程中实现高频次的链外支付。Plasma[58]在链下对区块链进行树形分支拓展，树形分支中的父节点完成子节点业务的确认，直到根节点与区块链进行最终确认。

一方面，沙盒环境承载了区块链节点运行条件，针对虚拟机展开的攻击更为直接；另一方面，智能合约直接对账本进行操作，其漏洞更易影响业务运行，因此控制层的安全防护研究成为热点。Luu 等[59]分析了运行于 EVM 中的智能合约安全性，指出底层平台的分布式语义差异带来的安全问题。Brent 等[60]提出智能合约安全分析框架 Vandal，将 EVM 字节码转换为语义逻辑关，为分析合约安全漏洞提供便利。Jiang 等[61]预先定义用于安全漏洞的特征，然后模拟执行大规模交易，通过分析日志中的合约行为实现漏洞检测。

4　技术选型分析

区别于其他技术，区块链发展过程中最显著的特点是与产业界紧密结合，伴随着加密货币和分布式应用的兴起，业界出现了许多区块链项目。这些项目是区块链技术的具体实现，既有相似之处又各具特点，本节将根据前文所述层次化结构对比特币、以太坊和超级账本 Fabric 项目进行分析，然后简要介绍其他代表性项目并归纳和对比各项目的技术选型及特点。

4.1　比特币

比特币是目前规模最大、影响范围最广的非许可链开源项目。图 9 为比特币项目以账本为核心的

运行模式，也是所有非许可链项目的雏形。比特币网络为用户提供兑换和转账业务，该业务的价值流通媒介由账本确定的交易数据——比特币支撑。为了保持账本的稳定和数据的权威性，业务制定奖励机制，即账本为节点产生新的比特币或用户支付比特币，以此驱动节点共同维护账本。

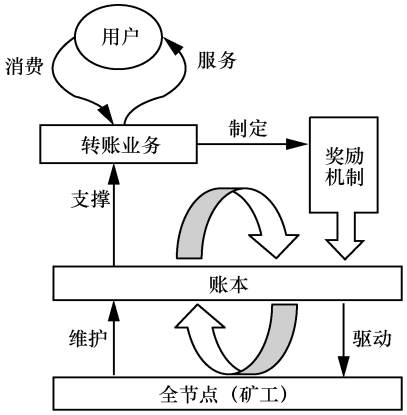


图 9 比特币运行模式

比特币网络主要由 2 种节点构成：全节点和轻节点。全节点是功能完备的区块链节点，而轻节点不存储完整的账本数据，仅具备验证与转发功能。全节点也称为矿工节点，计算证明依据的过程被称为“挖矿”，目前全球拥有近 1 万个全节点；矿池则是依靠奖励分配策略将算力汇集起来的矿工群；除此之外，还有用于存储私钥和地址信息、发起交易的客户端（钱包）。

1) 网络层

比特币在网络层采用非结构化方式组网，路由表呈现随机性。节点间则采用多点传播方式传递数据，曾基于 Gossip 协议实现，为提高网络的抗匿名分析能力改为基于 Diffusion 协议实现[33]。节点利用一系列控制协议确保链路的可用性，包括版本获取（Vetsion/Verack）、地址获取（Addr/GetAddr）、心跳信息（PING/PONG）等。新节点入网时，首先向硬编码 DNS 节点（种子节点）请求初始节点列表；然后向初始节点随机请求它们路由表中的节点信息，以此生成自己的路由表；最后节点通过控制协议与这些节点建立连接，并根据信息交互的频率更新路由表中节点时间戳，从而保证路由表中的节点都是活动的。交互逻辑层为建立共识交互通道，提供了区块获取（GetBlock）、交易验证（MerkleBlock）、主链选择（CmpctBlock）等协议；轻节点只需要进行简单的区块头验证，因此通过头验证（GetHeader/Header）协议和连接层中的过滤设置协议指定需要验证的区块头即可建立简单验证通路。在安全机制方面，比特币网络可选择利用匿名通信网络 Tor 作为数据传输承载，通过沿路径的层层数据加密机制来保护对端身份。

2) 数据层

比特币数据层面的技术选型已经被广泛研究，使用 UTXO 信息模型记录交易数据，实现所有权的简单、有效证明，利用 MKT、散列函数和时间戳实现区块的高效验证并产生强关联性。在加密机制方面，比特币采用参数为 Secp256k1 的椭圆曲线数字签名算法（ECDSA, elliptic curve digital signature algorithm）生成用户的公私钥，钱包地址则由公钥经过双重散列、Base58Check 编码等步骤生成，提高了可读性。

3) 共识层

比特币采用 PoW 算法实现节点共识，该算法证明依据中的阈值设定可以改变计算难度。计算难度由每小时生成区块的平均块数决定，如果生成得太快，难度就会增加。该机制是为了应对硬件升级或关注提升引起的算力变化，保持证明依据始终有效。目前该阈值被设定为 10 min 产出一个区块。除此之外，比特币利用奖惩机制保证共识的可持续运行，主要包括转账手续费、挖矿奖励和矿池分配策略等。

4) 控制层

比特币最初采用链上处理模型，并将控制语句直接记录在交易中，使用自动化锁定/解锁脚本验证 UTXO 模型中的比特币所有权。由于可扩展性和确认时延的限制，比特币产生多个侧链项目如 Liquid、RSK、Drivechain 等，以及链下处理项目 Lightning Network 等，从而优化交易速度。

4.2 以太坊

以太坊是第一个以智能合约为基础的可编程非许可链开源平台项目，支持使用区块链网络构建分布式应用，包括金融、音乐、游戏等类型；当满足某些条件时，这些应用将触发智能合约与区块链网络产生交互，以此实现其网络和存储功能，更重要的是衍生出更多场景应用和价值产物，例如以太猫，利用唯一标识为虚拟猫赋予价值；GitCoin，众筹软件开发平台等。

1) 网络层

以太坊底层对等网络协议簇称为 DEVP2P，除

了满足区块链网络功能外，还满足与以太坊相关联的任何联网应用程序的需求。DEVP2P 将节点公钥作为标识，采用 Kademlia 算法计算节点的异或距离，从而实现结构化组网。DEVP2P 主要由 3 种协议组成：节点发现协议 RLPx、基础通信协议 Wire 和扩展协议 Wire-Sub。节点间基于 Gossip 实现多点传播；新节点加入时首先向硬编码引导节点（bootstrap node）发送入网请求；然后引导节点根据 Kademlia 算法计算与新节点逻辑距离最近的节点列表并返回；最后新节点向列表中节点发出握手请求，包括网络版本号、节点 ID、监听端口等，与这些节点建立连接后则使用 Ping/Pong 机制保持连接。Wire 子协议构建了交易获取、区块同步、共识交互等逻辑通路，与比特币类似，以太坊也为轻量级钱包客户端设计了简易以太坊协议（LES, light ethereum subprotocol）及其变体 PIP。安全方面，节点在 RLPx 协议建立连接的过程中采用椭圆曲线集成加密方案（ECIES）生成公私钥，用于传输共享对称密钥，之后节点通过共享密钥加密承载数据以实现数据传输保护。

2) 数据层

以太坊通过散列函数维持区块的关联性，采用 MPT 实现账户状态的高效验证。基于账户的信息模型记录了用户的余额及其他 ERC 标准信息，其账户类型主要分为 2 类：外部账户和合约账户；外部账户用于发起交易和创建合约，合约账户用于在合约执行过程中创建交易。用户公私钥的生成与比特币相同，但是公钥经过散列算法 Keccak-256 计算后取 20 B 作为外部账户地址。

3) 共识层

以太坊采用 PoW 共识，将阈值设定为 15 s 产出一个区块，计划在未来采用 PoS 或 Casper 共识协议。较低的计算难度将导致频繁产生分支链，因此以太坊采用独有的奖惩机制——GHOST 协议，以提高矿工的共识积极性。具体而言，区块中的散列值被分为父块散列和叔块散列，父块散列指向前继区块，叔块散列则指向父块的前继。新区块产生时，GHOST 根据前 7 代区块的父/叔散列值计算矿工奖励，一定程度弥补了分支链被抛弃时浪费的算力。

4) 控制层

每个以太坊节点都拥有沙盒环境 EVM，用于执行 Solidity 语言编写的智能合约；Solidity 语言是图灵完备的，允许用户方便地定义自己的业务逻辑，这也是众多分布式应用得以开发的前提。为优化可扩展性，以太坊拥有侧链项目 Loom、链下计算项目 Plasma，而分片技术已于 2018 年加入以太坊源码。

4.3 超级账本 Fabric

超级账本是 Linux 基金会旗下的开源区块链项目，旨在提供跨行业区块链解决方案。Fabric 是超级账本子项目之一，也是影响最广的企业级可编程许可链项目；在已知的解决方案中，Fabric 被应用于供应链、医疗和金融服务等多种场景。

1) 网络层

Fabric 网络以组织为单位构建节点集群，采用混合式对等网络组网；每个组织中包括普通节点和锚节点（anchor peer），普通节点完成组织内的消息路由，锚节点负责跨组织的节点发现与消息路由。Fabric 网络传播层基于 Gossip 实现，需要使用配置文件初始化网络，网络生成后各节点将定期广播存活信息，其余节点根据该信息更新路由表以保持连接。交互逻辑层采用多通道机制，即相同通道内的节点才能进行状态信息交互和区块同步。Fabric 为许可链，因此在网络层采取严苛的安全机制：节点被颁发证书及密钥对，产生 PKI-ID 进行身份验证；可选用 TLS 双向加密通信；基于多通道的业务隔离；可定义策略指定通道内的某些节点对等传输私有数据。

2) 数据层

Fabric 的区块中记录读写集（read-write set）描述交易执行时的读写过程。该读写集用于更新状态数据库，而状态数据库记录了键、版本和值组成的键值对，因此属于键值对信息模型。一方面，散列函数和 MerkleTree 被用作高效关联结构的实现技术；另一方面，节点还需根据键值验证状态数据库与读写集中的最新版本是否一致。许可链场景对匿名性的要求较低，但对业务数据的隐私性要求较高，因此 Fabric 1.2 版本开始提供私有数据集（PDC, private data collection）功能。

3) 共识层

Fabric 在 0.6 版本前采用 PBFT 共识协议，但是为了提高交易吞吐量，Fabric 1.0 选择降低安全性，将共识过程分解为排序和验证 2 种服务，排序服务采用 CFT 类协议 Kafka、Raft（v1.4 之后）完成，而验证服务进一步分解为读写集验证与多签名

验证，最大程度提高了共识速度。由于 Fabric 针对许可链场景，参与方往往身份可知且具有相同的合作意图，因此规避了节点怠工与作恶的假设，不需要奖惩机制调节。

4) 控制层

Fabric 对于扩展性优化需求较少，主要得益于共识层的优化与许可链本身参与节点较少的前提，因此主要采用链上处理模型，方便业务数据的存取；而 PDC 中仅将私有数据散列值上链的方式则属于链下处理模型，智能合约可以在本地进行数据存取。Fabric 节点采用模块化设计，基于 Docker 构建模块执行环境；智能合约在 Fabric 中被称为链码，使用 GO、Javascript 和 Java 语言编写，也是图灵完备的。

4.4 其他项目

除了上述 3 种区块链基础项目外，产业界还有许多具有代表性的项目，如表 1 所示。

5 区块链应用研究

区块链技术有助于降低金融机构间的审计成本，显著提高支付业务的处理速度及效率，可应用于跨境支付等金融场景。除此之外，区块链还应用于产权保护、信用体系建设、教育生态优化、食品安全监管、网络安全保障等非金融场景。

根据这些场景的应用方式以及区块链技术特点，可将区块链特性概括为如下几点。1) 去中心化。节点基于对等网络建立通信和信任背书，单一节点的破坏不会对全局产生影响。2) 不可篡改。账本由全体节点维护，群体协作的共识过程和强关联的数据结构保证节点数据一致且基本无法被篡改，进一步使数据可验证和追溯。3) 公开透明。除私有数据外，链上数据对每个节点公开，便于验证数据的存在性和真实性。4) 匿名性。多种隐私保护机制使用户身份得以隐匿，即便如此也能建立信任基础。5) 合约自治。预先定义的业务逻辑使节点可以基于高可信的账本数据实现自治，在人–人、人–机、机–机交互间自动化执行业务。

鉴于上述领域的应用在以往研究中均有详细描述，本文将主要介绍区块链在智慧城市、边缘计算和人工智能领域的前沿应用研究现状。

表 1 代表性区块链项目

技术选型	Corda	Quorum	Libra	Blockstack	Filecoin	Zcash
控制合约	Kotlin, Java	GO	Move	Clarity 非图灵完备	非图灵完备	非图灵完备
执行环境	JVM	EVM	MVM	源码编译	源码编译	源码编译
处理模型	链上	链上/链下（私有数据）	链上	链下（虚拟链）	链下（IPFS）	链上
奖惩机制	—	—	Libra coins	Stacks token	Filecoin	Zcash/Turnstiles
共识算法	Notary 机制/RAFT, BFT-SMaRt	Quorum-Chain, RAFT	LibraBFT	Tunable Proofs, proof-of-burn	PoRep, PoET	PoW
信息模型	UTXO	基于账户	基于账户	基于账户	基于账户	UTXO
关联验证结构	散列算法 MKT	散列算法 MPT	散列算法 MKT	散列算法 Merklized Adaptive Radix Forest (MARF)	散列算法 MKT	散列算法 MKT
加密机制	Tear-offs 机制、混合密钥	基于 Enclave	SHA3-256/ EdDSA	基于 Gaia/Blockstack Auth	SECP256K1/BLS	zk-SNARK
组网方式	混合型	结构化	混合型	无结构	结构化/无结构	无结构
通信机制	AMQP1.0/单点传播	Wire/ Gossip	Noise-Protocol-Framework/Gossip	Atlas/Gossip	Libp2p/Gossip	Bitcoin-Core/ Gossip
安全机制	Corda 加密套件/TLS	证书/HTTPS	Diffie-Hellman	Secure Backbone	TLS	Tor
区块链类型	许可链	许可链	许可链	非许可链	非许可链	非许可链
特点	只允许对实际参与给定交易的各方进行信息访问和验证功能	基于以太坊网络提供公共交易和私有交易 2 种交互渠道	稳定、快速的交易网络	剔除中心服务商的、可扩展的分布式数据存储设施，旨在保护隐私数据	激励机制驱动的存储资源共享生态	基于比特币网络提供零知识证明的隐私保护
应用场景	金融业务平台	分布式应用	加密货币	互联网基础设施	文件存储与共享	加密货币

5.1 智慧城市

智慧城市是指利用 ICT 优化公共资源利用效果、提高居民生活质量、丰富设施信息化能力的研究领域，该领域包括个人信息管理、智慧医疗、智慧交通、供应链管理等具体场景。智慧城市强调居民、设施等各类数据的采集、分析与使能，数据可靠性、管理透明化、共享可激励等需求为智慧城市带来了许多技术挑战。区块链去中心化的交互方式避免了单点故障、提升管理公平性，公开透明的账本保证数据可靠及可追溯性，多种匿名机制利于居民隐私的保护，因此区块链有利于问题的解决。Hashemi 等[62]将区块链用于权限数据存储，构建去中心化的个人数据接入控制模型；Bao 等[63]利用区块链高效认证和管理用户标识，保护车主的身份、位置、车辆信息等个人数据。

5.2 边缘计算

边缘计算是一种将计算、存储、网络资源从云平台迁移到网络边缘的分布式信息服务架构，试图将传统移动通信网、互联网和物联网等业务进行深度融合，减少业务交付的端到端时延，提升用户体验。安全问题是边缘计算面临的一大技术挑战，一方面，边缘计算的层次结构中利用大量异构终端设备提供用户服务，这些设备可能产生恶意行为；另一方面，服务迁移过程中的数据完整性和真实性需要得到保障。区块链在这种复杂的工作环境和开放的服务架构中能起到较大作用。首先，区块链能够在边缘计算底层松散的设备网络中构建不可篡改的账本，提供设备身份和服务数据验证的依据。其次，设备能在智能合约的帮助下实现高度自治，为边缘计算提供设备可信互操作基础。Samaniego 等[64]提出了一种基于区块链的虚拟物联网资源迁移架构，通过区块链共享资源数据从而保障安全性。Stanciu[65]结合软件定义网络（SDN）、雾计算和区块链技术提出分布式安全云架构，解决雾节点中 SDN 控制器流表策略的安全分发问题。Ziegler 等[66]基于 Plasma 框架提出雾计算场景下的区块链可扩展应用方案，提升雾计算网关的安全性。

5.3 人工智能

人工智能是一类智能代理的研究，使机器感知环境/信息，然后进行正确的行为决策，正确是指达成人类预定的某些目标。人工智能的关键在于算法，而大部分机器学习和深度学习算法建立于体积庞大的数据集和中心化的训练模型之上，该方式易受攻击或恶意操作使数据遭到篡改，其后果为模型的不可信与算力的浪费。此外，数据采集过程中无法确保下游设备的安全性，无法保证数据来源的真实性与完整性，其后果将在自动驾驶等场景中被放大。区块链不可篡改的特性可以实现感知和训练过程的可信。另外，去中心化和合约自治特性为人工智能训练工作的分解和下放奠定了基础，保障安全的基础上提高计算效率。Kim 等[67]利用区块链验证联合学习框架下的分发模型的完整性，并根据计算成本提供相应的激励，优化整体学习效果。Bravo-Marquez 等[68]提出共识机制“学习证明”以减轻 PoX 类共识的计算浪费，构建公共可验证的学习模型和实验数据库。

6 技术挑战与研究展望

6.1 层次优化与深度融合

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。以比特币为代表的公链具有较高的安全性和完全去中心化的特点，但是资源浪费等问题成为拓展性优化的瓶颈。尽管先后出现了 PoS、BFT 等共识协议优化方案，或侧链、分片等链上处理模型，或 Plasma、闪电网络等链下扩展方案，皆是以部分安全性或去中心化为代价的。因此，如何将区块链更好地推向实际应用很大程度取决于三元悖论的解决，其中主要有 2 种思路。

1) 层次优化

区块链层次化结构中每层都不同程度地影响上述 3 种特性，例如网络时延、并行读写效率、共识速度和效果、链上/链下模型交互机制的安全性等，对区块链的优化应当从整体考虑，而不是单一层次。

网络层主要缺陷在于安全性，可拓展性则有待优化。如何防御以 BGP 劫持为代表的网络攻击将成为区块链底层网络的安全研究方向[19]。信息中心网络将重塑区块链基础传输网络，通过请求聚合和数据缓存减少网内冗余流量并加速通信传输[69]。相比于数据层和共识层，区块链网络的关注度较低，但却是影响安全性、可拓展性的基本因素。

数据层的优化空间在于高效性，主要为设计新的数据验证结构与算法。该方向可以借鉴计算机研究领域的多种数据结构理论与复杂度优化方法，寻

找适合区块链计算方式的结构，甚至设计新的数据关联结构。实际上相当一部分项目借鉴链式结构的思想开辟新的道路，例如压缩区块空间的隔离见证、有向无环图（DAG）中并行关联的纠缠结构（Tangle），或者 Libra 项目采用的状态树。

共识机制是目前研究的热点，也是同时影响三元特性的最难均衡的层次。PoW 牺牲可拓展性获得完全去中心化和安全性，PoS 高效的出块方式具备可扩展性但产生了分叉问题，POA 结合两者做到了 3 种特性的均衡。以此为切入的 Hybrid 类共识配合奖惩机制的机动调节取得了较好效果，成为共识研究的过渡手段，但是如何做到三元悖论的真正突破还有待研究。

控制层面是目前可扩展性研究的热点，其优势在于不需要改变底层的基础实现，能够在短期内应用，集中在产业界的区块链项目中。侧链具有较好的灵活性但操作复杂度高，分片改进了账本结构但跨分片交互的安全问题始终存在，而链下处理模型在安全方面缺少理论分析的支撑。因此，三元悖论的解决在控制层面具有广泛的研究前景。

2) 深度融合

如果将层次优化称为横向优化，那么深度融合即为根据场景需求而进行的纵向优化。一方面，不同场景的三元需求并不相同，例如接入控制不要求完全去中心化，可扩展性也未遇到瓶颈，因此可采用 BFT 类算法在小范围构建联盟链。另一方面，区块链应用研究从简单的数据上链转变为链下存储、链上验证，共识算法从 PoW 转变为场景结合的服务证明和学习证明，此外，结合 5G 和边缘计算可将网络和计算功能移至网络边缘，节约终端资源。这意味着在严格的场景建模下，区块链的层次技术选型将与场景特点交叉创新、深度融合，具有较为广阔的研究前景。

6.2 隐私保护

加密货币以匿名性著称，但是区块链以非对称加密为基础的匿名体系不断受到挑战。反匿名攻击从身份的解密转变为行为的聚类分析，不仅包括网络流量的 IP 聚类，还包括交易数据的地址聚类、交易行为的启发式模型学习，因此大数据分析技术的发展使区块链隐私保护思路发生转变。已有 Tor 网络、混币技术、零知识证明、同态加密以及各类复杂度更高的非对称加密算法被提出，但是各方法仍有局限，未来将需要更为高效的方法。此外，随着区块链系统的可编程化发展，内部复杂性将越来越高，特别是智能合约需要更严格、有效的代码检测方法，例如匿名性检测、隐私威胁预警等。

6.3 工业区块链

工业区块链是指利用区块链夯实工业互联网中数据的流通和管控基础、促进价值转换的应用场景，具有较大的研究前景。

工业互联网是面向制造业数字化、网络化、智能化需求，构建基于海量数据采集、汇聚、分析的服务体系，支撑制造资源泛在连接、弹性供给、高效配置的重要基础设施。“工业互联网平台”是工业互联网的核心，通过全面感知、实时分析、科学决策、精准执行的逻辑闭环，实现工业全要素、全产业链、全价值链的全面贯通，培育新的模式和业态。

可以看到，工业互联网与物联网、智慧城市、消费互联网等场景应用存在内在关联，例如泛在连接、数据共享和分析、电子商务等，那么其学术问题与技术实现必然存在关联性。区块链解决了物联网中心管控架构的单点故障问题，克服泛在感知设备数据的安全性和隐私性挑战，为智慧城市场景的数据共享、接入控制等问题提供解决方法，为激励资源共享构建了新型互联网价值生态。尽管工业互联网作为新型的产业生态系统，其技术体系更复杂、内涵更丰富，但是不难想象，区块链同样有利于工业互联网的发展。

“平台+区块链”能够通过分布式数据管理模式，降低数据存储、处理、使用的管理成本，为工业用户在工业 APP 选择和使用方面搭建起更加可信的环境，实现身份认证及操作行为追溯、数据安全存储与可靠传递。能够通过产品设计参数、质量检测结果、订单信息等数据“上链”，实现有效的供应链全要素追溯与协同服务。能够促进平台间数据交易与业务协同，实现跨平台交易结算，带动平台间的数据共享与知识复用，促进工业互联网平台间互联互通。

当然，工业是关乎国计民生的产业，将区块链去中心化、匿名化等特性直接用于工业互联网是不可取的，因此需要研究工业区块链管理框架，实现区块链的可管可控，在一定范围内发挥其安全优势，并对工业互联网的运转提供正向激励。

7 结束语

区块链基于多类技术研究的成果，以低成本解

决了多组织参与的复杂生产环境中的信任构建和隐私保护等问题，在金融、教育、娱乐、版权保护等场景得到了较多应用，成为学术界的研究热点。比特币的出现重塑了人们对价值的定义，伴随着产业界的呼声，区块链技术得到了快速发展，而遵循区块链层次化分析方法，能够直观地区别各项目的技术路线和特点，为优化区块链技术提供不同观察视角，并为场景应用的深度融合创造条件，促进后续研究。未来的发展中，区块链将成为更为基础的信任支撑技术，在产业互联网等更广阔的领域健康、有序地发展。

参考文献：

[1] 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(4): 481-494.
YUAN Y, WANG F Y. Blockchain: the state of the art and future trends[J]. Acta Automatica Sinica, 2016, 42(4): 481-494.

[2] 邵奇峰，张召，朱燕超，等. 企业级区块链技术综述[J]. 软件学报, 2019, 30(9): 2571-2592.
SHAO Q F, ZHANG Z, ZHU Y C, et al. Survey of enterprise blockchains[J]. 2019, 30(9): 2571-2592.

[3] YANG W, AGHASIAN E, GARG S, et al. A survey on blockchain-based internet service architecture: requirements, challenges, trends, and future[J]. IEEE Access, 2019, 7: 75845-75872.

[4] 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(1): 208-227.
HAN X, YUAN Y, WANG F Y. Security problems on blockchain: the state of the art and future trends[J]. Acta Automatica Sinica, 2016, 45(1): 208-227.

[5] ALI M, VECCHIO M, PINCHEIRA M, et al. Applications of blockchains in the Internet of things: a comprehensive survey[J]. IEEE Communications Surveys & Tutorials, 2019, 21: 1676-1717.

[6] CHAUM D. Blind signature system[M]. Advances in Cryptology: Proceedings of Crypto 83. Springer US, 1984.

[7] LAW L, SABEET S, SOLINAS J. How to make a mint: the cryptography of anonymous electronic cash[J]. The American University Law Review, 1997, 46: 1131-1162.

[8] JAKOBSSON M, JUELS A. Proofs of work and bread pudding protocols[C]//IFIP TC6/TC11 Joint Working Conference on Communications and Multimedia Security. IFIP, 1999: 258-272.

[9] 王学龙, 张璟. P2P 关键技术研究综述[J]. 计算机应用研究, 2010, 27(3): 801-805.
WANG X L, ZHANG J. Survey on peer-to-peer key technologies[J]. Application Research of Computers, 2010, 27(3): 801-805.

[10] DEMERS A, GREENE D, HOUSER C, et al. Epidemic algorithms for replicated database maintenance[J]. ACM SIGOPS Operating Systems Review, 1988, 22: 8-32.

[11] DECKER C, WATTENHOFER R. Information propagation in the bitcoin network[C]//IEEE Thirteenth International Conference on Peer-to-peer Computing. IEEE, 2013: 1-10.

[12] FADHIL M, OWENSON G, ADDA M. Locality based approach to improve propagation delay on the bitcoin peer-to-peer network[C]//2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM). IEEE, 2017: 556-559.

[13] KANEKO Y, ASAKA T. DHT clustering for load balancing considering blockchain data size[C]//2018 Sixth International Symposium on Computing and Networking Workshops (CANDARW). IEEE Computer Society, 2018: 71-74.

[14] KOSHY P, KOSHY D, MCDANIEL P. An analysis of anonymity in bitcoin using P2P network traffic[C]//Financial Cryptography and Data Security: 18th International Conference. Springer, 2014: 469-485.

[15] BIRYUKOV A, KHOVRATOVICH D, PUSTOGAROV I. Deanonymisation of clients in bitcoin P2P network[C]//ACM SIGSAC Conference on Computer and Communications Security. ACM, 2014: 15-29.

[16] VENKATAKRISHNAN S B, FANTI G, VISWANATH P. Dandelion: redesigning the bitcoin network for anonymity[C]//The 2017 ACM SIGMETRICS. ACM, 2017: 57.

[17] FANTI G, VENKATAKRISHNAN S B, BAKSHI S, et al. Dandelion++: lightweight cryptocurrency networking with formal anonymity guarantees[J]. ACM SIGMETRICS Performance Evaluation Review, 2018, 46: 5-7.

[18] HEILMAN E, KENDLER A, ZOHAR A, et al. Eclipse attacks on Bitcoin's peer-to-peer network[C]//USENIX Conference on Security Symposium. USENIX Association, 2015: 129-144.

[19] APOSTOLAKI M, ZOHAR A, VANBEVER L. Hijacking bitcoin: routing attacks on cryptocurrencies[C]//2017 IEEE Symposium on Security and Privacy (SP). IEEE, 2017: 375-392.

[20] REYZIN L, IVANOV S. Improving authenticated dynamic dictionaries, with applications to cryptocurrencies[C]// International Conference on Financial Cryptography & Data Security. Springer, 2017: 376-392.

[21] ZHANG C, XU C, XU J L, et al. GEM^2-tree: a gas-efficient structure for authenticated range queries in blockchain[C]// IEEE 35th International Conference on Data Engineering (ICDE). IEEE, 2019: 842-853.

[22] REID F, HARRIGAN M. An analysis of anonymity in the bitcoin system[C]//2011 IEEE Third International Conference on Privacy, Security, Risk and Trust. IEEE, 2011: 1318-1326.

[23] MEIKLEJOHN S, POMAROLE M, JORDAN G, et al. A fistful of bitcoins: characterizing payments among men with no names[C]//The 2013 Conference on Internet Measurement Conference. ACM, 2013: 127-140.

[24] AWAN M K, CORTESI A. Blockchain transaction analysis using dominant sets[C]//IFIP International Conference on Computer Information Systems and Industrial Management. IFIP, 2017: 229-239.

[25] SAXENA A, MISRA J, DHAR A. Increasing anonymity in

bitcoin[C]//International Conference on Financial Cryptography and Data Security. Springer, 2014: 122-139.

[26] MIERS I, GARMAN C, GREEN M, et al. Zerocoin: anonymous distributed e-cash from bitcoin[C]//2013 IEEE Symposium on Security and Privacy. IEEE, 2013: 397-411.

[27] SASSON E B, CHIESA A, GARMAN C, et al. Zerocash: decentralized anonymous payments from bitcoin[C]// 2014 IEEE Symposium on Security and Privacy (SP). IEEE, 2014: 459-474.

[28] YIN W, WEN Q, LI W, et al. A anti-quantum transaction authentication approach in blockchain[J]. IEEE Access, 2018, 6: 5393-5401.

[29] DOUCEUR J R. The sybil attack[C]//The First International Workshop on Peer-to-Peer Systems(IPTPS' 01). Springer, 2002: 251-260.

[30] KARAME G O, ANDROULAKI E, CAPKUN S. Double-spending fast payments in bitcoin[C]//The 2012 ACM conference on Computer and communications security. ACM, 2012: 906-917.

[31] LAMPORT L, SHOSTAK R, PEASE M. The byzantine generals problem[J]. ACM Transactions on Programming Languages and Systems, 1982, 4: 382-401.

[32] BANO S, SONNINO A, AL-BASSAM M, et al. Consensus in the age of blockchains[J]. arXiv Preprint, arXiv:1711. 03936, 2017.

[33] DWORK C, LYNCH N, STOCKMEYER L. Consensus in the presence of partial synchrony[J]. Journal of the ACM, 1988, 35: 288-323.

[34] TSCHORSCH F, SCHEUERMANN B. Bitcoin and beyond: a technical survey on decentralized digital currencies[J]. IEEE Communications Surveys & Tutorials, 2016, 18: 2084-2123.

[35] CACHIN C, VUKOLIĆ M. Blockchains consensus protocols in the wild[J]. arXiv Preprint, arXiv:1707.01873, 2017.

[36] CASTRO M, LISKOV B. Practical byzantine fault tolerance and proactive recovery[J]. ACM Transactions on Computer Systems, 2002, 20: 398-461.

[37] ONGARO D, OUSTERHOUT J. In search of an understandable consensus algorithm[C]//The 2014 USENIX Conference on USENIX Annual Technical Conference. USENIX Association, 2015: 305-320.

[38] BALL M, ROSEN A, SABIN M, et al. Proofs of useful work[R]. Cryptology ePrint Archive: Report 2017/203.

[39] MIHALJEVIC B, ZAGAR M. Comparative analysis of blockchain consensus algorithms[C]//International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). IEEE, 2018:1545-1550.

[40] KIAYIAS A, RUSSELL A, DAVID B, et al. Ouroboros: a provably secure proof-of-stake blockchain protocol [C]//Advances in Cryptology – CRYPTO 2017. Springer, 2017: 357-388.

[41] FISCH B. Tight proofs of space and replication[J]. IACR Cryptology ePrint Archive, ePrint-2018-702.

[42] BELOTTI M, BOŽIĆ N, PUJOLLE G, et al. A vademecum on blockchain technologies: when, which, and how[J]. IEEE Communications Surveys & Tutorials, 2019, 21: 3796-3838.

[43] WANG W B, HOANG D T, HU P Z, et al. A survey on consensus mechanisms and mining strategy management in blockchain networks[J]. IEEE Access, 2019, 7: 22328-22370.

[44] YOO J H, JUNG Y L, SHIN D H, et al. Formal modeling and verification of a federated byzantine agreement algorithm for blockchain platforms[C]//IEEE International Workshop on Blockchain Oriented Software Engineering. 2019: 11-21.

[45] ZHENG Z B, XIE S, DAI H, et al. An overview of blockchain technology: architecture, consensus, and future trends[C]// 6th IEEE International Congress on Big Data. IEEE, 2017: 557-564.

[46] YIN M, MALKHI D, REITER M K, et al. HotStuff: BFT consensus in the lens of blockchain[C]// ACM Symposium on Principles of Distributed Computing. ACM, 2019: 347-356.

[47] ALI S, WANG G, WHITE B, et al. Libra critique towards global decentralized financial system[C]// Communications in Computer and Information Science. Springer, 2019: 661-672.

[48] BENTOV I, LEE C, MIZRAHI A, et al. Proof of activity: extending bitcoin's proof of work via proof of stake[J]. IACR Cryptology ePrint Archive, ePrint-2014-25478.

[49] DECKER C, SEIDEL J, WATTENHOFER R. Bitcoin meets strong consistency[J]. arXiv Preprint, arXiv:1412.7935, 2014.

[50] KOKORIS-KOGIAS E, JOVANOVIC P, GAILLY N, et al. Enhancing bitcoin security and performance with strong consistency via collective signing[J]. Applied Mathematical Modelling, 2016, 37: 5723-5742.

[51] BUTERIN V, GRIFFITH V. Casper the friendly finality gadget [J]. arXiv Preprint, arXiv:1710.09437, 2017.

[52] TSCHORSCH F, SCHEUERMANN B. Bitcoin and beyond: a technical survey on decentralized digital currencies[J]. IEEE Communications Surveys & Tutorials, 2016, 18: 2084-2023, 2017.

[53] KIAYIAS A, MILLER A, ZINDROS D. Non-interactive proofs of proof-of-work [J]. IACR Cryptology ePrint Archive, ePrint-2017-963.

[54] LUU L, NARAYANAN V, ZHENG C, et al. A secure sharding protocol for open blockchains[C]//The 2016 ACM SIGSAC Conference on Computer and Communications Security(CCS'16). ACM, 2016: 17-30.

[55] KOKORIS-KOGIAS E, JOVANOVIC P, GASSER L, et al. OmniLedger: a secure, scale-out, decentralized ledger via sharding [C]//IEEE Symposium on Security and Privacy (SP). IEEE Computer Society, 2018: 583-598.

[56] LI S, YU M, AVESTIMEHR S, et al. PolyShard: coded sharding achieves linearly scaling efficiency and security simultaneously[J]. arXiv Preprint, arXiv:1809.10361, 2018.

[57] XIE J F, YU F R, HUANG T, et al. A survey on the scalability of blockchain systems[J]. IEEE Network, 2019, 33: 166-173.

[58] BURCHERT C, DECKER C, WATTENHOFER R. Scalable funding of bitcoin micropayment channel networks[C]//Stabilization, Safety, and Security of Distributed Systems. Springer, 2017: 361-377.

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

[60] BRENT L, JURISEVIC A, KONG M, et al. Vandal: a scalable security analysis framework for smart contracts[J]. arXiv Preprint, arXiv: 1809.03981, 2018.

[61] JIANG B, LIU Y, CHAN W K. ContractFuzzer: fuzzing smart contracts for vulnerability detection[J]. arXiv Preprint, arXiv:1807.03932, 2018.

[62] HASHEMI S H, FAGHRI F, CAMPBELL R H. Decentralized user-centric access control using pubsub over blockchain[J]. arXiv Preprint, arXiv:1710.00110, 2017.

[63] BAO S. CAO Y, LEI A, et al. Pseudonym management through blockchain: cost-efficient privacy preservation on intelligent transportation systems[J]. IEEE Access, 2019, 7: 80390-80403.

[64] SAMANIEGO M, DETERS R. Hosting virtual IoT resources on edge-hosts with blockchain[C]// IEEE International Conference on Computer & Information Technology. IEEE, 2016: 116-119.

[65] STANCIU A. Blockchain based distributed control system for edge computing[C]// International Conference on Control Systems & Computer Science. IEEE, 2017: 667-671.

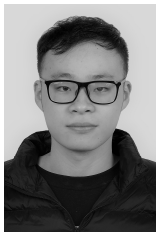
[66] ZIEGLER M H, GROMANN M, KRIEGER U R. Integration of fog computing and blockchain technology using the plasma framework[C]// 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). IEEE, 2019: 120-123.

[67] KIM H, PARK J, BENNIS M, et al. Blockchained on-device federated learning[J]. arXiv Preprint, arXiv:1808.03949, 2018.

[68] BRAVO-MARQUEZ F, REEVES S, UGARTE M. Proof-of- learning: a blockchain consensus mechanism based on machine learning competitions[C]// 2019 IEEE International Conference on Decentralized Applications and Infrastructures. IEEE, 2019: 119-124.

[69] 刘江, 霍如, 李诚成, 等. 基于命名数据网络的区块链信息传输机制[J]. 通信学报, 2018, 39(1), 24-33.
LIU J, HUO R, LI C C, et al. Information transmission mechanism of Blockchain technology based on named-data networking[J]. Journal on Communications, 2018, 39(1): 24-33.

[作者简介]



曾诗钦（1995– ），男，广西南宁人，北京邮电大学博士生，主要研究方向为区块链、标识解析技术、工业互联网。

霍如（1988– ），女，黑龙江哈尔滨人，博士，北京工业大学讲师，主要研究方向为计算机网络、信息中心网络、网络缓存策略与算法、工业互联网、标识解析技术等。

黄韬（1980– ），男，重庆人，博士，北京邮电大学教授，主要研究方向为未来网络体系架构、软件定义网络、网络虚拟化等。

刘江（1983– ），男，河南郑州人，博士，北京邮电大学教授，主要研究方向为未来网络体系架构、软件定义网络、网络虚拟化、信息中心网络等。

汪硕（1991– ），男，河南灵宝人，博士，北京邮电大学在站博士后，主要研究方向为数据中心网络、软件定义网络、网络流量调度等。

冯伟（1980– ），男，河北邯郸人，博士，工业和信息化部副研究员，主要研究方向为工业互联网平台、数字孪生、信息化和工业化融合发展关键技术等。