区块链信息系统研究进展与趋势

CCF 信息系统专业委员会

邢春晓[1]　于　戈[2]　李庆忠[3]　金澈清[4]　李瑞轩[5]　王　鑫[6]　张桂刚[7]

[1]清华大学，北京
[2]东北大学，沈阳
[3]山东大学，济南
[4]华东师范大学，上海
[5]华中科技大学，武汉
[6]天津大学，天津
[7]中国科学院自动化研究所，北京

摘　要

区块链应用系统的普及是区块链技术成熟的重要标志。本文从体系架构、建模方法、存储管理、联邦计算、跨链互操作、隐私保护、链上链下融合、云边端融合八个方面对区块链系统的国内外现状及比较做了系统的分析。从区块链＋数字金融、区块链＋电子政务、区块链＋电子商务、区块链＋智慧医疗、区块链＋智能制造以及区块链＋绿色农业几个方面进行了应用分析。最后，提出了区块链信息系统的发展趋势和展望。

关键词：区块链，信息系统，体系架构，建模方法，存储管理，联邦计算，跨链互操作，隐私保护，链上链下融合，云边端融合

Abstract

The popularization of blockchain application systems is an important sign of the maturity of blockchain technology. This development report makes a comparison of the current situation and comparison of blockchain systems at home and abroad from eight aspects: architecture, modeling methods, storage management, federated computing, cross-chain interoperability, privacy protection, on-chain and off-chain integration, and cloud-end integration. A systematic analysis. The application analysis is carried out from the aspects of blockchain + digital finance, blockchain + e-government, blockchain + e-commerce, blockchain + smart healthcare, blockchain + smart manufacturing, and blockchain + green agriculture. Finally, the development trend and outlook of the blockchain information system are proposed.

Keywords: blockchain, information systems, architecture, modeling methods, storage management, federated computing, cross-chain interoperability, privacy protection, on-chain and off-chain integration, cloud-edge fusion

1 引言

1.1 区块链信息系统的基本架构

2008 年，化名为“中本聪”（Satoshi Nakamoto）的学者提出了一种被称为比特币的数字货币，该数字货币在没有任何权威中介机构统筹的情况下，互不信任的人可以直接用比特币进行支付[1]。2013 年 12 月，Vitalik Buterin 提出了以太坊（ethereum）区块链平台，以太坊除了可基于内置的以太币（ether）实现数字货币交易外，还提供了图灵完备的编程语言以编写智能合约（smart contract），从而首次将智能合约应用到了区块链[2]。以太坊的愿景是创建一个永不停止、无审查、自动维护的去中心化的世界计算机。Linux 基金会发起的 Hyperledger 开源区块链项目，旨在发展跨行业的商业区块链平台。Hyperledger 提供了 Fabric、Sawtooth、Iroha 和 Burrow 等多个区块链项目，其中最受关注的项目是 Fabric。Hyperledger Fabric 专门针对企业级的区块链应用而设计，并引入了成员管理服务[3]。2016 年 4 月，R3 公司发布了面向金融机构的分布式账本平台 Corda[4]。该公司发起的 R3 联盟包括花旗银行、汇丰银行、德意志银行、法国兴业银行等 80 多家金融机构和监管成员，R3 声称 Corda 是受区块链启发的去中心化数据库，而不是一个传统的区块链平台，原因就是 R3 反对区块链中每个节点拥有全部数据，而注重保障数据仅对交易双方及监管可见的交易隐私性[5]。一般说来，区块链系统由数据层、网络层、共识层、激励层、合约层和应用层组成。如图 1 所示。

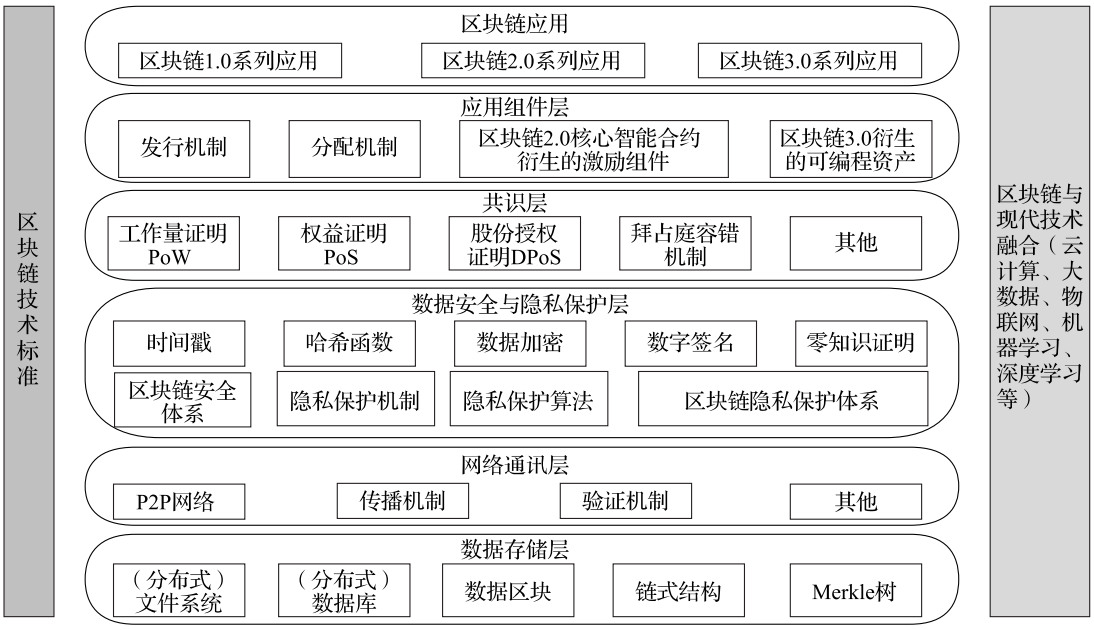

图 1　区块链基础架构模型

1.2 区块链信息系统的关键技术

区块链信息系统的关键技术包括共识机制、密码学技术、数据存储技术、智能合约等。

共识机制：共识机制保障区块链在不可信环境（即存在一定数量的拜占庭节点）中保持一致。常见的共识机制包括工作量证明机制（PoW）、权益证明机制（PoS）和实用拜占庭容错（PBFT）等，其中 PoW 与 PoS 常被用于公有链系统中，而 PBFT 主要定位于私有链或者联盟链。在 PoW 中，所有节点竞争解决一个哈希难题以获得记账权（出块），这会消耗大量算力；在 PoS 中，为了降低节点的算力消耗，账本的记账权由各节点所拥有的权益来决定；在 PBFT 中，各个节点轮流成为主节点并负责发起投票，整个过程包括一轮消息分发和两轮投票，从而达成一致。PBFT 是确定性共识算法，一旦共识达成就不可颠覆（不分叉），但该算法需要一定的同步网络假设且能够支持节点数量有限。

密码学相关技术：密码学相关技术支撑区块链在不可信环境下构建多方安全的计算模型，典型技术包括哈希、加解密、数字签名等。哈希算法将数据从原始空间映射到目标空间，且满足三个基本特性：1）抗冲突，极难找到两个哈希值相同的不同数据；2）不可逆，无法通过哈希值推断出原始数据；3）雪崩效应，任何原始数据的细微改变都会造成哈希值的显著变化。加解密算法可保护数据隐私等，通过赋予加密算法一些额外的特性可以使得密文具备一定的查询处理能力，例如同态加密和保序加密。数字签名可验证数据完整性，一些进阶的签名算法包含更复杂的功能，如盲签名、环签名、群签名等；聚合签名和门限签名可以将多个签名聚合成单个签名，这一特性可用于在 PBFT 等共识算法中压缩通讯量。

数据存储技术：区块链信息系统包含区块数据和状态数据。区块数据指的是组成区块链的链式结构中的每一个区块；状态数据是在采用账户模型的区块链系统中可供智能合约读取写入的键值对集合。通常状态数据采用 Merkle tree 及其变种进行组织管理，根节点的哈希值作为整棵树的摘要信息存储在链上。由于拜占庭节点的存在，区块链信息系统通常需要采取全副本存储机制，即需要在每个全节点都完整保存全体数据，但是会带来较大的存储压力。近年来，基于纠删码的区块链数据分片存储策略可以将全体数据分割存储到不同的节点上，从而极大降低了存储开销。

智能合约：智能合约是一段运行在区块链上的代码，在触发条件满足时可自动执行合约逻辑，并被全网共识。智能合约大致可以分为脚本型、图灵完备型和可验证合约型，其运行环境可以分为嵌入式运行、基于虚拟机运行和基于容器运行[6]。比特币支持嵌入式运行的智能合约脚本，可在交易过程中实现基于数字签名的电子货币交易或运行简单的逻辑过程；以太坊支持图灵完备的智能合约，在以太坊虚拟机（EVM）中执行，EVM 作为独立运行的沙盒，保证了执行合约代码时的隔离性；Fabric 的智能合约（链码）也是图灵完备的，在 Docker 容器中执行。

1.3 区块链信息系统的应用系统

利用区块链技术为数字社会构建一个信任的基础设施迫在眉睫。如果在数字社会中形成区块链应用生态，区块链技术需要跟各行业的应用进行深度融合。区块链技术充当信息系统应用的信任基础设施，传统的业务则使用传统的应用方式实现。这种应用融合方式已成为当前区块链信息系统的发展趋势。然而，当前区块链信息系统应用面临着许多挑战。

（1）区块链生态急需区块链体系架构具有应用独立性

一个区块链产业生态不只是由一个封闭的应用构成。同一个数字资产需要在多个机构、部门、企业、个体之间进行可信传递和流转，该数字资产会被多个应用处理，从而形成一个很长的区块链应用生态。因此区块链架构应该具有很强的应用独立性，使得不同应用开发商能够方便地在同一个区块链生态上开发不同的应用。

（2）区块链能够管理不同资产的不同状态

在数字经济与社会中，区块链所管理的数字资产不同于加密数字货币。数字经济与社会中的数字资产的状态是千变万化的，需要区块链底层能够支持资产的多重状态并保持完整和一致。

（3）智能合约与应用的融合

在我国支撑信息系统应用的区块链大都是联盟链，基于区块链的应用跟传统应用紧密结合，原中心化的应用与多中心化的区块链融合开发，在多个行业和场景中发挥作用。因此目前大多数基于区块链的应用并不依赖于智能合约。智能合约是对应用的规范和补充。迫切需要探讨和研究应用开发智能合约开发规范，合理设计应用与智能合约的职责。

（4）链内链外业务融合

基于区块链的信息系统应用需要打通链内链外数据，使得链外数据能够真实地进入区块链，形成区块链上的数字资产，同时区块链交易所产生的可信交易数据，也能够反馈回信息系统。由于数字资产内容容量较大或者隐私保护要求比较高，数字资产内容本身不易放到区块链上，信息系统需要将一部分数字资产的数据放到链下，一部分数字资产的数据放到链，实现链上链下数据统一管理。

（5）跨链应用

在数字经济社会中，价值和信任的传递往往会在多个区块链上进行。大多数文献中论述的多链一般是指跨链机制和技术，所描述的跨链机制和技术都是针对完全独立的多个区块链进行的，没有考虑统一主体身份的问题。在研究统一主体身份的同时，还需研究同一主体多个区块链账户融合机制、多链密钥管理机制以及多链加解密机制等等。

（6）行业应用

从当前行业发展状况来看，区块链已经发展到赋能个领域并不断实现落地的阶段。近年来，互联网公司、金融公司已经在区块链的探索中发布了自己的区块链平台，中小型企业也加快了区块链技术的探索。区块链信息系统在数字金融、电子政务、电子商务、

绿色农业、智慧医疗以及智能制造领域得到了初步的应用。

2 国际研究现状

2.1 区块链信息系统的体系架构

从最早应用区块链技术的比特币到引入智能合约的以太坊，再到应用最广的联盟链 Hyperledger Fabric，它们尽管在具体实现上各有不同，但在整体体系架构上存在着诸多共性。区块链平台整体上可划分为成网络层、共识层、数据层、智能合约层和应用层五个层次。

1）网络层。2001 年，Gribble 等人[7]提出将 P2P 技术与数据库系统进行联合研究。早期的 P2P 数据库没有预定的全局模式，不能适应网络变化而查询到完整的结果集[8-9]，因而不适合企业级应用。区块链网络节点具有平等、自治、分布等特性，所有节点以扁平拓扑结构相互连通，每个节点均拥有路由发现、广播交易、广播区块、发现新节点等功能[10]。在区块链网络中，节点时刻监听网络中广播的数据，当接收到邻居节点发来的新交易和新区块时，其首先会验证这些交易和区块是否有效，包括交易中的数字签名、区块中的工作量证明等，只有验证通过的交易和区块才会被处理（新交易被加入正在构建的区块，新区块被链接到区块链）和转发，以防止无效数据的继续传播。

2）共识层。为了解决节点自由进出可能带来的女巫攻击（sybil attack）[11]问题，比特币应用了工作量证明（Proof of Work，PoW）机制。PoW 源自 Dwork 等人[12]防范垃圾邮件的研究工作，即只有完成了一定计算工作并提供了证明的邮件才会被接收。比特币要求只有完成一定计算工作量并提供证明的节点才可生成区块，每个网络节点利用自身计算资源进行哈希运算以竞争区块记账权，只要全网可信节点所控制的计算资源高于 51%，即可证明整个网络是安全的[13]。为了避免高度依赖节点算力所带来的电能消耗，研究者提出一些不依赖算力而能够达成共识的机制。点点币（peercoin）应用了区块生成难度与节点所占股权成反比的权益证明（Proof of Stake，PoS）机制[14]；比特股（Bitshares）应用了获股东投票数最多的几位代表按既定时间段轮流产生区块的股份授权证明（Delegated Proof of Stake，DPoS）机制[15]。Hyperledger Sawtooth 应用了基于 Intel SGX 可信硬件的逝去时间证明（Proof of Elapsed Time，PoET）机制。基于证明机制的共识通常适用于节点自由进出的公有链，比特币与以太坊使用 PoW 机制；基于投票机制的共识则通常适用于节点授权加入的联盟链，Hyperledger Fabric 使用 PBFT 算法。

3）数据层。在数据结构的设计上，现有区块链平台借鉴了 Haber 与 Stornetta[16-18]的研究工作。时间戳服务器对新建文档、当前时间及指向之前文档签名的哈希指针进行签名，后续文档又对当前文档签名进行签名，如此形成了一个基于时间戳的证书链，该链反映了文件创建的先后顺序，且链中的时间戳无法篡改。在数据模型的设计上，比特币

采用了基于交易的数据模型，每笔交易由表明交易来源的输入和表明交易去向的输出组成，所有交易通过输入与输出链接在一起，使得每一笔交易都可追溯；以太坊与 Hyperledger Fabric 需要支持功能丰富的通用应用，因此采用了基于账户的模型，可基于账户快速查询到当前余额或状态[19]。

4）智能合约层。智能合约是一种用算法和程序来编制合同条款、部署在区块链上且可按照规则自动执行的数字化协议。该概念早在 1994 年由 Nick Szabo 提出[20]，起初被定义为一套以数字形式定义的承诺，包括合约参与方执行这些承诺所需的协议，其初衷是将智能合约内置到物理实体以创造各种灵活可控的智能资产。以太坊提供了图灵完备的脚本语言 Solidity、Serpent 与沙盒环境 Ethereum VirtualMachine（EVM）[21]，以供用户编写和运行智能合约。Hyperledger Fabric 的智能合约被称为 Chaincode，其选用 Docker 容器作为沙盒环境，Docker 容器中带有一组经过签名的基础磁盘映像及 Go 与 Java 语言的运行时和 SDK，以运行 Go 与 Java 语言编写的 Chaincode[22]。

5）应用层。比特币平台上的应用主要是基于比特币的数字货币交易。以太坊除了基于以太币的数字货币交易外，还支持去中心化应用（Decentralized Application，Dapp），Dapp 是由 JavaScript 构建的 Web 前端应用，通过 JSON-RPC 与运行在以太坊节点上的智能合约进行通信。Hyperledger Fabric 主要面向企业级的区块链应用，并没有提供数字货币，其应用可基于 Go、Java、Python、Node. js 等语言的 SDK 构建，并通过 gPRC 或 REST 与运行在 Hyperledger Fabric 节点上的智能合约进行通信。

2.2 区块链信息系统的建模方法

区块链信息系统具有多种建模方式。从网络建模角度出发，可分为全局网络建模方式和分片网络建模方式；从数据建模角度出发，可构建 UTXO 模型、账户模型和区块链数据库模型。

（1）网络建模：全局网络与分片网络

全局网络建模是指区块链中所有全节点通过共识机制对等协商，共同维护区块链。这些节点存储完整的账本数据（账户模型下还包括状态数据），并执行所有交易。这对系统的存储、计算和网络造成了较大压力，对参与的节点提出了更高的配置要求。

分片（sharding）网络建模将所有网络节点划分成多个小组（分片），各分片独立运行共识算法出块，从而提高交易吞吐量；但是单个分片的安全性也会降低，比如在极端情况下单个分片内部可能全部是拜占庭节点。典型工作包括 Elastico[23]、Omniledger[24]、Chainspace[25]、RapidChain[26]等。Elastico 首先采用 PoW 算法进行分组，再在组内通过 PBFT 共识出块。为了确保在单个分片内部的拜占庭节点数量不超过 1/3，各分片至少包含 600 个节点。为确保跨片事务的原子性，Omniledger 和 Chainspace 分别提出了拜占庭分片原子提交协议（Atomix）和分布式提交协议 *S*-BAC。RapidChain 将状态数据进行分片以提高系统的扩展性。

总体来说，全局网络建模方式的资源开销大，但是安全性高；分片网络建模方式提

高了执行效率，但是在分片的安全性与稳定性、跨分片事务处理等方面存在重大挑战。

（2）数据建模：UTXO 模型、账户模型与数据库模型

区块链数据建模主要包含三种方式，UTXO（Unspent Transaction Output，未花费交易输出）模型、账户模型和数据库模型。以比特币为代表的早期代币系统多采用 UTXO 模型，每笔交易需要指定一个或多个 UTXO，输出同样为一个或多个 UTXO；每个 UTXO 只能被引用一次，且被引用之后无法再被后续交易作为输入引用。这种方式的表达能力较弱，无法支持复杂场景。以太坊采用账户模型，每个实体对应一个账户。用户可以编写智能合约实现灵活复杂的业务逻辑，并维护账户余额或者合约内部存储等信息。

近年来，将区块链与数据库相结合以构建区块链数据库成为研究热点。BigchainDB 将区块链特性融入分布式系统中，兼具高吞吐、低延迟、大容量等分布式数据库特点和去中心化、不可篡改等区块链特点[27]。BigchainDB 网络中的节点通过 Tendermint 的 BFT 共识算法来达成一致，并将数据存放在分布式 MongoDB 数据库中。达姆施塔特工业大学研发 BlockchainDB 将区块链作为底层存储层，在区块链上抽象出数据库层，用户通过数据库层访问底层数据[28]。2019 年，Oracle 推出的 20c 版本融入了区块链特性，支持创建 blockchain table，该表中仅支持数据以“增添”（append）方式存入，且无法被修改。

可以看出，数据库模型的表达能力要远远优于 UTXO 模型和账户模型。

2.3 区块链信息系统的存储管理

目前绝大多数的区块链系统采用以 LevelDB 为代表的基于键值模型的数据库系统存储数据，并通过 LSM-tree 结构[29]提高对交易的存储写入效率和查询效率。其中较为典型的系统有：1）比特币系统中将区块数据存储在文件系统中并使用 LevelDB 存储区块数据的索引。2）以太坊的底层使用 LevelDB 作为数据存储系统同时存储区块链数据和对应的索引数据。3）超级账本 Fabric 系统在 0.6 版本及之前，其底层使用 LevelDB 存储系统。随后在 Fabric 1.0 版本的更新中，系统给用户提供了 LevelDB 与 CouchDB 两种存储系统作为选择。4）基于区块链的云存储系统 Storj[30]使用 LevelDB 存储区块链数据，并使用 LevelUP 接口作为系统与 LevelDB 之间的连接层。

以 LevelDB 为代表的键值数据存储系统无须安装部署且写性能高效，能够充分实现去中心化的理念，但是无法满足企业级业务需求。因此，越来越多的工作开始结合传统的数据库系统和区块链技术进行数据管理。BigchainDB 直接以分布式数据库系统为基础增加区块链特性，底层存储使用 MongoDB 数据库从而支持高吞吐量和大容量。BlockchainDB[31]将区块链作为存储层，并在其上构建数据库层，通过经典的数据管理技术（例如分片）以及标准化的查询接口来扩展区块链，将现有的区块链系统用作防篡改和分散的存储。ForkBase[32]通过设计高效的索引结构和数据模型，这使其能够与超级账本系统结合。

区块链系统具有非交易数据的分布式存储功能，但现有区块链系统为了保证链上存储空间的使用效率，都设计了相应的存储扩展机制实现对附加数据的存储，以避免非交易信息过多的占用区块空间。

1）链下存储机制。将存储在区块体中的数据转移到链下存储系统中进行存储，区块体中存储指向这些数据位置的“指针”和其他信息的存储扩展机制。当进行数据存储时，原始数据被存储在链下存储系统中，根据一定的规则生成原始数据存储位置的唯一标识，并将其存储在区块链系统中。当进行数据访问时，再根据这个唯一标识在链下存储系统中访问原始数据。目前常用的链下存储机制主要为星际文件系统（Inter-Planetary File System，IPFS），存储在 IPFS 上的文件将被自动分片并加密分散存储，同时自动消除重复文件，这保证了文件存储的安全性和高效性。

2）多链存储机制。将存储在一条区块链中的数据分别存储在多条区块链中，并根据一定的规则进行管理的存储扩展机制。电子货币 EDUCare 使用的框架采用并行多主链结构，分为 Token 链和 DApp 链，其中不同的主链可以采用不同的共识机制。这样，用户可以将账户信息存储在主链用户系统上，而基于智能合约的 DApp 存储在其他主链上。该框架为解决跨链资源交换问题设定的基本原则是不同主链上的代币交易所消耗手续费由交易发生主链决定。多链技术为区块链的存储容量扩展提供了有效的解决方案。

2.4　区块链信息系统的联邦计算

区块链信息系统使得用户在无须构建信任的前提下，自发地组成一个完整的分布式系统，通过发布自定义联邦计算算法发起联邦计算，使得普通用户能以很低的成本就能享受到联邦计算带来的好处，因而具有广泛的发展前景。联邦计算涉及分布式计算、分布式学习和联邦学习等技术，尤其是在 2016 年谷歌提出联邦学习[33]概念后，国际学者对涉及的相关领域进行了更加广泛的研究。

联邦学习作为一种分布式机器学习的框架，吸收了分布式计算和分布式学习的思想，客户端在中央服务器的协调下协作地训练模型，训练数据保留在客户端本地而无须上传至数据中心从而避免了数据泄露，同时通过本地多次梯度计算迭代减少了通信轮次从而提高了效率。针对联邦学习中心服务器不可信的问题，Lugan 等人[34]通过使用区块链和加密机制，提出了一种可扩展的安全计算架构，保证了分布式学习中数据隐私的安全、迭代学习的可信序列以及联盟成员之间共享学习模型的公平。Awan 等人[35]提出了一种基于区块链的隐私保护联邦学习框架，利用区块链的不可篡改性和去中心化特征来保证联邦学习模型的可靠更新。Lyu 等人[36]针对集中架构下中心服务器存在的可靠性和鲁棒性问题，提出了一种去中心化的深度学习框架，采用分层加密方案保护模型的梯度，并利用区块链的去中心化特性保证模型的可靠性。

在最近几十年，拜占庭容错协议和共识算法作为分布式系统的底层技术支撑，一直是分布式计算领域的研究热点。针对区块链信息系统环境下的容错和共识问题，Sivio Micali 等人[37]提出了一种称为 AlgoRand 的快速拜占庭容错共识算法，该算法利用密码抽签技术选择共识过程的验证者和领导者，通过减少新区块达成共识时的开销和分叉提高计算效率。Rafael Pass 等人[38]提出了一种称为休眠共识的新算法，针对大规模的共识节点中多数都处于离线状态，仅有少数节点在线参与共识过程时，传统共识算法无法保证

共识安全性的问题，新共识算法仅需在线诚实节点的数量超过故障节点的数量，即可保证系统的安全性和鲁棒性。

针对区块链信息系统的联邦计算研究，国外研究者目前主要集中在计算框架和共识算法方面，通过结合区块链技术和联邦学习的思想，构建更加安全可靠的可扩展计算框架，并通过优化共识过程提升计算效率。但是目前大量的研究工作仍然处于起步阶段，尚未形成成熟的联邦计算解决方案，相关问题还有待进一步研究。

2.5 区块链信息系统的跨链互操作

跨链互操作（cross-chain interoperability）是指支持跨过多个独立的、自主的区块链的链间处理，而在一个链内部由于业务或系统扩展需要而进行划分的多个物理子链之上的链内处理，称为多链操作（multi-chain operability））。在本文，将支持跨链互操作应用的区块链技术，称为跨链互操作技术。

目前，国际上使用的主要技术有四大类[39-40]：

（1）侧链/中继（Sidechains/relays）

侧链方案是由比特币核心开发者首先提出的，Blockstream 公司在 2014 年发布的白皮书中[41]，提出了楔入式侧链（Pegged sidechain）概念及其协议的实现方案，将提供了新功能的区块链作为侧链，与主链一起协同工作。BTC Relay 是以太坊基金会支持开发的第一个侧链[42]，实现以太坊区块链与比特币区块链的连接。2016 年 Blockstream 公司又提出了强联邦式侧链（sidechains with strong federation）[43]，支持多重签名，提高效率和互操作性。

侧链技术可以通过中继的方式实现，将中继器作为主链和侧链之间进行价值和信息交换的通道。区块链也可作为中继链，进行链间的可信验证和交易确认。目前，已开发了多种中继器，包括：BTC-Relayer 中的 Replayer[42]、Polkadot 中的 Replay Chain[44]、Cosmos 中的 Hub[45]。

（2）公证人模式（Notary Schemes）

公证人模式是基于 interledger 协议创造的一种技术框架[46]，与现实世界中的中介机制类似，引入交易双方能够共同信任的第三方充当公证人来作为中介，公证人既可以自动的监听和响应来自链上的交易请求和确认信息，也可以主动地对发生的事件或请求进行监听和响应。公证人模式分为单签名公证人、多签名公证人和分布式签名公证人。分布式签名公证人模式采用安全多方计算的思想，安全性更高，但实现难度也更大。

（3）哈希锁定（Hash-locking）

哈希锁定的算法思想见文献［47］，其本质上是使用哈希锁定智能合约来安全地进行 0 确认交易。闪电网络是哈希锁定技术综合的典型应用[47]，目的是安全地实现链下可扩展的小型即时交易，提升链下的交易处理能力。它有两种交易合约：到期序列可撤销合约 RSMC（Revocable Sequence Maturity Contract）以及哈希时间锁合约 HTLC（Hashed Timelock Contract）。HTLC 同时使用了哈希锁定和时间锁定，使得用户进行的 0 确认交易

与在比特币网络上一样安全。

(4) 分布式私钥控制 (Distributed Private Key Control)

分布式私钥控制是采用密码学中的私钥生成与控制技术，其代表项目有 Fusion[48] 和 Wanchain[49]。分布式私钥控制主要包括锁定和解锁的两个操作。锁定就是通过对于密钥控制的数字货币资产，实现分布式的控制权的管理以及对于资产的映射操作，解锁是利用分布式私钥对于锁定的代币进行解锁操作，使代币由原先的不可操作状态变成可转移可操作状态。在 Fusion 系统中[48]，利用分布式密钥生成算法和门限签名技术，保证了跨链的资产锁定和解锁由系统参与共识的所有节点共同决定，并且保证任一节点或者少数节点合谋都无法拥有该资产的使用权。

2.6 区块链信息系统的隐私保护

区块链的隐私保护及安全性研究受到各国机构和研究学者的关注。最初，比特币采用了简单的隐私保护方案，即采用伪匿名的方式将系统中节点的地址与现实用户的身份分离。但是随着人们对比特币研究的深入，以大数据分析、聚类分析为主构造的交易图技术一定程度上破坏了比特币的隐私性。2015 年发布的达世币，以中心化混币技术较好得解决了比特币的隐私保护缺陷。门罗币采用环签名等多种密码技术更好地实现了区块链的隐私保护。Zcash 使用承诺和零知识证明的技术实现了区块链的隐私保护。

达世币 (DASH)[50]是一种采用中心化混币的方案，也被认为是采用中心化混币最成功的方案。在 DASH 中，采用了类似押金的策略，作为执行混币操作的主节点，在参与混币之前，要先向系统提交 1000DASH 作为押金，一旦主节点存在做坏行为，押金就会被没收，这样增加了主节点做坏的代价，作为理智的主节点，正常情况下不会故意执行做坏行为。

门罗币 (Menero)[51]是一种运用大量密码学技术的以隐私保护著称的密码货币。在 Menero 中，同样存在混币操作，但是 Menero 的混币并不是简单的混币，这里的混币是通过环签名技术进行的。其最大的优势是混币操作可以在没有中心化第三方参与的情况下，由一个节点完成，这样既可以避免中心化混币带来的中心化问题，又可以解决去中心化混币中，参与混币节点相互通信，泄露混币过程以及黑客进行拒绝服务攻击的问题。不可链接性 (Unlinkability) 和不可追踪性 (Untraceability) 是比特币没有实现的属性，但是这两个属性是保证区块链隐私性的关键要素，Menero 中对这两个属性具有较好的实现。

Zcash[52]是在 Zerocoin 项目[53]基础上发展而来的一种加密货币。Zerocoin 项目的核心是要提高比特币的匿名性，进一步加强隐私保护。Zerocoin 主要通过在比特币主链上增加侧链的技术，来达到隐私保护的目的。一笔交易发出时，首先被拆分成多份小交易，发送到全网，然后在到达交易接收者地址之前，再将多笔小交易合并成之前的交易。而 Zcash 使用承诺函数将交易的发送地址、接收地址以及交易金额封装在多个参数中，而在验证交易时，使用零知识证明技术 zk-SNARKs[54]，从而保护交易发送者地址、交易接收

者地址和交易金额等信息不被泄露。

2.7 区块链信息系统的链上链下融合技术

链上链下融合机制是指实现信息系统与区块链系统之间业务融合的一类技术的总称，是实现信息系统与区块链系统无缝链接的桥梁。基于链上链下融合机制，信息系统与区块链对接以解决信息孤岛、防篡改等问题，实现信息共享、业务联动等。链上链下融合机制主要包括输入输出融合、数据融合、流程融合等关键技术，每种关键技术并非独立存在，互联共通实现共同实现业务融合。

（1）数据融合

数据融合是指在信息系统与区块链系统各存储部分数据的情况下实现业务融合，主要包括两种方式：1）链上存储数据的关键信息、链下存储数据内容，2）链下存储数据数字化信息，链下存储数字化数据链上的信息，例如索引、账户地址、交易地址等。

医疗是链上链下数据融合的应用案例最多、最常见的领域，例如，Azaria 等人[55]提出一种基于区块链的分布式 EMR 管理模型，通过链上存储 EMR 元数据与链下存储具体内容相结合的方式来解决 EMR 在不同医院、科研机构共享过程中真实性难以验证、不可篡改性难以保证等问题。

区块链是解决供应链溯源的一个有效途径，Malik 等人[56]提出了一种基于区块链的结合 IoT 的供应链管理模型，将商品、产品等数字化信息存储于区块链中，商品、产品等在区块链上的账户地址、交易地址等存储于链下信息系统，并且链下信息系统可通过区块链验证商品、产品的真实性，解决供应链溯源过程中信息的真实性、不可篡改性难以保证的问题。

（2）流程融合

流程融合是指信息系统与区块链系统各执行部分流程的情况下实现业务融合，主要包括两种方式：1）链下执行，链上存储结果，2）链上与链下混合执行。

Prybila[57]基于比特币区块链设计了一种运行时验证的业务流程机制，通过在区块链中为每个流程创建一个令牌，令牌存储流程的执行状态，例如流程 ID、下一个任务 ID、时间戳、前一个任务的结果的摘要值、下一个执行方的签名等信息；获取令牌的执行方再将本系统的执行结果写入令牌中并传递给下一个执行方；通过区块链存储各个流程执行方执行的流程的结果的验证与流程执行权的传递，实现分布式协作环境下流程的结果的互认与可验证。

Weber[58]设计了一种基于区块链的链上链下流程协同机制，将各方共享的流程结果及其执行结果编写成智能合约，各方通过监视器实时获取智能合约执行的结果并触发自己独有的处理流程，由此实现协作流程执行的监控过程中结果的互认、验证等。

（3）输入输出融合

输入输出融合是指将信息系统（链下）的数据自动采集到区块链系统中并将区块链系统的执行结果反馈至信息系统，预言机作为区块链获取外界数据的通道，将链下信息

系统中的数据根据预先设置的规则自动输入到区块链中，预言机广泛应用于金融、物流、供应链、物联网等领域。

Goel 等人[59]在不依赖可信信息提供者的情况下，设计了一种基于预言机的去中心化的分布式问答模型，用户将问题提交至区块链，服务提供商通过预言机获取外部答案并上传至区块链，通过承诺 - 披露机制与经济模型激励链下有效的输入正确答案。

Chainlink[60]设计了一种多异构数据源采集机制，基于声誉系统与激励机制解决单一数据源数据误差等中心化风险等，并提供了基于 TEE 安全方案，进一步保证数据采集、数据验证过程中的安全性。

2.8 区块链信息系统的云边端融合技术

边缘计算可在网络边缘处理或预处理终端收集或产生的数据，无需将全部数据上传云端，从而减轻云计算中心的网络负载与计算能耗、降低服务延迟与隐私泄露风险[61]。但在处理复杂的统计与分析任务时，边缘计算服务有限的计算和存储能力不能满足任务的需求，需要将边缘计算和云计算结合，互为补充，同时结合终端设备产生的海量数据构建一个层次型的云边端结构来满足复杂任务的需求。在云边端融合架构中，由于边缘服务器或不同的云服务节点等可能分属不同利益方，且在复杂环境下云边端系统易受到攻击，引入区块链技术为解决这些问题提供了新思路。

（1）融合区块链的云边端体系结构

Sharma 等人[62]利用软件定义网络（SDN）和区块链构建混合网络架构，每个边缘节点都作为一个 SDN 控制器，从而保证系统灵活、安全，降低硬件管理成本。另外，整体网络结构包括两部分：核心网络和边缘网络。核心网络由具有较高计算和存储资源的节点组成，主要扮演区块链网络的矿工节点，负责创建区块、产生工作量证明验证等；而能力较弱的边缘节点仅充当各个边缘区域的中央服务器，在靠近服务请求者的位置提供服务，降低服务响应延迟并减少网络负载。该体系结构最大的特点系统架构具有较好的弹性，同时可以限制恶意攻击或节点故障的影响范围。Stanciu[63]提出了一种云边端三层架构，在云端部署了 Hyperledger Fabric 验证节点，在边缘节点部署 Docker 容器实现边缘服务的功能模块、Kubernetes 平台用于协调跨边缘资源执行容器，并通过智能合约保证边缘交易执行的正确性和安全性，在边缘的物理设备和资源都被建模成为执行动作逻辑的元素来构建一个大型分布式系统处理终端产生的数据，响应终端请求的服务等。

另外，还有一些工作将云边端架构和区块链应用到具体的场景中，包括智能家居、智慧城市、共享经济、家庭医疗等。下面简单描述这些工作的基本思路：Dorri 等人[64]提出一种安全框架，将区块链技术集成到智能家居中来确保数据完整性、隐私性和可用性。Khan 等人[65]提出了一种基于区块链技术的边缘计算架构，实现不同行政部门对数据的细化和安全管理。Rahman 等人[66]利用区块链技术设计基础设施，以满足智能城市中智能合约的安全性和隐私性要求。在该架构中，地理标记的多媒体交易由边缘服务器处理，关键信息由人工智能技术提取，然后将处理结果保存在区块链和分布式云存储中，以支

持共享经济服务。Rahman[67]提出了一种家庭医疗管理框架，利用物联网节点和基于区块链的分布式移动边缘计算来支持数据共享场景下的低延迟、安全、匿名且高可用的时空多媒体治疗数据通信。

（2）云边端融合环境下区块链性能提升

在云边端融合的场景之下，终端和边缘计算设备的存储、计算能力有限，这对区块链在边缘环境下的实际部署造成巨大挑战。

Xiong 等人将计算服务提供商和矿工之间的交互建模为 Stackelberg 博弈，计算服务提供商首先设置计算的服务价格，矿工在知道计算服务提供商设定的价格之后决定自己的计算服务需求[68]。博弈的目的是找到 Stackelberg 平衡，确保计算服务提供商选择的服务价格来使其利润最大化，同时能够及时响应满足矿工的需求。Luong 等人将矿工挖矿的计算需求和计算服务提供商提供计算服务描述为一个拍卖过程，基于深度学习构造多层神经网络以实现针对边缘资源分配的最佳拍卖策略，并使用矿工的估值作为数据训练来调整神经网络的参数，从而优化损失函数（边缘计算服务提供商的预期负收益）[69]。Huang 等人通过存储元数据而非实际数据来压缩数据块，从而实现对等边缘环境的最佳资源分配[70]。元数据项包括用户签名来防止数据被非法修改，节点会将收到的元数据项包装成块。鉴于边缘环境下的节点特性差异显著，该文还设计了一个最佳数据存储策略以在边缘设备之间实现公平有效的数据分配。

3 国内研究进展

3.1 区块链信息系统的体系架构

根据赛迪全球公有链评估指数，仅作为评估对象的全球主流公链平台已超过 30 个。实际上，全球公有链项目远超过这个数目，而且数量上还在不断增加。不同区块链平台之间在设计理念和实现方面不尽相同，在区块链底层架构的标准尚未达成共识之前，区块链平台技术与应用的竞争日趋激烈。公有链方面，以以太坊、EOS 为代表的区块链平台在全球范围内具有极强的影响力，其技术与应用生态正得到市场的认同。国内 NEO、公信宝、星云链等公有链项目提出了各自基础架构设计理念并予以实现，同时积极推进开源社区建设和应用生态完善。但相比国外优秀公链项目，国内公有链平台仍处于跟随状态。联盟链平台方面，IBM 的 Fabric 已经成为联盟链技术平台的典范。基于 Fabric 的行业解决方案已经在金融、供应链、存证、物流等诸多领域得到广泛应用。国内微众银行、万向区块链及矩阵元三方共同开发了 BCOS 区块链开源平台，提供企业级应用服务。区块链 BaaS（区块链即服务）平台方面，国内互联网巨头纷纷战略布局。2017 年 4 月，腾讯发布区块链白皮书并推出可信区块链 Trust SQL；2018 年 3 月，京东全面启动了区块链技术在业务场景中的应用探索与研发实践；2018 年 8 月，阿里云宣布发布企业级 BaaS

平台，支持一键快速部署区块链环境，实现跨企业、跨区域的区块链应用。据不完全统计，截至2018年11月，已有9家大型互联网企业发布BaaS平台。2019年，区块链底层平台发展百花齐放，区块链底层平台研发、应用推广、生态培育的竞争愈发激烈。

3.2 区块链信息系统的建模方法

国内学者在分片网络建模和区块链数据库方面均已进行深入探索。

（1）分片网络建模

在分片网络中，验证和执行跨分片交易需要跨分片通信，会消耗大量网络传输资源。针对该问题，香港科技大学的Tao等人观察到若用户仅参与同一区块链上的智能合约，则可以独立验证、确认这些用户发送的交易，因此提出了针对智能合约的分片架构，将参与到一个智能合约的用户所发送的交易形成一个分片，从而减少跨分片通讯开销[71]。此外，为缓解分片间负载不均衡的现象，该文还设计了分片合并与分片内交易选择模式的博弈策略，并证明在该策略下系统的参与方最终会达到纳什均衡。香港科技大学的Huang等人考虑到不同区块链节点的性能存在差异，设计双链架构分别维护交易链和声誉链，其中交易链通过Raft机制产生共识，而声誉链利用集体签名的同步拜占庭容错算法在声誉评分和相关交易区块上进行共识[72]。利用声誉选出各分片内性能较强的领导者，不仅可提高系统吞吐率，还可在划分分片时避免恶意或不活跃节点过于集中，从而确保分片安全。上海交通大学的Zhang等人设计的CycLedger为每个委员会选择一个领导者和一个部分集负责片内共识、跨片通信[73]。部分集监督领导者的行为，并在检测到领导者的恶意行为时启动换主操作，让部分集中的其他节点替代恶意主节点。

（2）区块链数据库

国内学者在数据建模方面了一些显著尝试，包括众享比特公司的ChainSQL[74]、苏州大学的EtherQL[75]、华东师范大学的SEBDB[76]和香港浸会大学的vChain[77]等。ChainSQL的架构包含三个部分：区块链网络、普通数据库和客户端。区块链网络是由多个节点构成的Ripple网络，部分节点会配置数据库实例，操作以交易的形式存放到区块链和数据库实例之中；客户端发送的数据请求由数据库端和区块链节点端分别响应。EtherQL针对以太坊开发查询层，提供了用于分析区块链数据的高效查询原语，从而与其他应用程序集成。SEBDB通过对区块和交易添加关系语义来增强区块数据的表达能力和查询处理能力，区块链上的所有区块和交易都被建模为具有多个属性的关系，该平台提供类SQL的查询接口，并构建一个统一的查询处理引擎来处理两方面的数据，并且支持链上链下数据联动查询。vChain通过加密多重集合累加器生成集合属性的摘要以判断两个集合是否有交集；若无交集，则生成相关证明。vChain实现了范围查询等复杂查询，并确保查询结果完备。

3.3 区块链信息系统的存储管理

区块链平台常被用作去中心化数据库，然而现有的区块链平台使用起来远不如传统

数据库方便。国内近几年也涌现出较多与区块链存储相关的工作。本节将对国内提出的区块链数据库技术如 ChainSQL、EtherQL、SEBDB 以及具体的数据存储方案如 CU-based 共识单元，BFT-Store 进行介绍。

（1）区块链数据库技术

区块链独特的数据管理功能已经成为各领域应用中发挥其价值的关键。近年来国内学术界和工业界基于区块链技术和数据库的理论研究开发区块链数据库。

ChainSQL[74]是将区块链与数据库集成而开发的区块链数据库应用平台，通过在区块链系统上层使用其他数据库构建查询层来增强区块链系统的性能，即其展示了一个具有区块链的去中心化，分布式和可听性功能以及快速查询处理和精心设计的分布式数据结构的系统数据库。该系统具有防篡改，一致且具有成本效益的多活动数据库以及有效而可靠的数据级灾难恢复备份。该系统在实践中被证明是具有数据级灾难恢复备份功能的多活动数据库。

EtherQL[75]针对以太坊的高效查询层，提供了用于分析区块链数据的高效查询原语，包括范围查询和 top-k 查询，这些查询原语可以非常灵活地与其他应用程序集成。EtherQL 设计并开发了一种中间件来访问底层数据，该中间件可以自动实时地将以太坊公共网络中的区块链数据与内置的以太坊客户端进行同步，并为开发人员或数据分析人员提供开箱即用的数据查询层，可方便地访问整个区块链数据。该层包括四个模块：同步管理器、处理程序链、持久性框架和开发者接口。

SEBDB[76]将关系数据语义添加到区块链平台中，其中每个事务都是一个预定义表中具有多个属性的元组。使用类似于 SQL 的语言作为通用接口，而不是代码级 API，以支持便捷的应用程序开发，其中重新定义和重新实现内在操作以适合区块链平台。SEBDB 体系结构由五层组成，包括应用层、查询处理层、存储层、共识层和网络层。采用链上/链下数据融合的存储方式，链下数据采用关系数据库进行数据存储，链上数据被建模为多个关系，每个事务是属于某个关系的元组，可由用户自由选择存储方式。SEBDB 为链上数据提出了一种类似于 SQL 的语言来管理数据，即使用 CREATE，INSERT 和 SELECT 子句来创建表，添加新事务以及获取查询结果。

（2）区块链数据存储方案

与传统的数据库相比，目前的区块链技术仍然不能处理大量的事务，这是由协议一致性、块结构、存储挑战等诸多因素造成的。其中，较高的存储需求是阻碍区块链在各种设备上广泛使用的关键因素。因此，国内也提出多种数据存储方案来提升区块链性能。CUB[78]通过引入了一种称为共识单元（CU）的新概念将不同的节点组织到一个单元中，并让它们将至少一个区块链数据副本存储在系统中。进一步定义了块分配优化（BAO）问题并且证明了其为 NP 难问题。该问题确定块的最佳分配，以便充分利用存储空间并最大限度地减少查询成本。提出了三种有效的启发式算法来解决静态分配问题并提出了解决方案，以解决新块到达且节点加入或离开 CU 时的动态情况。BFT-Store[79]通过将纠删码与拜占庭容错共识协议相集成来增强存储的可伸缩性，每个块的存储消耗可以减少到 O(1)，可以在更多节点加入区块链时扩大总体存储能力。BFT-Store 也针对存储横向扩

展设计了有效的在线重新编码协议，并采用了混合复制方案来提高读取性能。

3.4 区块链信息系统的联邦计算

随着区块链技术和联邦计算的快速发展，国内研究者在区块链信息系统的联邦计算领域开始进行研究投入，在相关问题上也取得了一系列科研成果。

传统的联邦计算需要一个中心服务器来分配和协调各节点的计算任务，针对中心服务器可能存在不可信问题，北京大学王乐业等人[80]提出了一个在联邦学习环境下的安全矩阵分解框架 FedMF，通过使用同态加密技术来避免泄露用户的隐私。中山大学的 Sicong Zhou 等人[81]提出了一种基于区块链分片技术的安全计算框架 PIRATE，PIRATE 利用了基于分片的区块链协议和梯度异常检测，并可以消除产生有害梯度的恶意节点的影响，区块链的去中心化特性和梯度异常检测为模型参数可靠更新提供了保证。2019 年 2 月，香港科技大学教授和微众银行开源全球首个工业级联邦学习开源框架 FATE[82]，为联邦学习提供了高性能的安全计算支持。

区块链信息系统的联邦计算通过各节点间通信来传递数据，通信开销大是联邦计算中存在的普遍问题，针对此问题，清华大学姚鑫等人[83]提出了一种特征融合的方法来解决联邦学习通信开销大导致的性能下降问题，主要思想是通过将局部模型和全局模型的特征集合起来，可以以较少的通信开销获得更高的精度。在区块链信息系统的节点进行通信过程中，某些节点可能会受到恶意节点攻击，对此中国工程院刘明达等人[84]在论文中提出基于区块链的分布式可信网络连接架构 BTNC，充分融合了区块链去中心化、防篡改、可追溯的安全特性，能够防御常见的攻击。

区块链信息系统中没有中心节点，共识机制保证每笔交易所有节点上的一致性和正确性。针对区块链信息系统环境下的共识机制问题，上海交通大学张玲等人[85]基于区块链共识机制提出了多区域最优潮流分布式算法，引入代表选举与各个区域验证决策两个环节，在迭代优化过程中二者共同作用，摒弃被恶意篡改过的信息，可实现对恶意参与节点的抵御。

综上所述，目前国内学者对于区块链信息系统的联邦计算研究工作，主要集中在联邦计算框架方面，在一定程度上解决了联邦计算过程中的数据隐私和安全问题，但是缺少有关提升联邦计算效率的研究工作，对此国内学者需要开展更加广泛和深入的研究。

3.5 区块链信息系统的跨链互操作

目前，国内在侧链/中继链、哈希锁定等方面开发了一些新的技术。代表性的工作如下。

浙江大学和杭州趣链公司提出了一种通用的链间消息传输协议 IBTP[86]，开发了支持异构区块链间交易的跨链平台 BitXHub，它由中继链、应用链以及跨链网关（Pier）3 种角色构成，具有通用跨链传输协议、异构交易验证引擎、多层级路由三大核心功能，提

供了基于自组网的跨链网关、可动态升级的验证引擎、统一的跨链合约模板，支持异构区块链间的异步分布式事务，允许异构的资产交换、信息互通及服务互补。

中国人民大学和北京航空航天大学提出了一种基于哈希锁定的多方跨链协议[87]，设计了一种“边着色”自动撮合交易算法，可以在多方多链情况下快速匹配交易，实现多方跨链资产转移的清结算。

国内的工作主要集中在通信协议和密码学技术方面，在高层的逻辑处理方面，如跨链事务处理、跨链查询处理等方面，仍有许多工作去做。

3.6 区块链信息系统的隐私保护

根据保护隐私的对象分类，国内关于区块链信息系统的隐私保护的工作主要可以分为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；例如：黄步添等人[88]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漏隐患。

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；例如：申屠青春等人[89]提出一种基于椭圆曲线的盲签名混币方案，能够在保证匿名性的基础上提升计算效率。

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。

3.7 区块链信息系统的链上链下融合技术

国内在链上链下融合方面进行了大量的深入研究。

（1）数据融合

在数据融合方面，国内与国外文献的算法、模型、机制基本相似，主要包括两种方式：1）链上存储数据的关键信息，链下存储数据原始内容。2）链下数据数字化存储于区块链，链下存储数据的链上信息。

李等人[90]设计了一种支持索引、可追溯、可验证的云存储与区块链结合的存储模型。通过将云存储中的对象元数据存储在区块链上，利用ETag值检查Object内容是否发生变化的特性以及区块链上的数据不可篡改的特点，来验证云上存储的数据是否安全，以提高云上存储数据的可信性。除此之外通过区块链将一部分交易存储在本地，增加了区块链的存储容量的可扩展性。

Yang 等人[91]提出了一种基于属性密码系统和区块链技术的医学数据共享方案。通过将加密医疗数据存储在云中，并将存储地址和医疗相关信息写入到区块链，可以确保有效存储并消除数据不可逆修改的可能性；其次，该方案结合了基于属性的加密（ABE）和基于属性的签名（ABS），实现数据隐私和细粒度的访问控制，在保护签名人身份的同时验证了医疗数据源的真实性；此外，数据用户将医疗数据密文解密的大部分操作外包给云服务提供商（CSP），大大减轻计算负担。

（2）流程融合

在流程融合方面，国内与国外的算法、模型、机制基本类似，主要包括两种方式：1）链下执行，链上存储结果，2）链下与链上混合执行。

TrustSQL[92]通过将资产的数字化信息、资产的交易记录存储于区块链中，信息系统负责解析、解释数字资产，同时将数字资产的操作结果写入到区块链中，利用链下的信息系统的计算能力减轻链上计算的压力，同时解决流程执行过程中结果的不可篡改等问题，实现金融等领域数字资产流通过程中结果的多方互认互信。

Li 等人[93]通过将电子商务物流服务流程拆分为链上与链下，链上通过智能合约触发物流状态变化，链下各个参与方执行各自独立的流程，例如内部验证、审批等，提出一种支持区块链的工作流管理系统（BCWMS），实现客户信息系统安全共享异构动态物流资源的作用。

（3）输入输出融合

在输入输出融合方面，国内与国外的算法、模型、机制基本类似。

Wang[94]提出一种基于特定知识引擎（ASKE）的新颖 Oracle 实现方案，根据用户指定查询条件通过 Oracle 在异构源爬取相关信息，数据在链外爬取信息聚合以获得最终结果，返回至区块链智能合约，从而在保证数据真实、防篡改的前提下实现多数据源数据检索的方案。

3.8 区块链信息系统的云边端融合技术

国内学者在区块链信息系统的云边端融合方面也做了大量工作。

（1）融合区块链的在云边端系统体系结构

广东工业大学 Jiawen Kang 等人将车辆和移动边缘计算相融合，为了克服边缘计算服务器可能会被黑客攻击的风险，采用智能合约来防止未经授权的数据共享，并设计了基于信誉的车辆间数据高质量共享方案[95]。浙江大学邓水光团队提出了一种基于区块链与边缘计算的物联网数据管理方案，先利用 Kademlia 算法实现分布式数据存储，再构建基于区块链的主动访问控制机制，只有被授权用户才能访问 IoT 数据[96]。由于边缘计算在任务卸载过程中所传输的信息容易受到攻击，从而可能影响数据的完整性，南京信息工程大学徐小龙等人提出了一种计算卸载方法 BeCome，通过区块链来确保数据的完整性，采用非支配排序遗传算法（NSGA-III）生成资源均衡分配策略，通过简单累加加权（SAW）和多准则决策（MCDM）确定最佳卸载策略[97]。

国内学者在智能交通、边缘智能物联网等领域也做了一些探索。在智能交通领域，Li 等人通过结合车辆雾计算和区块链技术来支持条件隐私，实现了高效且隐私保护的拼车任务[98]。在智能电网领域，Gai 等人提出了一种模型许可的区块链边缘模型，以解决智能电网中的隐私安全和能源安全[99]。在边缘智能物联网方面，Lin 等人通过区块链实现边缘数据分享交易，促进边缘场景下数据共享[100]。

（2）云边端融合环境下区块链性能提升

鉴于终端设备将计算任务卸载到边缘节点会导致移动边缘计算服务提供商过载，Liu 等人提出了一种支持移动边缘计算的区块链框架，移动终端设备通过两种卸载模式将计算任务卸载到边缘节点[101]。其一是将全部计算任务卸载到附近的移动边缘计算服务器；其二是划分计算工作，再将划分之后的任务转发给附近的其他用户执行。计算任务卸载问题实质是一个优化问题，需综合考虑延时、任务划分及分配时的能源消耗和挖矿成功概率，并将原始的非凸问题转化为凸问题，该文基于乘数交替方向（ADMM）以分布式方式解决计算卸载问题。Chen 等人针对现有大多数计算卸载解决方案都假定所有工业物联网设备都可以直接连接到边缘服务器或云数据中心的问题，作者提出了一种多跳计算卸载解决方案，即通过邻居节点进行计算卸载，该解决方案同时针对数据处理任务和挖矿任务，从而最大限度地降低支持区块链的工业物联网和工业物联网设备的经济成本[102]。针对物联网设备连接受限的问题，这些设备需要连接到连接良好的相邻设备，作者将卸载问题建模为多跳计算卸载博弈（MCOG），并设计一种分布式算法，通过该算法博弈的状态可以快速收敛到稳定状态。鉴于在 UTXO 模型中每笔交易不能引用超过一次，Xu 提出所有输出全部被后一个交易引用的交易对于验证新生成的交易是无效的，将无效区块（即仅包含无效交易的区块）发送到云服务提供商中进行备份[103]。然后，这些块将从边缘设备中删除。通过这种方式来降低边缘区块链节点的数据存储量。

4 国内外研究进展比较

4.1 体系架构分析与比较

区块链核心技术、机制和应用部署等方面均存在诸多安全隐患，不法分子利用相关漏洞实施攻击，安全风险事件频出。本文将区块链安全问题分为区块链技术安全、区块链生态安全、区块链使用安全和区块链信息安全四类。区块链技术安全方面，主要是区块链本身核心技术或机制不完善造成的，包括共识机制和智能合约逻辑漏洞、密码算法安全、P2P 网络机制安全等。由此带来的安全攻击有“51%”攻击、女巫攻击、双花攻击、日食攻击等。2018 年 5 月，比特币黄金（BTG）遭遇 51% 双花攻击，损失 1860 万美元。同月，360 公司 Vulcan（伏尔甘）团队发现了区块链平台 EOS 的一系列高危安全漏洞，引发市场哗然。区块链生态安全方面，主要是指区块链产业生态中各种安全问题。

例如加密数字货币交易所、矿池、网站遭受 DDoS 攻击，钱包面临 DNS 劫持风险，以及交易所安全管理策略不完善或不当导致的各种信息泄漏、被钓鱼、账号被盗等。2018 年 3 月，世界大型交易所的“币安”被黑客攻击，大量用户账户被盗。区块链使用安全，主要是指用户使用区块链应用面临的潜在安全问题。例如私钥管理不善，遭遇病毒木马、账户窃取等。区块链信息安全方面，主要是不法分子利用区块链技术不可篡改特性将非法信息或文件上链所导致的安全监管问题。2018 年 4 月，北大网友将颇具争议公开信“向校方申请公布涉性侵丑闻的教授沈阳调查的少量问题”永久性记录至以太坊，引发社会关于区块链信息安全监管讨论。总的来看，区块链安全事件呈高发态势，需要引起注意。

中国区块链企业主要吸纳国外开源社区的区块链研究成果，自主研发的区块链平台并不多，仅有国内少数企业自主研发出 CITA、Bubichain、BROP、BCOS、ChainSQL 等平台，多数企业基于比特币、以太坊、超级账本等国外开源区块链产品进行开发和完善。尽管 2018 中国区块链专利位列世界第一，但整体价值不高，大部分企业围绕加密数字货币、钱包、存证溯源等应用层开展研发工作，较少涉及区块链关键技术。实际上，区块链平台性能不足、安全不够、难以互联互通等问题对共识算法、密码学、跨链等关键技术突破提出了更高的要求，从目前区块链最新技术理念和解决方案来看，如 PoS、DPoS 共识算法，分片、零知识证明、DAG、侧链、闪电网络等技术方案，大多数是外国技术社区提出，国内技术社区进行跟随和模仿，极少属于中国自主原创或最早提出。中国亟须在区块链关键技术方面有所突破，进而推动区块链技术在更大规模的商业场景中落地。

4.2　建模方法分析与比较

建模方法分为网络建模和数据建模。分片网络建模是近期的研究热点。表 1 对比了国内外在分片建模方面的主要工作。表 2 列举了国内外在数据建模方面的主要工作。

表 1　国内外在分片网络建模方面工作对比

第一单位	项目名称	分片划分方式	通讯复杂度	系统安全性	数据模型
新加坡国立大学（新加坡）	Elastico[23]	工作量证明	$O(n^2)$	不能确保事务原子性，不抗偏见	UTXO
洛桑联邦理工学院（瑞士）	OmniLedger[24]	RandHound/基于可验证随机函数的领导者选举算法	$O(n)$	客户端驱动的跨分片事务可能导致事务原子性不能保证	UTXO
伦敦大学学院（英国）	Chainspace[25]	*	$O(n^2)$	合约部署者指定信任的节点来保证合约的完整性	UTXO
Visa 研究院（美国）	RapidChain[26]	工作量证明/有限布谷鸟规则	$O(n)$	假设分片中的主节点是诚实节点；若主节点是节点，则无法确保系统安全	UTXO
香港科技大学（中国）	文献［71］	RandHound/基于可验证随机函数的领导者选举算法	*	通过矿工去检测并发现其他矿工的恶意行为，从而确保系统的安全性	账户模型

（续）

第一单位	项目名称	分片划分方式	通讯复杂度	系统安全性	数据模型
香港科技大学（中国）	RepChain[72]	*	*	可避免恶意、懒惰节点集中于单个或几个分片	UTXO
上海交通大学（中国）	CycLedger[73]	基于可验证随机函数的加密分类机制	$O(n)$	选择信誉高的节点作为分片内的领导者，通过激励机制来鼓励节点不作恶	UTXO

表 2　数据建模方面的主要工作对比

相关研究工作	数据模型	建模方式	存储引擎	支持的查询类型	查询实现
Bitcoin	UTXO	交易为转账日志	LevelDB	区块、交易查询、交易历史追溯	应用层实现
Ethereum	账户模型	交易为转账或合约调用，存储为账户余额 + 智能合约存储	LevelDB	区块、交易、账户状态查询、交易历史追溯、状态版本追溯	应用层实现
BigchainDB[27]	键值对模型	交易为资产转移日志	MongoDB	区块、交易查询	MongoDB 接口
BlockChainDB[28]	键值对模型	区块链底层存储 + 数据库查询与执行层	区块链	数据表的单点查询	key/value 查询接口
ChainSQL[74]	关系模型	交易为数据库操作日志	关系数据库	区块、数据表查询	SQL 语言
EtherQL[75]	关系模型	将 Ethereum 数据解析成结构化数据存储在关系数据库中	关系数据库	区块、交易、账户状态查询	SQL 语言
SEBDB[76]	关系模型	交易参数为数据表中记录	文件系统	区块、交易、数据表查询、交易历史追溯	SQL 语言
vChain[77]	集合模型	交易为包含集合元素	智能合约存储	布尔范围查询	布尔表达式查询

4.3　存储管理分析与比较

目前，区块链技术正在蓬勃发展，国内外学者、企业都在提出了自己的区块链信息系统存储管理方案。但是由于底层数据存储方案的不同，二者在交易吞吐量和对关系型数据存储与查询的支持上有着显著差异。

如表 3 所示，国外的区块链信息系统的存储方案主要以 LevelDB 为主要底层数据库。而国内的区块链信息系统的主流解决方案选择关系数据库作为底层数据库。在交易吞吐量方面，以比特币、以太坊和超级账本系统为代表的区块链系统远远低于国内系统。

表 3　存储管理分析与比较

	国际/国内 相关工作	使用的数据 存储系统	区块链中 存储的数据	对关系型 数据的支持	对关系型 查询的支持	吞吐量
国外	Bitcoin[147]	BerkeleyDB/LevelDB	用户数据	N	N	~7
	Ethereum[148]	LevelDB	用户数据	N	N	~15
	Hyperledger[149]	LevelDB/CouchDB	用户数据	N	N/Y	300~500
	BigchainDB[27]	RethinkDB/MongoDB	元数据	—	N	—
	Storj[30]	LevelDB	元数据	-	N	-
	Filecoin[150]	LevelDB	元数据	-	N	-
国内	ChainSQL[74]	MySQL、SQLite、DB2、Oracle、SQLServer 等	用户数据	Y	Y	>1000
	TrustSQL[92]	MySQL/MariaDB	—	—	Y	5000

在数据检索查询方面，LevelDB 类似于状态数据库的预写日志的数据库无法支持更加复杂的关系型数据，也无法提供对关系查询的支持。与之相对的，国内对区块链技术的应用更加注重与传统数据库系统的结合以及对关系数据和关系查询的支持。ChainSQL 基于插件式管理，其底层数据库支持 MySQL、SQLite 等多种关系数据库。TrustSQL 支持自适应的共识机制、5000TPS 的交易吞吐量、秒级交易确认及 Select、Insert 两种 SQL 语句。

4.4　联邦计算分析与比较

目前，国内外学者对于区块链信息系统的联邦计算都进行了广泛研究，虽然研究的重点领域存在一些差异，但主要还是提升联邦计算中的计算高效性、数据安全性和系统可靠性这三个方面。表 4 是国内外关于联邦计算的研究成果的侧重点分析和比较。

表 4　国内外联邦计算成果分析和比较

研究者	研究机构	时间	计算高效性	数据安全性	系统可靠性
Lugan 等人[104]	鲁汶大学（比利时）	2019	增加了额外加解密开销	保证了数据机密性	不能防御恶意用户攻击
Sana Awan 等人[105]	堪萨斯大学（美国）	2019	增加了恶意检测和加解密开销	保证了数据机密性	能够防御恶意用户攻击
Lyu 等人[106]	墨尔本大学（澳大利亚）	2019	增加了恶意检测和加解密开销	保证了数据机密性	能够防御恶意用户攻击
Silvio Micali 等人[107]	麻省理工学院（美国）	2018	大幅减少了交易确认时间	保证了数据机密性	能够减轻恶意用户攻击
Rafael Pass 等人[108]	康奈尔大学（美国）	2018	增加了额外加解密开销	保证了共识协议的安全	能够防御恶意用户攻击
王乐业等人[109]	北京大学（中国）	2019	增加了额外的同态加密开销	保证了密文的计算安全	不能防御恶意用户攻击

（续）

研究者	研究机构	时间	计算高效性	数据安全性	系统可靠性
Sicong Zhou 等人[110]	中山大学（中国）	2019	减小了模型存储开销	梯度未加密会泄露隐私	能够防御恶意用户攻击
杨强等人[111]	香港科技大学（中国）	2018	降低了联邦计算过程通信开销	保证了数据机密性	不能防御恶意用户攻击
姚鑫等人[112]	清华大学（中国）	2019	降低了联邦计算过程通信开销	梯度未加密会泄露隐私	不能防御恶意用户攻击
刘明达等人[113]	中国工程院（中国）	2019	增加了额外的存储开销	保证了数据机密性	能够防御恶意用户攻击
张玲等人[114]	上海交通大学（中国）	2020	增加了收敛性检验计算开销	数据未加密会泄露隐私	能够减轻恶意用户攻击

从表 4 中可以看出，近几年国内外研究者在该领域的研究进展大致同步，国外研究在三个方面的研究较为均衡，但是国内研究主要侧重提升数据安全性方面。从整体上看，国内研究者多集中在研究联邦计算的系统架构和模型，对于底层的共识研究较少，相关成果与国外相比，还存在一定的差距。但是随着国内研究者和研究机构对联邦计算领域的持续研究和投入，在该领域上与国外研究团队的差距将不断缩小。

4.5 跨链互操作分析与比较

表 5 对典型的跨链技术进行功能和性能上的比较[115-116]。

表 5 国内跨链技术成果分析和比较

系统/技术	跨链机制	原子交易	资产质押	跨链认证	跨链合约	互操作性	信任模型	交易效率	实现难度
BTC-relay[42]	中继	支持	支持	支持	困难	有中继的链	链失效或 51% 攻击	低	大
联盟式侧链[43]	中继	支持	支持	支持	困难	有中继的链	链失效或 51% 攻击	中等	大
Polkadot[44]	中继	支持	支持	支持	困难	有中继的链	链失效或 51% 攻击	低	大
Cosmos[45]	中继	支持	支持	支持	困难	有中继的链	链失效或 51% 攻击	低	大
BitXhub[86]	中继	支持	支持	支持	困难	有中继的链	链失效或 51% 攻击	高	大
Interleger[46]	公证人	支持	支持	支持	困难	全部链	链失效或 1/3 恶意节点	低	中等
闪电网络[47]	哈希锁定	支持	困难	支持	不支持	点到点	链失效或 51% 攻击	中等	容易
多方跨链协议[87]	哈希锁定	支持	困难	支持	不支持	点到点	链失效或 51% 攻击	高	容易
Fusion[48]	分布式私钥	支持	支持	支持	支持	全部	链失效或 51% 攻击	高	中等
Wanchan[49]	分布式私钥	支持	支持	支持	支持	全部	链失效或 51% 攻击	高	中等

当前的区块链跨链互操作技术还存在如下问题：

1）效率不高，跨链的交易速度有待提高。

2）跨链功能还不完善，多数技术不支持跨链智能合约。

3）实现有难度。部分跨链技术仅是技术方案，真正运行的系统还不多。

4）跨链安全性。在文献［117］中列出了 12 种跨链安全风险。包括：公证人信任性、侧链/中继安全性、哈希锁定安全性、孤块、长距离攻击、阻塞超时、竞争条件攻击、日蚀攻击、区块肿胀、失效蔓延、跨链重放攻击，以及升级兼容性等问题。

4.6　隐私保护分析与比较

区块链隐私保护是一个极其重要的研究问题，尤其在医疗领域尤其突出。在医疗领域，许多国家已经在逐步实现区块链隐私保护方面的措施和方案。爱沙尼亚是第一个在全国范围内使用区块链进行医疗保健的国家。2016 年，爱沙尼亚电子健康基金会启动了一个开发项目，旨在使用区块链技术在存档相关活动日志中保护患者健康记录。他们使用区块链作为额外的安全层，以帮助确保健康记录的完整性。方案由数据安全公司提供，该方案利用区块链技术为 100 多万名患者的医疗记录提供安全的信息保障服务。该方案把医疗保健信息的隐私和完整性保护作为首要任务，爱沙尼亚的每个访问过医生的人都可以拥有一个可以跟踪的在线电子健康记录。基于区块链的隐私保护系统，通过电子身份证识别，健康信息保持完全安全，同时可由授权个人访问。2018 年初，阿联酋最大移动通信商公布与阿联酋最大医疗保障服务商合作实现数字化医疗保健记录和系统。澳大利亚卫生部门计划推动使用区块链进行医学研究记录，安全云提供商和区块链创业公司联手为该部门提供跟踪健康数据研究的不可变记录，以此来证明谁在访问医疗数据，他们为什么要访问它，以及安全地记录研究查询。

目前，中国企业在一些区块链技术研发和应用落地方面均走在世界前列。例如针对区块链隐私保护的难题，迅雷集团旗下网心科技于 2017 年上线高性能区块链平台，迅雷链研发出可追溯隐私的保护技术，通过环签名、零知识证明等加密算法对数据加密隐藏，保证在不泄露数据隐私的前提下，证明数据的有效性并进行核验，从而保护用户隐私。该技术已在迅雷链与泰国那黎宣大学的合作中得到验证。泰国那黎宣大学管理着 490 多家医疗机构，总体覆盖人群规模约 100 万人，不同医院之间调用病例信息的情况一直是病人隐私保护的隐患。借助迅雷链的技术支持，那黎宣大学医院运用区块链的分布式、可追溯属性确保病例不被恶意篡改。此外，迅雷链还实现了在医生调用病例时，病人可通过管理系统对区块链密钥进行授权，从而充分保障病例资料安全和病人隐私。

4.7　链上链下融合技术分析与比较

区块链起源于美国，国外对区块链的研究起步较早，在金融、数据交易、数据共享、供应链、IOT、医疗、电力等方面，在信息系统与区块链融合方面率先进行了大量的实践与研究，提出了 IPFS、预言机、智能合约等关键技术，同时链下链上融合多体现在数据的共享过程中的访问控制、隐私保护或者分布式流程协作等方面，模式、算法、机制等

在默认数据源较为可信的情况下进行，对数据源的可靠性、真实性、可验证性方面缺乏相关保证机制。

中国起步较晚，目前仅在金融、供应链、政务、物联等少数领域开展了信息系统与区块链的融合，尤其是在政务、医疗、供应链领域开展了大量数据共享、隐私保护、权限控制等的研究，在输入输出融合方面研究相对较少，模式、算法、机制等在默认数据源较为可信的情况下进行，对数据源的可靠性、真实性、可验证性方面缺乏相关保证机制，在预言机、智能合约等关键技术缺乏更深一步的研究。随着国家的重视与扶持，相信链上与链下融合机制会在国内得到更好的发展。

4.8 云边端融合技术分析与比较

表6列举了国内外学者在云边端融合技术方面的工作。

表6 云边端区块链信息系统比较

第一完成单位	应用场景	架构设计	架构伸缩性	区块链扩展性设计
首尔科技大学（韩国）[62]	智慧城市	分为核心网络（运行区块链节点）和边缘网络（处理服务请求）	根据边缘节点的能力不同来分配计算任务（++）	只有计算能力较强的边缘节点部署区块链，其他边缘仅提供边缘计算服务
罗马尼亚国家信息学研发研究所（罗马尼亚）[63]	分布式控制系统	分为终端设备、边缘节点、云层服务三层	对延迟敏感的任务放到边缘端执行，对计算需求较大的任务放到云端执行（+++）	*
新南威尔士大学（澳大利亚）[64]	智能家居	分为云存储、覆盖网络和智能家居层	系统的任务划分清晰，可以充分利用云端的存储空间，伸缩性较强（+++）	覆盖网络中的集群领导者维护区块链，同时一些数据云端存储不需上链。
广东工业大学（中国）[98]	车联网	分为用户层、边缘层和云层	边缘层接收用户层发送的数据，并可进行预处理，通过云层的来统筹所有边缘节点（+++）	*
浙江大学（中国）[99]	物联网	包括消费者层、分布式存储层以及区块链层	区块链任务和边缘数据存储任务分别保存在各个边缘节点上，容易受到边缘存储能力的制约（++）	*
南京信息工程大学（中国）[100]	边缘计算卸载	包含计算或存储能力有限的智能设备和计算和存储较为充足的边缘计算层	将终端设备中的任务卸载到边缘，以缓解终端的计算压力；（++）	*
石溪大学（美国）[70]	*	整体分为两层，边缘终端设备和边缘计算层	通过横向的扩展来满足区块链的存储需求（++）	将区块数据分散存储在网络中减少存储开销，通过新型 PoS 共识机制减少计算开销

（续）

第一完成单位	应用场景	架构设计	架构伸缩性	区块链扩展性设计
南京邮电大学（中国）[106]	*	包含终端设备、边缘计算层和云层	将一些存储任务放到云端，系统的伸缩性较强（+++）	将旧区块存到云端；设计新型 PoC 共识算法减轻计算开销
北京邮电大学（中国）[104]	*	分为移动终端和边缘计算设备	受限于边缘计算有限的存储和计算能力，伸缩性有限（+）	将区块链等计算任务卸载到边缘计算设备上

5　区块链信息系统的典型应用

5.1　区块链 + 数字金融信息系统

区块链在数字金融信息系统领域的工作包括数字货币、金融资产交易结算等。

（1）数字货币

区块链是比特币的底层技术，区块链最早的应用场景就是数字金融。与由国家发行的主权货币相比，比特币没有第三方仲裁。同时，由于缺乏国家主权作为支持，比特币本身的价值缺乏支撑，币值变化非常大。近年来，一些大型企业也尝试打造基于区块链的加密数字货币。2019 年 2 月，摩根大通发布了 JPMcoin，拟用于大型银行或者国家间的实时交易结算和大额支付。JMPCoin 在企业级区块链项目 Quorum 上运行。2019 年 6 月，Facebook 发布加密货币项目天秤座（Libra）白皮书，旨在打造一种满足数十亿人日常金融需求的全球支付系统。Libra 采用 LibraBFT 协议执行共识，该算法一方面通过聚合签名降低通信复杂度，另一方面以流水线方式执行共识流程，使共识投票得以复用，从而提高共识效率。但是，这些超越国家主权的加密数字货币尚未获得主权国家的普遍支持。2019 年 9 月，法国财政部表示，法国和德国将共同抵制 Libra 加密货币，这使得该项目的推广面临困难。

我国很早就关注研制基于区块链技术的法定货币。早在 2014 年，央行就启动了关于数字货币方面的研究工作。2017 年，中国人民银行数字货币研究所成立，聚焦数字货币研究。2019 年 8 月份，中国人民银行召开 2019 年下半年工作电视会议，要求加快推进我国法定数字货币（DC/EP）的研究步伐。与比特币/天秤座项目最大的不同是，未来发行的法定数字货币（DC/EP）将在一定程度上替代现金。

（2）金融资产交易结算

区块链的属性使得金融资产交易的速度变得很快。2017 年 1 月，中国人民银行建立基于区块链的数字票据交易平台，通过数字货币进行结算实现数字票据交易的资金流和信息流同步转移，从而实现 DVP 票款对付结算；同时通过区块链数字身份方案解决了用

户重复实名认证的问题。该平台采用以太坊智能合约虚拟机技术，同时扩充相关指令操作码，实现同态加密保护数据隐私；针对现实业务需求加强了节点通讯加密、数据加密存储等；改造联盟链底层实现智能合约的干预机制，以满足司法干预等现实中存在的特殊需求等。蚂蚁集团基于蚂蚁区块链平台开发了供应链协作网络——双链通平台，通过蚂蚁自研区块链硬件隐私保护技术，保证多参与方之间的安全性和隔离性；基于支付宝账户与网银 U 盾构建安全保障体系，确保交易安全；业务实现云化，使得更多参与方直接通过 API 加入网络。此外，2018 年 6 月，蚂蚁集团实现了全球首个基于区块链的电子钱包跨境汇款服务。

在国外，2019 年，美国证券存管信托与结算公司（DTCC）使用区块链技术来简化重复程序，优化成员之间的协调工作。DTCC 贸易信息仓库中储存着价值 10 万亿美元的信用衍生品的信息，其中约有 5 万个账户的记录信息将转移至一个名为 AxCore 的定制数字分类账本中。2018 年，IBM 与多个银行机构协作开发了基于 Hyperledger Fabric 的贸易融资平台 Batavia，旨在协助银行及其客户将目前手动的纸质贸易融资流程自动化。

5.2 区块链 + 电子政务信息系统

对于政务系统来说，无论是从政府数据的公信力需求来看，还是从政务数据开放/授权共享来看，都需要在原有制度式保障的基础上，提供更加有力的技术支持。区块链能为政务系统的数据提供一个可信环境，其中的数据和针对数据的操作不可被恶意操纵或篡改，恰好可以对制度式信任形成有益的补充。

（1）政策公示

政策公示的本质就是通过将信息公开化获得大众群体的确认及共识[118-121]，与区块链达成共识后不可篡改的本质[122]。

区块链本身使用的分布式存储以及签名等底层技术，为数据带来不可篡改、不可抵赖的特征，有助于提高公信力[123]，打造全新一代信息公示服务。区块链可使用多重加密算法[124]，对政策公示中的敏感数据脱敏，保护隐私。跨部门政策的出台，也可以通过部门联合签名解决。区块链可信凭证，可让参与方共同构建、维护统一凭证[125]，并保障其真实有效、不可篡改。

（2）身份认证

机构间各自保存用户的身份信息[126-127]，对信息拥有绝对的掌控权，各机构互不联通，无法实现同一身份的统一操作。Lin[128] 等人提出基于区块链的安全互认证系统 BSeIn，旨在提供匿名认证、可审核性和机密性等隐私和安全保障。Chen[129] 等人提出基于区块链的开放身份认证结构，设计了物理身份注册协议、虚拟身份绑定协议和属性认证协议，Yu[130] 等人提出一种有效的隐私保护算法来保护社交网络中信息的隐私，利用区块链不篡改特性来存储和识别用户的公钥，可以很好地应对各种类型的攻击。

（3）政务数据确权与共享

Factom 与 Honduras 合作关于土地所有权登记项目[131-132]，达到减少登记成本、提高

透明度、防止欺诈行为的目的。Shrier[133]等人认为区块链将促使个人数据成为一种新的资产，在政务系统实现聚集与互通。Min[134]等人设计一个基于区块链的电子证照共享平台，各政府部门之间数据安全共享，有效提高政府部门人员以及公民的工作效率。实际应用中，区块链技术与电子资产权属管理领域相结合还仍有尚待解决的问题，比如隐私保护问题和数据多样性问题等。

（4）政府监管

区块链的数据共享能力和数据可信保证，对政府的监管体系改革极具意义。Mao[135]实现将食品供应链向区块链平台的整合，利用区块链平台中智能合约取代受信中介来对各参与方产生信用评估文本，构建一种客观授信的、不被篡改的信用评价体系。López-Pintado[136]等人对业务流程的区块链改造，支持创建流程模型实例，并允许用户跟踪流程实例的状态并执行其中的任务，对政务系统监控的可靠性具有重要提升。

区块链技术从透明的角度看待每一笔交易，从而根除腐败[137]，比如大型建设项目合同[138]，基于区块链技术的新模型可用于追踪多方之间的私人或公共法律协议。作为实际纸质合同的补充系统，这种系统方案在政府相关部门的引入，将有助于提高政府监管能力，防止出现资金挪用、拖延工作等问题。

5.3　区块链 + 电子商务信息系统

互联网的发展带动了工业的升级，传统电子商务也面临着革新。当前电商市场竞争越来越激烈，恶性竞争、监管不当等问题也渐渐凸显。安全问题已经成为制约电子商务发展的瓶颈，严重阻碍其进一步发展，需要有效的创新手段来改变安全隐患、信任危机、供应链运作、假货泛滥、侵犯知识产权、物流滞后、政府监管薄弱等一系列问题。而区块链的出现使得脱离中介仍可实现价值转移成为一种可能，在此基础上辅以共识机制、高度信任、抗篡改、防伪溯源、安全和可编程等特性，使我们看到了区块链与电子商务的融合势必会对互联网经济带来根本性的变革。区块链对电子商务业务的影响是多维度的，渗透于电子商务运作的各个环节，如表 7 所示。借助区块链技术提供的这些解决方案，可以帮助解决电子商务行业固有的问题，使得电商平台做到高品质、高效率、低成本、全透明、安全。

表 7　区块链在电子商务中的应用

电子商务	交易主体	买方	使用户获得交易数据所有权，可自行决定交易数据的使用
		卖方	采用区块链技术，交易记录、评价都是真实的，避免流量造假，有利于商家树立品牌
	交易事物	商品	防伪溯源，保障商品的真实性
	交易市场	电商平台	减少中间环节，采用共识机制解决交易纠纷，优化与消费者关系，提升信任。发通行证，去中心化经营，降低获客成本和运营建设成本
	三流	信息流	信息流快递快速安全，避免各环节信息泄漏
		资金流	实现较低的手续费，更快到账且更安全
		物流	实现物流整个环节的防伪溯源，有利于维权

当前区块链技术较多应用于商品溯源和跨境交易上，这也是区块链最容易落地的场景。在国家对跨境贸易政策大力支持和经济全球化的时代背景下，世界各国经济交流日益频繁，跨境电子商务得到了飞速发展，但同时跨境电商也面临着许多前所未有的挑战。物流方面，成本高耗时久、货物损坏时难以追责、货物追溯难度大；支付方面，跨境支付周期长且效率低。这些问题严重制约了跨境电子商务的发展。区块链技术去中心化、公开透明、分布式记账、点对点传输等特点可以完美解决跨境电商现存的问题。将区块链作为数据存储载体，通过实时或离线等方式将商品生产销售环节中的数据写入区块链，成为无法篡改的电子证据，可以提升各方主体造假抵赖的成本，进一步厘清各方的责任边界，同时还能通过区块链的链式结构，追本溯源，实现对物流实时监控和对货物进行溯源。区块链与跨境电商的结合，也可以保护用户的隐私，对商品质量提供保障，使得电商行业更加高效透明。目前已有多家公司投身于区块链研发，2018 年蚂蚁金服推出全球首个基于电子钱包的区块链跨境汇款平台。天猫国际和菜鸟也宣布启用区块链技术与跨境电商整合，构建出的系统可以轻松实现商品溯源和跟踪，方便消费者进行查验。英国区块链技术公司 Billon 集团发布的全球区块链金融贸易平台 DLT 在跨境电商方面有很强的助推作用。

5.4 区块链 + 智慧医疗信息系统

随着医疗数据呈现指数型的快速增长，自 2016 年国务院发布《关于促进和规范健康医疗大数据应用发展的指导意见》以来，医疗大数据正式纳入了国家发展轨迹。而根据国家卫健委统计信息中心的最新消息，我国 2020 年医疗卫生机构数达 101.1 万个，医疗卫生机构诊疗人次 2019 年 11 月份达到 7.3 亿人次。针对医疗数据存在的问题，如何高效地进行存储、管理、分享已成为限制行业发展的瓶颈。

医疗数据主要包括居民的个人电子病历、诊断检查结果记录和健康档案等重要隐私数据，容易造成患者信息泄露、医疗数据丢失等问题。另外一个则是医疗数据的安全共享问题。由于数据分散在各个不同的医疗机构，各个主体收集数据不完整，造成数据存储结构不同缺乏数据统一标准，缺乏严谨的数据管理和完善的共享规范和机制造成了信息孤岛，不能实现跨机构和跨岗位的及时的、准确的数据共享。

电子健康档案 EHR（Electronic Health Record）通过使用电子信息技术对患者病历和就医记录进行存储、管理和传输，使得医生能够很好地管理和掌握患者的健康状况，但其存储于医疗机构中心化数据库中，数据隐私泄露和数据在患者、医疗机构和医疗数据企业之间的流通共享问题依然存在。

区块链的去中心化、安全可信、集体维护、数据不可篡改等特点为数据存储、共享等方面提供了新的解决方案。随着医疗行业快速，在市场需求的驱动下和科技进步和融合的推动下，作为未来的趋势，近几年来区块链结合医疗行业的系统和应用数量日趋增长，国内外越来越多的企业和机构将聚焦于区块链和医疗项目的结合。

在国外，苹果一直致力于开发数字健康平台，新的苹果健康记录程序允许患者通过

iPhone 自己查看和更新自己的健康记录。Google 旗下的 AI 健康科技子公司 DeepMindHealth 宣称将使用区块链技术让医院、NHS、甚至病人自身都能实时跟踪其个人健康数据。美国食品药品监督管理局宣布与 IBM、Waston Health 共同合作，研究如何使用块链技术来共享健康数据以改善公共健康状况。医疗保健产品巨头飞利浦医疗专注于智能医疗设备的区块链技术应用，旨在通过设备实时监测病人健康信息。英国医疗集团 Groves 是首个应用区块链并接受加密货币支付的医疗机构。其系统基于 Hyperledger Fabric 开发，主要是面向近在 Groves 旗下的四个医疗中心的 3 万名患者的电子健康记录数据。

在国内，阿里健康宣布与常州市合作的“医联体 + 区块链”试点项目是我国第一个基于医疗场景实施的区块链应用。微信智慧医院 3.0 是一个面向监管方、医院、流通药企的一个联盟链。不仅整合联动了人社、医院、药企、保险等多方资源，而且加入了微信支付、AI 等其他腾讯产品的核心能力。众安保险 2017 年 5 月发布了基于区块链技术和大数据的“安链云”，并成功应用于辽宁等地医疗流程改革。台北医学大学附设医院公开了全球第一张区块链“智能健康随行卡”，它面向病患存储相关个人资料、就医记录、保险理赔等数据，而用户具有数据分享的权限。

清华大学也研发了基于区块链的智慧医疗信息系统。通过区块链技术实现医疗领域的数字化转型，不仅仅体现在医疗健康数据系统，还可通过将药品原材料采购、药品生产、药品销售完整供应链进行全程记录在医疗保险区块链中，从而实现对药品防伪的溯源和追踪。在医疗电子保单领域，可以通过智能合约的形式来自动完成保险项目推荐、自动赔付等过程。

5.5　区块链 + 智能制造信息系统

作为从自动化到数字化的一场新的工业革命，德国率先提出了工业 4.0 概念，美国提出了工业互联网，中国提出了中国制造 2025。工业 4.0 的核心是智能制造（smart manufacturing），其目标是实现更高的生产率、更低的低成本、更高的产品质量。智能制造是由人类专家和智能机器共同组成的人机一体化智能系统。为了实现智能制造，需要将许多技术和系统进行有效的集成，需要连接各种制造单元、设施、机器、供应商、零售商以及其他制造支撑产业，构造完整的制造价值链，形成一个智能制造网络。

智能制造系统必须提供互操作性、信息透明和去中心化决策。目前，区块链技术在智能制造中的主要应用领域包括[139]：

1）物联网数据采集。保证智能设备上数据的可靠性和可信性。

2）供应链管理。进行原材料防伪、产品认证和溯源、合同的自动签订和确认等。

3）运营管理。在审计和监督生产制造的各个环节，进行质量控制、产品管理、安全检查，保证产品质量、生产安全、开支合理。

4）知识产权保护。进行专利和软件著作权认证。

5）电子商务。支持去中介化的商务，节省交易费用。

下面分别介绍国外和国内的几个典型案例[140-141]。

美国 Middleware Technologies Lab 开发了一个面向服务的中间件系统 Man4Ware[139]，用于开发、执行和支持智能制造应用中的分布式应用。Man4Ware 提供的区块链服务包括：

1）数字身份标识。区块链可以为用户、机器、传感器、软件代理、其他实体等签发一个数据身份标识。该标识唯一代表该实体，用于进行验证、记录有关的活动和事件。

2）分布式安全账本。区块链使用分区化和分布式方法，保护记录在共享账本上的数据和交易，提供保密、防篡改、可验证和可靠性。

3）智能合约。支持在公共网络上不通过第三方就可履行可信的合同。能够进行协议的自动处理，例如，供应商、运输商、仓储商、分销商、分包商等合作伙伴，通过协商达成协议而自动记录为智能合约，而无须依赖第三方登记或烦琐的文案工作。

4）微控制。区块链不需第三方确认和外部保证而能够安全地记录事件和活动，使得企业可建立关于活动和流程的详细总账，实现在细粒度上进行微计量、微测量和动态调整。

中国科学院自动化所[141]设计了一个使用区块链作为数字基础结构的协作生产框架，支持社会制造模式（Social manufacturing）。该框架自底向上分为 5 层：

1）资源服务层，包括信息技术与资源、制造技术与资源以及区块链基础结构。区块链基础结构包括跨链部分和链下部分，主要有预言机（Oracle），链下管理和链下认证等，实现链与链之间、链与现实世界之间的交互。

2）网络互联层，包括数字身份认证、社区组织管理、P2P 可信通信、物理信息社会系统（CPSS）网络。企业、用户、设备在获得数字身份后，成为 CPSS 网络的可信节点。

3）市场协议层，包括个性化推荐、智能搜索等工具，以及智能合约。通过用智能合约取代传统的合同，支持去中心化自由职业市场和去中心化电子贸易市场。

4）协同管理层，包括：数据与版权管理、服务与资源管理、产品与项目管理、运营与监督管理、分析与优化管理。解决互操作、协作、安全性、监管问题。

5）价值互联层。包括金融科技、社区经济、代币（token）经济、共享经济和价值互联网，支持全球价值链的治理。

总之，区块链技术在智能制造中的应用正在兴起。在电子商务、供应链管理、知识产权管理等方面，技术上相对成熟一些。而在生产控制、生产管理、物联网、工业互联网等方面的应用，需要更多的研究和开发。需要解决的主要问题有：

1）实时性。现有的区块链系统没有考虑实时处理问题，设备实时处理要求确保能够及时地记录和确认设备产生的数据，以及及时地认证对于设备需要的操作数据。

2）执行效率。现有的主流区块链系统仍然存在效率低下问题，难以满足大规模生产过程中的数据处理需要。

3）可靠性和安全性。在工业环境下，对于区块链的可靠性和智能合约的安全性，要求更高的标准。现有的主流区块链系统必须经过严格的安全认证，才能满足要求。

5.6　区块链 + 绿色农业信息系统

在农业部门，区块链正被应用于供应链管理系统中，以提供供应链中所有操作的透明性、安全性、中立性和可靠性。本节对区块链技术在农业领域的应用方案进行讨论。

（1）区块链 + 农业产业链

区块链技术能够统合农业产业链中的农村土地、劳动力、人力资本、信息等要素，使其更加智能化、集约化。传统的“公司 + 农户”的农业产业链组织模式能够以区块链为纽带向着“数据平台 + 农户”的新型农业产业组织模式转化，从而实现农业的高效高质发展。文献［142］介绍了“善粮味道”运用新一代信息技术将区块链网络治理嵌入到农业产业链的治理当中，形成了更加数字化、智能化、集成化的数字制度供给的案例。通过区块链技术构建的“平台 + 基地 + 农户”的创新型农场模式实现了农产品从播种到食用的标准化闭环，促进了农业生产的高效性、高质量的发展。

（2）区块链 + 农产品质量溯源

区块链技术提供的去中心化存储机制，保证了农产品交易中买卖双方的信息透明度，不仅能够保证农产品买卖的信任机制，也能够有效监督农产品的质量安全。文献［143］针对区块链追溯系统信息数据存储负载大、查询效率低等问题，提出“数据库 + 区块链”的链上链下追溯信息双存储设计，本地数据库存储追溯明文数据，区块链上存储追溯数据加密后的哈希值，并在此基础上建立了外联数据库索引的查询方法。文献［144］研究基于农业物联网、智能防伪和区块链技术的去中心化溯源应用体系，将农产品从种植、仓储、加工到销售等全产业链进行追溯应用，通过商品追溯码在平台上验证农产品可信来源产业链信息。

除了以上提到的国内方案外，国外学者也对区块链在农业中的应用有着深入研究。其中较为突出的成果有：1）文献［145］提出了一个生产加工商的供应链系统平台及提高食品供应链效率的体系，使来自供应链任何部分的错误都很容易被发现。企业可以在短时间内找到解决方案，提高供应链效率。2）文献［146］基于区块链技术的分布式（分散的）超账平台，定义一个基于新的体验质量（QoE）食品指标的按需食品商业模式，以提供更好的执行价值链。提供透明和安全的供应链系统，以及对食品的原产地和整个生产、运输和市场分配过程的信任。

6　发展趋势与展望

6.1　区块链信息系统的基础平台研发

中国要想成为网络强国，必将在国产自主可控区块链信息系统的研发工作上持续发

力。在我国区块链领域的政产学研用结合上，国内各界将汇集智慧，通过开放合作的研究平台，共同推进区块链生态产业健康、有序的发展。

众所周知，区块链已经进入 2.0 到 3.0 的过渡时期。换句话说，区块链从以智能合约为典型特征，过渡到基于规则的可信智能社会治理体系为典型特征，这是全体系的演变。国内外的技术研发人员都兴奋地意识到区块链技术进展在改变社会关系与价值体系中将带来的全新面貌。在此时期，研发自主可控、安全的区块链关键技术将获得更广泛的关注和更深入的支持，具体表现为：

1）区块链底层技术的研发力度将持续加大。在去中心化的网络模型中，动态网络连接模式已经发生了根本性变化。区块链底层技术需要做系统性的技术研发和创新，技术上的差距及缺口将倒逼政府层面加大对区块链底层技术研发的政策倾斜。

2）自主创新的重视程度将提高。目前，西方发达国家更加侧重区块链基础技术平台及操作系统的研发，而国内则以仿制和应用落地为主，这与我国建设网络强国的要求严重不符。而区块链系统中的安全子系统、效率子系统和扩展子系统之间的动态耦合关系仍然是我们研究自主知识产权的区块链架构的发力点，是产生原始性创新和自主创新的土壤。

3）三元平衡寻优技术将成为新的研发重点。从科学和技术角度来讲，区块链实际上就是解决三元悖论，下一代区块链技术的核心是三元平衡寻优问题。解决了这一问题，就是破解了区块链底层技术目前的多重痛点，就可以实现广泛的落地应用，为我国经济社会发展作出积极贡献。

6.2 区块链信息系统的监管体系

区块链安全监管一方面需要从政策、法规和制度的角度出发，制定相关监管制度与法规，另一方面需要加强对区块链监管技术的研究。

（1）智能合约与监管技术相结合

智能合约作为外部治理的接口，使区块链本身能够对外部治理做出反应，将监管条例写成智能合约部署在链上，实现监管的自动运行，可以减轻监管机构在现有政治和企业治理系统方面的负担，让其他人可以获得可执行的、可验证的治理系统。

（2）用户准入及评估研究

建设完备的区块链准入机制，收集并分析主体在区块链上的各类行为，建立完备的主体可信评估机制，对主体进行可信评估并且反馈给监管方。通过主动发现主体异常行为，提前预防主体对区块链体系的更大破坏。实现用户规范监管的同时确保用户数据的隐私与安全，实现二者的博弈。

（3）区块链节点追踪与可视化

监管各类节点的网络地址、账户地址和交易信息的情况，方便管理者对一个区块链的参与者进行有效的管理。将监管沙盒机制应用在区块链技术发展上，设置区块链发展区域，进行真实环境下的大胆试错，逐步完善区块链技术和监管技术，最终实现区块链

与监管沙盒的双向纠错。

（4）“以链治链”

区块链治理可以借助区块链共识机制，将治理区块链的法律和合同等条款转化为代码规则，由底层区块链网络自动执行、多方共识。未来需要对以链治链制定统一的技术架构体系、治理流程和治理标准规范。

6.3　区块链信息系统的交叉学科融合

区块链信息系统对于数据共享、数据智能的有效支撑将会进一步加深与其他学科的交叉融合。最早的集中式数据共享方案将待共享数据部署在中心服务器上，客户端连接中心服务器并下载数据。基于点对点网络的数据共享方案将数据分散在网络中的多个节点上，以增强系统可扩展性。然而，以上两种方案均无法确保数据不被篡改。而基于区块链的数据共享方案则能够确保链上数据真实可信。区块链技术还可有效促进人工智能的发展。数据驱动的人工智能技术通过分析海量数据来提供智能化决策服务，在此过程中需要保障数据安全、保护用户隐私。区块链中的密码学技术对数据进行加密和匿名化处理，智能合约技术能够让个体客观、公正地沿着预设的规章制度来实施，共识和投票机制可协调不同个体的立场，激励和监管机制可成为大规模合作与协同的有效动力。

例如，开放教育（Open Education）的发展经历了三个阶段，即：教育资源开放共享、大规模教学交互、跨平台开放。这三个阶段均需要从技术上在参与者之间构建信任关系，包括第一个阶段的教育知识产权确权、第二个阶段的教育数字档案存证与追踪、第三个阶段的跨平台数据分享等。区块链技术能够为开放教育的发展提供技术支持。

6.4　区块链信息系统的标准体系

2016 年 9 月，国际标准化组织（ISO）成立了区块链和分布式记账技术标准化技术委员会（ISO/TC 307），主要工作范围是制定区块链和分布式记账技术领域的国际标准，以及与其他国际性组织合作研究该领域的标准化问题。截至 2018 年 12 月，ISO/TC 307 已成立了 4 个工作组（基础工作组，安全、隐私和身份工作组，智能合约及其应用工作组，治理工作组），2 个研究组（用例研究组，互操作研究组），以及 1 个联合工作组（区块链和分布式记账技术与 IT 安全技术）。2017 年下半年以来，ISO/TC 307 加快推动基础、智能合约、安全、隐私保护、身份和互操作等方向重点标准项目的研制工作。截至 2018 年 12 月，术语、参考架构、分类和本体等 11 项国际标准项目已正式立项，进入制定阶段。11 项国际标准项目的开展，将有助于打通不同国家、行业和系统之间的认知和技术屏障，防范应用风险，为全球区块链技术和应用发展提供重要的标准化依据。在参与国际标准化工作过程中，中国将《区块链参考架构》等团体标准成果作为贡献物提交至 ISO/TC 307，推动了参考架构等国际标准的立项。目前中国专家担任参考架构国际标准的联合编辑、分类和本体技术规范的编辑，并牵头区块链数据流动和数据分类相关

课题的研究工作。

6.5 区块链信息系统的开源联盟

近年来，国际上 R3 区块链联盟、CBSG 运营商区块链联盟、TloTTA 可信物联网联盟和 B3I 区块链保险行业倡议等联盟高速发展，中国也有越来越多的区块链技术产业联盟兴起，如金融区块链合作联盟、中国区块链技术和产业发展论坛，可信区块链联盟以及最新的重庆区块链应用创新产业联盟等，这些联盟凝聚政、产、学、研等各方资源，跟踪研究区块链技术和应用发展趋势，研究行业标准，构建区块链发展路线图。

产业方面，在各类新兴区块链技术不断出现的情况下，需要整合区块链产业公共资源，促进区块链产业要素流通，借助联盟和公共服务平台探索产业新生态，与实体经济深度融合，将区块链赋能在实体经济发展方面。技术方面，跨链互操作是区块链进化的重要方向，目前在跨链方面，行业还没有一项普遍接受的协议或者标准；其次，多方可信计算、预言机、数字身份、隐私保护、智能合约语言等领域也是重要探索方向。同时，应普及监管沙盒，以提供更舒适的运行和创新环境。开源是大势所趋，从云计算到边缘计算到万物计算，带来了巨大的数据量和计算量，需要大规模软件的支撑，企业积极参与到开源中去有利于吸引广大开发者不断进行创新。

6.6 其他创新技术与创新应用

基于区块链系统的生态环境，使用区块链的特性能够为大量领域带来新的应用模式。除了上面介绍的六大应用之外，区块链还有很多的创新技术和创新应用，包括：工业区块链、农业区块链、军事区块链、商业区块链、能源区块链等，正在形成新的产业生态，下面简单介绍几个例子。

在产业供应链领域，与产品和原料相关的生产、运输、仓储和销售等环节都需要记录大量的过程信息。使用区块链系统存储并管理供应链系统数据，能够支持供应链过程信息的深度溯源、查询和验证等核心功能，从而提高每个环节的可见度和可信度，降低欺诈和盗窃风险，大大提高物流效率。

在征信管理领域，区块链系统具有的信息不可篡改、数据加密授权保护、智能合约等特性能够有效地解决原有征信系统中信用信息孤岛问题、提高系统安全性和降低征信运营成本。

在公益慈善领域，区块链系统所构建的新型信任机制，能够实现公益信息的透明公开、有效监管，帮助公益慈善领域解决信任问题。区块链系统可以记录公益流程中的捐赠项目、募集明细、资金使用和受益人反馈等全部信息，同时由多家公益组织、支付机构、审计机构构成多方参与的联盟链，可以提高信息的安全性。

在文化创意产业领域，例如，为艺术博物馆等展览机构，提供基于区块链的藏品存证方式、基于区块链的艺术展览展品的溯源展示方式、基于区块链的文化产业内容输出

者版权保护机制、基于区块链的艺术博物馆溯源存证系统、基于区块链的文化艺术监管链条体系，实现展品信息的有效存档、藏品智能管理、观众有效传播，为建立智慧博物馆提供有效支撑。

区块链技术今后的发展，重点是4个方面：1）提高系统性能和可伸缩性（优化存储管理、优化通信开销、优化系统运行开销、提高事务处理吞吐度等）；2）提高跨链互操作性（优化原子事务提交机制、优化资产锁定机制、优化跨链交易验证机制、跨链查询处理和优化、跨链安全性等）；3）加强数据隐私保护（零知识证明协议、安全多方计算技术、同态加密技术等）；4）加强区块链监管与安全性（“以链治链”机制、内容访问控制和信息屏蔽技术、监管方友好兼顾隐私保护的交易审计技术、智能合约代码的安全性等）。

7 结束语

本文从体系架构、建模方法、存储管理、联邦计算、跨链互操作、隐私保护、链上链下融合、云边端融合八个方面对区块链系统的国内外现状及比较做了系统的分析和比较。同时，从区块链+数字金融、区块链+电子政务、区块链+电子商务、区块链+智慧医疗、区块链+智能制造以及区块链+绿色农业几个方面进行了应用分析。随着区块链应用场景的逐渐明晰和需求的日益增长，未来区块链应用系统会逐步覆盖到各行各业，真正服务于社会。

参考文献

[1] Swan M. Blockchain: Blueprint for a New Economy[M]. USA: O'Reilly Media Inc., 2015.

[2] Technical report by the UK government chief scientiflc adviser[Online], available: https://www.gov.uk/government/uploads/system/uploads/attachment data/flle/492972/gs-16-1-distributed-ledger-technology.pdf, February 21, 2016.

[3] Nakamoto S. Bitcoin: a peer-to-peer electronic cash system[Online], available: https://bitcoin.org/bitcoin.pdf, 2009.

[4] Ethereum White Paper. A next-generation smart contract and decentralized application platform [Online], available: https://github.com/ethereum/wiki/wiki/WhitePaper, November 12, 2015.

[5] Ding Wei. Block chain based instrument data managementsystem[J]. China Instrumentation, 2015, (10): 15-17.

[6] 范吉立，李晓华，聂铁铮，于戈. 区块链系统中智能合约技术综述[J]. 计算机科学，2019，46(11)：1-10.

[7] Gribble S D, Halevy A Y, Ives Z G, et al. What can database do forpeer-to-peer? [C]. Proceedings of the Fourth International Workshop on theWeb and Databases (WebDB), Santa Barbara, USA, 2001: 31-36.

[8] Yu Ming, Li Zhan-Huai, Zhang Long-Bo. P2P data management[J]. Journal of Software, 2006, 17(8): 1717-1730(in chinese)(余敏, 李战怀, 张龙波. P2P 数据管理. 软件学报, 2006, 17(8): 1717-1730).

[9] Qian Wei-Ning. Data management in peer-to-peer systems[Ph. D. dissertation]. Fudan University, Shanghai, 2004(in chinese)(钱卫宁. 对等计算系统中的数据管理[博士学位论文]. 复旦大学, 上海, 2004).

[10] Antonopoulos A M. Mastering bitcoin: Unlocking digitalcryptocurrencies. Sebastopol[M]. USA: O'Reilly Media, Inc., 2014.

[11] Douceur J R. The sybil attack//International Workshop on Peer-to-PeerSystems (IPTPS)[M]. Cambridge, USA, 2002: 251-260.

[12] Dwork C, Naor M. Pricing via processing or combatting junk mail[C]. Proceedings of the Advances in Cryptology-CRYPTO'92 (CRYPTO). Santa Barbara, USA, 1992: 139-147.

[13] Aspnes J, Jackson C, Krishnamurthy A. Exposingcomputationally-challenged Byzantine impostors[C]. New Haven, USA: Yale University, Technical Report: YALEU/DCS/TR-1332, 2005.

[14] King S, Nadal S. PPCoin: Peer-to-peer crypto-currency withproof-of-stake[C]. White Paper, 2012.

[15] Larimer D. Delegated proof-of-stake[C]. White Paper, 2014.

[16] Bayer D, Haber S, Stornetta W S. Improving the efficiency andreliability of digital time-stamping// Sequences II: Methods in Communication, Security and Computer Science. New York[M]. USA: Springer-Verlag, 1993: 329-334.

[17] Haber S, Stornetta W S. How to time-stamp a digital document//Proceedings of the Advances in Cryptology-CRYPTO'90 (CRYPTO)[M]. Santa Barbara, USA, 1990: 437-455.

[18] Haber S, Stornetta W S. Secure names for bit-strings//Proceedings of the 4th ACM Conference on Computer and Communications Security(CCS)[C]. Zurich, Switzerland, 1997: 28-35.

[19] Narayanan A, Bonneau J, Felten E, et al. Bitcoin and cryptocurrencytechnologies: A comprehensive introduction[M]. Princeton: PrincetonUniversity Press, 2016.

[20] Szabo N. Formalizing and securing relationships on public networks[J]. First Monday, 1997, 2(9).

[21] Dannen C. Introducing ethereum and solidity: Foundations ofcryptocurrency and blockchain programming for beginners[M]. Berkeley, USA: Apress, 2017.

[22] Shentu Qing-Chun. Development guide of blockchain[M]. Beijing: ChinaMachine Press, 2017(in Chinese)(申屠青春. 区块链开发指南. 北京: 机械工业出版社, 2017).

[23] L Luu, V Narayanan, C Zheng, K Baweja, S Gilbert, and P Saxena. A secure sharding protocol for open blockchains[C]. ACM CCS 2016: 17-30.

[24] E Kokoris-Kogias, P Jovanovic, L Gasser, N Gailly, E Syta, and B Ford. OmniLedger: A secure, scale-out, decentralized ledger via sharding[C]. IEEE S&P 2018: 583-598.

[25] M Al-Bassam, A Sonnino, S Bano, D Hrycyszyn, and G Danezis. Chainspace: A sharded smart contracts platform[C]. NDSS 2018.

[26] M Zamani, M Movahedi, and M Raykova. Rapidchain: Scaling blockchain via full sharding[C]. ACM CCS 2018: 931-948.

[27] BigchainDB 公司. BigchainDB 2.0: the blockchain database[C]. White Paper, 2018.

[28] Muhammad El-Hindi, Carsten Binnig, Arvind Arasu, Donald Kossmann, and Ravi Ramamurthy. BlockchainDB: a shared database on blockchains[J]. PVLDB, 12(11): 1597-1609.

[29] O'Neil P, Cheng E, Gawlick D, O'Neil E. The Log-Structured Merge-Tree (LSM Tree)[J]. Acta Informatica, 1996, 33(4): 351-385.

[30] SHAWN W, TOME B, JOSH B, etal. Storj A Peer-to-Peer Cloud Storage Network. [EB/OL]https://storj.io/storj.pdf. 2016.

[31] El-Hindi M, Binnig C, Arasu A, et al. BlockchainDB: ashared database on blockchains[J]. Proceedings of the VLDB Endowment, 2019, 12(11): 1597-1609.

[32] Wang S, Dinh T T A, Lin Q, et al. Forkbase: An efficient storage engine for blockchain and forkable applications[J]. arXiv preprint arXiv: 1802.04949, 2018.

[33] McMahan H B, Moore E, Ramage D, et al. Communication-efficient learning of deep networks from decentralized data[J]. arXiv preprint arXiv: 1602.05629, 2016.

[34] Lugan S, Desbordes P, Brion E, et al. Secure Architectures Implementing Trusted Coalitions for Blockchained Distributed Learning (TCLearn)[C]. IEEE Access, 2019: 181789-181799.

[35] S Awan, F Li, B Luo, and M Liu, Poster: A reliable and accountable privacy-preserving federated learning framework using the blockchain[C]. in Proceedings of the 2019 ACM SIGSAC Conference on Computer and Commumications Security, 2019, pp. 2561-2563.

[36] L Lyu, J Yu, K Nandakumar, Y Li, X Ma, and J Jin. Towards fair and decentralized privacy-preserving deep learning with blockchain[J]. arXiv preprint arXiv: 1906.01167, 2019.

[37] Gilad Y, Hemo R, Micali S, Vlachos G, Zeldovich N. Algorand: scaling byzantine agreements for cryptocurrencies[Online], available: http://eprint.iacr.org/2017/454, April 10, 2018.

[38] Pass R, Shi E. The sleepy model of consensus [Online], available: https://eprint.iacr.org/2016/918.pdf, August 16, 2018.

[39] Siris V A Nikander P Voulgaris S et al. Interledger Approaches[C]. IEEE Access vol.7, 2019.

[40] Buterin V. Chain Interoperability. https://www.r3.com/wp-content/uploads/2018/04/Chain_Interoperability_R3.pdf.

[41] Back A, Corrallo M, Dashjr L, et al. Enabling Blockchain Innovations with Pegged Sidechains. 2014-10-22. https://www.blockstream.com/sidechains.pdf.

[42] ConsenSys. BTC Relay's documentation. 2016.9.10. http://btc-relay.readthedocs.io/en/latest/.

[43] Johnny D, Andrew P, Jonathan W, Marta P, Ben G, Mark F. Strong federations: An interoperable blockchain solution to centralized third party risks. 2017.1.30. https://arxiv.org/pdf/1612.05491.pdf.

[44] Wood G Polkadot: Vision for a heterogeneous multi-chain framework draft 1. https://polkadot.network/PolkaDotPaper.pdf.

[45] Buchman E, Kwon J Cosmos: A Network of Distributed Ledgers. https://github.com/cosmos/cosmos/blob/master/whitepaper.md.

[46] Hope-Bailie A, Thomas S. Interledger: Creating a Standard for Payments[C]. The 25th Int. Conf. Companion on World Wide Web, April 11-15, 2016.

[47] Fromknecht C. Connecting blockchains: Instant cross-chain transactions on lightning. 2017.11.16. https://blog.lightning.engineering/announcement/2017/11/16/ln-swap.html.

[48] Fusion-A connected ecosystem for financial transactions. https://www.fusion.org/.

[49] Wanchain-Decentralized Finance Interoperability. https://www.wanchain.org.

[50] Dash. Dash is digital cash [EB/OL]. https://www.dash.org/.

[51] Bergan T, Anderson O, Devietti J, et al. CryptoNote v 2.0[J]. 2013.

[52] Sasson E B, Chiesa A, Garman C, et al. Zerocash: Decentralized Anonymous Payments from Bitcoin [C]. IEEE Symposium on Security and Privacy. IEEE Computer Society, 2014: 459-474.

[53] Rush A M, Chopra S, Weston J A neural attention model for abstractive sentence summarization [J]. Computer Science, 2015.

[54] Bensasson E, Chiesa A, Genkin D, et al. SNARKs for C: Verifying Program Executions Succinctly and in Zero Knowledge[J]. Lecture Notes in Computer Science, 2013, 8043: 90-108.

[55] Azaria A , Ekblaw A , Vieira T , et al. MedRec: Using Blockchain for Medical Data Access and Permission Management[J]. 2016: 25-30.

[56] S Malik, V Dedeoglu, S S Kanhere and R Jurdak, TrustChain: Trust Management in Blockchain and IoT Supported Supply Chains [C]. 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 2019, pp. 184-193.

[57] Prybila C , Schulte S , Hochreiner C , et al. Runtime Verification for Business Processes Utilizing the Bitcoin Blockchain[J]. Future Generation Computer Systems, 2017: S0167739X1731837X.

[58] Ingo Weber, Xiwei Xu, Régis Riveret, 等. Untrusted Business Process Monitoring and Execution Using Blockchain[M]. Business Process Management. Springer International Publishing, 2016.

[59] Goel N, van Schreven C, Filos-Ratsikas A, et al. Infochain: A decentralized, trustless and transparent oracle on blockchain[C]. Proceedings of the 29th International Joint Conference on Artificial Intelligence (IJCAI). 2020.

[60] Chainlink, https://chain.link/.

[61] W Shi, J Cao, Q Zhang, Y Li, L Xu. Edge Computing: Vision and Challenges[J]. IEEE Internet of Things Journal, 2016, 3(5): 637-646.

[62] P K Sharma, J H Park. Blockchain based hybrid network architecture for the smart city[C]. Futur. Gener. Comput. Syst. 2018, 86: 650-655.

[63] A Stanciu. Blockchain Based Distributed Control System for Edge Computing[C]. CSCS 2017: 667-671

[64] A Dorri, S S Kanhere, R Jurdak and P Gauravaram. Blockchain for IoT security and privacy: The case study of a smart home[C]. PerCom Workshops 2017: 618-623.

[65] Z A Khan, A G Abbasi, Z Pervez. Blockchain and edge computing-based architecture for participatory smart city applications[C]. Concurr. Comput. Pract. Exp., 2020, 32(12): e5566.

[66] M A Rahman, M M Rashid, M S Hossain, E Hassanain, M F Alhamid and M Guizani. Blockchain and IoT-Based Cognitive Edge Framework for Sharing Economy Services in a Smart City[C]. IEEE Access, 2019, 7: 18611-18621.

[67] M A Rahman, M S Hossain, G Loukas, E Hassanain, S S Rahman, M F Alhamid, and M Guizani. Blockchain-Based Mobile Edge Computing Framework for Secure Therapy Applications [C]. IEEE Access, 2018, 6: 72469-72478.

[68] Z Xiong, Y Zhang, D Niyato, P Wang and Z Han. When Mobile Blockchain Meets Edge Computing[C]. IEEE Communications Magazine, 2018, 56(8): 33-39.

[69] N C Luong, Z Xiong, P Wang and D Niyato. Optimal Auction for Edge Computing Resource Management in Mobile Blockchain Networks: A Deep Learning Approach[C]. ICC 2018: 1-6.

[70] Y Huang, J Zhang, J Duan, B Xiao, F Ye and Y Yang. Resource Allocation and Consensus on Edge Blockchain in Pervasive Edge Computing Environments[C]. ICDCS 2019: 1476-1486.

[71] Y Tao, B Li, J Jiang, H C Ng, C Wang and B Li On Sharding Open Blockchains with Smart Contracts

[C]. ICDE 2020: 1357-1368.

[72] Chenyu Huang, Zeyu Wang, Huangxun Chen, Qiwei Hu, Qian Zhang, Wei Wang, and Xia Guan. RepChain: A Reputation-based Secure, Fast and High Incentive Blockchain System via Sharding[J]. arXiv: 1901.05741v2, 2019.

[73] Mengqian Zhang, Jichen Li, Zhaohua Chen, Hongyin Chen, and Xiaotie Deng. CycLedger: A Scalable and Secure Parallel Protocol for Distributed Ledger via Sharding[C]. IPDPS 2020: 358-367.

[74] 众享比特公司. ChainSQL 技术白皮书. http://www.chainsql.net/PDF/ChainSQL 技术白皮书 v1.0.pdf.

[75] Yang Li, Kai Zheng, Ying Yan, Qi Liu, and Xiaofang Zhou. EtherQL: A Query Layer for Blockchain System[J]. DASFAA (2) 2017: 556-567.

[76] Y. Zhu, Z. Zhang, C. Jin, A. Zhou and Y. Yan. SEBDB: Semantics Empowered BlockChain DataBase [C]. ICDE 2019: 1820-1831.

[77] Cheng Xu, Ce Zhang, and Jianliang Xu. VChain: Enabling Verifiable Boolean Range Queries over Blockchain Databases[C]. SIGMOD 2019: 141-158.

[78] Xu Z, Han S, Chen L. Cub, a consensus unit-based storage scheme for blockchain system[C]. 2018 IEEE 34th International Conference on Data Engineering (ICDE). IEEE, 2018: 173-184.

[79] Qi X, Zhang Z, Jin C, et al. BFT-Store: Storage Partition for Permissioned Blockchain via Erasure Coding[C]. 2020 IEEE 36th International Conference on Data Engineering (ICDE). IEEE, 2020: 1926-1929.

[80] Di Chai, Leye Wang, Kai Chen, Qiang Yang. Secure Federated Matrix Factorization[J]. arXiv preprint arXiv: 1906.05108, 2019.

[81] Zhou S, Huang H, Chen W, et al. PIRATE: A blockchain-based secure framework of distributed machine learning in 5g networks[J]. arXiv preprint arXiv: 1912.07860, 2019.

[82] WeBank. FATE: An industrial grade federated learning framework. https://fate.fedai.org, 2018.

[83] X Yao, T Huang, C Wu, R Zhang and L Sun. Towards Faster and Better Federated Learning: A Feature Fusion Approach[C]. 2019 IEEE International Conference on Image Processing (ICIP), Taipei, China, 2019, pp. 175-179.

[84] 刘明达, 拾以娟, 陈左宁. 基于区块链的分布式可信网络连接架构[J]. 软件学报. 2019.

[85] 张玲, 陈思捷, 严正, 沈泽宇. 基于区块链共识机制的多区域最优潮流分布式算法[J]. 中国电机工程学报. 2020.

[86] 叶少杰, 汪小益, 徐才巢, 孙建伶. BitXHub: 基于侧链中继的异构区块链互操作平台[J]. 计算机科学, 2020, 47(06): 294-302.

[87] 张诗童, 秦波, 郑海彬. 基于哈希锁定的多方跨链协议研究[J]. 网络空间安全, 2018, 9(11): 57-62+67.

[88] Huang, B, Liu, Z, Chen, J, Liu, A, Liu, Q, & He, Q (2017). Behavior pattern clustering in blockchain networks[J]. Multimedia Tools and Applications, 76(19), 20099-20110.

[89] Shentu, Q, & Yu, J (2015). A Blind-Mixing Scheme for Bitcoin based on an Elliptic Curve Cryptography Blind Digital Signature Algorithm[J]. arXiv: Cryptography and Security.

[90] 李莹, 于亚新, 张宏宇, 李振国. 基于 TBchain 区块链的高可信云存储模型[J/OL]. 计算机科学: 1-16.

[91] Yang X, Li T, Pei X, et al. Medical Data Sharing Scheme Based on Attribute Cryptosystem and

Blockchain Technology[J]. IEEE Access, 2020, PP(99): 1-1.

[92] https://baas.qq.com/doc/dev.shtml? p = assetissueapply.

[93] Li M, Huang G Q. Blockchain-enabled workflow management system for fine-grained resource sharing in E-commerce logistics[C]. 2019 IEEE 15th International Conference on Automation Science and Engineering (CASE). IEEE, 2019.

[94] S Wang, H Lu, X Sun, Y Yuan and F Wang, A Novel Blockchain Oracle Implementation Scheme Based on Application Specific Knowledge Engines[C] 2019 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI), Zhengzhou, China, 2019, pp. 258-262.

[95] Jiawen Kang, Rong Yu, Xumin Huang, Maoqiang Wu, Sabita Maharjan, Shengli Xie, and Yan Zhang. Blockchain for Secure and Efficient Data Sharing in Vehicular Edge Computing and Networks[J]. IEEE Internet of Things Journal, 2019, 6(3): 4660-4670.

[96] 程冠杰, 黄诤杰, 邓水光. 基于区块链与边缘计算的物联网数据管理[J]. 物联网学报, 2020, 4(02): 1-9

[97] X Xu, X Zhang, H Gao, Y Xue, L Qi and W Dou, BeCome: Blockchain-Enabled Computation Offloading for IoT in Mobile Edge Computing[J]. IEEE Transactions on Industrial Informatics, 2020, 16(6): 4187-4195.

[98] M Li, L Zhu and X Lin. Efficient and Privacy-Preserving Carpooling Using Blockchain-Assisted Vehicular Fog Computing[J]. in IEEE Internet of Things Journal, 2019, 6(3): 4573-4584.

[99] K Gai, Y Wu, L Zhu, L Xu and Y Zhang. Permissioned Blockchain and Edge Computing Empowered Privacy-Preserving Smart Grid Networks[J]. IEEE Internet of Things Journal, 2019, 6(5): 7992-8004.

[100] X Lin, J Li, J Wu, H Liang and W Yang. Making Knowledge Tradable in Edge-AI Enabled IoT: A Consortium Blockchain-Based Efficient and Incentive Approach[J]. IEEE Transactions on Industrial Informatics, 2019, 15(12): 6367-6378.

[101] M Liu, F R Yu, Y Teng, V C M Leung and M. Song. Computation Offloading and Content Caching in Wireless Blockchain Networks With Mobile Edge Computing[J]. IEEE Transactions on Vehicular Technology, 2018, 67(11): 11008-11021.

[102] Wuhui Chen, Zhen Zhang, Zicong Hong, Chuan Chen, Jiajing Wu, Sabita Maharjan, Zibin Zheng, and Yan Zhang. Cooperative and Distributed Computation Offloading for Blockchain-Empowered Industrial Internet of Things[J]. IEEE Internet of Things Journal, 2019, 6(5): 8433-8446.

[103] Chenhan Xu, Kun Wang, Peng Li, Song Guo, Jiangtao Luo, Baoliu Ye, and Minyi Guo. Making Big Data Open in Edges: A Resource-Efficient Blockchain-Based Approach[J]. IEEE Transactions on Parallel and Distributed Systems, 2019, 30(4): 870-882.

[104] Lugan S, Desbordes P, Brion E, et al. Secure Architectures Implementing Trusted Coalitions for Blockchained Distributed Learning (TCLearn)[C]. IEEE Access, 2019: 181789-181799.

[105] S Awan, F Li, B Luo, and M Liu, Poster: A reliable and accountable privacy-preserving federated learning framework using the blockchain[C]. in Proceedings of the 2019 ACM SIGSAC Conference on Computer and Commumications Security, 2019, pp. 2561-2563.

[106] L Lyu, J Yu, K Nandakumar, Y Li, X Ma, and J Jin. Towards fair and decentralized privacy-preserving deep learning with blockchain[J]. arXiv preprint arXiv: 1906.01167, 2019.

[107] Gilad Y, Hemo R, Micali S, Vlachos G, Zeldovich N. Algorand: scaling byzantine agreements for cryptocurrencies[Online], available: http://eprint.iacr.org/2017/454, April 10, 2018.

[108] Pass R, Shi E The sleepy model of consensus [Online], available: https://eprint.iacr.org/2016/918.pdf, August 16, 2018.

[109] Di Chai, Leye Wang, Kai Chen, Qiang Yang. Secure Federated Matrix Factorization[J]. arXiv preprint arXiv: 1906.05108, 2019

[110] Zhou S, Huang H, Chen W, et al. PIRATE: A blockchain-based secure framework of distributed machine learning in 5g networks[J]. arXiv preprint arXiv: 1912.07860, 2019.

[111] WeBank. FATE: An industrial grade federated learning framework. https://fate.fedai.org, 2018.

[112] X Yao, T Huang, C Wu, R Zhang and L Sun. Towards Faster and Better Federated Learning: A Feature Fusion Approach[C]. 2019 IEEE International Conference on Image Processing (ICIP), Taipei, China, 2019, pp.175-179.

[113] 刘明达, 拾以娟, 陈左宁. 基于区块链的分布式可信网络连接架构[J]. 软件学报. 2019.

[114] 张玲, 陈思捷, 严正, 沈泽宇. 基于区块链共识机制的多区域最优潮流分布式算法[J]. 中国电机工程学报. 2020.

[115] 路爱同, 赵阔, 杨晶莹, 王峰. 区块链跨链技术研究[J]. 信息网络安全, 2019(08): 83-90.

[116] 郭朝, 郭帅印, 张胜利, 宋令阳, 王晖. 区块链跨链技术分析[J]. 物联网学报, 2020, 4(02): 35-48.

[117] 李芳, 李卓然, 赵赫. 区块链跨链技术进展研究[J]. 软件学报, 2019, 30(06): 1649-1660.

[118] 韩璇, 刘亚敏. 区块链技术中的共识机制研究[J]. 信息网络安全, 2017(9): 147-152.

[119] Miran Kim, Junghye Lee, Lucila Ohno-Machado, Xiaoqian Jiang: Secure and Differentially Private Logistic Regression for Horizontally Distributed Data[C]. IEEE Trans. Information Forensics and Security 15: 695-710(2020).

[120] Ameena Saad Al-Sumaiti, Abdullah Khamis Banhidarah, James L. Wescoat, Abdulla Kehinde Bamigbade, Hoach The Nguyen: Data Collection Surveys on the Cornerstones of the Water-Energy Nexus: A Systematic Overview[C]. IEEE Access 8: 93011-93027(2020).

[121] Noe Elisa, Longzhi Yang, Honglei Li, Fei Chao, Nitin Naik: Consortium Blockchain for Security and Privacy-Preserving in E-government Systems[C]. CoRR abs/2006.14234 (2020).

[122] 王继业, 高灵超, 董爱强. 基于区块链的数据安全共享网络体系研究[J]. 计算机研究与发展, 2017, 54(2): 742-749.

[123] Chao Qu, Ming Tao, Jie Zhang, Xiao yu Hong, Ruifen Yuan, Blockchain Based Credibility Verification Method for IoT Entities[J]. Security and Communication Networks 2018: 7817614: 1-7817614: 11 (2018).

[124] Jian Wang, Xu Liu, Xiaoyong Ji, A Secure Communication System with Multiple Encryption Algorithms [C]. ICEE 2010: 3574-3577.

[125] Zheng Dong, Kevin Kane, L. Jean Camp: Detection of Rogue Certificates from Trusted Certificate Authorities Using Deep Neural Networks[J]. ACM Trans. Priv. Secur. 19(2): 5: 1-5: 31(2016).

[126] 陈奇伟, 聂琳峰. 技术+法律: 区块链时代个人信息权的法律保护[J]. 江西社会科学, 2020, 40(06): 166-175.

[127] 刘建伟, 黑一鸣, 管晔玮. 基于区块链的身份信息共享认证方案[J/OL]. 密码学: 1-10[2020-07-18]. http://kns.cnki.net/kcms/detail/10.1195.TN.20200521.1745.019.html.

[128] C Lin, D He, X Huang, et al., BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0[C]. Journal of Network and Computer Applications, vol. 116, pp.42-52, 2018.

[129] Yuxiang Chen, Guishan Dong, Yao Hao, Zhaolei Zhang, Haiyang Peng, Shui Yu: An Open Identity Authentication Scheme Based on Blockchain[J]. ICA3PP (1) 2019: 421-438.

[130] R Yu, J Wang, T Xu, et al., Authentication with block-chain algorithm and text encryption protocol in calculation of social network[C]. IEEE Access, vol.5, pp.24944-24951, 2017.

[131] Underwood, S (2016) Blockchain beyond Bitcoin. Communications of the ACM, 59, 15-17. https://doi.org/10.1145/2994581.

[132] Factom-Making the World's Systems Honest, 2017. [Online]. Available: https://www.factom.com. [Accessed 28 April 2017].

[133] Shrier, David, Weige Wu, and Alex Pentland. Blockchain & infrastructure (identity, data security) [C]. Massachusetts Institute of Technology-Connection Science 1.3 (2016): 1-19.

[134] 闵旭蓉, 杜葵, 戴逸聪. 基于区块链技术的电子证照共享平台设计[J]. 指挥信息系统与技术, 2017, 8(02): 47-51.

[135] Mao, Dianhui, et al. Credit evaluation system based on blockchain for multiple stakeholders in the food supply chain[C]. International journal of environmental research and public health 15.8 (2018): 1627.

[136] López-Pintado, Orlenys, et al. Caterpillar: A Blockchain-Based Business Process Management System [C]. BPM (Demos). 2017.

[137] Kim, Kibum, and Taewon Kang. Does technology against corruption always lead to benefit? The potential risks and challenges of the blockchain technology. Paper submitted to OECD's Anti-Corruption and Integrity Forum. https://www.oecd.org/cleangovbiz/Integrity-Forum-2017-Kim-Kang-blockchain-technology.pdf. 2017.

[138] Schöbel, Lukas, and Alex Kulikov. Proposal of a Permissioned Blockchain Network To Supervise Cashflow in Large-Scale Projects.

[139] 孙柏林. 国内外区块链技术概况及其在制造业中的应用[J]. 自动化博览, 2018, 35(07): 48-53.

[140] N Mohamed and J Al-Jaroodi. Applying Blockchain in Industry 4.0 Applications[C]. 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 2019, pp.0852-0858.

[141] L Ouyang, Y Yuan and F Wang, A Blockchain-based Framework for Collaborative Production in Distributed and Social Manufacturing[C]. 2019 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI), Zhengzhou, China, 2019, pp.76-81.

[142] 付豪, 赵翠萍, 程传兴. 区块链嵌入、约束打破与农业产业链治理[J]. 农业经济问题, 2019 (12): 108-117.

[143] 杨信廷, 王明亭, 徐大明, 罗娜, 孙传恒. 基于区块链的农产品追溯系统信息存储模型与查询方法[J]. 农业工程学报, 2019, 35(22): 323-330.

[144] 高阳阳, 吕相文, 袁柳, 李勐. 基于区块链的农产品安全可信溯源应用研究[J]. 计算机应用与软件, 2020, 37(07): 324-328.

[145] Tse D, Zhang B, Yang Y, et al. Blockchain application in food supply information security[C]. 2017 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM). IEEE, 2017: 1357-1361.

[146] Davcev D, Kocarev L, Carbone A, et al. Blockchain-based Distributed Cloud/Fog Platform for IoT Supply Chain Management[C]. Eighth international conference on advances in computing, electronics and electrical technology (CEET). 2018: 51-58.

[147] Bitcoin[OL]. https://bitcoin.org/.
[148] Ethereum[OL]. https://ethereum.org/.
[149] Hyperledger[OL]. https://www.hyperledger.org/.
[150] Protocol Labs. Filecoin: A Decentralized Storage Network [EB/OL]http://www.filecoi-n.io/filecoin.pdf, 2017.

作者简介

邢春晓 1967年生，清华大学北京信息科学与技术国家研究中心研究员，博士生导师，可信软件与大数据研究部副主任，清华大学信息技术研究院副院长，WEB与软件技术研究中心主任。主要研究领域：数据库和数据仓库，大数据和知识工程，人工智能，软件工程，区块链技术，智慧医疗、智慧城市、数字图书馆和电子政务关键技术研究等。中国计算机学会信息系统专业委员会副主任、数据库专委会委员，中关村区块链产业联盟副理事长，中国电子学会区块链分会副会长，中国医疗保健国际交流促进会健康大数据和数字化医疗分会副主任。

于 戈 1962年生，东北大学计算机学院教授，博士生导师，中国计算机学会会士。1982年、1986年获得东北大学计算机学士学位和硕士学位，1996年获得日本九州大学计算机博士学位。主要研究领域包括：数据库理论与技术、分布与并行式系统、云计算与大数据管理、区块链技术与应用等。中国计算机学会信息系统专业委员会主任、数据库专委会委员，以及系统软件专委会委员。

李庆忠 1965年生，山东大学教授、博士生导师。山大地纬软件股份有限公司董事长。主要研究领域包括云计算、区块链以及数据科学等。作为项目负责人主持国家重点研发计划项目“众智科学理论与方法研究”。2015年开始率领研究团队进行区块链技术研究，开发了自主可控的区块链底层技术平台大纬链，获国家网信办第一批备案，大纬链在多个领域得到了应用。

金澈清 1977年生，华东师范大学数据科学与工程学院教授，博士生导师，副院长。主要研究领域包括：海量数据管理与分析、区块链技术与应用、智慧城市等。中国计算机学会高级会员，中国计算机学会数据库专委会委员。

李瑞轩 1974 年生，华中科技大学计算机学院教授，博导，副院长，智能与分布计算实验室主任，湖北省大数据安全工程技术研究中心副主任，中国计算机学会杰出会员，信息系统专委会副主任，分布式计算与系统专委会常委，大数据专家委员会委员。主要研究方向为大数据管理与分析，云计算与边缘计算，区块链技术与应用，系统安全与隐私保护。

王 鑫 1981 年生，天津大学智能与计算学部教授，博士生导师，人工智能学院副院长。主要研究方向包括：知识图谱数据管理、图数据库、大数据分布式处理。中国计算机学会高级会员，中国计算机学会信息系统专业委员会秘书长、数据库专委会委员。

张桂刚 1978 年生，中国科学院自动化研究所副研究员，硕士生导师。主要研究方向为：信息系统、人工智能、大数据、区块链、语义计算等。中国计算机学会高级会员，中国计算机学会信息系统专业委员会委员。