

文章编号:1007-9432(2020)03-0321-10

# 区块链关键技术及其应用研究进展

朱建明,张沁楠,高 胜

(中央财经大学 信息学院,北京 100081)

**摘 要:**区块链采用密码学、共识算法、点对点通讯等技术构建了分布式的信任基础,实现链上数据的防篡改和可追溯等功能。区块链技术是金融科技领域的重要技术创新,已在数据共享、电子存证、消息溯源等领域应用,与此同时大规模节点通讯引发的性能和可扩展性等问题也限制了区块链应用的进一步发展。本文从区块链基本概念入手,分别对区块链中的关键技术,包括密码学与分布式账本、共识机制、智能合约、可扩展性技术等进行详细分析;介绍了区块链技术的主要应用,并指出区块链技术发展和应用中面临的挑战。

**关键词:**区块链;共识机制;智能合约;可扩展性;区块链应用

**中图分类号:**TP311 **文献标识码:**A

**DOI:**10.16355/j.cnki.issn1007-9432tyut.2020.03.001 **开放科学(资源服务)标识码(OSID):**



## Research Progress of Blockchain Key Technologies and Their Application

ZHU Jianming, ZHANG Qinnan, GAO Sheng

(School of Information, Central University of Finance and Economics, Beijing 100081, China)

**Abstract:** The blockchain uses cryptography, consensus algorithm, point-to-point communication and other technologies to construct a distributed trust foundation, which realizes that the data on the blockchain can be temper-proof and traceable. Blockchain technology, originated from bitcoin, is an important technological innovation in the field of fintech. It has developed rapidly in data sharing, electronic certificate, message tracing and other fields. However, the performance and scalability problems caused by large-scale node communication limit the further development and implementation of blockchain applications. Starting from the concept of blockchain basic platform, this paper elaborates the key technologies in blockchain, including cryptography and distributed ledger, consensus mechanism, smart contract and cross chain technology, points out the existing problems and bottlenecks in the development of blockchain technology. Finally, the current application fields and challenges of blockchain technology are described from the perspective of application.

**Keywords:** blockchain; consensus mechanism; smart contract; scalability; blockchain application

2019年10月24日,中共中央政治局集体学习区块链技术发展现状和趋势,习近平总书记强调,要把区块链作为核心技术自主创新的重要突破口,区

块链技术要在“促进数据共享、优化业务流程、降低运营成本、提升协同效率、建设可信体系”等方面发挥作用。区块链技术上升为国家重要战略,并将成

\* 收稿日期:2020-03-09

基金项目:国家重点研发计划项目(2017YFB1400700)

通讯作者:朱建明(1965-),男,教授,博士生导师,主要从事信息安全、区块链技术、金融科技的研究,(E-mail)zjm@cufe.edu.cn

引文格式:朱建明,张沁楠,高胜.区块链关键技术及其应用研究进展[J].太原理工大学学报,2020,51(3):321-330.

为推进社会治理现代化的重要技术。

区块链技术起源于 2008 年中本聪(Satoshi Nakamoto)发表的关于比特币的论文<sup>[1]</sup>。其中比特币系统底层的区块链技术解决了加密数字货币中的双重支付问题,在去中心化的 P2P 网络中,保证了交易记录的真实有效。经过几年的发展,区块链技术被认为是价值互联网的基石,通过分布式计算、密码学、共识算法、智能合约等多种技术的组合,保障在不通过第三方中介机构信用背书的条件下,实现数据的不可篡改、不易伪造、可追溯、可审计等特性,共同创造了一种低成本高可靠的基础设施。

近年来,在区块链技术的支持下,比特币等加密数字货币发展迅速,截至目前已有超过 5 361 种加密数字货币,其中比特币仍占主导地位<sup>[1]</sup>。在比特币区块链的基础上,2013 年 12 月,BUTERIN 发布了《以太坊白皮书》<sup>[2]</sup>,致力于提出一种通用加密货币。瑞波币(Ripple)<sup>[3]</sup>通过有限数量的可信节点构建 Ripple 网络,减小交易确认时间。EOS<sup>[4]</sup>采用并行链和委托权益证明实现高性能区块链。IOTA<sup>[5]</sup>和 Byteball<sup>[6]</sup>采用有向无环图(DAG)实现并行链式结构,不同类型的事务可以在区块链网络中并行运行,链式模型效率更高。2015 年,Linux 基金会发起了跨行业区块链开源项目——超级账本(Hyperledger)。袁勇和王飞跃<sup>[7]</sup>将区块链定义为去中心化的共享账本和分布式计算范式。区块链也被认为是在互不信任节点构成的网络中能够正确执行的计算机程序<sup>[8]</sup>。总体而言,区块链是一种具有普适性的底层分布式存储技术,被认为是新一代互联网技术,有望重塑社会生产的形态。

区块链因去中心化、难篡改、可追溯和分布式等特点,使其在金融科技、信息存证、能源共享、教育信息化等领域具有广阔的应用前景。2019 年 9 月,中国人民银行印发《金融科技(FinTech)发展规划(2019—2021 年)》和《金融分布式账本技术安全规范》,未来三年的区块链技术将在金融科技领域率先落地应用。面对各行业日益增长的区块链应用需求,需要构建更加高效、安全、合规、灵活的区块链解决方案。本文将从区块链关键技术与应用场景来介绍区块链技术与其应用的研究进展和面临的问题。

## 1 区块链技术概述

区块链是一种由多方共同维护,使用密码学保证传输和访问安全,能够实现数据一致存储、难以篡改、防止抵赖的记账技术,也称为分布式账本技术。

区块链技术通过将区块数据形成链式存储结构,形成去中心化的信任基础,成为众多加密数字货币的核心底层技术。区块数据结构代表一定时期内发生的交易和状态,是经过共识后形成的交易数据;按时间序列将区块数据结构串联形成链式存储结构。比特币区块链中,矿工负责将一段时间接收到的交易数据打包,并计算满足条件的随机数值,形成共识后的区块结构后追加在当前区块链的结尾,可以避免交易数据的篡改。

现有区块链可以分为三种类型,即公有链、联盟链和私有链<sup>[9]</sup>,联盟链和私有链也被称为许可链,需要提前设定节点的准入规则。目前随着区块链技术的商业化,区块链技术已经从公链形式向联盟链方向发展,私有链也有广泛的应用场景。公有链中节点的加入没有限制,而联盟链中的节点需要经过多组织协商授权才能加入。Hyperledger Fabric 是典型的联盟链项目,具有很强的实用性和可扩展性。私有链参与节点的权限被严格限制,权限由单个组织或企业控制,类似于现有的分布式存储系统,例如摩根大通的 Quorum 项目<sup>[10]</sup>。目前,联盟链被普遍认为是最具应用前景的区块链类型。

如图 1 所示,区块链已经经历了几个阶段的技术演进历程<sup>[7]</sup>,区块链技术起源于电子货币、密码学领域,经历了以数字货币为代表的 1.0 时代,和以智能合约为代表的 2.0 时代,目前正在进入超越货币、并与各行业深度融合的 3.0 时代。区块链技术正在与大数据、人工智能等新兴技术深度融合,未来会出现更加复杂的异构森林结构、神经网络共识、链内链外算力共享等新型区块链技术,形成有效支持大规模产业级复杂应用的区块链 4.0 时代。当前,区块

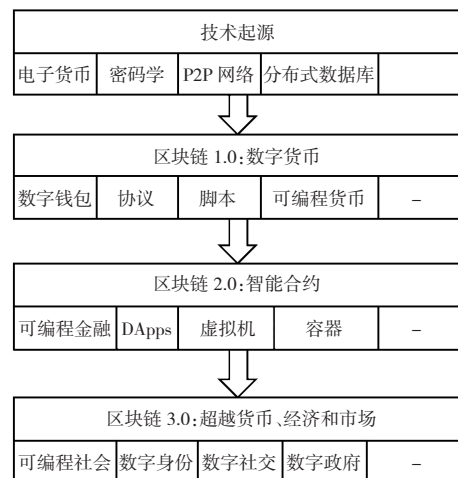


图 1 区块链技术演进历程

Fig. 1 Evolution of blockchain technology

链发展处在大发展、大融合的阶段,除区块链基础技术的研究外,工业界出现了区块链服务提供商的竞争,众多企业级的 PaaS 区块链云平台出现,单一区块链服务正在向区块链服务集成化快速演进。另外,区块链技术的不断演进和发展,进一步提升了性能和可扩展性,拓宽了应用领域和场景,为各行业带来深刻技术变革。

## 2 关键技术

### 2.1 密码学与分布式账本

区块链由密码学极客创建,密码学构成了区块链的基石。分布式账本技术是区块链区别于其他分布式数据存储的本质,各节点形成的分布式账本记录构建了区块链的骨架。传统有中心的分布式数据库系统设计了严格的用户权限管理和存取控制,而区块链的分布式账本数据则完全公开透明,链上节点可以随意读取查询数据,因此密码学极客采用 HASH 算法、数字签名、数字证书等密码学技术保障区块链交易数据的安全性和匿名性。

在比特币中,椭圆曲线加密算法(elliptic curve cryptography, ECC)用于生成私钥对应的公钥,公钥作为用户的钱包地址,可以区分不同的用户 ID,每个用户拥有多个公钥地址以实现交易的匿名性。为了保障交易的安全授权,比特币系统将每笔交易数据进行数字签名,比特币和以太坊都采用椭圆曲线签名算法(ECDSA),通过 secp256k1 的参数确定椭圆形状,实现非对称的高效签名算法。在比特币中,当一笔交易开始时,用户的公钥地址通过 SHA256 进行双 HASH 运算之后作为账户地址。验证交易数据时,使用用户公钥验签,实现交易的不可抵赖。公钥还可以用于验证 HASH 值是否与前一笔交易输出脚本的比特币地址一致,以实现每笔比特币的来源追踪。所有交易的完成都基于比特币系统中的输入脚本和输出脚本自动完成。

参与区块链的所有节点共同维护同一份区块链式数据,即分布式账本。不同于传统的账本技术,分布式账本具有去中心化、不可篡改、可编程等特点,在数字货币、电子存证、供应链中应用广泛。在比特币中,所有矿工在开始挖矿之前先同步账本数据,每一笔交易生成之后进行交易数据的转发,节点将接收到的交易数据存入特定存储区,大约每收集 10 笔交易打包成一个区块数据包,开始挖矿计算,挖矿过程中需要监控已经打包的交易是否已经被其他矿工挖矿成功,如有,则替换该笔交易继续挖矿。如果完

成指定条件的 HASH 运算,则挖矿成功,转发结果进行节点共识,共识成功后将打包好的区块数据追加在当前区块链的结尾,所有节点开始更新账本数据。

由分布式账本引起的性能和可扩展性问题是当前区块链技术的主要瓶颈。比特币中,每笔交易需要 6 个区块确认,系统最大的交易处理能力仅为 7 笔/s<sup>[11]</sup>,当前世界主流支付工具 VISA,交易处理能力为 2 000 笔/s,峰值的交易处理能力达 56 000 笔/s,且每笔交易秒级确认<sup>[12]</sup>。与现有商业系统巨大的性能差异极大地限制了区块链广泛的商业应用。高政风等(2019)提出采用有向无环图(DAG)的分布式账本可以提升区块链的并发性,有望解决区块链分布式账本的性能问题<sup>[13]</sup>。

### 2.2 共识机制

共识机制是区块链的核心,能保证在无中心控制下,各节点遵循相同的记账规则,实现分布式数据的一致性。区块链共识机制保证在不同的应用场景下,在决策权高度分散的去中心或多中心化系统中,使各个节点高效地达成一致。最早的共识问题是 EISENBERG E 和 GALE D<sup>[14]</sup> 提出的共识概率分布问题,其核心问题是容错节点的比例和收敛速度。区块链网络共识机制的研究目标是如何在节点可用性和一致性之间达成平衡,实现高效率认证。

共识机制主要解决两个基本问题:第一个是谁写入数据,另一个是如何同步数据。区块链中,每个节点都独立维护同一份数据,为了避免数据混乱,必须设计公平的选举机制和合理的激励机制。当被选举的节点写入数据后,其他节点必须准确及时同步数据,并验证写入数据的合法性,避免数据的伪造及非法写入。不同的共识算法的选举机制不同,在区块链的一次共识过程中,被选举的节点先打包交易构造区块链中最小的数据存储结构“区块”,并广播区块数据。其次,全网所有节点根据共识机制对接收到的区块数据进行合法性验证,如果是合法的区块数据,则将其追加在当前区块链的尾端,完成一次数据更新。

共识机制是区块链的关键技术,直接影响区块链系统的性能效率、可扩展性、资源消耗。目前,研究者已经在共识领域完成大量工作,从如何选举记账节点角度来看,现有的共识算法可以分为证明类、选举类、随机类、联盟链和混合类 5 种类型。下面分别介绍最常见共识算法类型和相关的研究进展情况。



### 2.2.1 证明类共识

证明类共识需要在每轮共识中有节点证明自己满足特定条件,通常表示为“Proof of X”,最常见的证明类共识有 PoW、PoS 和 DPoS。PoW 依赖算力消耗达成共识,PoS 通过币龄分配记账权的概率,DPoS<sup>[15]</sup> (delegated proof of stake)通过股份权益选举记账节点达成共识。PoA<sup>[16]</sup> (proof of activity)是 PoW 和 PoS 相结合的算法。

1993 年,DWORK C 和 NAOR M<sup>[17]</sup> 首次提出了工作量证明思想,用于提高垃圾邮件发送者的成本,其核心是通过消耗节点算力,保证共识过程的公平性。1999 年,JAKOBSSON M 和 JUELS A<sup>[18]</sup> 正式提出了工作量证明(proof of work,PoW),成为比特币中工作量证明算法的基础。PoW 可以应对拒绝服务攻击和服务滥用,通常需要掌握全网算力的 51% 以上才能对比特币系统进行安全攻击。但 PoW 存在因算力消耗引起的资源浪费,并且 10 min 左右的交易确认时间无法满足高效的业务需求。比特币采用的是依赖节点算力的 PoW 共识机制来保证分布式记账的一致性和共识的安全性。

随着区块链技术的不断进展,研究者陆续提出了一些不过度依赖算力而能达到全网一致的算法,比如权益证明共识(proof of stake,PoS)。SUNNY et al<sup>[19]</sup> 在点点币中首次实现权益证明 PoS 的共识机制,通过节点权益对比确定记账权。PoS 共识不需要算力消耗,可以提升共识效率,缩短共识时间。以太坊正逐步使用 PoS 替代 PoW,但是 PoS 权益证明容易产生马太效应,存在不完全公平性问题。

为了改进 PoW 存在算力浪费的问题,现有一些证明类共识算法基于特定的可信执行环境,例如共识节点采用安装 Intel SGX 安全硬件的 CPU 执行共识算法。在超级账本的 Sawtooth 项目中采用的消逝时间证明算法<sup>[20]</sup> (proof of elapsed time, PoET)通过每个节点的 SGX 计算生成区块和等待的时间证明,并被其他节点的 SGX 计算验证,保证了预言机的安全性,从而形成基于硬件安全的共识过程。

### 2.2.2 选举类共识

选举类共识中,参与共识节点在每一轮共识过程中通过投票选举方式选出当前记账节点,典型的选举类共识包括 PBFT、Paxos 和 Raft 等。PBFT 共识机制效率高,支持秒级出块,而且支持强监管节点参与,具备权限分级能力,在安全性、一致性、可用性等方面有较强优势。然而,在 PBFT 系统,无法

容忍超过三分之一以上的节点作恶。

1982 年,LAMPORT L et al<sup>[21]</sup> 基于分布式计算领域的共识问题首次提出了拜占庭将军问题,通过签名消息解决由于硬件、网络等问题引起的分布式节点故障。1999 年,图灵奖获得者 CASTRO M et al<sup>[22]</sup> 提出了实用拜占庭容错算法 (practical byzantine fault tolerance, PBFT),降低了拜占庭算法复杂度,提高了算法的实用性。PBFT 通常分为三个阶段共识:预备、准备和提交阶段。第一阶段选定主节点后,由主节点接受请求,并进行签名验证,验证通过后,对请求分配序号,并向全网广播;第二阶段共识节点收到请求后验证报文,并向全网广播验证结果;第三阶段,当收到超过三分之二节点的验证成功消息后,执行请求。PBFT 是首先得到广泛应用的 BFT 算法,随后,业界还提出了若干改进版的 BFT 共识算法。

文献<sup>[23]</sup>提出了一种可伸缩的故障容忍方法,系统可根据需要配置可容忍的故障数量,而不会显著降低性能。COWLING et al<sup>[24]</sup> 提出了一种混合拜占庭式容错状态机副本协议,在没有争用的情况下,采用轻量级的基于仲裁的协议,节省了副本间二次通信的成本。KING S 和 NADAL S<sup>[25]</sup> 提出了一种高吞吐量的拜占庭式容错架构,它使用特定应用程序的信息来识别和同时执行独立的请求。该体系结构提供一种通用的方法来利用应用程序间的并行性,在提高吞吐量的同时,还不损害系统工作的正确性。随后又提出了一种使用推测来降低成本并简化拜占庭容错状态机副本的协议<sup>[26]</sup>。ONGARO D et al<sup>[27]</sup> 在 2013 年基于 PBFT 进行简化,提出了 Raft 共识算法,目前已在多个开源语言实现。Raft 算法虽然不支持拜占庭容错,只支持节点宕机等故障性容错,但可以提高共识过程的性能与可扩展性。

## 2.3 智能合约

1994 年美国科学家尼克·萨博<sup>[28]</sup> (Nick Szabo)首次提出智能合约的概念,将智能合约定义为合同条款的计算机程序实现,在不需要可信第三方情况下,能够确保合同的正确履行。智能合约提出之后沉寂了很久,因为无法找到一个不存在可信第三方保证合约执行的环境,随着区块链技术的发展,其去中心化的可信平台为智能合约提供了天然的分布式可信执行环境,实现了区块链技术应用场景的拓展。

### 2.3.1 比特币脚本语言

比特币中没有智能合约的概念,只是采用一种

类似 Forth 的脚本语言实现简单的交易控制。该脚本语言有大小限制,不支持图灵完备,只能支持有限的逻辑,通常只作为账户拥有者的身份识别。

比特币基于未花费交易输出(UTXO)模式,每笔交易都可以追溯,直到最初的矿工挖矿。比特币交易的执行主要依赖于两种脚本:一种是锁定脚本,一种是解锁脚本。锁定脚本控制交易输出条件,解锁脚本验证输出条件是否满足,并控制未花费交易输出。

比特币的内置脚本是以太坊智能合约的雏形,因脚本不支持图灵完备,存在诸多限制,无法完成复杂的计算逻辑,但简单的脚本语言也保证了系统的轻量级并提升了系统的灵活性。目前,很多研究者也已经致力于基于比特币脚本进行叠加,以满足在比特币区块链上构建更为复杂的智能合约需求。

### 2.3.2 以太坊智能合约

以太坊(Ethereum)提供了图灵完备性的智能合约,使以太坊区块链拥有更广泛的应用场景。以太坊为智能合约的执行专门构建了以太坊虚拟机(EVM),方便了智能合约的编译运行。以太坊智能合约开发语言主要是 Solidity,可以支持编写逻辑代码。以太坊智能合约还提供了专门的浏览器开发平台 Remix,无需环境配置即可运行智能合约代码。

智能合约的安全性一直是人们关心的问题,而由智能合约的漏洞暴露出来的安全性事件也不断出现。例如 2017 年 6 月的以太坊平台的众筹智能合约 The DAO 遭受安全攻击的事件。The DAO 是搭建在以太坊网络上的智能合约,黑客利用递归函数的漏洞将面向公众筹集的 350 万个以太坊代币转向自己的地址,造成了巨大的经济损失。目前有多家公司从事与智能合约的安全性验证工作,如链安、慢雾等。

### 2.3.3 Fabric 链码

Hyperledger Fabric 采用高级编程语言 Go 或 Java 编写智能合约,被认为是执行在区块链上的代码,也被称为链码(Chaincode)。Fabric 基于 docker 容器运行链码可以提升宿主机隔离性和安全性。链码采用 Go 或 Java 语言编写,可以实现各种复杂的商业逻辑,功能强大。在比特币或以太坊上运行的智能合约可以看作是某个合约模板的多个实例,但是在 Fabric 中没有合约的实例,所有对区块链上数据的读写都必须经过链码来执行。

Fabric 链码基于高级语言开发,支持图灵完备,降低了开发者的学习门槛,并提升了智能合约的实

用性。但是目前对智能合约的定义和实现仍不统一,各区块链平台的智能合约开发语言也有很大差别,使得公众对智能合约认识有一些误差,没有统一的标准,不利于智能合约技术的长期发展<sup>[29]</sup>。

表 1 现有区块链平台智能合约对比  
Table 1 Comparison of smart contracts in existing blockchain platform

| 平台     | 执行环境    | 开发语言     | 共识算法        |
|--------|---------|----------|-------------|
| 比特币    | —       | 脚本       | PoW         |
| 以太坊    | EVM     | Solidity | PoW, PoS    |
| Fabric | Dockers | Go, Java | PBFT, Kafka |

## 2.4 区块链的扩展性

可扩展性<sup>[30]</sup>是指区块链系统处理交易以及适应交易增长而扩展的能力。区块链中,每个节点都要处理系统中的所有交易,随着交易数量快速增长,区块链的可扩展性问题日益凸显。以比特币和以太坊为例,比特币区块链平均每 10 min 产生一个区块,每个区块大小上限为 1 MB,每笔交易大小为 0.25 kB,因此交易频率为 6.67 笔/s;为抵抗双花攻击,完成一笔交易至少需要 6 个区块确认,全网确认一笔交易至少需要 1 h。与比特币区块链不同,以太坊的区块 gas 限制值决定区块容量,进而影响以太坊区块链交易性能。以太坊区块链产生一个区块需要 10~20 s,为抵抗“双花”攻击,达到与比特币区块链相似的安全性,完成一笔交易至少需要 12 个区块的确定,全网确认一笔交易至少需要 3 min。然而,以 Visa, Mastercard 等为代表的中心化支付平台可实现 2 000 笔/s~56 000 笔/s<sup>[12]</sup>。可见,现有区块链可扩展性已成为阻碍区块链规模化应用的重要障碍。

为解决区块链的扩展性问题,提出了高效共识算法、分片技术、链上扩容、链下扩容等可扩展性方法。

### 2.4.1 分片技术

2015 年,LUU L et al<sup>[31]</sup>将分片技术引入区块链领域,将节点划分成若干相对独立的分片,每个分片独立并行处理规模较小的片内交易,最后将分片摘要汇总给主链并由其生成新区块。根据处理层次不同,区块链分片技术可分为:网络分片、交易分片、状态分片。网络分片是指根据一定规则选取网络节点形成分片,是分片技术的基础;交易分片是指根据区块链数据模型按照一定规则将交易分配到不同分片,如基于账户模型可根据账户地址分片交易,典型技术如以太坊分片技术<sup>[35]</sup>, ZILLIQA<sup>[32]</sup>等;状态分片是指特定的分片只存储部分状态,而不是完整的区块链状态,典型技术如 OMNILEDGER<sup>[33]</sup>, RAP-

ID<sup>[34]</sup>等。

2018年,VITALIK<sup>[35]</sup>提出了一种基于双层设计的以太坊分片方案。以太坊区块链分为主链和分片链,主链通过验证管理合约(validator manager contract,VMC)来管理分片链,分片链采用PoS共识机制打包交易数据生成验证块,通过这些验证块最终生成主链上的区块。每笔交易都独立运行在其中一个分片,验证节点只校验所在分片的交易。为保证验证选择过程是强抗预测性,VMC采用随机抽样方式将验证节点分配到分片链上,同时校验所有分片提交的验证块头,并将校验通过的验证块头哈希记录到链上。此外,VMC采用UTXO模型和收据树实现跨片通信。

#### 2.4.2 链上扩容

链上扩容是通过改变区块链底层结构,使得单位时间内每个区块能容纳更多数量的交易,从而提高区块链吞吐量,例如增加区块容量、缩短出块时间等。

比特币改进提案(BIP)中有关扩容方案大致分为:根据比特币社区共识调整,如BIP-105;根据先前区块大小调整,如BIP-104、BIP-106、BIP-107中第二阶段;根据时间调整,如BIP-102、BIP-103、BIP-107中第一阶段。然而,区块大小的增加将延长网络传输效率,造成网络拥塞,同时加重存储设备负载,导致普通节点或小矿池退出,降低全节点运行比例,加剧区块链算力中心化风险;缩短出块时间将增加区块链分叉概率,造成有效算力分散,加剧双重支付<sup>[36]</sup>、自私挖矿<sup>[37]</sup>等风险。

2017年8月,BCH在比特币区块高度478558执行硬分叉,删除了隔离见证,将区块扩容到8M,期望通过该链上扩容解决比特币系统中区块拥堵和手续费高等问题。在此之后,BCH通过硬分叉的方式进行了4次升级。

#### 2.4.3 链下扩容

链下扩容是将交易过程放在链下完成,链上只记录最终交易结果或仲裁分歧交易。现有主要的链下交易方法有:隔离见证、状态通道、侧链等<sup>[38]</sup>。隔离见证通过将签名数据放到见证数据结构中,使得区块可以容纳更多数量的交易,提高了交易的延展性<sup>[39]</sup>。状态通道是通过在链下形成支付通道实现将大量交易带离链上,而区块链仅作为记录交易或处理支付过程中冲突或争议问题,从而极大提高区块链系统吞吐量。

侧链/中继(sidechains/relays)以轻客户端验证

技术为基础,在侧链上执行轻客户端功能的智能合约,通过验证链加密哈希树和区块头验证交易。Blockstream公司提出了楔入式侧链<sup>[40]</sup>概念,实现不同区块链系统间的资产转移,并进行多种跨链技术创新研究,提出了强联邦侧链<sup>[41]</sup>概念,引入多重签名,提升资产交换的安全性。ONELEDGER<sup>[42]</sup>是侧链应用的代表,通过侧链接入企业区块链,实现与企业级区块链系统的通讯。

### 3 区块链技术应用

区块链技术创建了去中心化的信任实体,具有分布式、去中心、难篡改、可编程、时序性和集体维护等特性,使区块链不仅能够应用于加密数字货币领域,同时在数字金融、电子存证、能源共享、电子医疗、农产品追溯方面也有广泛应用场景。

#### 3.1 数字金融

区块链技术最早应用起源于加密数字货币,其目的是解决数字货币的支付问题。区块链去中心化的特性对依赖第三方机构的电子支付和资金托管等领域有颠覆性变革。传统的金融交易需要经过中央结算机构,银行证券及交易所等多家中心机构的协调工作,利用区块链技术可以降低交易成本,简化金融业务流程。

区块链技术在数字货币中已有广泛应用,现有的大多私人数字货币都基于区块链底层技术。Facebook基于联盟链打造了服务数十亿用户的数字货币Libra,并实现了Move智能合约语言,共识机制采用了康奈尔大学提出的BFT改进算法,并将其命名为LibraBFT,实现了高性能的共识机制。为应对世界数字货币的挑战,人民银行从2014年开始研究法定数字货币,目前处于研究测试过程中。

在跨境支付场景中,Ripple Lab基于区块链创建了Ripple数字竞争币以降低跨境支付的成本。初创企业Circle公司推出跨界支付应用,并发布白皮书<sup>[43]</sup>,利用比特币充当跨币种交易的中介货币,提升跨境支付的效率,降低交易成本。现有的SWIFT系统交易成本高,速度慢,基于区块链的加密货币可以实现方便的跨境支付,比SWIFT系统更加安全便利<sup>[44]</sup>。

在供应链金融场景中,区块链技术从效率、成本、信任三个维度解决了企业融资过程中的痛点。区块链为供应链各参与方提供了平等协作的平台,大大降低机构间信用写作风险和成本。实现数据的实时同步和对账,防止数据的篡改和伪造。



### 3.2 电子存证

区块链数据的不可篡改,时间戳记录可以永久保存各类证明文件,并对证明文件的记录进行时间序列存证,实现去中心化的验证。目前区块链技术已经应用于知识产权保护、校园信息存证、互联网法院存证等领域。

区块链电子存证在教育领域应用前景突出。例如伦敦大学建立了基于区块链的学历认证平台 Gradbase 用于存储毕业生的学历信息,企业单位可以通过扫描平台形成的二维码,验证求职者的学历信息。

在电子资源产权保护方面,区块链+数字证书是存储、验证、共享资源权限的理想方案。电子资源的发布者、接受者、所有者、发布时间可以存储在区块链系统中,每次资源使用记录的增加都经过区块链节点的共识,从而保护电子资源所有者的产权。

### 3.3 区块链服务平台

未来的区块链的发展趋势是有效支持大规模产业级复杂应用。当前,以“区块链即服务”理念为基础的区块链服务平台已具有提供规模化区块链应用的雏形。

区块链服务平台旨在为用户提供集成化、可定制的区块链服务。在此之前,区块链服务是单一化、割裂化的,用户难以自定义区块链配置。区块链服务平台是基于主流区块链技术构建企业级 PaaS (platform as a service) 平台服务,可以帮助使用者快速构建安全稳定的生产级区块链环境,减少在区块链部署、运维、管理、应用开发的工作量,提供业务创新的便利。当前常见的区块链服务平台有腾讯 TrustSQL、百度 Xuper 链、阿里云区块链 BaaS 平台等。

### 3.4 区块链+教育

2016年,工信部发表《中国区块链技术和应用发展白皮书》,其中提到区块链技术在教育过程中涉及的档案管理、学生征信、学历证明、成绩证明、产学研合作中可发挥作用。

2018年,伦敦大学学院(University College London)宣布其区块链技术中心将开展一项试点项目,该项目的目的是让金融风险专业的学生能够通过区块链技术验证简历中学历信息的真伪。2018年,基于区块链的去中心化全球教育服务平台 EduCoin 面世。该平台通过区块链的分布式特征为多个教育节点建立连接,以执行与教育相关的服务或共享内容。EduCoin 平台拥有自身的加密货币

EDU,区块链节点之间可以通过 EDU 交换教育资源。在 EduCoin 平台上,资源提供者可以确定共享的教学内容的价格,而消费者可根据资源所提供的价格信息支付 EDU 以获得资源,其过程中无第三方机构参与而是通过智能合约保证交易的真实和可信。

因此,区块链技术不仅可以为教育数据共享与隐私保护问题、教学资源的知识产权保护与交易提供帮助,还可以为构建新的教学模式提供支持。区块链技术与人工智能、大数据、云计算结合将为教育信息化发展发挥更大的作用。

### 3.5 其他应用

区块链采用去中心化的分布式记账技术,为解决数据共享管理提供了新的思路。现有的数据共享存在权限不清晰、不方便管理等问题,数据的所有者并不能完全掌握数据的所有权。目前区块链可以用于解决不可信环境下的数据管理问题。

作为分布式账本技术的代表,区块链可用于智能供应链管理,实现货物流转、产品登记等信息的可追溯化管理,增强信息的透明度,提升整个供应链处理效率。区块链上数据保存在分布式的节点中,任何节点都不能随意操控数据,IBM 已推出了一项使用区块链技术改善供应链的案例,将其命名为“信任你的供应商”。

区块链交易的匿名性可以保障交易用户的隐私。在电子健康领域,SWAN<sup>[45]</sup>认为区块链可以保护个人健康数据的隐私性。LAZAROVICH<sup>[46]</sup>以医疗数据隐私保护为例阐述区块链在个人隐私保护方面的应用。ROEHRS et al<sup>[47]</sup>提出的 OmniPHR 系统利用区块链实现个人电子医疗健康数据保存和访问,确保数据的安全和防篡改。MEDSHARE<sup>[48]</sup>系统解决无信任环境下医疗数据安全共享问题,为电子医疗数据溯源审计提供了解决方案。

在能源共享领域,区块链的去中心化与分布式能源供给有较强的耦合性,使用区块链实现能源共享有助于实现智能充电桩之间的信息共享,降低能源交易成本。KANG et al<sup>[49]</sup>提出了一种点对点电力交易系统,构建了安全交易的联盟链系统,实现双重拍卖机制,实现了去中心化的电力交易。国内外已有基于区块链的微电网项目落地,增强了用电稳定性,降低了区域间用电的依赖性。

区块链在物联网领域也有广泛应用,包括在车联网领域中利用区块链保护用户隐私,利用区块链实现车联网中的联邦学习的安全数据共享<sup>[50]</sup>。

## 4 区块链技术与应用面临的挑战

区块链技术正处于快速发展过程中,还面临许多挑战。概况起来,主要表现在以下三个方面:

第一,区块链技术自身面临的挑战。

区块链融合了密码学、计算机科学、经济学、社会学等学科知识,是一种在不可信环境中构建信任的新型协作模式和计算范式。然而,其发展还处于非常早期的阶段,技术本身所存在的问题仍待进一步突破。

1) 可扩展性问题:区块容量、节点规模、共识效率、通信时延等因素使得单位时间确认交易数量受限,成为区块链可扩展性提升的主要瓶颈。高性能、高可扩展等技术瓶颈阻碍了区块链大规模商业落地应用。

2) 互操作性问题:当前,区块链技术平台呈现“百链竞发”态势,相较于信息互联网实现的泛在信息交互需求,不同技术底层的区块链之间缺乏统一的互联互通的机制,难以满足价值自由流转需求,极大阻碍了区块链应用生态形成。

3) 安全性问题:区块链安全研究分散在密码安全、网络安全、共识安全、智能合约安全、应用安全等不同维度,木桶原理表明区块链系统的安全性取决于最薄弱维度的安全性,单一维度的安全难以保障整个区块链系统安全,构建纵深防御的一体化的安全架构已成为区块链安全亟待突破的关键问题。

4) 隐私保护问题:区块链隐私大都采用密码学保护不同交易主体的身份隐私和不同交易的内容隐私等,距离大规模实用化有一定距离。此外,难以在保障区块链隐私条件下,实现准确高效监管。实用化、条件化隐私保护方法仍待进一步突破。

5) 可监管性问题:当前,大多采用被动监管方式,即由金融机构定期向监管机构报备,存在时效性差、数据易被篡改等问题。因此,如何利用区块链技术构建透明、动态、高效、精准、可视化的监管体系有待完善。

第二,区块链技术与人工智能、大数据等技术相结合面临的挑战。

目前,从技术成熟度来讲,大数据、云计算等技术趋于成熟,人工智能、物联网技术应用范围和领域不断扩大,而区块链受限于技术发展及投入产出比等缘由,仍处于发展的初级阶段。随着区块链技术的完善,人工智能、大数据等技术也会随之融合,出现新的技术局面,对于区块链产业来讲,将来想象空

间会很大。区块链与人工智能、大数据相结合具备颠覆传统行业的可能,使得相关业务公开化、透明化、公正化。但是,区块链技术如何与人工智能、大数据相结合还面临许多挑战。

第三,区块链技术应用面临的挑战。

目前,区块链的价值已经得到全社会的肯定和重视。截至目前,全国已有22个省(自治区、直辖市)将区块链写入2020年政府工作报告。大多数地方政府将区块链视作当地产业优化升级的技术助力、数字经济产业的新增长点,并对当地区块链发展提出了更为具体细化的目标。

区块链技术的应用始于数字货币和金融领域,区块链作为数字经济的重要组成部分,正在向其他应用领域迅速扩展,成为加快传统实体产业和现代服务业高质量发展的重要技术。区块链技术应用面临的挑战主要有:

1) 区块链与已有应用相结合面临的挑战。区块链技术作为底层技术,如何与应用领域的现有系统相结合是一个需要研究的问题。以电子政务为例,是以区块链为基础设计新的电子政务应用,还是在原来系统的基础上进行改造,目前还没有形成好的应用模式。

2) 区块链应用带来管理模式与制度的变化。区块链技术的主要特点之一是去中心化,通过共识机制自动达成共识。这与目前中心化的管理体系存在一定的矛盾。

3) 区块链应用创新的难度大。截至目前,最成功的区块链应用就是数字货币。除此之外,其他应用还没有形成与数字货币类似的影响,区块链应用创新任重道远。

## 5 结束语

区块链作为新一代互联网技术已经引起产学界的广泛关注,区块链技术在数据共享、协同工作、业务流程优化、可信体系建设等方面具备特有的优势。随着区块链技术的普及,区块链技术将广泛应用于当前数字经济时代的各类应用中,成为一种分布式可信数据存储的基础设施,通过其去中心化的信任基础重塑新的社会形态。

本文通过对区块链相关核心技术和应用领域研究进展的详细阐述,梳理了当前区块链核心技术的现有研究成果及挑战,并分析了区块链应用项目的落地瓶颈。现有制约区块链系统发展的技术挑战主要包括分布式账本的可扩展性、共识算法性能、尚未



标准化的智能合约、链上数据扩容、数据源安全性及链上数据隐私等。区块链应用落地的瓶颈主要在于交易延时与大规模请求的执行效率。虽然当前的区块链技术还存在很多性能和应用的挑战,但不可否认区块链技术正在促进各领域的技术创新。大多区块链技术仍需要进一步的研究和探索才能产生变革影响,国内外学者已经开展了多项区块链技术的探索和应用实践,需要更多的科研人员加入到区块链技术及应用的研究工作中,实现区块链核心技术瓶颈的突破。

当前,区块链技术的去中心化可信体系已经引

起了各行业的广泛关注。整个区块链行业正处于快速变化和演进过程中,未来的区块链行业将构建一个完善的生态系统,为人类生活创造新的可能。未来区块链生态系统的发展趋势包括:混合跨链交易和异构区块链实现高性能交易、非链式区块数据模型实现区块数据并行存储、混合网络协议提升共识通信效率、成立世界范围的可信区块链联盟组织等。区块链作为一种平等互信的互联网技术,需要有更优的互联网底层协议,进一步提升系统性能、优化共识算法、改进体系架构,探索更广阔的应用场景。

### 参考文献:

- [1] NAKAMOTO S. BITCOIN. A peer-to-peer electronic cash system[EB/OL]. [2008]. <https://coinmarketcap.com/>
- [2] BUTERIN V. A next-generation smart contract and decentralized application platform[EB/OL]. <https://github.com/ethereum/wiki/wiki/White-Paper>.
- [3] SCHWARTZ D, YOUNGS N, BRITTO A. The Ripple protocol consensus algorithm[EB/OL]. [https://ripple.com/files/ripple\\_consensus\\_whitepaper.pdf](https://ripple.com/files/ripple_consensus_whitepaper.pdf).
- [4] LARIMER D. EOS. IO technical white paper[EB/OL]. <https://github.com/EOSIO/Documentation/blob/master/Technical-WhitePaper.md>.
- [5] Popov S. The tangle[EB/OL]. [https://iotatoken.com/IOTA\\_Whitepaper.pdf](https://iotatoken.com/IOTA_Whitepaper.pdf).
- [6] CHURYUMOV A. Byteball: A decentralized system for storage and transfer of value[EB/OL]. <https://byteball.org/Byteball.pdf>.
- [7] 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. Current situation and prospect of blockchain technology development[J]. Journal of Automation, 2016, 42(4): 481-494.
- [8] ATZEI N, BARTOLETTI M, CIMOLI T. A survey of attacks on ethereum smart contracts soK[C]//MAFFEIM, RYAN M. Proc of the 6th Intl Conference on Principles of Security and Trust. New York: Springer-Verlag, 2017: 164-186.
- [9] BUTERIN V. On public and private blockchains[EB/OL]. [2015-08-07]. <https://blog.ethereum.org/on-public-and-private-blockchains>.
- [10] JPMORGAN CHASE & CO. Quorum whitepaper[EB/OL]. <https://github.com/jpmorganchase/quorum-docs/blob/master/Quorum%20White%20paper%20v0.2.pdf>.
- [11] GERVAIS A, KARAME G O, WÜS T K, et al. On the security and performance of proof of work blockchains[C]//ACM. Proceedings of the 2016 ACM SIGSAC conference on computer and communications security, 2016.
- [12] How a Visa transaction works (2015)[Online]. [2016-01]. <http://apps.usa.visa.com/merchants/become-a-merchant/how-a-visa-transaction-works.jsp>.
- [13] 高政风, 郑继来, 汤舒扬, 等. 基于 DAG 的分布式账本共识机制研究[J/OL]. 软件学报, [2020-03-10]. <https://doi.org/10.13328/j.cnki.jos.005982>.  
GAO Z F, ZHENG J L, TANG S Y, et al. Research on distributed ledger consensus mechanism based on DAG [J/OL]. Journal of software, [2020-03-10]. <https://doi.org/10.13328/j.cnki.jos.005982>.
- [14] EISENBERG E, GALE D. Consensus of subjective probabilities: the pari-mutuel method[J]. The Annals of Mathematical Statistics, 1959, 30(1): 165-168.
- [15] BITSHARES. Delegated proof of stake [EB/OL]. [2018-04-10]. <http://docs.bitshares.org/bitshares/dpos.html>.
- [16] BENTOV I, LEE C, MIZRAHI A, et al. Proof of activity: extending Bitcoin's proof of work via proof of stake[EB/OL]. [2018-04-10]. <http://eprint.iacr.org/2014/452>.
- [17] DWORK C, NAOR M. Pricing via processing or combatting junk mail[C]//Proceedings of the 12th Annual International Cryptology Conference on Advances in Cryptology. Santa Barbara, California, USA: Springer-Verlag, 1992: 139-147.
- [18] JAKOBSSON M, JUELS A. Proofs of work and bread pudding protocols (extended abstract)[M]. Boston, MA, Germany: Springer, 1999: 258-272.
- [19] KINGS, NADALS. PPCoin: Peer to Peer Crypto-Currency with Proof-of-Stake[EB/OL]. [2012]. <http://ppcoin.org/static/ppcoin-paper.pdf>.
- [20] BUNTINX J P. What is proof of elapsed time? [EB/OL]. [2018-04-10]. <https://themerke.com/what-is-proof-of-elapsed-time>.
- [21] LAMPORT L, SHOSTAK R, PEASE M C. The Byzantine generals problem[J]. ACM Trans on Programming Languages and Systems(TOPLAS), 1982, 4(3): 382-401.
- [22] CASTRO M, LISKOV B. Practical Byzantine fault tolerance[C]//Proceedings of the 3rd Symposium on Operating Systems Design and Implementation. New Orleans, USA: USENIX Association, 1999: 173-186.

- [23] ABD-EL-MALEKM, GANGER G R, GOODSON G R, et al. Fault-scalable byzantine fault-tolerant services[J]. ACM SIGOPS Operating Systems Review, 2005, 39(5): 59-74.
- [24] COWLING J, MYERS D, LISKOV B, et al. HQ replication: A hybrid quorum protocol for Byzantine fault tolerance[C]// Proc of the 7th Symp on Operating Systems Design and Implementation. USENIX Association, 2006: 177-190.
- [25] KOTLA R, DAHLIN M. High throughput Byzantine fault tolerance[C]// IEEE. Proc of the 2004 Int'l Conf on Dependable Systems and Networks. IEEE Computer Society, 2004: 575.
- [26] KOTLA R, ALVISI L, DAHLIN M, et al. Zyzzyva: Speculative byzantine fault tolerance[J]. ACM SIGOPS Operating Systems Review, 2007, 41(6): 45-58.
- [27] ONGARO D, OUSTERHOUT J. In search of an understandable consensus algorithm[C]// Proceedings of the USENIX Annual Technical Conference. Philadelphia, PA, USA: USENIX ATC, 2014: 305-319.
- [28] SZABO N. Smart Contracts[EB/OL]. [1994]. <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html>.
- [29] 王璞巍, 杨航天, 孟倍, 等. 面向合同的智能合约的形式化定义及参考实现[J]. 软件学报, 2019, 30(9): 2608-2619.  
WANG P W, YANG H T, MENG J, et al. Formal definition for classical smart contracts and a reference implementation[J]. Journal of Software, 2019, 30(9): 2608-2619.
- [30] CROMAN K, DECKER C, EYAL I, et al. On scaling decentralized blockchains[C]// Proc 3rd Workshop on Bitcoin and Blockchain Research, 2016.
- [31] LUU L, NARAYANAN V, ZHENG C, et al. A Secure sharding protocol for open blockchains[C]// ACM. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. Vienna, Austria: ACM, 2016: 17-30.
- [32] TEAM T Z. The ZILLIQA Technical Whitepaper[EB/OL]. <https://docs.zilliqa.com/-whitepaper.pdf>.
- [33] E K K P, J L G, et al. OmniLedger: A secure, scale-out, decentralized ledger via sharding[C]// IEEE. 2018 IEEE Symposium on Security and Privacy (SP), 2018: 583-598.
- [34] ZAMANI M, MOVAHEDI M, RAYKOVA M. RapidChain: scaling blockchain via Full Sharding[C]// ACM. Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. Toronto, Canada: ACM, 2018: 931-948.
- [35] VITALIK BUTERIN. On sharding blockchains[EB/OL]. <https://github.com/ethereum/sharding/blob/-develop/docs/doc.md>.
- [36] SOMPOLINSKY Y, ZOHAR A. Secure High-Rate Transaction Processing in Bitcoin[C]// International Conference on Financial Cryptography and Data Security. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015: 507-527.
- [37] SAPIRSHTEIN A, SOMPOLINSKY Y, ZOHAR A. Optimal Selfish Mining Strategies in Bitcoin[C]// International Conference on Financial Cryptography and Data Security, 2017.
- [38] 曾帅, 袁勇, 倪晓春, 等. 面向比特币的区块链扩容: 关键技术, 制约因素与衍生问题[J]. 自动化学报, 2019, 45(6): 1015-1030.  
ZENG S, YUAN Y, NI X C, et al. Scaling blockchain towards bitcoin: key technologies, constraints and related issues[J]. Acta Automatica Sinica, 2019, 45(6): 1015-1030.
- [39] ANDRYCHOWICZ M, DZIEMBOWSKI S, MALINOWSKI D, et al. On the Malleability of Bitcoin Transactions[C]// International Conference on Financial Cryptography and Data Security, 2015.
- [40] BACK A, CORALLO M, DASHJR L, et al. Enabling blockchain innovations with pegged sidechains[EB/OL]. <https://blockstream.com/sidechains.pdf>.
- [41] JOHNNY D, ANDREW P, JONATHAN W, et al. Strong federations: An interoperable blockchain solution to centralized third party risks[EB/OL]. <https://arxiv.org/pdf/1612.05491.pdf>.
- [42] ONELEDGER. A universal blockchain protocol enabling cross-ledger access through business modularization[EB/OL]. <https://oneledger.io/wp-content/uploads/2018/04/oneledger-whitepaper.pdf>.
- [43] CIRCLE CORPORATION. CENTRE. [EB/OL]. (2017-12-8)[2018-04-05]. <https://www.centre.io/>.
- [44] 朱建明, 丁庆洋, 高胜. 基于许可链的 SWIFT 系统分布式架构[J]. 软件学报, 2019, 30(6): 1594-1613.  
ZHU J M, DING Q Y, GAO S. Distributed framework of SWIFT system based permissioned blockchain[J]. Journal of Software, 2019, 30(6): 1594-1613.
- [45] SWAN M. Blockchain thinking: the brain as decentralized autonomous corporation[J]. IEEE Technology & Society Magazine, 2015, 34(4): 41-52.
- [46] LAZAROVICH A. Invisible ink: blockchain for data privacy[D]. Massachusetts: Massachusetts Institute of Technology, 2015: 36-40.
- [47] ROEHRS A, DA COSTA CA, DA ROSA RIGHI R. OmniPHR: a distributed architecture model to integrate personal health records[J]. J Biomed Inform, 2017, 71: 70-81.
- [48] XIA QI, SIFAH E B, ASAMOAH K O, et al. MeDShare: trust-less medical data sharing among cloud service providers via blockchain[J]. IEEE Access, 2017, 5(99): 14757-14767.
- [49] KANG JIAWEN, YU RONG, HUANG XUMIN, et al. Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains[J]. IEEE Transactions on Industrial Informatics, 2017, 13(6): 3154-3164.
- [50] LU Y L, HUANG X H, DAI Y Y, et al. Blockchain and federated learning for privacy-preserved data sharing in industrial IoT[J]. IEEE Transactions on Industrial Informatics, DOI 10.1109/TII.2019.2942190.

(编辑:贾丽红)