区块链关键技术及应用研究综述

章峰，史博轩，蒋文保
（北京信息科技大学信息管理学院，北京 100192）

摘　要：区块链技术的兴起是一个类似于互联网崛起的范式转换事件，引起广泛关注。区块链技术具有去中心化、不可篡改和追踪溯源等特性。通过分析近几年来国内外的区块链相关论文，解构区块链的核心技术原理，探讨应用区块链技术的场景，如金融服务、征信和权属管理、公共网络服务等领域，指出各应用领域仍存在的问题，对区块链技术的发展与应用提出一些见解，致力于为区块链技术与应用的相关研究提供帮助。

关键词：区块链；公式机制；智能合约；去中心化
中图分类号：TP319
文献标识码：A
doi: 10.11959/j.issn.2096-109x.2018028

Review of key technology and its application of blockchain

ZHANG Feng, SHI Boxuan, JIANG Wenbao
School of Information Management, Beijing Information Science & Technology University, Beijing 100192, China

Abstract: The rise of blockchain technology is a paradigm shift, which is similar to the rise of the Internet, and it has attracted wide attention. Blockchain has characteristics of decentralization, tamper-resistant, traceability and so on. The achievements of some papers about blockchain at home and abroad have been analysed in recent years, and the core technology principle of blockchain has been parsed. The application scenarios of blockchain were disscussed, such as financial services, credit management, tenure management, public network service and other fields. The existing problems in various application fields were pointed out. Some opinions on the development and application of blockchain were put forward, dedicated to blockchain and hoped to do contribution for the research about blockchain and its applications.

Key words: blockchain, consenus mechanism, smart contract, decentralization

1　引言

2008 年比特币开始出现，随后，区块链技术开始进入人们的视野之中，并引起了极大的关注。现在各国已经纷纷开始进行区块链的投资研发，区块链也渐渐进入区块链 3.0 时代。从狭义上讲，区块链是一种时序数据区块，相互连接组成一种链式结构，用密码学方式来确保分布式账本的不可篡改和不可伪造。从广义上讲，区块链技术是利用块链式数据结构验证与存储数据、利用分布式节点共识算法生成和更新数据、利用密码学的方式保证数据传输和访问的安全、利用由自动化脚本代码组成的智能合约编程和操作数据的一种全新分布式基础架构与计算范式。区块链技术具有去中心化、追踪溯源、不可篡改、可编程和集体维护等特性。本文主要总结近 2~3 年区块链技术发展研究的现状以及产生的问题，并从区块链的核心技术以及应用研究这 2 方面进行分析。

收稿日期：2018-02-14；修回日期：2018-03-20
通信作者：蒋文保，jiangwenbao@tsinghua.org.cn

2　区块链核心技术

现存的区块链应用大多与比特币的模型类似，仅在某些类似的特定环节中或多或少地采用比特币的变种模式。本文对区块链技术的基础架构模型归纳总结如图 1 所示，一般来说，区块链系统整体上由数据层、网络层、共识层、合约层和应用层这 5 个部分结构组成。

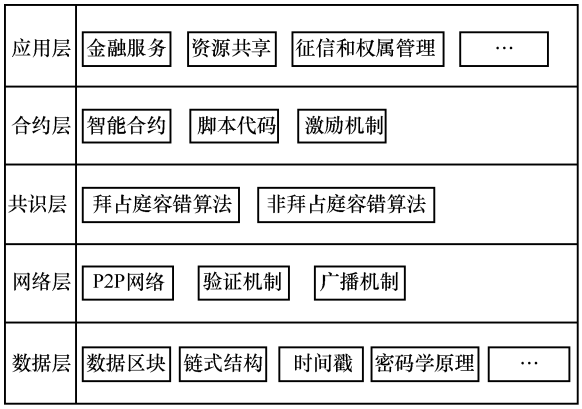

图 1　区块链基础架构模型

2.1　数据层

在区块链系统中，最底层的原始数据需要进一步加工才能存储到区块之中。底层数据最根本的是信息记录，其他的数据只是为了对信息记录进行封装。该过程涉及散列算法、Merkle 树和时间戳等技术。

最初，比特币采用的是 SHA-256 算法，SHA-256 算法是 2008 年公认的最安全、最先进的算法之一。但是因为显卡挖矿和矿池的出现，担心违背中本聪[1]最初的“一 CPU 一票”的设计理念，所以导致中心化的问题非常严重。之后，使用 SCRYPT 算法[2]的莱特币出现，SCRYPT 算法是由著名的 FreeBSD 黑客 Colin Percival 为他的备份服务 Tarsnap 开发的，当初的设计目的是降低 CPU 负荷，尽量少依赖 CPU 计算，利用 CPU 闲置时间进行计算。后来有人对 SCRYP 算法进行了改进，形成 Script-*N* 算法，其思路是一样的，为了追求更大的内存消耗和计算时间，组织 ASIC 专用矿机。之后，夸克币（Quark）首创使用多轮 Hash 算法，将多种 Hash 算法进行串联机码，只要一种算法被破解，整个算法就可以被破解。同样地，又有 Heavycoin（HVC）做了并联算法的尝试，实现了链上游戏，但在国内名不经传。

Ethash 算法[3]是以太坊采取的一个过渡算法，是 Dagger-Hashimoto 的一种改良算法。将 Hashimoto[4]结合 Dagger[5]产生的一个新变种，主要是用来抵御矿机性能以及实现轻客户端的快速验证。

素数币[6]（Primecoin）由 Sunny King 发明，其算法的核心理念是：做 Hash 运算的同时寻找大素数。通过 2 种方法进行测试，首先进行费马测试（Fermat test），通过后再进行欧拉–拉格朗日–立夫习兹测试（Euler-Lagrange-Lifchitz test），若仍然能通过测试就被视为素数。需要指出的是，这种方法并不能保证通过测试的每一个数都是素数，不过这并不影响系统运行，因为即便测试结果错误，只要每个节点都认为是素数就行。

最近在国内非常流行的是 Zcash，其采用的是 Equilhash 算法，由 Biryukov 和 Khovratovich[7]联合发明，其理论依据是一个著名的计算机科学及密码学问题——广义生日悖论问题。多数人认为，该算法在短时间内很难出现矿机。但是，Equilhash 算法只有抵御矿机性能的需求，并不确保 Equilhash 的安全性。

还有一些学者，如 Andrychowicz 等[8]受比特币启发，分别提出了在完全对等情况下，构建分布式加密协议。Bonneau 等[9]对时间戳以及随机数问题进行了研究，进一步地扩充了区块链加密算法的内容以及安全性。

2.2　网络层

网络层封装了区块链的组网模式、消息传播协议、数据验证机制等因素。在设定的消息传播协议与数据验证机制下，能够让区块链中的所有节点或者大部分节点参与区块数据的验证与记账过程，当大部分节点对区块数据校验成功后，区块数据才能记入区块中。

Apostolaki 等[10]研究了路由攻击 hijacking 对比特币的影响。结果是，比特币的潜在危害令人担忧，通过隔离部分网络或者延迟阻止传播，攻击者可以实现大量的采矿资源被浪费，并进行广泛的攻击破坏。Baqer 等[11]则对比特币做了基于垃圾邮件的“压力测试”DoS 攻击，指出比特币最低费用的变化会减少一些主题垃圾邮件的数

量。Miller 等[12]则提出了 HoneyBadgerBFT 的异步 BFT 协议，实现了数万个事物操作的吞吐量，每秒可以扩展到广域网上的 100 多个节点，良好地兼容底层网络，适合部署容错事务处理系统。

2.3 共识层

共识机制是为了保证分布式账本所有节点所存储信息的准确性与一致性而设计的一套机制，就像社会系统中“民主”和“集中”的对立关系，决策权越分散的系统达成共识的效率就越低，但是系统的满意度和稳定性会越高；反之，决策权越集中的系统越容易达成共识，但是整个系统的满意度和稳定性也就越低。共识机制的设计主要由业务与性能的需求决定，从 PoW（proof of work）到 PoS（proof of stake）再到 DPoS（delegated proof of stake）和 Paxos 以及各种拜占庭容错算法，共识机制不断创新，区块链平台性能也得到大幅提升。

在 PoS 中还有 TaPoS（基于交易的股权证明机制），该机制中的每笔交易都包括前一区块的散列值，但问题是没有定义谁来产生下一个区块。还有 Ripple 共识机制，该机制只尊重核心成员 51%的权力，外部人员没有影响力，导致其比其他的系统更加中心化。

在 DPoS[13]（授权股权证明机制）中，每个股东可以将其本身的投票权授予一名代表，获票数最多的前 100 位代表按既定时间表轮流产生区块。每一位代表分配一个时间段来产生区块。所有的代表将收到等同于一个平均水平的区块所含交易费的 10%作为报酬。

实用拜占庭容错[14]（PBFT, practical Byzantine fault tolerance）算法的突破性在于保证活性和安全性（liveness & safety）的前提下提供了 $\frac{n-1}{3}$ 的容错性。在分布式计算上，不同的计算机通过信息交换，达成共识；但有些时候，系统上的协调计算机（coordinator / commander）或成员计算机（member/lieutanent）可能因系统错误或交换错的信息，影响最终的系统一致性，也就是拜占庭问题。而在这个算法中拜占庭问题的可能解决方法为：在 $N \geqslant 3F+1$ 的情况下一致性是可能解决的。其中，N 为计算机总数，F 为故障计算机总数。但是该算法不如公有链上的共识机制的去中心化程模高。

Pool 验证池更加适用于私有链、联盟链。它是基于传统分布式一致性算法（如 Paxos[15]、Raft 等），再加上相关的数据验证机制，而形成的一套共识机制。但是去中心化程序不高，更加适合多中心模型。

还有一些自定义的共识机制，主要都是在现有的共识机制上，针对某些应用场景进行改进优化，如授权拜占庭容错（DBFT, delegated practical Byzantine fault tolerance）算法等。目前，并没有任何一种完美的共识机制，只有针对某种具体场景的局部最优解，若想获取全局最优解，仍然需要各位专家学者的研究。

2.4 合约层

合约层主要封装了区块链系统运行中需要的各类脚本代码、算法以及由此生成的更为复杂的智能合约。从本文以上对数据、网络和共识 3 个层次的介绍，可以看到这 3 层可作为区块链底层，分别承担数据表示、数据传播和数据验证的任务。合约层是建立在区块链底层之上的逻辑、算法或者规则策略，实现区块链系统灵活编程和操作数据等功能。

合约层的一个相关概念就是智能合约。智能合约是 20 世纪 90 年代由 Szabo[16]提出的理念。那个年代由于缺少可信的执行环境，智能合约并没有被应用到实际产业中，比特币诞生后，人们认识到比特币的底层技术区块链可以为智能合约提供可信的执行环境。一个成功的案例就是，以太坊看到了区块链和智能合约的契合点，发布以太币，打造以太坊平台。图 2 为智能合约的运行机制。

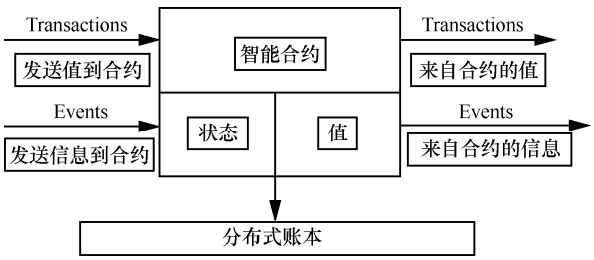

图 2 智能合约的运行机制

智能合约有很多种表现形式，如差价合约、代币系统、储蓄钱包、作物保险、多重签名智能

合约等都是以太坊中等的典型应用。

Mccorry 等[17]基于智能合约设计了一套在就 Ethereum 上运行的投票系统，经过测试，只需要满足最低限度的选举费用（0.73 美元/位）就可以正常使用。Luu 等[18]针对智能合约系统的安全性问题进行了深入研究，提出一套 Oyente 的工具来寻找潜在的安全漏洞，并指出以太坊现存的 19 366 种合约中有 8 833 项是脆弱的，这其中包括 TheDAO bug。其主要问题有：合同不退款、缺乏合适的密码学机制来实现公平性以及激励失准。

Kosba 等[19]提出的 Hawk，是一个分散的智能合约系统，可以自动生成一个高效的加密协议与区块链进行交互，从而保证交易的隐私性。但是，Hawk 要求可信的数据通过可信的 Web 服务器传输到可信硬件的智能合约上。

Delmolino 等[20]通过教学编写智能合约的最佳方法，来避免一些常见的错误，并且产生了用于编写智能合约的在线开放课程材料。

另外，在一些数字货币中还有激励层的存在，本文将数字货币中的激励层合并到合约层中。比特币中每个共识节点的根本目的是最大化自身利益，所以需设定激励机制来最大化节点的自身利益使其参与到数据验证和记账中。

如今已存在的主流矿池通常有比特币 PoW 共识中的经济激励机制，它由比特币奖励和交易流动过程中的手续费两部分组成，有其特定的发行机制和分配机制，还有 PPLNS（pay per last N shares）、PPS（pay per share）以及 PROP（PROPortionately）等激励机制，其最终结果是产生一个合法区块。所以在一些私有链甚至联盟链中，此激励机制可能并不适用。

3　应用研究

现阶段，区块链的大部分研究仍集中针对各个应用。区块链系统具有的分布式高冗余存储、时序数据、数据不可篡改和伪造、去中心化、智能合约、高安全性、建立信任等特性，使区块链技术的应用不仅局限于数字货币领域，而在经济、金融和社会系统中都可以有广泛的应用场景，如慈善领域的轻松筹、积微循环等。本文将区块链目前的主要应用简单地概括为：金融服务、征信和权属管理、资源共享、投资管理、物联网与供应链、公共网络服务、选举投票、社会公益共 8 个场景。同时还有 5 种应用模式，即公有链（public blockchain）、联盟链（consortium blockchain）、私有链（private blockchain）、混合链（hybrid blockchain）和许可链（permissioned blockchain）。本文主要从金融服务、征信和权属管理、资源共享、供应链、隐私保护、公共网络服务、其他研究这几个方向进行解读。

3.1　金融服务

提到区块链，就必须提到比特币，比特币是区块链的一项重要应用。比特币推动了其底层区块链的发展，其强大的技术社区和强大的代码审查流程使其成为各种区块链应用中最为安全可靠的。所以，目前来说，区块链的大部分应用仍旧着眼于金融行业。

首先，金融行业存在的弊端有：1) 金融机构间的对账、结算成本高，涉及很多手工流程，使很多小额支付业务难以展开；2) 证券领域中，交易流程耗时长，增加后台业务成本；3) 资产管理中，主要是由中介负责托管，提高了交易成本，也增加了伪造的风险；4) 用户身份识别，不同金融机构间的用户数据很难高效交互，容易出错并且增加用户身份信息被某些中介机构泄露的风险；5) 在跨国交易等情形下，交易双方往往存在不充分信任的情形，彼此不能直接进行交易，需要中介担保。

DLA Piper[21]、Accenture[22]、ECB[23,24]、LaelBrainard[25]、杨东[26]等诸多机构及学者对将区块链技术运用到金融业做了相关的研究报告。这些研究都利用区块链技术具有的数据不可篡改和可追溯特性，构建监管部门需要的精准、及时且多维度的监管。并且基于区块链技术实现点对点的价值转移，通过分布式技术以及数字化资产，提升交易流程效率和降低成本。通过智能合约建立相应的机制确保符合约定好的合约条件。另外，区块链技术可实现数字化身份，极大地保障了身份信息安全与可靠管理，提高了用户识别的效率且降低了成本。

总体来说，研究者都认可区块链技术对金融业的促进作用，并认为区块链技术是未来的发展

方向，会极大地规范市场，创造更加安全、可靠、有效的商业模式。他们也认为这并不是市场革命，而是一个循序渐进的过程：一方面，区块链的相关技术并不成熟；另一方面，业务、法律和治理问题都需要一定的时间进行处理。

但是，由于区块链技术发展迅速，相关的法律法规还没有及时完善，而且由于区块链去中心化的存在，建立合理的监管体制变得更加困难重重，并且，区块链的资源问题仍然没有得到合理的解决。还有就是区块链的数据隐私问题，因为在区块链中一个地址的交易记录是可以被查到的，一旦与真实身份相联系，后果将十分严重。而且现在主要由一些网站负责交易，其安全性是值得商榷的。针对不同的应用场景，需要做出不同的取舍，就像三角理论一样，不要局限于现有的技术场景，要结合实际业务流程，合理规避风险，实现目标。

3.2 征信和权属管理

征信管理是一个巨大的潜在市场。目前，与征信相关的数据都掌握在少数机构手中，由于数据具有敏感性，因而征信管理有着很高的行业门槛。所以，现在大量的互联网企业都在尝试从各种维度获取海量的用户信息，但是从征信的角度来看，获取的信息仍然存在很多问题：1) 数据量不足；2) 数据的相关性较差，现在用户对自己的隐私信息极度敏感，不会暴露过多的数据给第三方；3) 时效性不足，各个企业获得的数据往往是过时的，甚至是虚假的。

权属管理主要用于产权、版权等所属权的管理和追踪溯源，包括汽车、房屋、艺术品、数字出版物等。目前，权属管理存在几大难题：1) 物品所有权的确认和管理；2) 交易的安全可靠；3) 一定的隐私保护。利用区块链技术，可以将物品的所属权写在区块链上，谁都无法修改，一旦出现合同中约定的情况，区块链技术将确保合同能够得到准确的执行，也可以对资产所有权进行追踪（如基于区块链的学历认证系统或房屋租赁系统）。

Dunphy[27]、吴健[28]以及金义富[29]等诸多学者，都对区块链技术应用在征信和权属管理上做了相关研究，提出了基于区块链技术的应用于各行各业的模型机制。通过时间戳以及散列算法对物品确认属权，证明一段文字、视频、音频以及学历等有价值的东西的存在性、真实性以及唯一性，提供不可篡改的数字化证明。一旦属权被确认，其交易记录或变更记录都会被记录在区块链上，配合诸如生物识别等技术，从根本上保障数据完整性、一致性，从而保护属权的唯一性。另外，运用区块链技术对现存方案的不足之处进行优化，能够有效地简化流程，提高效率，还能及时避免信息不透明和容易被篡改的问题。由于区块链技术的可追溯特性，一旦出现问题，可以及时追溯并解决问题。

但是，现阶段针对征信和权属管理的研究仍然存在许多问题：1) 可用性的问题，用户能否进行有效的密钥管理；2) 个人资料存储的监管问题、透明度问题；3) 以教育为例，其基于区块链技术模型的公信力问题；4) 如何保障个人记录的属权问题；5) 现有的基础设施还不足以确保安全性和强大算力的同时，体现区块链的优势。以上只是本文中提到的一些问题，一旦投入运行，必然会有新的问题出现。到时候就需要结合实际的流程，做出相应的变动来贴合实际。

3.3 资源共享

资源共享面临的主要难题包括：1) 共享成本过高；2) 用户身份评分难；3) 共享服务管理难。例如，社区能源共享的 ConsenSys 和微电网开发商 LO3，主要难题有交易系统的构建，但是通过区块链技术打造的平台可以很容易地实现社区内低成本的可靠交易系统。还有大数据共享，问题是如何评估数据价值、如何进行交易和交换、如何避免数据在未经许可的情况下泄露出去。使用区块链技术构成的统一账本，数据在多方之间的流动将得到实时的追踪和管理，并且通过对访问权限的管控，可以有效降低对数据共享过程的管理成本。

Aitzhan[30]、Sikorski[31]以及张宁[32]等多位学者，都对“区块链+能源互联网”的新模式进行了探讨及研究。主要提出将区块链技术应用到能源互联网中，其优势包括：1) 不再需要统一的中心机构进行调度管控，系统中的所有个体都可以自调度决策；2) 跨能源系统的通用型，给不同的能源系统信息提供统一的平台；

3) 数据的保密性与可靠性；5) 实现了使用区块链技术、多签名和匿名加密信息的分散式能源交易系统的概念验证能够使同行匿名协商能源价格并安全地进行交易；6) 很好地解决了精确计量问题、交互问题、自律控制、优化决策等问题。随着微电网案例的成功，区块链技术在资源领域的应用充满了希望。

但是同样地，在能源系统中，也存在很多的问题，本文仅提出一些解决思路以供参考：1) 能源互联网的垄断使区块链产生信息安全风险；2) 仍有许多未开发的研究领域（如延迟、吞吐量、大小和带宽、侧链、多个链、可用性）；3) 这些研究局限于能源领域，缺乏普遍性。

3.4 供应链管理

物流供应链中往往涉及多个实体，包括资金流、信息流、物流等，这些实体之间存在大量的复杂协作和信息交流。不同的实体各自保存各自的供应链信息，导致供应链信息严重不透明，造成较高的时间成本和金钱成本，出现问题（冒领、假冒等）难以追查和处理。但是通过区块链技术可以很好地避免甚至是解决这些问题。

一个很好的例子就是，Tian[33]所写的基于射频识别（RFID, radio frequency identification）和供应链技术的可追溯的农产品供应链系统，涵盖了数据采集和处理全过程，可以对供应链各环节的信息管理实现监控、跟踪和追溯，保证了农产品的质量安全。同时，Hallikas[34]、Kim 等[35]诸多学者专家，都提出了基于区块链技术的权限管控、防伪、追溯以及相应的智能合约，分别进行了流程化的建模叙述。

但是，这些研究仍然存在一些亟待解决的问题。1) 现在还基本处于概念证明的阶段，需要实现系统框架和原形，并逐步优化细节。2) 相应的成本比较高，如 RFID 标签最低为 0.3 美元；并且建立这种可追溯系统需要对配套设备进行大量投资，并对原有系统进行更新。3) 区块链的交易能力受限制，但是闪电支付或许是一个突破口。4) 区块链并不能提供一些模型中需要的技术，需要进行相互磨合。

3.5 隐私保护

随着互联网技术的蓬勃发展，个人隐私问题引起越来越广泛的注意，如医疗数据、财务数据等。涉及个人重要隐私的问题，都需要密切保护，避免造成重大的损失。而区块链的安全可信机制使区块链技术与隐私保护问题存在着很好的结合点，还能让数据拥有者切实管理数据的透明性与访问权限。

Heilman 等[36]学者提出了一种电子货币激励技术，用来提高在交易过程中的匿名性，提供安全、公平的交易，而且抗 DoS 攻击和 Sybil 攻击。Zyskind 等[37]则结合 blockchain、offblockchain 存储构建个人数据管理关注隐私的平台，利用分布式 Hash 表技术来加密数据，并保证高可用性，并通过合理的合约设计来保证隐私保护，并且讨论了区块链如何在可信计算中成为一个重要角色。优势就是解决了区块链的公共性，并且让用户在不影响安全性或者限制的情况下控制个人数据以及敏感数据，不需要信任第三方。在可信计算中，可以不让服务观察到原始数据，只让其运行计算，在网络上获取结果。这样就可以用安全额 MPC 安全地评估任何功能。

但问题是如何证明服务或者平台的提供者是善意的；另外，关于服务器的安全性，需要进一步考量；用户的操作、可用性是否符合规范，是否会造成密钥泄露等情况都需要考虑。此外，还需要高效安全可靠的智能合约来实现系统自治。

3.6 公共网络服务

当前 Internet 技术架构下的 IP 地址、根域名服务器等关键资源采用了集中式的组织和管理模式，域名服务系统依赖于根域名服务器的解析，是以根服务器为核心的中心化网络拓扑结构。为了解决根域名服务系统的中心化问题，目前国内越来越多的学者开始研究根域名服务体系的去中心化方案。中国工程院院士方滨兴提出一个“域名对等扩散”的方法[38]，让各个顶级域名所有者向其他国家级根域名掌握者报告其顶级域名服务器的地址信息。为了建立去中心化 DNS 体系，张宇等[39]提出了一个自主开放的互联网根域名解析体系，通过将根区解析服务独立出来，实现去中心化的根域名解析体系。刘井强[40]提出了基于私有根域名的 DNS 解析实验系统，这个系统通过区块链、Docker 等技术进行网络数据存储、划分、

映射，实现了私有根域名的 DNS 解析。但是其区块链架构采用的以太坊架构有些不太适合 DNS 体系。

蒋文保教授带领的团队提出了一种去中心化的网络域名服务系统模型 DDNS[41]，在此基础上提出了一种安全可信的网络互联协议（STiP）模型[42]。STiP 新型可信网络采用了一种安全高效的身份标识与地址定位之间的映射解析机制，在各国主权范围内采用树形层次结构，在国际间采用去中心化结构。该团队近期进一步开展了 Paxos、EPaxos、PBFT 等共识机制在去中心化网络域名服务根系统中的应用分析等研究。

3.7 其他研究方向

除了本文所述的几个研究方向外，还有相关学者进行了物联网、智能制造、攻击、比特币的钱包研究、更高的扩展性、侧链与闪电网络、社会学与人类学分析、P2P 以及对等网络、犯罪等研究，主要都是围绕区块链本身技术的不足之处进行优化。例如，物联网，一方面是物联网的设备增多，计算需求增强，大量的设备之间需要采用分布式自组织的管理模式，并且对系统的容错性要求很高。另一方面，区块链自身的分布式和抗攻击的特点可以很好地运用到这一场景，可以降低物联网应用的成本，而物联网设备的增多可以加强区块链的算力资源。在智能制造领域，区块链与物联网的结合可以更好地采集数据，提供安全的运营机制以及高效优秀的流程服务。

很多学者都在对区块链本身的技术进行优化，以拓展区块链的扩展性以及可用性，另外，区块链的资源问题为人担忧，所以有效、可靠的共识机制需要学者们的积极探究。区块链的快速发展，很有可能给不法分子提供成犯罪的机会，并给社会形态带来冲击，这些都需要学者大量的努力。

4 结束语

从 2009 年~2018 年，区块链技术已经走过了 9 个春秋，经历了区块链 1.0 时代，目前处于区块链 2.0 向区块链 3.0 迈进的时代，一些应用已经开始出现，但仍然还有发展与改进的空间。在设想中，区块链 1.0 是可编程货币时代，从另一方面来讲，更适合被称作狭义区块链技术的时代，其代表为比特币；区块链 2.0 是可编程金融时代，同时也是功能强大的智能合约时代，可以实现更高级更复杂的功能，极大地拓宽了区块链技术的应用场景；区块链 3.0 是可编程社会的时代（高级智能合约），是将区块链技术的去中心化和共识机制发展到新的高度、影响全人类意识形态以及社会形态的时代。区块链技术的发展，类似于互联网技术的诞生，其发展历程，也应该与互联网的发展类似，相信区块链技术将会逐渐改善人们的生活与意识形态。

参考文献：

[1] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[J]. Consulted,2008:1-49.

[2] PERCIVAL C, JOSEFSSON S. The scrypt password-based key derivation function[R]. 2016.

[3] WOOD G. Ethereum: a secure decentralised generalised transaction ledger[J]. Ethereum Project Yellow Paper, 2014, 151: 1-32.

[4] DRYJA T. Hashimoto: I/O bound proof of work[R]. 2014.

[5] BUTERIN V. Dagger: a memory-hard to compute, memory-easy to verify scrypt alternative[R].2013.

[6] KING S. Primecoin: cryptocurrency with prime number proof-of-work[R]. 2013.

[7] BIRYUKOV A, KHOVRATOVICH D. Equihash: asymmetric proof-of-work based on the generalized birthday problem[J]. Ledger, 2017, 2: 1-30.

[8] ANDRYCHOWICZ M, DZIEMBOWSKI S. Distributed cryptography based on the proofs of work[J]. IACR Cryptology ePrint Archive, 2014: 796.

[9] BONNEAU J, CLARK J, GOLDFEDER S. On Bitcoin as a public randomness source[J]. IACR Cryptology ePrint Archive, 2015: 1015.

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

[11] BAQER K, HUANG D Y, MCCOY D, et al. Stressing out: Bitcoin “stress testing”[C]//International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2016: 3-18.

[12] MILLER A, XIA Y, CROMAN K, et al. The honey badger of BFT protocols[C]//The 2016 ACM SIGSAC Conference on Computer andCommunications Security.2016: 31-42.

[13] LARIMER D. Delegated proof-of-stake (dpos)[R]. Bitshare whitepaper.2014.

[14] CASTRO M, LISKOV B. Practical Byzantine fault tolerance[C]//OSDI. 1999: 173-186.

[15] LAMPORT L. Paxos made simple[J]. ACM Sigact News, 2001, 32(4): 18-25.

[16] Szabo N. Smart contracts: building blocks for digital markets[J]. EXTROPY: The Journal of Transhumanist Thought, 1996,(16).

[17] MCCORRY P, SHAHANDASHTI S F, HAO F. A smart contract

for boardroom voting with maximum voter privacy[C]//International Conference on Financial Cryptography and Data Security. 2017: 357-375.

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

[19] KOSBA A, MILLER A, SHI E, et al. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts[C]//Security and Privacy (SP)2016: 839-858.

[20] DELMOLINO K, ARNETT M, KOSBA A, et al. Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab[C]//International Conference on Financial Cryptography and Data Security. Springer. 2016: 79-94.

[21] DLA P. Blockchain and the law: practical implications of a revolutionary technology for financial markets and beyond[R]. 2016.

[22] Accenture. Banking in a world of programmable assets[R]. 2016.

[23] ECB. Distributed ledger technologies in securities post-trading[R]. 2016.

[24] ECB. A brave new world? What impact will distributed ledger technology have on the financial industry?[J]. 2016.

[25] BRAINARD L. The use of distributed ledger technologies in payment, clearing, and settlement [J]. Speech, 2016.

[26] 杨东, 潘婴东. 区块链带来金融与法律优化[J]. 中国金融, 2016(8):25-26.
YANG D,PAN Z D. Block chain bring financial and legal optimization [J]. China finance , 2016(8):25-26.

[27] DUNPHY P, PETITCOLAS F A P. A First Look at Identity Management Schemes on the Blockchain[C]//IEEE Security and Privacy Magazine special issue on Blockchain Security and Privacy. 2018.

[28] 吴健, 高力, 朱静宁. 基于区块链技术的数字版权保护[J]. 广播电视信息, 2016(7):60-62.
WU J, GAO L, ZHU J N. Digital copyright protection based on block chain technology [J]. Radio and Television Information , 2016(7): 60-62

[29] 金义富. 区块链+教育的需求分析与技术框架[J]. 中国电化教育, 2017(9):62-68.
JIN Y F. Block chain + education demand analysis and technical framework [J]. China Educational Technology , 2017 (9) : 62-68.

[30] AITZHAN N Z, SVETINOVIC D. Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams[C]//Transactions on Dependable and Secure Computing.2016.

[31] SIKORSKI J J, HAUGHTON J, KRAFT M. Blockchain technology in the chemical industry: Machine-to-machine electricity market[J]. Applied Energy, 2017, 195: 234-246.

[32] 张宁, 王毅, 康重庆,等. 能源互联网中的区块链技术:研究框架与典型应用初探[J]. 中国电机工程学报, 2016, 36(15): 4011-4022.
ZHANG N, WANG Y, KANG C Q, et al. Blockchain technique in the energy Internet: preliminary research framework and typical applications[C]//Proceedings of the CSEE.2016, 36(15):4011-4022.

[33] TIAN F. An agri-food supply chain traceability system for China based on RFID &blockchain technology[C]//Service Systems and Service Management (ICSSSM).2016: 1-6.

[34] KORPELA K, HALLIKAS J, DAHLBERG T. Digital supply chain transformation toward blockchain integration[C]//proceedings of the 50th Hawaii international conference on system sciences. 2017.

[35] KIM H M, LASKOWSKI M. Towards an Ontology-driven blockchain design for supply chain provenance[C]// Submitted: workshop on information technology and systems. 2016.

[36] HEILMAN E, BALDIMTSI F, GOLDBERG S. Blindly signed contracts: anonymous on-blockchain and off-blockchain bitcoin transactions[C]//International Conference on Financial Cryptography and Data Security. 2016: 43-60.

[37] ZYSKIND G, NATHAN O. Decentralizing privacy: using blockchain to protect personal data[C]//Security and Privacy Workshops (SPW). 2015: 180-184.

[38] 方滨兴. 从“国家网络主权”谈基于国家联盟的自治根域名解析体系[J]. 信息安全与通信保密,2014,12:35-38.
FANG B X.Country autonomous root domain name resolution architecture from the perfective of country cyber sovereignty[J]. Information Security and Communi-cation Privacy,2014,12:35-38.

[39] 张宇, 夏重达, 方滨兴,等. 一个自主开放的互联网根域名解析体系[J]. 信息安全学报, 2017, 2(4):57-69.
FANG B X, XIA C D, FANG B X. An autonomous open root resolution architecture for domain name system in the internet[J]. Journal of Cyber Security, 2017, 2(4):57-69.

[40] 刘井强. 基于私有根域名的 DNS 解析试验系统设计与实现[D]. 哈尔滨：哈尔滨工业大学, 2017.
LIU J Q, Design and implementation of DNS resolution test system based on private root domain[D]. Harbin: Harbin Institute of Technology, 2017.

[41] 朱国库, 蒋文保. 一种去中心化的网络域名服务系统模型[J]. 网络空间安全, 2017, 8(1): 14-18.
ZHU G K, JIANG W B. A decentralized domain name system for the network[J]. Cyberspace Security, 2017, 8(1): 14-18.

[42] 蒋文保, 朱国库. 一种安全可信的网络互联协议(STiP)模型研究[J]. 网络空间安全, 2017, 8(1):24-31.
JIANG W B, ZHU G K. Research on the secure and trusted Internet protocol[J]. Cyberspace Security, 2017, 8(1): 24-31.

[作者简介]

章峰（1994-），男，江苏宿迁人，北京信息科技大学硕士生，主要研究方向为区块链技术、信息安全。

史博轩（1995-），男，北京人，北京信息科技大学硕士生，主要研究方向为区块链技术、网络安全监测与监控。

蒋文保（1969-），男，湖南永州人，北京信息科技大学教授，主要研究方向为可信网络、信任管理、区块链、网络空间主权。