文章编号:1007-5321(2018)02-0001-08 **DOI**:10.13190/j.jbupt.2018-039

区块链技术研究综述

黄俊飞[1], 刘 杰[2]

(1. 北京邮电大学 网络技术研究院, 北京 100876; 2. 北京邮电大学 电子工程学院, 北京 100876)

摘要: 区块链技术具有匿名性、去中心化、无法篡改、无需信任的共识机制等特征,去除了各类系统应用中的诸多约束条件,为很多想法的实现提供了技术可能性. 区块链技术在虚拟货币、金融科技、首次代币发行等领域发展迅速,但是其底层技术和基础理论的研究还相对落后. 笔者从区块链平台的概述入手,分别从点对点(P2P)协议、共识算法、智能合约的角度描述了区块链技术目前主要的研究内容和进展情况,然后从应用的角度阐述了区块链技术的几种主要应用场景.

关 键 词: 区块链; 以太坊; 共识机制; 智能合约

中图分类号: TP311 **文献标志码**: A

Survey on Blockchain Research

HUANG Jun-fei[1], LIU Jie[2]

(1. Research Institute of Networking Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China;
2. School of Electronic Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China)

Abstract: As a bitcoin-originated technology, the blockchain is becoming a hot area of technology research as virtual currencies such as bitcoin skyrocket. It is believed that the blockchain that creates the bitcoin miracle is with a much broader application prospect. The blockchain provides anonymity, decentralization, tampering, trust-free consensus mechanisms that removes constraints of various types of system applications and technical possibilities for the realization of many ideas. The blockchain is developed rapidly in the industrial sectors such as virtual currency, financial technology and initial coin offering , however, the research on underlying technology and basic theory is still relatively backward. Starting from the overview of blockchain platform, the article describes the main research content and progress from the point of view of peer to peer protocol, consensus algorithm and intelligent contract respectively. From the perspective of blockchain application, several application scenarios are discussed as well.

Key words: blockchain; Ethereum; consensus mechanism; smart contract

作为比特币的底层核心技术,区块链技术起源于2008 年化名为“中本聪(Satoshi Nakamoto)”的学者在密码学邮件组发表的奠基性论文《比特币:一种点对点电子现金系统》[1]. 比特币在过去这些年的快速发展也反过来验证了区块链这种技术在无需借助第三方可信中介结构情况下,互不信任的多方可以实现可信对等的价值传输. 2013 年 12 月, Buterin 提出了以太坊(Ethereum)区块链平台[2],除了可基于内置的以太币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. 超级账本(Hyperledger)是 Linux 基金会于 2015 年发起的推进区块链数字技术和交易验证的开源项目,目标是让成员共同合作,共建开放平台,满足来自不同行业各种用户的需求,并简化业务流程. 通过创建分

收稿日期: 2018-03-06

作者简介: 黄俊飞(1977—), 男, 讲师, E-mail: huangjunfei@bupt.edu.cn.

布式账本的公开标准,实现虚拟和数字形式的价值交换,如资产合约、能源交易、结婚证书,能够安全、高效、低成本地进行追踪和交易[3]. 虽然还存在各种质疑,但一种普遍的观点认为,区块链技术是下一代云计算的雏形,有望像互联网一样彻底重塑人类社会活动形态,并实现从目前的信息互联网向价值互联网的转变[4].

虽然还没有对区块链形成公认的定义,但通常所指的区块链技术包含了分布式存储、共识机制、加密算法、点对点传输等几个方面. 蔡维德等[5]认为从技术层面上看区块链的核心要素包含3个方面:① 块链结构,即每一区块有时间戳,都使用前一区块的散列加密信息,对每个交易进行验证;② 多独立拷贝存储,即每个节点都存储同样信息,享有同样权利,独立作业,互相怀疑,互相监督;③ 拜占庭容错,即容忍少于1/3的节点恶意作弊或被黑客攻击,保证系统仍然能够正常工作.

2016年10月,工信部颁布《中国区块链技术和应用发展白皮书》,指出"区块链系统的透明化、数据不可篡改等特征,完全适用于学生征信管理、升学就业、学术、资质证明、产学合作等方面,对教育就业的健康发展具有重要的价值"[6]. 以此为例,区块链技术在应用层面所包含的极难篡改性、智能合约、参与各方拥有完整的历史数据等特征,使得其在金融、征信、证券、安全、能源、教育等各个领域存在大量潜在的应用机会.

区块链不是单一技术名词,而是由多种技术合作构成的技术体系或技术族. 邵奇峰等[3]把区块链平台划分为网络层、共识层、数据层、智能合约层和应用层5个层次. 何蒲等[7]介绍了区块链的运行原理和关键技术,探讨了区块链技术的应用和发展趋势. 笔者将从区块链关键技术研究和应用这2个方面来呈现区块链技术的研究进展情况.

1 区块链概述

从字面上理解,区块链的基本内容包括:

1) 区块:记录一段时间内发生的交易和状态,是对当前账本状态的一次共识;

2) 链:由一个个区块按照发生顺序串联而成,是状态变化的日志记录.

区块链提供了一种去中心化的、无需信任积累的信用建立范式,因此区块链也是众多加密数字货币的核心,包括比特币、以太坊、莱特币、狗狗币等. 维护区块链的共识机制方式主要有工作量证明(PoW, proof-of-work)、权益证明(PoS, proof-of-stake)、授权股权证明(DPoS, delegated proof-of-stake)、Pool验证池、Ripple等.

区块链又可以分为公有链、联盟链和私有链. 公有链是最早的区块链,也是目前应用最广泛的区块链. 联盟链指的是由某个群体内部指定多个预选的节点为记账人,每个块的生成由所有的预选节点共同决定(预选节点参与共识过程),其他接入节点可以参与交易,但不过问记账过程的区块链. 私有链是指其写入权限由某个组织和机构控制的区块链,参与节点的资格会被严格限制.

通常,公有链中所有的节点可自由地加入或退出,而联盟链中的节点必须经过授权才可加入.

公有链中应用最广泛的通用平台是以太坊,目标是打造成一个运行智能合约的去中心化平台,平台上的应用按程序设定运行,不存在停机、审查、欺诈、第三方人为干预的可能. 联盟链中应用最广泛的通用平台主要是Hyperledger Fabric,其拥有IBM、Intel、J. P. Morgan、R3、DTCC、SWIFT等130多名成员[8],试图打造一个透明、公开、去中心化的超级账本项目,作为区块链技术的开源规范和标准. 以太坊的共识算法包括PoW/PoS,Hyperledger Fabric的共识算法有实用拜占庭容错(PBFT, practical Byzantine fault tolerance)和简化拜占庭容错. 以太坊的智能合约语言是Solidity/Serpent,而Hyperledger Fabric的智能合约语言支持Go/Java.

基于成熟的云计算技术体系,业界也出现了区块链即服务(BaaS, blockchain as a service)的平台,主要提供联盟链及公有链这2种服务,包括IBM的Bluemix、微软的Bletchley、万向区块链实验室的万云平台、腾讯的TBaaS等.

2 P2P协议

点对点(P2P,peer to peer)协议既是一种技术,也是一种思想,它的一个重要特点是改变互联网现在的以网站为中心的状态,重返"非中心化",并把权力交还给用户. 区块链平台通常选择完全分布式且可容忍单点故障的P2P协议作为网络传输协议,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. 针对文件分享和流媒体应用,P2P技术已经在区块链技术出现之前得到了广泛的研究和应用,Napster是该领域的先锋,BitTorrent是其架

构的一种演变，而专门针对区块链 P2P 技术的研究相对较少. 在比特币网络中，新的交易向全网进行广播，当一个节点找到了一个 PoW 时，它也向全网进行广播.

目前有 2 种不同的 P2P 技术应用在区块链上，比特币和以太坊的 P2P 协议是基于 TCP 协议实现的；Hyperledger Fabric 则使用建立在 HTTP/2 上的 P2P 协议来管理分布式账本，使用 gRPC 来做 P2P 通信.

除了 P2P 协议，区块链技术也会用到其他协议，如 Stratum 协议就应用于挖矿以及轻量级或者移动端比特币钱包中.

3　共识算法

一致性问题研究的核心指标是容错的节点比例和收敛速度，分布式网络的核心难题是如何高效地达成共识. 如何在一致性和可用性之间进行平衡，在不影响实际使用体验的前提下还能保证相对可靠的一致性，是研究共识机制的目标[9].

分布式数据库是传统共识机制的主要应用领域，互联网的发展促进了分布式共识问题的研究，包括拜占庭将军问题(Byzantine faults)，问题中的节点有可能被怀有恶意的人控制，从而以不可预知的方式运行. 区块链网络可以看作是一个通过点对点传输协议连接起来的共享账本，其结构类似于分布式数据库，但是比分布式数据库更为分散. 每个参与者都能在账本上记录信息，每一条记录包含一定时间内的交易信息，并且会广播到整个网络上，所有的节点保持着账本信息的同步.

问题在于谁拥有更新记录的权力. 每个节点都可能更新有利于自己的信息，哪一个更新是应该相信的？这个问题和拜占庭将军问题相同，Lamport 等[10]在 1982 年提出了这个共识问题.

区块链系统跟传统分布式系统不同，其处理性能无法通过单纯增加节点数进行扩展，实际上，很大程度上取决于单个节点的处理能力. 基于 PoW 机制的比特币区块链平均每 10 min 生成一个区块，平均每秒只能处理 7 笔交易，不适合用于高频交易领域. 如何提高验证速度一直是研究热点之一. Li 等[11]提出了基于信任度的多链路并发通信模型和综合因子通信树算法，来提升区块链的交易验证效率和可靠性. 另外，闪电网络、侧链(side chain)、影子链(shadow chain)这些都是值得借鉴的设计思路.

PoW 通过算力的比拼达成共识，PoS 通过币龄来分配获得记账权的概率达成共识，DPoS 通过选举出的记账节点来获得共识，PBFT 通过经典的三阶段协议来获得共识，Paxos 作为第 1 个被证明的共识算法基于两阶段提交并扩展协议达成共识. 除此之外，还有 Paft Raft 算法、拜占庭容错委托、Pool 验证池、重要性证明、存在证明、流逝时间量证明等各类共识算法应用于不同的区块链中.

下面主要介绍最常见的几种共识算法和相关的研究进展情况.

3.1　PoW

PoW 是比特币的区块链所使用的共识机制[1]，通过在区块中添加一个随机数 nonce，若使得该区块的随机散列值以若干个 0 开头，则表示验证通过，发现这个随机数的设备拥有向区块中写入数据的权力.

在找到这个有效随机数之前，区块链网络的大量节点都在做这个计算. 由于随机散列值的伪随机性，假设要找到 4 个前导 0 的随机散列值，大概要进行 2^{16} 次尝试. 考虑到硬件计算能力的高速增长，比特币区块链网络通过调整随机散列值开头 0 的数量来修改网络搜寻随机数的难度，从而始终保证大概每隔 10 min 生成一个区块. Kraft[12]研究了各种散列率情况下区块生成时间的预测，并提出了具有更好稳定性的难度更新方法. 实际被比特币的区块链网络使用的 PoW 函数是 SHA256.

PoW 机制实际上就是为信息的传递加入了成本因素，从而降低了信息传递的速度. 其在区块链网络中的共识流程如下：

1) 每一笔新的交易向全网进行广播；

2) 每一个节点都将收到的交易信息纳入一个区块中，并计算出区块头部的 Merkle 根，预设区块头部的 nonce 值，并计算随机散列值，直至达到前导 N 个 0 的难度要求，向全网进行广播；

3) 收到广播的节点对交易(当且仅当包含在该区块中的所有交易都是有效的且之前未存在过的，其他节点才认同该区块的有效性)和 nonce 随机数的有效性进行验证，如果正确，将该区块加入区块链，并开始建下一个区块.

基于 PoW 的区块链通过高耗能和低性能换来了区块链的安全性和数据的一致性. 比特币系统平均每 10 min 产生一个区块，区块尺寸上限为 1 MB，普通交易(包含 1 个输入与 2 个输出)的尺寸约为

250 B,每秒交易量约为7 TPS[13].

对基于PoW机制的区块链而言,如果要实现对区块链的攻击,就必须计算从某个区块开始往后所有区块的nonce值,并且计算速度要超过主链;要确保攻击是成功的,就需要掌握全网算力的51%以上. Eyal等[14]还提出了一种"自私挖矿"的攻击策略,通过部分矿工的相互勾结,将当前产生的区块进行扣留,并在扣留区块上进行挖矿,一旦网络中的区块生成速度赶上恶意矿工的区块生成速度时,勾结的恶意矿工将扣留的区块释放到网络中,使其成为最长链. 通过这种挖矿策略,恶意矿工只需25%的计算能力就可对整个比特币网络发起51%攻击. 总体而言,基于PoW机制的区块链被攻击的难度和成本都是很高的.

PoW被世人诟病的另一个原因就是,PoW的本质意味着比特币需要消耗能源来维护运行. Nomura的报告指出,2017年11月份比特币挖矿消耗的电量同比增长了26%,现在已经接近每年36 TW·h的水平,相当于330万户家庭的用电量. 如果将比特币看成一个国家,它的耗电量可以排在59位.

3.2 PoS

最初引入PoS[15]共识机制既是作为一种手段来对抗已知的比特币网络攻击,尤其是51%攻击,也是用于解决PoW过度浪费算力资源(能源)的替代方案.

在PoS模式下,有一个名词叫币龄(coin age),每个币每天产生1币龄,节点拥有的权益与持有货币的量和时间(所有币龄的总和)有关. PoS指的就是权益(数字货币)所有权的一种证明,PoS确实可以替代PoW的功能,因为它也是不能够轻易伪造的. 从哲学的角度来说,金钱也是过往工作的一种证明形式.

基于PoS的区块链矿工不用挖矿,节点拥有的权益越多,挖矿的整体难度就会越低. 在PPCoin中[15],PoS区块将根据交易中所消耗的币龄产生数字货币. 以太坊则计划在2018年实现将PoW机制改为PoW/PoS混合共识机制,即以太坊区块链上的交易仍然使用当前的PoW共识算法,但是每100个区块中有一块使用PoS共识算法.

DPoS类似于董事会的投票机制,先通过PoS选举出n个记账节点,节点提交的提案被这些记账节点投票决定谁是正确的.

3.3 PBFT

1999年,Castro等[16]提出了PBFT算法,可以在异步网络中不保证活性(liveness)的情况下解决拜占庭将军问题,并且该算法进入无限循环的概率非常低,解决了原始拜占庭容错算法效率不高的问题,将算法复杂度由指数级降低到多项式级,使拜占庭容错算法在实际系统应用中变得可行.

拜占庭容错经过3个阶段达成一致性. 这些阶段可能因为失败而重复进行,在$N \geqslant 3F+1$(N为计算机总数,F为有问题计算机总数)的情况下一致性是可能解决的,所以算法能够容纳将近1/3的恶意节点,即如果有超过2/3的正常节点,区块链网络就能保障数据的一致性和安全性,IBM创建的Hyperledger就是使用了该算法作为共识算法. 邵奇峰等[3]详细描述了PBFT在区块链网络中的共识流程,并指出在节点数为N的网络中,该算法有2个阶段需要传输的网络消息为$O(N^2)$,其会造成很大的网络开销,目前基于PBFT算法的区块链系统性能并不高[17].

有的应用使用PoW的可扩展性和PBFT的安全性来达成共识,如Byzcoin和Elastico首先用PoW来确定运行PBFT的共识组.

4 智能合约

密码学家尼克·萨博(Nick Szabo)提出的智能合约背后的基本思想是在硬件和软件中嵌入合同条款,使得合约不能被破坏或者违约的成本极其高昂[18]. Szabo[19]建议将合同条款(抵押品等)翻译成代码,并将其嵌入可自行执行的设备(硬件或软件)中,以尽量减少交易各方之间对可信中介的需求以及恶意或意外的情况.

智能合约是安全可靠的,可以自动执行合约条款的计算机程序,虽然这个概念和互联网几乎同步出现,但是智能合约一直没有完美的技术方案予以支撑,签署合约的多方如何互相信任,并达成一致以及合约执行过程的安全可靠性问题长期以来都缺乏技术基础.

区块链则为上述问题的解决提供了技术可能性. 在区块链上,智能合约是存储在区块链中的脚本(与关系数据库管理系统中的存储过程大致相似[20]),拥有唯一的地址,基于交易来触发执行. 基于区块链的智能合约一旦启动就自动运行,不需要合约签署方的干预. 合约执行的规则可以放在共识

算法中，合约的状态和执行代码也放在区块链上，合约触发后自动执行合约代码，并将执行结果保存在区块链中. 也就是说，区块链技术成为了一个智能合约的可信计算环境.

区块链技术为智能合约开启了长足发展的大门；反过来，智能合约也对区块链技术具有重要意义. 基于智能合约的区块链，可以成为社会信任的基石，可降低商业社会信用构建的难度，并为价值互联网的发展奠定应用基础.

比特币网络有内置的脚本功能，为了保持比特币的向前兼容和简单稳定，比特币的开发者对其脚本做了诸多限制，如脚本中没有循环语句.

支持比特币交易的区块链支持不相互信任的交易对手之间的资产转移. 而支持智能合约的区块链进一步考虑了这一点，并允许在互不信任的交易对手之间进行多步骤处理：① 在决定参与合同之前检查代码并确定其结果；② 具有执行的确定性，因为代码已经部署在一个完全无法控制的网络上；③ 整个过程具有可验证性，因为所有的交互都是数字签名的. 合约出现争议的可能性被消除，因为参与者不能不同意合约的最终结果[21].

图灵完备是指一个能计算出每个图灵可计算函数的计算系统. 比特币的脚本系统是图灵不完备的，而以太坊则是一种具有高效共识机制、图灵完备性并支持智能合约的区块链，它使区块链拥有了更广泛的商业应用场景. 以太坊是一个通用的全球性区块链，也是一个平台和编程语言，包括数字货币以太币和用来构建、发布分布式应用的智能合约编程语言[2]. 如图 1 所示，以太坊的结构与比特币相比并没有本质的差别，但是它全面实现了智能合约的概念，支持了全新的合约编程语言以及为了运行合约增加了一个以太坊虚拟机.

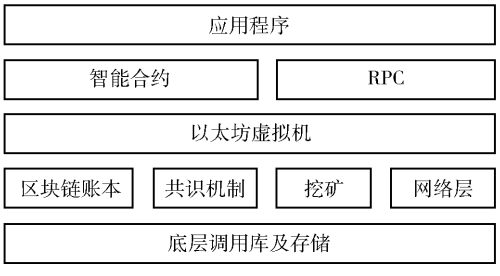

图 1　以太坊结构

以太坊中的智能合约是运行在以太坊虚拟机上的，这是一个智能合约的沙盒，合约存储在以太坊的区块链上，并被编译为以太坊虚拟机字节码，通过虚拟机来运行.

Hyperledger Fabric 提供的智能合约叫作 chaincode，即链码，使用 Docker 容器来运行智能合约，基于 Docker 提供的隔离性和安全性来实现宿主主机的安全性. 可基于 Go 和 Java 高级语言开发智能合约，这些语言不但图灵完备、技术成熟，而且可降低合约开发者的学习门槛.

随着技术的发展，智能合约的形态也还会不断演化，例如，具有权限控制的和没有权限控制的智能合约设计就可能不尽相同，有内部代币和没有内部代币的智能合约设计又有显著区别[22].

智能合约的另一个重要影响就是引发了“分散自治组织（DAO，decentralized autonomous organization）”的概念和思考，相对于用体制等级制度来管理的社会组织形态，DAO 则指出了非层级社会治理模式的可能性，社会的决策权力分散在整个网络的节点上，而不是集中在某个中心[23]. DAO 可能是未来互联网上组织形态的雏形，不受任何个体的控制，却又有明确的目标，能够自己进化和发展.

5　区块链技术的应用

区块链在不引入第三方中介机构的前提下，可以提供去中心化、不可篡改、安全可靠等特性保证. 因此，所有直接或间接依赖于第三方担保信任机构的活动，均可能从区块链技术中获益.

5.1　金融应用

区块链作为广受追捧的金融科技，金融行业是其最重要的应用领域. 区块链技术公开透明和不可篡改的属性提供了一种去中心化的信任机制，具备改变金融基础架构的潜力，使其在金融领域具有广阔的应用前景.

1）数字货币：2015 年，Coinbase 推出一款新型比特币借记卡，只要收款方接受 Visa 卡，这款 Coinbase 卡片的美国用户就可以直接进行比特币支付. 2017 年，中国人民银行数字货币研究所悄然挂牌成立；2018 年初，相关报道指出，中国央行数字货币拟采用双层投放体系.

2）金融交易：纳斯达克利用区块链技术建立了交易平台 Linq；Ripple 基于区块链技术实现了快捷低成本的跨境支付.

3）资产管理：商业积分、电子券、预付卡、游戏装备、保险卡单等各类数字资产正快速通过区块链

技术进行融合变异. 区块链技术一方面提供了可靠的确权机制;另一方面也促进了各类数字资产的流动.

5.2 数据保护/隐私保护

区块链的一个主要特征是其执行匿名交易的能力,这种匿名性为数据或隐私的保护提供了透明机制. Swan[24]提到健康隐私问题的严重性,认为区块链技术可以提供一个保护个人健康隐私数据不受侵犯的机制. 章宁等[25]通过代入具体应用场景将区块链技术个人隐私保护机制进行了详细阐述. Lazarovich[26]提出了基于分布式存储的第三方数据库 Escrow 以及基于区块链审计的隐形墨水系统,并以医疗信息个人隐私保护为例来阐明区块链技术在个人隐私问题上的应用. Zyskind 等[27]阐述了一种基于区块链的自动访问控制管理协议,用于实现去中心化的个人数据管理系统,并确保用户能够拥有和控制他们的数据. Roehrs 等[28]提出的 OmniPHR 系统利用区块链技术来实现个人健康数据的保存和访问,以确保数据的安全和防篡改. MeDShare 系统旨在解决医疗大数据保管人在无信任环境下共享医疗数据的问题,利用区块链对云存储中的共享医疗数据提供数据溯源、审计和控制等能力[29].

5.3 其他

Kang 等[30]提出了一种 P2P 的电力交易系统,用于在智能电网中的插电式混合动力电动车辆(PHEV)之间的本地电力买卖,其中包括用于提升交易安全性的联盟链和双重拍卖机制,充电和放电插电式混合电动汽车可以交易电力,而不依赖于值得信赖的第三方.

Dorri 等[31]提出了如何在车联网中利用区块链技术保护用户的隐私,并提供了车辆生态系统的安全性架构,且通过无线远程软件更新等业务验证了这种安全架构的功效.

Lei 等[32]提出了一个基于区块链的动态秘钥管理系统,包括异构网络的秘钥传递方法和动态的交易收集期限,并将这一系统用于智能交通系统.

另外, Christidis 等[21]认为结合物联网和区块链可能引起重大的行业变革,为新的商业模式和新型分布式应用铺平了道路. 基于区块链的物联网安全问题也是研究的热点之一,尤其是考虑到欧洲通用数据保护条例将在 2018 年生效. 区块链去中心化和无需第三方信任中介的功能使其成为物联网解决方案基础要素的理想组件,区块链可以用账本的形式保留物联网设备历史的无可争议的记录[33-35]. Sharma 等[36]提出了一种基于区块链的新型分布式云架构,为物联网提供了低成本、安全和按需访问的基础设施.

6 结束语

从 2009 年开始,技术极客利用区块链独特的技术特征创造了比特币、以太坊等软件奇迹. 面对区块链绕开银行业中心化架构的挑战,2015 年银行业开始尝试结合利用这一新的技术,并逐步引起各国央行乃至政府的重视.

区块链技术在展示其无限可能的同时,在金融、资产管理、溯源、数据保护、物联网等各类惠及民生的领域,已经展开了一轮又一轮的尝试. 虽然众多的应用离真正落地还有一定的距离,并且不断受到来自法律、伦理、安全等方面的挑战,但区块链正在被越来越多的行业所认知和理解. 随着技术原理的普及和技术门槛的下降,曾经归属于极客世界的区块链将成为一种软件基础设施,成为各类应用的一个重要基础组件.

笔者介绍了区块链在各个相关技术和应用层面的研究进展,目前区块链技术基础理论和应用的研究还处于起步阶段. 区块链达成共识的效率相对于中心化体系是低效的,共识账本的公开使得参与方之间的信息传输具有泄露的可能性,智能合约也有各种类型且可以被攻击的漏洞[37]. 这种应用发展远胜于理论研究的情况,导致了很多应用产品存在致命性弱点,不利于区块链长远的发展. 希望有更多研究人员参与到区块链相关原理、算法、体系架构等领域的研究中来.

总之,区块链虽然还有许多有待解决的问题,但是并不影响今后它在价值互联网、金融科技、数字货币等领域的发展与应用,在未来很长一段时间内它仍然会是人们研究的一个热点.

参考文献:

[1] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system [EB/OL]. [2017-11-23]. https://bitcoin.org/bitcoin.pdf.

[2] Buterin V. A next-generation smart contract and decentralized application platform [EB/OL]. GitHub: ethereum/wiki, 2014. https://github.com/ethereum/wiki/wiki/%5BEnglish%5D-White-Paper.

[3] 邵奇峰, 金澈清, 张召, 等. 区块链技术: 架构及进展

[J]. 计算机学报, 2018, 41(5): 969-988.
Shao Qifeng, Jin Cheqing, Zhang Zhao, et al. Blockchain: architecture and research progress [J]. Chinese Journal of Computers, 2018, 41(5): 969-988.

[4] 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 Yong, Wang Feiyue. Blockchain: the state of the art and future trends [J]. Acta Automatica Sinica, 2016, 42(4): 481-494.

[5] 蔡维德, 郁莲, 王荣, 等. 基于区块链的应用系统开发方法研究[J]. 软件学报, 2017, 28 (6): 1474-1487.
Tsai WeiTek, Yu Lian, Wang Rong, et al. Blockchain application development techniques [J]. Journal of Software, 2017, 28 (6): 1474-1487.

[6] 周平, 杜宇, 李斌, 等. 中国区块链技术和应用发展白皮书[Z]. 北京: 中国区块链技术和产业发展论坛, 2016: 36-37.

[7] 何蒲, 于戈, 张岩峰, 等. 区块链技术与应用前瞻综述[J]. 计算机科学, 2017, 44(4): 1-7.
He Pu, Yu Ge, Zhang Yanfeng, et al. Survey on blockchain technology and its application prospect [J]. Computer Science, 2017, 44(4): 1-7.

[8] Hyperledger. About Hyperledger[EB/OL]. USA: The Linux Foundation Projects, 2017. https://www.hyperledger.org/about.

[9] 沈鑫, 裴庆祺, 刘雪峰. 区块链技术综述[J]. 网络与信息安全学报, 2016, 2(11): 12-18.
Shen Xin, Pei Qingqi, Liu Xuefeng. Survey of blockchain[J]. Chinese Journal of Network and Information Security, 2016, 2(11): 12-18.

[10] Lamport L, Shostak R, Pease M. The Byzantine generals problem [J]. ACM Transactions on Programming Languages and Systems, 1982, 4(3): 382-401.

[11] Li Jiao, Liang Gongqian, Liu Tianshi. A novel multi-link integrated factor algorithm considering node trust degree for blockchain-based communication [J]. KSII Transactions on Internet and Information Systems, 2017, 11(2): 3766-3788.

[12] Kraft D. Difficulty control for blockchain-based consensus systems [J]. Peer-to-Peer Networking and Applications, 2016, 9(2): 397-413.

[13] Wattenhofer R. The science of the blockchain [M]. Charleston, USA: CreateSpace Independent Publishing Platform, 2016.

[14] Eyal I, Sirer E G. Majority is not enough: bitcoin mining is vulnerable [C] // International Conference on Financial Cryptography and Data Security. Berlin, Heidelberg: Springer, 2014: 436-454.

[15] King S, Nadal S. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake [EB/OL]. USA: archive.org, 2012[2018-01-03]. https://peercoin.net/assets/paper/peercoin-paper.pdf.

[16] Castro M, Liskov B. Practical byzantine fault tolerance and proactive recovery [J]. ACM Transactions on Computer Systems (TOCS), 2002, 20(4): 398-461.

[17] Dinh T T A, Wang Ji, Chen Gang, et al. Blockbench: a framework for analyzing private blockchains[C] // Proceedings of the 2017 ACM International Conference on Management of Data (SIGMOD). Chicago, USA: [s.n.], 2017: 1085-1100.

[18] Szabo N. Formalizing and securing relationships on public networks [J/OL]. First Monday, 1997 [2017-01-12]. http://www.firstmonday.org/ojs/index.php/fm/article/view/548/469.

[19] Szabo N. The idea of smart contracts [EB/OL]. USA: Nick Szabo's Papers and Concise Tutorials , 1997 [2018-01-12]. http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_idea.html.

[20] Oracel. MySQL reference manual - using stored routines (procedures and functions) [EB/OL]. USA: Oracle.com, 2016 [2018-01-12]. http://dev.mysql.com/doc/refman/5.7/en/stored-routines.html.

[21] Christidis K, Devetsikiotis M. Blockchains and smart contracts for the Internet of things[J]. IEEE Access, 2016(4): 2292-2303.

[22] Daniele Magazzeni, Peter McBurney, William Nash. Validation and verification of smart contracts: a research agenda [J]. Computer, 2017, 50(9): 50-57.

[23] Tomaso Aste, Paolo Tasca , Tiziana Di Matteo. Blockchain technologies: the foreseeable impact on society and industry [J]. Computer, 2017, 50(9): 18-28.

[24] Swan M. Blockchain thinking: the brain as decentralized autonomous corporation[J]. IEEE Technology & Society Magazine, 2015, 34(4): 41-52.

[25] 章宁, 钟珊. 基于区块链的个人隐私保护机制[J]. 计算机应用, 2017, 37(10): 2787-2793.
Zhang Ning, Zhong Shan. Mechanism of personal privacy protection based on blockchain [J]. Journal of Computer Applications, 2017, 37(10): 2787-2793.

[26] Lazarovich A. Invisible ink: blockchain for data privacy [D]. Massachusetts: Massachusetts Institute of Tech-

nology, 2015: 36-40.

[27] Zyskind G, Nathan O, Alex. Decentralizing privacy: using blockchain to protect personal data[C]// IEEE Security and Privacy Workshops. [S. l.]: IEEE Computer Society, 2015: 180-184.

[28] 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.

[29] 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.

[30] 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.

[31] Dorri A, Steger M, Kanhere S S, et al. Blockchain: a distributed solution to automotive security and privacy [J]. IEEE Communications Magazine, 2017, 55(12): 119-125.

[32] Lei Ao, Cruickshank H, Cao Yue, et al. Blockchain-based dynamic key management for heterogeneous intelligent transportation systems [J]. IEEE Internet of Things Journal, 2017, 4(6): 1832-1843.

[33] IBM. Understand the fundamentals of IBM blockchain [EB/OL]. USA: IBM, [2018-02-03]. https://www.ibm.com/blockchain/what-is-blockchain.html.

[34] Conoscenti M, Martin J C D. Peer to peer for privacy and decentralization in the internet of things[C]// IEEE/ACM, International Conference on Software Engineering Companion. [S. l.]: IEEE, 2017: 288-290.

[35] Nicola Fabiano. Internet of things and blockchain: legal issues and privacy. the challenge for a privacy standard [C]//2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). Tunisia: IEEE 2017: 727-734.

[36] Sharma P K, Chen MuYen, Park J H. A software defined fog node based distributed blockchain cloud architecture for IoT[J]. IEEE Access, 2018, 6: 115-124.

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