计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.200700020

区块链共识算法效能优化研究进展

张彭奕　宋　杰
东北大学软件学院　沈阳 110169
(1187778272@qq.com)

摘　要　近年来,区块链及其相关技术发展迅速,区块链也迅速成为了学术界的热门领域。然而,区块链的共识算法在资源花销、能源耗费和性能上都饱受诟病,因此需要制定一个能衡量其执行效率的指标,以评价其设计是否优良。由于共识算法的资源花销、能源耗费以及性能之间相互关联且关系复杂,因此有必要从"效能"的角度对现有区块链的共识算法加以分析,并总结研究思路。文中总结了区块链共识算法的效能优化研究进展。首先定义区块链共识算法的效能为"在正确性和有效性的前提下计算的共识算法性能、所需资源和能源消耗",并分析这3个影响因素的关联;然后从公有链与联盟链两方面对共识算法的效能优化进行整理与总结;最后从多链区块链、多个区块链与BaaS这3个方面提出关于共识算法的资源共享问题,以供研究人员参考。

关键词:区块链;共识算法;效能;资源优化;能耗优化;性能优化
中图法分类号　TP311

Research Advance on Efficiency Optimization of Blockchain Consensus Algorithms

ZHANG Peng-yi and SONG Jie
Software College,Northeastern University,Shenyang 110169,China

Abstract　Blockchain and its related technologies have developed rapidly in recent years,and blockchain has rapidly become a hot field in the research field. However,blockchain consensus algorithm has been criticized in terms of resource consumption,energy consumption and performance. Therefore,it needs to develop an indicator that can measure its execution efficiency,so as to evaluate the design quality of consensus algorithm. However,the correlation between resource consumption,energy consumption and performance of consensus algorithm is complicated,so it is necessary to analyze the existing blockchain consensus algorithm from the aspect of efficiency and summarize the research ideas. This paper summarizes the progress of the efficiency optimization of blockchain consensus algorithms. First of all,we define the efficiency of blockchain consensus algorithm as "the performance of consensus algorithm,required resources and energy consumption calculated under the premise of correctness and effectiveness",and analyze the correlation of the three factors. Then the efficiency optimization of consensus algorithm is collated and summarized from the two aspects of public chain and alliance chai. Finally,the resource sharing problems of consensus algorithm are put forward from three aspects of multi-chain blockchain,multiple blockchain and BaaS for the reference of researchers.

Keywords　Blockchain,Consensus algorithms,Efficiency,Resource optimization,Energy consumption optimization,Performance optimization

1　引言

近年来,区块链技术迅速走红,作为一种按时间顺序存储数据的数据结构,其去中心化、安全性高以及不可篡改的特点被学术界和工业界所认同。2008年,中本聪发表了"Bitcoin:a peer-to-peer electronic cash system"一文,比特币问世,"区块链"这一概念首次被提及。此后,区块链的应用越来越广,包括银行、交易所、医院、政府和教育部门等诸多领域。

区块链主要分为3类:公有链、联盟链和私有链。公有链是一种信息完全公开、任何人都可以参与使用的链。任何人都可以在公共链上进行交易,还可以随时参与网络上形成共识的过程。私有链仅在私有组织使用,区块链上的读写权限、参与记账权限按私有组织的规则来制定。与公有链相比,私有链达成共识的时间相对较短,交易速度更快,效率更高,成本更低。联盟链则介于二者之间,由若干组织共同合作维护一条区块链,且该区块链必须具备带有权限的访问控制限制。

随着区块链的迅速发展,与区块链相关的技术也随之快速发展。区块链的核心技术包括分布式账本、非对称加密、共识机制以及智能合约,每种技术都在区块链中发挥着各自的作用,其中最为重要的是共识机制。

到稿日期:2020-07-01　返修日期:2020-09-14　本文已加入开放科学计划(OSID),请扫描上方二维码获取补充信息。
基金项目:国家自然科学基金(61672143)
This work was supported by the National Natural Science Foundation of China(61672143).
通信作者:宋杰(songjie@mail.neu.edu.cn)

在基于分布式系统的 P2P 网络中，去中心化思想需要一种新的方法来使所有的节点达成共识，共识机制应运而生。共识机制是一种分布式系统的特殊机制，通过网络间特殊节点的投票，可以在短时间内达成共识，从而完成对交易的验证与确认，而共识算法的产生主要是为了解决分布式系统中的一致性问题。早在 1980 年，Lamport 等就提出了分布式领域的共识问题，该问题的定义为：在一组可能存在故障节点、通过点对点消息通信的独立处理器网络中（P2P 网络），非故障节点如何针对特定值达成共识。1982 年，Leslie 等[1]首次提及了网络中节点从中作恶的情况，即“拜占庭将军问题”。随着时间的推移，分布式一致性问题逐渐可以按照是否出现恶意节点伪造信息的情况分为两类：“拜占庭错误”（Byzantine fault）与“非拜占庭错误”（Non-byzantine fault）。前者表现为恶意节点伪造信息，或者通信网络中断、节点发生故障等情况；后者则主要表现为通信存在物理错误或通信处理延迟。2008 年比特币问世，“共识机制”成为了区块链的核心技术之一。

不同种类的区块链中所需的共识算法也不同。私有链的适用环境一般不考虑集群中存在作恶节点，只考虑由于系统或者网络的原因而出现的故障节点，故采用分布式系统的传统共识算法，其中常见算法为 Raft 与 Paxos。联盟链的适用环境除了需要考虑集群中存在故障节点，还要考虑集群中存在作恶节点。对于联盟链，每个新加入的节点都需要验证和审核，常见算法为 PBFT 与 DPoS。公有链的适用环境与联盟链类似，常用算法为 PoW 与 PoS，这些算法与参与者的利益相关。这 3 种区域链的相关资料如表 1 所列。

表 1　区块链的种类及对应的共识算法

Table 1　Types of blockchain and corresponding kind of consensus algorithms

区块链种类	适用环境	常用的共识算法	备注
公有链	需要考虑集群中存在故障节点，还需要考虑集群中存在作恶节点	PoW，PoS	算法与参与者的利益相关
联盟链	与公有链相同	PBFT，DPoS	节点的加入需要审核与验证
私有链	不考虑集群中存在作恶节点，只考虑由于系统或者网络的原因而导致的故障节点	Raft，Paxos	采用分布式系统的传统共识算法

随着时间的推移，人们发现部分共识算法存在诸多问题。这些问题集中表现在 3 个方面：资源、能耗与算法性能。首先，部分共识算法浪费资源。以 PoW 算法为例，其通过计算符合要求的 Nonce 串来获得记账权利，而该计算过程需要很大的算力，且其 Hash 值的计算复杂度会随着计算机算力的提升而提升，因此额外的资源投入并不能带来等效的性能提升。如何对资源消耗高的算法进行优化成为了当下的研究热点。目前，PoW 优化算法已有很多，常见的有 PoS，DPoS 等。其次，共识算法的性能效率也存在一定问题。在生成区块的时间方面，如 PoW，该算法控制 10 min 生成一个全新的区块，即每次 Hash 计算至少需要 10 min。在记录越发频繁的今天，10 min 一次的效率远不及秒级算法。如今人们对区块链的记账效率进行了优化，可以达到秒级。共识算法性能优化仍然有很大空间，如针对区块链系统网络性能的优化与算法复杂度的优化等，这些都是学界关注的研究热点，也是未来共识算法性能优化的重点。最后，共识算法的能耗问题也是区块链的一个重要问题。随着比特币、以太坊等一众区块链系统的迅速发展，能耗问题也随之而来。目前最大的耗能区块链系统为比特币系统，其年耗电量高达全球总用电量的 1%，可见当前公有区块链系统的电能消耗之高。区块链的能耗问题主要来自硬件的消耗，而硬件主要用于实现共识算法。因此，共识算法的能耗问题也是一个亟待解决的问题。

综上所述，为了优化区块链共识算法，本文分析了算法的资源消耗、能耗与算法性能之间的关系，并整理了现有优化方法的研究进展。本文第 2 节定义了区块链的效能，并将效能优化分解为 3 个方面，然后对 3 个方面之间的逻辑关系进行了梳理；第 3 节和第 4 节分别整理与分析了公有链和联盟链的效能优化研究进展；第 5 节提出了共识算法的资源共享的问题，分别从多链区块链、跨区块链与 BaaS 3 个方面着手。

2　优化目标

2.1　共识算法的效能

在区块链中，共识算法作为去中心化网络中的新型技术，只有各节点遵循共识机制，区块链网络才能够正常运行。因此，共识算法被称为区块链的“经脉”，算法的效率越高，复杂度越低，区块链网络的性能就越好。除此之外，共识算法还影响了区块链的资源消耗。网络中的节点在实现算法的过程中往往需要提升硬件配置，以便进行快速计算。最初，节点采用 CPU 执行算法，而随着算力需求的增加，CPU 资源投入越来越大，且 CPU 需要很强的通用性来处理各种不同的数据类型，同时支持逻辑判断引入的大量分支跳转和中断处理。这些都使得 CPU 的内部结构异常复杂。GPU 面对的则是类型高度统一且相互无依赖的大规模数据的纯净的计算环境。一些共识算法更适合用 GPU 这种大规模并行的处理器来处理，如人们采用 GPU“矿机”参与比特币的挖矿过程。但是，算力的提升并未解决计算资源成本与回报不成正比这一问题，导致大量的计算资源浪费。未来节点算力仍呈上升趋势，若不对共识算法加以优化，反而一味地优化硬件，只会使得成本越发昂贵。

同时，算力提高的另一个代价是电能的消耗。硬件实现了算力，而电能维持着硬件的工作。随着算力的不断提高，如果不提高硬件性能，那么能耗自然会提升。即使优化了硬件，算力的提升与区块链的普及仍会使得电能消耗变高。对于能耗，究其根本是来自共识算法的大量无用计算。因此，未来的共识算法应对计算方式进行优化，以避免大量的无用计算耗费电能。

目前共识算法需要一个能衡量其执行效率的指标，用于评价共识算法设计的优劣。效能原指事物所蕴藏的有利的作

用，可以引申为事情的效率与效果，相应地，共识算法的效能指共识算法对区块链系统的效率与效果。再结合前文所述的3个区块链的效率影响因素（共识算法的性能、资源消耗与能耗），我们可以将共识算法的效率指标定义为共识算法性能，同时定义共识算法的效能为“在正确性和有效性的前提下计算共识算法性能所需的资源和能源消耗”。高效能的区块链共识算法意味着在算法执行时尽量消耗较少的计算资源和电能并获得较好的性能。效能的定义指出了性能、资源、能耗与算法效能之间的关系，即资源花费越小、性能越好、能耗越低的共识算法效能越高。这3个因素之间彼此也存在着定性或定量的联系。首先，在资源与能耗之间，计算资源投入得越多，能耗就越高。绝大部分资源的花费用于硬件，而能耗的来源也是硬件，当硬件花费增加时，在算力相同的情况下，单位时间内所消耗的能源也越多。其次，在性能与能耗之间，性能的优化会降低能耗，当然这并不是绝对的，目前也有部分优化是将能耗用于有用的计算之中，这虽然不会降低能耗，但是也一定程度地优化了性能，即相同资源量下性能越好，执行时间越短，能耗就越低。最后，在性能与资源之间，资源花费的减少带来了硬件的提升，而硬件的提升也使得区块链的网络性能更加稳定，因此大部分资源花费减少的情况会优化性能，但少部分共识算法的资源投入和性能提高不成正比。这3个因素互利共生，且三者也是影响共识算法效率与作用效果的直接因素，因此本文将其定义为共识算法的效能。

2.2 优化分类

前文定义了区块链共识算法的效能，并分析了共识算法效能的影响因素以及它们之间的关系。本节将对效能优化进行具体分类。

若按照区块链的种类进行分类，不同类型的区块链应用的共识算法类型是不同的，其效能优化方式与优化程度也有所不同。在公有链中，由于其公开透明的特性，因此会发生恶意节点入侵的情况。公有链采用的共识算法多为算力要求高、安全性高的算法，如PoW，PoS，因此其在效能上具有较大的提升空间。联盟链相比公有链有着更高的权限要求，即消耗更少的能耗，拥有更少的节点，因此对性能与安全的要求更高，效能也更高。但联盟链是部分去中心化的，在共识上相比公有链也有所差别。而私有链由于其高权限，且没有拜占庭错误出现，因此在私有链中很少出现共识的情况。因此，共识算法的效能优化主要体现在公有链与联盟链上。本文第3节和第4节将按2.1节中的效能影响因素介绍公有链和联盟链的效能优化方法。

3 公共链优化方法

根据前文的定义，公有链的效能优化可分为3个部分，而公有链共识算法的效能优化正逐步成为共识算法优化的研究热点。在3个因素中，目前性能优化是学术界研究得最多的，而资源优化是三者中研究得最少的。

3.1 资源优化

资源分为很多种，如硬件资源、软件资源、自然资源和社会资源，这些资源在共识算法中均起到了重要的作用，同时也是衡量共识算法设计是否优良的指标之一。本节将对公有链共识算法效能的资源优化进行总结。

所有资源中，最重要的是节约社会资源，即降低成本与花销。公有链的开销很大，目前已有学者开展了此方面的优化研究。为了减少电力资源浪费，Dong等[2]设计了一款dApp：Proofware，以便利用现有的基于公共/人群的计算资源轻松地构建其dApp。基于此App，他们又设计了新的共识算法PoUW。该新算法并非依赖于一个集中的会计制度，而是每个dApp都有一个嵌入式货币系统，以保持整个激励系统的分散、公平、透明、稳定和可持续。在仿真实验中，Dong等将该App与Amazon EC2进行了对比，结果显示，基于PoUW算法的App的运行开销仅为Amazon EC2运行开销的5.4%，远远降低了电力成本。

当前基于共识算法资源优化的研究相对较少，由于公有链的能耗较高，而能耗归根结底来自硬件，如PoW算法，目前的硬件最大算力可达每秒数亿亿次，未来这个数值还会继续上升，因此未来会对公有链共识算法的硬件进行继续优化。

3.2 性能优化

在公有链中，共识算法的效率饱受诟病。本节按照优化方法，对当前的算法效率优化研究成果进行分类，如表2所列。

表2 公有链性能优化文献总结

Table 2 Summary of public chain performance optimization literature

文献	算法名称	优化方法	性能优化结果
[3]	MPoW	优化Hash算法	节省30%的挖矿时间
[4]	PoM	优化Hash算法	10000次挖矿，最后只有3次共识出空区块，且从未发生分叉
[5]	QoS	投票机制	12个区域的网络，每秒可以达到9.7KTPS
[6]	不确定不串通的投票协商机制	投票机制	理论分析，减少错误选举且避免贿赂选举
[7]	PoT	信任证明机制	有效降低了节点带来的网络时延，大大降低了共识时延
[8]	PoN	信任管理	个块创建中比传统的共识机制更有效
[9]	TCON	量化信任	相比PoW能源消耗更少且性能更佳
[10]	RSF	博弈	能源与钱财消耗更少，且安全性更高
[11]	两阶段博弈论模型	博弈	有效增加吞吐量，公平性更高
[12]	MinMax	拓扑结构	有效增加了网络的吞吐量
[13]	DLatice	有向无环图	缩短了公有区块链的达成共识时间

3.2.1 优化PoW算法的Hash算法

该方法主要基于PoW的SHA256哈希算法进行优化，以提高计算效率与网络性能。Zeng等[3]提出了一种基于PoW的MPoW算法。该算法对原有PoW算法的SHA256哈希算法进行了优化，并将哈希表转化成满足自己定义的两个标准的矩阵运算，为利用矩阵的性质并实现高效、安全的区块链共识提供了一种新方法。在仿真实验中，该算法相比Hash算法最多可节省30%的挖矿时间，有效地提高了效率。针对目前公有链共识机制的去中心化程度不高和容易临时分叉的问题，Yu等[4]提出了一种基于哈希随机选主的最小值证明共识机制（PoM），PoM的空区块结构如图1所示。在PoM中，Yu等利用哈希算法的强混淆性来提高去中心化程度，同时还利用哈希算法的抗碰撞性来降低临时分叉的概率。在仿真实验中，他们共设计了211个矿工来模拟挖矿，并连续进行10000次挖矿。最后只有3次共识出空区块，且从未发生分

叉，增强了算法的去中心化程度，也证明了该算法具有良好的可行性。

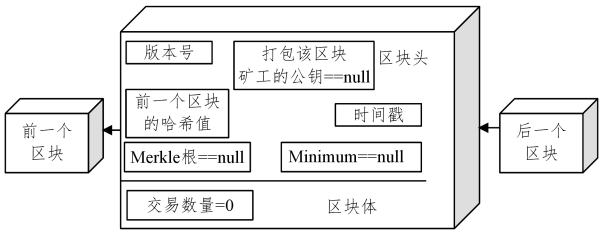

图 1 PoM 的空区块结构

Fig. 1 Empty block structure of PoM

3.2.2 修改共识选取机制

在公有链共识算法中，达成共识与选取节点的方式十分重要。通过优化选取节点的方法，可以尽可能地避免贿赂矿工与恶意节点侵入等恶意情况的发生。对共识算法的共识选取机制进行优化也是一种很常见的方式，而且人们还会采取不同的方法进行具体优化。

(1)投票机制

该方式通过投票表决的方式选取出节点。在常见的共识算法中，DPoS 采取的也是投票共识方式。Yu 等[5]针对 PoW 算法具有的吞吐量局限这一特点，提出了基于服务质量(QoS)的区块链共识协议。该协议对原有的网络进行区域性划分，并在每个区域内通过区域投票机制选取节点来统一进行 BFT 共识。仿真实验显示，对于 12 个区域的网络，该协议每秒可以达到 9.7KTPS，相比 PoW 有了很大的提升。Wang 等[6]基于原有共识算法中可能出现的错误选举或贿赂选举等情况，提出了一种新的不确定不串通的投票协商机制。该算法采用了投票机制与可信度评价算法。前者可以减少错误选举，并权衡选举的公平与效率；后者则通过激励相容评分准则来避免贿赂选举。

(2)增加信任度管理

在共识过程中，目前人们采用“信任度”来衡量节点，以尽可能地避免出现贿赂矿工的情况。Huang 等[7]提出一种基于动态授权的信任证明机制(PoT)，该机制将不同节点进行区分，并对创建区块赋予信任度，信任度越高，上链几率就越大。仿真实验的结果表明，本机制有效地缩短了节点带来的网络时延，同时也大大缩短了共识时延。传统的公有链中会出现贿赂矿工与攻击矿工等对区块链不利的情况。针对这一状况，Feng 等[8]提出了一种协商证明机制(PoN)。该机制引入了信任管理制度来评判矿工的可信度，使得每一次创建区块都是随机且诚实的，并将矿工团队划分为一定数量的组，使其可以同步或异步地实现挖矿过程。仿真结果表明，PoN 在逐个块创建中比传统的共识机制更有效，且在创建块时 PoN 算法相比传统共识机制更有效。Prabhakar 等[9]基于物联网框架设计了商业式轻量级信任依赖共识机制(TCON)，这是学术界首次对信任进行量化。在该机制中，Prabhakar 等首先使用 SmartContract 为资源的物联网设备提供隐私安全保护，然后通过对信任进行量化来实现区块链共识机制的商业化。仿真实验的结果表明，该机制相比 PoW 能源消耗更少，且性能更佳。文献[3]也使用了可信度评价方法，以尽可能地避免出现贿赂情况。

(3)采用博弈方式

在公有链中会出现恶意节点攻击区块链的情况。为了避免恶意节点在共识过程中的恶意侵犯，可以采取博弈的方式，经过层层博弈之后才可参与记账。通过这种方式，恶意节点侵入的几率呈指数级下降，因此当前有一些公有链优化算法采用此方式进行优化。Kim 等[10]以生活中的博弈方式“剪刀石头布”为模型，设计了一种新的共识算法 RSF，并基于“剪刀石头布”中的 3 种静态平衡状态——“剪刀”石头”“布”，以及 3 种平衡状态之间的竞争关系，实现了常规算法的博弈共识过程，算法的具体流程如图 2 所示。同时，该方式也尽可能地阻止了恶意节点的入侵，该算法可以在由多个用户组成的区块链网络中有效地工作。通过与常规算法 PoW 与 PoS 进行对比发现，RSF 耗费的能源与钱财更少，且安全性更高。文献[11]提出了一个两阶段博弈论模型。在该模型中，每个时间段的总交易被划分为一个碎片，通过议价的方式为基于碎片的共识问题提供一个基于公理的战略解决方案，同时动态地响应当前的区块链网络环境。仿真实验结果表明，该算法不仅可以有效增加吞吐量，而且相比其他共识算法，其公平性更高。

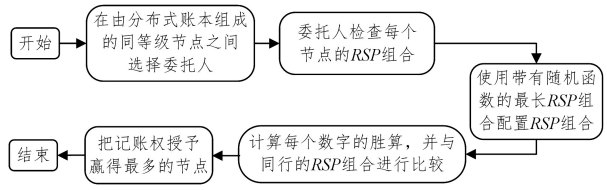

图 2 RSF 算法的执行过程

Fig. 2 Execution process of RSF algorithm

3.2.3 其他优化方式

除上述几种常见的优化方式外，还有一些特殊的优化方式。文献[12]提出了一种 MinMax 算法，用于解决动态网络的稳定共识问题，其能解决稳定共识问题的原因是其拓扑结构具有很强的动态性，并且不具有强连通性。仿真实验结果表明，该算法有效地增加了网络的吞吐量。文献[13]提出了一种新式双有向无环图体系的算法结构(DLatice)。该算法为无许可算法，每个账户均有自己的有向无环图，且所有账户又形成了一个有向无环图。该算法采用了一种新的只在用户间达成共识的 DPOS-BA-DAG 协议。仿真实验结果表明，该算法使得区块链在 10 s 内即可达成共识，大大缩短了公有区块链达成共识的时间。

3.3 能耗优化

在公有链中，用户需要通过投入大量的算力来争夺记账权，因此耗费了大量的电能。能耗作为效能的影响因素之一，是对算法性能与系统硬件性能进行评测的最好指标。因此，本节将按照优化方法对当前已有公有链共识算法能耗优化的研究成果进行梳理。

目前在公有链算法资源优化方面的研究是针对 PoW 的高能耗进行的优化。

人们可以对共识过程中的不同步骤进行优化，首先可以从奖励机制上进行优化。奖励机制是公有链的一种重要的记账方式，通过对记账者进行奖励，促使人们参与到记账行列中，从而直接推动交易的进行，间接维持区块链的平稳运行。文献[14]提出了一种基于门限群签名理论的保证金模型

(TCCM)。在该模型中,Wang 等[14]首先建立了保证金模型,通过抵押保证金来抑制节点的拜占庭行为,并利用门限群签名技术来提高保证金的安全;其次建立了记账权竞价模型,即新的奖励机制,通过参与共识的节点之间的相互竞价来产生区块链的记账节点,同时利用多方参与决策来抑制拜占庭节点的恶意行为;最后设计新的共识机制的区块构造方式与初始化方式,进行区块检验。在 TCCM 中,共识算法的能耗从 PoW 的高能耗降至了低能耗,而且在时间开销上,从 PoW 的 10 min 一次缩短至不到 1 min 一次,实现了对共识算法能耗的降低。

其次,可以对交易机制进行更新优化。公有链的应用主要面向新型的数字货币系统,在数字货币中交易机制的好坏直接决定了该数字货币的价值。文献[15]提出了一种新的共识算法,即联邦学习证明(PoFL),该共识算法提出了一种基于反向博弈的数据交易机制,用于解决公有链中训练集的泄露问题。在模型验证时,通过已有数据可明显看出,该方法可降低共识算法的能耗,从而节约能源。

然后,还可以通过设计新的共识原语来进行优化。区块链的原语不同于操作系统的原语,其强调一种"动机",是由密码学衍生而来的。例如,比特币系统中的核心原语就是签名算法与哈希算法。而在区块链中,原语依托的是共识算法。一般来说,高安全性的原语所需的资源也更多,如比特币系统的哈希算法,依靠的是极大的算力支持,但是这也导致了比特币系统的耗能严重。Milutinovic 等[16]通过设计新的共识原语,既提高了区块链执行事务的效率,又节约了能源,并提出 3 个启用 TEE 的、使用现有工作证明方案的、系统的建块设计方案,即支持 TEE 的工作证明、时间证明和所有权证明;之后 Milutinovic 等重新设计了原语,将原语的使用范围扩展至既具有时间证明,又具有所有权证明;最后基于以上改进,文献[16]提出了新的 PoL 共识算法,并在设计新算法时对该算法的能耗进行了估计。结果显示,该算法可使采矿变得有效,从而减少能源消耗。

最后,有学者结合其他共识算法的计算能力来优化 PoW 算法。Yang 等[17]将 PoW 算法的计算能力引入 DPoS 中,并通过进一步的修改,减小了计算资源和利害关系对生成区块的影响,以便在协商一致过程中实现更高的效率、公平和权力下放,从而得出新算法 DDPoS。然后,Yang 等提出了一种降级机制来快速替换恶意节点,进而提高安全性。最后,其通过仿真实验证明了该算法可以有效地降低能耗,且在性能上优于 PoS 与 PoW,实现了能效的提高。

极少数的基于 PoS 的节能优化算法采用创建可靠的长期共识的方法来进行优化。文献[18]提出了一种新型优化算法,其利用初始设施的引导,在初期实现公平分布的挖掘,从而实现长期的共识,进而节省能源。

由此可见,目前基于 PoW 算法的能耗优化研究较多,且优化方式多样化。随着区块链的发展,共识算法的能耗问题日益明显,而对能耗较大的共识算法的优化也迫在眉睫。基于当前社会节能的大趋势,未来公有链共识算法的能耗优化也将成为热点话题。

4 联盟链优化方法

目前联盟链的应用也获得了不错的成果,如超级账本 HyperLedger 和蚂蚁金服,联盟链也因监管友好等特点逐渐成为各行各业步入区块链的首选链型。但是联盟链和公有链一样,都可能受到恶意节点的入侵,且由于其较高的性能要求,其效能也需要优化。

4.1 资源优化

第 2 节提到了公有链与联盟链之间的优化差别,其中在资源开销上,公有链比联盟链的资源开销大得多。因此,仅从节省资源开销的角度来看,人们对联盟链的共识算法的研究要少于对公有链的共识算法的研究。

Wang 等[19]认为 PBFT 算法不能有效地激发可靠节点的积极性,而且大量的通信资源被用于达成共识。基于此,他们提出了一种授予信誉的拜占庭容错算法(CDBFT)。该算法提出了一种投票奖惩方案及对应的信用评价方案,以便在激发可靠节点的积极性的同时减少异常节点参与共识过程,从而建立系统的良性循环。此外,该算法还提出了基于 PBFT 的一致性和检查点协议,以提高系统的效率和灵活性。在仿真实验中,共识过程中异常节点的参与概率可以降低到 5%,同时通信的资源开销也有所降低。

资源优化一直是区块链的研究目标,而通过优化共识算法来降低资源开销的研究仍然很少,希望在未来研究者们更多地关注共识算法的资源优化。

4.2 性能优化

联盟链共识算法的工作可分为 3 步:选取记账权、划分节点和验证,如图 3 所示。联盟链的性能优化可从以上几个方面展开,相关研究成果如表 3 所列。

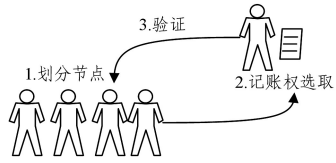

图 3 联盟链共识算法的基本工作流程

Fig. 3 Basic workflow of alliance chain consensus algorithm

表 3 联盟链性能优化研究成果总结

Table 3 Summary of alliance chain performance optimization literature

文献	算法名称	优化方法	性能优化结果
[20]	K-medoids	聚类划分节点	有效地加速共识进程
[21]	Proteus	选取根委员会	无论网络中遇到多少故障数,Proteus 都能提供一致的性能
[22]	EROC	可验证的随机函数	13 s 内可以对 30 个 2 M 大小的区块进行共识
[23]	FRChain	多播树集体签名	有效地扩展事务吞吐量与网络性能
[24]	PBCM	双层链,主从多链	提高交易吞吐量
[25]	ELGamal	环签名	较好地解决网络中节点动态加入退出问题
[26]	SDVP	有向无环图	TPS 在 600～1 400 之间
[27]	Gosig	协议层多轮投票与实现层优化相结合	每秒可实现超过 4 000 个事务,且交易确认时间短于 1 min
[28]	CloudPBFT	结合云计算的基本原理	节点数目在 40 以内时,该算法可有效降低时延

4.2.1 优化节点划分方式

在共识机制中,对节点的划分非常重要。将节点按照一

定规则进行划分后，再进行记账权的选取，是避免恶意节点入侵的有效方式。Chen 等[20]基于 K-medoids 聚类算法对参与共识的大规模节点进行聚类划分，并将改进的多中心化 PBFT 应用于这种聚类后的分层模型中，聚类后的区块链结构模型如图 4 所示。为了使聚类更准确，Chen 等[20]进一步改进了 K-medoids 聚类算法，最终提出了 K-PBFT 算法。基于该模型，他们还进行了网络拓扑仿真环境实验，即通过 NS2 配合 GT-ITM 拓扑生成器进行仿真实验。实验过程中，通过 20 次重复对比 PBFT 与 K-PBFT 的单次共识平均时长，得到结果为：PBFT 单次共识的平均耗时为 580.7 ms，K-PBFT 单次共识的平均耗时为 447.7 ms，有效地加快了原有算法的共识进程。Jalalzai 等[21]提出了一种新的基于 BFT 的 Proteus 共识协议。该算法选择全部节点中的一个子集作为根委员会，并用少部分节点调节所有节点的共识。在 AmazonEC2 上对 200 个节点进行测试，实验结果表明，无论网络中遇到多少故障数，Proteus 都能提供一致的性能，而其他 BFT 协议因网络中的故障数达到阈值而导致性能下降。

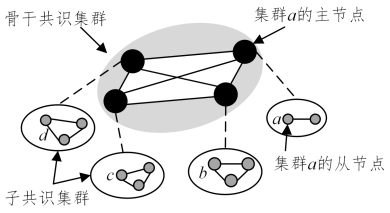

图 4 执行聚类算法后的区块链模式

Fig. 4 Blockchain mode after clustering algorithm is executed

4.2.2 优化验证方式

共识机制中，对节点进行验证处理可以加强区块链的保密性与安全性。在现有联盟链算法优化研究中，有部分是针对节点的验证方式进行优化的。Zhong 等[22]针对当前共识机制的高延迟与倾向中心化等问题，提出了具有分散属性的 EROC 共识算法。在该算法中，Zhong 等使用可验证的随机函数(VRF)对分区进行加密，并将投票与区块在系统中进行广播，由用户进行验证，得到大多数选民投票的区块将被成功共识。仿真实验结果显示，该算法在 13 s 内可对 30 个 2 M 大小的区块进行共识，从而有效地提升了共识机制的效率。为了解决封闭业务环境下无许可区块链的替代问题，Chander 等[23]开发了 FRChain 共识协议，该协议适用于许可链，并且具有可扩展与高性能的优点，其通过在多播树上进行集体签名来实现区块的验证与传播。在仿真实验中，Chander 等选取多个数据中心进行测试，测试结果表明该协议可以有效扩展事务吞吐量与网络性能。Min 等[24]提出了许可链多中心动态共识机制(PBCM)。在该结构中，Min 等设计了两层区块链结构，以构建主从多链，并通过全局区块链链接多个主体区块链。同时，该算法会生成动态验证节点集，以保证数字化资产的全局一致性。该算法还通过引入全局区块与主体区块来实现交易分流，以提高交易吞吐量。Fang 等[25]在环签名理论、ELGamal 数字签名算法与 PBFT 算法的基础上，提出了一种新式 PBFT 算法。该算法对环签名算法进行安全性分析，运用环签名方案来改进 PBFT 算法的签名及验证过程，并对区块链测试框架 Calipier 进行改进测试。在仿真实验中，Fang 等选取了多个节点的不同组合进入网络，并模拟节点动态进入网络的过程。实验结果表明，基于环签名方案的改进 PBFT 共识算法可较好地解决网络中节点动态加入退出的问题，且能够达到原 PBFT 算法的拜占庭节点容错率。

4.2.3 优化记账权选取方式

与公有链共识选取节点的方式类似，联盟链也可以采取一定措施对选取节点的方式进行优化，例如目前，人们通过引入投票机制来对联盟链算法进行优化，如 Cao 等[26]提出了一种 SDVP 共识模型。传统的区块链中的链状结构和挖矿过程增加了交易的延迟，从而使得每秒的交易数量(TPS)减少。针对以上情况，Cao 等通过引用有向无环图结构与基于投票的 PBFT 算法，显著提高了事务生成、验证与处理效率。仿真实验结果表明，该模型的 TPS 在 600～1 400 之间，有效地提高了原有算法的处理效率。Li 等[27]针对 BFT 在联盟链中面临的挑战，提出了基于协议层多轮投票与实现层优化相结合的Gosig 共识算法。该算法保证了系统的安全，即使在一个由对手完全控制的网络中也可以同时提供可证明的活性。在仿真实验中，Li 等在 AmazonEC2 服务器上构建广域实验平台。实验结果表明，该算法每秒可实现超过 4000 个事务，且交易确认时间不到 1 min。

4.2.4 其他优化方式

除以上 3 种常见方式外，当今还有其他方式可对联盟链的共识算法进行优化。Zhou 等[28]根据云计算与区块链的技术特点，融合二者各自的优势，给出了物流区块链和云物流区块链的定义，并提出了基于云计算的物流区块链模型(Cloud-PBFT)。该模型结合 PBFT 算法与云计算的基本原理，实现了对区块链的去中心化与不可抵赖性。在仿真实验中，分别选取 0，20，40，60，80 个节点进行时延检测。实验结果显示，当节点数目在 40 个以内时，该算法可有效降低时延。

4.3 能耗优化

在联盟链中，由于拜占庭问题的存在，共识算法必须通过一定的机制来抑制恶意节点的入侵，这也导致了共识算法能耗高的问题。目前研究者们已从多方面对联盟链的能耗优化进行研究。Dai 等[29]针对当前主流共识机制仅奖励那些拥有主要利益的节点的现象，提出了价值证明机制(Proof-Of-Value)。该机制为一种新型奖励机制，奖励所有创造价值的用户。在该机制中，Dai 等通过一种激励系统调整算法来奖励创造价值与控制价值的用户，并设计了一个脱离链的事务系统——Hypernet。测试结果表明，该系统算法的损耗仅为 2%，且性能是传统许可链系统性能的 4 倍，有效地提升了性能且降低了消耗。Li 等[30]针对当前公有链共识机制不足以部署新兴联盟链的问题，提出了一种投票证明算法(Proof-Of-Vote)。该算法的共识过程由联盟链中的合作者控制的分布式节点进行表决。该表决机制为网络中的投票参与者建立不同的安全身份，因此在区块验证与提交时，无需第三方中介，完全由机构的投票结果决定。在仿真实验中，通过与 PoW 算法进行对比发现，POV 具有安全性与可靠性高、能耗低、处理事务的延迟低、链不会分叉等优点。Puthal 等[31]引入密码认证机制，提出了认证证明算法(Proof-of-Authentication)。该算法基于 PoW 算法进行了改进，改进后适用于许可链与私有链，其加密身份验证机制补足了 PoW 因设备资源限制而无法实现对加密身份的验证的缺陷。PoAh 算法保持了系统的可

持续性与可扩展性，并且可以在物联网与边缘计算的区块链集成中使用。仿真实验结果显示，该算法降低了计算机的延迟，且减小了能耗。

5 共识算法资源共享问题

作为分布式系统，区块链也可以实现信息的资源共享。区块链的资源共享主要遵从无中心模式，又可细分为规模扩张模式与跨链模式[32]。目前区块链的资源共享是通过通信网络的相互连接来进行的，而在共识过程中，各个节点的信息资源是不予共享的。共识过程中，信息的获取是基于网络的广播，如交易的确认、区块的验证。目前区块链中的资源共享机制也存在缺陷，这些缺陷可以通过改善共识机制来进行优化。

5.1 多链资源共享

多链，即抛弃了“一链治所有”的传统方案，采用“一链一合约”的新方案重新设计了一个保证每个合约都能正常运行的公链。设想一下，若将区块链应用到支付中，每秒交易请求高达几万次，每日交易数高达几亿笔，用户交易达到秒级响应体验，而单链区块链无论在性能还是存储上都具有局限性。因此，多链这一创新极大地简化了架构，降低了数据处理压力，确保一条链上的流量激增不会影响到另一条链的效率，在链上进行的任何业务都不会受到其他业务的干扰，从而有效地实现了资源隔离。

目前市面上已有成型的多链技术——EKT 多链技术。EKT 多链技术生态是一个并行多主链的结构，其采用“多链多共识”的方法进行共识过程，EKT 主链采用 DBFT 算法，目前其余基于 EKT 生成的主链也采用 DBFT 算法，未来还会陆续支持 PoW 和 PoS 等主流算法。由于多链系统的资源隔离，多个主链之间在资源共享上也会存在一定的瓶颈，并且在加入主流算法后，多主链的效能好坏也是一个问题。因此，根据前文所述，在今后的多链共识算法中可以采用优化效能的共识算法，其首先可以提高效能，其次通过对硬件的共享实现 Shared something，从而实现跨主链的资源共享。

5.2 跨链资源共享

首先，区块链中信息交易速度较低，且公链中的交易速度远远低于私有链与联盟链，这在大规模的信息资源共享环境中易形成瓶颈。这一点可以通过改善共识算法来进行优化，如 PoW 算法通过复杂的数学计算来防止恶意节点入侵，但导致了共识算法的效率降低与计算资源的浪费。因此，出现了大量的新型共识算法来解决区块链中交易验证效率低下的问题，如容量证明算法 PoC 和授权拜占庭容错算法 dPBFT 等。

其次，目前共识算法主要采用 Shared nothing 架构，这使得区块链中各节点相互独立，各自处理自己的数据，处理后的结果可能向上层汇总或在节点间流转，因此并行处理和扩展能力更好。这样的架构虽然效率高，但是由于每个节点都需要独立的硬件，因此高昂的成本成为了这种架构的缺点。而且如果要访问所有的数据，必须所有节点都可用，这也是目前区块链存在的问题。

针对以上问题，结合本文的共识算法效能优化问题，可以在资源、能耗、性能之间通过定量比较来达到最大效能，即消耗多少能源、花费多少资源可以得到尽可能高的性能。而基于现有的 Shared nothing 架构，可以通过实现 Shared something 来在某些硬件或软件资源上实现共享，从而达到定量比较的最高性能。因此，未来在共识算法的资源共享问题方面，Shared something 与共识算法效能的结合会成为一个热点话题。

5.3 区块链即服务的资源共享

“区块链即服务”(BaaS)[33]，指利用区块链产生的数据，提供基于区块链的搜索查询、任务提交等一系列操作服务。在区块链即服务的模式下，区块链协议被用于维护基础的完全去中心化的分布式平台。

目前的 BaaS 应用是在公有链上开发的，而且只有各大公链的区块浏览器可以称为 BaaS 应用。由于 BaaS 应用为公链应用，其采用的共识算法也为公有链共识算法，在资源共享模式上采用 Shared nothing 架构。基于前文的描述，公有链共识算法在资源与能耗上均饱受诟病，且 Shared nothing 架构依旧存在效能方面的问题。因此，结合影响共识算法效能的 3 个要素，可以通过实验得到三者之间的定量关系，从而达到效能最大化，实现对能耗、资源和性能的三重优化。

结束语 本文对共识算法的效能优化研究进展进行了总结分析，首先给出了区块链共识算法效能的定义，并根据该定义介绍了 3 个影响共识算法效能的因素——资源、能耗和性能。其次，说明了三者对效能的影响以及三者之间的关联。然后，按照公有链与联盟链的分类，结合当前已有的研究文献，对每一种影响算法效能的因素按照优化方法进行分类总结。最后，从多链区块链、多个区块链与 BaaS 3 个方面提出了相应区块链的共识算法资源共享问题。共识算法作为区块链最重要的技术，其效率与执行效果对区块链的影响巨大。目前区块链处于研究的上升阶段，而共识算法的相关研究有限，因此希望本文能为研究者们提供参考与启发。

参 考 文 献

[1] LAMPORT L, SHOSTAK R E, PEASE M, et al. The Byzantine Generals Problem [J]. ACM Transactions on Programming Languages and Systems, 1982, 4(3): 382-401.

[2] DONG Z L, LEE Y C, ZOMAYA A Y. Proofware: Proof of Useful Work Blockchain Consensus Protocol for Decentralized Applications [J]. arXiv: 1903.09276, 2019.

[3] ZENG L, XIN S, XU A, et al. Seele's New Anti-ASIC Consensus Algorithm with Emphasis on Matrix Computation [J]. arXiv: 1905.04565, 2019.

[4] YU B G, GONG S M, PANG X Q, et al. Fair and Efficient Consensus Mechanism: Proof of Minimum[J]. Computer Engineering and Applications, 2020, 56(1): 63-68.

[5] YU B, LIU J, NEPAL S, et al. Proof-of-QoS: QoS based blockchain consensus protocol [J]. Computers & Security, 2019, 87(11): 101580.1-101580.13.

[6] WANG S L, QU X D, HU Q, et al. An Uncertainty and Collusion-Proof Voting Consensus Mechanism in Blockchain [J]. arXiv: 1912.11620, 2019.

[7] HUANG J H, XIA X, LI Z C, et al. Proof of Trust: Mechanism of Trust Degree Based on Dynamic Authorization [J]. Journal of Software, 2019, 30(9): 2593-2607.

[8] FENG J Y, ZHAO X Y, CHEN K X, et al. Towards random-

honest miners selection and multi-blocks creation: Proof-of-negotiation consensus mechanism in blockchain networks [J]. Future Generation Computer Systems, 2020, 105: 248-258.
[9] PRABHAKAR A, ANJALI T. TCON－A lightweight Trust-dependent Consensus framework for blockchain [C]// 11th International Conference on Communication Systems & Networks. New York: IEEE, 2019: 19-24.
[10] KIM D H, ULLAH R, KIM B. RSP Consensus Algorithm for Blockchain [J]. Journal of the Institute of Electronics Engineers of Korea, 2019, 56(8): 39-44.
[11] KIM S W. Two-phase Cooperative Bargaining Game Approach for Shard-based Blockchain Consensus Scheme [J]. IEEE Access, 2019, 7: 127772-127780.
[12] CHARRONBOST B, MORAN S. MinMax Algorithms for Stabilizing Consensus [J]. arXiv: 1906. 09073, 2019.
[13] ZHOU T, LI X F, ZHAO H. DLattice: A Permission-Less Blockchain Based on DPoS-BA-DAG Consensus for Data Tokenization[J]. IEEE Access, 2019, 7: 39273-39287.
[14] WANG Z, TIAN Y L, YUE C Y, et al. Consensus Mechanism Based on Threshold Cryptography Scheme [J]. Journal of Computer Research and Development, 2019, 56(12): 2671-2683.
[15] QU X D, WANG S L, HU Q, et al. Proof of Federated Learning: A Novel Energy-recycling Consensus Algorithm [J]. arXiv: 1912. 11745, 2019.
[16] MILUTINOVIC M, HE W, WU H, et al. Proof of Luck: an Efficient Blockchain Consensus Protocol [J]. arXiv: 1703. 05435, 2016.
[17] YANG F, ZHOU W, WU Q Q, et al. Delegated Proof of Stake With Downgrade: A Secure and Efficient Blockchain Consensus Algorithm With Downgrade Mechanism [J]. IEEE Access, 2019, 7: 118541-118555.
[18] AHMED M, KOSTIAINEN K. Don't Mine, Wait in Line: Fair and Efficient Blockchain Consensus with Robust Round Robin [J]. arXiv: 1804. 07391, 2018.
[19] WANG Y H, CAI S B, LIN C L, et al. Study of Blockchains's Consensus MechanismBased on Credit [J]. IEEE Access, 2019 (7): 10224-10231.
[20] CHEN Z H, LI Q. Improved PBFT Consensus Mechanism Based on K-medoids [J]. Computer Science, 2019, 46(12): 101-107.
[21] JALALZAI M M, BUSCH C, RICHARD III G G. Proteus: A Scalable BFT Consesus Protocol for Blockchains [C]// 2019 IEEE International Conference on Blockchain. New York: IEEE, 2019: 308-313.
[22] ZHONG L, DUAN X H, WANG Y J, et al. eRoc: A Distributed Blockchain System with Fast Consensus [C]// International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery. New York: IEEE, 2019: 205-214.
[23] CHANDER G, DESHPANDE P, CHAKRABORTY S. A Fault Resilient Consensus Protocol for Large Permissioned Blockchain Networks [C]// 1st IEEE International Conference on Blockchain and Cryptocurrency. New York: IEEE, 2019: 33-37.
[24] MIN X P, LI Q Z, KONG L J, et al. Permissioned Blockchain Dynamic Consensus Mechanism Based Multi-Centers [J]. Chinese Journal of Computers, 2018, 41(5): 1005-1020.
[25] FANG Y, DENG J Q, CONG L H, et al. An Improved Scheme for PBFT Blockchain Consensus Algorithm Based on Ring Signature [J]. Computer Engineering, 2019, 45(11): 32-36.
[26] CAO K T, LIN F, QIAN C H, et al. A High Efficiency Network Using DAG and Consensus in Blockchain [C]// 2019 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking. New York: IEEE, 2019: 279-285.
[27] LI P L, WANG G S, CHEN X Q, et al. Gosig: Scalable Byzantine Consensus on Adversarial Wide Area Network for Blockchains [J]. arXiv: 1802. 01315, 2018.
[28] ZHOU J, LI W J. Research on logistics block chain consensus algorithm based on cloud computing [J]. Computer Engineering and Applications, 2018, 54(19): 237-242.
[29] DAI W Q, XIAO D S, JIN H, et al. A Concurrent Optimization Consensus System Based on Blockchain [C]// 26th International Conference on Telecommunications. New York: IEEE, 2019: 244-248.
[30] LI K J, LI H, HOU H X, et al. Proof of Vote: A High-Performance Consensus Protocol Based on Vote Mechanism & Consortium Blockchain [C]// 19th IEEE International Conference on High Performance Computing and Communications. New York: IEEE, 2017: 466-473.
[31] PUTHAL D, MOHANTY S P, YANAMBAKA V P, et al. PoAh: A Novel Consensus Algorithm for Fast Scalable Private Blockchain for Large-scale IoT Frameworks [J]. arXiv: 2001. 07297, 2020.
[32] ADAM B, MATT C, LUKE D, et al. Enabling Blockchain Innovations with Pegged Sidechains [EB/OL]. http://www. blockstream. com/sidechains. pdf.
[33] ZHU Y J, YAO J G, GUAN H B. Blockchain as a Service: Next Generation of Cloud Services [J]. Journal of Software, 2020, 31(1): 1-19.

ZHANG Peng-yi, born in 2000, postgraduate student. His main research interests include big data management and blockchain.

SONG Jie, born in 1979, Ph. D, professor. His main research interests include big data management, green computing and machine learning.