区块链共识机制综述

杨宇光　　张树新
（北京工业大学信息学部　北京　100124）
（yangyang7357@bjut.edu.cn）

Review and Research for Consensus Mechanism of Block Chain

Yang Yuguang and Zhang Shuxin
(*Department of Informatics*, *Beijing University of Technology*, *Beijing* 100124)

Abstract　Blockchain is the core supporting technology of the digital cryptocurrency system represented by Bitcoin, which can bring profound changes to finance, economy, science and technology and even politics. It integrates distributed systems, cryptography, game theory and other disciplines, thus established a new type of trust model. As the core of the blockchain technology, the consensus mechanism plays an important role in maintaining the stable operation of the blockchain system and mutual trust between nodes. In recent years, with the widely discussion of block chain technology, consensus algorithm has made considerable progress. This article first analyzed the application of the consensus mechanism and the problems to be solved by analyzing the core technology of the blockchain. Then we introduced and thoroughly analyzed the most representative consensus mechanism. We hope to provide ideas and lessons for the study of consensus mechanisms.

Key words　blockchain; Bitcoin; cryptography; consensus mechanism; distributed system

摘　要　区块链是以比特币为代表的数字加密货币体系的核心支撑技术，可以为金融、经济、科技甚至政治等领域带来深刻变革.它融合了分布式系统、密码学、博弈论等学科建立了一种新型的信任模型.共识机制作为区块链技术的核心，有着维护区块链系统稳定运行和节点相互信任的重要作用.近年来随着区块链技术的火热，共识算法较之前有了长足进步.首先通过分析区块链的核心技术引出共识机制的应用场景和要解决的问题，随后深入介绍了共识机制发展到目前为止代表性的算法并进行分析，希望能对共识机制的研究提供思路和借鉴.

关键词　区块链；比特币；密码学；共识机制；分布式系统

中图法分类号　TP309

1　比特币与区块链技术

2008 年，一位化名“中本聪”的学者以一篇《比特币：一种点对点的电子现金系统》的文章[1]，阐述了一种数字加密货币的实现思路.一年之后作者释放出了以论文为原型设计出来的加密货币——比特币[2].历经近 10 年的发展，比特币一直保持着

收稿日期：2018-03-15

交易量和市值全球第一的地位，与此同时，支撑比特币运行的核心技术——区块链——凭借去中心化、易验证、难篡改，已成为各国政府、国际组织关注的一个热点，许多金融巨头和研究机构纷纷在该领域投上宝贵的精力.各种区块链相关项目爆发式增长.对于区块链技术，目前普遍的观点是其对未来的改变是不可预估的.

1.1 比特币的工作原理

作为一个分布式的 P2P 网络系统.比特币没有运行中心，也没有管理员.比特币的来源是采矿.任何节点都能作为矿工，发挥自己的计算优势来验证和记录交易.并收到相应的报酬.

比特币的优势来自其发明以前的数字货币，如 b-money[3]和文献[4]的 hashcash，之前就已经创造了一个完全分散的电子现金系统，不依赖于货币的担保或结算交易验证，保证中央的权威.主要的不同点是使用了工作量证明机制(PoW)，使网络集中同步事务记录.巧妙地解决了一个核心问题——“双花”问题.在此之前，双重支付问题是数字货币的痛点，只能通过一个中心处理所有交易.

比特币的独创性表现在它为拜占庭将军问题提供了一种可行解.这是分布式计算中一个尚未解决的问题.简而言之，该问题就是想在一个低容错的异构网络上，通过信息传送达成行动的一致性比特币中的解决方案，可以在没有可信中央机构下达成一致行动，是分布式计算领域的一个进步，具有超越货币的广泛适用性.它可以实现公平选举、彩票、资产登记、数字公证等集中的网络中的共识.

1) 比特币交易

我们可以把比特币交易理解为复式记账中的每一行.在交易的一头是大于等于 1 个输入(input)，另一头是 1 个或者多个输出(output).输入之和输出之和不要求必须相等.相反，当输出略小于输入时，两者差额代表隐含的“矿工费”，这也是矿工将这笔交易记入账簿的 1 笔小额付款.如图 1 所示，描述了作为记账簿的比特币交易.交易中最常见的形式是从一个支付地址到另一个支付地址(P2PK)，输出中包含自己的地址是“找零”.

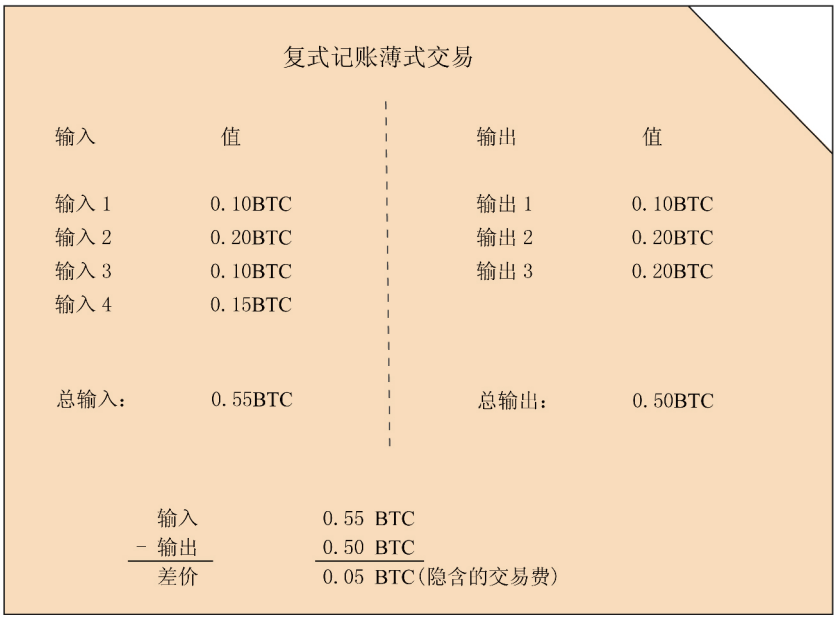

图 1 比特币交易

2) 比特币的密钥、地址、钱包

比特币所有权由 3 部分建立：付款地址、密钥和数字签名.出于安全原因，数字密钥不会在网络中流通，而是基于用户生成的公钥生成，并存储在一个文件或一个称为“钱包”的简单数据库中.数字密钥可以由钱包软件生成，独立于比特币协议而存在，并且可以离线生成.该密钥包含比特币的许多功能，包括分布式管理、所有权认证和基于加密的安全模型.

在交易数据包中，有一个特殊的字段专门存

储签名，并且有效的数字签名只能由被认可的数字密钥才能产生.因为在比特币交易的支付过程中，收款人是用比特币地址来标识的，签名作为验证的一个重要组成部分而存在.但并不是所有的收款地址都是公钥，除了 P2PK 之外的交易使用脚本作为支付对象.比特币地址可以通过单向加密哈希算法作用在公钥上获得，常用的算法是 SHA（secure hash algorithm）和 RIPEMD（the RACE integrity primitives evaluation message digest），特别是 SHA256 和 RIPEMD160.通常用户的比特币地址编码采用“Base58Check”.图 2 示出了如何从公钥生成比特币地址.

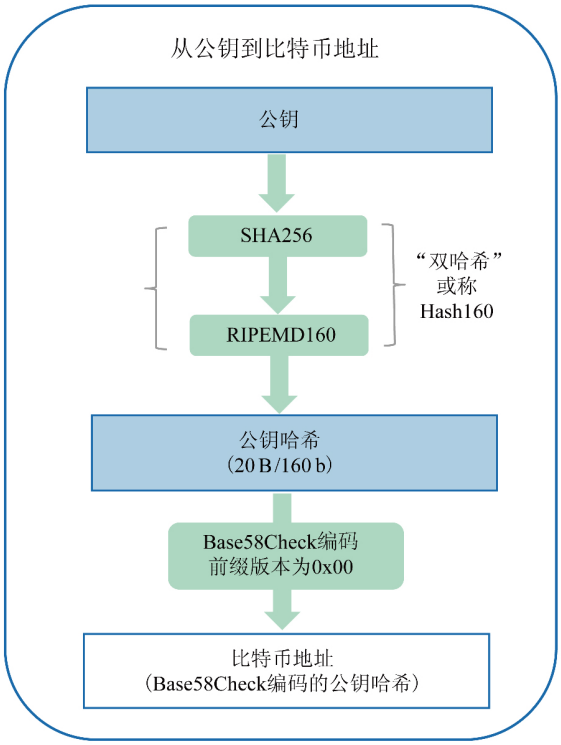

图 2　公钥到比特币地址

为了在网络传播中保证数据的准确，使用错误检查代号来检查转录中数据的错误.在数据前我们添加一个记录版本的字节作为前缀.例如，在比特币地址的前缀是 0（16 进制是 0x00），而私钥的前缀是 128（16 进制是 0x80）.因而结果变为 3 部分：前缀、数据和校验码.称之为 Base58Check 编码，图 3 描述了编码过程.

3）挖矿

挖矿是比特币系统中最有趣和值得研究的地方，比特币通过挖矿来产生，它还保证比特币的稳定、安全诚实的运行.矿工们在竞赛中胜出，获得记账的权利.把一段时间之内的交易验证通过，再添

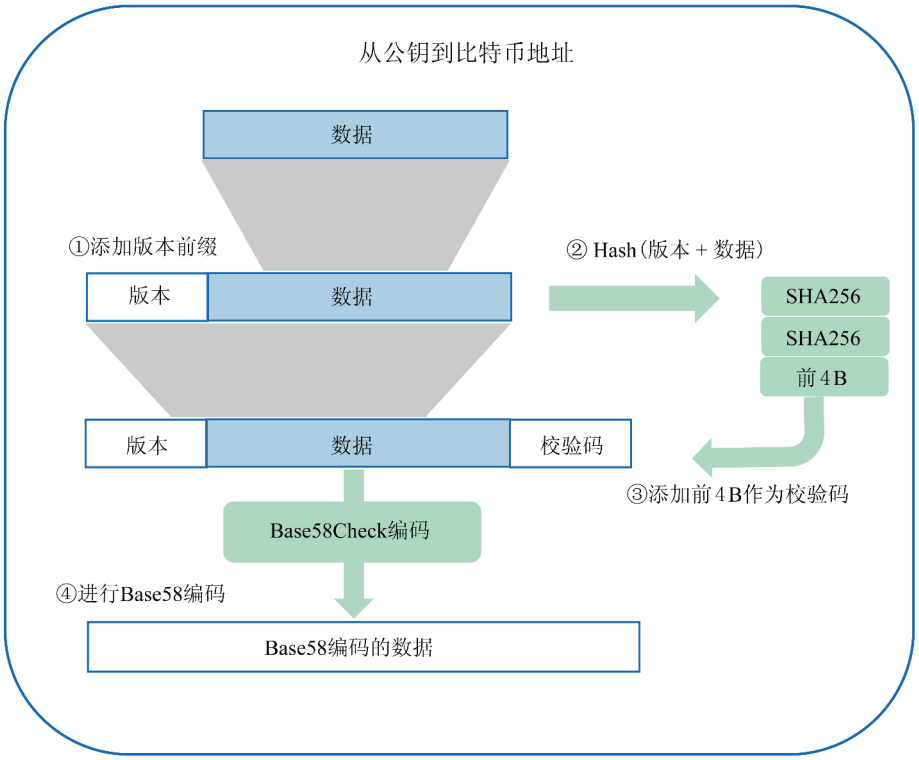

图 3　Base58Check 编码过程

加到链中.我们称“把交易包含在块中并添加到链中”作为“确认”交易.交易确认后,新所有者只能使用他们在交易中获得的比特币.矿工在采矿中获得2种奖励:创造一个新的区块的奖励,以及交易中所包含的交易成本.

个人认为“挖矿”一词有一定的误导性,从而让我们将注意力集中在奖励上,虽然挖矿会带来一部分奖励,但它主要的目的不是奖励本身,或者新币的产生,反而把手段当成了目的.挖矿是一个以结算为中心的过程,每一笔交易都要经过结算处理和检查.比特币挖矿保护系统在没有中央机构实施情况下也可以使比特币网络达成一致.它与我们主要讨论的共识机制有着千丝万缕的联系.

1.2 区块链技术

作为支持比特币服务的核心技术,区块链是一种基础设施,是加密货币或者其他应用的底层根本.它使用链式数据结构来验证和存储数据,并使用分布式节点协商机制来生成和更新数据.

根据不同的应用场景,区块链分为公共链、联盟链和专有链.

1)公共链.节点可以自由地连接和退出网络,参与链上数据的读写操作.目前,基于区块链的数字货币或智能合约平台属于公共链的范畴.

2)联盟链.其实现是在现实生活中有相应的组织结构,并通过授权节点加入和退出网络.组织形成利益相关的联盟,共同维护系统的健康运行,当前企业界更多关注联盟链的搭建和使用.

3)专有链.每个节点的写权限都是内部控制,读权限可以选择性地对外开放.专有链具有多节点操作的通用结构,适用于特定组织的内部数据管理和审计.

2 区块链技术的应用前景

与其在讨论某项技术的发展前景,不如说我们关注的是其作用方式.区块链最近几年热度很高,部分企业已经在自己现有的业务上找到了应用模式,但很多企业仍处于不断的反复尝试中.事实上,要找到合适的应用场景,重点应该在分析区块链本身的特性[5],即在不引入第三方中介的前提下,连续的区块存储和共识算法提供的难篡改性、安全性和可靠性的保障.因此,直接或间接依赖可信任的第三方的活动可以从该技术中受益.

1)物联网和物流供应链

IBM在物联网领域具有数十年的技术和理论,致力在自己擅长的领域引入区块链技术,解决了存在的一些问题,比如成本和安全问题.于是在2016年初,IBM和三星宣布他们合作开发了ADEPT[6]系统,目的是使用区块链技术创建一个可行的分布式网络.该系统使用BitTorrent和Ethereum,TeleHash,Visa和DocuSign则联合推出了使用区块链技术维护的出租车服务.Skuchain基于商品流动和资本流动的区块链同步,创造了一种新的供应链解决方案,以解决假冒商品问题.京东万象利用区块链技术将一头牛从育种免疫、屠宰等过程转变为自己的联盟链,确保信息真实性的安全性.

2)金融服务

在金融领域中,为了使交易成本降低,减小组织交互之间的风险,金融组织和银行将区块链技术落地的愿望更加迫切,同时也会让区块链技术加速成熟.中国人民银行行长周小川表示,央行的数字货币可以采用区块链的技术模式,从而将彻底改变传统的货币流通模式.而在这方面英国的银行已经先走了一步,他们实现了数字货币系统——Rscoin[7].Rscoin的目标是提供一个由中央银行控制的数字货币.它采用2层供应链结构,提高了2PC[8]提交和多链交叉验证机制在区块链技术的运行效率.通过中国人民银行和附属银行的信托基础,可以提供更好的业绩.2016年10月,中国邮政储蓄银行宣布与IBM合作推出基于区块链技术资产托管的系统,这是中国银行业首次成功地将其核心业务发布到区块链接技术平台.新的业务系统消除了重复结账过程,比原有业务流程缩短了约60%~80%的时间,提高了信用交易的效率.2015年10月,纳斯达克证券交易所推出了区块链平台Nasdaq Linq[9],实现了将区块链技术应用到交易股票的一级市场.2017年2月,R3联盟成员招商银行宣布将区块链技术应用于总行.香港分行和永隆银行台湾之间的直接结算系统,减少交易时间并减少查询程序.此外,在区块链技术的基础上涌现出了大量的创新型支付企业.例如Ripple[10]:实现了一个跨地区、多币种、低成本的实时

交易平台，引入了类似银行的网关概念.

目前来看区块链主要在以上 2 个领域有比较好的应用实践，另外在其他领域大家都在积极地探索区块链的应用.

3 区块链中共识机制的发展和实现

3.1 共识机制和拜占庭将军问题

分布式计算和集群异构系统的一个基本目标是在部分错误的进程下，保证系统的可靠性，这往往需要在计算过程中对一些协议所需的信息达成一致.为了在一个问题上达成共识，协商的过程需要多方参与多方作用，因此共识问题在本质上是一个一致性问题.

分布式存储系统等多数分布式系统在建立之初首先要解决的就是一致性问题.如果分布式系统中的每个节点都能保证具有很强性能（即时响应和高吞吐量）的操作，无需故障，协商一致过程的实现并不复杂，可以通过组播过程简单地进行投票.不幸的是，在现实中这样一个“理想”的场景并不存在.主要有以下需要考虑的点：

1）节点之间的网络通信是不可靠的，包括任意延迟中断和内容故障；

2）节点的处理可能是错误的，甚至节点自身随时可能宕机；

3）同步调用会让系统变得不具备可扩展性；

4）存在恶意节点故意要破坏系统.

一般情况下，失败（非响应）的情况被称为“非拜占庭错误”，而恶意响应的情况称为“拜占庭错误”.一致性问题是 20 世纪 70 年代以来研究的经典问题.为一致性问题设定上限的 3 位科学家 Fischer，Lynch 和 Patterson[11]，他们在 1985 年发表的论文中提出了 FLP 不可能性.作为分布式理论的重要定理之一. 他们认为，在完全异步系统下没有任何协议可以容忍甚至一个进程的失败. FLP 定理定义了分布式系统一致性算法的上界. Leslie Lamport[12]描述分布式系统容错与一致性问题设想并首次提出拜占庭将军问题：拜占庭位于伊斯坦布尔，现在的土耳其.为了保卫国家，各军相距甚远，将军之间沟通必须依靠信使.为了统一地进攻和撤退必须就行动达成一致.但有些将军可能是叛徒，他们会故意发送错误信息干扰别人.忠诚的将军如何在明知有叛徒的情况下统一作战计划.由此，比特币的每一个节点都可以看作是一个将军.

链中的链式数据结构仅用于形成链中的元素.如何形成这样的存储结构，如何保证其可信度，如何保证其安全性，如何确保分布式存储的一致性，都取决于共识机制. 因此，共识机制是区块链的灵魂，区块链的工作原理和应用场景取决于共识机制.区块链协商的目标就是让普通的节点形成一致的区块链结构，需要满足以下属性：

1）一致性.所有诚实节点保存的区块链的前缀部分完全相同.

2）有效性.由某诚实节点发布的信息终将被其他所有节点记录在自己的区块链中.

3.2 Paxos 和 Raft

1990 年，Lamport 的 Paxos[13]算法从工程的角度，最大化地实现了分布式系统一致性.Chubby 和 Zookeeper 使用的就是由 Paxos 启发而来的算法.算法中将节点分为 3 种类型：

1）proposer.提交建议等待批准的人.它通常的角色是客户.

2）accepter.负责对提案进行表决.服务器端的普遍角色.

3）learner.被告知协商的结果，并与之相统一，不参与表决过程.可能为客户端或服务端.

基本过程包括申请人的建议，当超过一半的支持时，将结果发送给所有人确认.一个很小概率的情况是在每一次新一轮的提案中，proposer 都崩溃，系统将不会达成共识.因此如果 Paxos 可以保证系统能达到共识，必须有超过 1/2 的正常节点存在.

Raft[14]算法是 Paxos 算法的简化实现，它包括 3 个角色：领导者（leader）、候选人（candidate）和跟随者（follower），基本过程是：

1）领导人选举.每一位候选人都会在某一段时间内随机提出一个选举方案，拥有最新阶段的多数选票将被选为领导人.

2）同步 Log.当选的领导者会找到系统中日志最新的记录，并强制所有的跟随者刷新到这个记录.

3.3 BFT 和 PBFT

拜占庭的问题中，如果总的节点数为 N，恶意

将军数为 F，当 $N \geqslant 3F+1$ 时，拜占庭问题才有解决方法，也就是 BFT（Byzantine fault tolerant）算法.

Lamport 证明了在诚实者不少于 1/3 时存在有效的算法能取得一致的结果.如果有太多的叛变者难以保证一致性.在超过 1/3 的叛国者的情况下有解决办法吗？假设有叛徒 f 个和 g 个忠诚者，叛徒故意给了错误的结果或者故意不作出回应.在某个时刻上，f 个叛徒都不会作出回应，而大多数忠诚的拥护者由于占多数就可以得到正确的结果.当 f 个叛徒给出恶意的建议，并有 g 个离线的忠诚者时，$g-f$ 个忠诚者无法分辨正确和错误.如果要确保大多数仍然可以正常工作，因此，$g-f>f$，$g>2f$，所以整体系统大小要大于 $3f$.

PBFT[15]是 Castro 和 Liskov 在 1999 年提出.是第 1 个广泛使用的 BFT 算法.只要系统中 2/3 个节点正常工作就可以保证一致性.该算法由 3 个阶段组成：准备之前、准备和提交.

这类机制的特点是很快出块，很快地达成共识，以至于没有时间允许分叉.但这类机制要求在一个封闭的节点集合中两两节点进行通信，因此比较适合于节点数量不多的联盟链和私有链.联盟链多采用技术成熟的 PBFT 机制及其相应的变种 RAFT，DBFT 和 HBFT 等来达成共识，如 2016 年 Linux 基金会发起的开源超级账本（HyperLedger）、IBM 推出的 Fabric 基础设施项目等.

Schwartz 等人[16]提出了 Ripple 协议共识算法（ripple protocol consensus algorithm，RPCA），将失效节点数量控制在 1/5 以内.因此可以在秒级达成一致性.

3.4 Proof of Work

即工作量证明，比特币区块链采用了该机制来实现共识[17].在比特币系统中时刻都在产生新的交易，而节点需要将合法交易放入块中.区块头包含 6 部分，分别是版本号、前一个区块哈希值、Merkle 根、时间戳、难度目标 nouce 和随机数.参与者需要寻找随机数使区块头哈希值小于或等于难度目标[18].例如，困难目标的二进制表示由 32 个 0 组成，平均需要 2^{32} 次尝试来解决这个问题.困难的目标将在达到每 2 016 块时调整，使出块的平均速度保持在每 10 min，所以难度目标将每 2 周更新 1 次（2 016×10 min）.PoW 保证一段时间内出现在系统中的交易是可以计算的.

截至目前，PoW 机制或多或少地存在于 Dogecoin，Litecoin 等数字货币中.

3.5 PoS 系列

2011 年，数字货币爱好者 Bitcointalk 论坛上，署名为“Quantum Mechanic”的爱好者提出 PoS（proof of stake）机制.经过讨论后社群同意并认可. 如果 PoW 竞争是计算力，挖矿概率与计算力正相关. 然后，PoS 竞争的是资产.节点越多挖掘块的概率就越大.PoS 合格区块的评判标准可以表述为 $F(Timestamp)<Target\times Balance$.

与 PoW 相比，公式中的难度值成为时间戳.在等式的右边，还有作为因子的均衡因素. 这样，整体目标值受平衡值和时间的影响.时间有限，所以出块的时间必须在一定范围内. 过早或过晚的块不会被其他节点接受.在某些加密货币实现思路里将公式中的平衡因子改为所持货币量产生了所谓的“币龄”.由于时间戳有限，PoS 锻造块的成功率主要与平衡因子有关.与采矿业的竞争性质不同，PoS 更像是一个彩票，积累了更多的货币年龄来争取获胜的机会，但由于一旦消耗了一定的价值，再赢的概率就减少了，避免了“富人更富”[19].在 PoS 中，主链被定义为最高消费链，每个块的交易将被提交，给块增加得分.在这种情况下，攻击者发起对主链的攻击就必须有很多的资金，并在 PoS 系统积累了很多时间，攻击者获得了大量的金钱，同时消耗得更多.并且一旦出现了攻击和破坏，攻击者自身的资金也会受损.它可能是从一开始就杜绝了攻击者的行为动机，一旦区块生成，其年龄立即被清除，这将确保攻击者不能继续攻击.

在 PoS 思想出现后，很多协议基于此进行二次开发可以看作是 PoS 系协议.

1) PoSV[20]

PoSV 意味着权利和频率，在 PoS 中，“币龄”受时间的线性影响，因此会出现囤币现象.瑞迪币（Reddcoin）改进 PoS 中的这个问题，将线性函数改造为指数衰减函数，使币龄的增长率趋于 0.在一定程度上解决了 PoS 的囤币问题.瑞迪币在发展前期使用 PoW 进行发币，后期使用 PoSV 维护系统运行.

2) DPoS[21]

DPoS(delegated proof of stake)即为授权股权证明,比特股(BTS)最先采用.顾名思义,DPoS类似与股份制公司,各个节点首先投票选举出社区可信度较高的来作为达成共识过程中的决策者.当然,每个节点支持的票数由其持有的货币数量决定. 这些可信节点可以被视为"挖矿池",它们之间具有相同的权利. 普通节点可以选举或驱逐不合格的"股东".在比特股中这个股东数量被控制在100个.

3) LPoS

LPoS(lease proof of stake)也就是租赁权益证明,在传统的PoS中,拥有少量余额的持有人不太可能会投注一个块,就像计算哈希能力弱的矿工不太可能在比特币中挖矿一样.网络中有很多节点多年才产生一个区块,这意味着许多拥有较低余额的持有者不会运行节点,并且将网络维持在数量有限的大型玩家身上.由于参与者越多网络安全性越好,因此激励这些较小的持有者参与是非常重要的.LPoS通过允许持有者将其余额租赁给节点来实现这一目标.租赁资金完全由持有人控制,随时可以转移或消耗(租赁结束时).通过借硬币增加了被允许在区块链中添加交易区块的机会,收到的任何奖励与承租人按比例分摊,这是Waves[22]采取的方法.

4) PoA

PoA(proof of activity)即活跃度证明[23].为了避免恶意通货膨胀,比特币选择了产生一定数量的货币,然后就是通货紧缩.奖励每4年减半,在分摊结束时,矿工的参与率下降,比特币的安全性值得关注.PoA为了避免这种情况,奖励线上的主动节点,大部分当前电子货币在"发布"后切换到离线状态,从而减少在线交易.PoA机制中的矿工开采过程与PoW机制类似,当矿工发现新块时,他们随机选择n个活动节点来广播新发现的块.$n-1$主动节点验证新发现的数据块并对其进行签名,第n个主动节点除了验证数据块和签名外,还会封装并广播该数据块.矿工和n个活跃节点将收取奖励费用.如果n个活动节点中存在不活动的节点,它将不能签署该块,因此不会收到适当的奖励费用.因此,PoA机制可以有效解决囤积钱的行为,并且在点对点网络中有非常重要的应用.现在Decred是使用PoA的唯一数字货币.

5) Casper[24]

Casper是Ethereum即将采用的新的一致性算法.不同于PoW中以块为单位连续的记录交易信息,它以链为单位.一个典型的场景是如果你提交了2个一样序号的交易,你将失去所有的保证金.有一定的惩罚机制,所以非法节点可以通过恶意攻击进行交易,但他们也面临着巨大的赔钱风险.本协议下的验证器主要有2个活动:出块过程和PoW类似.投注过程比较复杂,目前采用模拟PBFT的验证策略.

3.6 PoI

PoI(proof of importance)就是重要性证明,是一个更公平的算法.人们不需要使用更强大的机器,也不需要持有更多的股票以获得更多的回报.它只需要证明自己的重要性,才能获得出块权从而得到奖励.它不需要特殊的采矿设备,可以运行在树莓派,因此节省了电力资源.此外,在重要性的证明下,货币资产不是决定重要性的主要因素.它更关心的是交易量、活动量以及交易双方的关系.这些特点可以消除PoS系统中的其他弊端.NEM[25]中使用的就是PoI,其中具体是根据钱包交互次数和货币资产判断一个节点的重要性.相比之下,其他数字货币没有考虑到节点对网络的支持.为了鼓励用户积极地在NEM网络上交易维护,它后期会将传输数量也作为一个彰显重要性的因素.

3.7 Tendermint

2014年,Tendermint[26]团队中的Kwon着眼于现存算法的速度、可扩展性和资源问题,旨在以一种更安全更高效的方式实现共识.他们改进了20世纪80年代MIT开发的BFT算法,并概念性地证明利益概念证明(PoS)货币的安全性,以解决NXT和BitShares1.0中存在的"Nothing at Stake"问题出发提出了Tendermint共识机制.

Tendermint基于圆形投票机制(如图4所示).一个投票过程需要3个处理步骤:首先验证器提出一个块,然后发送提交意图,最后提交一个新块.在这个圆形投票机制中,原子广播安全状态可以被复制,Tendermint责任层基于此使问题可以被追踪.Tendermint共识算法首先让验证人员保

持区块链的完整副本，并利用公共密钥来识别被验证的身份.在每个新块的高度上，轮流提出块.每一轮投票只需要一个验证器，用相应的私钥进行验证签名，这样，一旦出现错误，负责的验证者就很容易被找到.然后其余的验证者将需要对每一个提案进行投票，投票用的是个人的私钥签名，这些构成了一个圆.然而，由于网络的异步需要，可能会提交一个新的块数轮.

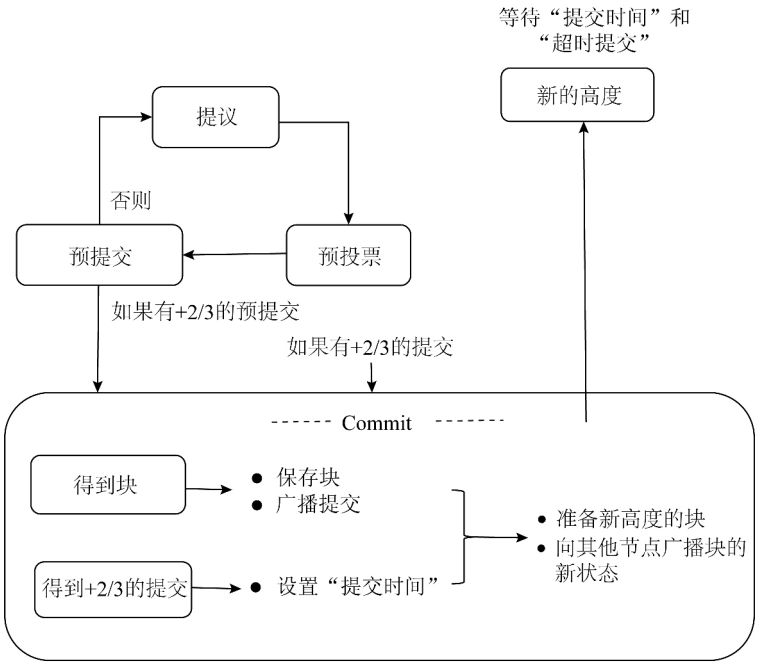

图 4 Tendermint 共识机制过程

3.8 混合共识算法及其他

1) Proof of Luck

伯克利大学的研究人员基于 TEEs(trust execution environments)设计了一种新型的共识机制，他们运行在支持 SGX 的 CPU 上，来抵御挖矿以及对能源的消耗.算法分为 2 个函数：PoLRound 和 PoLMine，其中所有参与者都运行这 2 个函数，得到以同一区块为祖先的不同区块.PoLMine 会选择一个介于 0 到 1 之间的随机数字(运气)，最大数字意味着运气最好，将所持有的区块作为被用作区块链中的下一个块.由于在 SGX 环境中发生随机数选择，所以不能伪造它.在论文中研究人员使用的是 Intel 的 TEE——SGX，基于 Intel 的硬件环境提出了对应的共识协议——POET(proof of elapsed time).据 Intel 自己的实验数据该算法可以拓展到数千节点.但是问题就是这些算法依赖底层 CPU 需要把信任交给 Intel，这却与区块链去中心化的思想相悖.

2) PoDD(proof of DDos)[27]

在 USENIX 技术研讨会上，一个新的加密数字货币 DDOSCoin 被科罗拉多大学和密歇根大学的研究人员提出，旨在用于奖励用户使用他们的电脑参与 DDoS 攻击.在 DDOSCoin 中，矿工工作量的计算是依据建立的 TLS 连接，这导致其只适用于已启用 TLS 加密的网站.他们使用的共识机制就是 PoDD，参与 DDoS 攻击会给矿工数字货币，矿工便可将货币转换成比特币或其他法定货币，这可以认为是 PoW 的另一种形式.恶意的“DDoS 身份验证”操作是让矿工连接到 Web 服务器.将响应作为链接证据，在现代版本的 TLS 中，服务器在握手过程中签署客户端提供的参数，并在连接的密钥交换中使用服务器提供的值.这允许客户向其他人证明他已经与服务器通信.此外，服务器返回的签名值对于客户端来说是不可预知且随机分布的.

3) PoB(proof of burn)[28]

至于 PoB，和开发比特币的过程也很相似.但 PoB 是通过将货币转移到不可逆转的地址上以销毁货币，而不是投资到计算硬件上.这种转移也叫作“燃烧”.货币被你转到了某个很难找到的地址，

基于随机选择程序的系统上，你就相当于获取了挖矿的终生权力.同时，你也可以转移本地货币或者其他区块链的数字货币.你燃烧货币的数量是和你被选中挖下一块币的概率是成正比的.时间越久你在这个系统的份额可能会逐渐减少，所以你会愿意通过燃烧更多的数据货币来获取更多的挖矿机会.

尽管 PoB 是 PoW 的一种有趣的替代选择，但是这种协议仍旧造成了很多不必要的资源浪费.另一种批评就是挖矿能力只会被那些愿意燃烧更多资金的人所掌控.PoB 的应用场景有 Counterparty[29]，TGCoin，Slimcoin 等.

4) PoC(proof of contribution)

到目前为止，共识机制的目的无非是既让用户积极参与又要防范不法分子进行恶意的行为.如何在这两者之间求得平衡，Cybervein 给出了他们的答案——PoC(贡献证明机制).他们认为使用 PoC 和其他机制可以在攻击的同时获得更多的用户参与和贡献，从而达到同样的预防效果.整个网络参与者的贡献可以是硬盘容量、带宽、功率、数据等各种资源.所以根据贡献力的方式可以分为 Proof of Storge 和 Proof of Space 等.在 Cybervein PoC 中，尽管一些参与者的贡献可能集中在长尾效应的曲线的头部，而贡献力量分布在正态曲线的尾部是非常小的，但在这部分人数占据整个网络的参与者多数.为了保证参与者的利益，随着时间的推移，这部分小贡献的比例逐渐增加，形成了上述正态分布曲线的“长尾”，贡献的积累将带来充足的收入，而大贡献者作为制衡的角色，以实现公平的状态，所以会有更多的人参与其中.Burstcoin[30]采用这种机制实现共识.

4 共识机制的分析和对比

4.1 评价标准

区块链上采用不同的共识机制，鉴于共识机制在区块链技术中的重要性，从以上分析也可以知道有很多种实现思路，为了便于分析，在满足一致性和有效性的同时，系统的整体性能也会产生不同的影响.鉴于共识机制的不同特点，可以在下面几个方面进行评估：

1) 安全.无论是防止 2 次支付、私自开采攻击，还是对错误的宽容程度都是将系统作为一个整体对外提供服务角度来判断的.从内部来看，Eclipse[31]攻击控制目标对象的网络通信，阻碍交易的传播.Sybil[32]攻击通过类似于 DoS 的方式让大量的无意义节点影响系统安全.

2) 扩展.是否支持网络节点扩展.可扩展性是区块技术设计中需要考虑的关键因素之一.扩展性大体由 2 部分组成：提高系统节点数和验证确认次数的增加.并由此而带来的通信负载和运行负载的提高.一般用吞吐量来衡量.

3) 性能.是从事务生成到节点存储系统中最终记录下来的过程中的延迟. 换句话说，系统可以处理每秒响应的数量.比如，比特币系统每秒最多有 7 笔交易.与现有集中交易系统的交易量相差甚远.

4) 资源.各节点在共识协议的指导下，对交易的处理达成一致所消耗的计算机的性能资源包括 CPU、内存、电池等.

4.2 各共识机制的不足

1) 工作量证明机制存在一些问题.首先，工作量证明机制存在严重的效率问题：每个区块的产生需要耗费时间，同时新产生的区块需要后续区块的确认才能保证有效，这需要更长的时间，严重影响系统效率；其次，工作量证明机制的安全性要求攻击者所占的计算资源不超过全网的 50%，然而从目前比特币矿池挖矿算力情况来看，算力排名前 5 矿池的总算力所占比例已经过半[33]，对系统的安全性和公平性造成严重威胁；最后，被批评是浪费资源.矿机日夜运转消耗大量计算资源、电力能源，人力资源，造成巨大浪费.据估计，电力需要将大于 1 GW(100 万 kW)，几乎相当于整个爱尔兰的电力消耗.也有很多人在致力于 PoW 的优化，提出了 PoUW[34](proof of useful work).原理一般是通过求解最短路径等问题代替无意义的随机数，但收效甚微.

2) 后来，权益证明机制实现了改进 PoW 的目标.但 PoS 并不完美，首先是初币的分发，一种是依旧使用 PoW 进行挖矿，另一种是 IPO，前者依旧存在 PoW 的问题，后者缺乏信任基础，容易滋生贸易犯罪.在应用方面，基于 PoS 的共识机制有很多应用，但是还没有完全基于 PoS 的区块链技术.另外，在高延迟网络环境下很容易产生分叉，影

响一致性.如果恶意节点在这种情况下发起攻击，它将通过控制网络进行通信，形成脑裂.

3）DPos 能耗比较低，具有比较快的出块时间.但是其缺点也是有的：因为普通节点话语权比较低，投票的积极性有待提高.如果发现一个恶意节点，处理流程不是很高效而且存在中止的情况.此外，代表的选举做不到实时，并且该系统还是依赖于代币，不适合公有链.

4）BFT 算法的安全性和可扩展性也存在一些问题.通过以上分析，BFT 的安全性取决于系统中无效节点数的比例.实际应用中，恶意节点实施 Sybil 攻击.许多伪造的客户端出现，稀释了正常节点的比例，进而影响到系统的稳定运行.因此，在节点比较多的区块链系统上扩展性比较差.而且一轮共识中对主节点的依赖太强.

4.3 展 望

在达成一致性的前提下，平衡效率、扩展性和资源是共识机制的痛点.在此基础上如何因地制宜结合共识机制，设计最佳协商机制，是未来研究的主要方向.而且我们可以看到，依据系统授权程度的高低，依次分为无需许可、公共的共享系统、需要许可、公共的共享系统，需要许可的、私有的共享系统.越开放的系统达成共识的代价越高.鉴于共识机制的优缺点，我们可以尝试将不同的共识机制结合起来，形成一种新的共识机制.比如将 PoW 和 PoS 结合，将 PoS 和 BFT 结合.

对于现存区块链的一些问题，要结合加密算法和底层存储技术的改进，共识机制才能发挥出最大效果，比如零知识证明[35]、环签名、闪电网络、DAG、HashGraph[36].随着全球对区块链的关注，越来越多的人投入其中研究开发，未来会有更多工作高效设计巧妙的共识机制被设计出来.

5 结束语

区块链技术的重要基石无疑是共识机制.学术界和商界越来越关注共识机制，以便更好地应用这项技术.区块链要想落地开花离不开精妙的共识算法，但是，现有可用于区块链技术的仍存在这样那样的问题.令人欣慰的是，随着区块链的发展热度，共识机制相关的算法逐年增加，各种设计思想比比皆是.作为分布式计算中解决一致性问题的共识机制的应用场景分析也很重要，在一定程度上决定了区块链技术的未来.下一个创新是降低复杂性并提高一致性适应能力.

参 考 文 献

[1] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system [EB/OL]. [2018-03-20]. https://bitcoin.org/bitcoin.pdf

[2] Bitcoin Core. Integration/staging tree [OL]. 2009 [2018-03-20]. https://github.com/bitcoin/bitcoin

[3] Dai W. b-money [EB/OL]. 1998 [2018-03-20]. http://www.weidai.com/bmoney.txt

[4] Back A. Hashcash—A denial of service counter-measure [C] //Proc of USENIX Technical Conf. Berkeley, CA: USENIX Association, 2002: 15-25

[5] 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

[6] Panikkar S, Nair P. ADEPT: An IoT practitioner perspective DRAFT copy for advance review [EB/OL]. 2015 [2018-03-19]. https://ibm.biz/devicedemocracy

[7] 蔡维德，赵梓皓，张弛，等. 英国央行数字货币 RSCoin 探讨[J]. 金融电子化，2016 (10)：78-81

[8] Bernstein P. Two-phase commit protocol [EB/OL]. (2018-01-23) [2018-03-23]. https://en.wikipedia.org/wiki/Two-phase_commit_protocol

[9] Underwood S. Blockchain beyond bitcoin [J]. Communications of the ACM, 2016, 59(11): 15-17

[10] Baliga A. Understanding blockchain consensus models [EB/OL]. 2017 [2018-03-21]. https://www.persistent.com/wp-content/uploads/2017/04/WP-Understanding-Blockchain-Consensus-Models.pdf

[11] Fischer M J, Lynch N A, Paterson M S. Impossibility of distributed consensus with one faulty process [C] //Proc of ACM SIGACT-SIGMOD Symp on Principles of Database Systems. New York: ACM, 1983: 1-7

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

[13] Lamport L. The part-time parliament [J]. ACM Trans on Computer Systems, 1998, 16(2): 133-169

[14] Ongaro D, Ousterhout J. In search of an understandable consensus algorithm [C] //Proc of USENIX Conf on USENIX Technical Conf. Berkeley, CA: USENIX Association, 2014: 305-320

[15] Castro M O, Liskov B. Practical Byzantine Fault Tolerance [J]. OSDI, 1999, 99: 173-186

[16] Schwartz D, Youngs N, Britto A. The ripple protocol consensus algorithm [EB/OL]. 2014 [2018-03-22]. https://ripple.com/files/ripple_consensus_whitepaper.pdf

[17] 周邺飞. 区块链核心技术演进之路——共识机制演进(1)[J]. 计算机教育, 2017 (4): 155-158

[18] Antonopoulos A M. Mastering Bitcoin: Unlocking Digital Crypto-Currencies [M]. Boston: O'Reilly Media, Inc, 2014

[19] Houy N. It will cost you nothing to 'Kill' a proof-of-stake crypto-currency [J]. Social Science Electronic Publishing, 2014, 34(2)

[20] Ren L. Proof of stake velocity: Building the social currency of the digital age [EB/OL]. 2014[2018-03-23]. https://www.reddcoin.com/papers/PoSV.pdf

[21] Larimer D. Delegated proof of stake consensus [EB/OL]. [2018-03-22]. https://bitshares.org/technology/delegated-proof-of-stake-consensus/

[22] Alexander I. Waves platform [EB/OL]. (2018-03-19) [2018-03-23]. https://en.wikipedia.org/wiki/Waves_platform

[23] Bentov I, Lee C, Mizrahi A, et al. Proof of activity: Extending Bitcoin's proof of work via proof of stake [J]. ACM SIGMETRICS Performance Evaluation Review, 2014, 42(3): 34-37

[24] Danny R. Casper proof of stake FAQ [EB/OL]. (2018-03-04) [2018-03-23]. https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ

[25] Beikverdi A. NEM (cryptocurrency) [EB/OL]. (2018-03-08) [2018-03-23]. https://en.wikipedia.org/wiki/NEM_(cryptocurrency)

[26] Kwon J. Tendermint: Consensus without mining [EB/OL]. 2014[2018-03-23]. https://www.github.com/tendermint/tendermint/wiki

[27] Wustrow E, Vandersloot B. DDoSCoin: Cryptocurrency with a malicious proof-of-work [C] //Proc of USENIX Conf on Offensive Technologies. Berkeley, CA: USENIX Association, 2016: 168-177

[28] Stewart I. Slimcoin a peer-to-peer crypto-currency with proof-of-burn, mining without powerful hardware [EB/OL]. 2014[2018-03-23]. http://www.doc.ic.ac.uk/~ids/realdotdot/crypto_papers_etc_worth_reading/proof_of_burn/slimcoin_whitepaper.pdf

[29] Jansen R. A TorPath to TorCoin: Proof-of-bandwidth altcoins for compensating relays [J/OL]. 2014 [2018-03-23]. https://petsymposium.org/2014/papers/Ghosh.pdf

[30] Quibus B. Burstcoin—The green innovative cryptocurrency [EB/OL]. 2017 [2018-03-23]. https://www.burst-coin.org/proof-of-capacity

[31] Heilman E, Kendler A, Zohar A. Eclipse attacks on Bitcoin's peer-to-peer network [C] //Proc of USENIX Conf on Security Symp. Berkeley, CA: USENIX Association, 2015: 129-144

[32] Eyal I, Sirer E G. Majority is not enough: Bitcoin mining is vulnerable [C] //Proc of Int Conf on Financial Cryptography and Data Security. Berlin: Springer, 2014: 436-454

[33] 全球算力分布[EB/OL]. [2018-03-20]. http://qukuai.com/pools

[34] Marshall B, et al. Proofs of useful work [J/OL]. IACR Cryptology ePrint Archive, 2017 [2018-03-23]. https://allguantor.atj/blockchainbib/pdf/ball2017proofs.pdf

[35] Wacław B, Stefan D, Daniel M. Efficient zero-knowledge contingent payments in cryptocurrencies without scripts [C] //Proc of European Symp on Research in Computer Security. Berlin: Springer, 2016: 261-280

[36] Baird, Leemon. Hashgraph consensus: Fair, fast, byzantine fault tolerance [EB/OL]. 2016 [2018-03-23]. http://www.swirlds.com/wp-content/uploads/2016/2016-05-31-Swirlds-Consensus-Algorithm-TR-2016-01.pdf

杨宇光

1976 年生,博士,教授,主要研究方向为信息安全及信息安全与其他学科的交叉学科.

yangyang7357@bjut.edu.cn

张树新

1993 年生,硕士研究生,主要研究方向为信息安全及区块链.

zhangshuxinmj@163.com