加密数字货币系统共识机制综述①

夏 清[1,2], 张凤军[1], 左 春[3]

[1](中国科学院软件研究所 互联网金融技术研究中心, 北京 100190)
[2](中国科学院大学 计算机与控制学院, 北京 100190)
[3](中科软科技股份有限公司, 北京 100190)

摘 要: 共识机制是以区块链技术为支撑的加密数字货币系统的核心, 分析并比较了现有的三种典型共识机制, 为区块链开发者设计共识机制提供参考和建议. 解析了三种主流共识机制 PoW、PoS、DPoS 的基本思想、运行过程与优缺点, 随后从公平性、运转开销、可持续性等几个方面归纳出每种共识机制的特点, 然后从信用的去中心化程度、授权等多个角度进行分析比较, 考量不同应用场景下的共识需求. 从应用场景出发, 将两种或以上共识机制结合使用, 在完全去中心化与中心化中间寻找到适合的平衡点, 更符合未来共识机制的应用需求.

关键词: 共识机制; 加密数字货币; 区块链; 去中心化; 开发

Review for Consensus Mechanism of Cryptocurrency System

XIA Qing[1,2], ZHANG Feng-Jun[1], ZUO Chun[3]

[1](Research Center for Internet Finance Technology, Institute of Software Chinese Academy of Sciences, Beijing 100190, China)
[2](School of Computer and Control Engineering, University of Chinese Academy of Sciences, Beijing 100190, China)
[3](Sinosoft Company Limited, Beijing 100190, China)

Abstract: Consensus mechanism is the core of the cryptocurrency system which is based on the block chain technology. This paper analyzes and compares the three typical consensus mechanisms to provide references and suggestions for the design of consensus mechanism for block chain developers. The basic idea, operation process and advantages and disadvantages of the three mainstream consensus mechanisms, PoW, PoS and DPoS, are analyzed. Then the characteristics of each consensus mechanism are summarized from the aspects of fairness, running cost and sustainability. And then we analyze and compare them from the credit to the degree of decentralization, authorization and other aspects, consider the consensus needs under the different application scenarios. From the application scenario, two or more consensus mechanisms are used in combination to find a suitable balance point between the complete de-centralization and the centralization, which is more in line with the application requirements of the future consensus mechanism.

Key words: consensus; cryptocurrency; blockchain; decentralization; development

近年来, 以比特币为代表的加密数字货币使用范围日益扩大, 交易规模也快速增长, 逐渐引起人们的广泛关注. 比特币系统从 2009 年开始正式运行, 到今天已经成功运转了 7 年, 虽然其中经历了几次货币价格的大涨大跌, 但通过对等网实现的比特币自身的匿名性、不可更改、低成本跨境支付[1]等特点使它越来越受到重视, 并为加密数字货币领域的研究发展提供了新的思路.

区块链作为比特币系统的底层支撑技术, 以其具备的分布式、去中心化、可追溯、不可篡改[2]等特点, 在全球金融技术领域掀起一波新的讨论热潮. 区块链是一种分布式数据库技术, 它维护了一个持续增长并且不可被篡改和修改的数据记录列表, 系统中的有效信息按时间顺序排列存放在一个个区块中, 除了创世区

① 收稿时间:2016-07-18;收到修改稿时间:2016-10-12 [doi:10.15888/j.cnki.csa.005773]

块外每个区块还包含指向前一个区块的链接信息, 从而形成一个从前往后有序链接的数据结构链条[3]. 区块链技术已成为金融技术领域最具颠覆性的前沿技术, 除了数字货币领域外, 金融、物联网、公证等其他领域人士也在积极探索基于区块链的落地项目.

区块链本质上是一种对等的分布式系统, 所有节点共同保障系统的正常运行. 在这种分布式系统中, 除了互联网本身面临的网络延时、传输错误等固有问题, 还有由于去中心化而带来的不能信任任意参与者、可能存在恶意节点、各方利益不一致导致数据分歧等问题, 为了防范这些潜在的威胁, 区块链系统需要一种共识机制来使各个节点达成共识, 保证数据的最终一致性.

在基于区块链技术的加密数字货币系统中, 中央银行的角色不再存在, 货币发行和交易流通的职责由所有节点共同承担[4]. 选择哪个节点来发行货币、如何识别一笔交易是否是双重支付、交易链条出现分叉时如何处理等重要问题需要节点采用共识机制来解决, 一个良好的共识机制是保证数字货币系统准确高效运转的必要条件.

基于此, 本文对数字货币领域实践运行的五种共识机制进行研究. 比较典型的有 PoW(Proof-of-Work, 工作量证明)、PoS(Proof-of-Stake, 权益证明)及其变种 PoSV(Proof-of-Stake-Velocity, 权益和活动频率证明)和 PoA(Proof-of-Activity, 行动证明)、DPoS(Delegated Proof-of-Stake, 授权股权证明), 通过对这些共识机制的分析比较, 探究在不同的应用场景下合适的共识方案.

1 共识机制和拜占庭将军问题

分布式计算和多代理系统中的一个基本目标是在部分进程出错的前提下实现整个系统的可靠性[5], 这往往需要在计算过程中对于某些所需信息达成一致, 例如是否将某个交易提交到数据库, 是否认证某个参与者的领导者身份等. 这种为了达成关于某个问题的一致意见的过程即是形成共识的过程, 共识问题实质上就是一致性问题[6].

分布式数据库和大多数的分布式系统都构建在一致性问题上, 这个问题听起来很简单, 但却是从上世纪 70 年代就开始研究的经典问题. Fischer, Lynch 和 Patterson 在 1985 年发表的《Impossibility of Distributed Consensuswith One Faulty Process》[7]一文中提出了重要的分布式系统定理——FLP 不可能性. 该理论认为没有一个完全异步的共识协议可以容忍哪怕仅仅一个进程失效. FLP 定理限定了分布式系统共识算法求解上限.

在比特币系统中可能存在恶意节点的情况下, 共识机制要解决双重花费问题, 并使所有节点在期限内就一个记录所有交易信息的总账本达成一致. 中本聪通过引入经济激励和奖惩机制在算法体系之外对共识机制进行突破, 使比特币系统以很小的概率出现系统不可用的情况, 满足实际应用场景.

一个正确的分布式共识协议需要满足以下三个条件:

① 协商——所有节点针对相同的值进行表决;

② 终止——所有节点在有限时间内达成一致;

③ 有效——最后达成一致的值由系统中的节点提出[8,9].

可以看出, 比特币的共识协议均满足这三个条件, 是一个灵巧的针对共识问题的解决方案. 在比特币系统中, 当节点发现一个新区块后, 立即在全网广播, 所有节点通过验证区块的有效性来决定是否同意该区块, 当区块拥有大多数节点的确认后, 即可被认为有效. 比特币共识问题就是一个典型的拜占庭将军问题.

1981 年 Leslie Lamport 在《The Byzantine generals problem》[10]一文中描述分布式系统容错与一致性问题设想时首次提出拜占庭将军问题. 拜占庭位于现在土耳其的伊斯坦布尔, 是东罗马帝国的首都. 由于当时拜占庭罗马帝国国土辽阔, 为了防御敌人, 每个军队都分隔很远, 将军与将军之间只能靠信差传递消息. 在战争时期, 拜占庭军队内所有将军必须达成一致共识, 发现有赢的机会时才去攻打敌人的阵营, 但是有些将军可能是叛徒, 他们会故意发出错误信息竭力扰乱其他人. 忠诚的将军们如何在已知有叛徒的情况下达成一致协议, 这就是拜占庭将军问题. 比特币的每个节点可以看做是一位将军, 将军们想对系统总账内容达成一致, 节点中可能存在恶意节点, 它们想方设法对总账内容进行篡改, 从而使自身获得更大经济利益.

在传统货币体系中, 中央银行拥有货币发行权, 负责货币供给并维持货币稳定性, 而在以比特币为代表的加密货币体系中, 所有节点共同协作实现中央银

行的两大功能: 发行货币和维护一个记录货币所有权流转的总账本.

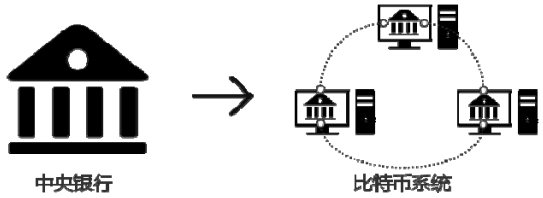

图 1 传统货币体系和比特币系统对比图

如图 1 所示, 比特币系统中没有中央银行的概念, 或者可以理解为系统中的每个参与者都是一个小银行, 因为每个节点现在都有发行货币的机会, 同时也都要维护一个总账本, 从而确定货币与人的对应关系. 哪个节点拥有货币发行权, 在货币不断流转的过程中如何明确货币所有权, 这就是加密货币系统中的共识机制主要解决的问题[11]. 而货币所有权的确定则是一个更加棘手的问题, 因为分布式网络的种种特点, 恶意参与者可能发起双重支付、拒绝服务攻击等扰乱系统正确运行.

2 加密数字货币系统中的共识机制

依据货币系统网络中节点的权利大小进行分类, 共识协议可分为无授权(permissionless)协议和有授权(permissioned)协议[12]. 无授权协议中典型的是 PoW, 所有节点权利平等, 有授权协议中根据授权程度的不同, 较典型的有 PoS 和 DPoS. 三种共识机制分别对应不同的应用场景, 授权程度由弱到强, 因此下文将对这三种典型共识机制进行介绍、分析与比较, 同时展望加密数字货币共识机制的未来.

2.1 PoW

PoW 即工作量证明, 是比特币系统中采用的共识机制. 比特币交易的合法性是由整个网络合力验证的, 只有大多数参与者认同某笔交易, 该交易才被视为有效[13]. 然而, 在这种机制下, 假身份的问题凸显出来, 即敌手可能发起女巫攻击(Sybil attack)[14]. 交易发起方可以伪造多个身份, 随后对自己的交易进行确认, 由于“大多数人”都认同这笔交易, 即便是双重支付, 接收方也会相信并接受该交易. 基于控制系统中大部分算力比控制大部分实体难得多的假设, 比特币协议使用工作量证明来防止女巫攻击. 在确认交易前, 参与者需要做一些工作来证明他们的真实实体身份, 这项工作是解决一个密码学难题, 人为地提高了确认交易的计算成本. 因此, 验证交易的能力取决于算力, 而不是实体身份数量.

比特币系统中不断产生新交易, 节点需要将合法交易放进一个区块中. 区块头由版本号、前一个区块哈希值、Merkle 根、时间戳、难度目标和随机数六部分组成, 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[15]. 比特币协议中使用 SHA-256 哈希算法, 除非算法被攻破, 否则最有成效的方法是尝试不同随机数, 直到满足目标, 例如, 难度目标为二进制哈希值以 48 个 0 开头, 则平均要经过 2^{48} 次尝试才能解决难题.

难度目标每经过 2016 个区块后会进行调整, 使区块的平均速度保持在每 10 分钟一个, 因此每两周(2016*10min)难度目标会更新, 新难度值 T 的计算公式为:

$$T = T_{prev} * \frac{t_{actual}}{2016*10\,\text{min}}$$

其中, T_{prev} 是旧难度目标, t_{actual} 是最近产生的 2016 个区块的实际花费时间. 难度目标值越小, 寻找到满足条件的随机数就越困难, 如果 t_{actual} 小于两周时间, 意味着区块确认速度加快, 网络算力提升, 因此新难度值将变小使区块平均生成时间延长从而保持系统稳定性.

解决工作量证明难题需要花费算力, 实际上就是花费金钱, 为了鼓励节点共同参与进来维护网络安全, 比特币协议提供了一个激励机制, 给第一个解决数学难题的节点一笔回报, 包括挖矿奖励和交易费. 比特币区块的第一笔交易被称为 coinbase 交易, 在此交易中系统将一定数量的比特币发送到解决工作量证明难题的矿工账户. 挖矿奖励最开始设置为 50 个比特币, 每经过 210000 个区块(即接近四年的时间)奖励减半, 预计到 2140 年左右比特币开采完毕, 随后网络安全的维护全取决于交易费, 挖出来的共 $21*10^6$ 个比特币在系统内流通[16]. 激励机制既是货币发行手段, 同时也保障了系统的网络安全.

比特币系统中的主链定义为累积了最多难度的区块链, 一般情况下, 也是包含最多区块的那个链. 当两个区块在较短的相隔时间内被挖出来时, 主链就会产生分叉, 此时系统会将分支保留, 如果在未来的某

个时刻他们中的一个延长了并且在难度值上超过了主链, 那么后续的区块就会引用它们.

工作量证明机制从货币供应、防止双重支付、采取激励措施保证安全、在有限时间内对于交易达成一致四个方面保障了比特币系统的安全运行, 为拜占庭将军问题提供了一种解法[17].

2.2 PoS

比特币网络的安全由物理稀缺资源进行保障, 包括执行哈希操作的物理硬件和电力两部分, 为了增加挖矿报酬, 矿工们不得不参与竞争日益激烈的挖矿军备竞赛, 因此从能源角度来看, 工作量证明是一种生态不友好的共识机制, 这也导致了能源消耗较少的共识机制——权益证明的出现[18].

权益证明即 PoS, 目前点点币(Peercoin)[19]、未来币(Nextcoin)等多种加密货币都使用了这种共识机制, 它的出发点在于解决工作量证明的能源浪费问题. 权益证明基于币龄的概念, 币龄被定义为货币数量和货币持有时间的乘积, 例如, Bob 从 Alice 那里收到了两个币, 并持有了 90 天, 那么 Bob 就收集到了 180 币天(2*90)的币龄, 而当 Bob 将这笔钱花费以后, 收集到的币龄则被销毁. 权益证明蕴含的理念是区块链应该由那些在其中具有经济权益的人进行保障.

PoS 挖矿在 2012 年由匿名开发者 Sunny King 发布的点点币中首次实现. 在点点币区块中有一个称为 coinstake 的交易, 命名类似于比特币区块中的 coinbase 交易. 在 coinstake 交易中, 规定货币所有者将持有的货币发送给他们自己(保证生成权益区块后币龄归零), 用来产生点点币区块并得到部分利息, 得到利息币的代价是币龄的消耗. 和比特币系统中类似的是, 点点币区块也要求参与者寻找随机数使区块头哈希值满足目标难度, 不同之处在于点点币系统中每个参与者产生区块的难度目标值各不相同, 难度目标和 coinstake 交易中消耗的币龄成反比, 参与者累积的币龄越多, 生成区块的几率也就越大[20].

可以将 PoS 中币龄的概念想象为 PoW 中的算力, 如果某人将一大笔钱持有很长一段时间, 那他在下次挖矿中就相当于拥有一次使用强有力的 ASIC 矿机的机会, 但这种机会不依赖于硬件设施的购买和电力的消耗, 而是取决于用户在系统中的存款以及储蓄时间. 不同于 PoW 挖矿中竞赛的性质, PoS 更像是抽奖, 累积币龄越多越有机会中奖, 而一旦中奖由于币龄已经被消耗, 再次中奖概率就降低了, 避免了“富人越富”[21]情况的发生.

PoS 中将主链定义为消耗币龄最高的链, 每个区块的交易都会将其消耗的币龄提交给该区块, 以增加区块得分. 在这种情况下, 攻击者如果想发起对主链的攻击, 必须要拥有一大笔钱, 并且要累积到足够多的币龄才行, 攻击者得到 PoS 系统中一大笔钱的花费似乎比掌握比特币系统中大部分算力代价更高, 而且一旦实施攻击, 破坏货币体系的同时自身拥有的大量货币也会受损, 这可能从一开始就降低了攻击者的行为动机. 而一旦区块生成后币龄立即清零, 这也保障了攻击者不能进行持续攻击.

在 PoS 出现后, 一些针对其中某个缺点进行修改而诞生的新协议被称作 PoS 的衍生协议, 比如 PoSV 和 PoA[22].

PoSV 针对 PoS 中币龄是时间的线性函数这一问题进行改进, 致力于消除货币持有者的屯币现象. PoSV 意为权益和活动频率证明, 是瑞迪币(Reddcoin)目前使用的共识机制, 瑞迪币在前期使用 POW 进行币的分发, 后期使用 PoSV 维护网络长期安全. PoSV 将 PoS 中币龄和时间的线性函数修改为指数式衰减函数, 即币龄的增长率随时间逐渐减少最后趋于零,因此新币的币龄比老币增长得更快, 直到达到上限阈值, 这样在一定程度上缓和了货币持有者屯币现象.

PoA 意为行动证明, 也是 POS 的一种改进方案. 它的本质是通过奖励参与度高的货币持有者而不是惩罚消极参与者来维护系统安全. PoA 将 PoW 和 PoS 结合在一起, 主要思想是将 PoW 挖矿生成币的一部分以抽奖的方式分发给所有活跃节点, 而节点拥有的股权与抽奖券的数量即抽中概率成正比.

2.3 DPoS

为了进一步加快交易速度, 同时解决 PoS 中节点离线也能累积币龄的安全问题, Daniel Larimer 于 2014 年 4 月提出 DPoS[23]. DPoS 是 PoS 的衍生物, 意为股份授权证明机制, 股东们将权利授予一定数量的受托人(delegates), 由受托人负责维护货币系统运行, 这在某种程度上类似于代议制制度, 但和现实中的议会议员有所不同的是, 选民有权在一段时间后根据受托人的表现重新选举, 如果对他们的工作表现不满意, 也可以要求罢免受托人. DPoS 目前是比特股、Crypti 平台内置的共识机制.

在 DPoS 中, 股东投票给某个受托人, 系统根据股东所持股权在系统中占比计算出票数最高的一定数量受托人, 受托人们按照事先规定的顺序轮流负责生成区块. 通过所有股东的投票后, 系统中的信任已经由全体参与者集中到了少数参与者, 节点发起交易后不用再等待相当数量未授信任节点的确认, 而只需要让受托人对交易进行验证, 这就大大缩短了交易的确认时间. 例如, 比特股可以达到每个块 10 秒的区块生成速度, 相比于比特币平均每个区块接近 10 分钟的生成时间有了重大提升.

在一些 DPoS 协议版本中, 节点要获得竞争成为受托人的资格首先得付出一定代价, 比如缴纳一笔保证金到某个安全账户, 如果节点作恶保证金将被没收[24]. 受托人维护系统运行将获得报酬, 他将与其他受托人共享区块交易费, 酬劳对其形成正向反馈从而激励受托人更加努力维护系统安全. 由于区块被受托人轮流签署, 如果某位受托人因离线错过了签署区块, 他将面临被其他候选受托人取代的风险, 因此为了营利, 受托人必须保证充足的在线时间. 需要缴纳保证金的这种 DPoS 协议也被称作基于存款的股权证明协议 (deposit-based proof of stake).

3 三种共识机制的对比

3.1 PoW 的特点

工作量证明的最大特点及优点体现在协议的公平性上, 具体表现为若矿工所持算力占全网总算力的 p%, 则相应地有 p%的可能性生成区块并获得报酬. 这也侧面说明了攻击的困难性, 攻击者的算力需要同全网其它诚实结点共同竞争才能生成对其“有利”的区块. 工作量证明算法保障着比特币网络从诞生开始安全运行至今, 然而随着越来越多人使用比特币进行交易, 它的缺陷逐渐体现出来. 工作量证明的初衷是采用“一个 CPU 一票”的“全民”公投方式达到去中心化民主实现共识, 这种方式达成共识是一个耗时的过程. 此外, 由于比特币价格上涨, 利益驱动使市场上出现专业挖矿设备, 购置矿机的用户数量增多导致越来越多小矿工的流失, 民主基础受到损害, 垄断问题凸显出来[25].

随着越来越多用户参与比特币挖矿, 为了降低挖矿门槛, 也为了提升比特币开采稳定性使矿工薪酬趋于平稳, 系统中出现众多商业矿池. 矿池一般是对外开放的团队开采服务器, 将众多用户的算力汇聚到一起组队进行挖矿, 目前较为著名的有 AntPool, F2Pool, BW.COM, BTCC Pool 等.

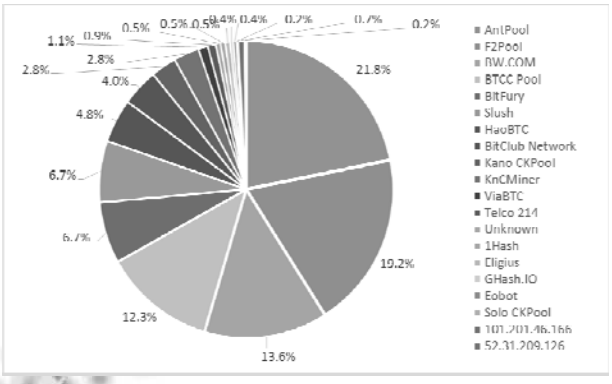

图 2 比特币矿池哈希算力分布

如图 2 所示, 在截止至 2016 年 7 月 14 日的前四天时间中, 超过 50%的区块被前三大矿池开采出, 超过 80%的区块被前六大矿池开采出, 矿池掌握了及其庞大的算力资源是不可否认的事实. 在 PoW 的共识机制中, 算力即代表着记账权. 如果单个矿池算力超过了 50%, 或者几家大矿池私下组成联盟, 就可以对比特币系统轻易发起 51%攻击, 垄断开采权、记账权、分配权.

其次就是一直受人诟病的能源浪费问题, 矿机夜以继日地运转浪费掉大量电力, 而这些能源除了生成比特币以外没有任何其他作用.

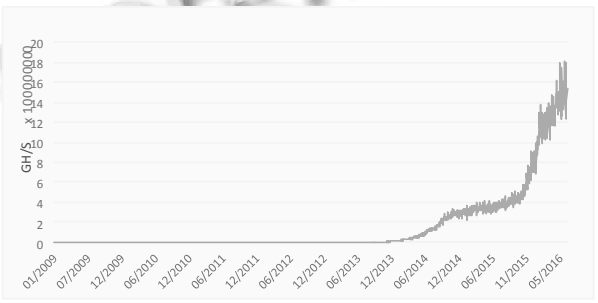

图 3 比特币网络哈希算力变化图

从图 3 中可以看到, 从 2013 年底开始, 比特币网络的算力大体上以指数级别在不断增长. 2016 年 7 月, 哈希算力已经达到 1500 000 000GH/s, 表示每秒可以进行 $15*10^{17}$ 次哈希运算, 据估计, 目前运行比特币网络需要的电力会超过 1GW(100 万千瓦), 差不多相当于整个爱尔兰耗费的电力.

最后当我们畅想比特币网络的未来时, 难免会看到公地悲剧的影子. 公地悲剧是一种涉及个人利益与公共利益对资源分配有所冲突的社会陷阱, 有限的公共资源被大众无限攫取就会发生这种情况, 最终资源损耗的代价会转移到所有可使用资源的人们身上. 比特币系统中的公地悲剧有两方面, 分别是用户群体和矿工群体[26]. 对用户群体来说, 支付交易费为矿工提供激励从而保证系统安全涉及到用户公共利益, 然而对用户个人而言, 让其他用户付交易费是个人利益最大化的途径, 如果大部分用户都抱有这种想法, 挖矿最终将会无利可图, 矿工也不再维护系统. 对于矿工群体来说, 让用户每笔交易支付较高交易费有利于公共利益, 但由于将一笔交易打包进区块的成本相对于区块交易费来说可以忽略不计, 矿工为了个人利益在交易费极低的情况下也会打包, 就会造成矿工自己将交易费压低的后果.

3.2 PoS 的特点

PoS 类似于股东大会决策, 区块生成由“权益大的股东”说了算, 共识机制设计基础的转变带来以下优点.

首先, PoS 使 PoW 挖矿浪费的问题有所缓解, 在比特币系统中, 生成区块的概率和矿工工作量成正比, 而在权益证明系统中, 区块生成的概率和币龄成正比, 因此证明者不要求完成一定数量的计算工作来抢夺打包权, 矿工们也不再需要投入大量钱财进行算力军备竞赛. 其次, 攻击者对货币系统攻击难度加大, 由于掌握大量货币成为了攻击者实施成功攻击的必要条件, 而在一个活跃的货币系统中, 这个代价无疑是高昂的. 最后, 能力越大, 责任越大, 维护货币系统的责任回归到了货币所有者和利益相关人的身上, 因为这群人持有系统大量货币, 一旦网络遭到攻击, 货币价格下跌, 他们将遭受最大的损失[27].

但 PoS 共识机制也并不是完美的.

首先是初始币的分发. 目前使用权益证明机制的加密货币使用两种方式对初始币进行供应, 一种是初期仍用 PoW 进行挖矿后期用 PoS 进行系统维护, 另一种是用 IPO(首次公开募股)的方式. 但用后者发行货币是缺乏信任基础的, 货币集中在开发者和少数人手中, 而不像在 PoW 机制中每个人都有分得货币的机会. 其次是鼓励了屯币行为. PoS 区块中的 coinstake 交易通过销毁币龄来生成区块和获得利息, 但被打包进区块的其他普通交易的币龄也会被重置为零, 这些币龄并没有为货币持有者带来利益, 对货币持有者来说它们只是白白消失了. 最后是节点离线, 这是 PoS 机制中的最大问题[28]. 由于币龄在节点离线时也会累积, 因此节点可能会倾向选择偶尔上线, 在币龄累积到一定程度后参与区块生成, 以此获利. 缺乏足够的在线节点将使网络攻击变得容易.

3.3 DPoS 的特点

DPoS 机制类似于现实世界中的董事会决策, 是一种代议制共识, 通过投票机制将所有用户的权利集中到了少数人手中, 形成一种有约束的中心化, 这种中心化大大加快了交易的确认速度, 确认时间缩短到秒级, 将加密货币技术带到了一个新的层次. 但与现实情况类似的是, 权利一旦集中到少数人手中, 我们就不得不提防这群人是否会为了自身利益损害公正.

以比特股为例, 系统中共选举出 101 个代表生成区块, 第 101 个代表将获得交易费用的 1/101, 但第 102 个代表却一无所获, 收益的陡峭下降可能会促使第 102 个代表与某些用户达成协议, 通过某些手段使自己跻身前 101 名, 例如和手握股权的人分享部分交易费用. 除此之外, 用户不得不担心代表是否会为了赚取交易费而迎合大股东, 做出损害普通用户利益的事情.

3.4 三种共识机制的比较

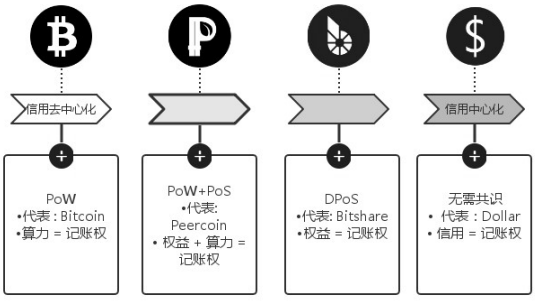

图 4 信用的去中心化程度

如图 4 所示, 从信用的去中心化角度考虑货币系统, 比特币和法币是两个极端. 比特币系统的信用是完全去中心化的, 货币信用依靠算力维持, 但目前可以看出, 算力已经走向中心化, 而法币信用由政府背书, 是完全中心化的. 点点币所代表的 PoS 和比特股所代表的 DPoS 共识机制介于其间, 属于信用的部分

去中心化. PoS 中币龄的特点导致大股东对系统安全影响较大, 一定程度上用户需要信任大股东不会做坏事, 因为这会损害他们自身利益, DPoS 类似于代议制, 选出一定数量代理人维持系统安全, 同样我们得信任这群代理人能公正办事.

表 1 三种典型共识机制的特征对比

特征 \ 共识机制	PoW	PoS	DPoS
记账权的竞争	算力	算力+权益	权益
挖矿成本	耗电	币龄+耗电	保证金
交易吞吐量	10min/块	10min/块	10s/块
安全威胁	算力集中	节点离线	候选人作弊

通过表 1 可以看出, 加密数字货币的共识机制由 PoW 发展到 PoS 再到 DPoS, 权益竞争逐渐部分甚至完全代替了算力竞争, 挖矿成本呈现逐渐降低的趋势, 而交易速度随着需求增大逐渐提升. 共识机制在发展的过程中, 基于权益所有者不愿意破坏货币系统使自身受损的假设, 权益的重要性逐渐被机制设计者们注意到[29]. 但 PoS 也有不少缺点, 因此出现许多基于 PoS 进行改进的共识机制, 即 PoS 的变种, 比如前面提到的 PoSV 和 PoA. DPoS 因为其交易速度快以及节能优点, 越来越受到开发者的关注, 以太坊作为有名的“下一代加密货币与去中心化应用平台”, 宣称将来要将 DPoS 运用到系统维护中, 虽然现在他们使用的是 PoW 共识机制.

图 5 系统授权程度与运转费用关系图

依据系统授权程度的高低, 可将现有的加密数字货币系统分为图 5 中的三类[30]. 比特币系统是典型的无需许可、公共的共享系统, 节点可以随时自由进入或退出货币系统, 所有节点权利也是均等的, 这种完全平等的系统需要达成共识的代价也是最高的, 如果我们将目前为止系统运作的电能费用均摊到每笔被确认的交易上, 每笔交易的确认费用在 1-6 美元之间, 而这笔钱目前是由矿工和比特币投机者出的. 因此若想得到良好的去中心化特质就需要付出达成共识的高昂代价.

从左到右的三类系统某种程度上对应着现实生活中的公有链、联盟链、私有链三种应用场景. PoW 作为无授权协议, 更适应于公有链系统, 这种系统虽然网络维护费用高但却是完全去中心化系统安全运行的保障. PoS 作为需要授权但授权程度较低的共识机制, 在需要许可的, 公共的共享系统中更有其发挥余地. 而 DPoS 则是需要许可的、私有的共享系统的较好选择, 因为委托人群体的原因, 保障系统安全运转无需较大花费.

4 展望

共识机制是加密货币系统的核心, 通过对几种现有共识机制进行分析比较后, 我们看出在共识机制的发展过程中, 权益机制由于其可以避免资源浪费的天然优势, 越来越引起人们重视, 而事实也证明, 对基于权益的共识机制进行改进是共识机制未来的一个发展方向.

不同应用场景需要采用不同共识机制, 现有的共识机制都有其缺点, 因此实际中也可以采取将几种共识机制混合使用的做法, 以便结合发挥彼此长处, 例如以太坊和点点币都采用的是工作量证明和权益证明的混合机制. 为了避免出现算力集中的问题, 需要在完全去中心化和完全中心化之间寻找一个平衡点, 折中处理, 这也符合现实生活中大部分应用场景的真实情况.

参考文献

1 Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. 2008.

2 Antonopoulos A. Mastering bitcoin. 2015.

3 谭磊,陈刚.区块链 2.0.北京:中国工信出版社,2016.

4 高航,俞学劢,王毛路.区块链与新经济:数字货币 2.0 时代. 北京:电子工业出版社,2016.

5 Castro M, Liskov B. Practical byzantine fault tolerance. In OSDI, 1999.

6 Pinna A, Ruttenberg W. Distributed ledger technologies in securities post-trading revolution or evolution? ECB Occasional Paper, 2016, (172).

7 Fischer MJ, Lynch NA, Paterson MS. Impossibility of

distributed consensus with one faulty process. Journal of the ACM (JACM), 1985, 32(2): 374–382.

8 Eyal I, Gencer AE, Sirer EG, van Renesse R. Bitcoin-NG: A scalable blockchain protocol. In NSDI, 2016.

9 Lamport L, Shostak R, Pease M. The Byzantine generals problem. ACM Trans. on Programming Languages and Systems, 1982, 4(3): 382–401

10 张铮文.一种用于区块链的拜占庭容错算法.http://www.onchain.com/paper/66c6773b.pdf, 2016.

11 Pass R, Shi E. Hybrid Consensus: Scalable Permissionless Consensus.

12 Cryptape.共识算法,区块链的引擎. http://cryptape.com/consensus-the-engine-of-blockchain.html, 2016.

13 崔屹东,郑晓彤.对新型货币比特币的经济学分析.现代经济信息, 2012,(16):8.

14 Sybil attack. https://en.wikipedia.org/wiki/Sybil_attack.

15 Antonopoulos AM. Mastering Bitcoin: Unlocking Digital Crypto-Currencies. Oreilly Media Inc Usa, 2015.

16 Tschorsch F, Scheuermann B. Bitcoin and beyond: A technical survey on decentralized digital currencies. IEEE Communications Surveys & Tutorials, 2015, 18(3): 2084–2123.

17 Garay JA, Kiayias A, Leonardos N. The bitcoin backbone protocol: Analysis and applications. In Eurocrypt, 2015.

18 Bentov I, Gabizon A, Mizrahi A. Cryptocurrencies without proof of work. arXiv preprint arXiv:1406.5694, 2014.

19 King S, Nadal S. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. self-published paper , 2012.

20 徐明星,刘勇,段新星,郭大治.区块链:重塑经济与世界.北京:中信出版集团,2016.

21 Houy N. It will cost you nothing to 'kill' a proof-of-stake crypto-currency. Ssrn Electronic Journal, 2014(2), 1038–1044.

22 Wood G. Ethereum: A secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper, 2014.

23 ThePiachu's Bitcoin Blog. Thoughts on delegated proof of stake and bitshares. http://www.8btc.com/thoughts-on-delegated-proof-of-stake-and-bitshares, 2014.

24 Larimer D, Kasper L, Schuh F. BitShares 2.0: Financial Smart Contract Platform. 2015.

25 Laszka A, Johnson B, Grossklags J. When bitcoin mining pools run dry. International Conference on Financial Cryptography and Data Security. Springer Berlin Heidelberg. 2015. 63–77.

26 Kroll JA, Davey IC, Felten EW. The economics of Bitcoin mining, or Bitcoin in the presence of adversaries. Proc. WEIS. 2013.

27 BitFury Group . Proof of Stake versus Proof of Work White Paper. http://bitfury.com/content/5-white-papers-research/pos-vs-pow-1.0.2.pdf. 2015.

28 Lampson B. How to build a highly available system using consensus. Distributed Algorithms, 1996: 1–17.

29 Canetti R. Universally composable security: A new paradigm for cryptographic protocols. In FOCS. 2001.

30 Walport M. Distributed ledger technology: Beyond blockchain. UK Government Office for Science, Tech. Rep, 2016, (19).