关于区块链共识算法的概述

薛荣坤
(西安交通大学，710079，西安)

摘要： 区块链技术不断发展，从早期的金融领域到现在的数据存储，数据验证，网络安全，正在成为社会技术发展的中坚力量.而共识算法在区块链中平衡其三个特点具有极为重要的作用，本文从区块链的基础概念出发，通过分析共识框架下的交易基本流程，重点介绍了一些单一共识算法和混合共识算法的基本原理，和这些算法的特点和不足。

关键词： 比特币 点对点网络 区块链 工作量 POW POV POA

1 区块链

1.1 区块链技术概述

传统网络中，支付宝或者微信的在线支付平台的可靠性基本取决于业务系统的服务商，而极为重要的个人身份信息，交易记录的保密性也完全依赖于第三方机构，2008年11月1日，中本聪在他的论文中“*Bitcoin：a peer-to-peer electronic cash system*“对比特币的原理做了基本的概述，在之后的10年里，人们通过这一底层技术实现了在传统中心化系统的基本功能。

这个技术基于密码算法，P2P 网络，将交易的数据按照一个特定的结构组织成为新的区块，在通过人们选定的共识机制和智能合约等技术，将这个区块添加到主链，具有去中心化，数据不可篡改，集体维护，高度透明，安全可信的特点。目前区块链技术已经广泛运用在金融，物联网，物流管理等多个领域。

1.2 区块链类型

根据网络范围，也即是否严格维护去中心化的的区别，区块链被分为公有区块链，联盟区块链以及私有区块链。

1.2.1共有区块链

一般来说，共有区块链是不许可区块链，任何人都可以发送交易数据到该区块链，同时区块链也对这一笔交易进行确认。这一技术目前仍广泛应用在虚拟货币领域。

1.2.2联盟区块链

通常情况下，联盟区块链和私有区块链都是许可链。在共识的过程中往往会受制于某一个预选的节点，比如在超级账本和 R3CEV 这样的领域。在这个过程中，仅有某些特定的节点被选为记账人，而大多数情况，其他节点的用处仅仅是货币的交易，不关心记账的这些过程。

1.2.3私有区块链

私有区块链一般仅在私有的组织内部使用，有私有组织自己决定节点的读写权限和记账权限，私有链安全可靠，不可以被篡改，同时也可以被溯源。从某些角度来说，联盟链目前的发展已经越来越趋向于私有链。同时共识算法在这一领域的应用保持高度的一致性，比如目前正在广泛使用的PKI(*public key infrastructure*)机制的数字证书来对节点进行认证。

2 共识算法

共识是意见统一的过程，涉及了社会生活，管理学和计算机学科等许多领域，简而言之，共识的过程类似于日常生活中进行投票，只不过表决的环境变成了分布式的系统。

实际上，对于区块链技术来说，一个核心的问题就是如何在一个复杂且去染发信任机制的开放互联网环境中维护一个记录系统中所有历史交易的账本。

某种程度上，区块链系统中的节点本质上是一个个接入互联网的普通计算机，但是其内部采用了P2P 的组织方式，即每一个点都处在同样的地位。带宽，内存，数据等资源可供其他节点使用。每一个节点都维护着存放了交易信息的区块链账本，因此共识算法就是需要解决集群内部不同节点处数据推送的不一致性的问题。

2.1 POW 算法简述

定义1与用 SHA-1的碰撞概率和算法的不可预测性一样，比特币中定义了难度值 *Difficulty(D)*，同时一个区块中容纳的全部数据 *tradeData*,计算满足条件的 *Nounce*,使得两次 SHA-256计算得到的值小于 *D*. $SHA256(SHA256(tradeData||nonce)) \leq D$。

POW 算法在1999年被提出，但是其实际是为了应对当时频繁的垃圾邮件攻击。发件人发送的邮件正文必须含有由收件人的地址，发送的时间，和

一个 Counter 组成的邮件签名，Counter 使得在发送时生成一个前20位均为0的160Bit 哈希值，而邮件服务器通过 SHA-1运算确定邮件的可靠性。

其中，在 tradeDate 确定(新区块中“区块体”中的交易 信息已确定)的情况下，不断重复选取随机数 Nonce,直至找到满足条件的 Nonce 为止。在共识算法中，矿工只有不断改变输入的 Nonce 值才能在竞争中获胜，而竞争力的大小由矿工节点的算力大小决定，因此算法的竞争最后转变到比特币网络中哈希算力的竞争上。另外,难度值 D 的大小用于控制比特币的出块时间在系统约定的 10 min 左右，新难度值 *Dnew* 与旧难度值 *Dold* 之间的关系为: $D_{\text{new}} = D_{\text{old}} \times \frac{\text{Usedtime}}{20160}$ 。

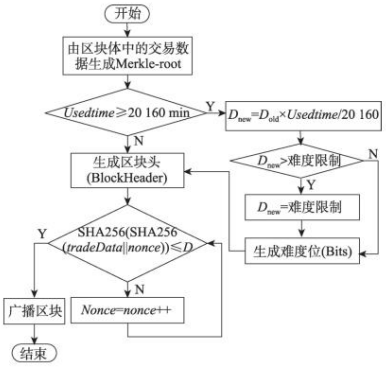
从比特币源码我们不难发现，其只使用了4Byte 字段来设置难度的大小，从算法角度来说采用了目标值的方法。目标值是比特币第一个区块的 Bits 字段值和难度值的比值，即确定值0x1d00FFFF 除以 Difficulty。

2.2 区块链共识模型

以比特币系统作为例子，区块链技术构建了一次交易产生到最后被全网确认的过程。

(1)生产交易 这一阶段，往往是在手机客户端，或者在线的交易平台上完成，交易者需要提供交易的输入金额，输入账户，输出账户等信息，但是此时的交易被称作原始交易(raw transaction)，指的是不被矿机接受确认的原始区块。

(2)交易签名 这一阶段，用户使用自己的私钥对于自己的交易进行确认，一般在法律认定中，经过数字签名后的交易就具有了法律效益，也就是合法的交易。



(3)交易广播 和其字面意思相近，将交易信息在交易区块后进行确认后，在该区块链上进行广播，但此时实际上并没有被整个区块链系统所认可，广播到确认的时间差给攻击者提供了类似芬尼攻击的思路。

(4)工作量证明 在这一阶段，将交易信息和节点缓存中已签名的交易打包进区块形成完整的区块体，通过 Merkle tree 算法生成 Merkle-root。判断距上次难度值调整时是否已经产生了 2016个区块，如果是，马上进行难度值的调整，以获得新的难度位(Bits);否则使用原来的难度值继续挖矿。将区块头部当前版本号，前一区块哈希、当前难度值、随机数、Merkle- root 以及时间戳这6个数据作为工作量证明的输入值，不断调整随机数 Nonce，并对每次调整后的区 块头进行双 SHA-256 运算，将运算值与当前的难度值进行比较，如果小于难度值则挖矿成功。

(5)交易被区块链记录 这一阶段，之前获取记账权力的节点们往往立刻广播他们的新区块，其他节点核对该区块记账的正确性，没有错误后，他们会在该合法区块后竞争下一区块，从而避免了分叉的产生，维护了主链的唯一性。

由于越来越多的网络节点参与这个过程，全网的算力大幅度的提高，比特币系统每过一段时间会调整 POW 的难度系数，保证世界平均约10分钟产生一个新的区块。而当一笔交易被从记录该交易的区块开始的6个以上区块确认后，从数学原理上，交易是绝对安全且不可篡改的，同时即使比特币矿工期望通过作弊或者进行欺诈交易，但是所有比特币节点都会拒绝非法的无效区块，这也保证了没有一个个体能够控制区块链中的内容，比特币网络仍具有很强可靠性和安全性。

Table 2 PoW and its improved algorithms

名称	年份	能耗	出块速度	分叉	算力分布
PoW[48]	1999	高	10 min	有	集中
Ethash[56]	2014	较高	15 s	易	分散
Bitcoin-NG[61]	2015	较低	主块 10 min、微块 10 s	易	较集中
ByzCoin[63]	2016	较低	区块 1 MB时约 1/100 s	易	较集中
ByzCoinX[65]	2018	较低	—	无	较集中
FruitChains[66]	2017	低	—	—	分散
Conflux[67]	2018	低	< 1/6 000 s	无	分散

2.3 POW 算法的局限性

POW 算法的本质时进行一场算力之间的竞争，其本质是制造了计算上严重不对称的两个角色：发布者和确认者，前者需要提交一个计算极其困难的计算结果，后者只需要通过简单的验证即可通过。

区块链开发者们提出了一种针对此种算法运作下的区块链攻击方法，攻击者只需要掌握51%以

上的算力，就可以垄断区块的产生，篡改或者撤销以往的交易。随着区块被确认数量的增加，现在攻击的概率已经显著降低。

具体进行攻击的方法有很多，这里我们介绍一个很经典的案例。设 A 要与 B 进行一笔 10BTC 的交易，第一笔交易被打包到100号区块，当后面再增加5个区块后，6次即可确认该交易。这时，A 又发起了一次给自己 10BTC 的交易。如果 A 向全网广播，这笔交易是不会被处理的，所以 A 选择不广播，而是对主链进行“分叉”，生成另外一个100号区块，并在其中打包第二笔交易。由此，产生了两条子链。其他矿工继续在原来的链上打包数据，而 A 则在新分叉的链上挖矿，两条链开始赛跑。由于 A 具有超51%的算力资源，很快，新链的长度就会超过旧链。这时，按照最长链优先原则，其他矿工也会自动转到新链上，使新链变成了主链。旧链则会被抛弃，之前打包在旧链上的所有交易，都会变为无效。结果是 A 不花一分钱就拥有了属于 B 的商品，这就是“51%攻击”。

2.4 POS 算法

2011 年，Quantum Mechanic 首次提出了 PoS 共识算法，算法中规定了用节点拥有的比特币数量来替 PoW 共识算法中基于算力求解哈希值的过程，即矿工拥有的比特币数量越多挖到矿的可能性就越大。

定义2(币龄) 币龄(coinAge)是指持币数量 (coins)与持币时间(holdTime)的乘积:

coinAge = coins × holdTime

定义 3(PoS 共识算法) 给定一个全网统一的难度值 D，以及新打包进区块的元数据 tradeData，寻找 满足条件的记数器 timeCounter，使得:

HASH256(HASH256(tradeData||timeCounter))< D × coinAge

2.4 POS 算法和 POW 算法的比较

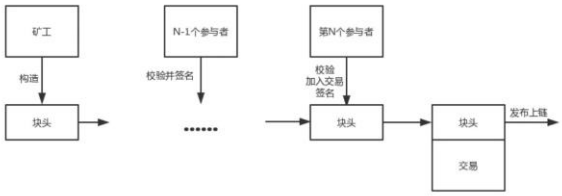
POS 的本质是通过权益来寻找哈希值，所以不会造成大量的算力浪费。同时当挖矿者找到一个有效区块后，该使用者的币龄将会被清零。同时因为用户在线的时间和挖矿的概率有明显的关系，因此 P2P 网络有相当强大的健壮性，对抵御51%攻击有明显作用。

然而值得提出的是，这种共识算法是很容易产生分叉，同时也显然降低了区块链去中心化的特点。

2.5 POS 和 POW 的混合算法

单一算法在安全，能效等方面总是有一定问题的，数字货币现在渐渐开始转向混合型的算法以实现更高的可靠性等。

因为出块奖励和收取交易费用是矿工们挖矿的主要来源。和比特币一样，大多数的币都会随着运行时间和全网算力的提高，其出块奖励会减少。挖矿者逐渐更加重视交易费用，但是当交易费用也不能使之满意使，其可能会停止挖矿，造成系统的不安全甚至是崩溃。



Bentov 提出，可以采取一种活跃证明的共识算法（POA），其大致流程如下：

（1） 每个矿工挖矿在 Hash 计算时，会生成一个符合难度的空区块头，其只包含前一区块的公钥地址，区块序号，随机数等。

（2） 当其他人挖到后，立刻将这个特殊区块向全网广播，首先将本区块头的 Hash 值与前一区块头的 Hash 值进行串联，再与一个固定值串联，然后计算串联后 数据的 Hash 值;对计算得到的 Hash 值利用算法进行 N 次随机运算，依次生成 N 个幸运股权持有者。

（3） 前 N-1的幸运者签名并广播，最后一名向空区块头添加交易的内容。

（4） 所以活跃节点在收到最后一个人的广播后验证，若验证通过，则加入主链。而系统也会自动随机调整 N 的数量。

3 总结

在区块链作为新技术的趋势下，新的共识算法和新的问题也正在不断被提出。从激励角度出发，激励机制决定了用户是否参与到这样的活动，比特币迅速的崛起正源于此，如果说早期的激励来源于经济的刺激，算法的激励，现在应该怎样做，才能唤醒更强烈的更高效的挖矿行为。

从用户的隐私，还是系统整体的安全性出发，系统该如何平衡二者之间的关系，共识算法作为平衡二者的墙梁我们不难发现，偏向中心化的算法带

来的安全性是极高的，但是区块链本身的生命力又源于匿名的民主，所以我们还需要不断探索新的动态平衡。

总之我们不难发现，利用和不断扩展区块链已经成为了新的社会热潮，在网络安全，金融贸易等各个行业产生了极其深远的技术影响。

参考文献：

【1】 刘明熹,甘国华,程郁琨,肖琳,刘帅,房勇.区块链共识机制的发展现状与展望[J].运筹学学报,2020,24(01):23-39.

【2】 张亮,刘百祥,张如意,江斌鑫,刘一江.区块链技术综述[J].计算机工程,2019,45(05):1-12.

【3】 BACK A. Hashcash—a denial of service counter-measure [EB/OL]. (2002-08-01)[2021-08-30]. http://www.hashcash. org/papers/hashcash. pdf.

【4】 WAHAB A, MEHMOOD W. Survey of consensus protocols [J]. arXiv:1810.03357, 2018.

【5】 CONTI M, KUMAR E S, LAL C, et al. A survey on security and privacy issues of bitcoin[J]. IEEE Communications Sur- veys & Tutorials, 2018, 20(4): 3416-3452.

【6】 [53] CHERNET H F, JILLEDI S K. A next-generation smart con- tract and decentralized blockchain platform: a case study on ethiopia[J]. Journal of Business Analytics and Data Visu- alization, 2020, 1(1): 28-34.

【7】 王晨旭, 程加成, 桑新欣, 等. 区块链数据隐私保护: 研究 现状与展望[J]. 计算机研究与发展, 2021, 58(10): 2099-2119. WANG C X,

【8】 [5] 袁勇, 倪晓春, 曾帅, 等. 区块链共识算法的发展现状与展 望[J]. 自动化学报, 2018, 44(11): 2011-2022.

【9】 YUAN Y, NI X C, ZENG S, et al. Blockchain consensus al- gorithms: the state of the art and future trends[J]. Acta Auto- matica Sinica, 2018, 44(11): 2011-2022.

【10】 夏清, 窦文生, 郭凯文, 等. 区块链共识协议综述[J]. 软件 学报, 2021, 32(2): 277-299.

【11】 靳世雄, 张潇丹, 葛敬国, 等. 区块链共识算法研究综述 [J]. 信息安全学报, 2021, 6(2): 85-100.

【12】 马兆丰. 区块链技术开发指南[M]. 北京: 清华大学出版 社, 2021.

【13】 ABRAHAM I, MALKHI D, NAYAK K, et al. Solida: a blockchain protocol based on reconfigurable Byzantine consensus[J]. arXiv:1612.02916v2, 2016.

【14】 As Ghash.io’s total hashrate approaches the feared 51% mark, there has been no official word from the pool’s operating exchange, CEX.IO.[EB/OL] https://www.coindesk. com/cex-io-response-fears-of-51-attack-spread.

【15】 King S, Nadal S Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. self-p ublished paper. August 2012

【16】 Iddo Bentov, Charles Lee, Alex Mizrahi, et al. Proof of Activity: Extending Bitcoin's

【17】 Proof of Work via Proof of Stake[J]. 2014.
Kwon Y , Kim D , Son Y , et al. Be Selfish and Avoid Dilemmas: Fork After Withholding (FAW) Attacks on Bitcoin[J]. 2017.