DOI:10.19729/j.cnki.1009-6868.2018.06.002
网上出版地址:http://kns.cnki.net/kcms/detail/34.1228.TN.20181119.0929.002.html

区块链共识机制发展与安全性

Development and Security of Blockchain Consensus Mechanism

王李笑阳/WANG Lixiaoyang
秦波/QIN Bo
乔鑫/QIAO Xin
(中国人民大学,北京 100872)
(Renmin University of China, Beijing 100872, China)

中图分类号:TN929.5 文献标志码:A 文章编号:1009-6868 (2018) 06-0008-005

摘要: 在总结了共识机制发展的基础上,着重对共识机制当前存在的攻击威胁以及防范策略进行解析,并据此提出了区块链共识机制的4种信任基础即对数学、密码学的信任,对节点注重自身利益的信任,多人信任以及人为信任。指出目前共识机制发展方向之一是同一信任之下的信任对象替换。

关键词: 共识算法;安全性;区块链;分布式系统;拜占庭容错

Abstract: The attack threats and preventive strategies existing in consensus mechanism are analyzed in this paper, and four trust bases of blockchain consensus mechanism are put forward, including trust in mathematics and cryptography, trust in nodes focusing on their own interests, multi-person trust and artificial trust. Finally, it points out that one of the development directions of the current consensus mechanism is the replacement of trust objects under the same trust.

Key words: consensus algorithm; security; blockchain; distributed system; Byzantine fault tolerance

区块链本质上是一种去中心化的、节点与节点之间地位平等的数据库,其概念首次出现在中本聪的《比特币:一种点对点式的电子现金系统》一文中[1]。区块链通过运用加密算法、时间戳、共识机制和奖励机制,帮助陌生的节点建立了信任,目前广泛应用于代币以及分布式系统之中。区块链有着匿名性与安全性的特点,避免了中心化带来的数据丢失风险和管理问题。在区块链基础上,又延伸出超级账本、智能合约等概念。作为区块链中构建信任的核心,共识机制也愈发受到学界的不断关注。

由于区块链中节点众多,节点地理分布较广,且不同节点之间的通信存在延迟,因此需要一种算法决定新块的记账权以保证节点数据的一致性,这种算法被称为共识机制[2]。共识机制以所有诚实节点数据保持一致为目标,同时要求在节点互相平等的情况下明确记账权的归属。由于共识机制的存在,用户无需信任交易,另一方同时也无需信任第三方机构即可完成交易。区块链支持多种共识机制,这些共识机制在效率、安全性、资源消耗等方面各不相同,因此文章中我们着重探讨了常见共识机制的发展历史、效率以及安全性。

收稿日期:2018-10-17
网络出版日期:2018-11-19
基金项目:国家重点研发计划(2017YFB1400700)、国家自然科学基金面上项目(61772538,61532021)、国家自然科学基金重点项目(91646203,61672083)、信息保障技术重点实验室装备预研基金项目(61421120305162112)、"十三五"国家密码发展基金密码理论课题(MMJJ20170106)

1 共识机制发展

1.1 共识机制的概念

共识机制,即多个个体达成一致的机制。共识机制可以根据达成共识的个体,分为算法共识和决策共识2类[3]。算法共识致力于研究复杂的网络环境下,去中心化的网络如何达成一致的问题,本质是多个机器达成共识。决策共识目的是帮助人达成一致,在分布式人工智能领域较为常见。区块链中共识算法属于前者,目的在于在多个节点中记录同样的账本。区块链中共识机制要求满足2个性质:一致性,即不同的节点记录的数据必须相同;有效性,节点记录的数据格式和内容必须满足区块链规则。

1.2 非拜占庭容错共识机制

共识问题,首先在数学界受到关注。早在1959年,EISENBERG E和GALE D研究了特定条件下如何在一组个体中形成共识概率分布问题。随后共识问题受到了不同学界的广

泛关注。

在计算机界，尤其是分布式系统部分，共识问题引起了广泛关注。在共识问题的发展过程中，首先仅考虑了节点的可靠性，之后加入了容错问题，但节点依然要求相对可信。在当前常用的共识算法中，许多算法允许节点随意加入网络而不要求较高的可信性。

1989年，LAMPORT L已经提出了Paxos算法[4]，但由于Paxos算法过程较为复杂，且文章内容过于晦涩难懂，直到1998年才通过评审。此种算法基于消息传递模型，适用于多个过程需要达成共识的场合。

2013年，ONGARO D和OUSTERHOUT J在《In Search of An Understandable Consensus Algorithm》一文中提出了Raft共识算法[5]。作者基于Paxos进行了改进，使之更容易理解。它与Paxos相当，对构建实际系统起了促进作用。目前百度公开了Raft开源实现代码。

验证池共识机制在基于传统的共识算法上进行了改进，适用于几大商业中心的联合建链。该方案是基于传统的拜占庭容错（BFT）及其变种的共识方案，需要参与者能够相互辨识，不需要发币即可实现。验证池算法十分高效，可以实现秒级共识。

1.3 BFT上的突破

拜占庭将军问题，指的是地理上有一定间隔且可能不诚实的节点如何达成一致的问题。BFT指的是在整个系统中节点共有n个，最终要求诚实节点达成一致的情况下最多允许多少非诚实节点。经典算法下，要求非诚实节点数量t与整个系统节点数量n满足$n \geq 3t+1$。最早在1999年的《Practical Byzantine Fault Tolerant》[6]一文中作者就给出了容错量为1/3的算法。在分布式数据库中，为了避免部分服务器被黑客侵入造成整个网络崩溃的问题，采用了带有容错的公式算法。更进一步地，中本聪在设计区块链网络时提出了创新算法思路，增加了提出议案的经济成本，采用经济惩罚来制约破坏者。

2008年，中本聪提出了工作量证明（PoW）共识机制。该共识机制沿用了PoW的概念[7]。这一算法要求节点在提出议案之前必须进行大量工作（运算），并且提出议案时必须同时提交做出了大量工作的证明，这一方案将节点容错量转换为算力容错量，对女巫攻击进行了有效防范，可以允许节点自主添加到网络。在此之后提出的Proof of X的共识方案也是基于此种思想。传统分布式网络要求节点需要相对可信且进入网络需要认证，而这一共识机制使其变为了任意节点均可加入网络，使比特币可以应用于现实环境。

1.4 BFT共识算法与应用

早在中本聪提出比特币之前，BFT算法已经存在，1999年LISKOU B等提出了实用拜占庭容错算法。该算法达成共识需要“请求、预准备、准备、确认、回应”5个步骤。其中“预准备、准备、确认”3个步骤用于保障一致性。该算法虽然拥有1/3的容错性，但并不能防范女巫攻击，因此不能用于公有链类型货币中。实用拜占庭容错算法（PBFT）是传统一致性算法的改进，算法十分高效，在不需要货币体系的许可链或者私有链中较为常用。目前，IBM创建的超级账本就是使用了该算法作为共识机制。

秉持分布式系统无法同时兼顾一致性、可用性与分区容忍性（CAP）原理[8]，中本聪设计了PoW共识机制。现阶段常见共识算法其中一类为证明类共识，即Proof of X共识方案，是在PoW共识方案之上的变种，将PoW改换为其余证明。PoW算法现阶段依然盛行，使用PoW共识的代表货币比特币依然占据最大市值。

2011年7月，一位名为MECHANIC Q的数字货币爱好者首次提出权益证明（PoS）共识算法[9]。该算法以节点持有币数乘持有时间作为一个节点的权益，当前权益最高的节点最可能获得生成新块的权力。点点币、黑币采用了PoW与PoS混合的共识算法，同时以太坊共识机制拟采用PoW与PoS混合的方案。

SCHWARTZ D提出了瑞波协议共识算法，该算法在产生新块之前要求多轮投票，不需要挖矿。此算法较为高效，但BFT能力为仅$(n-1)/5$且节点必须提前确定。代表性应用为瑞波币。

2013年8月，股份授权证明（DPoS）算法由比特股项目提出。该算法根据权益投票选举，选举中得到票数最多的前N个节点成为“代表”，轮流产生新块。DPoS目前应用于EOS中，支持了EOS的高效率交易。

2015年，小蚁链（NEO）白皮书提出授权拜占庭容错（DBFT）共识算法。DBFT允许大规模节点参与投票，拜占庭容错量为1/3。DBFT在生成新的区块前需要先经过投票。为了减少资源消耗，NEO需要通过投票确定多个记账人组成记账人团体，记账人团体间按BFT算法达成一致。

当前阶段，共识算法呈现出百花齐放的态势，例如2-hop[10]，限制51%攻击者在拥有51%以上算力的同时还需要拥有51%以上的权益。目前燃烧证明（PoB）、活跃证明（PoA）等共识机制成为了新研究方向。另外，存在共识算法在PoW基础上添加了Ghost协议，将无用的挖矿算力转换为解决有效问题。这些算法大多是PoW、PoS或者传统一致性算法的改进或混合，《区块链共识算法发展现状与展望》[3]一文将当前的共识协议进行总结并对其脉络进行梳理，指出了共识协议的发展方向。

2 共识机制分析

2.1 共识机制本质

区块链的创新在于在去中心化系统中如何取得信任，并以此获得可

容错性、抗攻击性、抗共谋性。而作为取得信任的核心，共识机制是区块链的神韵。目前，共识机制面对场景多种多样，共识机制的设计也多种多样，然而共识机制的本质始终相同，即消耗资源以换取信任。因此，共识机制的评判标准可以总结为“消耗多少资源，换取多少节点的信任，换取信任的程度，换取信任的速度，换取是否需要前提条件”，即资源消耗问题、节点扩展性问题、安全性问题、效率问题以及开放性问题。不同的场景中对以上问题的注重程度不同，因此所适用的共识机制不同，例如：大额资金交易过程中安全性的重要程度远远高于资源消耗的重要程度，因此大多选择 PoW 共识机制。而小额资金交易过程中，对效率要求较高，因此 DPoS 是一个较好的选择。

共识机制使用资源换取效率的过程并不是凭空产生的，而是有着一定的前提。当前共识机制信任来源总结如下，其中一种共识机制不一定基于全部信任来源：

（1）对数学、密码学的信任。任何共识机制都不能离开数学基础，例如：PoW 建立在哈希函数的单向性之上，任何挖矿手段也都需要数学的参与，甚至随机选择过程中同样需要数学知识。对数学的信任是最有力的信任，人为条件不能改变这种信任。

（2）相信节点注重自身利益。此种信任是强有力的信任，中本聪曾经提到：占据整个系统 51%算力的节点为了自身利益，会自动维护整个系统，而不至于发动攻击。这种思想即建立于节点足够理性、足够注重利益的基础之上。同时一些保证金制度、投票制度同样基于此种信任。

（3）多人信任。多人信任是指大部分认定的即为正确。这种信任借用了在生活中的信任，例如：只需要一定数目的商家支持比特币支付，那么比特币就可以流通。在 PoW 共识中，多算力认定的数据即为正确。多人信任不仅局限于人，同时也可能为算力、权益等。目前存在的“一中央处理器（CPU）一票”思想也是基于此种信任，选举类共识机制是基于此种信任的典型代表。

（4）人为信任。人为信任包括身份认证和证书等其他事先约定的信任。无论是在传统的一致性算法还是在区块链共识算法中都十分常见。分布式系统中的管理员是身份认证的典型代表。在区块链中一些联盟链需要证书认证都基于此种信任。基于人为信任会极大影响区块链的去中心化程度，但由于事先约定的缘故，不需要大量资源换取信任，是代价最小的一种方式，同时可能换取效率的提升。

同时，在区块链中共识机制与激励机制息息相关，许多共识机制的改进是为了更好地设计激励机制，文章中我们对此不做讨论。

2.2 PoW、PoS、Dpos 详情

目前存在的主流共识机制大多为 PoW 的改进（PoX 系列）、PoS 的改进、传统共识算法的改进或者 PoW 与 PoS 的结合。虽然共识机制经过多年改进，仍然有着部分缺陷，面临着严重威胁。本文针对 PoW、PoS、DPoS 三大共识机制对其基本方案、效率以及面临攻击和问题进行探究。

（1）PoW：是目前数字货币最为普遍的算法之一，代表案例为比特币。比特币效率较低，生成一个区块时间为 10 min，不能适用于小额快速交易。参照《Mastering Bitcoin》[11]中的详细描述，挖矿公式简记为 H(*block header*) < *difficulty*，其中 *block header* 为区块头，H 为某一哈希函数，*difficulty* 为挖矿难度。挖矿难度根据生成块的时间进行调整，保证生成块的时间为 10 min 左右。矿工只能通过遍历的方式使区块头满足上述公式，遍历的过程即为工作量。PoW 共识较为安全但效率不高且存在大量算力浪费。该共识机制下节点加入不需要验证，因此去中心化程度较高，但目前存在矿池集中的现象。

（2）PoS：是当前数字货币的典型共识算法之一，在最早的点点币版本中，挖矿难度同代币数量与持有时间的乘积成反比。挖矿公式为：$H(H(B_{prev}),A,t)\leqslant \text{balance}(A)\text{m}\times Age$，其中 H 为某一哈希函数，$H(B_{prev})$ 为对上一块进行哈希运算，t 为时间戳，balance(A) 为余额，m 为事先定义值，*Age* 为持币时间。目前改进方案中，权益与 *Age* 不再线性相关。由于不再花费大量时间进行运算，PoS 速度较快，效率较 PoW 高。

（3）DPoS：意为股份授权证明，同样秉持着权益越高越容易计算新块的思想。该方案类似于股份制公司。用户根据持有代币的多少拥有不同数量的选票，同时可以投票选举相对可信的代表，并且由代表轮流产生新块。在比特股中，代表的数量被限定为 101 个。该算法效率极高，使用该共识算法的 EOS 号称每秒百万级处理速度，然而要求代表相对可信，去中心化程度不如前二者。

2.3 共识算法攻击方式

文章中我们仅讨论针对共识机制的攻击方式，并不考虑例如双花攻击、日蚀攻击、整数溢出攻击、分布式拒绝服务（DDoS）等针对区块链其余部分的攻击方式。白帽汇安全学院列举了 5 种针对共识机制的攻击方式[12]，部分攻击方式仅针对部分共识算法。

（1）短距离攻击。短距离攻击步骤为：首先向全网提交一个交易，然后攻击者试图回滚该交易，攻击者在该交易之前的区块上继续进行挖矿，在该交易得到 n 次确认后，若不含该交易的分叉区块数足够长，则该分叉成为主链，成功回滚交易。

短距离攻击的典型代表是贿赂攻击。贿赂攻击的核心思想在于使用贿赂促使节点选择在对攻击者有利的链。典型攻击步骤如下：

1）攻击者购买商品，并使用数字

货币支付；

2）商户开始等待交易入链；

3）攻击者宣称奖励不包含此次交易的最长链，如果这条主链被广泛接受，攻击者被认为没有交易；

4）当步骤3中产生的链足够长时，攻击者使用更大的奖励贿赂一部分矿工生成包含此次交易的链条。虽然存在更长主链，但矿工为了自身利益，会选择从之前开始重新挖矿；

5）在此次交易得到6次确认之后，攻击者顺利地造成了交易得到确认而主链上并没有此笔交易的情况，此时攻击者停止奖励；

6）货物到手，由于包含交易的链较不包含交易的链短，不包含交易的链成为主链。

对于矿工而言，如果不存在奖励（贿赂）的情况下，是否添加攻击者进行的交易获得的奖励是相同的，因此攻击者在步骤3只需要较少奖励即可诱使矿工在主链中不加入这笔交易。攻击者在整个攻击过程中，只需要贿赂金额小于商品金额即可攻击成功。

对于不等待确认的商户来说，只需要很小甚至不需要贿赂即可简单的促使这笔交易失效。

（2）长距离攻击。长距离攻击与短距离攻击不同，指攻击者在拥有一部分资源的情况下，直接对已经存在的区块进行分叉，可能获得更多的挖矿奖励或者否认某笔交易。

长距离攻击的代表为51%攻击，恶意节点占据了整个节点的主要部分。这一攻击和共识机制的去中心化程度有着密切联系，常用于采用PoS共识的区块链和小型采用PoW共识的系统中。中本聪在提出比特币构想中秉持了大多数原则，即大多数算力所在的链即为正确的链。为了获得挖矿奖励，对于诚实的节点而言，在最长的链上生成区块是有利的。由于生成新的区块的权力只与算力相关，在大部分节点诚实的情况下，对攻击者有利的链长度赶超经过6次确认的合法区块链概率极低。然而，假设攻击者拥有系统一半以上的算力，那么经过足够长时间之后必然可以使整个系统按照攻击者想法运行。中本聪认为：拥有51%算力的攻击者是系统的实际受益者，在足够理性的情况下并不会攻击系统。然而，现实中已经存在51%算力攻击的实际案例：一些老牌大型PoW共识区块链矿工入侵新型PoW区块链。在PoS中不要求算力，生成块的速度相对较快。因此，攻击者可能期望重写整个区块链。

目前已有学者在在51%攻击基础上进行改进，大约只需要1/3的算力即可达到与51%攻击相同的效果。

（3）币龄累积。币龄累积是针对初期PoS共识机制的常见攻击方式，不存在于PoW。因为持币时间越长，获得记账权的概率越大。在攻击者拥有足够代币之后，可以通过累积时间来达到控制网络新生成块的目的。在代币足够的情况下，攻击者甚至可以将自身代币分散于多个节点，这一攻击方式可以帮助攻击者多次生成有利块，比如回滚以进行双花攻击。占有代币1%的攻击者可以通过2个月不进行交易来进行攻击。基于同样的理由，PoS可能出现冷启动的问题。

（4）预计算。在新一代的PoS共识机制中，挖矿公式可简写为H(H(B_{prev}),A,t)≤balance(A)m。由于新块的挖矿只与时间、余额以及上一块的哈希值有关，因此控制当前块的生成可以帮助攻击者得到新块的挖矿权。在某一节点拥有一定数量代币以及算力足够的情况下，该节点可以通过随机试错方式控制第N块的哈希值使得攻击者有能力对N+1块进行挖矿。

（5）女巫攻击。在《The Sybil Attack》[13]一文中，DOUCEUR J R详细地描述了女巫攻击的全过程。女巫攻击的核心思想在于：通过控制多数节点或者伪造多个节点进行攻击。女巫攻击的条件在于对等网络中实体为一个运行程序，且同一实体可以拥有多个网络身份。例如：在一投票的对等网络中，攻击者可以通过伪造多个IP达到多次投票的目的。不仅仅在区块链网络中，现今许多投票项目同样可以通过女巫攻击攻破。

2.4 可能存在的问题

（1）挖矿耗能问题。在PoW共识机制中，挖矿仅为简单的遍历，浪费了大量的算力。根据加密货币信息网站Digiconomist的数据称：目前投入到比特币和以太坊挖矿当中的电力可以在所有国家和地区消耗电力中排名第71位，其中比特币矿机消耗功率为14.54万兆瓦[14]。这些耗能仅用于交易的确认，造成了巨大的浪费。同时，挖矿造成了显卡等产品的大量损耗，造成产品单价激增。

（2）去中心化程度不足问题。在PoS以及PoW共识机制中，节点与节点之间地位完全平等，因此去中心化程度较高。然而由于比特币等货币算力不断上涨，单个设备挖矿已经很难获得挖矿的奖励。促使一些“bitcointalk”上的极客开发出一种可以将少量算力合并联合运作的方法，使用这种方式建立的网站便被称作“矿池”。对于比特币而言，目前全球约70%的算力在中国矿池手中，这可能会造成去中心化程度不足与51%攻击。由于PoS对硬件要求较小，普通计算机可以挖矿，因此去中心化程度更高。对于DPoS而言，节点之间并不完全平等，因此去中心化程度不如PoW与PoS。

（3）冷启动问题。对于PoS共识机制而言，持币量和持币时间的增长会降低挖矿难度。因此在PoS共识下，初期持有代币的节点更加倾向于不进行交易，以获得挖矿利润。这就会造成代币不流通的问题，系统的启动较为困难。

（4）账本分叉问题。在区块链中，通常以最长的链作为主链，矿工在最长的链上进行挖矿。在PoW共

识算法下，由于矿工算力有限，面临多条链时，矿工通常会在最长链上进行挖矿。然而在PoS共识机制下，矿工为了自身利益，通常会选择多个链进行挖矿，这可能导致区块链的分叉。同时，攻击者如果使用了预计算与币龄累积攻击同样可能造成账本分叉。

2.5 共识算法的防范与改进

（1）PoW。由于PoW要求大量运算力，因此贿赂攻击很难实现，攻击者需要贿赂大部分节点才可以实现贿赂攻击，这往往得不偿失。同样由于挖矿需要大量算力，女巫攻击失去了效果。同时51%攻击要求攻击者拥有51%算力，攻击条件十分苛刻。在新生PoW链中，为了防止原有的大型PoW链矿工发动51%攻击，往往改动地址生成过程中的哈希函数。针对PoW耗能过高问题，目前部分节点采用Ghost协议，此协议将无用的挖矿改为了计算大素数等数学问题，部分解决了耗能问题。

（2）PoS。对于短距离攻击，最常见的解决方式为在PoS共识机制中引入保证金和惩罚措施，这基于“节点注重自身利益”这一条件下，目前以太坊拟采用casper协议抵御攻击。在引入保证金机制后，节点会为保证金反对做出对区块链不利的决策。惩罚措施可以使节点得不到攻击者事先声明的报酬，促使节点做出对区块链有利的决策。针对币龄累积攻击，通常限制持币时间对挖矿难度的降低作用。蜗牛币提出了股份速率证明（PoSV）机制，将难度函数改进为指数衰减函数。在PoSV共识下，节点累计足够长的时间之后，继续累积很难提高收益，解决了币龄累积攻击。针对冷启动问题，目前大多数区块链采取了在链初期首先使用PoW机制，中期使用PoW+PoS结合方式，最后采用纯PoS共识机制。

（3）DPoS。DPoS机制本身对短距离攻击与预计算攻击有较强防范，其余防范方式与PoS基本相似。

2.6 共识机制效率与安全性对比

共识机制经过了数年的发展，在经过探索和开放式创新之后，势必进入到性能安全性等的比拼之中。表1分别为PoW、PoS、DPoS面临的攻击威胁表。

为了保证较高的安全性，一部分共识算法在效率方面做出了退步，表2为当前主流共识机制性能、特点的对比。

总结来看：当前PoW共识机制的安全性较高、面临攻击威胁小，但效率较低；PoS和授权股权证明效率较高，但牺牲了部分安全性。传统共识机制对各种攻击防范较为到位并且效率比较高，但是大多不能进行拜占庭容错。

3 结束语

目前共识机制应用的场景越来越广泛，且不同场景下对共识机制安全性与效率要求不同，能否找到一种适用于大多数场景的共识成为关键。

共识机制的发展目标在于资源消耗问题、节点扩展性问题、安全性问题、效率问题以及开放性问题5个方面的提升，例如：Ghost协议是在PoW基础之上缓解了部分资源消耗的问题。在5个维度不能同时提升的情况下根据特定情况选择牺牲一部分换取另一部分的提升同样是当前研究的热点。当前为了适应实际生活的交易，牺牲部分安全性以换取效率的共识机制十分常见，例如：DPoS机制。

根据基于方案的不同，当前共识机制可以归结为传统一致性算法的改进、PoW算法的改进、PoS算法的改进，以及PoW与PoS的结合。PoW与PoS的结合是当前共识机制的发展趋势之一，通常属于时间效率与安全性的妥协。

根据基于信任来源的不同，当前共识机制许多是在同一信任类型下的替换，例如：Proof of X类型的共识协议，通常是在多人信任之下修改信任的对象。是否可以找到一种可信

➡下转第40页

▼表1 工作量证明、权益证明、授权股权证明面临威胁

面临威胁	PoW	PoS	DPoS
短距离攻击	低	高	低
长距离攻击	低	高	高
币龄累积	低	高	高
预计算	低	高	低
女巫攻击	高	高	高
冷启动	无	高	中
挖矿耗能	高	低	低
账本分叉问题	低	高	高

DPoS：股份授权证明　PoW：工作量证明
PoS：权益证明

▼表2 共识机制性能

共识机制	时间效率	拜占庭容错	资源消耗	代表应用
PoW	高延迟	是（<1/2）	高	比特币
PoS	低延迟	是（<1/2）	低	点点币
DPoS	低延迟	是（<1/2）	低	EOS
委托拜占庭共识	低延迟	是（<1/3）	低	小蚁币
PBFT	低延迟	是（<1/3）	低	超级账本
瑞波共识	低延迟	是（<1/5）	低	瑞波币
Paxos（族）	低延迟	否	低	Chubby
Raft	低延迟	否	低	Etcd

Chubby：Google设计的提供粗粒度锁服务的一个文件系统
DPoS：股份授权证明
EOS：一种为商用分布式应用设计的区块链操作系统
Etcd：一个开源的、分布式的键值对数据存储系统
PBFT：实用拜占庭容错算法
PoS：权益证明
PoW：工作量证明