doi:10.3969/j.issn.1671-1122.2017.09.034

区块链技术中的共识机制研究

韩璇[1,2,3]，刘亚敏[1,2]

（1. 中国科学院信息工程研究所信息安全国家重点实验室，北京 100093；2. 中国科学院数据与通信保护研究教育中心，北京 100093；3. 中国科学院大学网络空间安全学院，北京 100049）

摘　要：区块链作为比特币系统中的底层技术受到了广泛关注，是解决分布式系统一致性问题的一种可行方法。区块链技术的核心是如何实现共识。良好的共识机制可提升系统性能，促进区块链技术的应用。文章从现有区块链技术中的共识机制出发，对工作量证明、权益证明和拜占庭一致性协议等基本共识机制进行总结，从安全性、扩展性、性能效率等方面对这些共识机制进行评价。未来区块链上共识机制的研究将根据各共识机制的不同特点，围绕不同共识机制的组合展开设计。

关键词：区块链；共识机制；工作量证明；权益证明；拜占庭一致性

中图分类号：TP393　　**文献标识码：**A　　**文章编号：**1671-1122（2017）09-0147-06

中文引用格式：韩璇，刘亚敏. 区块链技术中的共识机制研究[J]. 信息网络安全，2017(9)：147-152.

英文引用格式：HAN Xuan，LIU Yamin. Research on the Consensus Mechanisms of Blockchain Technology[J].Netinfo Security,2017(9):147-152.

Research on the Consensus Mechanisms of Blockchain Technology

HAN Xuan[1,2,3], LIU Yamin[1,2]

(1.*State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093, *China*; 2.*Data Assurance and Communication Security Research Center, Chinese Academy of Sciences, Beijing* 100093, *China*; 3.*School of Cyber Security, University of Chinese Academy of Sciences, Beijing* 100049, *China*)

Abstract: As the underlying technology in Bitcoin, the blockchain technology has gained wide attention. Blockchain is a kind of feasible method to solve the consistency problem of distributed system. Consensus mechanism is the core of the blockchain technology. Delicate consensus mechanism can improve system performance and promote the application of blockchain in many fields. Based on the consensus mechanisms in existing design of blockchain, this paper summarizes the basic consensus mechanisms including proof of work, proof of stake and Byzantine consistency agreement, and evaluates them from various aspects such as security, scalability, performance, etc. The future research on the blockchain consensus mechanism will be based on the different characteristics of the consensus mechanisms, and design should be carried out around the combination of different consensus mechanisms.

Key words: blockchain; consensus mechanism; proof of work; proof of stake; Byzantine consistency

收稿日期：2017-8-1

基金项目：国家重点研发计划 [2017YFB0802502]；国家自然科学基金 [61379140]

作者简介：韩璇（1992—），女，辽宁，硕士研究生，主要研究方向为信息安全；刘亚敏（1983—），女，湖南，助理研究员，博士，主要研究方向为信息安全。

通信作者：刘亚敏 liuyamin@iie.ac.cn

0 引言

区块链技术最初由中本聪在《比特币：一种 P2P 电子现金支付系统》[1] 一文中提出，为解决分布式系统的一致性问题带来新的技术思想。共识机制是分布式系统的核心。在 P2P 网络中，互相不信任的节点通过遵循预设机制最终达到数据的一致性称为共识。区块链技术设计的关键是共识机制的设计，目的在于如何解决区块链的安全性、扩展性、性能效率和能耗代价等问题。区块链技术上支持的典型共识机制有工作量证明（Proof of Work）、权益证明（Proof of Stake）和拜占庭一致性协议等机制，也包括不同机制的相互结合。

1 比特币与区块链技术概述

1.1 比特币的运行机制

2008 年，中本聪发表《比特币：一种 P2P 电子现金支付系统》[1]，提出在交易中去掉银行这一中心机构，在 P2P 网络中实现基于工作量证明的、去中心化的、分布式匿名电子现金支付系统。用户的支付行为通过交易来完成。交易只记录货币的流向，每枚货币的产生和每次交易都是可追溯的。如何监测和防止二次支付行为是支付系统最根本的安全性问题 [2]。比特币系统通过全网所有节点共同维护区块链来防止二次支付。比特币是区块链技术的第一个应用实例，比特币的兴起引发了世界各界的广泛关注 [3-7]。

用户发起一次交易，广播对该交易的签名，之后等待矿工验证交易并将这笔交易记录到区块链中。矿工在当前区块链状态下挖矿，挖矿的过程就是完成工作量证明的过程。工作量证明完成之后产生的新区块包含上一个区块的哈希值、接收到的待确认有效交易集合以及时间戳等信息。随后，矿工广播该区块，等待其他矿工对该区块进行验证并在其后继续挖矿产生后续区块。当该区块连接了一定数量的后续区块之后，就可以极高的概率相信这个区块已被写入整个网络的区块链中，其包含的交易被最终确认。

1.2 区块链技术

1.2.1 基本概念

《中国区块链技术和应用发展白皮书（2016）》从应用角度将区块链技术看作是互联网时代的创新应用模式 [3]，是一种去中心化、公开透明、用于存储交易等信息的数据库，可应用于分布式数据存储、点对点传输、共识机制、加密算法等计算机技术领域。区块中存储交易等信息，区块之间前后相继，形成一条链，共同存储一系列有序交易。图 1 以比特币系统为例，介绍底层区块链的数据结构。由于上层共识机制不同，相应的区块链数据结构也略有不同。

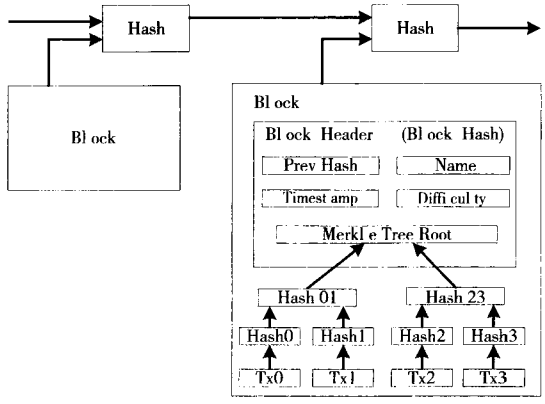

图 1 比特币系统中区块链技术的数据结构

也可以将区块链看作是一种分布式数据库。与分布式数据库不同之处在于，区块链技术中的每一个节点保存的区块链前缀部分都是完全相同的，仅区块链末端有所差异。

区块链本身的数据结构和共识机制使得其具有防篡改的性质。区块之间都通过密码学证明的方法连接在一起。当主区块链具有足够长度时，若对其中的某一区块内容进行增加、修改、删除等操作，其后所有区块都将受到影响，由此就破坏了前后相继的链式结构。此时，就必须通过一系列的密码学证明对后续区块进行修改。如果被篡改区块处于主区块链中靠前的位置，则篡改区块的代价要远超篡改者所具有的能力和篡改后可获得的利益。

在区块链中，除了区块之间的连续性外，数据的每一次变更都通过合法的数字签名存储在区块链上。区块链上记录着一条数据从产生到消亡之间的每一次修改，提供了数据的可追溯性。数据可追本溯源也间接保证了数据的公开透明性。

1.2.2 应用场景

由于区块链技术具有去中心化、防篡改、可追溯等特点，吸引了各国政府的高度关注。国内外科研机构和科技金融公司也纷纷展开了对区块链理论研究和实际应用的探索。2015 年，Linux 基金发起超级账本（Hyperledger）开源项目 [4]，提供开放式的区块链应用开发平台，推进区块链技术的研究。世界经济论坛在 2016 年金融服务会议上对如何借助

区块链技术重塑金融服务进行了分析和展望[5]。我国央行也关注区块链和数字货币的发展[6]，开始尝试利用区块链技术设计数字票据交易平台原型。

目前，区块链技术与金融行业相结合的项目众多[7]，尤其是第二代区块链技术智能合约（Smart Contract）[8]提出以后，区块链技术在解决跨机构跨行业的金融支付、结算、清算业务中的优势日渐突出。此外，区块链技术在金融服务、供应链服务、公共服务、公共慈善和物联网等多个领域都具有极大的潜在价值。表 1 是区块链技术在部分行业中的应用场景。

表 1 区块链技术的应用场景

行业	应用实例
金融服务	金融交易支付（跨机构、跨境支付），结算，清算，保险，证券，众筹
供应链服务	供应链金融、供应链溯源
公共服务	知识产权保护、版权保护、共享经济、档案管理、身份认证、数字病历
公共慈善	公共捐赠平台、善款追踪与管理
物联网	物品的溯源、追踪、仿伪、认证

1.3 共识机制

1.3.1 基本概念

区块链作为一种按时间顺序存储数据的数据结构，可支持不同的共识机制。共识机制是区块链技术的重要组件。区块链共识机制的目标是使所有的诚实节点保存一致的区块链视图，同时满足两个性质[9]：

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诚实节点记录在自己的区块链中。

1.3.2 评价标准

区块链上采用不同的共识机制，在满足一致性和有效性的同时会对系统整体性能产生不同影响。综合考虑各个共识机制的特点，从以下 4 个维度评价各共识机制的技术水平：

1）安全性。即是否可以防止二次支付、自私挖矿[10]等攻击，是否有良好的容错能力。以金融交易为驱动的区块链系统在实现一致性的过程中，最主要的安全问题就是如何防止和检测二次支付行为。自私挖矿通过采用适当的策略发布自己产生的区块，获得更高的相对收益，是一种威胁比特币系统安全性和公平性的理论攻击方法。此外，Eclipse 攻击[11]控制目标对象的网络通信，形成网络分区，阻隔交易传播。Sybil 攻击[12]通过生产大量无意义的节点影响系统安全性。

2）扩展性。即是否支持网络节点扩展[13]。扩展性是区块链设计要考虑的关键因素之一。根据对象不同，扩展性又分为系统成员数量的增加和待确认交易数量的增加两部分。扩展性主要考虑当系统成员数量、待确认交易数量增加时，随之带来的系统负载和网络通信量的变化，通常以网络吞吐量来衡量。

3）性能效率。即从交易达成共识被记录在区块链中至被最终确认的时间延迟，也可以理解为系统每秒可处理确认的交易数量。与传统第三方支持的交易平台不同，区块链技术通过共识机制达成一致，因此其性能效率问题一直是研究的关注点。比特币系统每秒最多处理 7 笔交易，远远无法支持现有的业务量。

4）资源消耗。即在达成共识的过程中，系统所要耗费的计算资源大小，包括 CPU、内存等。区块链上的共识机制借助计算资源或者网络通信资源达成共识。以比特币系统为例，基于工作量证明机制的共识需要消耗大量计算资源进行挖矿，提供信任证明完成共识。

2 现有的共识机制

2.1 工作量证明

最初提出工作量证明机制是为了防止垃圾邮件[14]。在比特币系统中，采用工作量证明机制保证所有节点对一个待确认交易集合达成一致。只有完成工作量证明的节点才能提出这一阶段的待定区块，之后网络中的节点在这个区块后继续尝试完成工作量证明，产生新的区块。当某一节点收到两个不同的待定区块时，选择链更长的那个区块进行验证。链越长意味着该链所包含的工作量越多。

工作量证明通常包含 3 个算法[15]：产生挑战 c 的随机算法、生成 s 解决挑战 c 的算法和验证挑战 c 是否被 s 解决的算法。工作量证明机制中用到的随机算法都是基于计算问题的。在比特币系统中，用于产生挑战 c 的随机算法是基于 SHA-256 的，挑战 c 由当前区块链的状态决定。解决挑战 c 就是寻找一个 s，使得其与挑战 c 通过 SHA-256 可以映射到一个以连续几个 0 开头的二进制困难系数上，表示为

$$Hash(s,c) < Difficulty \quad (1)$$

工作量证明机制所选取的计算问题要满足如下性质：

1）伪随机性。保证节点完成工作量证明的概率仅依赖于自身所占有的计算资源的比例，保证相对公平性。

2）难度可控。所选取的计算问题可根据近期网络计算资源波动进行适度调整，保证系统有效运行。计算问题难度过高，则生成区块的时间间隔过长，影响系统效率；难度太低，则完成工作量证明过于容易，会产生分叉，影响系统一致性。

3）可公开验证。由于去中心化的性质，要求计算问题的求解结果可通过简洁的操作公开验证。

采用工作量证明机制可以实现区块链的一致性。当区块链很长时，除了结尾的几个区块，其余已得到全网确认，实现了一致性。节点可自由加入区块链，节点的加入或撤离不会影响区块链的一致性和安全性。每个节点完成工作量证明的概率由它所拥有的计算资源决定，攻击者无法通过创建多个公钥地址来提高自己完成工作量证明的概率，这样可以有效抵御 Sybil 攻击。同时在诚实方拥有的计算资源占多数的情况下，可有效抵御二次支付，保证系统的安全性。

然而，工作量证明机制也存在一些问题。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。例如，比特币系统平均 10 分钟产生一个区块，需等待 6 个后续区块进行确认，这样对于一个交易，需等待近 60 分钟才能保证被确认。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 的矿池的总的算力所占比例已经过半[16]，对系统的安全性和公平性造成严重威胁。第三，工作量证明过程通常是计算一个无意义的序列，需要消耗大量计算资源、电力能源，造成浪费，即使后来提出的有用的工作量证明机制（Proof of Useful Work）[15] 尝试通过求解正交向量、3SUM、最短路径等问题，代替寻找无意义的二进制数来抵消需要消耗的资源，仍无法解决效率等问题。

2.2 权益证明

由于工作量证明机制资源消耗大且计算资源趋于中心化，权益证明机制受到广泛关注。如果把工作量证明中的计算资源视为对区块进行投票的份额，那么权益证明就是将与系统相关的权益作为投票的份额。合理假设，权益的所有者更乐于维护系统的一致性和安全性。

假设网络同步性较高，系统以轮为单位运行。在每一轮的开始，节点验证自己是否可通过权益证明被选为代表，只有代表可以提出新的区块[17]。代表在收到的最长的有效区块链后提出新的待定区块，并将自己生成的新的区块链广播出去，等待确认。下一轮开始时，重新选取代表，对上一轮的结果进行确认。诚实的代表会在最长的有效区块链后面继续工作。如此循环，共同维护区块链。

与工作量证明类似，单纯的权益证明也包含 3 个算法：产生挑战 c 的随机算法、验证节点权益状态 s 是否可解决挑战 c 的算法和公开验证挑战 c 是否被 s 解决的算法。与工作量证明的不同点在于，能否解决挑战 c 仅与节点拥有的权益有关，与节点拥有的计算资源无关。节点所占权益越多，被选为代表的概率就越大。多数情况下，本地验证算法和公开验证算法是相同的。例如，PPCoin[17] 采用交易金额和币龄作为权益的两个因子，挑战 c 由当前状态决定，包括获得的最长的有效区块链和权益的分布情况。验证算法验证以当前状态 c 和该节点拥有的一个尚未支付的交易 s 作为输入得到的哈希值是否满足以下条件，即

$$Hash(s,c) \leqslant d \cdot s.time \cdot s.value \quad (2)$$

其中，当前时间以秒为单位，逐渐增加。该节点每一秒都可以进行一次新的尝试，验证是否被选为代表。参数 d 用来调节选代表的时间间隔和代表数量。

权益证明机制在一定程度上解决了工作量证明机制能耗大的问题，缩短了区块的产生时间和确认时间，提高了系统效率，但目前尚没有完善的基于权益证明的区块链的实际应用。权益证明每一轮产生多个通过验证的代表，也就是产生多个区块，在网络同步性较差的情况下，系统极易产生分叉，影响一致性。若恶意节点成为代表，就会通过控制网络通信，形成网络分区。向不同网络分区发送不同待定区块，就会造成网络分叉，从而可进行二次支付攻击，严重影响系统安全性。恶意敌手也可以对诚实代表进行贿赂，破坏一致性。权益证明的关键在于如何选择恰当的权益，构造相应的验证算法，以保证系统的一致性和公平性。不

当的权益会影响系统公平性。例如，PPCoin 采用币龄作为权益的一个因子，若部分节点在进入系统初期就保持一部分小额交易不用于支付，则币龄足够大，该节点更容易被选为代表，影响系统公平性。

2.3 拜占庭一致性协议

拜占庭一致性协议最初用于小范围服务器复制问题，后来服务器数量可扩展至数十台。拜占庭一致性协议主要研究在分布式系统中，如何在有错误节点的情况下，实现系统中所有正确节点对某个输入值达成一致。

以实用拜占庭容错协议（Practical Byzantine Fault Tolerance, PBFT）[19] 为例，协议要求在有 $3f+1$ 个节点的分布式系统中，失效节点数量不超过 f 个。实用拜占庭容错协议的每一轮包括 3 个阶段：预准备阶段、准备阶段和确认阶段。在预准备阶段，由主节点发布包含待验证记录的预准备消息。接收到预准备消息后，每一个节点进入准备阶段。在准备阶段，主节点向所有节点发送包含待验证记录的准备消息，每一个节点验证其正确性，将正确记录保存下来并发送给其他节点。直到某一个节点接收到 $2f$ 个不同节点发送的与预准备阶段接收的记录一致的正确记录，则该节点向其他节点广播确认消息，系统进入确认阶段。在确认阶段，直到每个诚实节点接收到 $2f+1$ 个确认消息，协议终止，各节点对该记录达成一致。

在去中心情况下，利用拜占庭一致性协议可以实现区块链的一致性，剔除多余的计算量，避免资源浪费。此外，在某一时刻，只有一个主节点可以提出新区块，其他节点对该区块进行验证，避免分叉，缩短了交易确认和区块确认时间，提高了系统效率。

拜占庭一致性协议在安全性和扩展性方面还存在问题。拜占庭一致性协议的安全性依赖于失效节点数量的限制，失效节点数量不超过全网节点的 1/3。在区块链系统中，恶意节点可通过实施 Sybil 攻击产生多个节点，使其控制的节点比例超过全网节点的 1/3，从而破坏系统的一致性和安全性。拜占庭一致性协议的效率依赖于参与协议的节点数量，该协议不适用于节点数量过大的区块链系统，扩展性差。此外，一轮是否可以取得共识也依赖于主节点是否诚实，若主节点提出无效区块，则本轮不会产生区块，影响效率。

2.4 共识机制的组合

对现有区块链上的工作量证明、权益证明和拜占庭一致性协议等共识机制从一致性、安全性、扩展性、性能效率、资源消耗等方面进行对比分析，它们在区块链应用上的优劣如表 2 所示。

表 2 区块链上的共识机制对比

共识机制	一致性	安全性（容错率）	扩展性	性能效率	资源消耗
工作量证明	有分叉	<50%	差	高延迟	高
权益证明	有分叉	<50%	良好	低延迟	低
拜占庭一致性协议	无分叉	<33%	差	低延迟	低

针对各共识机制的优缺点，可尝试将不同的共识机制结合起来，形成新的共识机制 [20,21]。

1）工作量证明和权益证明的结合

采用工作量证明机制时，节点可通过自私挖矿策略获得更高的相对收益，影响系统的公平性和安全性。2-hop 区块链尝试将工作量证明和权益证明相结合 [20]，利用权益证明机制减少系统的资源消耗，提高公平性和安全性。系统以轮为单位，每轮包含工作量证明阶段和权益证明阶段。在工作量证明阶段，节点尝试完成工作量证明，提出新区块。随后进入权益证明阶段，由完成权益证明的节点对新区块进行验证和确认。通过交替进行工作量证明和权益证明，使得系统即使出现占有大量计算资源的节点，也能保证系统的安全性。同时，削弱初始状态下计算资源占优势的节点对区块链的影响，进一步提高系统的安全性和公平性。

2）拜占庭一致性和权益证明的结合

以 Algorand 系统 [21] 为例，考虑到拜占庭一致性协议存在扩展性差等问题，Algorand 系统将权益证明机制和拜占庭一致性协议相结合，通过权益证明限制参与拜占庭一致性协议的节点数量，以提高系统的可扩展性。首先，节点通过权益证明机制验证自己是否被选为代表，通过验证的节点可提出待定区块。然后，进行新一轮的权益证明选出新的代表对待定区块的有效性进行验证。有限轮次之后，代表之间通过拜占庭一致性协议在优先级最高的区块上达成一致。通过权益证明选出代表，有效解决了拜占庭一致性协议的扩展性和效率问题，同时利用拜占庭一致性协议避免了权益证明易分叉的弱点，提高了一致性和安全性。

在保证安全性和一致性的基础上，对于共识机制的研究一直围绕在如何平衡系统的性能效率、扩展性和资源消耗等因素上。由于不同共识机制的特点不同，如何将各具

优势的共识机制巧妙组合，设计综合评价最优的共识机制，是未来研究的主流方向。

3 结束语

共识机制作为区块链技术中至关重要的一个组件，备受学术界和企业界关注[22]。良好的共识机制有益于区块链技术在理论和实践中的推广。然而，现有的可用于区块链技术的共识机制都不尽完善。对于区块链技术中的共识机制分析，可以从一致性、安全性、扩展性、性能效率、资源消耗等维度综合考量。将工作量证明、权益证明和拜占庭一致性协议等基本共识机制进行改进和组合是未来共识机制的研究重点。（责编 马珂）

参考文献：

[1] NAKAMOTO S. Bitcoin: A Peer-to-Peer Electronic Cash System[EB/OL]. https://www.researchgate.net/publication/228640975_Bitcoin_A_peer-to-peer_electronic_cash_system,2017-6-11.

[2] KARAME G O, ANDROULAKI E, CAPKUN S. Double-spending Fast Payments in Bitcoin[C]// ACM.ACM Conference on Computer and Communications Security, October 16 - 18, 2012. Raleigh, North Carolina, USA. New York: ACM, 2012:906-917.

[3] 中国区块链技术和产业发展论坛．中国区块链技术和应用发展白皮书(2016) [EB/OL]. http://www.cbdforum.cn/index/article/rsr-6.html, 2016-10-18.

[4] Hyperledger. Hyperledger Whitepaper [EB/OL]. https://www.hyperledger.org/, 2017-6-21.

[5] World Economic Forum. The Future of Financial Infrastructure: An Ambitious Look at How Blockchain Can Reshape Financial Services [EB/OL]. https://www.weforum.org/reports/the-future-of-financial-infrastructure-an-ambitious-look-at-how-blockchain-can-reshape-financial-services, 2016-8-12.

[6] 徐忠，姚前．数字票据交易平台初步方案[J]. 中国金融，2016(17):31-33.

[7] 谢辉，王健．区块链技术及其应用研究[J]. 信息网络安全，2016(9):192-195.

[8] ETHEREUM WiKi. White Paper [EB/OL]. https://github.com/ethereum/wiki/wiki/White-Paper, 2015-6-18.

[9] GARAY J, KIAYIAS A, LEONARDOS N. The Bitcoin Backbone Protocol: Analysis and Applications[A]// Advances in Cryptology - EUROCRYPT 2015 [M]. Heidelberg :Springer Berlin Heidelberg, 2015:281-310.

[10] EYAL I, SIRER E G. Majority Is Not Enough: Bitcoin Mining Is Vulnerable[J]. Computer Science, 2013, 8437:436-454.

[11] HEILMAN E, KENDLER A, ZOHAR A, et al. Eclipse Attacks on Bitcoin's Peer-to-Peer Network[C]// UsENIX. The 24th USENIX Conference on Security Symposium, August 12 - 14, 2015. Washington, D.C. Berkeley: USENIX Association, 2015:129-144.

[12] DOUCEUR J R. The Sybil Attack[A]// Peer-to-Peer Systems[M]. Heidelberg:Springer, Berlin, Heidelberg, 2002:251-260.

[13] EYAL I, GENCER A E, SIRER E G, et al. Bitcoin-NG: A Scalable Blockchain Protocol[C]// USENIX . The 13th Usenix Conference on Networked Systems Design and Implementation, March 16 - 18, 2016. Santa Clara, CA. Berkeley:USENIX Association, 2016:45-59.

[14] DWORK C, NAOR M. Pricing via Processing or Combatting Junk Mail[A]// Advances in Cryptology — CRYPTO' 92[M]. Heidelberg :Springer Berlin Heidelberg ,1992:139-147.

[15] MARSHALL B, ALON R, MANUEL S, et al. Proofs of Useful Work [EB/OL]. http://eprint.iacr.org/2017/203.pdf, 2017-2-27.

[16] 区块．全球算力分布 [EB/OL]. http://www.qukuai.com/pools, 2017-6-25.

[17] 王皓，宋祥福，柯俊明，等．数字货币中的区块链及其隐私保护机制 [J]. 信息网络安全，2017(7):32-39.

[18] KING S, NADAL S. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake[EB/OL]. http://peerco.in/assets/paper/peercoin-paper.pdf, 2012-8-19.

[19] CASTRO M, LISKOV B. Practical Byzantine Fault Tolerance[EB/OL]. http://dts-web1.it.vanderbilt.edu/~dowdylw//courses/cs381/castro.pdf,2017-4-15.

[20] DUONG T, FAN Lei, ZHOU Hongsheng. 2-hop Blockchain: Combining Proof-of-Work and Proof-of-Stake Securely[EB/OL]. http://eprint.iacr.org/2016/716.pdf, 2017-4-15.

[21] CHEN Jing, MICALI S. Algorand[EB/OL]. https://arxiv.org/abs/1607.01341, 2016-7-5.

[22] 赵阔，邢永恒．区块链技术驱动下的物联网安全研究综述 [J]. 信息网络安全，2017(5)：1-6.