

**研究生学位论文开题报告**

**报告题目 无线区块链系统中共识算法的研究**

**学生姓名 张利 学号 201818020629027**

**指导教师 姚郑/张宝贤 职称 教授**

**学位类别 工学博士**

**学科专业 计算机应用技术**

**研究方向 区块链**

**培养单位 人工智能学院**

**填表日期**

**中国科学院大学制**

**填 表 说 明**

1. 本表内容须真实、完整、准确。
2. “学位类别”名称填写：哲学博士、教育学博士、理学博士、工学博士、农学博士、医学博士、管理学博士，哲学硕士、经济学硕士、法学硕士、教育学硕士、文学硕士、理学硕士、工学硕士、农学硕士、医学硕士、管理学硕士等。
3. “学科专业”名称填写： “二级学科”全称。

目录

[1选题的背景及意义 4](#_Toc97046044)

[2国内外本学科领域的发展现状与趋势 5](#_Toc97046045)

[2.1 单链区块链共识算法 5](#_Toc97046046)

[2.1.1 基于工作量证明的共识算法 6](#_Toc97046047)

[2.1.2 基于权益证明的共识算法 8](#_Toc97046048)

[2.1.3单委员会混合共识算法 10](#_Toc97046049)

[2.1.4多委员会混合共识算法 13](#_Toc97046050)

[2.1.5其他共识算法 16](#_Toc97046051)

[2.2 基于有向无环图存储结构的区块链共识算法 17](#_Toc97046052)

[2.2.1 经典DAG区块链共识算法 18](#_Toc97046053)

[2.2.2 基于主链的DAG区块链共识算法 19](#_Toc97046054)

[2.2.3 基于平行链的共识算法 20](#_Toc97046055)

[3课题主要研究内容、预期目标 21](#_Toc97046056)

[4拟采用的研究方法、技术路线、实验方案及其可行性分析 22](#_Toc97046057)

[4.1技术路线方案 22](#_Toc97046058)

[4.1.1基于节点稳定性的无线区块链共识算法 22](#_Toc97046059)

[4.1.2基于稳定委员会的区块链共识算法 25](#_Toc97046060)

[4.1.3基于稳定分片的无线区块链共识算法 28](#_Toc97046061)

[4.1.4基于稳定主链的无线DAG区块链共识算法 31](#_Toc97046062)

[4.2可行性分析 33](#_Toc97046063)

[5研究工作计划与进度安排 33](#_Toc97046064)

[参考文献： 35](#_Toc97046065)

# 1选题的背景及意义

随着互联网的蓬勃发展和多方协作的规模的扩大，传统的第三方信任机构会伴随着较高的人为决策风险和成本。因此，在中心化机制已经无法满足大规模多方协作的安全性和可信性需求的情况下，区块链技术作为新的信用体系应运而生。

自2008年中本聪[1]提出比特币后，其底层技术—区块链技术受到了工业和学术领域的高度关注。区块链本质上是一个去中心化的数据库，结合了P2P网络、分布式数据库、共识算法、非对称加密等多种技术。区块链系统中各节点的地位平等且有相同的网络权力，不存在中心化的服务器。所有节点间通过特定的软件协议共享部分计算资源、软件或者信息内容。在不可信场景中，区块链技术提供了一种能安全可靠地进行信息与价值传递交换的协作模式，解决了多方协作面临的信任和安全问题。

区块链的发展大致经历了三个发展阶段：分为区块链1.0时代、区块链2.0时代和区块链3.0时代。在区块链1.0时代，区块链技术主要是作为数字货币的底层支撑技术。此时,区块链技术的发展与数字货币密切相关,应用普遍集中在货币转移、兑换和支付等方面。在区块链2.0时代，区块链技术主要是解决市场的去中心化，为智能合约技术的发展提供技术支持。V.Buterin[2]首次将智能合约和区块链技术结合，提出能实现智能合约编写的以太坊区块链平台。区块链为智能合约提供了可信任的执行环境,智能合约为区块链的应用超越了货币，提供了更大的兼容性。区块链3.0时代是区块链全面应用的时代，通过区块链技术构建一个大规模协作社会。此时，区块链在除了金融和经济领域外的社会生活领域应用更为广泛，比如政府、健康、科学、文化和艺术等领域。区块链技术无论是在构建信息和价值自由流通的互联网，还是在建立基于多中心数据共享的联合企业，都有着广阔的应用前景。

随着5G和物联网的普及，在具有小世界和超密集特征的无线网络中管理节点设备、共享消息和执行计算任务等面临的安全和信任问题变得难以处理。无线网络具有高灵活性、便捷性、易于网络规划和调整、故障定位容易以及易于扩展等优点。但是，无线网络节点具有移动性、通信时信道不稳定、容易受到干扰、网络拓扑动态变化和环境等因素会导致严重的网络安全问题，包括女巫攻击、无线信道劫持攻击、日蚀攻击、窃取网络资源等。这些安全问题都会对建立在无线网络上的应用产生致命伤害。

区块链的安全可信任特性可以为无线网络的应用提供安全和信任保障。将无线网络应用中数据的上传和在应用中的操作都当作区块链交易或合约来处理，则可以在传输层面保护数据和通信安全。区块链可以将无线设备中数据的上传视为由智能合约验证的交易事务，使用加密技术来确保事务信息的完整性，使用区块链技术的无线网络应用的安全性得到了极大的提高。

区块链技术可以有效地解决以无线网络作为底层网络基础设施的应用中的安全和信任问题，确保应用数据的安全性、可信性和完整性。但是，区块链技术应用于无线网络环境还面临着一些挑战。一方面，区块链系统的性能很大程度上是受共识算法的限制的。目前主流的区块链共识算法主要有工作量证明(Proof of Work, PoW)共识算法，权益证明(Proof of Stake, PoS）共识算法以及实用拜占庭容错(Practical Byzantine Fault Tolerant, PBFT)共识算法等。这些共识算法具有能耗巨大、效率低、依赖代币和网络通信复杂度高等缺点。另一方面，无线网络中节点之间网络通信可用资源的波动性和移动节点设备可用计算资源的有限性，无法满足目前需要耗费大量计算资源和稳定的网络传输数据的区块链系统的需求。因此，亟需根据无线网络的特性设计高效节能的区块链共识算法，使得融合区块链技术的无线网络应用具有很好的扩展性和安全性。

# 2国内外本学科领域的发展现状与趋势

共识算法是区块链技术的基础和核心，影响着区块链系统的可扩展性和安全性。无线区块链系统中共识算法的设计需要重点考虑系统模型和共识过程。系统模型包括网络模型、（同步、部分同步、异步）、节点模型（动态节点、静态节点）、故障模型（拜占庭故障、非拜占庭故障）、网络可用资源（功率、信道、存储资源等）；共识过程包含共识节点的选举、交易排序、区块的生成和验证以及区块上链。为了降低区块链系统中的共识时延和提高交易吞吐量，学术界和工业界对区块链共识算法开展了大量的研究。下面将阐述与本报告研究内容相关的典型工作：基于单链存储结构的区块链共识算法和基于有向无环图(Directed Acyclic Graph ,DAG)存储结构的区块链共识算法。

## 2.1 单链区块链共识算法

单链区块链系统的共识算法可以分为以下几类：基于工作量证明的共识算法、基于权益证明的共识算法、基于委员会的混合共识算法（单委员会混合共识算法和多委员会混合共识算法）和其他共识算法。

### 2.1.1 基于工作量证明的共识算法

工作量证明(Proof of Work, PoW)最早由C.Dwork和M.Naor[3]在1992年提出，用来解决垃圾邮件问题.该机制要求邮件在被发送之前必须找到某个数学难题的答案来证明发送者确实执行了一定量的工作。A.Back在1997年提出，并在2002年正式发表的Hashcash[4]通过寻找哈希函数原像实现工作量证明。在1999年，M.Jakobsso[5]正式提出了工作量证明的概念。这些工作都为比特币的共识机制奠定了坚实的基础。

为了解决无第三方交易的信任问题，中本聪[1]采用工作量证明作为共识算法为电子货币的交易达成安全共识。在区块链中，工作量证明主要用来防止敌手制造假身份发起女巫攻击。这种共识算法中所有参与共识的节点需要消耗算力解一个数学难题，通过求得的解证明自己完成了一部分计算工作来获得生成区块的权限。区块链系统通过一个链式区块链结构来确保达成共识的账本不可篡改，保证了账本的安全性。节点需要等到区块被确认后，才可以获得系统的奖励以及区块中所有交易费用。

区块链工作量证明共识算法出现之后，一些研究者针对比特币的安全性进入深入研究。J.Garay等人[6]提取和分析了比特币的协议核心，定义了区块链的共同前缀、链质量和链增长特性，证明了在算力充足和同步网络下区块链的安全性，为加密货币的共识算法提供了首个“可证明安全”模式。R.Pass等人[7]在此基础上进一步分析了区块链在部分同步的网络环境下区块链的安全性。此外，工作量证明共识算法也存在被敌手攻击的可能性，常见的攻击有日蚀攻击[8]、双花攻击以及自私挖矿攻击[9]等。I.Eya[10]分析比特币中自私挖矿的成功概率，最终证明了敌手只需要控制全网的少部分算力就能攻击系统成功。

采用工作量证明作为共识算法的区块链系统中，节点可以集中计算资源发起自私挖矿攻击而获益。为了解决比特币中挖矿资源集中化的问题，以太坊[2]设计了能够抵抗ASIC且支持轻量级客户端快速验证的基于工作量证明的共识算法Ethash。为了让拥有较少算力资源的用户获得奖励，Ethash降低了找到工作量证明的难度。但是，降低挖矿难度会提高出块速率，以太坊中出现分叉的频率也会提升。对于低算力矿池和节点缺乏分支竞争力的问题，以太坊中采用的叔块(Uncle block)机制解决链分叉问题。Ethash确保以太坊系统区块链的安全性，提升交易吞吐量，降低了交易确认延时。除了在电子加密货币上的应用，区块链也可以作为智能合约的底层技术。以太坊第一个能够运行智能合约的公共区块链平台，允许双方在没有可信第三方的情况下实现可信交易。

为了解决比特币中自私挖矿攻击导致的诚实用户链质量的下降的公平性问题，R.Pass和E.Shi[11]提出了水果链（FruitChains）。水果链使用基于工作量证明的共识算法，并且采用两种数据结构：区块和水果（Fruits）。区块和水果的产生都是通过寻找工作量证明来完成，但是生一个区块需要完成工作量证明的难度要远远高于生成水果的难度，其中水果是与交易绑定挂靠在区块下的。新挖到水果被放入有效水果集(Fruit Set)中，这个集合会随着水果的挖出不断更新。新挖到的区块将有效水果集中的水果放入到区块中，由于系统需要确保水果的新鲜度（Fresh），因此自私挖矿生成的区块和水果不会被诚实矿工接受。最终几个区块和水果的奖励会平均奖励给所属节点。在水果链中,节点不需要加入矿池就能频繁获得挖矿收益，提升了节点获取奖励的公平性。

针对比特币中ASIC设备算力集中化问题，M.H.Ashilk等人[12]提出采用回合制的过滤工作证明共识算法 (FPoW)来解决。在每一回合开始时，都会有一个一定难度级别的虚拟数学谜题来计算采矿设备的计算能力。所有基于ASIC 采矿设备都将在列表的顶部，因此系统能够找出基于ASIC的挖矿节点。根据该列表，系统会从网络中移除一些算力比其他节点更大的挖矿节点。在完成过滤后，将原工作量证明共识算法将在剩余的挖矿节点之间运行。最先找到工作量证明的挖矿节点将获得出块权限，创建一个新区块并获得奖励。在每一回合之后，网络将允许连接新节点或移除旧节点。这个共识算法可以较好的防止由于ASCI设备带来的算力集中化问题，提高参与共识的节点获得奖励的公平性。

采用工作量证明共识算法的区块链系统面临着交易吞吐量低的问题，研究者对提升交易处理速率做了深入研究。I.Eyal等人[10]提出的Bitcoin-NG也是一种基于工作量证明的共识算法。Bitcoin-NG采用的关键块和微块数据结构提升了比特币中完成一次工作量证明能够处理交易的数量。同时，Bitcoin-NG也改变了比特币的激励机制，提升了诚实矿工愿意在诚实链后添加区块的积极性，降低了区块链分叉的概率。Bitcoin-NG中共识过程将交易区块与关键块出块节点选举的过程分离开来, 提升交易吞吐率的同时保证协议的安全性和公平性。

工作量证明的共识算法面临着严重的能耗问题和算力集中化的问题。现有的基于工作量证明的共识算法主要是解决自私挖矿攻击引起的不公平问题，提升交易的处理速率。但是计算工作量证明需要投入大量的算力，这对于资源有限的节点是非常不友好的。同时，消耗大量的算力用于工作量证明的寻找并不能产生其他的效益，造成十分严重的能源浪费。基于工作量证明的共识算法只具有弱一致性，敌手可以使区块链分叉发起双花攻击来获益。工作量证明共识算法对这种攻击只能通过降低敌手的攻击意愿，并没有比较好的方式能够完全杜绝这类攻击。

### 2.1.2 基于权益证明的共识算法

针对工作量证明共识算法能源消耗巨大的问题，提出了节能的权益证明(Proof of Stake, PoS)共识算法。权益证明共识算法中节点根据拥有资产的比例来决定成为下一个出块者的概率。任何节点生成区块不需要消耗大量的算力，对环境比较友好。

由S.King和S.Nadal[13]提出的Peercoin首次引入了权益证明共识算法。该共识算法根据用户持有代币的币龄来选择生成新区块的节点。节点代币越多、持币时间越长则成为出块节点的概率越大。权益证明共识算法可以快速生成区块，具有较大的交易吞吐量和较低的交易确认延时。但是，基于权益的共识算法面临着节点长期离线和敌手攻击的威胁，主要安全攻击有无利害关系攻击[14]、打磨攻击[15]、长程攻击[16]、权益窃取攻击[17]等。

针对权益证明共识算法面临着无利害关系攻击、长期离线攻击和长程攻击的问题，V.Buterin等人[18]提出的Casper FFG是用于以太坊的基于PoS共识算法。区块产生仍然依靠以太坊的Ethash工作量证明算法，每隔50个区块出现一个检查点，验证者通过权益证明共识算法对检查点完成最终确定。Casper FGG共识算法中的检查点机制解决了纯权益证明共识算法中的长程攻击。Casper FGG采用质押机制来解决对于无利害关系攻击的问题。验证者需要将持有的以太币质押到系统的智能合约中，节点被选中的概率与其质押的以太币成正比。如果发现参与者想要发起发利害关系攻击，就没收其保证金。对于权益证明共识算法中节点长期离线的问题，也采用罚没一定数量的代币来确保节点愿意保持在线，确保系统的安全性与活性。

针对权益证明共识算法中节点长期离线问题和交易处理效率低的问题，委托权益证明(delegated proof of stake, DPoS)[19]采用委托人的方式确保系统中共识过程的高效性。权益持有者投票（票数与其权益大小成比例关系）给信任的委托人，最终选出一定数量的委托人以平等的权利轮流作为出块节点行使权利。如果委托人在委任期间未按规则产生正确区块，所有权益持有者将选出新的超级节点替代不作为的委托人，避免了共识节点长期离线的问题。委托权益证明共识算法消除了交易需要等待一定数量的区块被验证的时间，降低了交易确认延时。同时，委员会机制也避免了参与者在不同分支上生成区块的无利益关系攻击和长程攻击。DPoS以选举委托人的形式实现共识,但是为区块链系统带来了中心化问题。

针对权益证明共识算法处理交易的效率低和打磨攻击的问题，A.Kiayias等人[20]提出了一种新的基于权益证明的共识算法Ouroboros。该共识算法利用形式化的方法建立了PoS共识算法的模型,并证明了Ouroboros能够确保区块链的安全性。该共识算法将时间分为多个时期，每个时期分为多轮，每轮最多产生一个区块。在每个时期开始，共识算法根据节点所持有的权益选出这个时期的出块节点，并随机的选举出每一轮的首领节点。Ouroboros使用安全多方计算协议生成随机数来随机选举出块节点，使得共识过程在存在敌手时具有较高抗偏置性，即具有抗打磨攻击性。Ouroboros通过多方验证交易和区块的方式防止敌手对共识算法发起无利益关系攻击。Ouroboros的激励机制是将多个区块的交易费根据节点的贡献度按比例分配，这个机制激励权益持有者愿意保持在线获得收益，从而解决节点长期离线问题。

为了防止Ouroboros共识算法中敌手对出块者发起的贿赂攻击或DDoS攻击，B.David 等人[21]提出的Ouroboros Praos改进了Ouroboros中出块者的选举方式。这个共识算法中在成功生成区块之前，节点只能确定自己是否被选为出块者但不能提前判断其他节点是否被选中，这样有效防止了敌手做坏的可能。对于Ouroboros共识算法中新加入节点的安全自启问题和长程攻击问题，C.Badertscher 等人 [22] 提出了Ouroboros Genesis。共识算法中新加入的节点通过比较多个节点的链最终确定同步与其他链有共同前缀且最长的链。Ouroboros Genesis利用公共前缀的性质在没有采用检查点机制的前提下能够抵抗长程攻击,并且在通用可组合(universally composability)模型下, 形式化证明了协议的安全性。

对于权益证明共识算法中节点的离线、候选者节点选择机制被敌手偏置和腐蚀等问题，P.Daian等人[23]提出的Snow White是基于权益证明的可重配置共识算法。候选者重配置的间隔时间短暂,能够满足节点随机加入和退出网络的需求。通过重配置过程选出最近的权益拥有者作为候选者集合，然后按集合中成员权益占比随机选择每一轮的出块节点，提高了共识算法的抗偏置性。即使节点离线，这个候选人重配置机制也能够提高共识过程的安全性。Snow White中候选者集合随着系统中权益的变化而重新选择,防止敌手的后来腐化(Posterior Corruption)攻击。共识算法的激励机制是将几个区块的奖励和交易费用平均分给出块者，提高了节点参与共识的活性和公平性。同时，采用了类似于水果链（Fruit Chains）的区块和水果生成机制提高区块链的交易处理效率，提升区块链系统的交易吞吐量。

基于权益证明的共识算法虽然解决了工作量证明共识算法能耗高的问题，但是却面临着敌手攻击的危险。权益证明共识算法也是一个具有弱一致性的共识算法，因此面临着敌手利用无利益关系攻击、长程攻击和打磨攻击来发起双花攻击的。当前的研究工作主要通过押金机制来降低无利益关系攻击，通过检查点机制和单链区块链公共前缀来降低长程攻击，通过随机数机制来提高系统的抗打磨攻击性。新节点自启机制则可以根据单链区块链公共前缀来保证安全。通过增加生成单个区块处理交易的数量和降低交易确认时延可以提高共识算法的交易处理速率，但是这样的方式能够提升的交易吞吐量是非常有限的。

### 2.1.3单委员会混合共识算法

区块链混合共识算法是将经典分布式一致性算法与当前的区块链共识算法相结合，即采用PoW或PoS的方式选举特定的委员会，在委员会内部运行经典分布式共识算法生成区块。混合委员会共识算法又分为单委员会混合共识算法和多委员会混合共识算法。采用单委员会的混合共识算法选举一个委员会负责全网所有交易的处理，而多委员会的混合共识共识算法将选举多个并行运作的委员会，将全网划分为多个片区来分片处理网络中的交易。混合共识算法的一般流程是：选举委员会成员、选举委员会首领、执行委员会内一致性算法、广播区块、重置委员会。

C.Decker等人[24]提出的PeerCensus将经典的分布式一致性算法PBFT与PoW共识算法结合，利用比特币作为底层链选出一定数量的节点完成身份认证，通过在这些节点之间执行PBFT一致性协议来实现区块的生成和确认。该共识算法能够通过工作量证明认真身份来抵抗女巫攻击，执行一致性协议确保强一致性共识极大地降低链分叉概率。由于PeerCensus中节点的进入和离开都需要委员会达成共识，敌手会利用的离开检测机制不断制造离开提议的方式降低整个系统的运行效率。单委员会混合共识算法需要解决以下问题：

1. 新节点安全自启问题：共识算法需要在不依赖可信启动的方式来完成初始化委员会配置，确保节点获取交易信息真实有效和识别虚假信息。
2. 委员会选举：选择委员会成员的时候需要确保诚实成员达到一定比例。委员会内共识的运行需要由领导者发起，因此需要安全的领导者选取机制防止领导者不作为或恶意行为。
3. 委员会一致性协议：委员会内需要解决提交区块快速响应问题。可以通过降低委员会通信复杂度、计算复杂度和并行区块提高委员会内一致性算法运行效率。
4. 委员会重置：一个委员会工作时间对应一个时期，共识算法需要合理设置每个时期的长度，防止敌手腐蚀委员会成员。在委员会任期结束后，共识算法需要解决委员会成员交替时区块的处理问题和敌手干扰委员会新成员选择问题。

针对委员会成员被敌手腐蚀和委员会成员选举过程被敌手偏置的问题，E.Kokoris-Kogias等人[25]提出的ByzCoin采用滑窗方式来实现委员会重置。该共识算法采用PoW的方式防止敌手发起女巫攻击，同时采用Bitcoin-NG的思想来提升交易处理效率。为防止委员会成员被敌手腐蚀，Byzcoin采用滑动窗口的方式重置委员会。通过找到最近的144或1008个关键区块的节点进入委员会，节点的投票权由关键块的比例决定。委员会采用群体签名对微块达成共识，提高交易处理效率。相较于PeerCensus共识算法，该算法中节点的进出委员会不用委员会成员协商提高了效率。但是这个算法没有解决节点自启的问题，还面临着委员会成员更换时区块的处理问题。此外，委员会成员的更新速率取决于工作量证明，难度过高会使得委员会成员更换比较慢并且需要消耗大量计算资源。

为了解决了委员会重配置时正在进行区块处理的问题，I.Abraham等人[26] 采用Paxos思想提出了Solida共识算法。首先，系统为每个领导者赋予不同等级，新节点加入委员会重配置进入委员会之后等级增加并成为新的领导。Solida共识算法的委员重配置是利用PoW机制进行随机更新。当节点找到一个工作量证明时，该节点的生存时期增加并成为委员会领导，当一个节点长期成为领导时需要更换委员会。新领导出现将打断当前领导任期，新领导接管委员会后重新对之前被打断的区块发起共识。为了防止自私挖矿带来链质量的下降，Solida在PoW中嵌入了随机数，将每一轮共识最终得到的多个签名嵌入到区块中，保证诚实用户的链质量。但是这个共识算法中委员会成员的更新速率比较慢，这会使得委员会成员容易被敌手腐蚀。对于初始委员会的配置问题也没有解决，新节点的安全自启问题也还未解决。

为了解决初始委员会配置问题和交易的响应速度慢的问题，R.Pass和E.Shi[27]提出Hybrid consensus将PoW与BFT算法结合的混合共识机制,采用滑窗机制更换委员会成员。Hybrid consensus 共识算法首先利用Snailchain选出一个初始静态委员会，诚实节点会根据其局部链去掉尾部中不稳定的个区块，并选择前个区块的出块者作为BFT委员会成员。当诚实节点的链达到长度时第个委员会成员也是去掉尾部个不稳定区块，选择最后个区块的出块者成为委员会成员。委员会内运行BFT协议来确认交易直到收到停止命令，委员会成员会逐渐输出已确认的交易。提交的交易会被记录在每日日志中。该算法首次利用形式化的安全模型和模块化的设计建模混合共识机制，并证明了其能够满足一致性和活性等安全特性。这个共识算法中委员会成员的更新速率比较慢，这会使得委员会成员容易被敌手腐蚀。采用该共识算法的区块链也容易出现分叉，最终导致委员会成员可能会有不一致的问题。

为了解决区块链系统采用PoW和一致性算法结合的共识算法中能耗高、委员会更新时间长、交易处理效率低的问题，Y.Gilad等人[28]提出了将PoS与经典分布式一致性算法结合的混合共识算法Algorand。该共识算法采用随机可验证机制选择委员会首领和随机更换机制来重置委员会成员。首先根据上一轮的区块信息计算本轮的随机数，设置两个不同的值判定节点是否选中成为首领或委员会成员。委员会成员内部执行新的拜占庭一致性算法⋆ 来解决敌手腐蚀问题。每一轮投票的成员是利用PoS共识算法在所有权益持有者中随机选择一定数量的委员会成员, 基于PoS选择成员的方式更加快速、高效,可以快速更新委员会。Algorand具有较高的交易吞吐量和扩展性，可用于规模较大的应用场景。该共识算法具有强一致性特性，区块链分叉概率很小,交易能够得到较快速度的确认。

针对PBFT一致性算法固有的二次消息复杂性，在网络中的节点数量方面存在可扩展性问题，M.M. Jalalzai等人[29]提出了一种新的基于BFT的共识协议Proteus。该共识算法选择个节点组成的节点子集作为根委员会保证稳定的性能。无论网络中的故障数量如何，它将典型的基于 BFT 的协议的二次消息复杂度降低到 ，Proteus降低了二次消息复杂性，确保了一致性协议与网络故障数量无关，提高了系统的安全性和性能。

针对单委员会中首领节点的恶意行为缺乏验证的问题，P.Berrang等人[30]提出一种新的结合推测BFT一致性算法和PoS的共识算法Albatross。该共识算法通过选择与权益成比例的验证者列表使其无需许可进入系统。Albatross使用随机可验证函数来增加对自适应对手的抵抗力，根据区块的推测BFT协议执行来提高达成一致的性能。该共识算法通过验证者机制检测节点的恶意行为、更换视图和惩罚机制来确保共识过程的安全性。此外，Albatross采用Bitcoin-NG的思想来提升处理交易的效率。

区块链单委员会混合共识算法具有强一致性，能够极大概率的降低区块链的分叉风险，提高交易处理效率。但是，快速安全地实现系统自启机制，委员会选举确保委员会内诚实成员达到一定比例都是这类共识算法需要重点考虑的问题。针对委员会重置，采用基于PoW的滑窗机制或者随机机制重置委员会具有更新缓慢、耗能高和委员会成员容易被腐蚀的问题，采用基于PoS机制的随机重置委员会将带来公平性和安全性问题。

### 2.1.4多委员会混合共识算法

为了提高区块链处理交易的扩展性，利用多个委员会来并行处理交易的混合共识算法被提出。目前的分片分为通信分片、计算分片以及存储分片。

1. 通信分片：将全网分为不同的片区，每个片区由一个对应的委员会处理。每个委员会内部成员大部分时间只需内部通信，每个分片内部的其他节点可以通过与该分片内委员会通信获得目前区块链的状态。通信分片可以极大地降低系统中地通信复杂度，降低网络通讯资源的消耗。
2. 计算分片：每个分片委员会只负责处理其对应的交易，对交易运行委员会内一致性算法,验证该交易的合法性,最终决定该交易是否被添加到区块链中。计算分片使不同的交易以并行的形式被不同的委员会处理,当网络中节点数量增多时,可以增加更多的委员会,这样交易处理性能随着网络中节点数量的增多而增加, 进而提高交易处理的扩展性。
3. 存储分片：在不同分片委员会将处理后的交易分片存储,每个分片委员会只负责处理本分片对应的交易,将交易放到本分片专属的交易区块链上。存储分片将整个区块链系统的交易数据或未花费的交易输出数据分片存储,降低了节点的存储负担。采用存储分片的区块链系统中每个分片各自生成和广播其区块链,不存在全局的区块链。

为了提高交易处理的效率，L.Luu等人[31]提出通过分片并行处理交易的共识算法ELASTICO。该共识算法将节点分为多组，每组委员会在一轮共识中会输出一个区块，通过目录委员会整合输出一个总区块。ELASTICO通过工作量证明和随机数的方式选择出一个时期内的共识节点可以避免女巫攻击和敌手偏置。该共识算法通过目录委员会机制来为多个委员会分配成员，委员会内部都运行PBFT一致性算法并将其内部共识结果发送给目录委员会。目录委员会内部也运行PBFT一致性协议对最终总区块中交易的顺序和有效性达成共识，通过随机数生成协议为下一轮的委员会节点的选择增加随机性和可验证性。但是ELASTICO抗敌手偏置性差、且无法实现跨分片交易。分片共识在实现交易处理可扩展性的同时,引入了一些新安全性问题的问题。

1. 委员会选举和分配：选举和分配的委员会需要确保诚实成员数量达到一定比例，避免委员会中恶意节点数量过多使得敌手控制委员会。因此，为了防止敌手在此过程中影响委员会成员选举和分配,需要设置合理的选举和分配策略。
2. 委员会一致性算法：每个分片委员会都运行相同的一致性协议对部分区块达成共识，因此需要解决分片委员会最终区块交易排序和确认的问题。每个分片执行一致性协议都需要选举分片首领，需要设置安全的委员会首领的选举算法防止首领不作为或恶意行为。
3. 跨片交易：针对跨分片交易需要解决多个分片共同安全和高效协作地处理交易的问题。在处理跨分片交易的过程中需要解决双花攻击、重放攻击[32]和交易锁死等问题。跨分片交易需要多个分片通信协作，因此需要采取措施提升交易的处理速度。针对频繁通信处理跨分交易的分片，可以采取融合分片的方式降低分片之间的通信频率，提高交易处理效率。

针对ELASTICO中分片共识中抗偏置性低以及无法处理跨片交易的问题，E.Kokoris-Kogias等人[33]提出跨片交易防锁死的共识算法Omniledger。该算法通过RoundHound算法生成本轮随机数作为随机置换函数的种子对委员会成员进行分片，采用密码学抽签的方式选举分片首领，提高了委员会分配的抗偏置性。对于委员会重置问题，Omniledger设置合理的挖矿难度来随机选举新的成员部分替换委员会中的成员，这样可以提高系统容错率和抗偏置性。Omniledger针对网络中不同分片的节点只处理和存储该分片对应的UTXO数据，利用原子性跨片交易防止跨片交易锁死。为了更好的防止敌手使得委员会选举出现偏置问题，文献[34]对Omniledger使用的随机数生成算法改进,采用公开可验证秘密分享算法确保了随机数的不可预测性、抗偏置性和公开可验证性。但是Omniledger的身份确认采用的工作量证明算法，使得每一轮委员会的重置会耗时较长，具有被敌手腐蚀的危险。同时，基于工作量证明的身份证明需要耗费大量算力对环境不友好。

针对分片区块链系统中交易和智能合约跨片处理的问题，M.Al-Bassam等人[35] 将智能合约的执行和验证分离，提出了BFT协议和原子提交协议结合的原子提交协议—Chainspace，实现了交易和智能合约的通信分片和计算分片，在确保其安全性的同时提供较高的交易吞吐量。但是Chainspace并没有考虑委员会的选择和分配问题，也没有考虑委员会重置问题，更没有解决节点的身份验证问题。

针对区块链系统中节点存储有限的问题，M.Zamani等人[36]提出的RapidChain很好实现了计算分片、通信分片和存储分片大大地提高了系统的性能。这个共识算法主要包括启动 (bootstrap)过程、共识过程和重配置过程。RapidChain采用随机图（Random Graph）的方式选出根群组(Root Group)，利用根群组运行分布式随机数生成协议生成目录委员会，目录委员会再负责生成其他的分片委员会。每个委员会在时期内负责区块的生成和共识的达成，每个任期又分为多个轮，每一轮每个委员会内部执行同步拜占庭容错协议。当委员会任期结束之后，系统采用有界布谷鸟规则(Bounded Cuckoo Rule)尽量确保新节点替换掉委员会中不活跃的旧节点。该共识算法在网络层中采用消息扩散算法(Gossip Protocal)[37]能够将区块传播速度提升。RapidChain 对于跨分片交易采用将交易拆分的方式，并在对应交易所属的分片中达成共识，最终根据共识结果分片存储。但是由于每个时期中委员会内部的共识采用的是同步网络模型，这将导致交易确认不能满足快速响应的特性。

针对跨分片事务处理花费昂贵的问题，Y.Liu等人[38]提出了一种新颖的混合共识算法SSHC。针对委员会成员的分配问题。SSHC共识算法提出了一个公平的分片选择方案分片内共识，设计了流水线BFT一致性协议将流水线技术与阈值签名相结合提高共识效率。SSHC采用一种响应式分片事务批处理机制来处理跨分片事务，减少了对BFT一致性协议的调用次数。对于委员会重置问题，该共识算法设计了一种安全的委员会重新配置方法来有效地更新分片成员。SSHC采用正式的安全框架来设计和分析分片区块链，证明了提出的共识算法可以实现一致性和活性。

针对随机分片区块链系统安全性和吞吐量低，分片协作的激励开销大的问题，C.Huang等人[39]提出了基于声誉分片和首领节点选举共识算法RepChain。RepChain共识算法可以有效提高分片中诚实成员的比例，防止首领节点不作为或者恶意行为。该共识算法采用一种新的双链架构—交易链和信誉链。对于交易链，提出了一种高效的基于 Raft 的同步共识。对于信誉链，结合集体签名的同步BFT一致性协议可以防止对信誉评分和相关交易块的攻击。同时，该共识算法为激发节点合作提供了高激励，并且支持具有中等生成速度的高吞吐量交易链。

针对PBFT一致性算法通信复杂扩展性低的问题，W.Li和M.He[40]提出了一种分层和基于组的 BFT 共识算法—高效 BFT（EBFT）。 这个一致性算法利用一种新颖的网络拓扑结构将节点之间的通信时间降低到。通过将PBFT 一致性协议中未分片的节点划分为不同的层和组，提出分层和基于组的区块链模型。然后在这个模型的基础上修改了PBFT的共识协议，采用的签名机制减少节点之间的通信提高性能。

区块链多委员会混合共识算法通过分片并行处理交易极大地提升区块链的交易吞吐量。相较于单委员会混合共识算法，多委员会混合共识算法引入了跨分片交易处理问题、委员会成员动态管理问题和恶意委员会检测与恢复问题。如果分片委员会成员分配过程受到敌手的偏置,可能导致某些委员会中恶意成员个数超过限制，敌手可能进一步控制分片委员会影响系统的安全和性能。因此，如何检测恶意委员会并建立恢复机制是多委员会混合共识算法需要解决的问题。

### 2.1.5其他共识算法

针对工作量证明能耗高对环境不友好的问题，有些研究工作提出新的能耗低的共识算法。A.Miller等人[41]提出了文件存储证明共识算法—Permacoin。该共识算法要求参与节点有能力存储大文件的一部分。通过一个挑战应答机制来确定节点是否存储了文件部分，若节点挑战应答成功则获得出块权限。节点最保险的方式是存储整个文件，从而就会确保挑战成功的高概率，但这对节点的存储空间要求极大。这个共识算法需要节点付出存储资源，因此系统能够抵抗女巫攻击，即节点不能通过伪造身份来提升被选中成为出块节点的概率。

针对文件存储证明共识算法需要消耗大量的存储空间问题，S.Park等人[42]提出采用非交互式空间证明(proof of space)共识算法的Spacecoin。空间证明共识算法以参与节点能够使用的硬盘空间大小作为标准选举区块的生产者，共识节点通过一次性付出的硬盘空间来获的出块权限。为了防止硬盘空间造假，节点初次加入系统的时候根据选择的存储空间大小，存储一部分具有特定序列的数据。校验节点验证时向证明者发送一个挑战，证明节点根据挑战信息生成对应数据的哈希值给校验节点。校验节点再根据返回的值判定证明者是否硬盘空间造假。通过多次验证的方式来避免证明人的作弊行为。这个校验节点存储空间的方法在原来的文件存储证明共识算法的基础上上加入了随机性，使得节点共识过程更具有公平性。但是存在无利益攻击、长程攻击和双花攻击的风险。

针对共识算法都具有资源消耗大、安全性低等问题，消逝时间证明[43]共识算法应运而生。这个共识算法是基于硬件芯片执行某个命令的等待时间来实现的,其实质是利用可信硬件产生随机数来决定下一个区块生产者。参与节点在发布块之前都需要向Intel SGX中的飞地获取一个随机的等待时间,等待时间最短的节点被选为出块节点。消逝时间证明共识算法具有低能耗、高交易吞吐量和公平性的优点。但是，这个共识算法需要可信硬件的辅助，一旦硬件出现问题共识过程将不再可信。

针对PoW共识算法能耗高，性能低以及PoS公平性和安全性低等问题，D.Schwartz等人[44]提出了Ripple共识算法，通过信任节点列表分别对交易和区块达成共识。在确保交易安全性的前提下提高性能。目前的交易确认时间只需要4s，吞吐量可高达1500TPS。但是这类共识算法的容错率比较低，并且通信复杂度比较高。

## 2.2 基于有向无环图存储结构的区块链共识算法

单链区块链系统的交易吞吐量的提升是受到了区块大小和区块生成时间间隔的限制，且容易出现链分叉影响系统的安全性和扩展性。为了提升交易吞吐量，打破区块链系统扩展性额瓶颈，新的区块链存储结构—有向无环图（DAG）应运而生。DAG区块链中的每个单元代表系统中节点发起的一笔交易（或一个区块）,每一条从子单元指向父单元的有向边代表一种验证关系。节点创建交易（或区块）的时候需要对先前的交易（或区块）单元进行验证,将验证有效的单元的哈希值包含到自己的新交易（或区块）单元的数据结构中。当前的交易单元称为被验证交易单元的子单元,被验证的交易单元称为当前交易单元的父单元。每笔交易（或每个区块）可以有多个父单元也可以有多个子单元,这些单元构成有向无环图的结构。DAG区块链中历史交易数据不可篡改,一旦更改则会引起整个DAG区块链的变更。DAG区块链的交易处理速度随着网络中节点的增多而提高, 能够实现交易处理的高扩展性。

基于DAG区块链的研究工作有许多，现在的DAG区块链共识算法可分为Tangle共识算法，基于主链的共识算法和基于平行链的共识算法。这些共识算法在为系统提高了交易处理性能的情况下，也面临着新的安全性问题。

1. 节点自启机制：区块链系统需要确保新加入节点能够快速获取可信区块链信息。由于基于DAG区块链的系统具有交易并发性，因此每个节点维护的账本是不同的，因此如何确保新加入的节点获取的是最新的账本是需要解决的问题。
2. 双花攻击问题：由于DAG区块链中允许分叉，因此容易被敌手利用发起交易双花攻击，区块链系统需要共识算法对双花交易中的有效交易安全地达成一致。
3. 激励机制：DAG区块链通常没有挖矿费用，因此没有奖励费用。共识算法需要解决节点由于没有收益而丧失维护区块链系统的活性和积极性的问题。
4. 长程攻击问题：由于节点生成交易并不需要耗费非常多的资源，因此敌手可以伪造大量交易来确保自己的交易最终被确认，这些都为DAG区块链带来严重的安全问题。

### 2.2.1 经典DAG区块链共识算法

DAG区块链系统可以利用DAG区块链的拓扑结构，通过投票机制进行共识。典型的代表是Dagcoin[45]和IOTA[46]。

由S．D．Lerner提出的Dagcoin[45]是首个以交易为基本单元的DAG区块链，节点在创建交易时需要进行一定量的工作量证明，验证并引用当前DAG区块链中的一个或多个交易，随后将该交易广播并记录到DAG区块链中。为了解决双花交易问题，Dagcoin引入确认分数机制(Confirmation Score Mechanism)。每个交易都会其直接会间接引用的交易贡献1个单位确认分数。当引用交易出现冲突时，则确认分数高的哪个交易才会被引用。虽然Dagcoin并未给出交易确认所需要的确认分数阈值，也没有深入分析安全边界，但是为之后的DAG区块链提供了参考。

IOTA[46]继承了Dagcoin的思想，其采用的Tangle共识算法以交易为基本单元，每个交易单元引用两个父交易，并且每个交易都有一个自权重。交易的权重会随着直接或间接支持它的交易数量的增加而变大。当一个交易累积权重足够大，满足系统预设的确认阈值时，该交易将显示确认状态。为了解决双花攻击问题，IOTA引入马尔可夫蒙特卡洛随机游走算法，交易累积权重小的冲突交易将不会被引用。理论上,如果整个网络中有足够多的交易流,则交易确认过程可以快到在几秒钟内完成。但是，当交易流较小的时候，旧的交易确认时延比较长甚至无法被最终确认。因此，IOTA引入了一个由基金会运行的协调节点来定期发布检查点进行交易确认，这可能会带来新的安全性问题。

Y. Sompolinsky等人提出的SPECTRE[47]是以区块为基本单元的DAG区块链，每个诚实节点在挖矿时需要引用自己的DAG区块链中所有顶端区块。为了解决双花攻击中交易确认的问题，SPECTRE引入了一个投票机制。节点根据DAG区块链中所有的区块对于冲突区块进行排序投票，最终根据投票结果确认有效的交易。通过根据DAG区块链的拓扑结构的投票算法解决冲突交易排序问题，从而达成区块链全局共识。但是SPECTRE智能确定有效交易集合，并不能对所有交易进行全局排序。因此，Y. Sompolinsky和A. Zohar提出了PHAMTOM[48]，通过引入k-cluster概念和贪心算法确定区块以及交易的全序，证明了该共识协议具有极高的可扩展性与活性

经典的DAG区块链共识算法的创新之处在于不采用网络中的一个子集(如矿工)来专门负责维护共识,而是全网所有的参与节点都来进行网络交易的验证和确认工作。经典的DAG区块链共识算法可以在没有任何交易费用的情况下提高交易处理效率，但是会面临着冲突交易确认问题和全局交易或区块的排序问题。此外，全网维护的DAG区块链不具有全局一致性，因此新节点的安全自启机制问题需要给出相应的解决方案。没有激励机制很难保证节点维护区块链系统的活性，并且面临拒绝服务攻击和垃圾信息攻击。

### 2.2.2 基于主链的DAG区块链共识算法

DAG区块链具有可确定全序的特性，即从DAG拓扑中根据一条共识主链来进行拓扑排序。

Y. Sompolinsky和A. Zohar提出了基于树形DAG的共识协议GHOST(greedy heaviest-observed sub-tree)[37],通过改进树形DAG结构解决传统区块链在高并发情况下存在的问题。为了解决双花交易问题，GHOST采用最大权重子树原则选取主链作为最终主链。GHOST考虑了并发情况后继区块构成的子树权重，确保了在出块速率较高的系统中的主链安全性。Inclusive Blockchain Protocol[49]和Conflux[50]都继承了GHOST在DAG中选举主链的思想。由于CHOST主链外的区块是不被承认的，因此会造成系统算力浪费和性能受限。因此，Inclusive Blockchain Protocol可以引用多个父区块，且所有区块都会被视为DAG区块链中的一部分。为了解决双花交易问题，通过DAG中共识主链和拓扑结构对所有的区块排序，根据交易所在区块的顺序决定冲突交易中的有效交易。但是Inclusive Blockchain Protocol并没有详细给出排序算法。针对GHOST和Inclusive Blockchain Protocol中存在的问题，Conflux做了进一步改进，对区块的引用做了分类并且明确了排序规则。在确保安全性的情况下使得系统吞吐量能够随着算力线性提升。

Byteball[51]是一种基于交易单元的DAG区块链，通过引入见证人机制构建DAG区块链系统的共识主链，并确定其上的稳定点。见证人通常是系统中长期实名且具有较高声誉的节点，他们维护系统并自愿频繁的发起交易单元，消极的见证人可以被替换掉。最优父单元的选择是根据单元级别、见证级别以及交易的哈希值来确定的。通过选择最优父单元可以找到一条从任意顶端单元出发到创世单元的最优路径作为一条候选主链。多条候选主链会在某个交易单元处相交，这个相交的交易单元是一个稳定点。在每个节点中，从稳定点到创世单元的路径是相同的，这部分主链称为稳定主链。所有与稳定主链相关的交易单元可以进行一个全局排序，为每个单元分配一个主链号，最终建立在DAG区块链上的主链总序达成全网共识。若出现冲突交易单元，则全序中出现最早的将会被认为是合法的。但是Byteball中主链算法和见证人发布交易的频率有关系，交易确认的时间是不确定的。

为了解决Byteball中因交易流小而无法快速确认交易甚至有交易可能永远不会被确认的问题，TrustNote[52]采用双层共识的机制来解决。通过PoW机制选举出公证共识的节点发布公正单元到DAG区块链上，根据公证单元构建主链进行交易单元的全局排序解决双花问题。当公证单元成为主链上的稳定单元之后，公证节点才能获得公证奖励。为了避免出现垃圾交易，该共识算法要求所有节点提交新单元时支付交易费用。交易费用分别被支付给其最小哈希子单元和公证子单元的节点。通过这个激励机制可以吸引更多节点维护DAG区块链，提高区块链系统活性。此外，激励机制也促使节点尽可能引用最新的靠近主链的父交易单元，进而有效地减少分叉。但是基于PoW的TrustME共识机制需要耗费大量的算力资源，且生成公证单元速率比较慢。这个共识算法还面临自私挖矿攻击的危险，需要解决计算资源集中化问题确保算力较小的公证节点也能获得出块权和奖励。同时，还需要一个安全的节点自启机制来确保新节点最新的、真实的区块链信息。

### 2.2.3 基于平行链的共识算法

在基于平行链的DAG区块链共识算法中，网络中各个参与共识的节点只需要维护记录本地信息的一条链，各链之间通过交互引用构成平行的DAG区块链形式。

Hashgraph[53]共识算法通过虚拟投票的方式在DAG区块链中实现无需首领进行提案的拜占庭容错共识。Hashgraph使用Gossip协议使得节点可以随机选择另一个节点同步自己的信息，接收到同步信息的节点在本地创建一个记录同步历史的事件。每个事件包括时间戳、交易和哈希。其中哈希中两个哈希域分贝指向自己维护的链上最新事件和与自己同步信息的节点链上的最新事件。节点通过与自己同步信息的节点链上的最新事件构成Hashgraph的DAG区块链，使得Hashgraph不需要通信就能完成拜占庭共识，最终实现所有事件的全局排序。Hashgraph是一种快速、公平和安全的共识算法，开创性的异步BFT共识不会引发突发大规模消息传递风暴。Hashgraph利用Gossip协议和虚拟投票将共识所需的通信要求降到了最低，本地计算也保证了共识的高效性。但是这个算法的共识过程比较复杂至少需要两轮才能确认事件，且还未在大规模公链环境下运行，安全性还没有得到具体验证。

Nano[54]是一种基于区块点阵(Block Lattice)结构的新型加密货币，其共识算法采用了一个账户维护一条链的方式，每条链只记录该账户的所有交易历史。Nano允许交易并行执行提供秒级的交易速度和无限可扩展性。此外，这个共识算法允许交易异步更新到网络的其余节点，以极小的资源开销获得快速的交易确认。Nano中一笔完整的转账交易由发送交易和接收交易构成，通过接收交易组成不同账户之间的引用关系，形成平行链DAG结构。交易数据的收发可以是异步的，因此允许多笔金额同时汇入一个账户。若出现节点离线，未到账的金额会被标记，直到节点在线时完成即可。Nano使用DPoS共识算法处理系统中的冲突问题，由账户（账户的投票权重与账户拥有的系统代币数成正比）的指定代表（每个代表的权重为选定其为代表的账户余额之和）为其投票进行共识，最终得票最多的区块被认为是有效的。Nano中使用的PoW机制只是防止垃圾交易的产生。共识算法中每个节点维护自己的账本可以很好的避免自己账本被篡改的风险，如果敌手篡改自己的账本会立即被其他节点检查到使得篡改无效。采用这种共识算法的区块链面临着新的安全问题，网络分离后重新加入时可能会影响分叉的投票过程和结果。DPoS共识算法存在中心化程度高的缺点, PoW生成交易可以防止垃圾交易但也会消耗计算算力，尤其当交易数量多的时候，算力的消耗也将是巨大的。

# 3课题主要研究内容、预期目标

本课题的研究目标是针对建立在无线自组织网络上的区块链系统，考虑无线网络节点具有移动性、且节点计算资源有限、网络通信质量不稳定、干扰以及环境等因素，以低能耗，稳定达成系统共识、提高交易处理效率为目标，设计安全高效的无线区块链共识算法，主要内容包括以下几个方面：

1. 基于节点稳定性的无线区块链共识算法

考虑无线自组织网络中节点具有移动性、网络拓扑动态变化且在系统中活动时间有限等约束，以降低共识节点计算资源开销和提高交易处理效率为目标，设计一个公平的、稳定的、高效的无线区块链共识算法。

1. 基于稳定委员会的无线区块链共识算法

针对单出块节点的区块链共识算法中区块确认延时高，容易出现链分叉以及无线自组织网络拓扑动态变化的问题，以降低链分叉概率、快速确认交易为目标，设计快速、稳定的基于委员会的无线区块链共识算法。

1. 基于稳定分片的无线区块链共识算法

在组网规模大，节点分布区域广的无线自组织网络场景，针对区块链共识时延长、交易处理效率低、网络拓扑高动态变化等问题，以降低网络共识节点通信开销、提高交易处理效率、降低区块确认时延、高效处理跨分片交易为目标，设计稳定的、高效的基于多委员会的无线区块链共识算法。

1. 基于稳定主链的无线DAG区块链共识算法

在无线自组织网络场景中，针对区块链性能受到区块大小和区块生成时间间隔的限制、链分叉降低区块链性能、见证人容易被敌手偏置以及网络拓扑动态变化等问题，以不依赖可信见证节点、提高交易处理效率、抗双花攻击为目标，设计安全、稳定、高效的基于稳定主链的无线DAG区块链共识算法。

# 4拟采用的研究方法、技术路线、实验方案及其可行性分析

## 4.1技术路线方案

### 4.1.1基于节点稳定性的无线区块链共识算法

区块链共识算法需要平衡好去中心化、安全性和扩展性三者之间的关系。单出块节点的区块链共识算法具有较好的去中心化性和安全性，其共识过程主要包括节点自启时获取最新可信的区块链信息、选举出块节点、生成区块并广播，验证交易和区块达成共识更新区块链。考虑在节点资源有限和网络通信质量不稳定、网络拓扑动态变化的无线自组织网络场景中，直接采用通过消耗物理资源获得出块权限的单共识节点算法是不合适的。因此，设计适用于无线区块链系统的共识算法要满足低能耗、高效率并且对节点的移动性不敏感等要求，需要考虑以下问题：

1. 如何使共识算法能够抵抗女巫攻击的同时没有巨大的物理资源消耗。
2. 如何使得敌手在诚实节点出块之前无法知道出块节点的信息，防止出块节点被腐蚀。
3. 如何防止由于无能耗或者低能耗的出块面临的无利害关系攻击和长程攻击。敌手为了确保自身获利在每个分叉上都添加区块，或者通过获取之前出块者的重要私钥来伪造一条新的长链。
4. 如何防止日蚀攻击。新节点或者离线节点加入网络时，敌手可以发起日蚀攻击使得节点无法获得最新区块链或者真实区块链。

无线自组织网络中，每个无线节点在系统中活动的时间都是有限的，为了确保无线区块链共识过程的稳定性和安全性，最好是选举一定时间内不会离开系统并且比较可信的节点作为出块节点。因此，拟结合节点在系统中的活动时间和历史共识频率，设计一个稳定、低能耗、高效的无线区块链共识算法。

研究方案：

1. 网络建模：考虑在无线自组织网络环境中，无线网络节点随意部署在一个二维平面中。每个节点的计算资源和网络资源是有限的，节点可以在网络区域之内随意移动，并且可以随意进入和离开这个区域。网络节点之间通过发送无线信号通信，每个节点的通信半径是相同的。对于无线网络节点之间的通信干扰采用标准信号干扰的信噪比模型SINR。每个节点局部地维护自己的区块链。各区块通过引用前一个区块的哈希最终形成一条链式结构的形式。每个区块中包含有多个交易、自身区块的哈希、父区块的哈希、时间戳、区块高度等信息。
2. 单出块节点共识算法面临的问题：
3. 工作量证明共识算法生成区块需要消耗大量算力，而无线网络节点的计算资源非常有限；
4. 传统区块链的共识过程依赖可信的网络通信，而无线网络通信面临着信道质量不稳定、干扰、环境等约束；
5. 传统的区块链共识算法中新节点进入网络直接同步最近接入节点的区块链信息，而无线网络节点可以移动，容易发起日蚀攻击同步陈旧或者错误的区块链信息给新加入的节点。拟设计一个低能耗、稳定的、高效率的共识算法，确保在开放的无线自组织网络中能够实现安全节点自启，稳定共识过程、高效的处理交易。
6. 基于稳定性的无线区块链共识算法：共识算法主要包括出块节点选举，区块的生成、广播，区块的验证、确认和区块链更新。但是，节点的安全自启机制关系到参与共识节点的安全性，考虑到无线网络中节点的易受攻击性，因此需要无线网络节点自启机制确保新节点的安全性。
   1. 节点自启机制：拟采用公共前缀最长链的机制来解决新节点进入系统后获取可信区块链信息的问题。比较多个节点的区块链，找到具有相同前缀并且最长的链复制为新节点的本地链，确保新节点获得的区块链是最新的和真实的。
   2. 出块节点选取：拟采用类PoS机制选举出块节点防止敌手发起女巫攻击伪造多个身份给系统带来安全性的威胁。无线网络节点进入区块链系统后需要质押金钱获得系统中活动的时间，活动时长与质押金成比例。根据节点在系统中的稳定度选举出块节点。根据节点在系统中的剩余活动时间和在最近个确认区块中参与共识比值来定义节点的稳定度。通过节点的稳定度选举具有较好稳定性和可信性的节点作为出块节点。为了确保出块节点选举过程不被敌手偏置，拟采用一个可验证随机抽签的方法选举出块节点。每个节点只能知道自己是否被选中成为共识节点，并不能知道其他节点是否会被选中。但是每个节点可以验证被选中节点的有效性，确保出块节点在生成区块之前都不会被敌手偏置。一旦节点确定自己被选中成为出块节点，则对交易排序，并打包成区块广播到网络中。
   3. 区块验证和确认：接收到区块的节点会验证区块和出块节点的有效性。出块节点只有在区块被确认之后才能获得区块奖励。为了防止区块确认过程中的二次通信导致敌手干扰区块确认，拟采用门限签名的方式确认区块。接收到待确认区块的节点在验证区块和出块节点的有效性成功后，在区块中附上自己的签名并广播。当区块签名份额数量达到一个阈值后签名份额能够组成一个区块的最终签名确认区块。
   4. 分区恢复机制：无线自组织网络容易发生网络分区，从而引起区块链出现分叉。拟采用一个基于最长链原则的分区恢复机制，确保网络分区后区块链系统的安全性。设置一个检查点机制，定期比较系统中所有节点的区块链信息，最终确定具有公共前缀的最长区块链作为有效区块链，其他分叉上的区块会被孤立。确保区块链系统只维护唯一的、最新的区块链。
   5. 奖惩机制：当区块被确认后，生成区块的节点将获得部分区块奖励和交易费用，剩余部分的奖励将分发给后一个区块的生成者。这样的奖励机制可以使得诚实节点更愿意在新区块后面挖矿，减小分叉的概率提高安全性。当节点在系统中活动时间内没有任意不作为或者恶意行为时，在活动时间结束后将全额返还押金。同时也能激励系统中的节点积极维护系统区块链，提升系统的活性。如果节点在未到活动时间结束之前离开系统，则会扣除部分押金。当发现有节点作恶后系统也会扣除押金。

**创新点：**

1. 采用类PoS机制确保系统能够抵抗女巫攻击，定义无线网络节点的稳定度，提出根据稳定度选举出块节点的共识算法，提高区块链共识过程的稳定性和安全性；
2. 改进节点自启机制，确保新节点参与共识之前能够获得可信的最新区块链信息；
3. 提出了一个分区恢复机制，确保全局区块链的一致性，降低由于分区导致区块链分叉的概率，提高区块链的性能；
4. 改进区块确认机制，采用门限签名机制来确认区块，降低区块确认延时的同时确保系统能够抵抗无利益关系攻击和长程攻击。

### 4.1.2基于稳定委员会的区块链共识算法

在较大规模的无线自组织网络中，单出块节点共识算法只有弱一致性，且区块确认时延长。在节点具有动态性、资源有限、网络拓扑动态变化的无线自组织网络场景，针对交易处理速率低、区块链出现分叉以及无限自组织网络动态变化等问题，以降低链分叉概率、提高交易处理速率和提高共识过程的稳定性为目标，设计快速、稳定且具有强一致性的单委员会无线区块链共识算法。设计这类共识算法需要解决以下问题：

1. 安全自启问题：在不依赖可信启动机制的情况下完成初始化委员会配置的问题。
2. 委员会选举：选举委员会时要确保诚实节点数量达到一定比例，因此需要防止敌手偏置委员会选举过程。
3. 委员会一致性算法：委员会执行一致性协议需要选举首领提出区块，因此首领节点的选举和提交区块快速响应都是需要解决的问题。考虑到无线网络通信不稳定的情况，需要提高委员会内执行一致性协议的效率。
4. 委员会重置：在委员会重置时需要解决委员会中诚实成员达到一定比例问题；委员会成员交替时交易的处理问题；敌手影响新委员会成员加入委员会的问题。

研究方案：

1. 网络建模：考虑在较大无线自组织网络环境中，无线网络节点随意部署在一个二维平面中。每个节点的计算资源和网络资源是有限的，节点可以在网络区域之内随意移动，且节点可以随意进入和离开这个区域。网络节点之间通过发送无线信号通信，每个节点的通信半径是相同的。对于无线网络节点之间的通信干扰采用标准信号干扰的信噪比模型SINR。每个节点局部地维护自己的区块链。各区块通过引用前一个区块的哈希最终形成一条链式结构的形式。每个区块中包含有多个交易、自身区块的哈希、父区块的哈希、时间戳、区块高度等信息。
2. 单委员会混合共识算法面临的问题：
3. 敌手偏置委员会选举使得诚实节点的比例较低，进一步控制委员会。由于无线网络节点之间通信不稳定，敌手可以偏置委员会首领节点的选举，最终选出的首领可能不作为或恶意行为；
4. 由于无线网络节点的移动性，委员会成员在共识过程中可能无法稳定通信甚至可能离开系统。此外，无线网络通信信道不稳定会委员会执行一致性协议通信时延比较高，二次通信也可能会给敌手腐蚀无线网络节点的可能。
5. 委员会重置过程容易受到敌手偏置，进一步控制委员会，影响区块链系统的安全性和效率。
6. 稳定的单委员会无线区块链共识算法：共识算法主要包含委员会选举、委员会首领节点的选举、委员会一致性协议和委员会重置。
7. 委员会选举：由于无线网络通信资源的有限性，为了确保委员会共识过程的稳定性，拟采用基于节点稳定度的委员会选举机制。根据节点的共识比值和剩余活动时间定义节点的稳定度。随后根据稳定度选举委员会成员，确保委员会成员在共识过程中的稳定性。
8. 委员会首领选举：为了降低共识过程中委员会节点之间的通信，防止敌手偏置首领选举过程，拟根据委员会节点的位置和可验证随机抽签机制来选举委员会首领。
9. 委员会一致性协议：选举委员会成员和首领节点后，委员会内执行一致性协议。首领节点会生成区块并将其作为提案广播给委员会成员。委员会成员会验证区块、首领节点的合法性并对提案做出投票。为了防止敌手利用二次通信干扰委员会一致性协议结果，拟采用基于门限签名机制的一致性协议。降低委员会成员之间通信的同时安全达成一致性结果。接收到区块提案得委员会成员验证成功后会将其签名份额放入区块中并广播。当签名数量达到阈值后会组成区块的最终签名，此时说明一定数量的委员会成员承认区块，最终委员会对区块达成一致。委员会成员会将区块链接到本地区块链上并广播给其他非委员会成员。接收到确认区块的节点验证区块有效性后，将区块连接到本地链上。
10. 委员会重置：委员会任期结束之后需要更换委员会成员。根据委员会的容错率来决定更换委员会成员的数量。新的节点将取代原来委员会中稳定性较低的旧节点。委员会重置后，新一轮首领会将之前被打断的区块提案重新作为新提案达成一致性。
11. 奖惩机制：委员会任期结束，委员会内所有节点将平分任期内所有生成区块的奖励和交易费用。这样的奖励机制能激励系统中的节点积极维护系统区块链，提升系统的活性。如果节点在未到活动时间结束之前离开系统，则会扣除部分押金。当发现有节点作恶后系统也会扣除押金。这个机制会降低节点离线和作恶的机会。

**创新点：**

1. 改进基于节点稳定度和随机可验证抽签的委员会选举机制，确保选举过程不被敌手偏置，且委员会成员在无线网络环境中能够稳定达成共识。
2. 提出基于节点位置或者跳数的首领选举机制，降低执行一致性协议时节点之间的通信。
3. 改进委员会内的一致性协议，采用基于门限签名机制的一致性协议提高容错性的同时避免共识过程的二次通信，提高委员会达成一致性的效率。

### 4.1.3基于稳定分片的无线区块链共识算法

在大规模无线自组织网中构建的区块链系统，具有节点分布区域广、节点设备资源有限、具网络拓扑动态变化的特点。单共识节点的区块链共识算法无法满足交易处理的高效性和时效性。由于无线网络通信受到信道不稳定、干扰、网络拓扑变化不可预测和环境等因素的约束，共识时延长导致区块链更容易出现分叉问题。单委员会混合共识算法在大规模组网中，节点的通信会随着参与共识的节点数量增加而增加，无线链路的不稳定会导致长距离通信时消息丢失概率大。针对在组网规模大，节点分布范围广的无线自组织网络场景中，考虑无线节点间通信不稳定、网络拓扑动态变化、达成系统共识的网络开销大、网络分区等问题，以降低共识所需的网络开销和提升交易处理效率为目标，设计具有高稳定性、能处理并发交易的基于多委员会的无线区块链共识算法。

多委员会区块链共识算法通过网络分片、计算分片和存储分片的方式极大地提升区块链系统的交易处理效率。采用多委员会共识算法的区块系统通常会构建多个委员会，每个委员会可以并行处理交易，也可以协同处理交易。此外，多委员会共识算法也面临着一些安全问题：

1. 初始委员会选举：系统不依赖可信启动完成初始化委员会配置，并且需要确保委员会中诚实节点达到一定的比例。
2. 分片委员会分配：在分配分片委员会成员的时候需要防止敌手偏置分配过程，确保诚实节点数量达到一定比例。
3. 委员会一致性算法：委员会一致性协议需要解决提交区块快速响应问题，通过降低委员会通信复杂度和计算复杂度，并行达成区块共识来提高委员会内一致性算法运行效率。
4. 委员会重置：委员会重置时需要考虑手影响委员会成员更换导致诚实成员比例低的问题，委员会成员交替时区块的处理问题，委员会更换成员的数量不能影响委员会的安全性的问题。

研究方案：

1. 网络建模：考虑在较大无线自组织网络环境中，无线网络节点随意部署在一个二维平面中。每个节点的计算资源和网络资源是有限的，节点可以在网络区域之内随意移动，且节点可以随意进入和离开这个区域。网络节点之间通过发送无线信号通信，每个节点的通信半径是相同的。对于无线网络节点之间的通信干扰采用标准信号干扰的信噪比模型SINR。每个节点局部地维护自己的区块链。各区块通过引用前一个区块的哈希最终形成一条链式结构的形式。每个区块中包含有多个交易、自身区块的哈希、父区块的哈希、时间戳、区块高度等信息。
2. 分片委员会共识算法面临的问题：
3. 由于无线网络节点具有移动性，采用传统多委员会区块链共识算法选举委员会成员可能会在共识或分配过程中离开委员会，导致最终无法完成区块链共识过程。
4. 由于无线节点之间网络通信信道不稳定，跨分片交易可能由于需要多分片协作而无法快速处理，甚至面临交易锁死的问题。
5. 委员会重置可能会被敌手偏置导致委员会成员中诚实节点比例低，最终敌手控制委员会。由于无线链路的不稳定性，委员会更替时被打断共识过程的区块需要重新高效处理。此外，为了确保委员会的安全性，委员会成员不能全部更换，因此需要计算一个委员会更换的安全上界。
6. 稳定分片的无线区块链共识算法：分片区块链共识算法主要包含根委员会选举和分配、委员会一致性算法以及委员会重置。
7. 委员会选举和分配：无线网络节点有限的通信资源会影响委员会共识过程的稳定性，拟采用基于节点稳定度的委员会选举机制。根据节点的共识比值和剩余活动时间定义节点的稳定度。根据节点稳定度和随机可验证抽签机制选举和分配委员会成员，确保委员会成员在选举、分配和共识过程的稳定性和抗偏置性。
8. 委员会首领选举：为了降低共识过程中委员会节点之间的通信，防止敌手偏置首领选举过程，拟根据委员会节点的位置和可验证随机抽签机制来选举委员会首领。
9. 委员会一致性协议：选举委员会成员和首领节点后，委员会内执行一致性协议。首领节点会生成区块并将其作为提案广播给委员会成员。委员会成员会验证区块、首领节点的合法性并对提案做出投票。为了防止敌手利用二次通信干扰委员会一致性协议结果，拟采用基于门限签名机制的一致性协议。降低委员会成员之间通信的同时安全达成一致性结果。接收到区块提案得委员会成员验证成功后会将其签名份额放入区块中并广播。当签名数量达到阈值后会组成区块的最终签名，此时说明一定数量的委员会成员承认区块，最终委员会对区块达成一致。委员会成员会将区块链接到本地区块链上并广播给其他非委员会成员。接收到确认区块的节点验证区块有效性后，将区块连接到本地链上。
10. 委员会重置：委员会任期结束之后需要更换委员会成员。根据委员会的容错率来决定更换委员会成员的数量。新的节点将取代原来委员会中稳定性较低的旧节点。拟采用基于节点稳定度和随机可验证抽签的机制重置根委员会成员，随后重新更换每个分片中的成员。委员会重置后，新一轮首领会将之前被打断的区块提案重新作为新提案达成一致性。
11. 跨片交易防锁死机制：在分片区块链系统中交易是分片存储和处理的。跨分片交易需要多分片协作处理，由于无线网络中节点之间的通信信道不稳定，跨分片节点之间通信延时高，会极大的影响跨分片交易处理的效率。拟采用一个分片融合的原子交易机制防止跨片交易被锁死，并且快速处理跨分片交易。
12. 奖惩机制：委员会任期结束，委员会内所有节点将根据贡献度分配任期内所有生成区块的奖励和交易费用。这样的奖励机制能激励系统中的节点积极维护系统区块链，提升系统的活性。如果节点在未到活动时间结束之前离开系统，则会扣除部分押金。当发现有节点作恶后系统也会扣除押金。这个机制会降低节点离线和作恶的机会。

**创新点：**

* 1. 提出一种结合节点稳定度和随机可验证抽签机制的委员会选举和分配机制，确保无线网络区块链系统中分片委员会成员的稳定性和安全性。
  2. 改进跨分片交易处理机制，确保跨分片交易可以在不稳定的无线网络环境中快速安全的处理。

### 4.1.4基于稳定主链的无线DAG区块链共识算法

传统的单链区块链系统的性能受到区块大小和区块生成时间间隔的限制，区块链分叉会极大地影响区块链系统的性能。但是，无线自组织网络容易发生网络分区，区块链出现分叉的概率会随着网络分区频率的增加而提升。此外，由于通信质量不稳定，基于委员会的混合区块链共识算法的共识延时会随着网络规模的增加而增加，进一步降低区块链系统的性能。针对大规模无线自组织网络场景，考虑节点资源有限、网络拓扑动态变化和网络分区等问题，以提高共识过程的稳定性、提升交易处理效率和提高抵抗双花攻击性为目标，设计稳定、高效的无线DAG区块链共识算法。

DAG区块链共识算法面临着严重的安全性问题。

1. 节点自启机制：DAG区块链系统中每个节点局部地维护区块链，新节点加入系统后需要获取最新的、真实的区块链。由于基于DAG区块链的系统具有交易并发性，因此如何确保新加入的节点获取的是最新的区块链是需要解决的问题。
2. 双花攻击问题：在DAG区块链系统中允许区块链分叉，敌手可以利用链分叉发起双花交易攻击。因此，DAG区块链共识算法需要确定双花交易中的有效交易，避免交易双花威胁系统的安全。
3. 激励机制：DAG区块链系统中没有挖矿费用，因此需要解决共识节点由于没有收益而缺乏维护系统的活性的问题。

研究方案：

1. 网络建模：在无线自组织网络环境中，无线网络节点随意部署在一个二维平面中。每个节点的计算资源和网络资源是有限的，节点可以在网络区域之内随意移动，且可以随意进入和离开这个区域。网络节点之间通过发送无线信号通信，每个节点的通信半径是相同的。对于无线网络节点之间的通信干扰采用标准信号干扰的信噪比模型SINR。每个节点局部地维护自己的DAG区块链。各交易单元通过引用多个区块的哈希最终形成有向无环图的形式。每个交易单元中包含有一个交易、自身交易单元的哈希、父交易单元的哈希、时间戳等信息。
2. DAG区块链共识算法面临的问题：
3. 节点自启机制：DAG区块链的系统具有交易并发性，因此每个节点维护的区块链是不同的。无线网络中节点具有移动性，且敌手容易发起日蚀攻击，因此如何确保新加入的节点获取最新的区块链是需要解决的问题。
4. 构建主链：为了确认交易并且解决交易双花问题，需要通过构建主链为交易全局排序。拟采用见证委员会生成的人见证交易构建主链。但是，无线网络拓扑动态变化，且节点通信资源有限。因此，无线区块区块链系统需要选举具有较高稳定性和可信性的委员会成员，确保能够快速稳定地生成见证交易并且达成一致性，使得见证交易具有一定的信用价值。
5. 见证委员会重置：敌手可以偏置见证委员会重置过程，使得委员会中诚实节点数量低于安全值，进而控制见证委员会。因此，区块链系统需要解决敌手偏置委员会重置的问题。
6. 稳定的DAG区块链共识算法：DAG区块链共识算法主要包含节点自启机制、见证委员会选择机制、一致性协议、主链机制、委员会重置机制。
7. 节点自启机制：针对节点加入系统时需要获取可信的区块信息和节点信息问题，拟采用改进共同主链最重链自启机制。通过比较多个节点的DAG区块链，选择具有公共前缀且最重的区块链作为可信区块链，最后同步到自己的本地存储中作为最新的区块链账本。
8. 见证委员会选举：针对无线网络中具有移动性，拟采用基于节点稳定度的委员会选举机制确保委员会的稳定性。节点的稳定度可以通过节点的见证交易共识比值和节点剩余活动时间定义。
9. 见证委员会一致性协议：考虑无线链路的不稳定性，为了快速生成见证交易和提高委员会对见证交易的快速响应，拟改进可验证随机函数机制来确保见证交易提案快速达成一致性。
10. 主链机制：针对DAG区块链中的交易双花问题，拟采用主链机制来构建交易的全序。根据交易的全序安全地拒绝后出现的交易解决交易双花问题。
11. 见证委员会重置：委员会在任期结束后要更换委员会成员。新的节点将取代原来委员会中稳定度低的旧节点。拟采用基于节点稳定度和主链度的方法来重置委员会。对于委员会重置时正在处理交易，将在新的委员会选定之后重新提案交易单元。
12. 奖惩罚机制：当一个交易单元被确认后，该交易的交易费会分发给其最小子交易和稳定见证交易所属的见证委员会成员。通过激励机制可以激励节点的活性以及节点成为见证委员会成员的积极性，进而提高系统的安全性。如果节点在未到活动时间结束之前离开系统，则会扣除部分押金，如果发现有节点作恶也会扣除押金，从而降低节点离线和作恶的动机，最终就使得系统更加的安全。

**创新点：**

1. 提出一种基于见证委员会构建主链的方式，考虑无线链路的不稳定性，采用结合节点稳定度和随机可验证抽签的见证委员会成员选举机制，确保委员会稳定的同时防止敌手偏置选举和重置委员会过程。
2. 结合节点的位置和区块链账本的主链机制，改进新节点的加入系统后的安全自启机制，确保节点进入系统后能够快速获得正确的区块链信息。

## 4.2可行性分析

本课题拟定的研究内容和研究方案是作者在已有工作成果，在对实际应用需求充分调研，并对当前研究现状详细分析基础上提出的。同时，国内外学者在区块链共识算法的研究中取得了大量的研究成果，这些都为本课题的研究奠定了坚实的基础，提供了可借鉴的内容。

除了上述分析之外，本人已经查阅了大量该领域的研究论文，并且熟悉多种编程语言和多种仿真手段。因此，本课题的研究方案是切实可行的。

# 5研究工作计划与进度安排

2022年1月-2022年3月：

1. 调研区块链的应用和区块链共识算法最新研究状况。
2. 归纳总结区块链共识过程和当前的研究存在的问题，总结分析共识算法面临的问题，查找整理当前的相关解决方案，总结当前的方案存在的问题，针对无线网络环境提出相应的解决方案。

2022年4月-2022年12月：

1. 根据提出的解决方案进行理论分析证明，确定新方案可以用于单节点共识算法、单委员会共识算法、分片委员会共识算法以及DAG区块链共识算法中，并分析用于不同的共识算法中的差异性和面临的新的难点。
2. 通过仿真实验证明新方案能够适用于节点资源有限、网络拓扑动态变化、通信信道不稳定的无线自组织网络场景中，并且提高区块链的安全性和交易处理效率。
3. 撰写相关共识算法的论文报告。

2023年1月-2022年5月：

撰写和提交毕业论文。

# 参考文献：

[1] S. Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf, 2008.

[2] G. Wood. Ethereum: A Secure Decentralized Generalized Transaction Ledger. Ethereum Project Yellow Paper, vol. 151, pp. 1-32, 2014.

[3] C. Dwork and M. Naor,Pricing via processing or combatting junk mail[C]. In: Advances in Cryptology— CRYPTO’92. Springer Berlin Heidelberg, 1993: 139–147. [DOI: 10.1007/3-540-48071-4\_10

[4] A. Back, . Hashcash—A denial of service counter-measure[EB/OL]. 2002. http://www.hashcash.org/papers/hashcash.pdf.

[5] M.Jackbsson and A.Juels. Proofs of Work and Bread Pudding Protocols[C]// Ifip Tc6/tc11 Joint Working Conference on Secure Information Networks: Communications & Multimedia Security. Kluwer, B.V. 1999.

[6] J. Garay, A. Kiayias, and N. Leonardos. The Bitcoin Backbone Protocol: Analysis and Applications. In Proceedings of the 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, 2015.

[7] R. Pass, L. Seeman, and A. Shelat. Analysis of the Blockchain Protocol in Asynchronous Networks. Annual International Conference on the Theory and Applications of Cryptographic Techniques Springer, Cham, 2017.

[8] E.Heilman, A.Kendler, A.Zohar, et al. Eclipse attacks on Bitcoin's peer-to-peer network[c]. In: Proceedings of 24th USENIX Security Symposium (USENIX Security 15). USENIX, 2015: 129–144.

[9] I. Eyal. The Miner’s Dilemma. 2015 IEEE Symposium on Security and Privacy, San Jose, CA, May 2015, pp. 89-103, doi: 10.1109/SP.2015.13.

[10] I. Eyal and E. G. Sirer. Majority is not Enough: Bitcoin Mining is Vulnerable. In Financial Cryptography and Data Security. Springer, November 2014, pp. 436õ454.

[11] R. Pass and E. Shi. Fruitchains: A fair blockchain. In Proceedings of the ACM Symposium on Principles of Distributed Computing, ser. PODC ’17. ACM, 2017, pp. 315–324. [Online]. Available: http://doi.acm.org/10.1145/3087801.3087809

[12] M. H. Ashik, M. M. Shahriar Maswood, A. G. Alharbi and D. Medhi. FPoW: An ASIC-resistant Proof-of-Work for Blockchain Applications. 2020 IEEE Region 10 Symposium (TENSYMP), 2020, pp. 1608-1611, doi: 10.1109/TENSYMP50017.2020.9230915.

[13] S. King and S. Nadal. PPCoin: Peer-to-peer crypto-currency with proof-of-stake. https://archive.org/details/PPCoinPaper (2012).

[14] N. Houy. It will cost you nothing to‘kill’a proof-of-stake crypto-currency[EB/OL]. 2014. ftp://ftp.gate.cnrs.fr/RePEc/2014/1404.pdf.

[15] A. Chepurnoy. Interactive proof-of-stake[EB/OL]. 2016. http://arxiv.org/abs/1601.00275.

[16] J. Kwon. Tendermint: Consensus without mining. Draft v. 0.6, fall, 1(11), 2014. https://tendermint.com/static/docs/tendermint.pdf.

[17] P. Gazi, A. Kiayias, A. Russell. Stake-bleeding attacks on proof-of-stake Blockchains[C]. In: Proceedings of 2018 Crypto Valley Conference on Blockchain Technology (CVCBT 2018). IEEE, 2018: 85–92. [DOI: 10.1109/ CVCBT.2018.00015]

[18] V. Buterin and V. Griffith. Casper the Friendly Finality Gadget[J].2017. https://arxiv.org/pdf/1710.09437.pdf

[19] I. Grigg. EOS—An introduction[EB/OL]. 2017. https://eos.io/documents/EOS\_An\_Introduction.pdf.

[20] A. Kiayias, A. Russell,B. David, et al. Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol[C]. In: Advances in Cryptology—CRYPTO 2017, Part I. Springer Berlin Heidelberg, 2017: 357–388. [DOI: 10.1007/978-3-319-63688-7\_12]

|  |
| --- |
|  |

[21] B. David, P.Gazi, A. Kiayias, et al. Ouroboros Praos: An adaptively-secure, semi-synchronous proof-of-stake Blockchain[C]. In: Advances in Cryptology—EUROCRYPT 2018, Part II. Springer Cham, 2018: 66–98. [DOI:10.1007/978-3-319-78375-8\_3]

[22] C. Badertscher, P. Gazi, A. Kiayias, et al. Ouroboros Genesis: Composable proof-of-stake Blockchains with dynamic availability[C]. In: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS 2018). ACM, 2018: 913–930. [DOI: 10.1145/3243734.3243848]

[23] P. Debian, R. Pass, E. Shi. Snow White: Robustly reconfgurable consensus and applications to provably secure proofs of stake[J]. IACR Cryptology ePrint Archive, 2017: 2016/919. https://eprint.iacr.org/2016/919.pdf

[24] C. Decker, J. Seidel, R. Wattenhofer. Bitcoin Meets Strong Consistency. In Proceedings of the 17th International Conference on Distributed Computing and Networking. ACM, 2016: 13:1–13:10. [DOI:10.1145/2833312.2833321]

[25] E. Kokoris- Kogias, P. Jovanovic, N. Gailly, I. Khoffi, L. Gasser, B. Ford. Enhancing Bitcoin security and performance with strong consistency via collective signing. In Proc. 25th conference on USENIX Security Symposium, 2016 : 279–296.

[26] I. Abraham, D. Malkhi, K. Nayak, et al. Solida: A Blockchain protocol based on reconfgurable Byzantine consensus[C]. In: Proceedings of 21st International Conference on Principles of Distributed Systems (OPODIS 2017). Lisbon, Portugal, December 18–20, 2017: 25:1–25:19. [DOI: 10.4230/LIPIcs.OPODIS.2017.25]

[27] R. Pass and E. Shi. Hybrid consensus: Efcient consensus in the permissionless model[C]. In: Proceedings of 31st International Symposium on Distributed Computing (DISC 2017). Vienna, Austria, October 16–20, 2017: 39:1–39:16. [DOI: 10.4230/LIPIcs.DISC.2017.39]

[28] Y.Gilad, R. Hemo, S. Micali, et al. Algorand: Scaling Byzantine agreements for cryptocurrencies[C]. In: Proceedings of the 26th Symposium on Operating Systems Principles, Shanghai, China, October 28–31, 2017: 51–68. [DOI: 10.1145/3132747.3132757]

[29] M. M. Jalalzai, C. Busch and G. G. Richard. Proteus: A Scalable BFT Consensus Protocol for Blockchains. 2019 IEEE International Conference on Blockchain (Blockchain), 2019, pp. 308-313, doi: 10.1109/Blockchain.2019.00048.

[30] P. Berrang, P. von Styp-Rekowsky, M. Wissfeld, B. França and R. Trinkler, Albatross–An optimistic consensus algorithm. 2019 Crypto Valley Conference on Blockchain Technology (CVCBT), 2019, pp. 39-42, doi: 10.1109/CVCBT.2019.000-1.

[31] L.Luu, V. Narayanan, C. Zheng, et al. A secure sharding protocol for open Blockchains[C]. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2016: 17–30. [DOI: 10.1145/2976749.2978389]

[32] A.Sonnino, S. Bano, M. AL-Bassam, et al. Replay attacks and defenses against cross-shard consensus insharded distributed ledgers[EB/OL]. 2019. http://arxiv.org/abs/1901.11218

[33] E. Kokoris- Kogias, P. Jovanovic, L. Gasser, et al. OmniLedger: A secure, scale-out, decentralized ledger via sharding[C]. In: Proceedings of 2018 IEEE Symposium on Security and Privacy (SP 2018). IEEE, 2018: 583–598. [DOI: 10.1109/SP.2018.000-5]

[34] P.Schindler, A. Judmayer, N. Stifter, et al. HydRand: Practical continuous distributed randomness[J]. IACR Cryptology ePrint Archive, 2018: 2018/319. https://eprint.iacr.org/2018/319.pdf.

[35] M. AL-Bassam, A. Sonnino, S. Bano, et al. Chainspace: A sharded smart contracts platform[C]. In: Proceed ings of 25th Annual Network and Distributed System Security Symposium (NDSS 2018). San Diego, CA, USA, February 18–21, 2018. http://wp.internetsociety.org/ndss/wp-content/uploads/sites/25/2018/02/ndss2018\_09-2\_Al-Bassam\_paper.pdf.

[36] M. Zamani, M. Movahedi, M. Raykova. RapidChain: Scaling Blockchain via full sharding[C]. In: Proceed ings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS 2018). Toronto, ON, Canada, October 15–19, 2018: 931–948. [DOI: 10.1145/3243734.3243853]

[37] Y. Sompolinsky and A. Zohar. Secure high-rate transaction processing in Bitcoin[C]. In: Financial Cryptography and Data Security—FC 2015. Springer Berlin Heidelberg, 2015: 507–527. [DOI:10.1007/978-3-662-47854-7\_32]

[38] Y. Liu, J. Liu, Q. Wu, H. Yu, H. Yiming and Z. Zhou. SSHC: A Secure and Scalable Hybrid Consensus Protocol for Sharding Blockchains with a Formal Security Framework. In IEEE Transactions on Dependable and Secure Computing,PP(99):1-1, 2020. doi: 10.1109/TDSC.2020.3047487.

[39] C. Huang, Z. Wang, H. Chen, et al. RepChain: A Reputation-Based Secure, Fast, and High Incentive Blockchain System via Sharding. In IEEE Internet of Things Journal, vol. 8, no. 6, pp. 4291-4304, 15 March15, 2021, doi: 10.1109/JIOT.2020.3028449.

[40] W. Li and M. He. EBFT: A Hierarchical and Group-Based Byzantine Fault Tolerant Consensus Algorithm. 2021 IEEE 12th International Conference on Software Engineering and Service Science (ICSESS), 2021, pp. 32-37, doi: 10.1109/ICSESS52187.2021.9522233.

[41] A. Miller, A. Juels, E. SHI E, et al. Permacoin: Repurposing Bitcoin work for data preservation[C]. In: proceedings of 2014 IEEE Symposium on Security and Privacy (SP 2014). IEEE, 2014: 475–490. [DOI: 10.1109/SP.2014.37]

[42] S. Park, K. Pietrzak, J. Alwen, et al. Spacecoin: A cryptocurrency based on proofs of space[J]. IACR Cryptology ePrint Archive, 2015: 2015/528. https://eprint.iacr.org/2015/528.pdf

[43] HyperLedger, Intel: Sawtooth Lake (2017). [PoET 1.0 Specification — Sawtooth v1.2.6 documentation (hyperledger.org)](https://sawtooth.hyperledger.org/docs/core/releases/latest/architecture/poet.html#introduction)

[44] D. Schwartz, N. Youngs, A. r Britto. "The Ripple Protocol Consensus Algorithm[EB/OL]." https://ripple.com/files/ripple\_consensus\_whitepaper.pdf, 2018.

[45] S. D. Lerner．DagCoin:a cryptocurrency without blocks[EB/OL]. https://bitslog.files.wordpress.com/2015/09/dagcoin-v41.pdf, 2015.

[46] S.Popov. The Tangle [EB/OL]. 2016. WWW.descryptions.com/Iota.pdf, 2018.

[47] Y. Sompolinsky, Y. Lewenberg, A. Zohar. SPECTRE: Serialization of proof-of-work events: Confirming transactions via recursive elections. 2016. https://eprint.iacr.org/2016/1159.pdf

[48] Y. Sompolinsky,A. Zohar. PHANTOM: A scalable BlockDAG protocol. IACR Cryptology ePrint Archive, 2018. 104.

[49] Y. Lewenberg, Y. Sompolinsky, A. Zohar. Inclusive block chain protocols. In: Proc. of the Int’l Conf. on Financial Cryptography and Data Security. Berlin, Heidelberg: Springer-Verlag, 2015. 528–547. [doi: 10.1007/978-3-662-47854-7\_33]

[50] C. L, P. Li, W. Xu,and et al. Scaling Nakamoto consensus to thousands of transactions per second. arXiv Preprint arXiv:1805.03870, 2018.

[51] A. Churyumov. Byteball: A decentralized system for storage and transfer of value[EB/OL]. 2016.https://byteball.org/Byteball.pdf.

[52] Technical White Paper. TrustNote: Fast, Scalable, Developer Friendly. https://github.com/ringringringring/document/blob/master/TrustNote-TR-2018-03.pdf, 2018.

[53] B. Leemon, H. Mance, M. Paul. Hedera: A governing council and public hashgraph network[EB/OL]. 2018.https://www.hedera.com/hh-whitepaper-v1.4-181017.pdf.

[54] C. Lemhieu．Nano:A feeless distributed cryptocurrency network[EB/OL]. https://content.nano.org/whitepaper/Nano\_Whitepaper\_en.pdf