

本科毕业论文



论文题目：**一种新的共识机制及其在数字金融中的应用**

姓 名：陈家豪 学 号：19307130210

院 系：计算机科学计算学院

专 业：计算机科学与技术

指导教师：阚海斌 职 称：教授

单 位：复旦大学

完成日期： 2023年 5月 15日

|  |
| --- |
| **论文撰写人承诺书**  本毕业论文是本人在导师指导下独立完成的，内容真实、可靠。本人在撰写毕业论文过程中不存在请人代写、抄袭或者剽窃他人作品、伪造或者篡改数据以及其他学位论文作假行为。  本人清楚知道学位论文作假行为将会导致行为人受到不授予/撤销学位、开除学籍等处理（处分）决定。本人如果被查证在撰写本毕业论文过程中存在学位论文作假行为，愿意接受学校依法作出的处理（处分）决定。  **承诺人签名：**  **日期： 2023年 5 月 6日** |

|  |  |  |  |
| --- | --- | --- | --- |
| 指导教师对论文学术规范的审查意见：  □ 本人经过尽职审查，未发现毕业论文有学术不端行为。  □ 本人经过尽职审查，发现毕业论文有如下学术不端行为：  **指导教师签名： 日期： 20 年 月 日** | | | |
| 指导教师评语：  **签名**：  **20 年 月 日** | | 答辩委员会（小组）评语：  **签名**：  **20 年 月 日** | |
| **学分** |  | **成绩** |  |
| **备注：** | | | |

目录

[第一章 引言 1](#_Toc7675)

[第二章 区块链技术分析 2](#_Toc5009)

[2.1 区块链的定义和技术原理 2](#_Toc11058)

[2.2 区块链的优劣势分析 4](#_Toc10196)

[第三章 综述：区块链技术在数字金融中的应用 6](#_Toc8525)

[3.1 数字金融的概念和特点 6](#_Toc30965)

[3.2 区块链技术在数字金融中的应用场景和优势 7](#_Toc12083)

[3.3 区块链技术推动数字金融发展的困境 10](#_Toc30856)

[第四章 改进方案：新的共识机制 11](#_Toc11592)

[4.1 原理介绍 11](#_Toc7679)

[4.2 工作流程 13](#_Toc7020)

[4.3 优缺点分析 15](#_Toc32538)

[第五章 改进方案的应用与实验 19](#_Toc8219)

[5.1 数字货币应用场景 19](#_Toc31019)

[5.2 代码模拟实验 23](#_Toc22798)

[第六章 总结与展望 37](#_Toc29958)

# 摘要

区块链技术已经成为数字金融领域中一个备受关注的话题，本文意在研究区块链技术在数字金融领域的应用现状，探讨区块链技术在数字金融领域的发展趋势和未来潜力。本文通过文献综述的方式分析了现今区块链的应用场景，分析了区块链技术原理以及其优缺点，提出了一种创新的优化方法并用代码实现，最后探讨了区块链技术的发展前景。

关键词：区块链，共识机制，数字金融

# ABSTRACT

Blockchain technology has become a highly discussed topic in the field of digital finance. This paper aims to investigate the current application of blockchain technology in the digital finance domain and explore its development trends and future potential. Through a literature review, this paper analyzes the current application scenarios of blockchain, examines the principles of blockchain technology, and assesses its advantages and disadvantages. Additionally, it proposes an innovative optimization method and implements it through coding. Finally, the paper discusses the prospects for the development of blockchain technology.

Key words： blockchain, consensus mechanism, digital finance.

# 引言

区块链技术和数字金融是近年来兴起的两个领域，它们都与现代金融领域的数字化和自动化有关。

区块链技术是一种去中心化的分布式账本技术，它的主要特点是去除了传统中心化机构的控制，通过网络中的多个节点共同维护一个分布式的账本，保证数据的公开透明、不可篡改和安全性。区块链技术最初是作为比特币的底层技术而被应用，但随着技术的不断发展，它在金融、供应链、医疗等领域也得到了广泛应用。[1]

数字金融是金融行业数字化的结果，其主要特点是通过互联网、移动互联网等数字技术来实现金融产品和服务的生产、流通和交易，包括支付、贷款、投资、保险等方面。数字金融的出现和发展是由于数字技术的不断发展和金融市场需求的不断变化，数字金融的发展对于提高金融行业的效率、降低交易成本和提高服务质量等方面都具有重要意义。[2]

区块链技术和数字金融的结合是一种颇有前途的趋势，区块链技术的特点可以解决数字金融中的一些难题，比如数据的安全、透明和减少中间环节的成本等问题。本研究的目的是为了深入分析区块链技术在数字金融中的应用现状和未来发展趋势，探索其优势和应用场景，为相关领域的实践和理论研究提供参考和借鉴，进一步推动数字金融领域的发展。

# 区块链技术分析

## 区块链的定义和技术原理

区块链（Blockchain）是一种去中心化的分布式数据库技术，它可以实现多方之间的可信交互，从而达到数据共享、交易和管理的目的。

区块链的数据结构是将多个数据块首尾相连形成的一个单链式结构，每个数据块称为区块，每个区块包含了区块头、交易数据等信息，其中区块头包含了许多与安全性相关的信息，包括区块hash，前区块hash，merkle根，工作量证明等。

区块链的核心特点包括去中心化、公开透明、不可篡改性和安全性。去中心化意味着没有中心化机构控制区块链，而是由网络中的多个节点共同维护。公开透明指的是所有交易和区块信息都可以在网络中公开查看。不可篡改指的是数据在区块链中被保存为不可修改的状态，一旦存储在区块链中，就无法被删除或篡改。安全性指的是区块链使用密码学技术和分布式系统原理来保证数据的安全和可信性，确保每一笔交易的真实性和有效性。

区块链的关键原理可以分为密码学和共识机制两部分。

1）区块链通过密码学来保证数据的真实性和不可篡改性。以比特币为例：

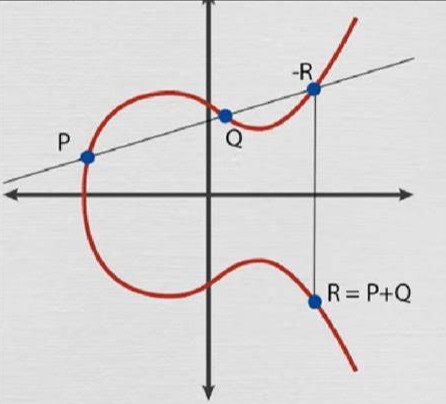
非对称加密算法保证交易真实性。

比特币用户以钱包账户为唯一凭证，进行比特币交易和挖矿。钱包使用ECC加密算法进行加密，每个钱包由一对公钥私钥组成，并且由公钥哈希生成一个更易读的钱包地址。用户A向用户B发送比特币时，需要写上发送方和接受方的地址，且需要附上A的公钥，并将这条交易用A的私钥进行加密生成签名。任何人可以用A的公钥对签名进行解密，验证交易是否是由A发起。非对称加密算法和数字签名保证了交易不可伪造、不可抵赖。

ECC算法的原理如下：

简单来说，椭圆曲线算法是在一条特定的曲线上面定义的一种广义的加法运算，一般的椭圆曲线方程为, 而比特币采用secp256k1这条特殊的椭圆曲线：。

椭圆曲线上点的加法为：过曲线上的两点 P、Q画一条直线，找到直线与椭圆曲线的交点，交点关于x轴对称位置的点，定义为P+Q，即为加法。

而2P就是指过P作椭圆曲线的切线与曲线的交点关于x轴的对称点。

而kP(k为正整数)就表示k个P相加后的结果。

如果当k特别大时，已知P和kP，是无法直接计算出k值的。而已知P和k，可以较快计算出kP。ECC加密原理就是基于这个特性。ECC密钥包括3个重要参数：基点G，私钥k，公钥kG。

比特币中的私钥取值介于，即是一个256bit的二进制数。由基点G和k可以计算出Q = kG，即k对应的公钥。

ECC算法的公钥加密、私钥解密过程：

待加密报文为Message，发送者首先将Message转码成椭圆曲线上一点M，然后生成密文：(r为随机数)。解密时，接受者为了获取M，只需要计算，再解码为Message即可获得明文。

ECC算法的签名过程：

签名时，发送方选择随机数r，待签名消息M。

则签名为： ， 其中。

验证签名时，接收方计算：

如果验证结果为rG，则验证签名成功。

哈希算法保证交易数据不可篡改性。

区块使用Merkle Tree 算法保证交易信息不被篡改。矿工在对区块进行打包时需要对区块体的所有交易信息用Merkle Tree算法进行哈希，当任何一条交易数据被篡改时，可以通过merkle根验证得知，防止区块的交易信息被篡改。

且每个区块都在区块头中记录了上一个区块的id为preId，在计算本区块id时会将preId，merkle根等进行哈希运算，如果区块链中的任意一个区块改变，其id会被改变，则会链式影响到后续区块，保证了区块链的历史数据不被篡改。

1. 区块链通过共识机制来保证数据的一致性和可靠性。

共识机制是指通过多个节点之间的交互来达成共识，从而保证每一笔交易的真实性和有效性。目前主流的共识机制包括工作量证明POW（Proof of Work）、权益证明POS（Proof of Stake）、权益共识DPOS（Delegated Proof of Stake）等。其中，工作量证明是最早也是最为流行的共识机制。[3]

在工作量证明POW中，矿工打包区块时需要计算一个数学难题：寻找一个特殊正整数值Nonce，使其满足（前区块id+区块id+时间戳+Nonce）进行sha256哈希之后得到的二进制数的前n位都为0（n为设置的难度系数）。由于哈希的不可逆性，矿工只能将Nonce从1开始递增代入计算，直到得到一个满足要求的Nonce。

矿工会将这个数打包进区块后发送给其他节点，其他节点接收到区块后会进行检验，看Nonce值是否满足难度值要求。如果满足，则会将区块加入本地的区块链，否则就不接受。比特币系统以这样的共识机制保证计算出来的区块被所有人接受，以及控制平均每10分钟才能生成一个区块，避免区块链被攻击。

权益证明PoS与PoW不同，PoS不需要矿工通过解决复杂的数学问题来竞争获取记账权。相反，根据持有的加密货币数量和时间，网络中的参与者拥有不同的权益，持有更多权益的人在创建新区块的机会上相对更高。

通过使用POS权益证明，网络的参与者可以锁定一定数量的加密货币作为抵押品，并将其用作验证和创建新区块的权益。这种机制有助于提高网络的安全性，因为攻击者必须掌握大量的加密货币才能对网络进行攻击。此外，PoS消耗的能源较少，相对环保。

POS权益证明是许多加密货币项目中使用的共识机制，例如以太坊（Ethereum）正在进行从PoW到PoS的过渡。这种共识机制的目标是提高效率、降低成本，并为加密货币网络提供更好的可扩展性和安全性。

## 区块链的优劣势分析

* + 1. **区块链的优势**

区块链最大的优势在于其数据的安全性，我将从几个方面描述区块链如何保证数据安全：

1）哈希与链式结构保证历史数据不可篡改

假设区块链有A->B, 在计算区块B的hash值时需要包含区块A的hash和B的merkle根，那么如果攻击者只修改了区块A的内容，则A的hash会变（因为A的merkle根会变），这会导致B的hash无法通过检验，除非改变B的hash值。然而区块链运行越久，区块就越多，这使得修改历史数据需要连锁修改成千上万个块，且修改区块后需要重新计算Nonce值（在工作量证明机制中），耗时巨大，这保证了区块链的历史数据难以被修改。

2）分布式系统保证无法从单节点破坏区块链

电子数据单节点存储，存在服务器崩溃导致数据丢失以及攻击者直接篡改数据的风险，这也是现实中一些电子数据无法直接作为司法证据的原因。如果区块链只在单机运行，该机操作者还是可以依次篡改区块链数据。但由于区块链是分布式系统，网络中有非常多个节点都保存了区块链本体，节点会根据少数服从多数的原则选择被更多结点承认的区块链，除非攻击者篡改51%以上的节点，否则区块链不会被破坏。

3）工作量证明机制避免双花攻击

双花攻击的含义是“一笔钱花两次”，通常是，攻击者在花费比特币的同时，又伪造一笔交易将比特币发给自己另一个钱包，并在本地打包，让区块链形成两条分支A,B。当A分支上的正常交易被确认后，攻击者得到了现金或商品，他会在B分支上继续挖矿，使其长度超过A，从而使A分支失效（最长链原则），让交易另一方没有得到比特币。

而工作量证明机制让这种攻击变得很难以实施。

首先，在攻击者构建自己的私链时，网络中的其他矿工也在继续正常挖矿，攻击者要想他的私链成为最长链，他必须挖得比其他矿工更快，即拥有超过全网51%的算力。

而且比特币系统会调整难度值控制生成一个新区块的平均时间是10分钟，这会保证区块链分叉的概率更小，确保网络中的矿工都在同一个分支上挖矿。我们假设任何一个新的区块传遍网络需要1分钟，那么在新区块在传播过程中，没收到它的节点又生成了一个新区块的几率是1/10（假设大家都是10分钟挖出一个区块）。然而，如果2分钟产生一个区块的话，那么产生一个分叉的概率就是1/2。如果区块链中长期存在分叉，那么全网矿工就会随机选取一个分叉进行挖矿，全网算力也被分摊，那么攻击者构建最长链的可能性也会增大，这也是比特币为何不能减少区块产生时间的原因。

**2.2.2 区块链的劣势**

显然，区块链是牺牲了效率来满足安全性，区块链的劣势就在于它的效率低下，算力消耗严重。由于分布式需求，一个新区块产生后需要发布到全网的结点，且每个结点都需要保存数据副本，效率比传统的数据中心低。而且在支付领域，和电子货币相比，以比特币为例的采用POW机制的区块链数字货币的效率更低，比特币10分钟才产生一个区块，一个区块装载4000条交易，导致其完全不能作为日常支付使用。而且比特币的工作量证明机制存在极大的算力浪费和不公平性，只有算力大的矿工才有机会打包，算力弱的矿工在一轮竞争中很难先挖到矿，导致矿工的算力被浪费。为了挖到矿，矿工集结算力组成矿池进行挖矿的现象更加普遍，这也与区块链分布式的初衷相违背。POS权益证明机制虽然避免了算力的浪费，将打包权赋予给资本更多的矿工，但这也缺乏了公平性，而且需要矿工先“充值”再挖矿，可当区块链还未发展壮大时谁有权打包也是一个问题，目前机制尚不成熟。

总之，区块链是一种去中心化的分布式数据库技术，其核心原理是使用密码学技术和分布式系统原理来保证数据的安全传输和存储，通过共识机制来保证数据的一致性和可靠性，其核心特点包括去中心化、公开透明、不可篡改和安全性。区块链保证了数据的安全性但是牺牲了效率，存在一定的缺陷。

# 综述：区块链技术在数字金融中的应用

* 1. **数字金融的概念和特点**
     1. **数字金融的概念**

数字金融的概念一般是指传统金融机构与互联网公司利用数字技术实现融资、支付、投资和其他新型金融业务模式。举例来说，移动支付、物联网信贷、数字货币都属于数字金融。一般来说，我国将2004年底的支付宝诞生看作中国数字金融的初始萌芽期，而2013年6月推出的“余额宝”，则真正标志着我国数字金融开始发展。

* + 1. **数字金融的特点**

1. 更低的服务成本

数字金融通过数字化技术替代了地域网点和人力投入，减少了金融机构的开支。传统金融机构需要承担线下铺设经营点和拓展分部组织的固定成本，尤其是在低密度偏远地区，增设服务点的收入无法覆盖支出成本，导致金融服务供给受阻。而数字金融则通过数字化技术，减少了地域网点和人力投入，降低了服务新用户的成本，从而减少了金融机构的开支。

1. 更高的效率

传统金融机构由于信息不对称和风险控制要求高等因素，导致产品推广和交易流程繁琐，推广宣传效率低下。然而，数字金融利用先进的科技解决方案，如大数据技术，可以多维度分析用户数据信息，准确识别需求并进行精准营销。这大大缩短了金融服务供求双方的搜寻和匹配时间，降低了金融机构拓展新客户的成本，提高了金融服务的效率，实现了商业可持续性。

1. 更大的覆盖范围

传统金融服务需要依靠物理网点和分支机构的布局，通常只在人口稠密和经济发达地区投放资源，而忽略人口密度低、地理位置偏远和经济欠发达的地区。数字金融通过互联网和移动信息技术，突破了地域限制，实现了跨越空间的无差别金融服务。从县级到村庄、社区各层面，数字金融得到了根本性发展。

1. 更广泛的服务对象

数字金融不仅实现了普惠金融的目标，普及金融服务对象，而且通过技术支持实现了灵活性。例如，利用大数据技术，可以帮助低收入群体和中小型企业满足金融服务的需求，解决他们在传统金融机构信用评估阈值限制下的问题。此外，新技术的发展也拓宽了普通用户和各类金融资本参与金融活动的渠道与机会。[4]

总的来说，数字金融是传统金融与新兴技术的融合，数字金融的新技术新思想催生了共享经济、网络经济等商业模式，为创新创业提供了空间；数字金融将传统金融服务的成本降低，优化金融风险控制方式，扩大覆盖范围，为原本难以获得有效金融服务的低收入者、小微企业等提供有效的金融服务，推动了中国普惠金融的建设。

* 1. **区块链技术在数字金融中的应用场景和优势**

区块链技术是一种去中心化、安全性高的分布式账本技术，因其独特的技术特点，已经在数字金融领域得到了广泛的应用。以下是对区块链在数字金融中的应用相关研究状况的综述：[5]

* + 1. **数字货币领域**

数字货币是以数字形式存在、没有物理载体的货币。数字货币的工作原理与传统的货币不同，它不需要中央机构来管理或控制，而是依靠分布式账本技术来实现去中心化的交易记录和管理。

数字货币是区块链技术应用的重要领域之一，大多加密数字货币都采用区块链作为其底层技术。数字货币相比于传统货币有以下几点优势：

1. 避免了通货膨胀和货币政策的调控问题。由于数字货币的发行和流通是由区块链来控制的，没有中央银行或政府来掌控，因此可以避免通货膨胀和货币贬值的风险。
2. 数字货币具有高度的安全性。区块链的交易记录是公开可查的，且具有可追溯、防篡改等特点，并且利用了数字加密、数字签名等技术，防止了伪造交易的风险。
3. 数字货币具有较强的匿名性。目前的支付工具，无论是银行卡还是微信、支付宝，都是与银行账户体系绑定的，银行开户是实名制，无法满足匿名诉求。数字人民币与银行账户松耦合，可以在技术上实现小额匿名。数字货币对用户隐私的保护，在现行支付工具中是等级最高的。[8]
4. 数字货币的流通速度非常快。数字货币不需要传统的中介机构，如银行或交易所，来进行交易，交易可在用户间直接进行。传统的货币在进行跨国交易时需要进行繁琐的流程，而数字货币则不存在障碍，可以极大地提高货币流通速度。

区块链技术的去中心化、可追溯、防篡改等特点使其在数字货币的发行、交易、监管等方面具有独特的优势。目前，比特币、以太坊等数字货币已经成为了区块链技术在数字金融领域的代表性应用。

* + 1. **供应链金融领域**

供应链金融是区块链技术应用的另一个重要领域。

供应链金融起源于供应链管理。供应链管理流程一般为：计划-》采购-》生产-》存储-》分销-》服务。供应链上的企业一般分为上游企业、核心企业、下游企业。其中核心企业一般具有较大的规模和信用，经营压力小，而处于上游和下游的小微企业一般具有较小的话语权，存在较大的资金压力。中小企业融资难一直是我国一大社会难题。中小企业因为自身信用级别较低，固定资产等抵押担保品较少、财务信息不透明等原因，很难在银行等金融机构贷款大笔资金。为了解决这一难题，与之合作的核心企业希望利用自身良好信用帮助中小企业取得金融机构的贷款，于是，供应链金融应运而生。

供应链金融是一种新型融资方式，专门为中小企业而设计。它将资金流与供应链管理过程有机结合，利用核心企业的信用担保，将低成本的资金引入供应链上下游的中小企业，解决它们的资金短缺问题，确保整个供应链的资金流动高效运转。[6]

然而传统的供应链金融存在一些问题，企业间和银行间信息不对称，信息真实性难以证明，可能存在企业捏造数据骗取银行贷款，导致信用评估代价增加。

而区块链技术的引入可以优化供应链金融的以上问题，供应链上的企业可以将企业的业务关系、经营状况等信息上传至区块链，区块链技术的可信任性、去中心化等特点使其能够有效地解决信息不对称等问题，从而提高了供应链金融的效率和可靠性，便于银行对供应链上的中小企业进行信用评估。目前，国内外的企业已经开始将区块链技术应用于供应链金融领域中。

* + 1. **智能合约领域**

“智能合约”的概念于1994年由计算机科学家尼克·萨博于《智能合约》（Smart contracts）一文中被正式提出。智能合约是指一个能够自动执行合约条款的数字化程序，通过从外部获得的数据信息予以识别判断，当程序设定的条件满足时便自动执行合约条款。尼克·萨博指出智能合约的条款（如抵押品、产权划分等）应可以嵌入到处理硬件和软件中，通过采用这样的方式来使得违约成本非常昂贵且不可抵赖。而实现智能合约的最大障碍是计算机程序不能真正地触发支付，金融机构仍然需要手动批准资产的转移，在这种情况下，意味着智能合约的目标就没有实现。

而区块链技术的应用使智能合约得以实现。合约双方对相关合约代码签名后，智能合约即可上链，相关资金就会按照合约执行，任何一方不能控制或者挪用资金，确保交易安全。记录在区块链上的智能合约具备不可篡改和无需审核的特性。区块链技术的不可篡改、去中心化、公开透明等特点，使其在智能合约的执行、管理等方面具有独特的优势。目前，国内外的企业已经开始将区块链技术应用于智能合约领域中。[7]

总的来说，区块链技术在数字金融领域中的应用已经成为了当前研究的热点之一。未来，随着区块链技术的不断发展和完善，其在数字金融领域中的应用将会越来越广泛。

* 1. **区块链技术推动数字金融发展的困境**

虽然区块链技术为数字金融的发展带来了许多重大突破，但现在数字金融的应用状况仍存在一些困境。

1. 区块链的不可篡改性与“删除权”相悖

区块链的历史数据不可篡改是其重要特性，保证了历史数据的安全。然而这与个人数据的“删除权”相违背，个人的交易记录等数据将被永久记录在区块链上，可能对个人隐私有一定风险。“不可篡改”的特性也可能存在一些应用瓶颈。[8]

1. 现有数字货币效率低下

以比特币为例，由于比特币采用POW（proof of work）共识机制，生成一个新区块的速度被限制在10分钟左右，这导致了系统的交易成交速度约等于7 tps(每秒7笔交易成交)，而且一笔交易最少也要10分钟才能被确认。且金额较小的交易不一定能被打包上链，由于手续费较少，可能一直不会被矿工选取，存在“排不上号”的情况。

显然，这个交易速度无法满足全球使用者的日常支付需求。基于区块链的数字货币存在应用场景的局限，不适用于日常支付，只适用于大额交易。

# 改进方案：新的共识机制

区块链技术目前无法应用到交易量大，交易迅速的应用场景中，比如数字货币日常支付。本文在此提出一个改进方案，主要是提出一个创新的区块链共识机制：委派机制。

* 1. **原理介绍**

委派机制的原理如下：数字货币系统存在一个可信的中央节点和很多挖矿节点，每个节点都可以接收交易信息。当有用户上传新的交易信息时，他会将消息广播，中央节点和所有的挖矿节点都收到交易信息，并放入本地的“待分配交易队列”。中央节点有权力将待分配的交易分配给一个矿工进行打包，它会广播一条“分配”消息，将id为a,b,……的交易分给矿工A打包。所有矿工收到“分配”消息后，会将id为a,b,……的交易从“待分配交易队列”放入“已分配交易队列”并标记打包者为A。

全网只有A可以打包这些交易，因为结点在收到一个新的区块时，会检验区块里的交易是不是存在于“已分配交易队列”，以及交易是不是被分配给了区块的打包者。如果B打包了分配给A的交易，他打包的区块不会被其他节点认可，会被直接丢弃，这使得矿工间没有算力竞争。

而且在分配交易时，中央节点已经确认好了区块的顺序，中央会告知矿工A他打包的区块的位置height，并计算好前置区块的id告知A，这样节点在乱序收到不同的区块时也能正确地组装，不会产生分支。

中央节点分配任务的策略是“排队策略”：想要获取打包权的矿工需要向中央申请进入一个候选队列，中央依次选取队列中的矿工分配任务。在候选队列的矿工需要承担校验新区块的职责，他们需要一直维护完整的区块链，接收新的区块并校验，在校验成功时向中央返回一个“确认”信息，使区块链得到足够多的确认，保证安全性。

* 1. **工作流程**

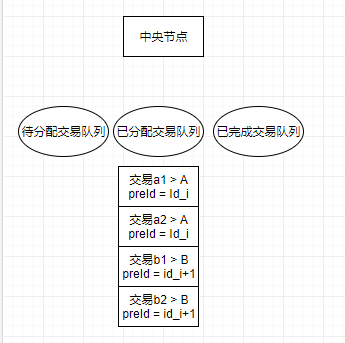


图4.1 中央节点接收到交易信息

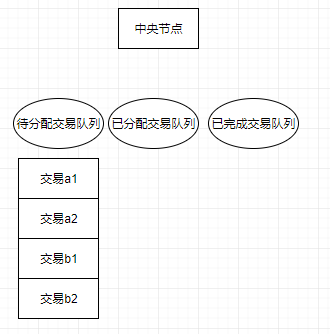


图4.2 中央节点分配交易给矿工A,B，并给出区块位置和前区块Id

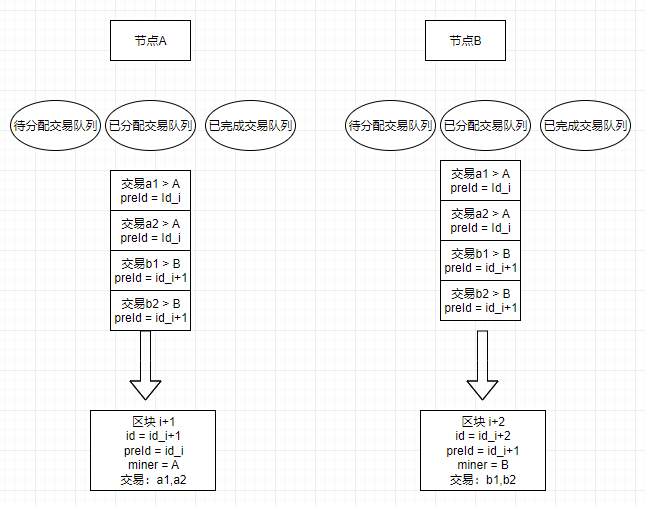


图4.3 节点收到委派指令，矿工将分配给自己的交易打包，不打包其他交易

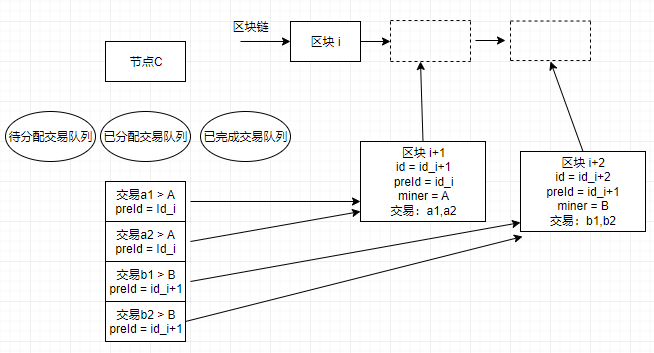


图4.4 节点收到A,B打包的区块，会对其进行检验，各项都符合时区块上链，返回确认

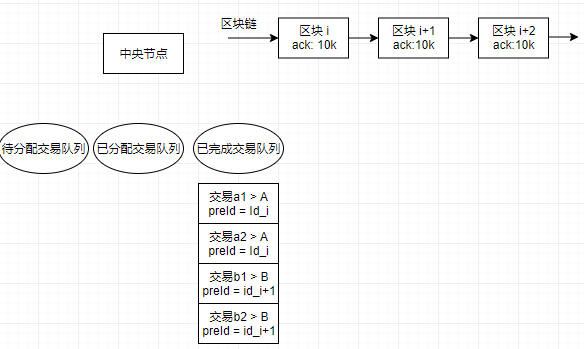


图4.5 中央节点会记录区块的确认数ack（每个节点确认区块无误都会返回确认），当确认足够多时，将交易移至已完成队列。

如果区块打包失败，则重新将任务委派给下一位矿工

* 1. **优缺点分析**
     1. **优点**

委派机制的区块链数字货币相比于传统POW数字货币有如下优点：

在公平性上，区块链网络中的矿工通过排队策略依次获得打包权，只要为维护区块链付出贡献，每个矿工都有机会打包，矿工在自己打包的区块上链后会获得奖励，这样保证了矿工的公平性和较高的参与度，避免了POW中的矿工间的算力竞争和结队挖矿，利于让更多结点参与到维护区块链中，提高了区块链的安全性和分布性。

在效率上，委派机制相比于POW会有前所未有的提升。首先，委派机制让区块链的构建变成了并发进行的。假如要构建一条区块链为：->A->B->C，传统的方式是依次打包ABC，依次上链，而委派方式可以一次性将ABC分给矿工a，b，c打包，三人完成后各自向网络发送区块。由于提前确定好了顺序，即使一个节点乱序接收到包ABC，节点也能将区块正确组装。

最重要的是，矿工在打包时不必再花很长时间计算数学难题，因为POW这样做的意义在于避免让区块链产生太多分叉，而委派机制由于提前确认了区块顺序，不会产生分支，所以花费算力计算数学难题不再有必要。这意味着，交易流量的上限几乎就是中央节点分配任务的速度上限，交易被确认的速度几乎就是一个区块传遍全网的速度。

在安全性上，该机制基本上没有违背区块链的设计初衷，同样有传统区块链一样的防篡改、去中心等特点。虽然区块间是并发打包的，但区块链保留了preId（交给中央节点计算），区块间保持链式哈希结构，可以像传统区块链一样防止历史信息被篡改。

而且凭借中央节点提前指定序列，该机制避免了传统的分叉问题，可以避免私链攻击。对于双花攻击，由于“已分配交易池”的机制，每一笔交易都需要由中央结点分配才会被确认，那么攻击者构建的私链是不会被其他结点承认的，从而避免了双花攻击。

* + 1. **缺点**

委派机制也存在如下缺点：

1. 防篡改性变弱

如果攻击者篡改了某历史区块，则区块的id改变，需要重新计算Nonce值，并且需要连锁修改这个区块之后的其他区块。POW机制下的区块链计算出一个区块Nonce值需要较长的时间，如果攻击者修改了倒数第N个区块，那么他需要计算N个区块的Nonce值。这将是几乎不可能完成的，因为攻击者在篡改历史数据的同时，网络中的其他矿工节点也在持续地挖矿，持续地添加新的区块，攻击者在修改历史区块的同时，还要赶超其他矿工的挖矿进度，才能让自己的区块链有效，这要求攻击者拥有远超网络中其他矿工的算力。

但委派机制下，计算区块Nonce值不必花费太多时间，攻击者只要有一定算力就可以很快地完成整个区块链的连锁篡改，数据的安全性会变弱。如果只在单机上运行，是无法保证区块链不被篡改的。但是由于区块链分布式的特性，每个矿工节点都独立保存了区块链的副本，任一节点在获取区块链时可以采取“多数”原则，选择大多数节点都认同的区块链。只要网络中参与的矿工足够多，且超过一半都是“诚实”矿工，那么系统仍然会保留正确的区块链，不会承认被篡改后的区块链。只要攻击者无法同时篡改全网50%以上的“诚实节点”，就无法破坏区块链系统。

1. 单点失效问题

传统的区块链货币每个结点都可以记账，任何结点失效都不会影响整个系统。然而在委派机制下，区块链会存在单点失效问题。

如果中央结点被攻击导致节点瘫痪，交易将无法被委派，也就无法被矿工打包上链，这会对系统造成严重影响。攻击者可以采用DDoS攻击等方式挤占中央节点的流量，即可瘫痪区块链网络，使交易无法被处理。

而且被委派打包任务的矿工节点如果失效也会引发问题。中央节点无法预估被委派矿工是否具有处理能力，如果矿工处理超时或者只是一个虚假节点，不处理打包任务，则委派给他的交易会延迟上链确认。如果交易的确认超时，中央节点还需要重新将任务委派给另一个矿工节点，耽误交易的处理。如果是传统的区块链则不会存在这个问题，因为网络中是有多个矿工在竞争打包。这是委派机制相对于传统区块链的一个劣势。

1. 中央结点的可信度问题

由于中央结点的重要地位，中央结点的运营者必须要具有一定的公信力。中央结点的运营者可以靠作弊来谋取利益，比如将打包权一直赋予给自己的矿机来获取挖矿奖励，破坏其他矿工节点的权益。如果运营者无法取得大众的信任，那么矿工对区块链的参与度就不会太高，区块链的安全性就会降低。但是相比于传统的数据中心，运营者作弊的程度仍是十分有限的，他不能伪造交易（由于数字签名技术），不能篡改历史数据（由于区块链采用多数原则），不能操控某个用户的账本，也不能控制全网其他结点，所以委派机制下的区块链依然保有传统区块链的可信度。

1. 中央节点的压力问题

在委派机制中，中央节点被赋予了更多的职责，不仅需要存储全网矿工节点的地址信息，分配打包任务，还需要在分派任务时计算该区块的id。过多的职责让中央节点的逻辑更加复杂，承载压力更大，可能会导致处理交易的速度上限降低，可能会存在程序出错的情况。

# **改进方案的应用与实验**

* 1. **数字货币应用场景**

数字货币在数字金融中是一个非常重要的领域，推动数字货币的建设有助于数字金融的深入发展。数字货币相较于传统货币和电子货币有自己特有的优势，在安全性和流通性上都有较大的提升。虽然现有的区块链数字货币技术存在应用瓶颈，但经过改进后的采用委派机制的区块链数字货币可以满足以下应用场景。

* + 1. **双离线支付**

现有的电子货币支付手段最流行的是支付宝、微信等平台，通过计算机网络系统以电子信息传递形式实现流通和支付。现有的支付方式其实已经具有足够的便利性和安全性，已经可以作为个人的“数字钱包”。但仍存在“双离线支付”的瓶颈。[10]

然而基于区块链的数字货币却可以实现“双离线支付”。区块链数字货币的交易概念其实类似于先“打白条”，再支付。例如，A要向B转账100元，他们可以通过某个“数字钱包”终端，生成一笔交易记录:{“send”: A, “receive”: B, “amount”: 100}，这条交易会由A用私钥写上数字签名，相当于“打白条”。当A或B上线后，将终端上的交易记录上传至网络，交给矿工打包上链，实现交易的完成。

由于区块链交易有数字签名的存在，交易具有防伪性和抗抵赖性，只要有A的私钥签名，这条交易就一定是由A发起的，一定会被上链记录，否则就是虚假交易，不会被记录。

所以只要交易双方有自己的公钥私钥，有一个终端可以完成私钥加密以及交易数据的记录，那么即使没有网络，该笔交易也会保持有效性，完成双离线支付。

* + 1. **高交易量快速零售支付**

改进后的数字货币最大的特点就是可以用于大流量的快速日常零售支付。传统的数字货币的一个痛点就是效率太低，成本太高，用户在日常支付时不会愿意等待较长的时间确认交易以及支付交易手续费。数字货币无法用于日常零售支付，这将成为数字金融深度发展的一个瓶颈。

2018年微信总交易笔数为4664.75亿笔，平均每日超13亿笔交易，那么平均每秒有超1.5万笔交易。2017年双11支付宝峰值完成每秒25.6万笔交易。现有移动支付的吞吐量是区块链数字货币不可比拟的，因为区块链有更多限制速度的瓶颈，比如需要计算Nonce值，数据需要在更多网络节点间相互传递等。

然而如果采用委派机制下的区块链数字货币，交易效率将大大提高。首先，委派机制的数字货币每秒处理交易数量的上限仅取决于中央节点的性能，中央节点每秒最多能委派的交易数量就是系统的最大吞吐量，因为委派出去的打包任务都是并发进行的，而且假定总有多余的矿工在等待分配任务。以这个为系统吞吐量上限的话，只要中央节点有一台较好的服务器，就能处理很大的交易流量。然后，交易被确认的速度也会大大增加，因为矿工节点不再需要计算数学难题，打包区块就几乎不再需要时间，那么交易确认的时间几乎就是三倍的网络传输时间：中央节点分配任务->矿工打包后发给网络其他节点->其他节点返回确认给中央节点。这个时间完全可以满足用户日常支付的需求。

而且，数字货币还有较强的抗压能力。数字货币的交易不一定要立即上链记录，只要对交易签名后，交易就永久有效，所以可以等系统压力较轻的时候再上链记录。比如在“双十一”等瞬时交易量高的时候，商家可以先将用户的付款记录保存下来，先即时完成交易，然后缓慢等待交易上链记录。商家不用担心因为流量问题导致交易记录丢失，因为只要他保存着交易信息，交易就是永久有效的。委派机制的数字货币因为离线支付的机制，拥有较强的抗压能力，可以避免流量过大时交易信息的丢失。

* 1. **代码模拟实验**

本文用java SpringBoot框架编写了委派机制区块链的基本模型，代码的源码地址为：<https://github.com/cjhhgs/BlockChain。>

实验环境: 编译器为IDEA 2023, 语言为java 8, 操作系统为windows10。

* + 1. **代码说明**

项目结构如下：

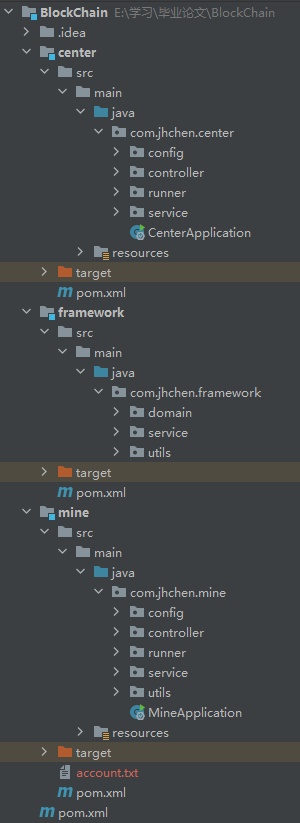


图5.1 项目文件结构

项目分为3个模块，center,mine,frame。

frame模块提供公用的数据结构类、通用方法，比如提供了ECC加密算法相关的方法，区块链、交易池的数据结构，HTTP数据传输的工具类。

center模块提供了中央节点的相关服务。启动主类CenterApplication即可以启动一个中央节点服务。center提供的服务有：

1. 维持一个区块链，且区块链初始仅包含一个创世区块；
2. 维持一个交易池，交易池中有未分配交易、已分配交易、已完成交易三个队列；
3. 记录全网注册节点，维持一个矿工排队队列。可以接收任何用户节点的注册和排队申请。
4. 接收新的交易信息。用户节点可以将交易信息创建好后发送给中央节点，中央节点会对信息进行校验成功后，放入“未分配交易”队列中。
5. 委派矿工对交易进行打包。中央节点可以从等待队列中选取第一位矿工，将部分未分配交易分配给他打包，委派的方式是将未分配交易装配成已分配交易并放入已分配交易队列，并广播给所有用户节点，让其他节点知晓委派信息。
6. 接收新的区块。中央节点可以接收其他节点发送的区块，会检验区块信息是否正确，打包者是否是被委派的矿工，如果检验通过则会将区块放入区块链相应位置。如果收到乱序区块，由于区块链采用数组的结构，中央节点还是可以将其放入指定的位置。
7. 接收其他节点的确认。其他节点也会接收到新区块，他们在校验成功后会向中央发出一个对该区块的确认信息，中央节点会记录确认次数。

mine模块提供了矿工节点的相关服务。启动主类MineApplication即可以启动一个中央节点服务。mine提供的服务有：

1. 和中央节点一样维持一个区块链，交易池，全网注册节点信息。
2. 生成或从本地文件加载一个账户信息。初次启动矿工节点需要用程序随机生成一个区块链账户，包含公钥私钥，地址，ip。加密算法采用与比特币相同的ECC加密算法生成。系统会将账户信息记录在本地文件，下次启动服务会自动加载。
3. 向中央申请注册或排队。可以将自己的账户和ip在中央节点和其他节点注册，这样可以收到全网节点广播的信息。申请排队后，可以等待中央委派打包任务，获取奖励。
4. 创建交易，广播交易，接收交易信息。mine作为用户节点，可以创建交易（只能让自己作为发送方），创建后将交易存储在本地的未分配交易队列，并向全网节点发送此信息。mine节点拥有和中央节点一样的接收校验交易信息的功能，且仅接收中央节点的分配指令。
5. 和中央节点一样接收、检验新的区块。
6. 挖矿功能。当检测到已分配队列中有分配给自己打包的交易时，挖矿节点会进行挖矿操作，将交易打包成区块，广播给全网节点
   * 1. **代码运行效果展示**
7. 基本运行流程演示。

程序在IDEA中运行，采用SpringBoot框架，基本功能通过调用接口演示，并且采用了swagger-ui模块展示接口调用过程。首先启动中央节点和一个用户节点，以下是swagger-ui前端页面，展示了部分可调用的接口。

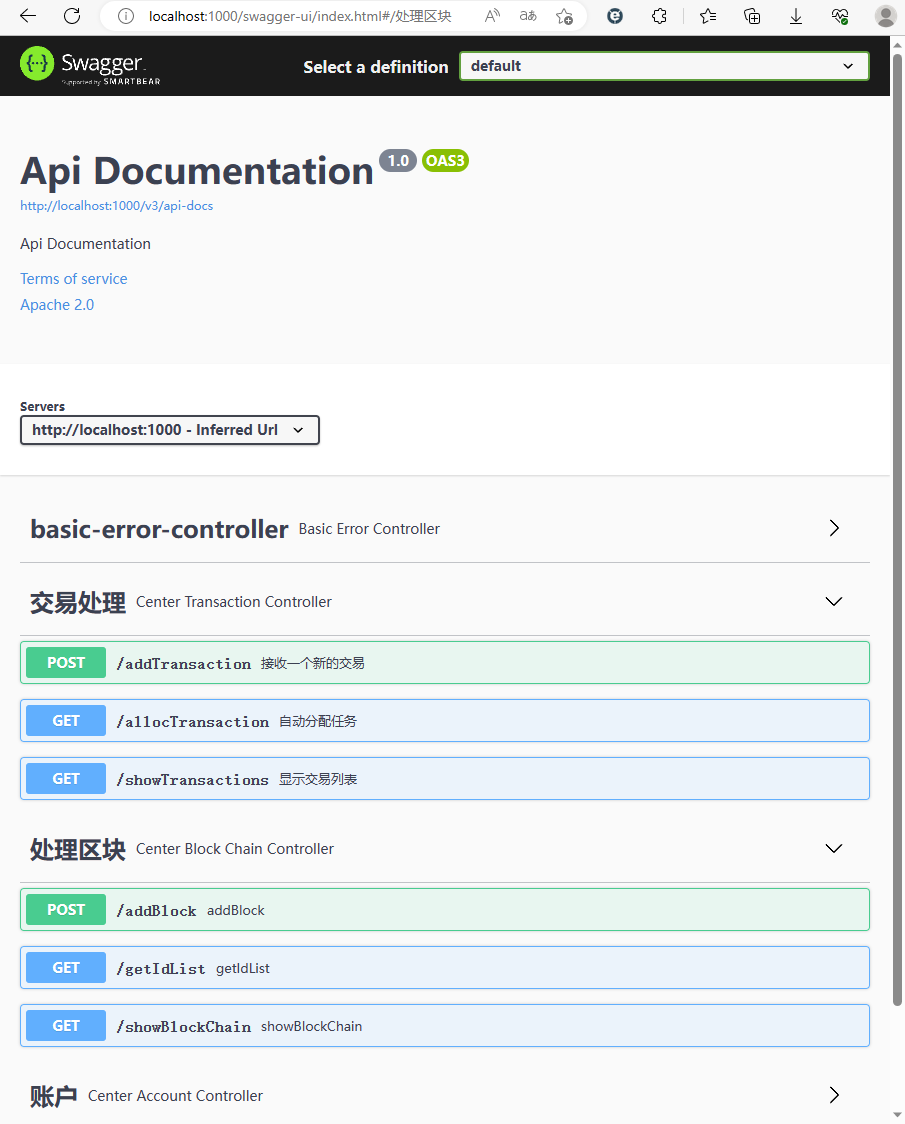


图5.2 前端交互演示

用户节点在启动后会执行一系列初始化，会从中央获取区块链副本和交易池副本。用户节点还会尝试从本地文件加载账户信息（账户文件地址在profile文件中设置）。

加载本地账户：

{"addr":"1NtHXf16mG5dLTQyVUA4QvPPWQzx2UaeiS","ip":"http://localhost:8081","privateKey":"MIGNAgEAMBAGByqGSM49AgEGBSuBBAAKBHYwdAIBAQQguLLbZ9vhIdJzZtHRjKofJ7PYNezH9+Wlo4fwiJ+csMygBwYFK4EEAAqhRANCAARmZpvFYsApqmoehO810oY8CjqpOP6W8RyhYvno8h5UxLv06n7QNhM6rxxLgEOtdDfcErQtlzRC5Bj3Rhy/oy8f","publicKey":"MFYwEAYHKoZIzj0CAQYFK4EEAAoDQgAEZmabxWLAKapqHoTvNdKGPAo6qTj+lvEcoWL56PIeVMS79Op+0DYTOq8cS4BDrXQ33BK0LZc0QuQY90Ycv6MvHw=="}

获取交易列表

TransactionPool(transactionList=[], allocatedTransactionList=[], finishedTransactionList=[])

获取区块链

{"code":200,"msg":"success","data":[{"height":0,"id":"0","preID":null,"merkle":null,"targetBits":0,"nonce":null,"timestamp":0,"body":null,"minerAddr":null}]}

Block(height=0, id=0, preID=null, merkle=null, targetBits=0, nonce=null, timestamp=0, body=null, minerAddr=null)

blockChain:[Block(height=0, id=0, preID=null, merkle=null, targetBits=0, nonce=null, timestamp=0, body=[], minerAddr=null)]

加载中央节点ip

finish init

如果还没有本地账户，用户节点首先需要调用接口创建一个账户并存储在本地。效果如下：

{

"code": 200,

"msg": "操作成功",

"data": {

"addr": "1PqHV5LNUtHp91oKAAEeq8uFXSBY5A7Wn4",

"publicKey": "MFYwEAYHKoZIzj0CAQYFK4EEAAoDQgAEBqBPT3pqCj09O2NAGO50mrYnTKMg6CUAF+RGEUn79jUGip5q8NxSJJykFBOYg5Jl5N+5aaWHBuViGxyjYwfTHw==",

"privateKey": "MIGNAgEAMBAGByqGSM49AgEGBSuBBAAKBHYwdAIBAQQg9A6c6aOHstnnd6ISkMKtWEEch8Waeca5YfVMQ4ep+C2gBwYFK4EEAAqhRANCAAQGoE9PemoKPT07Y0AY7nSatidMoyDoJQAX5EYRSfv2NQaKnmrw3FIknKQUE5iDkmXk37lppYcG5WIbHKNjB9Mf",

"ip": "http://localhost:8081"

}

}

随后节点需要向中央注册或申请排队，方便接收中央节点的消息以及获取打包权。

节点可以创建交易信息，每条交易都只能由发送方创建并签名才有效。在创建好后，节点自动将交易信息存入本地交易池并发送到中央节点。此时查看交易池可以看到所有的交易信息。

GET /showTransactions 显示交易列表：

{

"code": 200,

"msg": "操作成功",

"data": {

"transactionList": [

{

"hash": "3ab264eb22fa94d9dd3e7707cfa13936d1dbac45a51a408158b8c639f10e2c41",

"publicKey": "MFYwEAYHKoZIzj0CAQYFK4EEAAoDQgAEBqBPT3pqCj09O2NAGO50mrYnTKMg6CUAF+RGEUn79jUGip5q8NxSJJykFBOYg5Jl5N+5aaWHBuViGxyjYwfTHw==",

"transaction": {

"send": "1PqHV5LNUtHp91oKAAEeq8uFXSBY5A7Wn4",

"receive": "1CUpy3wC2wtvSPBWsR1hRSr6mUw8RdvoNj",

"amount": "10"

},

"sign": "MEUCIAwkjr8wTNzo0kgt2vdYSNbd/2bkkkKRiHWc/Z53Hi9vAiEAwH8HHJAre9LMIciuPKWFylMrkg0xsMe+KrangzQT1hc=",

"createTime": 1683953105421

}

],

"allocatedTransactionList": [],

"finishedTransactionList": []

}

}

调用:POST /createTransaction 创建交易：

{

"code": 200,

"msg": "操作成功",

"data": {

"hash": "3ab264eb22fa94d9dd3e7707cfa13936d1dbac45a51a408158b8c639f10e2c41",

"publicKey": "MFYwEAYHKoZIzj0CAQYFK4EEAAoDQgAEBqBPT3pqCj09O2NAGO50mrYnTKMg6CUAF+RGEUn79jUGip5q8NxSJJykFBOYg5Jl5N+5aaWHBuViGxyjYwfTHw==",

"transaction": {

"send": "1PqHV5LNUtHp91oKAAEeq8uFXSBY5A7Wn4",

"receive": "1CUpy3wC2wtvSPBWsR1hRSr6mUw8RdvoNj",

"amount": "10"

},

"sign": "MEUCIAwkjr8wTNzo0kgt2vdYSNbd/2bkkkKRiHWc/Z53Hi9vAiEAwH8HHJAre9LMIciuPKWFylMrkg0xsMe+KrangzQT1hc=",

"createTime": 1683953105421

}

}

中央节点的交易池如下：

中央节点随后需要从交易池的未分配队列中选取数条交易并从等待队列中选取一个节点赋予打包权。此时交易池状态如下，之前的交易已放入已分配队列。

{

"data": {

"transactionList": [],

"allocatedTransactionList": [

{

"transaction": {

"hash": "3ab264eb22fa94d9dd3e7707cfa13936d1dbac45a51a408158b8c639f10e2c41",

"publicKey": "MFYwEAYHKoZIzj0CAQYFK4EEAAoDQgAEBqBPT3pqCj09O2NAGO50mrYnTKMg6CUAF+RGEUn79jUGip5q8NxSJJykFBOYg5Jl5N+5aaWHBuViGxyjYwfTHw==",

"transaction": {

"send": "1PqHV5LNUtHp91oKAAEeq8uFXSBY5A7Wn4",

"receive": "1CUpy3wC2wtvSPBWsR1hRSr6mUw8RdvoNj",

"amount": "10"

},

"sign": "MEUCIAwkjr8wTNzo0kgt2vdYSNbd/2bkkkKRiHWc/Z53Hi9vAiEAwH8HHJAre9LMIciuPKWFylMrkg0xsMe+KrangzQT1hc=",

"createTime": 1683953105421

},

"minerAddr": "1PqHV5LNUtHp91oKAAEeq8uFXSBY5A7Wn4",

"finished": false,

"allocateTime": 1683954577192,

"finishTime": null,

"height": 1

}

],

"finishedTransactionList": []

}

}

随后矿工节点会接收到分配信息，并调整自己的本地交易池。如果检查到分配给自己的任务或手动调用挖矿接口，矿工就会开始打包操作，从已分配队列中选取分配给自己的交易打包成区块上传网络。首先需要向中央查询区块链预定id列表，获取前一个区块的id，查询结果如下：

{

"code": 200,

"msg": "操作成功",

"data": [

"0",

"e34495bc4fdfe603dfc313501fcbb26ff2ed0829fffba5766c44168fa6393699"

]

}

中央在每次分配任务时都会计算当前区块的id（id = hash(preId + merkle)），则矿工此次打包区块的preId = 0（前一个区块为创世区块）。

随后生成区块，查看中央节点的区块链如下，说明矿工此次打包成功：

{

"data": [

{

"height": 0,

"id": "0","preID": null,"merkle": null,"targetBits": 0,"nonce": null,"timestamp": 0,"body": null,"minerAddr": null

},

{

"height": 1,

"id": "e34495bc4fdfe603dfc313501fcbb26ff2ed0829fffba5766c44168fa6393699",

"preID": "0",

"merkle": "f3c018967a6847664c23058308e11b3528cb2b1ae859f2d726fb4932ecd75589",

"targetBits": 22,

"nonce": 964486,

"timestamp": 1683955889,

"body": [

{

"hash": "3ab264eb22fa94d9dd3e7707cfa13936d1dbac45a51a408158b8c639f10e2c41",

"publicKey": "MFYwEAYHKoZIzj0CAQYFK4EEAAoDQgAEBqBPT3pqCj09O2NAGO50mrYnTKMg6CUAF+RGEUn79jUGip5q8NxSJJykFBOYg5Jl5N+5aaWHBuViGxyjYwfTHw==",

"transaction": {

"send": "1PqHV5LNUtHp91oKAAEeq8uFXSBY5A7Wn4",

"receive": "1CUpy3wC2wtvSPBWsR1hRSr6mUw8RdvoNj",

"amount": "10"

},

"sign": "MEUCIAwkjr8wTNzo0kgt2vdYSNbd/2bkkkKRiHWc/Z53Hi9vAiEAwH8HHJAre9LMIciuPKWFylMrkg0xsMe+KrangzQT1hc=",

"createTime": 1683953105421

}

],

"minerAddr": "1PqHV5LNUtHp91oKAAEeq8uFXSBY5A7Wn4"

}

]

}

1. 多矿工节点并发打包

委派机制的一个重大创新就是多矿工节点的并发打包，以下是实验演示。

实验依然采用以上框架，分别用本机的8081、8082、8083，3个端口开启矿工节点服务，并向中央节点注册、申请排队。查询中央节点记录的节点信息如下：

{

"code": 200,

"msg": "操作成功",

"data": [

{

"addr": "1PqHV5LNUtHp91oKAAEeq8uFXSBY5A7Wn4",

"publicKey": "MFYwEAYHKoZIzj0CAQYFK4EEAAoDQgAEBqBPT3pqCj09O2NAGO50mrYnTKMg6CUAF+RGEUn79jUGip5q8NxSJJykFBOYg5Jl5N+5aaWHBuViGxyjYwfTHw==",

"privateKey": "MIGNAgEAMBAGByqGSM49AgEGBSuBBAAKBHYwdAIBAQQg9A6c6aOHstnnd6ISkMKtWEEch8Waeca5YfVMQ4ep+C2gBwYFK4EEAAqhRANCAAQGoE9PemoKPT07Y0AY7nSatidMoyDoJQAX5EYRSfv2NQaKnmrw3FIknKQUE5iDkmXk37lppYcG5WIbHKNjB9Mf",

"ip": "http://localhost:8081"

},

{

"addr": "1CUpy3wC2wtvSPBWsR1hRSr6mUw8RdvoNj",

"publicKey": "MFYwEAYHKoZIzj0CAQYFK4EEAAoDQgAE5JttSmU2+3JU6Kum+Sh+dR1++7zXitn/wiVYLh5hYzv/f1CBWbVkp/Av6Jxf+C7HlMlVCNSIoWGzMWeFlvYWFw==",

"privateKey": "MIGNAgEAMBAGByqGSM49AgEGBSuBBAAKBHYwdAIBAQQgMbTwZ5h/N8z5fLeUoBDL/pJgybtuFnH9UlzSzrzZoV+gBwYFK4EEAAqhRANCAATkm21KZTb7clToq6b5KH51HX77vNeK2f/CJVguHmFjO/9/UIFZtWSn8C/onF/4LseUyVUI1IihYbMxZ4WW9hYX",

"ip": "http://localhost:8082"

},

{

"addr": "13DyHJUj2F3UjVnCz6YMyz1QmkViWjGHFS",

"publicKey": "MFYwEAYHKoZIzj0CAQYFK4EEAAoDQgAE0RLUU7nkZtpRwHI4/ArUMVOpJZjSovXUPWKmQxibYtRrI4HzfdjScBsKMwWmJphsse0E95Xretyq6tlZaj6cTQ==",

"privateKey": "MIGNAgEAMBAGByqGSM49AgEGBSuBBAAKBHYwdAIBAQQgWNC3nM+CwxlR5QeYfmEtDhlT6zBI3gByNeQQwF3WkUugBwYFK4EEAAqhRANCAATREtRTueRm2lHAcjj8CtQxU6klmNKi9dQ9YqZDGJti1GsjgfN92NJwGwozBaYmmGyx7QT3let63Krq2VlqPpxN",

"ip": "http://localhost:8083"

}

]

}

随后创建数条交易，中央节点按排队顺序分配任务给矿工节点1，2，3。此时中央节点已经将所有待处理交易分配，矿工可以分别挖矿。为了展示并发效果，矿工节点服务不采用自动挖矿，而采用手动调用接口，让排在最后的节点3开始挖矿。结果如下所示：

{

"data": [

{

"id": "0",

"height": 0,"preID": null,"merkle": null,"targetBits": 0,"nonce": null,"timestamp": 0,"body": null,"minerAddr": null

},

null,

null,

{

"height": 3,

"id": "05b67fa9751df048674eec0576f6d26fcb8b056ac7d52f771e6399c019d2c7dd",

"preID": "d7d295229283feab43eb0708eb78e7b026e5ad9b21e3ffb87502ae3e337d9ded",

"merkle": "73d1c0434304ca9968aba016d894c288f797af6587ab3f92599d9d965c699e9e",

"targetBits": 22,

"nonce": 1423574,

"timestamp": 1683973466,

"body": [……],

"minerAddr": "13DyHJUj2F3UjVnCz6YMyz1QmkViWjGHFS"

}

]

}

可以看到，在前置区块未上链的情况下，height为3的区块依然可以成功上链。再验证height为2的区块：

"data": [

{

"id": "0",

"height": 0

},

null,

{

"height": 2,

"id": "d7d295229283feab43eb0708eb78e7b026e5ad9b21e3ffb87502ae3e337d9ded",

"preID": "01833f4c2bb9f856d13eca6bdb09adaecee4633fa1e6a70a132ed2b5fa1f6f1f",

……

"minerAddr": "1CUpy3wC2wtvSPBWsR1hRSr6mUw8RdvoNj"

},

{

"height": 3,

"id": "05b67fa9751df048674eec0576f6d26fcb8b056ac7d52f771e6399c019d2c7dd",

"preID": "d7d295229283feab43eb0708eb78e7b026e5ad9b21e3ffb87502ae3e337d9ded",

……

"minerAddr": "13DyHJUj2F3UjVnCz6YMyz1QmkViWjGHFS"

}

]

}

实验表明，区块2的id和区块3的preId相符合，乱序生成的区块链同样符合规定，说明委派机制下的区块链成功地实现了区块并发上链的功能。

1. 常规攻击防御演示

私链攻击：如果攻击节点没有遵循中央节点的分配私自打包，他发出的区块不会被其他节点所接受。以下为演示过程。

中央节点重置，攻击节点将之前测试中节点1打包的区块发送给中央节点

POST /addBlock 向中央节点发送区块

{

"height": 1,

"id": "7fe370c973810cead8755a5d4420d22f8601781c61cf53febb7a3ad1ee473516",

"preID": "0",

"merkle": "e179cd0130b33258cb77c89be758f5d6ceca062643085a78d8f48155a2264df7",

"targetBits": 22,

"nonce": 3333786,

"timestamp": 1683978302,

"body": ……

"minerAddr": "1PqHV5LNUtHp91oKAAEeq8uFXSBY5A7Wn4"

}

响应：

{

"code": 504,

"msg": "区块验证出错"

}

经上一个实验的检验，这个区块没有任何格式上的错误，传统区块链会接收该区块，但是委派机制下的区块链有特殊的验证机制，由于中央节点并未将相关交易分配给攻击节点，所以会响应区块验证出错，防止了私链攻击。

由于私链不被承认，则双花攻击也无法实施。

区块链节点检验区块正确性的流程有以下2步：

1. 检验区块结构是否合规。这一步与传统区块链的检验流程相同，需要检验区块是否含有必要的字段，区块体中的交易是否都有效（每一条交易都要检验其是否由发送方签名），merkle根是否正确，是否满足难度系数，id是否正确哈希。只有满足基本结构正确的区块才能进入下一步检验。
2. 检验区块体中的交易是否分配给了打包者。节点的交易池记录了已分配交易，检验区块时需要看区块体中的交易是否在已分配交易池中，并且区块的打包者必须是交易被委派者。

委派机制依靠第二步检验提高了区块链的安全性，同时几乎不影响性能。

“垃圾节点”攻击

如果等待队列中被注入了很多“垃圾节点”（指一些矿工节点，不响应中央节点的委派任务进行挖矿，仅占据等待队列中的位置），那么区块链可能存在长时间无法打包新区块的问题。

如果有一个节点被中央节点委派了打包任务，我们假设信息在网络中从一端到一端的传输时间都是T，那么从委派任务到中央节点收到区块的最短期望时间是2T（中央节点发送委派信息给矿工节点花费1T，矿工打包区块几乎不花费时间，矿工再把区块发送给中央节点花费时间T）。如果考虑到网络延迟等问题，中央节点收到新区块的时间可能为4T或者更多。

目前区块链采用超时重发的机制，如果我们将一个委派任务的最长完成时间设为T1，则中央节点在从委派任务开始过了T1后还没接收到目标区块的话，就会将之前委派的交易撤回，重新委派一位矿工打包。

T1需要根据网络情况设置成合适的时间。如果T1设置得太短，则有可能一个正常矿工节点打包的区块还在传输途中，中央节点却让该区块变得无效，频繁地撤销委派会让区块链的效率变得更低。如果T1设置得太长，则中央节点不能高效地委派任务。如果队列中有大量连续垃圾节点存在时，中央节点需要一个一个地选取节点并等待T1长的时间，可能一个打包任务被委派好几次都不会被成功处理。

目前系统仍没有一个能防止垃圾节点攻击的方法。这个问题是传统区块链中所没有的，传统区块链中即使有节点不“挖矿”，但总有节点在正常工作，这也是矿工之间竞争的好处。但在委派机制中，如果被委派的矿工不工作，则没有其他矿工及时地替补他的工作。

# 总结与展望

本片论文分析了区块链技术的底层原理和优缺点，综述了区块链技术在数字金融中的应用场景和应用现状，分析了区块链技术对数字金融发展起到的推动作用，以及区块链技术现有的瓶颈。论文针对区块链现有的效率低、速度慢，无法应用到数字货币日常支付领域的问题提出了一种解决方案，即提出了一种创新的区块链共识机制——委派机制。该机制与传统的POW，POS机制不同，主要优势在于不需要花费算力计算数学难题、且实现区块间并行计算，可以极大地提升区块链的效率。如果将该机制应用到数字货币领域中，可以实现快速的日常零售支付，且拥有较强的抗压能力，可以处理较大的信息流量。

论文利用java SpringBoot框架编写了委派机制区块链的仿真模型进行实验，实现了委派机制设想的基本功能，且进行了相应功能演示；并且实验测试了针对委派机制区块链的私链攻击，虚假信息攻击，发现均能抵抗。实验结果表明，委派机制下的区块链数字货币拥有较快的确认速度和较高的安全性，可以满足日常支付电子货币的使用，突破了传统区块链电子货币所不能应用的领域。

但委派机制仍存在一定问题，比如单点失效问题，如果系统的矿工等待队列中存在大量“垃圾节点”，被委派的任务将迟迟无法完成，将造成较大的时延。且创建一个数字货币账户的成本很低，无法追溯到个人，识别垃圾节点也比较困难。

而且当网络中的节点过多时还可能存在信息传输量过大导致的网络问题。以及当区块链过长时用户账本的余额查询耗时较长的问题。

笔者对于委派机制还有以下展望：

1. 寻找识别垃圾节点的解决方案。如果系统能够减少矿工中的垃圾节点，那么将提升系统的效率，降低被攻击的损失。可以从以下几个角度寻找解决方案：增加矿工节点排队的成本，矿工节点在打包前需要向系统质押一定金额，成功打包后才返还；注册矿工节点时增加资质审核，避免攻击者批量注册太多账户。
2. 优化网络方案。实验中采用了http协议来传输数据，在实际应用中可能会有较大延时，可以设计一套专用的网络传输方案，底层采用UDP类的快速的网络协议，实现成本更低、速度更快的网络传输方式。

数字货币是一个颇有前景的领域，数字货币的推广有利于货币流通，节约交易成本，增加交易安全性。本文的委派机制算法仅作为一个创新的思路，系统完备性仍未经过严格检验，或许存在其他未发现的问题。

笔者希望本文的委派机制可以为成熟数字货币的研发提供灵感和思路，早日研发出兼具效率和安全性的数字货币系统。

**参考文献**

1. Bitcoin: A Peer-to-Peer Electronic Cash System[J]. Social Science Electronic Publishing.
2. 韩梅.数字金融发展的现状分析[J].经济研究导刊,2022(11):113-115.
3. 左晓静,徐晨莉,王荣.区块链原理及核心技术分析[J].计算机产品与流通,2019(03):85.
4. 陈思晶. 数字金融发展与收入分配[D].浙江大学,2021.DOI:10.27461/d.cnki.gzjdx.2021.001057.
5. 袁勇,王飞跃.区块链技术发展现状与展望[J].自动化学报,2016,42(04):481-494.DOI:10.16383/j.aas.2016.c160158.
6. 唐萌萌.区块链技术在供应链管理中的应用[J].中国储运,2023,No.271(04):204-205.DOI:10.16301/j.cnki.cn12-1204/f.2023.04.05
7. Lin, Shi Yi,Zhang, Lei,Li, Jing,Ji, Li li,Sun, Yue. A survey of application research based on blockchain smart contract[J]. Wireless Networks,2022(prepublish).
8. 沈蒙,车征,祝烈煌等.区块链数字货币交易的匿名性：保护与对抗[J].计算机学报,2023,46(01):125-146.
9. Lv Yarong. Data privacy protection based on homomorphic encryption[J]. Journal of Physics: Conference Series,2021,2037(1).
10. 赵越强,徐迎迎,李小平等.多边央行数字货币安排:发展动因、运行机制与应用前景[J].国际贸易,2023,No.496(04):81-88.DOI:10.14114/j.cnki.itrade.2023.04.012.
11. Ren Xiaohang,Zeng Gudian,Zhao Yang. Digital finance and corporate ESG performance: Empirical evidence from listed companies in China[J]. Pacific-Basin Finance Journal,2023,79.

**致谢**

在完成这篇论文的过程中，我要向许多人表达我衷心的感谢。

我要感谢我的父母，在我成长过程中对我的支持，你们的无私奉献和信任是我坚持学业的动力和力量源泉。我要感谢我的每一位老师和朋友们，感谢你们对我学业和生活上的帮助，为我解答学习研究上的疑惑。此外，我要感谢学校为我提供的学术资源和学习环境，让我度过了一个充实而舒适的大学生活。

再次向所有给予帮助和支持的人表示衷心的感谢。你们的贡献对我来说是无价之宝。

致以最诚挚的谢意。