学校代码 10530　　学　　号 201721562049
分 类 号 TP391　　密　　级 公开

湘潭大学

硕 士 学 位 论 文

高并发区块链架构及其在数字彩票系统中的应用研究

学 位 申 请 人 李 聪
指 导 教 师 刘新　副教授
学 院 名 称 计算机学院·网络空间安全学院
学 科 专 业 计算机技术
研 究 方 向 智能信息处理技术

二〇二〇 年 七 月 三十 日

Highly Concurrent Blockchain Architecture and Its Application Research in Digital Lottery System

Candidate Li Cong

Supervisor Prof. Liu Xin

College College of Computer Science& College of Cyberspace Security

Program Computer Technology

Degree Master of Engineering

University Xiangtan University

Date Jul.30th 2020

湘潭大学

学位论文原创性声明

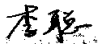
本人郑重声明：所呈交的论文是本人在导师的指导下独立进行研究所取得的研究成果。除了文中特别加以标注引用的内容外，本论文不包含任何其他个人或集体已经发表或撰写的成果作品。对本文的研究做出重要贡献的个人和集体，均已在文中以明确方式标明。本人完全意识到本声明的法律后果由本人承担。

作者签名：  日期： 2020 年 8 月 8 日

学位论文版权使用授权书

本学位论文作者完全了解学校有关保留、使用学位论文的规定，同意学校保留并向国家有关部门或机构送交论文的复印件和电子版，允许论文被查阅和借阅。本人授权湘潭大学可以将本学位论文的全部或部分内容编入有关数据库进行检索，可以采用影印、缩印或扫描等复制手段保存和汇编本学位论文。

涉密论文按学校规定处理。

作者签名：  日期：2020 年 8 月 8 日

导师签名：  日期：2020 年 8 月 8 日

摘 要

随着互联网信息技术的快速发展，价值的传递方式也在不断改变，经历了从纸币到移动支付为主的电子货币。互联网的发展虽然做到了让货币以数字的形式流通，但都依赖于第三方机构，从而就会产生依赖第三方的信任问题。区块链技术的迅速发展，为第三方信任依赖问题提供了新的解决方案。区块链最大的特点就是“去中心化”和“安全透明”，在区块链技术的基础上已经有了很多成功的应用和开发平台。区块链技术不仅适用于电子货币，而且适用于社会各行业的商业场景。

区块链技术的研究和基于高并发区块链架构的项目都处于快速发展的阶段。区块链技术能高效的解决很多行业的痛点。当前，区块链技术的发展与进步主要集中在应用层和共识层。通过对区块链应用层的改进，使区块链技术应用于不同的商业场景；通过对区块链共识层的改进，提高了区块链的并发能力和减少了能源消耗。本文的研究方向是通过对区块链技术的分析以及对当前基于高并发区块链架构的项目的缺陷进行对比，提出自己的改进方案。

本文介绍了区块链的发展历程以及发展历程中具有代表性的区块链应用，介绍了构建区块链的相关技术——分布式存储、加密算法、共识机制以及智能合约。本文介绍了构建高并发区块链架构的难点，介绍了基于 DAG 的高并发区块链——主要包括增强的有向无环图；增强 DAG 共识和公证人选择的 BA-VRF 共识机制的双层共识机制；同构多链架构。

本文研究了基于可延时验证的高并发区块链系统，提出了利用超级节点验证交易信息来提高交易确认速度。在区块链中超级节点不作为唯一的验证中心，普通节点通过随机抽样方式与超级节点共同参与验证交易信息。交易信息在验证出错的情况下由普通节点提出全网共识验证，既保证了交易的安全性又提高了区块链的吞吐量。通过与基于 DAG 的区块链项目的实验数据对比，验证了本方法的可行性。

在高并发区块链架构的基础上设计了一套完整的数字彩票发行系统方案。在中国，发行彩票必须通过民政部门的彩票中心，我们不可能设计一种完全无中心化的区块链来应用到彩票系统上。本文研究的可延时验证的高并发区块链架构存在超级节点可作为彩票中心，并且超级节点可提高彩票系统的并发量，但是超级节点的加入增加了作恶的可能性。本文设计了一种延时验证的方法来防止超级节点的作恶。具体来说，首先通过随机抽样方式抽取普通彩民节点与超级节点共同参与验证购买彩票信息，防止了超级节点的完全中心化；同时在验证出现错误时，

彩票系统针对出错的情况提出全网共识，保证了购买彩票信息的安全性和一致性。基于可延时验证区块链的数字彩票系统根据区块链的特性改造了现有彩票系统的发行流程，并设计了一套完全随机的中奖号码产生算法。该方案包括彩票中心在内的任何机构或个人都无法控制开奖与中奖过程，中奖结果对所有人都公开可查，同时又保护了用户隐私，大大提高了数字彩票发行的可信度。
关键字：区块链；高并发；延时验证；彩票系统

Abstract

With the rapid development of Internet information technology, the way in which value is transferred is also constantly changing, going from paper money to mobile payment-based electronic money. Although the development of the Internet has enabled currency to be circulated in the form of numbers, they all rely on third-party institutions, which may cause trust problems depending on third parties. The rapid development of blockchain technology provides a new solution to the problem of third-party trust dependence. The biggest feature of blockchain is "decentralization" and "security and transparency", and there have been many successful applications and development platforms based on blockchain technology. Blockchain technology is not only applicable to electronic currency, but also applicable to business scenarios in various industries in society.

The research of blockchain technology and projects based on highly concurrent blockchain architecture are in a stage of rapid development. Blockchain technology can effectively solve the pain points of many industries. At present, the development and progress of blockchain technology are mainly concentrated on the application layer and the consensus layer. Through the improvement of the blockchain application layer, the blockchain technology is applied to different business scenarios; through the improvement of the blockchain consensus layer, the concurrency of the blockchain is improved and the energy consumption is reduced. The research direction of this article is to analyze the blockchain technology and compare the shortcomings of current projects based on highly concurrent blockchain architecture, and propose their own improvement plans.

This article introduces the development process of the blockchain and the representative blockchain applications in the development process, and introduces the relevant technologies for building the blockchain-distributed storage, encryption algorithms, consensus mechanisms and smart contracts. This article introduces the difficulties of building a high-concurrency blockchain architecture, and introduces a high-concurrency blockchain based on DAG-mainly including an enhanced directed acyclic graph; enhancing the duality of DAG consensus and the BA-VRF consensus mechanism selected by a notary Layer consensus mechanism; homogeneous multi-chain architecture.

This paper studies a highly concurrent blockchain system based on delayable verification, and proposes to use super nodes to verify transaction information to improve the speed of transaction confirmation. Super nodes do not act as the only verification center, ordinary nodes participate in verification transaction information with super nodes through random sampling. When the transaction information is verified incorrectly, the common node proposes a network-wide consensus verification, which not only ensures the security of the transaction but also improves the throughput of the blockchain. The feasibility of this method was verified by comparison with experimental data of DAG-based blockchain projects.

Based on the high-concurrency blockchain architecture, a complete digital lottery issuance system is designed. In China, the issuance of lottery tickets must go through the lottery center of the civil affairs department. It is impossible for us to design a completely decentralized blockchain to apply to the lottery system. The high-concurrency blockchain architecture studied in this paper has super nodes that can be used as lottery centers, and super nodes can increase the concurrency of the lottery system, but the addition of super nodes increases the possibility of evil. This paper designs a delayed verification method to prevent super nodes from doing evil. Specifically, firstly, common lottery nodes and super nodes are randomly selected to participate in the verification of the purchase of lottery information, which prevents the complete centralization of the super nodes; at the same time, when there is an error in the verification, the lottery system proposes a network-wide consensus for the error. Ensure the security and consistency of purchasing lottery information. The digital lottery system based on the blockchain that can be verified with delay has transformed the issuance process of the existing lottery system according to the characteristics of the blockchain, and designed a completely random winning number generation algorithm. This solution, including the lottery center, cannot control the lottery draw and winning process. The winning results are publicly available to everyone, while protecting user privacy and greatly improving the credibility of digital lottery issuance.

Keywords： Blockchain; high concurrency; delayed verification; lottery system

目录

第1章 绪论

1.1 研究背景及意义

近年来随着互联网信息技术的发展，价值的传递方式也在不断改变。价值的传递方式经历了从纸币到移动支付为主的电子货币。互联网的发展提高了信息的传输效率，在整个网络中点对点的传输高效且廉价。然而，对于信息传输可靠性的保护却存在很多问题，在网上复制和篡改一些信息的成本几乎为零。传统互联网无法保证点对点传递带有所有权信息的可靠性。互联网的发展虽然做到了让货币以数字的形式流通，但是都依赖第三方机构，会产生第三方的信任问题，同时也提高了交易成本。

区块链技术就是在这样的背景下诞生的。信息和价值是不可分割的，利用区块链技术在互联网中进行信息传输时，能够确保有价值的信息被可靠地传输。区块链技术的核心是建立了一个独立于第三方的可信网络。互联网具有信息传递功能，区块链技术能确保在信息传递中价值的可靠性。区块链技术通过特殊的数据结构和加密算法来保证数据的不可篡改，通过共识算法来达到去中心化的目的。

区块链技术具有去中心化和安全的特性，这使得它非常适用于涉及多方间安全的场景、需要获取真实性信息的企业以及基于分布式的市场商业新模型。在物联网中，随着新的分布式经济模型的普及，覆盖着数以亿计的机器，机器之间会涉及大量的交易情况，安全、分布式的交易模型就显得极其重要，区块链对于处理这种分布式交易情况高效且安全。区块链技术也适用于解决金融业的问题，金融业的核心之一是风险评估，获得的真实信息越多，风险就会越低。目前，跨境支付都是由第三方机构完成清算支付，这同时也将存在信息同步时差，并且成本将非常高。通过区块链技术应用的分布式数据库和一致性账本可以实现即时清算。区块链适用于各种各样的场景和行业，并不局限于各种代币，区块链在未来还将有更大的发展空间。

1.2 国内外研究现状

2008 年，一位化名“中本聪”的学者发表了一篇题为《比特币：一种点对点电子现金系统》的论文[1]，并在该论文基础上创建了比特币，从而产生了区块链技术。目前，区块链技术的发展经历了三个重要过程。区块链 1.0 是一种用来建立加密账户和进行数字支付的货币，它具有去中心化、数据不可篡改、不可伪造、可追溯等特点。区块链 1.0 的主要代表是比特币，它是目前最成功的区块链应用

程序，它通过分布式和分散的数据库分散存储货币、金融交易、数据和信息，并通过分布式和分散的数据库存储信息。区块链 1.0 不需要可信的第三方，如银行或其他金融机构，来验证金融交易。区块链 2.0 在区块链 1.0 的基础上增加了智能合约，采用了不同的共识机制。智能合约是在满足某些条件时自动运行得到结果的函数方法。区块链 2.0 的主要代表是 ethereum，所有人可以在 ethereum 平台上开发其他区块链应用程序。在 ethereum 平台，每秒交易量相较于比特币有很大的提高。区块链发 3.0 的主要代表是 EOS，其目标是为各行各业提供去中心化的解决方案，包括通过区块链进行资历认证、数据存储、产权的确认等[2]。

区块链 1.0 到 3.0 都是对应用层或者共识层进行改进，目前也出现了很多对区块链底层的研究，其中被研究的最多的就是基于 DAG 的区块链架构。DAG 即有向无环图，在基于 DAG 的区块链中，没有区块的概念，通过所有的交易组成一个有向无环图。具体来说，在基于 DAG 的区块链中，要验证新的交易前，必须直接验证之前的两个交易，这也使得在这两个交易之前所有被验证过的交易得到间接验证。通过 DAG 的拓扑结构来存储区块，可以解决区块链的效率问题。区块链只有一条单链，打包出块无法并发执行。如果将区块的链式存储结构变成 DAG 的网状拓扑，则可以并行写入。在区块打包时间不变的情况下，网络中可以并行打包 N 个区块，网络中的交易就可以容纳 N 倍[3]。

当前，许多国家和地区都将区块链作为发展战略，区块链也日益受到国内各级政府的重视和关注。国际上关于区块链的研究与应用表现出联盟化、金融级、全盘布局的特点。主要参与对象既有大型商业银行、银行卡组织，也有科技公司、咨询公司，意在对金融基础设施进行优化和重构。金融机构通过与区块链科技公司合作，协助业务设计和开发。瑞士银行、德意志银行、桑坦德银行、纽约梅隆银行和 ICAP 宣布与区块链企业 Clearmatics 共同发行基于区块链技术的新型“Utility Settlement Coin”(USC 代币)，用于金融市场交易结算及清算过程，希望有效减少支付清算成本、加快清算速度、保证资金安全;三菱东京日联银行与 IBM 进行区块链合同管理试验，利用区块链技术开展与合作伙伴签署合同时的设计、运营和执行;富国银行与澳新银行合作开发区块链平台，以创建和共享大量关系银行账户，提高跨境关系银行的支付和结算速度。目前国内也有越来越多的产业机构开始重视并参与到区块链技术和应用的探索中来，推动区块链应用从单一的数字资产应用，延伸拓展到供应链管理[4]、物流[5]、信息安全[7]、跨境电商[19]、物联网[24]、医疗[37]、版权保护[44]、教育就业[47]等经济社会的多个领域，推动区块链生态加速形成。目前，区块链也成为产学各界探讨的对象。区块链不仅是一项技术，更是一种社会问题的解决方案[52]。随着区块链在实体经济中越来越多的应用，利用区块链技术服务实体经济已经成为社会的共识。

1.3 主要内容和创新点

本文在进行了大量的资料查询和文献阅读，并对目前已经落地的一些区块链应用进行了研究之后，阐述了区块链的关键技术及发展难点，并针对区块链技术中急需解决的问题提出了自己的解决方案。本文主要研究内容包括区块链的一些关键技术、如何实现高并发的区块链架构以及具体的区块链应用实现

本文设计了基于可延时验证的高并发区块链系统。在区块链中采用超级节点来提高验证交易的速度。普通节点的交易信息在验证出错的情况下，可以延时提出全网共识，通过全网共识来保证每笔交易的安全性。

本文设计了一个具体的区块链应用系统，即一个基于高并发区块链的数字彩票发行系统。基于可延时验证区块链的数字彩票系统通过加入超级节点可以提高并发量，而且法律规定福彩中心要能主导彩票发行事业，还要从中提取费用作为残疾人的福利，所以彩票发行系统中必须有超级节点的存在。但是另外一方面加入超级节点就容易作恶。本文设计了一种延时验证的方法来防止超级节点的作恶。具体来说，首先通过随机抽样方式抽取普通彩民节点与超级节点共同参与验证购买彩票信息，防止了超级节点的完全中心化；同时在验证出现错误时，彩票系统针对出错的情况提出全网共识，保证了购买彩票信息的安全性和一致性。整个彩票系统的运作流程是：首先是彩票普通节点购买彩票数字并向全网广播购买信息；彩票普通节点随机抽样参与验证的普通节点；然后直接通过抽样的普通节点与管理员超级节点共同验证购买信息来提高验证速度和吞吐量；当验证出现错误时，普通节点可以提出全网共识，以保证购买信息的安全性；最后通过智能合约实现随机选择开奖号码和自动派奖，以保证彩票系统的公开透明。

主要创新点如下：

1. 本文设计了一种带有超级节点的高并发区块链架构。在区块链中超级节点不作为唯一的验证中心，普通节点通过随机抽样方式与超级节点共同参与验证交易信息。交易信息在验证出错的情况下由普通节点提出全网共识验证，既保证了交易的安全性又提高了区块链的吞吐量。

2. 本文在高并发区块链架构的基础上设计了一套完整的数字彩票发行系统方案。基于可延时验证区块链的彩票系统根据区块链的特性改造了现有彩票系统的发行流程，并设计了一套完全随机的中奖号码产生算法。该方案包括彩票中心在内的任何机构或个人都无法控制开奖与中奖过程，中奖结果对所有人都公开可查，同时又保护了用户隐私，大大提高了数字彩票发行的可信度。

1.4 论文组织结构

第 1 章主要介绍了区块链的产生背景和研究意义。进一步介绍了区块链的发

展现状，以及本文的研究内容和组织结构。

第 2 章主要是区块链中使用的技术介绍。首先是分布式存储的介绍，包括 P2P 存储、分布式和分布式账本。然后介绍了加密算法，主要包括两类，哈希算法和非对称加密技术。然后，介绍了区块链常见的一致性共识机制。最后，介绍了区块链的智能合约。

第 3 章主要介绍了目前区块链发展过程中的难点，介绍了基于 DAG 的区块链架构——主要包括有向无环图，双层共识机制和同构多链。介绍了本文设计的基于可延时验证的高并发区块链系统，通过区块链中的超级节点以及抽样的普通节点进行验证来提高确认速度，并且在出错的情况下，普通节点可以发起全网共识，保证普通节点交易的不可篡改。本章还进行了基于 DAG 的区块链项目和基于可延时验证的区块链系统的实验对比。

第 4 章主要介绍了区块链技术实现的具体应用——基于高并发区块链的数字彩票发行系统。详细介绍了目前传统互联网彩票系统的一些弊端，基于高并发区块链的数字彩票发行系统的分层结构、关键技术以及需求和架构设计，最后还给出了基于高并发区块链的数字彩票发行系统的软件设计和具体实现，包括一些实现难点和具体功能模块展示。

第 5 章总结了本文主要的研究内容——可延时验证的高并发区块链架构，还总结了基于高并发区块链的数字彩票发行系统的研究内容。并就区块链技术的发展及今后将涉及到哪些领域，提出了自己的看法和展望。

第2章 相关技术的研究

2.1 分布式存储

传统的互联网采用的是集中式存储，把数据存储在一台足够大的服务器上。部署的方式简单，部署一个服务节点即可，维护起来也很方便。因为它将所有数据保存在同一台服务器上，所以对数据的操作就变得简单了，例如存取。随着互联网的发展，移动互联网的兴起，主机数据和计算量越来越大，用户的并发访问也越来越多，那么在单一的大型主机服务器上进行扩容是非常难的，还存在严重的单点故障问题。目前大型企业基本都会部署多台服务器，部署的成本也非常高。在节约成本方面，区块链的分布式存储有着巨大的优势[48]。

区块链由多个区块连接而成，一个完整的区块包括作为区块分隔符的神奇数，区块大小，区块头，交易列表以及交易数。具体如下表 2-1 所示：

表 2-1 区块链的区块

字段	字节	说明
神奇数		0xD8B4AEF，作为区块的分隔符
Block Size	4	区块大小为 4 字节
Block Header	80	区块头
Transactions Counter	1-9	记录区块的交易数量
Transactions	m*n(n>=250)	交易列表

区块链的分布式存储是将数据分成很多块，每个块的数据都记录在区块链上，这样可以防止被修改，我们在区块链上读取数据时就是读取每一个块的数据，然后拼接成完整的数据。区块链分布式存储采用全网络节点共同参与数据的存储，每个节点都是对等的，没有中心机构的控制，每个节点都保存了完整的数据账本，整个区块链共用一个账本来保证数据的可靠性[13]。区块链存储是将数据同步到全网节点，所有节点都参与数据的维护，这样还可以降低数据维护的难度。

分布式存储的相关关键点介绍：

1、 P2P 存储

P2P 存储是区块链中节点对等，不存在控制节点的一种存储方式。P2P 存储开放了存储空间，提高了网络的运作效率，可以解决传统分布式存储的服务器瓶颈和带宽问题[31]。

2、 分布式

分布式是通过区块链的 P2P 实现的。区块链的分布式是描述一个计算机系统具有在多台计算机上同时运行和维护的完整副本，没有任何中心化第三方机构来控制这个系统[10]。

3、 分布式账本

整个区块链网络都可以获取完整的相同账本，每个节点可以从其他节点获取账本的数据库[25]。区块链中的节点都可以获得唯一且完整的副本，所以这个账本是难以进行篡改的，同时也就保证了分布式账本的安全性。

2.2 加密算法

区块链底层的实现离不开加密算法，区块链的核心是去中心化和安全透明，所有相互不信任的节点都必须在加密算法下保证数据的不可修改性[32]。区块链用到的密码学算法有两大类算法：哈希算法和非对称加密算法。

2.2.1 哈希算法

哈希算法是区块链中用的最多的一类算法，它主要用于构建区块链和确认交易的完整性[22]。哈希算法是一类数学函数算法，也被称为散列函数。哈希函数一般是输入任意的字符串，由确定的哈希函数产生固定的输出，并能在较快的有效时间内得到输出[11]。哈希算法在区块链中要达到密码学安全还要求具备三个条件，一是要有碰撞阻力，即保证不同的输入会产生不同的输出，二是要有不可逆性，在哈希函数 y=Has(x)中可以通过输入 x 得到输出 y，但无法通过输出 y 推出输入 x，三是对于算法中 y=Hash(x)在已知 y 的情况下只能通过暴力枚举的方式不断尝试得到 x。

区块链中常用的哈希函数是 SHA256。SHA256 是一种安全散列函数，对于任意长度的消息，SHA256 都会产生一个 256 位的 hash 值，将这个 hash 值作为消息摘要。SHA256 哈希计算前要进行两个步骤[27]：

1. 对消息进行补位处理，保证最终的长度为 512 位的倍数
2. 以 512 位为单位对消息进行分块为 $M^{(1)}$,$M^{(2)}$,….$M^{(N)}$

SHA256 的压缩函数对 512 位的消息区块和 256 位的中间哈希值进行操作，本质上，它是一个通过将消息区块作为密钥对中间哈希值进行加密的 256 位加密算法。

2.2.2 非对称加密算法

对称加密技术只有一个密钥，用这个密钥加密的同时也用它解密。非对称加密技术的密钥有公钥和私钥之分，公钥对所有人可见，私钥单独由每个使用

者保存[40]。使用公钥加密只能由私钥解密，使用私钥加密也只能由公钥解密。非对称加密是区块链技术中很重要的一个部分，区块链的每个节点都保存一对密钥，公钥公开所有用户可见，私钥由每个区块链节点单独保存。在比特币中就是每个用户一对密钥，使用公钥作为交易账户。

应用于区块链中的非对称加密算法有很多种，主要有 RSA、ECDSA 等，在比特币中使用的就是 ECDSA 算法。

RSA 算法步骤如下[55]：

1. 任意选取两个大质数 P 和 Q 计算它们的乘积 n= P* Q，以及计算 n 的欧拉函数$\varphi(n)$（欧拉函数是指从 1 到 n 之间与 n 互质的个数），即$m = \varphi(n) = (P-1)*(Q-1)$
2. 随机取一个大整数 e 在 1<e<m 之间，且 e 满足条件gcd $(e，\varphi(n)) = 1$, 整数 e 作为加密密钥
3. 确定解密密钥 d，解密密钥 d 满足$(e*d)modm = 1$
4. 将整数 n 和 e 公开，秘密保存 d
5. 将明文 data 加密成密文 c 的过程$c = data^e modn$
6. 将密文 c 解密成明文 data 的过程$data = c^d modn$

RSA 算法中将整数 n 和 e 作为公钥，n 和 d 作为私钥。

ECDSA 算法是基于椭圆曲线建立的加密机制。首先需要定义椭圆上的运算规则[41]：

1、 加法：过椭圆两点 K 与 T 的一条直线与椭圆相交于 P，则交点 P 关于 X 轴对称的 P’点就是定义 K+T 的加法：K+T=P’。如下图 2-1 所示：

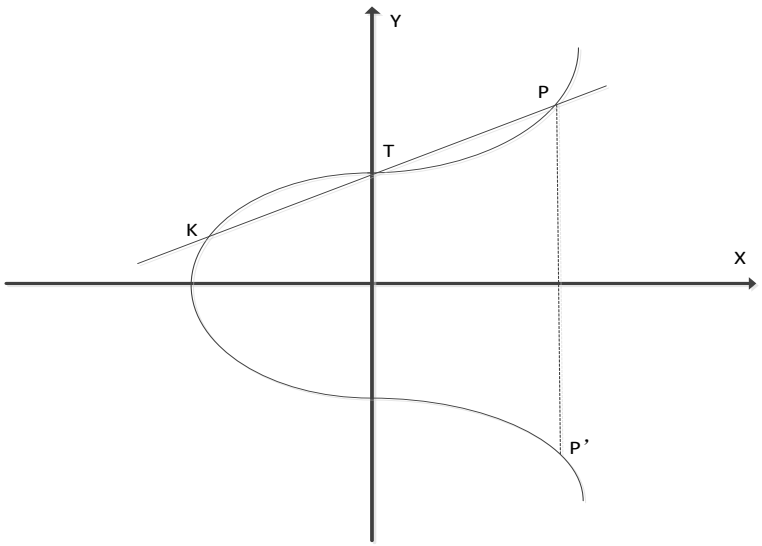


图 2-1 椭圆曲线加法

2、 二倍运算：加法规则无法解释 K 点与 T 点重合的情况即 K+K。所以在这

种情况下就是过椭圆的切点 K 的一条直线与椭圆相交于 P 点，则交点 P 关于 X 轴对称的 P’点就是定义 K+T 的二倍运算：K+K=2K=P’。如下图 2-2 所示：

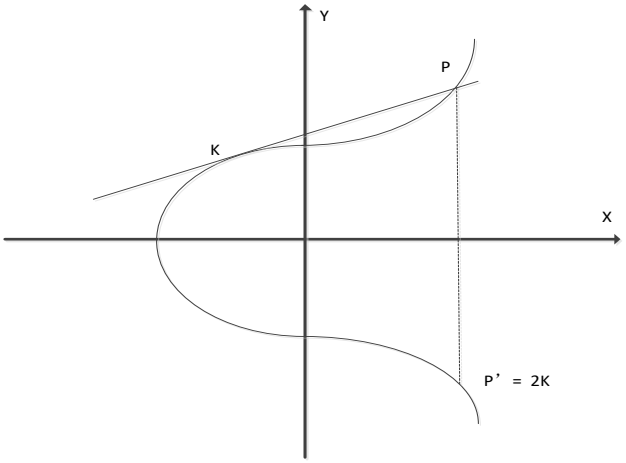


图 2-2 椭圆二倍运算

3、 正负取反：正负取反运算就是 K 点关于 X 轴对称的-K 点。如下图 2-3 所示：

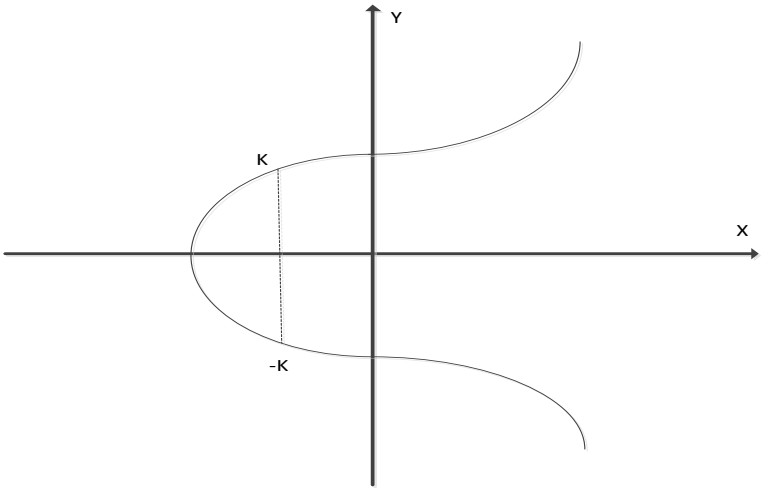


图 2-3 椭圆曲线的正负取反

4、 无穷远点：无穷远点是 K 与-K 相加，则过 K 与-K 的直线与 Y 轴平行，则可认为直线与 Y 轴相交于无穷远点。如下图 2-4 所示：

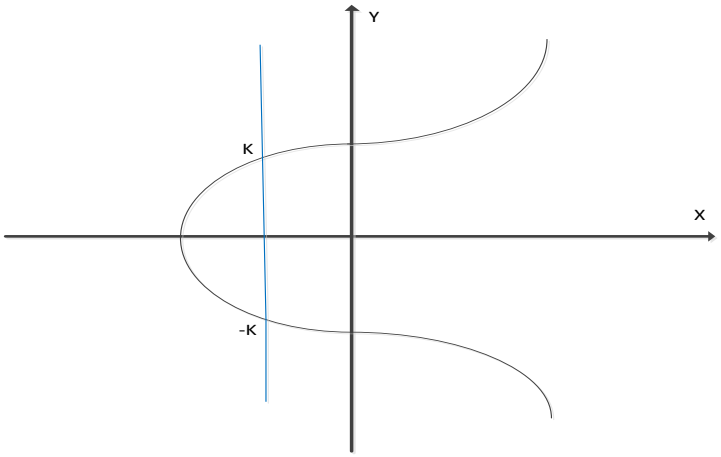


图 2-4 椭圆曲线的无穷远点

由以上定义的规则，对于某一椭圆上的点 R，可以利用运算规则算出 2R、3R（R+2R）、4R……等等，所以可以得出已知 R，当给定 x，求 xR 可以利用运算规则算出，而已知 xR，求 x 就会变得非常困难，这是非常符合非对称加密技术的，因此可以将 x 设为私钥，xR 设为公钥。

2.3 区块链的交易过程

区块链中的交易通过转账的方式实现，具体的交易流程如下用户 1 将代币支付给用户 2：

1、 用户 1 写好交易信息：data。

2、 用户 1 使用哈希函数将交易信息 data 进行计算得到哈希值 V=Hash(data)，然后再使用保存的私钥签名得到 Sign(V)，用私钥进行签名主要防止交易信息被篡改。

3、 通过区块链的网络将签名 Sign(V)和交易信息传递给用户 2。

4、 用户 2 通过用户 1 公开的公钥来对 Sign(V)进行解密，得到哈希值 V。

5、 用户 2 还需要通过哈希函数对交易信息 data 进行计算得到 V2=Hash(data)。

6、 对比两个哈希值，如果得到 V==V2，则交易信息没有问题。同时也证明用户 1 使用了自己的私钥进行签名，则可以开始这次交易。

7、 整个区块链中的所有节点都可以通过上述步骤进行验证。

2.4 共识机制

区块链是一种分布式系统，不同的节点间通过异步通信的方式构成了区块网络。如何达成共识是区块链的核心[26]。一种良好的共识机制能够提高系统性能，

推动区块链技术的应用[42]。在区块链网络中，为了保证各节点对交易数据达成一致的状态共识，需要在节点之间进行状态复制。区块链网络的运行需要定义默认的容错协议，以保证各节点安全可靠地达成状态共识，共识机制正是为了实现这一目标。共识机制用于保证由区块链中的每个节点生成的每笔交易都是一致和正确的[33]。区块链的核心是共识机制，它保证了区块链在不依赖第三方的基础上仍然能够有效地运行整个区块链网络。目前在区块链应用中常用的共识机制有工作量证明、权益证明、委托权益证明、实用的拜占庭容错算法，以及验证池共识机制。

2.4.1 工作量证明

工作量证明是指耗费计算机的算力来完成一定的工作量，在比特币中由最先完成工作量的节点来获取奖励[20]。在比特币区块链网络中，工作量证明是每个节点都致力于解决一个一定难度的难题。工作量证明在比特币中又称为挖矿，挖矿挖的是比特币中的每一个区块。每个区块都通过交易、时间和一个自定义的数值这三个条件来计算 Hash。规则就是这个区块的哈希值必须满足前导位有 N 位为零，这需要不停地尝试修改自定义的这个值来完成这个工作量。显然可知，零的个数越多，则算出这个 Hash 的难度越高。寻找的是一个 hash 值，这是一个概率问题，所以无法确切知道进行尝试的计算次数。存在有节点提供一个符合条件的区块，则表明这个节点进行了大量的工作量尝试，即此节点的工作量证明。这种共识机制虽然在比特币中验证了它的可靠性，但是对算力要求极高，同时也会造成资源的损耗。

2.4.2 权益证明

工作量证明存在节点之间的相互竞争，对于资源极其浪费，权益证明是为了解决这一问题而提出的。权益证明是通过选举的方式选择任意的节点来验证区块。权益证明中没有挖矿的矿工，只有验证者[8]。验证者不是完全随机选取的，是根据节点持有的数字货币的量和时间，得到一个币龄值，币龄值大小决定了被选为验证者的几率。验证者在被选取后生成新区块，同时被选取的验证者节点的币龄就会请零，避免形成一种第三方垄断的情况。在权益证明中币龄越大，被选中的概率也就越大。

2.4.3 委托权益证明

权益证明在效率方面也有自身的缺陷，委托权益证明对于效率有很大的提升。委托权益证明是让每一个持有股份的人进行投票得到固定数量的代表，这些代表作为区块链网络中的超级节点，并且这些超级节点的权利是完全相等的，新区块

的生成由这些节点轮流控制[9]。如果这些节点没有在需要他们生成新区块的时候生成新区块，就会对这些节点进行除名，再选择出新的超级节点。

2.4.4 实用拜占庭容错算法

拜占庭容错算法是很早就提出的一类分布式容错算法，实用拜占庭容错算法是这种分布式算法的一种具体实现[36]。实用拜占庭容错算法是状态机利用副本来复制的一种算法，每个服务都是状态机，在分布式系统中将此状态机在每个节点之间进行副本复制[35]。假设所有节点的状态机副本为集合 R，则一共有 0 到 R-1 个副本，用 0 到 R-1 整数表示这些副本。设 R=3f+1，f 表示可能失效的最大副本数。实用拜占庭容错算法分为三个阶段，预准备阶段，准备阶段，确认阶段。预准备阶段主要是确认同一次请求中包含的信息被其他副本节点确认的序列。准备阶段和确认阶段是保证那些请求中以及被确认的信息在发生更改后依然能保持原有的序列。具体的过程如下：

1) 在集合中取一个作为主节点，其他都作为备份
2) 用户发送服务请求到主节点
3) 主节点发送请求给其他所有节点
4) 所有副本执行请求并返回结果给用户
5) 用户收到 f+1 个不同副本返回的相同结果，就把此结果作为最后的结果。

实用拜占庭容错算法也存在自身的缺陷，首先成为参与者的节点过多会影响计算效率，因此不适合包含大数量节点的区块链系统；另外，参与者节点的数量是固定的，不适合公有链的开放环境；最后还有一点是，总节点数为 3f+1，因此不能有超过 f+1 的失效作恶节点，容错率相对较低。流程图如下所示：

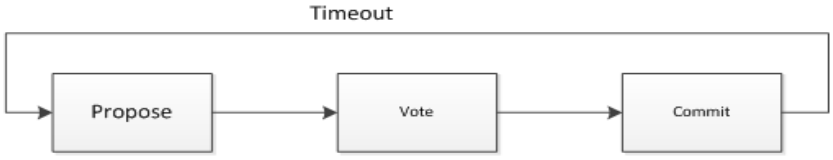


图 2-5 实用拜占庭容错算法流程图

2.4.5 验证池共识机制

验证池共识机制由一种分布式一致性技术实现，主要进行对数据的检验[52]。它主要使用的分布式一致性算法有 Pasox 和 Raft，这两种算法都是比较成熟的，也是经过验证可以较快甚至达到秒级的验证速度。

Pasox 算法中主要包括了三个角色，分别是建议人、接受人和学习人。建议人负责提出建议，接收人负责对建议进行裁决，学习人负责学习建议结果。多个建议人可以提出多个建议，通过一致性算法保证只有一个建议被选中。Pasox 算

法的具体执行过程分为两个阶段。阶段一是准备阶段，所有建议人选出一个建议N，并将建议 N 发送给半数以上的接收人，作为 Prepare(N)，如果接收者响应过的建议编号大于 N，则拒绝，否则，接收者就会将它反应过的最大编号的建议反馈给建议人。阶段二是接受阶段，当一个建议人收到半数以上的接收人对Prepare(N)的响应，那么它就会发送一个包含[N,V]的 accept 请求，其中 V 是阶段一反馈收到的最大编号的建议；当接收人接收到一个针对 N 编号的 accept 请求，只要接收人没有接受过大于 N 编号的 accept 请求，则接受此建议，如果接收人已收到过大于 N 编号的 accept 请求，则拒绝，注意在此处如果建议人没有接收到过半数的响应，则会进入第一阶段，按编号递增的提交建议。

Raft 算法也主要分为三种角色，领导人、候选领导人和跟随人。领导人是关键角色，负责日志的提交，并且日志只能由领导人向跟随人单向复制。具体的执行过程主要分为两个阶段：阶段一是领导人选举，在一开始所有节点都是跟随人角色，在随机超时后接收到领导人或者候选领导人消息，则角色转变为候选领导人，提出选举请求，在最近的选举阶段得票数超过一半者当选为领导人，如果领导人没有被选出，就进入新的阶段并开始重试。领导人主要负责接收日志，并将日志发送到其他节点。阶段二是同步日志，由领导人找到系统中的最新日志记录，并由领导人单向的向所有跟随者复制日志。

2.5 智能合约

智能合约是运行在区块链上的一段可执行代码。区块链上的智能合约具有去中心化，可信任，可编程，不可篡改等特性，可灵活嵌入各种数据和资产，有助于实现安全高效的信息交换，价值转移和资产管理，最终有望深入变革传统商业模式和社会生产关系，为构建可编程资产，系统和社会奠定基础[17]。智能合约就是一段写在区块链上的代码，一旦某个事件触发了智能合约上的条款或满足了设定的某种条件，就会自动执行。智能合约主要的工作原理就是构建、存储和执行。智能合约一般是由区块网络链上多个不同用户共同参与指定，智能合约中一般会明确双方的权利和义务，以编码的方式将权利和义务电子化，代码中也包含智能合约执行的条件[18]。共同参与制定的智能合约一旦编码完成，就会上传到区块链网络中，全网节点都可以验证这份智能合约。智能合约也会设定周期时间来检查是否有符合智能合约某个方法的事件发生，如果有，就让符合要求的事件进入一个可以被验证的队列中。区块链上的验证用户会先对这些事件进行验证来保证其有效性，只有大多数来进行验证的用户达成一致后，智能合约才可以被执行，并将执行结果通知给用户。已经成功执行的智能合约被移出区块链，未执行的智能合约等待下一轮的处理。

2.6 本章小结

本章主要介绍了构建区块链的相关技术。首先是对区块链分布式存储的介绍，主要包括三个关键点，P2P 存储、分布式以及分布式账本。其次是对区块链中加密算法的介绍，主要包括哈希算法和非对称加密算法。简单介绍了区块链中的交易流程。然后是对区块链中共识机制的介绍，介绍了几种不同的共识机制。最后是对区块链中智能合约的介绍

第3章 高并发区块链架构

3.1 从区块链 1.0 到区块链 3.0

互联网主要传递的是信息，在信息中必然存在着价值传递的情况，区块链网络能够保证价值传递的安全。

互联网最初的设计是使用信息传输管道来传输数据，底层协议并不关心上层传输的数据有什么不同，对于底层的交换机和路由器来说，传输的只是机器码 0 和 1。区块链技术的实践是，数据传输完成后，在全网节点之间进行数据共享，每个节点所传输的数据不再由该节点单独拥有所有权，采用这种全网同步共享的方式，既实现了价值信息的传递，又保证了价值的安全[15]。

区块链目前的发展主要是应用层的改进，发展主要经历了区块链 1.0、区块链 2.0 和区块链 3.0 三个阶段。

区块链 1.0 实现了比特币这一区块链应用，它实现的是可编程货币，同时也产生了重大影响，让更多的人了解了区块链。区块链 2.0 主要是一些区块链应用开发平台，比如以太坊，它实现了可编程金融。与区块链 1.0 相比，区块链 2.0 最大的不同之处在于，它不仅提供了开发去中心化应用程序的平台，而且还可以在许多情况下扩展到金融领域[6]。区块链 3.0 主要是以 EOS 为代表的区块链应用，其目标是面向涉及社会各行业的业务的可编程应用。区块链网络中，不仅记录了各种交易信息，而且各种有价值的信息都可以用代码来表示。在任何需要信任的行业业务场景中，都可以应用区块链技术。比特币、以太坊和 EOS 等区块链平台都形成了自己的体系架构[12]。

3.2 区块链的发展难点和解决方案

区块链作为一种新兴技术，其价值是不可否认的，但也有许多制约其发展的因素。第一是效率不高，区块链计算机在理论上是图灵完备的，也就是说，当速度和存储器无限大时，任何可编程的问题都可以解决，但是仍然受到诸如网络延迟等因素的影响。现有的一些区块链应用在向整个区块链网络写入数据时需要大约十分钟的等待时间，同时还需要将所有数据同步到区块链网络中的其他节点上，这一过程要花费更多的时间，因此区块链应用程序也会有一些交易延迟。第二个是能源消耗问题，比如比特币中的矿工，他们的挖矿行为需要消耗能量。第三是隐私保护问题，在区块链的公有链中，所有节点都可以获得包含全部的完整数据，全部的交易结果也是对所有节点可见的，对于某些商业组织来说，某些重要的交

易信息涉及财富信息和商业机密。最后是博弈问题，区块链的去中心化，所有信息数据的安全是由所有节点保证的，没有中心化机构或者国家的监管，可能会被非法机构所利用。

对于当前存在的特定业务场景下的这些问题，有一些方法可以解决，被研究得最多的就是基于 DAG 的区块链——通过增强的有向无环图修改底层数据结构，设计新的共识机制，采用同构多链[28]。然而，基于 DAG 的高并发性区块链也存在其缺陷。第一，交易时间长不可控制，基于 DAG 的区块链验证规则是后面发生的交易对前面的交易进行验证，因此很容易出现最后的交易延迟验证的情况，特别是在整个网络发展初期，节点数较少，导致交易时间无法预测。第二，DAG 作为一种谣言传播算法，它的异步通信机制提高了网络的可扩展性，同时也带来了一致性的不可控制问题。区块链是利用同步操作验证机制来保证较高的一致性。但 DAG 作为一种异步操作，没有全局排序机制，在运行智能合约时，这很可能导致节点间存储的数据在运行一段时间后发生偏差。最后就是安全性尚未进行大规模验证。DAG 技术并非新事物，但它在最近几年才被应用到去中心化的账本中。它也不像比特币那样经历了 10 年之久的安全验证。这也是区块链中基于 DAG 大规模部署 DAPP 的最大障碍。

针对基于 DAG 的区块链的缺陷，本文设计研究的是一种基于可延时验证的高并发区块链架构。本文设计的区块链网络存在作为管理员的超级节点，它作为一个记账中心，普通节点的交易信息通过抽样的普通节点加上超级节点直接进行共识验证，在不出错的情况下，可以极大的减少共识时间；在出错的情况下，普通节点可以提出全网共识，在有一半以上的节点交易信息确认出错时，则此次交易自动取消。本文设计研究的可延时验证区块链主要针对的是彩票系统的应用场景。在中国，发行彩票需要通过民政部门的授权和监管，所以设计的彩票系统必须存在彩票中心。可延时验证的区块链架构中可以将超级节点作为彩票中心，符合彩票系统运行的实际情况。

3.3 基于 DAG 高并发区块链原理

当前应用较广的高并发区块链架构是基于 DAG 设计的。基于 DAG 高并发区块链架构改变了底层的数据结构，采用增强的有向无环图——哈希网的数据结构，这种结构可以大大地减少存储节点的空间，并能提高底层数据存储的效率和安全性。它在分布式共识机制层面采用了双层共识机制，即基于哈希网的增强 DAG 共识和公证人选择的 BA-VRF 共识机制，这种双层共识机制可以加快整个区块链网络达成一致的速度。它在整个区块链网络设计中采用了同构多链架构，用以加快处理区块链节点的并发请求。

3.3.1 增强的有向无环图

当前基于区块链技术的主流应用的影响因素有区块链的规模、区块生成速度、交易确认速度等。目前大多数区块链应用底层采用的是块链式数据结构，这种数据结构对并发性有一定的影响。基于 DAG 的区块链底层采用有向无环图，没有区块概念，没有区块容量的限制，整个区块链都是通过交易来连接的。增强的有向无环图在有向无环图的基础上限定了图的宽度。增强式的有向无环图记录了整个网络所有节点以何种顺序发送数据给其他节点。每个不同节点都存储的有下图 3-1 那样一个哈希图的拷贝。每个节点（下图的 A、B、C、D、E）拥有一个放置顶点的柱子。最新发生的事件，与之前的事件相连记录在如图 3-1 中。

如下图 3-1 所示：

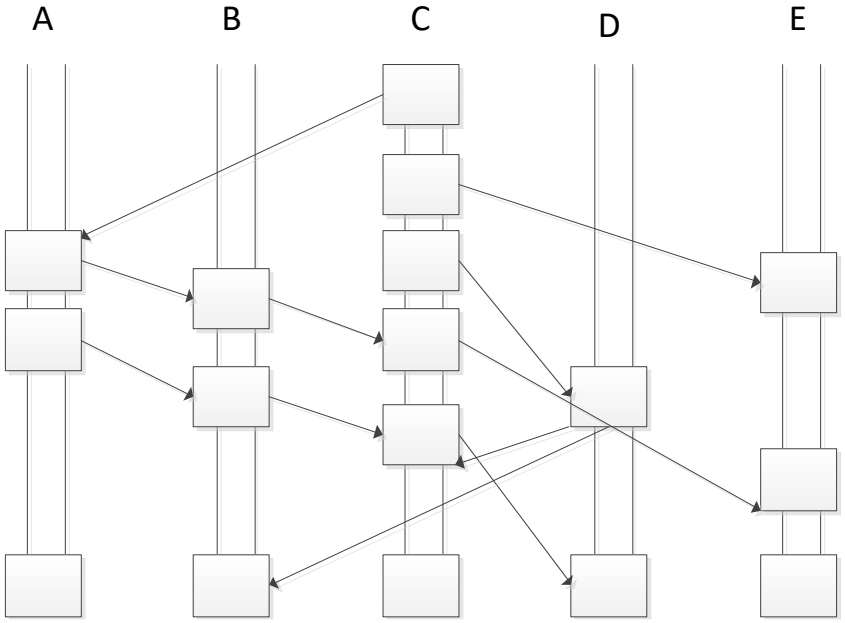


图 3-1 增强的有向无环图

3.3.2 双层共识机制

DAG 结构与一般的区块链结构有所不同，一般的区块链只能沿着一个方向进行，无论中间有多少分叉，都只能将最长的一条链确认为有效链，其他所有的分支链都是无效的。基于 DAG 的区块链网络中，每一次交易都在帮过去的交易做确认，每次的交易的参与者也同样是记账者。在这种情况下，不需要挖矿也能进行交易确认，可以极大减少资源消耗，但是由于没有矿工费的刺激，对安全性有一定的影响，会有一些作恶节点拒绝服务，因此还采用了公证人选择的 BA-VRF 共识机制。

BA-VRF 共识机制是一种采用随机函数算法的拜占庭协商共识机制。VRF

这种可以验证的随机函数，拥有随机和方便验证的两种特性。VRF 实现的方式是本地抽签，每个节点都自己抽签，对于抽中的结果可以很容易地验证是不是此节点的抽签结果。VRF 的具体操作流程是：

1、 证明者生成一对密钥pk、sk

2、 证明者计算如公式(3-1)：

$$result = VRF\_Hash(sk, info)、proof = VRF\_Proof(sk, info) \quad (3\text{-}1)$$

3、 证明者把计算的$result$、$proof$结果传递给验证者

4、 验证者计算如公式(3-2)：

$$result = VRF\_P2H(proof)、True/False = VRF\_Verify(pk, info, proof) \quad (3\text{-}2)$$

如果得到的结果为 True，则表示结果通过，如果得到的结果为 False，则没有通过。通过的具体含义是 proof 是通过传入信息 info 生成的，再通过 proof 是否能算出 result，可以得到 info 是否与 result 匹配，这个结果是证明是否证明者给的材料是正确的。以上的各个 VRF 表达式分别为 VRF_Hash:$F_{sk}(x) = e(g,g)^{1/(x+sk)}$、VRF_Proof:$P_{sk}(x) = g^{1/(x+sk)}$、VRF_P2H:$e\big(g, P_{sk}(x)\big) = F_{sk}(x)$、VRF_Verify:$e\big(g^x pk, P_{sk}(x)\big) = e(g,g)$

采用这种双层共识机制运用在基于区块链的系统中既可以避免其他一些共识机制对于资源的浪费，又可以保证整个基于区块链系统达成强一致共识。

3.3.3 同构多链架构

同构多链，顾名思义就是多条链，每条链上运行的程序是相同的，它把区块链上所有节点用户的请求分发到不同的链上进行处理[46]。如下图 3-2 所示，有 A，B，C，D 四个节点用户同一时刻发起请求，请求在链 1 上有 A->B，A->C，A->D，在链 2 上有 A->B，在链 3 上有 A->C，在链 4 上有 A->D。A，B，C，D 的请求可以根据路由规则将请求落到不同的链上，这四条链并行的对这些请求进行处理。如果一条链的每秒打包请求的速度能够达到一千，那么在千条链级别下，就可以达到百万 TPS。具体的请求并落到链上的路由规则可以采用取模的方式，将这些节点用户的请求较均匀的分布到各条链上。在基于区块链的系统中使用这种同构多链体系结构，可以加速处理由多个节点同时发起的请求，保证了系统具有更高的并发性。

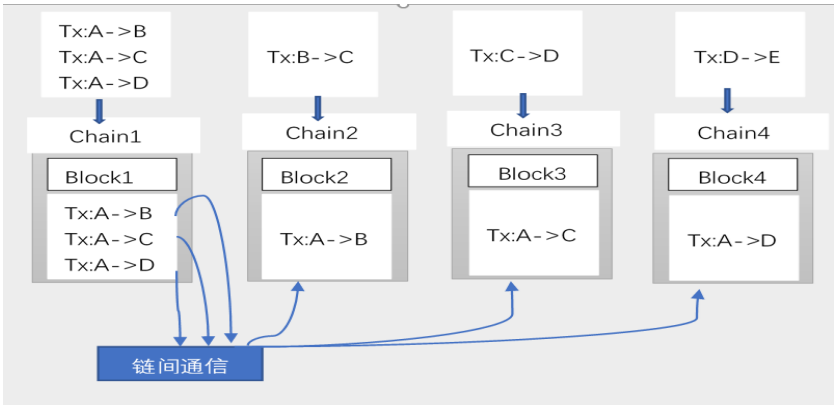


图 3-2 同构多链架构

3.4 可延时验证的高并发区块链设计

基于 DAG 的高并发区块链存在着自身的缺陷。首先是交易时长不可控，基于 DAG 的区块链的验证规则是后面产生的交易验证前面的交易，因此很容易出现最后的交易迟迟无法被验证的情况，尤其是在整个网络发展的初期节点数量比较少的情况下，造成交易时长无法预测。其次是它很难支持强一致性，DAG 作为一种谣言传播算法，其异步通讯机制在提高了扩展性的同时也带来了一致性的不可控问题。最后是它的安全性也没有得到大规模的验证。针对基于 DAG 的区块链的问题，本文设计研究一种可延时验证的高并发区块链架构，主要内容包括超级节点的设计，普通节点的随机选取以及保证数据安全性的延时验证。

3.4.1 超级节点

本文研究的区块链利用目前区块链的节点模型进行改进，在整个区块链网络系统中设计了一个作为管理员的超级节点。本文的研究目标是基于高并发区块链架构的数字彩票系统。在中国，法律规定由福彩中心主导彩票发行事业，并且要求能够从中提取一定的费用用于福利事业，所以彩票发行系统中必须有彩票中心的存在。本文设计的区块链中的超级节点可作为彩票中心。超级节点参与每一笔交易的验证以及直接负责新区块的生成，超级节点不作为唯一的验证中心，交易信息的验证会随机抽样其他节点与超级节点共同验证。参与验证交易信息的其他节点通过随机抽样产生，超级节点无法控制随机抽样的过程，因此超级节点与随机抽样节点共同作恶的成本较大，保证了可延时验证的区块链系统的安全性。超级节点的存在减少了整个系统参与验证交易的节点数量，可以加快每笔交易的确认速度，从而明显提高整个系统的吞吐量。总体而言，本文设计的超级节点既保证了它不作为完全中心化的机构，又提高了整个系统的可扩展性。

3.4.2 普通节点的随机选取

可延时验证的高并发区块链系统在选取普通节点参与验证交易信息时需要保证选取普通节点的随机性。本文利用网络噪声得到输入信息，再通过 SHA256 算法对输入信息进行处理得到选取的普通节点的唯一编号。具体步骤如下：

1. 将网络中传输的最后一个包的时间，发送的 ip 地址，包的大小拼接作为输入信息 data

2. 将总数为 n 的普通节点编号 0 到 n-1，计算第一个选取的普通节点如公式（3-3）：

$$N1 = (int)\big(sha256(data)\big)\ mod\ n \tag{3-3}$$

3. 后续将 sha(data)作为新的 data，重复进行步骤 2 的计算得到 N2，若 N2 节点已被选取，则 data 加 1 继续计算直到选取到新的节点

4. 选取到目标数量的普通节点，则停止计算

3.4.3 延时验证

本文设计的区块链系统通过延时验证保证整个系统中数据的安全性和一致性。普通节点的交易信息在与超级节点或者随机抽样的其他节点验证出错的情况下，这笔交易会延时进行全网共识验证，如果整个网络中有超过一半的节点存在共识错误，那么这次交易就会失败。本文设计的区块链系统会根据延时验证的结果对作恶节点设置惩罚方案，每次作恶服务都会受到一定金额的惩罚，在达到三次时会自动将作恶节点清除出区块链网络中。

3.4.4 工作流程设计

基于可延时验证的高并发区块链中每个节点都参与维护数据的安全性，同时又利用超级节点来提高交易验证速度。它具体的运作流程如下：

1. 区块链中的普通节点向全网广播自己的交易信息

2. 区块链中的普通节点随机抽样四个普通节点与超级节点共同验证自己交易信息的正确性

3. 超级节点将所有正确的交易信息写入到新的区块中

4. 随机抽样的普通节点或者超级节点交易验证出现错误时，则提出全网共识验证

5. 全网共识验证交易出现错误，则交易失败，否则交易将作为正确的交易写入到下一个区块中

3.4.5 架构设计

区块链由所有节点按照一定的区块链标准和合约运行，整个区块链系统交易数据的一致性是由可延时验证来保证的。基于可延时验证的区块链系统中的每一笔交易的验证都涉及到超级节点和随机选取的普通节点共同参与验证。参与验证的普通节点选取得不可控性，保证了数据的安全性。在验证出错的情况下，区块链系统会针对出错的交易提出全网共识，保证了整个区块链系统数据的一致性。

本文构建的可延时验证的区块链包含了应用层的钱包和交易界面，链上代码的智能合约，接收别的节点交易信息、数据同步和验证确认广播等的接口，共识层的验证交易信息，网络层的 P2P 传播，以及数据层的存储方式。图 3-1 基于可延时验证的区块链系统的架构图。

(1) 应用层：钱包和交易界面。展示数字货币和交易界面。

(2) 链上代码的智能合约：部署在区块链上可执行的一段代码。

(3) 接口：交易的接口、退款接口、数据同步接口、广播接口等。

(4) 共识层：通过可延时验证的方法保证整个区块链上数据的一致。

(5) 网络层：P2P 网络、传播机制。各个用户之间传输各自的信息，确认后转发出去。

(6) 数据层：区块数据、链式结构、非对称加密、数字签名以及哈希函数。保存着每次所有通过确认的节点提交的交易的数据。

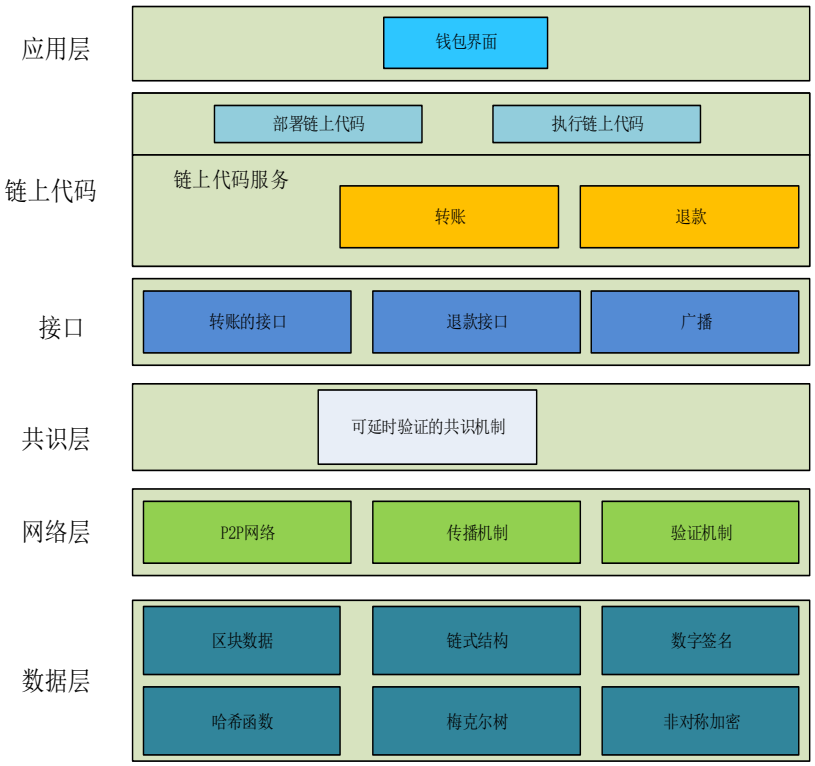


图 3-3 基于可延时验证的区块链系统的架构图

3.4.6 节点模型设计

基于可延时验证的高并发区块链构架的网络是按照 P2P 协议运行的节点集合。节点所拥有的完整功能有交易功能、钱包、完整区块链和路由功能。基于可延时验证的区块链节点网络图如图 3-4 所示。

(1) 钱包功能：节点的数字资产。

(2) 交易功能：输入交易用户地址和金额进行交易。

(3) 延时验证功能：在与抽样的普通节点加上超级节点验证出错时，可以提出全网共识

(4) 完整区块链：记录了所有历史记录，并且通过特殊结构保证历史记录的安全性，还可以用来验证新开奖记录的合法性

(5) 路由功能：信息交互和同步数据

基于可延时验证的区块链节点网络图如下，中间的橙色节点为超级节点，可与所有其他普通节点进行交易信息的快速验证：

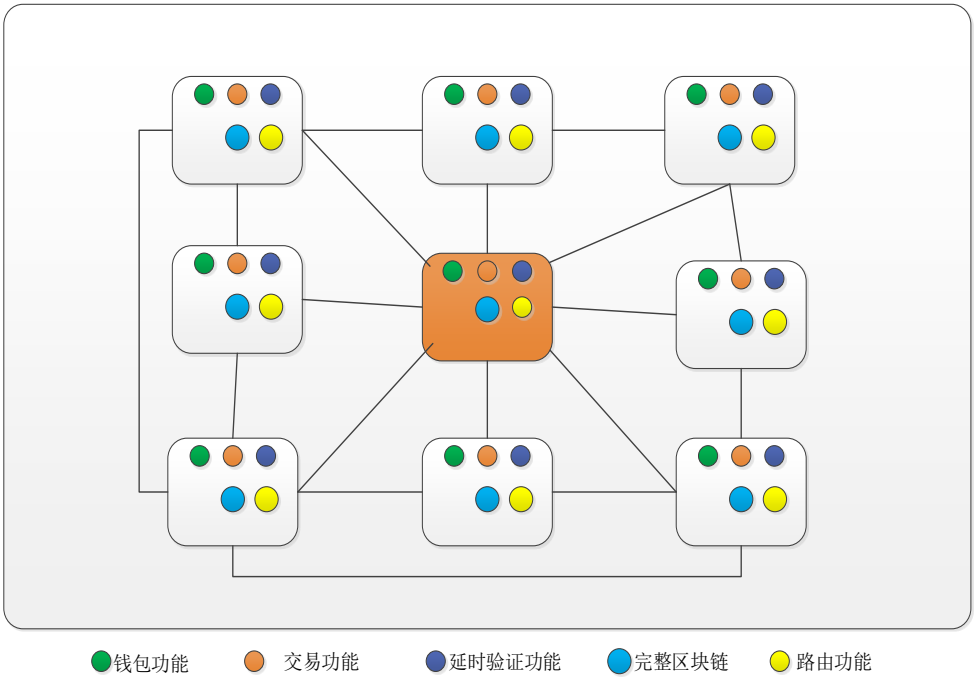


图 3-4 基于可延时验证的区块链节点网络图

3.5 实验数据对比

目前有一些项目是基于 DAG 的高并发区块链架构实现，比如 IOTA。本文就 IOTA 项目的并发测试结果与本文设计的采用超级节点的可延时验证的区块链的并发测试结果进行对比。

3.5.1 测试环境搭建

运用 docker 容器在服务器中配置区块链节点的方法。每个服务器可以部署多个 docker 容器，每个 docker 容器中运行一个区块链节点。并发测试的过程就是利用脚本让多个区块链节点同时发送交易，计算所有交易处理完成时间，通过交易量与交易时间得到吞吐量。节点的部署如下图 3-5 所示：

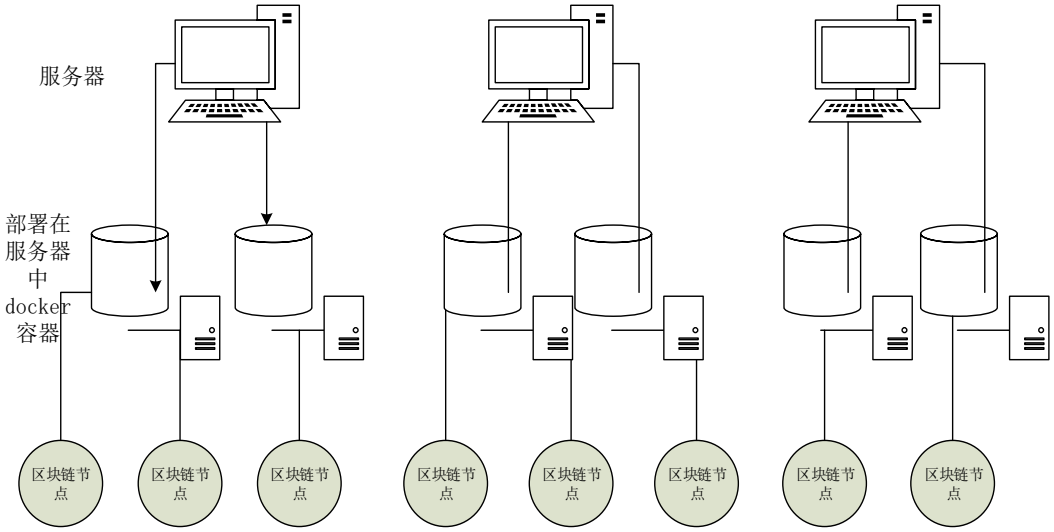


图 3-5 节点的部署

3.5.2 实验数据对比

通过搭建好测试环境，对基于 DAG 的区块链项目和基于可延时验证的区块链系统进行各个流程的测试，将测试结果统计进行对比。

3.5.3 测试流程

基于 DAG 的区块链项目和基于可延时验证的区块链系统进流程的测试主要包括测试花费时间的统计，测试网络的配置，编写好脚本执行以及测试结果如何分析。

1. 测试花费时间

要了解到整个交易花费的时间需要在源码各个执行方法前后打印出时间，然后计算出完成整个交易所花费的时间。

2. 测试网络的配置

在每个服务器中，根据测试配置测试网络各个参数，包括每个服务器部署几个区块链程序 docker 镜像，具体启动多少区块链节点，其中哪个服务器为超级节点，配置节点基本功能，启动各个节点以及需要的配置文件等。准备就绪之后，按照相应测试要求启动测试网络；正常测试情况下，需要启动一个超级节点和多个普通节点，超级节点负责与普通节点验证交易、打包

交易产生区块，而普通节点发送交易，也可以与其他节点验证并提出全网共识，所有节点都与超级节点相连。

3. 脚本的执行

测试网络配置完成后，运行各个节点，需要根据并发交易量来进行相应测试。测试网络中的普通节点负责产生多笔交易，具体通过编写的自动发送交易脚本实现，在每个节点启动时，根据节点类型，为普通节点配置需要的交易发送脚本文件。编写好脚本，通过调用发送交易的 API 接口的方式实现每个节点的交易发起，并可根据需求调节发送交易速率，经实验测量，单个节点最高稳定发送交易速率可为每秒 80 笔交易。

4. 测试结果如何分析

基于 DAG 的区块链项目 IOTA 在服务器上部署了多个 IOTA 节点，利用脚本发送多笔交易，再计算出完成这些交易所花费的时间，最后通过并发交易量和交易时间得到吞吐量。基于可延时验证的区块链系统也是在服务器中部署多个节点，但会将其中一台服务器只部署超级节点用于与其他节点的确认。基于可延时验证的区块链系统的普通节点也是通过交易脚本发送交易以及计算出完成这些交易的时间得到吞吐量。

3.5.4 测试结果

基于 DAG 的区块链项目 IOTA 的测试情况如下表 3-1 所示。测试情况包括了并发交易量在 100、200、500 和 1000 这四种情况。

表 3-1 基于 DAG 的区块链项目 IOTA 测试情况

并发交易量	响应时间（秒）	吞吐量（交易数/秒）
100	20	5.0
200	26	7.69
500	27	18.51
1000	27	37.0

基于 DAG 的区块链项目 IOTA 在并发交易数较少时，系统的吞吐量并没有很高。主要原因是采用的共识机制在全网区块链达成共识花费的时间较多，特别是需要选择有向无环图中当前交易的后续出度交易作为公证人花费的时间较多。在并发交易数量较多时，吞吐量有明显的提升。相较于目前应用较广的区块链项目，比如比特币——吞吐量 7-8TPS，以太坊——吞吐量 15-16TPS，还是有一些

提升的。

基于可延时验证的区块链系统的测试情况如下表 3-2 所示。作为比对测试情况也是在并发交易量为 100、200、500 和 1000 这四种情况。

表 3-2 系统测试情况

并发数	响应时间（秒）	吞吐量（交易数/秒）
100	5	20
200	6	33.33
500	10	50
1000	11	90.91

基于可延时验证的区块链系统在不同并发交易量的情况下的吞吐量都有一定的提升，这四种情况是在没有出错的情况下得到的测试结果。出错情况下也只是当前出错节点需要提出全网共识，影响的也只有出错的这一笔交易，对整个区块链系统的吞吐量影响不大。本文设计研究的基于可延时验证的区块链系统还可以就作恶节点设计可行的惩罚机制，避免出现更多的恶意情况。

从实验结果可得知基于可延时验证的区块链系统在吞吐量上有明显的提升。基于可延时验证的区块链系统直接利用超级节点进行新区块的生成，而基于 DAG 的区块链项目需要花费时间选取公证人；基于可延时验证的区块链系统通过随机选取的普通节点与超级节点共同验证交易信息，实际情况中出错的交易较少，整个验证过程不需要大量的节点参与，所以整个系统的并发量会有明显的提升，而基于 DAG 的高并发区块链项目会花费一定的时间在系统的共识上，通过后面的交易验证前面的交易这种方法也会造成验证时间的不可控性。

3.6 本章小结

本章首先介绍了目前区块链发展经历的阶段，其次介绍了区块链发展中的难点，然后阐述了目前构建高并发区块链架构的方法——目前构建高并发区块链架构的关键技术主要包括了增强的有向无环图、双层共识机制以及采用了同构多链架构。本章还设计研究了基于可延时验证的高并发区块链架构。最后本章进行了基于 DAG 的高并发区块链架构的项目与本文设计的基于可延时验证的高并发区块链架构的实验对比，包括测试实验流程以及得到的实验结果，从实验结果可知本文设计研究的基于可延时验证的高并发区块链系统吞吐量有一定的提升。

第4章 基于高并发区块链的数字彩票发行系统的实现

4.1 引言

随着彩票事业的大力发展，彩票的种类也越来越多，比较流行的就是数字型彩票，给定一组数字，一般是在其中选取六个数字，开奖后选中的数字越多奖金越多。

数字型彩票在整个发展过程中，存在一些无法解决的难题，最主要的就是彩票中心不可信任的问题。彩票中心控制着抽出中奖号码的摇奖机器，摇奖器真正的运行过程是不可知的，所有得到的结果是否可以人为控制也是未知的；还有一些数据，比如彩民购买彩票的具体时间、购买金额的多少等情况也只有彩票中心自己知道；最后中奖者的身份也是保密的。存在如此多的彩票中心人为可控的因素，购买彩票的用户多少也会对这种购买模式产生怀疑，长此以往购买彩票的用户也会越来越少。

为了扩大彩票市场，彩票中心又引入了互联网彩票发行模式，这种代购模式引发了更多的问题。由于买彩票的金额会达到千万级别，而中奖金额只有百万级别，中奖的几率非常小，互联网彩票站点会想方设法将这些彩票私吞，这就是“吃票”。而与此同时，这些互联网彩票站点也开始坐私庄。更为严重的还有“黑彩”，这是非法的、完全受彩票网站控制的地下彩票，他们可以通过暗箱操作和“赌博”获取大量不义之财。上述问题的存在，在一定程度上将阻碍彩票业的健康发展。产生这些问题的原因，最主要的还是彩票中心的控制，目前的技术无法保证数据的公开和透明。

而使用区块链技术正好可以解决这些存在于彩票系统中的信任问题。第一，中奖号码确实可以实现随机生成；第二，所有信息包括中奖号码、中奖金额和中奖者加密的地址都可以公开显示，加密的地址还能保证中奖者的安全；最后，兑奖的实时性。由于区块链技术的推动，没有真正的第三方彩票中心的控制，彩票系统的整个操作流程都可以公开，因此彩民购买这种完全随机的彩票数量也会越来越多。

在中国，发行彩票必须通过民政部门的彩票中心，我们不可能设计一种完全无中心化的区块链来应用到彩票系统上。如前文所述，本文研究的可延时验证的高并发区块链架构存在超级节点可作为彩票中心。超级节点可提高彩票系统的并发量，并且从技术上通过普通节点的随机选取和延时验证防止了超级节点作恶的可能性。基于可延迟验证区块链的数字彩票发行系统解决了传统网络彩票系统对第三方的依赖问题，符合彩票系统的实际应用场景，提高了区块链的吞吐量，使

数字彩票发行系统具有良好的扩展性。

4.2 系统的分层

基于高并发区块链的数字彩票发行系统的分层一共有五层，首先最底层是数据层、然后是通讯网络层、一致共识层、发行和分配代币的激励层、最后是智能合约层。系统具体的分层如下图 4-1 所示：

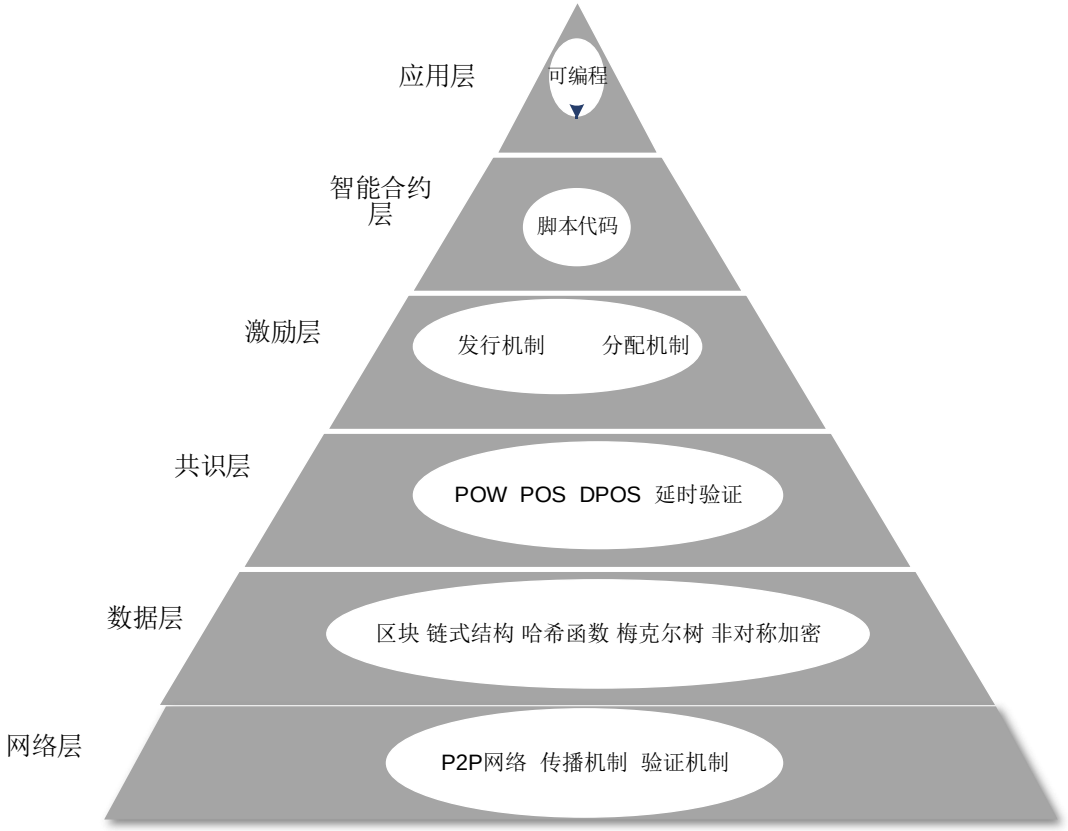


图 4-1 系统分层图

(1) 数据层。数据层是最底层的技术，主要是存储区块数据，保证账户和交易的安全。数据存储主要链式结构，通过区块的方式实现。账户和交易的安全是基于数字签名，哈希函数以及非对称加密技术实现的。

(2) 网络层。网络层主要通过 P2P 网络实现节点的连接和通讯，没有中心服务器，用户之间互相交换信息，每个用户节点都有服务器的功能。

(3) 共识层。共识层让区块链网络中的全部节点对各种结果达成相同的认证，防止各种不一致攻击，所以在这一层使用的算法叫做共识算法，目前主要有工作量证明、权益证明、实用拜占庭容错算法、股份授权证明、POOL 验证池等。基于高并发区块链的数字彩票发行系统采用的可延时验证的共识机制。

(4) 激励层。激励层是利用设计好的发行的形式来发行区块链中的电子货币，

设计好的分发形式来分发代币。

(5) 智能合约层。智能合约就是一段可执行的计算机程序，满足条件时即自动执行。区块链中的运行智能合约是通过设定好的逻辑来运行得到各种想要执行结果；整个的运行过程和结果都在区块链网络中完成。

区块链一般分为公共使用的公有链、私人使用的私有链以及各个机构联合使用的联盟链。公有链是指对任何符合的节点都可以自由的进入和离开区块链网络；私有链是由某个特定的人或机构组织控制的，可以选择性的开放区块链；各个机构联合使用的联盟链是指每个节点对应的是一个机构，进入和离开都需要得到授权。对于企业而言，机构联合使用的联盟链将是未来的重点研究对象。目前主要是公有使用的公有链的各种应用场景。

基于可延时验证区块链的数字彩票发行系统利用公有链进行改进，在区块链中设计了超级节点。数字彩票发行系统虽然存在超级节点，但信息的验证会随机抽取其他彩民节点共同参与，在出错的情况下，会进行全网共识，保证了整个数字彩票发行系统的安全性，最后的开奖结果也是由随机算法控制的。

4.3 系统的需求

1.数据一致性的需求

基于高并发区块链的数字彩票发行系统要保证数据的一致性，每个不出错节点都能确认自己的提交的数据。在本文提到的基于高并发区块链的数字彩票发行系统是用可延时验证的共识机制来保证节点的一致性。不采用工作量证明的共识算法，可以避免大量计算力的浪费。

2.彩票系统设计的需求

基于高并发区块链的数字彩票发行系统不同一于般传统的系统。设计好的区块链本身就具有安全透明、不可篡改的优点，所有的购买彩票号码信息会向全网广播，杜绝了彩票中心作弊的可能，这也是未来彩票系统发展所需要的。

3.链上代码智能合约的需求

基于高并发区块链的数字彩票发行系统的智能合约也是系统安全的关键部分。链上代码的智能合约是一直都在运行的，得到满足条件就返回结果。智能合约的设计要安全可靠且符合彩票系统。链上代码的复杂性也不太高，实现的功能就是由设计好的选择算法选择出中奖号码以及用中奖号码去匹配彩民所买彩票号码，自动开奖。智能合约是自动执行的，虽然不具有法律效应，但是却有足够

的可靠性。如果以后能加上法律限制，那就是真正的合约了。对于智能合约真正要关注的就是安全性，设计的智能合约要能避免很多不必要的安全漏洞，也要避免一些误操作异常。

4.4 系统的关键技术

区块链技术具有去中心化和安全透明的特点。但为了达到节点间信任，需要适当的算法来实现。对于彩票系统而言，必须保证开奖号码选择的随机性和不可控性、数据一致性以及开奖过程不可逆的自动执行。考虑到这些必须因素，本节介绍了系统的开奖时间节点、开奖号码的随机性选择以及开奖过程智能合约的自动执行等关键技术。

4.4.1 开奖的时间节点

数字彩票发行系统中有几个比较重要时间点，第一个时间节点是彩民提交购买的彩票数字截止时间，此时提交购买的彩票数字以及金额，整个提交的信息使用加密算法加密，秘钥由彩民自行保管，密文发布到链上供所有节点记录。超过此时间节点，就不再允许提交购买的彩票数字和金额。

第二个时间节点是与管理员超级节点以及随机抽样的普通节点验证时间，在此时间节点之前，彩民需提交自己购买彩票和金额的加密信息，超级节点和抽样的普通节点通过保存在区块链上的购买信息进行验证，此过程所有区块链上的节点均可以与超级节点重复验证。

第三个时间节点是普通彩民节点提出全网共识验证时间，在此时间截止之前，所有彩民节点在与超级节点或者随机抽样出来的普通节点验证出错的情况下，可以提出全网验证共识。此节点过后，即进入自动派奖环节，由智能合约自动执行。具体的时序图如下图 4-2 所示：

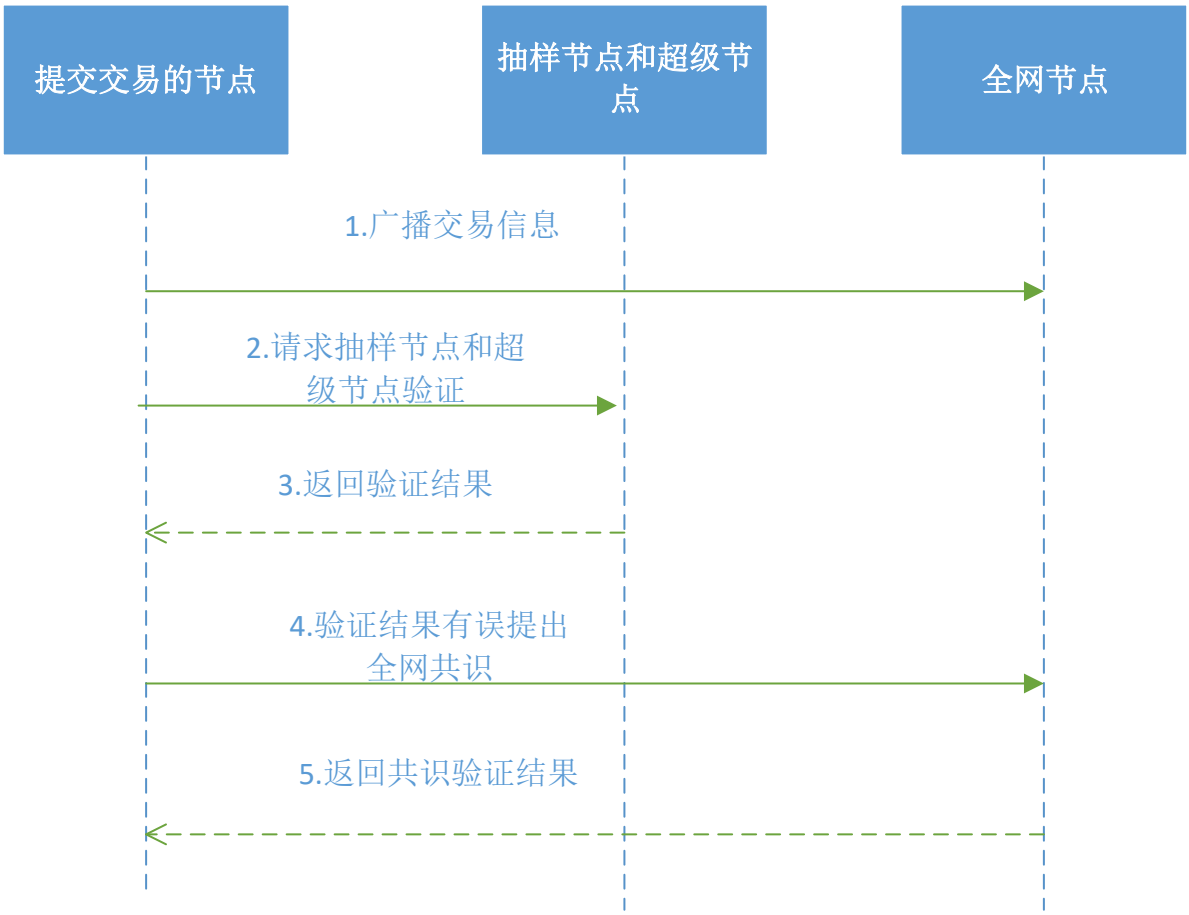


图 4-2 时序图

4.4.2 开奖号码的随机性控制

传统彩票的中奖号码是由摇奖机产生的，是否真正能保证随机性一直备受质疑。本文设计数字彩票发行系统中，中奖号码是由 SHA256 算法对不可控的数据进行散列计算得到的。开奖过程中，执行智能合约的开奖方法，开奖号码的选择是利用 SHA256 的算法，对开奖前生成的最后一个区块的 hash 值、区块链的时间戳以及参与人数进行加密得到十六进制数，再将十六进制数转换为十进制数 Numbers。计算公式如(4-1)：

$$Numbers = (int)SHA(BlockHash, timestamp, LotteryBuyers) \quad (4\text{-}1)$$

利用这个十进制数选出 1~36 中六位不重复的数。设计的算法步骤是：

1. 第一个中奖号码直接为：$Lottery1 = Numbers \ mod \ 36$
2. 后面中奖号码计算方法如公式(4-2)：

$$LotteryN = (int)SHA\big(BlockHash, timestamp, Lottery(N-1)\big) \ mod \ 36 \quad (4\text{-}2)$$

如果中奖号码与前面的中奖号码重复，Lottery(N-1)加 1 在重复计算直到不

再与前面的中奖号码重复。利用计算公式一共取得六个数字作为开奖号码。

SHA 系列的安全散列算法具有单向性，只要加密信息不可控，那么所有人都无法反向推出正确的散列值，这保证了开奖号码选择的随机性和安全性。通过以上算法可以保证取到的 6 位中奖号码的随机性

4.4.3 开奖的智能合约

智能合约的特点是代码对所有人可见、不能窜改和永久运行。开奖过程的智能合约是得到多方节点认证并且预先设定好满足条件，即按照随机算法选定的中奖号码匹配的多少分级派奖，再与每个节点早已提交的买彩票的号码进行比较自动派奖。全过程不受任何人为因素或中心机构的影响，基于高并发区块链的数字彩票发行系统智能合约作为链上代码一直在运行，只要满足条件，即可执行。在本文设计的彩票系统中，智能合约可以部署在彩票中心节点上运行，不需要本地 EVM。智能合约根据编写好的算法随机选择出 6 个中奖号码，自动执行开奖。智能合约还会保存彩民提交的购买彩票数字以及统计所有购买的金额作为奖金池，通过 6 个开奖号码和彩票购买数字对比，将奖金池中的金额按预先确定的比例自动派奖，少部分盈利转入彩票中心的账户作为彩票基金。从选择中奖号码到开奖全过程是安全透明的，人人可见，任何用户都可以在区块链中查询数据。

4.5 系统的架构模型

将区块链技术与实际应用场景相结合，构建一个公共使用的数字彩票发行系统。在彩票系统运作流程中，不存在一个中心机构能够控制开奖过程，所有节点都按照一定的区块链标准和合约来运行。整个区块链彩票系统的一致性是通过可延时验证的共识机制来实现的。彩票系统首先要保证系统的安全性，因此在这个基于高并发区块链的数字彩票发行系统中，可以把出错的节点排除在彩票系统之外，从而保证系统的强一致性。

本文构建的基于高并发区块链的数字彩票发行系统中包含应用层的彩票系统界面，链上代码的智能合约，接口来接收彩民购买的彩票号码、公私钥同步和验证确认广播等，共识层的超级节点确认，普通节点全网共识，网络层的 P2P 传播，以及数据层的存储方式。图 4-3 基于高并发区块链的数字彩票发行系统的架构图。

(1) 应用层：彩票系统。彩民节点提交彩票的号码和下注金额。

(2) 链上代码的智能合约：开奖号码选择和派奖过程的智能合约的方法执行。保证开奖、派奖过程的不可逆不可修改。且部署在区块链上一直执行。

(3) 接口：买彩票的接口、派奖接口、验证接口、广播接口等。

(4) 共识层：可延时验证的共识机制。保证整个基于高并发区块链的数字彩票发行系统的一致性。

(5) 网络层：P2P 网络、传播机制。各个用户之间传输各自的信息，确认后转发出去。

(6) 数据层：区块数据、链式结构、非对称加密、数字签名以及哈希函数。保存着每次所有通过确认的节点提交的号码的数据。

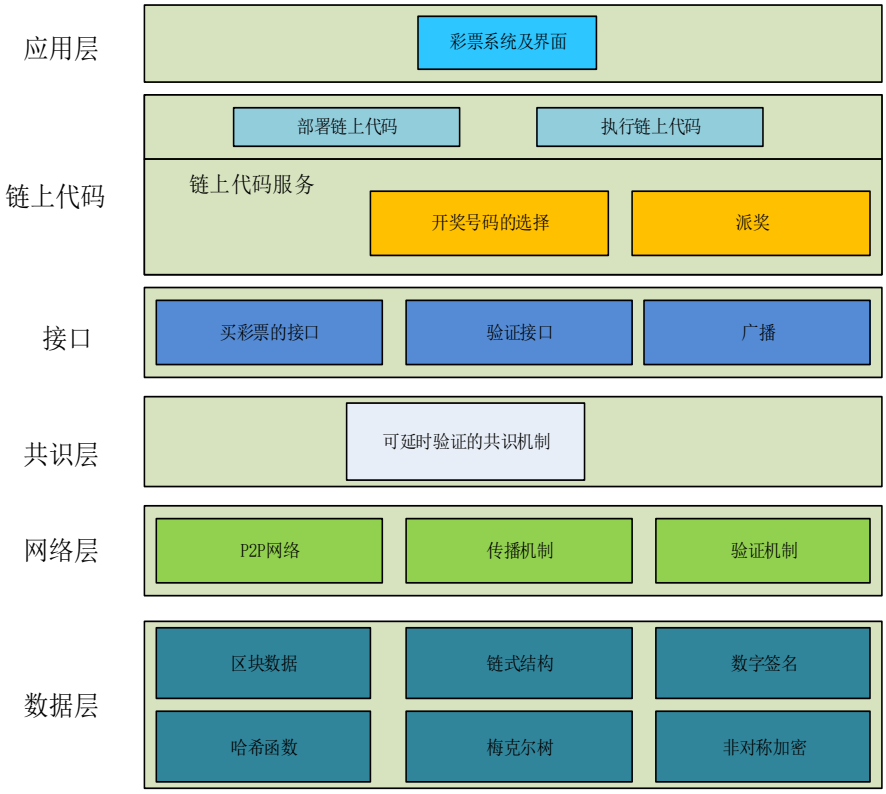


图 4-3 基于高并发区块链的数字彩票发行系统架构

4.6 系统的工作流程

基于高并发区块链的数字彩票发行系统通过应用层界面购买彩票号码和下注金额并加密来生成可验证的信息，通过 SHA256 算法得到不可控开奖号码，并将所有节点提交的购买彩票号码与 SHA256 算法得到的开奖号码进行比较，从而进行开奖。普通节点通过接口向全网广播自己的购买彩票信息并随机抽样参与验证的普通节点，在共识时间内由超级节点和随机抽样的普通节点共同验证购买彩票信息，如果出现验证错误，则采用延迟的共识验证机制，以保证购买信息的一致性和正确性。所有验证通过的购买信息由超级节点生成新区块来记录这些信息，最后通过链上代码的智能合约的自动运行其中的方法来开奖派奖。系统详细的工作流程如下：

1. 购买彩票数字和下注金额通过 hash（用户地址，购买彩票数字，金额）得到信息摘要 hash 值，向全网节点广播，这是开始时间，相当广播某个地址用户的购买彩票信息。

2. 共识时间，随机选取四个普通节点参与验证。

3. 每个节点与超级节点以及随机抽样的普通节点验证自己购买彩票信息是否正确。

4. 如果正确此节点购买的彩票有效，将购买的记录保存在智能合约中。

5. 如果购买彩票信息与超级节点或者普通节点验证的信息有误，普通节点可以提出全网共识。全网共识的结果是有一半及以上的节点出错，则此节点的此次购买无效，退款回节点账户。

6. 智能合约的开奖方法会利用 SHA256 算法对不可以控的区块链 hash 值，区块链中的时间戳，参与人数进行加密，利用设计好的选取中奖号码算法得到开奖号码。

7. 通过对比购买记录与开奖号码进行开奖。

8. 最后智能合约会利用编写好的派奖方法将中奖金额发送到中奖用户地址。

系统的工作流程如下图 4-4 所示：

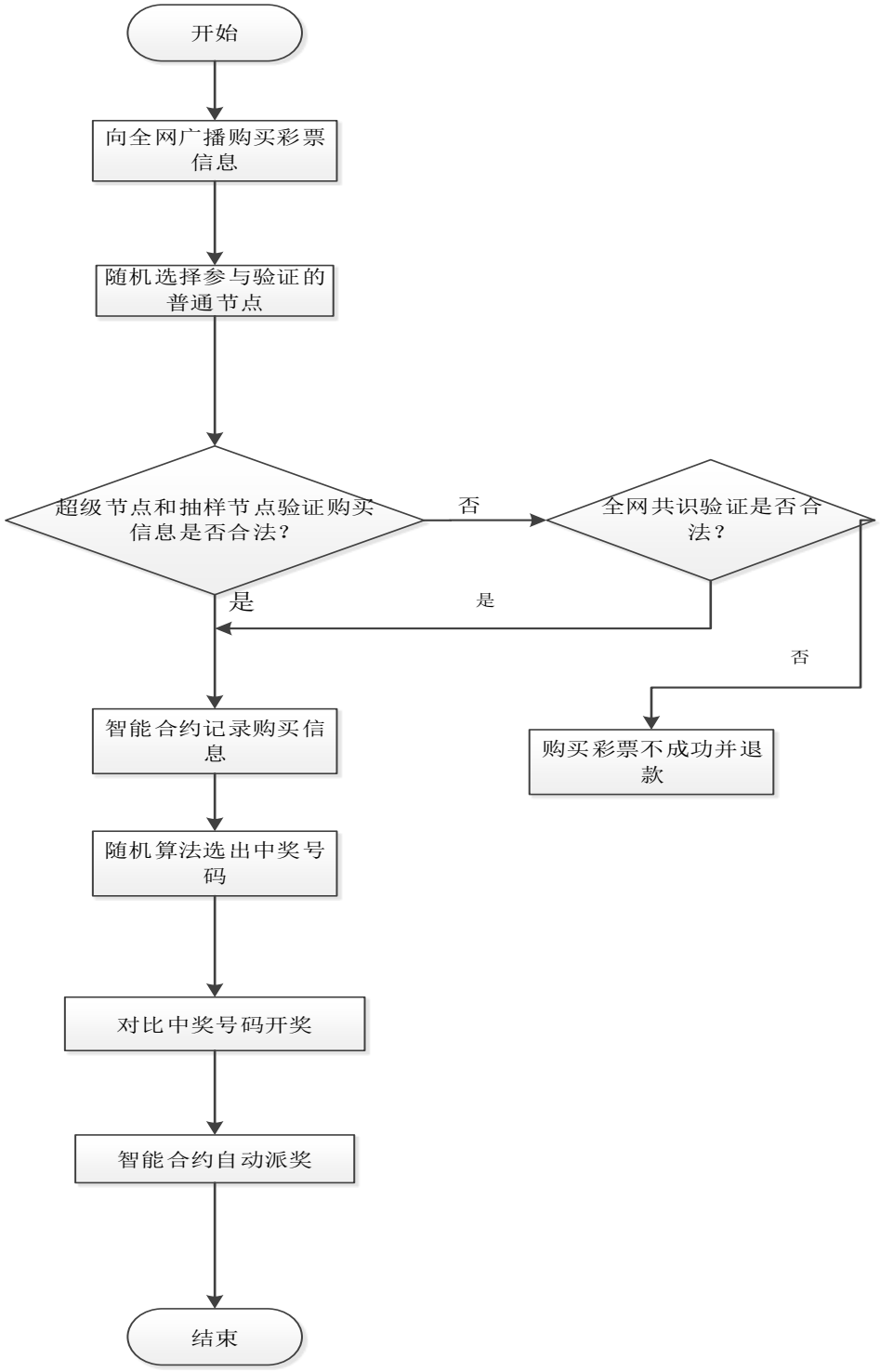


图 4-4 基于高并发区块链的数字彩票发行系统流程图

4.7 系统的网络模型

基于高并发区块链的数字彩票发行系统的网络是按照 P2P 协议运行的节点集合。节点所拥有的完整功能包括彩票购买功能、交易功能、验证功能、钱包、

完整区块链和路由功能。节点网络图如图 4-5 所示。

(1) 彩票购买功能：提交自己所购买的彩票号码和下注金额。

(2) 交易功能：与其他节点进行交易。

(3) 验证功能：与其他节点进行数据验证。

(4) 钱包：节点的数字资产。

(5) 完整区块链：记录了所有历史开奖记录，并且通过特殊结构保证历史开奖记录的安全性，还可以用来验证新开奖记录的合法性

(6) 路由功能：把其他节点的提交数据及验证结果等信息传送给更多的节点。

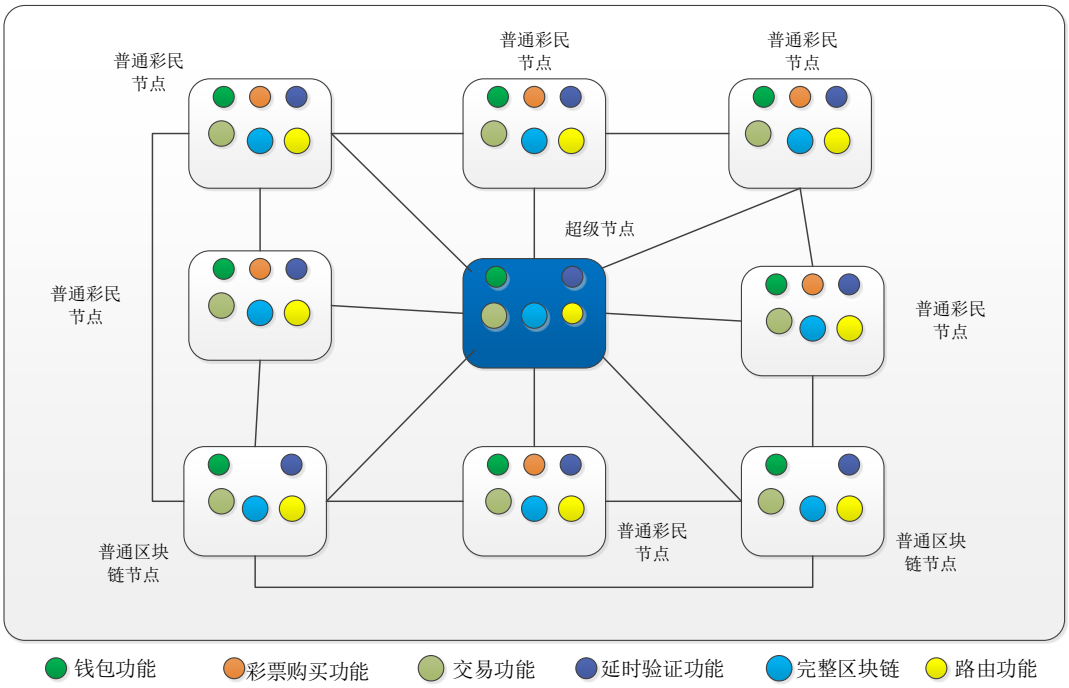


图 4-5 彩票系统节点网络

4.8 系统的功能模块

基于高并发区块链的数字彩票发行系统使用 react 框架实现前端界面，通过 web3. js 与区块链测试链进行交互，主要是与部署在测试链上的智能合约交换信息。基于高并发区块链的数字彩票发行系统作为一个开源的系统，智能合约部署的地址是可查询的，智能合约的代码也可以查询和获取，保证了没有第三方机构的控制。

彩票系统采用 B/S 架构，主要包括管理员、彩民两类用户。彩民作为普通用户只有提交购买彩票号码功能，管理员拥有开奖和退款的功能。功能的具体执行方法都是由部署好的智能合约来执行。

基于高并发区块链的数字彩票发行系统可实现彩民提交的彩票信息加密互

传，没有彩票中心的控制，管理员只负责开奖，并且可以设置为倒计时自动开奖。

基于高并发区块链的数字彩票发行系统软件实现难点存在有：

(1) 操作与处理的数据量大

主要体现在所需传输的彩票数据量大，一个彩民的数据就可能多达几十条，又由于不同时间段，购买彩票的数量差异较大（高峰时期可能一秒上万的数据量）。所以节点间互传信息时，整个信息量的处理也是十分庞大的。在对中心化彩票系统进行统计/汇总时，所操作的数据将达到数十万条。

(2) 超级节点验证数据量大

主要体现在彩票系统后期购买彩票的人数增加，超级节点是需要参与验证每一笔交易的，超级节点需要更好的计算力。

(3) 如何保证中奖号码的随机性。

主要体现在彩票系统选择中奖号码时是否完全随机，增加了彩票系统开奖设计的难度。

(4) 并发量大

采用开奖在倒计时二十四小时后智能合约自动开奖。在购买彩票时间段将会有大量的用户进行操作，如何设计智能合约在大量数据处理后，能够较快时间开奖来满足较高的并发数，是必须要考虑的问题。

基于高并发区块链的数字彩票发行系统的功能模块主要分为智能合约部署模块、彩票购买管理模块、彩票系统开奖模块、彩票退款模块，彩票开奖记录模块。

1. 智能合约部署模块

智能合约部署，此功能是管理员将智能合约部署到测试链，如表 4-1 所示：

表 4-1 智能合约部署模块

功能描述	智能合约部署
输入	编译彩票系统智能合约
处理	通过 web3 和 infura api 部署到测试链
输出	输出部署地址和智能合约 abi

2. 彩票购买管理

彩票号码购买，此功能针对使用彩票系统的普通用户，如表 4-2 所示。

表 4-2 彩票购买管理模块

功能描述	购买彩票号码
输入	选择号码购买
处理	通过本地浏览器前端展示与智能合约进行信息交换
输出	输出购买成功

3. 彩票开奖模块

彩票系统进行开奖，此功能是管理员进行开奖，通过智能合约编写的方法选出随机数。随机数是交易难度，区块链时间戳，和购买人数进行 sha3 加密得到。如表 4-3 所示

表 4-3 彩票开奖模块

功能描述	彩票系统开奖
输入	直接调用智能合约的开奖方法
处理	选择出不可控的随机数
输出	买彩票中奖了的用户账户增加相应得的钱

4. 彩票退款模块

彩票系统在规定时间没有进行开奖，通过智能合约的退款方法直接将购买金额通过用户地址返回给用户账号。如表 4-4 所示。

表 4-4 彩票退款模块

功能描述	彩票系统退款
输入	直接调用智能合约的退款方法
处理	在开奖时间到达后一定时间内没有开奖
输出	将购买金额通过用户地址返回给用户账号

5. 彩票开奖记录模块

彩票系统记录往期的中奖人地址和开奖金额，通过智能合约的开奖返回中奖

人地址和金额记录到 web 系统的数据库做展示。如表 4-5 所示。

表 4-5 彩票开奖记录模块

功能描述	彩票开奖记录
输入	调用智能合约的方法得到返回中奖人地址和金额
处理	将智能合约返回的数据存到数据库
输出	将所有往期数据展示在前端页面

4.9 系统的实现

基于高并发区块链的数字彩票发行系统主要包括两方面实现，一是实现的 react 前端界面利用 web3.js 与测试链上部署的智能合约交互，二是利用 JavaWeb 项目记录往期的中奖情况并且做展示。web3.js 可以获取和调用账号，交易以及合约的一些信息，利用 web3.js 就可以通过提交的购买的彩票号码调用智能合约的方法进行购买彩票和管理员调用智能合约开奖方法进行开奖和兑奖，在出现问题的情况下，管理员还可以调用智能合约的退款方法退款。JavaWeb 项目是通过 web3.js 与智能合约交互返回的每次彩票系统开奖数据保存到数据库中，再从数据库中取出数据做页面展示。

系统目前设计只有购买彩票号码这类彩票购买模式，后续还会进行其他彩票项目的设计实现。彩民通过彩票界面填写好彩票号码，在可购买时间段提交，验证购买信息的合法性，最后通过我们部署好的智能合约进行开奖号码选择和兑奖。智能合约根据开奖方法的 SHA256 算法选出开奖号码，对于兑奖申请自动执行兑奖。普通用户彩票系统信息和投注如下图 4-6 所示

图 4-6 普通用户彩票系统信息和投注

每个用户在本地前端界面购买彩票号码利用 web3 将数据提交到智能合约上，智能合约会用 string 数组和 address 数组将买的彩票号码和用户地址存起来。用户选择六个号码组成字符串作为购买彩票序列，默认投注 0.1 个以太币。每个人购买会增加参与人数和奖池奖金，通过 web3 获取到这些信息显示在页面上。点击立即投注会打开本地 MetaMask，进行支付确认。

MetaMask 如下图 4-7 所示：

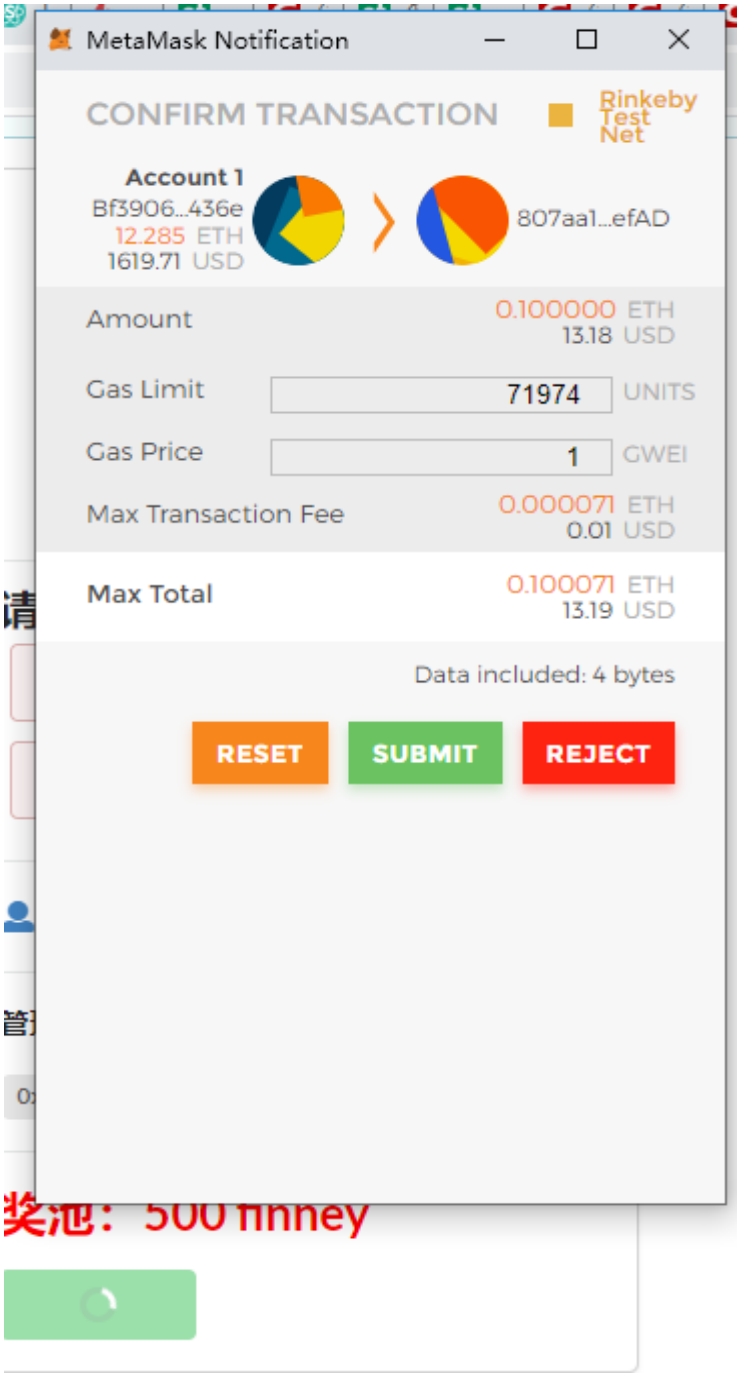


图 4-7 MeatMask

管理员彩票系统的界面相比于普通用户多了开奖和退款的功能和按钮显示。开奖主要是利用 SHA256 对区块的 hash 值，区块时间戳，以及购买人数的进行加密得到十六进制的数，在转为十进制的数按确定算法规则取到六位当作最后的开奖号码。这些所取的值都是认为不可控的，进行的加密也是不可逆的，所以无法控制最后的随机数取值。最后将保存的用户购买彩票数组与开奖号码对比进行开奖和兑奖。开奖和兑奖是智能合约直接将中奖金额发送到中奖者的地址账户。

退奖是将每个用户购买的彩票的金额退回到用户的账户。

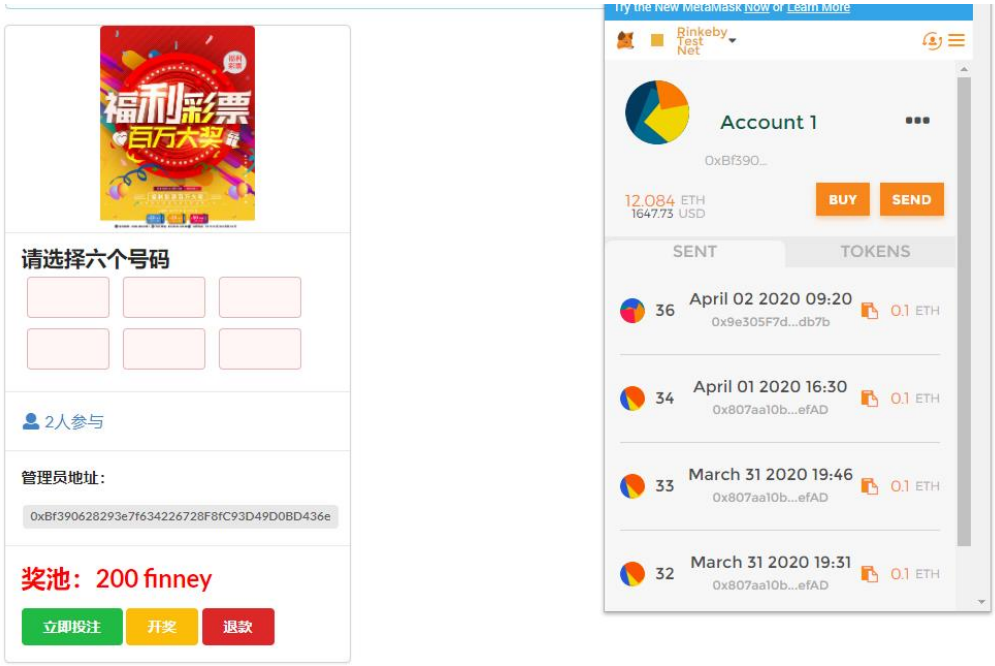


图 4-8 管理员彩票系统信息

彩票开奖记录通过 web3.js 与智能合约交互所得，智能合约开奖方法将返回每次的彩票系统开奖数据保存到数据库中，再从数据库中取出数据做页面展示。页面展示内容包括每次开奖的中奖人地址、开奖的金额以及开奖时间。这个部分还设计了开奖记录的数据库以及对应的彩票记录表图。数据库实体为彩票开奖记录实体：记录 id、开奖时间、开奖号码、中奖人地址、开奖总金额

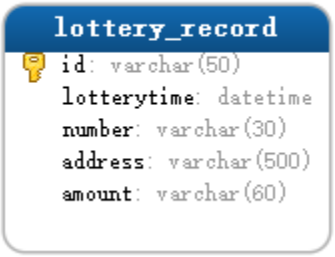


图 4-9 彩票记录表图

还有具体页面如下图 4-10 所示：

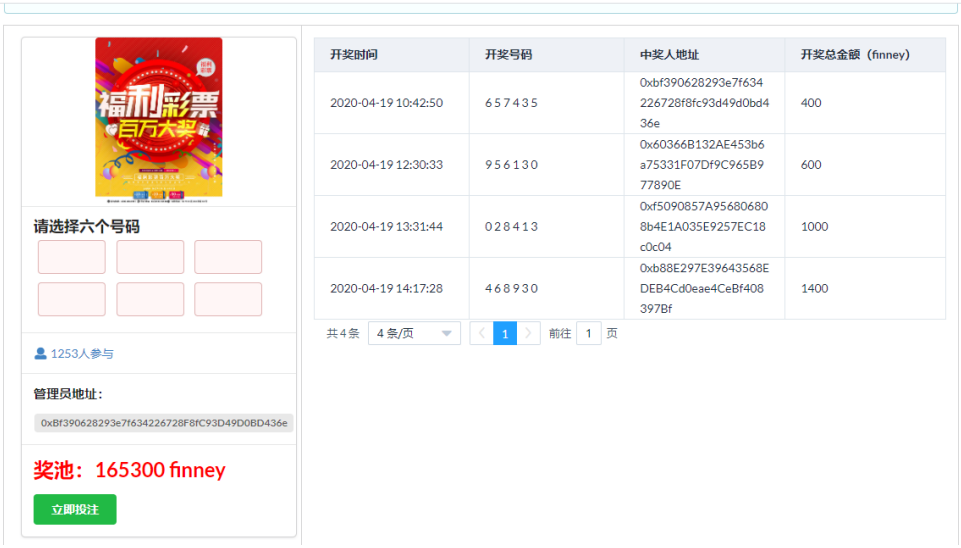


图 4-10 彩票开奖记录信息

基于高并发区块链的数字彩票发行系统的简单实现目前被划分为四个部分，通过这四个部分的结合使用，实现数字彩票系统中用户购买彩票号码，随机选择中奖号码，中奖后将中奖金额发送到中奖用户账户。测试链上所部署的智能合约具有透明查询性，确保数字彩票系统选择中奖号码和开奖过程没有第三方机构控制。Java web 项目仅仅是为已经被授予奖项的过去数据做一个页面显示，为彩民提供过去数据查询。

4.10 本章小结

本章主要研究了基于高并行区块链架构的数字彩票发行系统。本章将可延时验证的区块链技术应用于数字彩票发行系统，主要研究了系统的层次结构描述，系统的关键技术点，系统的需求，系统的架构模型，系统的工作流程，系统的网络模型，系统的功能模块，系统的工程实现。

第5章 总结与展望

5.1 总结

本文从区块链的研究背景出发，研究了如何构建一个区块链网络，主要包括存储的方式、怎样进行加密和达成一致的机制。介绍了目前基于 DAG 的高并发区块链架构，主要包括有向无环图、双层共识机制以及同构多链架构。本文设计研究了基于可延时验证的高并发区块链系统，提出了利用区块链网络中的超级节点和随机抽样节点验证来提高交易确认速度，并在普通节点的交易信息验证出错时，可延时提出全网共识，以保证区块链系统的安全性。基于可延时验证的区块链设计了一个数字彩票发行系统，主要包括分层架构、关键技术、需求和架构设计以及软件设计。

当下区块链这一技术和基于高并发区块链的各种项目都处于高速成长的时期，区块链技术能高效的解决很多行业的痛点。金融机构使用区块链技术可以对每一笔交易涉及的完整信息进行记录，很明显区块链技术可以改善交易透明度，可以从根本上解决传统互联网第三方机构的信任问题。类似彩票这种销售管理行业利用区块链技术可以减少彩票中心的控制，增加整个流程的透明度。

5.2 展望

目前，区块链这一技术主要应用于电子货币相关的业务场景下，随着区块链技术的发展也向着其他各种不同场景延伸。区块链技术被认为是继云计算、无线传感器网络和大数据之后的另一种颠覆性技术[29]。同时它可以为云计算、大数据等新一代兴起的产品带来新的机遇，并且在与云计算[54]、大数据、物联网[38]等技术结合使用的情况下有机会能带来再一次互联网大变革[49]。所以我也希望企业和高校科研团队能够把握住当前的机遇，做好应对区块链过程变化带来的挑战。

未来区块链技术将主要向三个方向发展：一是提升区块链的并发能力，提高效率，还需要不断改进共识机制和尝试新的共识机制，采用更加适合的运行引擎和存储系统；二是增加更多契合实际应用场景的功能，优化改进智能合约语言，加强约束检查的力度；三是与开发研究者有更好的交互，采用声明式编程语言，提升区块链技术的普及学习。当然未来区块链技术的研究重点应该放在提高区块链网络的并发性上，如何构建与业务场景结合的高并发的区块链网络也将会成为研究核心[16]。本文研究的内容也是面对未来区块链发展的核心内容。

参考文献

[1] 洪蜀宁.比特币:一种新型货币对金融体系的挑战[J].中国信用卡,2011(10):61-63.

[2] 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.

[3] 高政风,郑继来,汤舒扬,龙宇,刘志强,刘振,谷大武.基于 DAG 的分布式账本共识机制研究[J].软件学报,2020,31(04):1124-1142.

[4] 许荻迪.区块链技术在供应链金融中的应用研究[J].西南金融,2019(02):74-82.

[5] 梁雯,司俊芳.基于共享经济的“区块链+物流”创新耦合发展研究[J].上海对外经贸大学学报,2019,26(01):60-69.

[6] 张锐.基于区块链的传统金融变革与创新[J].国际金融,2016(09):24-31.

[7] 刘敖迪,杜学绘,王娜,李少卓.区块链技术及其在信息安全领域的研究进展[J].软件学报,2018,29(07):2092-2115.

[8] 夏昌琳,宋玉蓉,蒋国平.一种优化的权益证明共识策略[J].计算机工程,2019,45(05):25-28+34.

[9] 黄嘉成,许新华,王世纯.委托权益证明共识机制的改进方案[J].计算机应用,2019,39(07):2162-2167.

[10] Pim Otte,Martijn de Vos,Johan Pouwelse. TrustChain: A Sybil-resistant scalable blockchain[J]. Future Generation Computer Systems,2017,40(2):11-20.

[11] 黄秋兰,程耀东,陈刚.分布式存储系统的哈希算法研究[J].计算机工程与应用,2014,50(01):1-4+77.

[12] 邵奇峰,金澈清,张召,钱卫宁,周傲英.区块链技术:架构及进展[J].计算机学报,2018,41(05):969-988.

[13] 骆慧勇.区块链技术原理与应用价值[J].金融纵横,2016(07):33-37+76.

[14] Kaspars Zīle,Renāte Strazdiņa. Blockchain Use Cases and Their Feasibility[J]. Applied Computer Systems,2018,23(1):12-20.

[15] 钱卫宁,邵奇峰,朱燕超,金澈清,周傲英.区块链与可信数据管理:问题与方法[J].软件学报,2018,29(01):150-159.

[16] Alexander Savelyev. Copyright in the blockchain era: Promises and challenges[J]. Computer Law & Security Review: The International Journal of Technology Law and Practice,2018,34(3): 550-561.

[17] 欧阳丽炜,王帅,袁勇,倪晓春,王飞跃.智能合约:架构及进展[J].自动化学报,2019,45(03):445-457.

[18] 郭少飞.区块链智能合约的合同法分析[J].东方法学,2019(03):4-17.

[19] 李海波.利用区块链技术促进我国跨境电商发展[J].财会月刊,2019(03):142-146.

[20] Akihiro Fujihara. PoWaP: Proof of Work at Proximity for a crowdsensing system for collaborative traffic information gathering[J]. Internet of Things,2020,10.

[21] Haibo Yi. Securing instant messaging based on blockchain with machine learning[J].

Safety Science,2019,120.

[22] 祝烈煌,高峰,沈蒙,李艳东,郑宝昆,毛洪亮,吴震.区块链隐私保护研究综述[J].计算机研究与发展,2017,54(10):2170-2186.

[23] 龙云安,张健,艾蓉.基于区块链技术的供应链金融体系优化研究[J].西南金融,2019(01):72-79.

[24] 葛琳,季新生,江涛,江逸茗.基于区块链技术的物联网信息共享安全机制[J].计算机应用,2019,39(02):458-463.

[25] 曾繁荣.基于分布式账本技术的数字货币发展研究[J].西南金融,2016(05):63-68..

[26] 韩璇. 区块链技术中的共识机制研究[C]. 中国计算机学会.第 32 次全国计算机安全学术交流会论文集.中国计算机学会:中国计算机学会计算机安全专业委员会,2017:155-160.

[27] 朱凤霞. 基于区块链技术的交易数据库加密技术[J]. 电子设计工程, 2020, 28(03):93-97.

[28] 李芳,李卓然,赵赫.区块链跨链技术进展研究[J].软件学报,2019,30(06):1649-1660.

[29] Qi Liu,Xiao Zou. Research on trust mechanism of cooperation innovation with big data processing based on blockchain[J]. EURASIP Journal on Wireless Communications and Networking,2019,2019(1).

[30] Fabian Knirsch,Andreas Unterweger,Dominik Engel. Implementing a blockchain from scratch: why, how, and what we learned[J]. EURASIP Journal on Information Security,2019,2019(1).

[31] Haibo Yi. Securing e-voting based on blockchain in P2P network[J]. EURASIP Journal on Wireless Communications and Networking,2019,2019(1).

[32] Yan Zhu,Khaled Riad,Ruiqi Guo,Guohua Gan,Rongquan Feng. New instant confirmation mechanism based on interactive incontestable signature in consortium blockchain[J]. Frontiers of Computer Science,2019,13(6).

[33] Johann Kranz,Esther Nagel,Youngjin Yoo. Blockchain Token Sale[J]. Business & Information Systems Engineering,2019,61(6).

[34] 蔡恒进,郭震.供应链金融服务新型框架探讨:区块链+大数据[J].理论探讨,2019(02):94-101.

[35] 王海勇,郭凯璇,潘启青.基于投票机制的拜占庭容错共识算法[J].计算机应用,2019,39(06):1766-1771.

[36] 甘俊,李强,陈子豪,张超.区块链实用拜占庭容错共识算法的改进[J].计算机应用,2019,39(07):2148-2155.

[37] 徐健,陈志德,龚平,王可可.基于区块链网络的医疗记录安全储存访问方案[J].计算机应用,2019,39(05):1500-1506.

[38] 王艺超.基于区块链技术的物联网安全解决对策[J].电子技术与软件工程,2019(01):170-171.

[39] Lu Wang,Xin (Robert) Luo,Frank Lee. Unveiling the interplay between blockchain and loyalty program participation: A qualitative approach based on Bubichain[J]. International Journal of Information Management,2019,49.

[40] Don D.H. Shin. Blockchain: The emerging technology of digital trust[J]. Telematics and Informatics,2019,45.

[41] Ziyu Wang,Hui Yu,Zongyang Zhang,Jiaming Piao,Jianwei Liu. ECDSA weak randomness in Bitcoin[J]. Future Generation Computer Systems,2020,102.

[42] 袁勇,倪晓春,曾帅,王飞跃.区块链共识算法的发展现状与展望[J].自动化学报,2018,44(11):2011-2022.

[43] 房永壮,王辉,王博.基于大数据共享环境下图书馆“区块链”技术应用研究[J].现代情报,2018,38(05):120-124.

[44] 王海龙,田有亮,尹鑫.基于区块链的大数据确权方案[J].计算机科学,2018,45(02):15-19+24.

[45] 闵新平,李庆忠,孔兰菊,张世栋,郑永清,肖宗水.许可链多中心动态共识机制[J].计算机学报,2018,41(05):1005-1020.

[46] 李彬,曹望璋,张洁,陈宋宋,杨斌,孙毅,祁兵.基于异构区块链的多能系统交易体系及关键技术[J].电力系统自动化,2018,42(04):183-193.

[47] 陈晓玲,罗恺韵.基于区块链的学生档案管理系统架构[J].电子技术与软件工程,2019(23):170-171.

[48] 王冰钰,颜拥,文福拴,周自强,林少娃,陈星莺.基于区块链的分布式电力交易机制[J].电力建设,2019,40(12):3-10.

[49] 陈新忠.区块链技术的本地化云计算大数据应用[J].科学技术创新,2019(33):90-91.

[50] 张婷,王永胜.区块链技术对高校图书馆数字资源建设的影响[J].山西科技,2019,34(06):54-56.

[51] 李斯维,李军祥.基于区块链技术的冷链物流体系构建研究[J].电子商务,2019(11):5+12.

[52] 左鹏,孙云刚,袁梦,张海阔,杨卫平,陈连栋,王珏.基于区块链和 DNSSEC 的身份认证模型[J].计算机系统应用,2019,28(11):161-167.

[53] 黄穗,陈丽炜,范冰冰.基于 CP-ABE 和区块链的数据安全共享方法[J].计算机系统应用,2019,28(11):79-86.

[54] 梁贺君,韩景倜.基于区块链的云计算资源去中心化交易共识机制研究[J].计算机科学,2019,46(S2):548-552.

[55] R. L. Rivest,A. Shamir,L. Adleman. A method for obtaining digital signatures and public-key cryptosystems[J]. Communications of the ACM,1983,26(1).

致谢

不知不觉已经从本科到研究生在湘大呆了快七年了，在这么长一段愉快时光中，我不仅在专业知识上提升了很多，也清楚知道自己需要担负的社会责任，对我未来的发展和树立个人的目标都有了清楚的认识。当然，这所有的成长都离不开学校、老师、同学、亲人的对我的帮助。

首先我要感谢我的导师刘新老师，在研究生的三年时光里，刘老师不仅言传身教的帮助我提高自己的专业能力，而且在我遇到困难时总能提醒我陷入的误区，就是在刘老师不断的帮助下，我才能顺利的完成这篇论文。刘老师认真的态度，对待每个知识点的严谨，对待每个问题细心的解答，都让我受益颇丰。

感谢湘潭大学给了我一个良好的学习环境和氛围，让我能够不断提高自己，感谢所有老师给予我的帮助，让我可以了解更多的知识，学习到更多帮助我成长的东西。

感谢所有的同学，有机会能一起学习，互帮互助，共同进步。感谢同门的师兄师姐对我学习的帮助和生活上的照顾。感谢李梦磊、赵梦凡共同陪我度过三年美好时光，祝他们前程似锦，事业有成。感谢师弟刘龙、蔡林杰、唐朝、李广、马中昊、黄浩钰，你们让我的研究生生活变的更加丰富多彩。

感谢我的亲人对我不断的支持，使我能够勇往直前的不断进步。

附录 A：攻读硕士学位期间科研成果及参与的研究项目

一、学术论文

[1] 李聪, 刘新, 李梦磊, 赵梦凡等. 一种基于区块链的数字彩票发行系统[J]. 信息安全研究, 2018, 004(012):P.1142-1148.

二、专利

[1]刘新，李聪，李梦磊，赵梦凡，孙道秋，郭炳元，刘京麦野 基于区块链的数字彩票发行方法及区块链节点，公开号 201811041023.1