同济大学
TONGJI UNIVERSITY

硕士学位论文

基于区块链的扶贫资金管理平台关键技术的研究与设计

姓　　名：李一鸣

学　　号：1531636

所在院系：电子与信息工程学院

学科门类：工 学

学　　科：控制科学与工程

指导教师：马小峰 副教授

二〇一八年三月

同濟大學
TONGJI UNIVERSITY

A dissertation submitted to

Tongji University in conformity with the requirements for

the degree of Master of Science in Engineering

Research and Design of the Key Technology of Fund Management Platform Based on Block Chain

Candidate: Li Yiming

Student Number: 1531636

School/Department: College of Electronics and Information Engineering

Discipline: Engineering

Major: Control Science and Engineering

Supervisor: Prof. Ma Xiaofeng

March, 2018

基于区块链的扶贫资金管理平台关键技术的研究与设计

李一鸣

同济大学

学位论文版权使用授权书

本人完全了解同济大学关于收集、保存、使用学位论文的规定，同意如下各项内容：按照学校要求提交学位论文的印刷本和电子版本；学校有权保存学位论文的印刷本和电子版，并采用影印、缩印、扫描、数字化或其它手段保存论文；学校有权提供目录检索以及提供本学位论文全文或者部分的阅览服务；学校有权按有关规定向国家有关部门或者机构送交论文的复印件和电子版；在不以赢利为目的的前提下，学校可以适当复制论文的部分或全部内容用于学术活动。

学位论文作者签名：

年　　月　　日

同济大学学位论文原创性声明

本人郑重声明：所呈交的学位论文，是本人在导师指导下，进行研究工作所取得的成果。除文中已经注明引用的内容外，本学位论文的研究成果不包含任何他人创作的、已公开发表或者没有公开发表的作品的内容。对本论文所涉及的研究工作做出贡献的其他个人和集体，均已在文中以明确方式标明。本学位论文原创性声明的法律责任由本人承担。

学位论文作者签名：

年　　月　　日

摘要

脱贫攻坚是“第一民生工程”，是普惠千万贫困百姓的举措。中央、国务院和各级党委政府前所未有地高度重视，举全社会之力脱贫攻坚。贵州省积极响应党中央脱贫攻坚的号召，设立贵州脱贫攻坚投资极贫乡（镇）基金，实现政府资金引导、社会资本参与、项目提前实施，有效解决极贫乡（镇）资金缺口问题，实现与全省、全国同步小康的战略目标。扶贫基金涉及的资金总体规模巨大，所以需要强化对资金的管理，提高使用效率，降低资金风险。

作者有幸参与了 2017 年贵州省脱贫攻坚项目，在实际项目的基础上开展研究，提出并设计了“脱贫攻坚+区块链”的解决方案。区块链技术的运用，为实时、全面的了解扶贫资金的使用情况和项目的开展情况，保障数据的可追踪和不可篡改，实现精准的资金管控提供了可能的实现手段。

本文遵循“理论研究与分析——实践与开发——优化与提升”的基本思路。根据实际项目需求，提出了“脱贫攻坚+区块链”的解决方案。设计并实现了基于区块链技术的扶贫资金管理平台，设计了基于区块链技术的链上“数字汇票”和实时对账系统，双管齐下，做到了对扶贫资金从发行、流转到最终使用的全流程闭环监控。

基于实际项目需求，本论文对区块链技术现阶段存在的相关问题进行研究，对共识机制和系统架构做出了分析并改进。本文通过分析当前区块链共识机制存在的问题，提出了基于信用评分的主节点切换协议的 CBFT(Credit-based Byzantine Fault Tolerance)共识算法，保障了区块链系统的安全性和活性。在系统架构方面，本文设计了多链架构，对请求进行并行处理，从而提升了区块链系统的 TPS(Transactions Per Second)。

本文一方面探索了区块链在扶贫场景的应用模式。另一方面，研究并设计了新的共识算法和系统架构，经过实验验证，提高了区块链系统的安全性和 TPS。本论文是国内较早探索区块链在扶贫场景应用的研究，为区块链技术在中国的实际落地应用提供了借鉴经验。

关键词：脱贫攻坚，区块链，共识机制，多链

ABSTRACT

Poverty alleviation is ‘The most important livelihood project’, and this move will benefit millions of poor farmers. Today central and local governments at all levels have attached great importance to this project, and the strength of the whole society is taken to achieve it. This paper is based on the poverty alleviation project of Guizhou Province in 2017. Guizhou province responds positively to the call of the Party Central Committee for poverty alleviation and set up a poverty alleviation fund to investment poor townships and towns. The fund will help to achieve goals that government’s funding works as guidance, social capital investment the project, and the project could begin in advance. The fund could effectively solve the capital shortage problem in extremely poor townships (towns). And the well-off society will be built at these poorer region as other regions in our country. Because of large scale of the fund, we need to strengthen the management of the fund, improve the use efficiency and reduce the risk of capital.

It is my honor to participate in the project of poverty alleviation in Guizhou province in 2017. Based on the actual project, this paper proposed and designed a scheme of "Poverty Alleviation + blockchain". The use of blockchain technology provides a feasible implementation solution to understand the project progress and the capital transfer information timely and comprehensively ,ensure the data traceable and tamper-resistant, control the capital accurately.

This paper follows the basic idea of "theoretical research and analysis - practice and development - optimization and promotion". According to the characteristics of poverty alleviation fund business, I designed and implemented a management platform for poverty alleviation fund based on the technology of blockchain. I put forward a new concept called "digital chain draft" in order to ensure that the fund's authority and credit accessibility, besides, I researched and designed a two pronged real-time reconciliation system based on blockchain technology to regulate the fund from the issuance, circulation and use.

Based on the actual project needs, this paper has studied some problems of the blockchain technology at this stage, then analyzed and improved the performance of consensus mechanism and system architecture. By analyzing the problems of the

blockchain consensus mechanism at current stage, a CBFT (Credit-based Byzantine Fault Tolerance) consensus algorithm based on credit score is proposed, which ensures the security and activity of the blockchain system. In terms of system architecture, this paper presents a multi chain architecture and a method of parallel processing of requests, which all could enhance the TPS (Transactions Per Second) of the blockchain system.

On the one hand, this paper explores the application mode of blockchain in the poverty alleviation scene. On the other hand, the new consensus algorithm and system architecture are studied and designed, and experiments show that the security and throughput of the block chain system are improved. This paper is an early study of the application of block chain in the poverty alleviation scene in China, which provides experience for practical application of block chain technology.

Key Words: Poverty alleviation, Blockchain, Consensus mechanism, Multi chain architecture

目录

摘要.....I
ABSTRACT.....II
第 1 章 绪论.....1
1.1 研究背景.....1
1.2 研究问题.....2
1.3 研究意义.....2
1.4 研究现状.....3
1.5 论文创新点.....6
1.6 论文结构.....6
第 2 章 区块链相关技术.....8
2.1 概述.....8
2.2 区块链的类型.....11
2.3 区块链的特征.....11
2.4 区块链的核心技术.....12
2.4.1 共识机制.....12
2.4.2 智能合约.....13
2.4.3 安全技术.....14
2.4.4 分布式存储.....15
2.5 主流区块链技术介绍.....17
2.5.1 比特币.....17
2.5.2 以太坊.....20
2.5.3 超级账本.....23
第 3 章 共识机制的研究与优化.....28
3.1 痛点分析.....28
3.2 算法设计.....28
3.2.1 系统模型.....28
3.2.2 模型假设.....29
3.2.3 算法定义.....29
3.2.4 符号说明.....30
3.2.5 算法流程.....31
3.2.6 主节点切换协议.....33
3.3 本章小结.....34
第 4 章 区块链架构的研究与设计.....35

4.1 痛点分析.....35
4.2 现有方案对比.....35
4.3 解决方案.....36
4.3.1 方案架构.....36
4.3.2 执行流程.....38
4.3.3 关键模块.....38
4.4 本章小结.....44
第5章 系统测试.....46
5.1 性能测试.....46
5.1.1 测试环境.....46
5.1.2 测试算法.....46
5.1.3 TPS测试.....47
5.2 本章小结.....51
第6章 平台的设计与实现.....52
6.1 业务介绍.....52
6.2 业务痛点分析.....53
6.3 解决方案.....53
6.3.1 基于区块链的数字汇票系统.....53
6.3.2 基于区块链的实时对账系统.....57
6.4 技术路线.....60
6.5 技术选型.....61
6.6 系统展示.....62
6.7 本章小结.....66
第7章 总结与展望.....67
7.1 总结.....67
7.2 展望.....67
致谢.....69
参考文献.....70
个人简历、在读期间发表的学术论文与研究成果.....74

第1章 绪论

1.1 研究背景

脱贫攻坚是“第一民生工程”，是普惠千万贫困农民的举措。中央、国务院和各级党委政府前所未有地高度重视，举全社会之力脱贫攻坚。2013 年，习近平总书记在湖南调研时，首次提出“精准扶贫”；2015 年，他在贵州考察时，进一步就扶贫开发工作提出“六个精准”的基本要求；中共十八大报告明确提出了到 2020 年全面建成小康社会的宏伟目标，确保农村贫困人口实现脱贫。（《中共中央国务院关于打赢脱贫攻坚战的决定》）2017 年 10 月，习近平总书记在中国共产党第十九次全国代表大会开幕会上再次提出，要坚决打赢脱贫攻坚战。

为加快贵州省极贫乡（镇）脱贫步伐，贵州省通过设立贵州脱贫攻坚投资极贫乡（镇）基金，实现政府资金引导、社会资本参与、项目提前实施，有效解决极贫乡（镇）资金缺口问题，实现与全省、全国同步小康的战略目标，根据贵州省人民政府批准的《贵州脱贫攻坚投资基金设立方案》，贵民集团拟定了《贵州脱贫攻坚投资极贫乡（镇）基金设立方案》和《贵州脱贫攻坚投资极贫乡（镇）基金管理办法(试行)》。该方案第一阶段募集极贫基金总规模为人民币 173 亿元。其中贵州脱贫攻坚投资基金有限责任公司（以下简称“脱贫基金公司”）出资 6 亿元，20 个极贫乡（镇）所在县级政府指定的国有独资公司（以下简称“县级国有公司”）出资 4 亿元，金融机构出资 163 亿元。极贫基金投资于省委省政府确定的 20 个极贫乡（镇）。名单如下：威宁县石门乡、晴隆县三宝彝族乡、从江县加勉乡、赫章县河镇彝族苗族乡、望谟县郊纳镇、黄平县谷陇镇、册亨县双江镇、贞丰县鲁容乡、镇宁县简嘎乡、纳雍县董地苗族彝族乡、德江县桶井土家族乡、盘县保基苗族彝族乡、榕江县定威水族乡、平塘县大塘镇、雷山县大塘镇、紫云县大营镇、水城县营盘苗族彝族白族乡、长顺县代化镇、石阡县国荣乡、务川县石朝乡。极贫基金主要投向极贫乡（镇）区域内“十三五”期间政府资金不能覆盖或投资不足的农村基础设施、公共服务、产业发展、改善农村人居环境等方面。

扶贫资金总体规模巨大，由于传统的组织架构和管理方式的限制，由此给监管带来了同样巨大的压力。监管方需要能实时、全面的了解到扶贫资金的使用情况和项目的开展情况。同时，还存在着诸如资金“碎片化”，“各自为政、条块分割”，项目多头申报、资金重复安排等诸多问题。为了解决这些问题，目前往

往采用增加管理层级的方式，但是，这又带来了管理成本上升、资金沉淀比例增加等问题。

1.2 研究问题

(1) 区块链在扶贫场景的应用模式

新技术的发展为扶贫工作提供了全新的解决方案。区块链技术具有安全可靠、可追溯、不可篡改、透明性高、利于多方协同等特点。因此，区块链技术的运用，为实时、全面的了解扶贫资金的使用情况和项目的开展情况，保障数据的可追踪和不可篡改，实现精准的资金管控提供了可能的实现手段。如何将区块链技术应用于扶贫场景，是本论文研究的首要问题。

(2) 共识机制的优化

共识机制是区块链系统的核心与灵魂所在，在传统的区块链技术中，如比特币、以太坊等采用 PoW 共识机制，虽然 PoW 共识机制可以有效的保证区块链的可信性，并且很好的实现了去中心化，但是该算法依然存在诸如性能低下、高耗能、弱一致性等问题。针对以上问题，本论文提出了基于信用评分的主节点切换协议的 CBFT 共识算法，在保障区块链系统的一致性的前提下，提升了区块链的 TPS，降低了区块共识所需消耗的资源，提高了区块链系统的安全性。

(3) 区块链 TPS 的提升。

区块链的性能一直是制约区块链发展的重要瓶颈。提高区块链系统的吞吐量，提高区块链对其上层业务的处理能力，才能应对更多的应用场景。本文经过研究，对区块链系统架构进行了优化和改进，设计多链架构，对请求进行并行处理，结合优化后的共识机制提升了区块链的 TPS。

(4) 智能合约的设计

智能合约是连接区块链底层和业务前端的桥梁，要将区块链与脱贫攻坚投资极贫乡（镇）基金业务相结合，智能合约的设计至关重要。智能合约需要完成脱贫攻坚投资极贫乡（镇）基金业务全生命周期的所有重要流程，包括基金募集、基金投资、基金管理、风险防控和基金退出等，使扶贫资金全生命周期运行在区块链中，形成一个完美的闭环。

1.3 研究意义

扶贫资金使用的一个难点是如何使得扶贫资金安全的用在最需要的地方而不是被挪用、延误或浪费。本文设计并实现了基于区块链技术的扶贫资金管理平

台，提供了对扶贫资金的有效管理途径。通过智能合约，在资金划拨阶段前就规定好其用途、使用条件、依赖性、时间限制等各种明确的量化标准，资金跟着项目的事先约定“自动走”。资金在流转中的每一步都在区块链上留痕，可追溯，防篡改，提供了按照资金的详细足迹进行全生命周期完整监督的能力，实现更规范的资金管理、更高效的资金使用。

同时，由财政资金精准投放使用带来的是社会资本对扶贫领域的关注与投入，发挥杠杆作用，撬动银行信贷资金和其他社会资金，引导全社会共同参与扶贫战略。这样形成一种良性循环机制，避免一些贫困区县仍然依赖于财政资金和“等、靠、要”的想法，切实解决贫困地区的融资困难问题，扭转商业银行储蓄资金外流造成的“抽血”为主动“造血”。

最后，本文对区块链技术现阶段存在的问题进行探索与研究，对共识机制和系统架构做出了新的改进。本文通过分析当前区块链共识机制存在的问题，提出了基于信用评分的主节点切换协议的 CBFT 共识算法，保障了区块链系统的安全性和活性。系统架构方面，本文设计多链架构，对请求进行并行处理，从而提升了区块链的 TPS。

本文一方面探索了区块链在扶贫场景的应用模式。另一方面，研究并设计了新的共识算法和系统架构，经过实验验证，提高了区块链系统的安全性和吞吐量。本论文是国内较早探索区块链在扶贫场景应用的研究，为区块链技术在中国的实际落地应用提供了借鉴经验。

1.4 研究现状

(1) 国内研究现状

区块链技术随着比特币的推广越来越受到社会各界的关注，2016 年是区块链这一概念被提出以来发展最为迅猛的一年。袁勇和王飞跃对区块链系统性的概括和研究对中国学术界对区块链的认识推上一个新的高度，他们认为区块链是随着比特币等数字加密货币的日益普及而逐渐兴起的一种全新的去中心化基础架构与分布式计算范式。目前国内学术界对于区块链的研究可分为三类，一是对数字货币与区块链的研究，比如杨晓晨等对比特币运行原理、典型特征、与前景展望的研究，陈道富等对比特币风险特征、监管建议的研究，这些学者的研究受到早期比特币的影响，仅仅把区块链认为是比特币的底层技术模块。第二种是对区块链技术在非数字货币场景中的应用，比如丁未对区块链在仪器数据管理中应用的研究，荣希对区块链在资产证券化中的应用的研究，黄永刚对区块链在电子健康档案安全建设中应用的研究。第三种是对区块链技术本身研究，随着越来越多

的学者意识到区块链是一个能够从数字货币剥离出来形成一种具有颠覆性和革命性的技术模式和技术架构，一些学者开始对区块链的支撑技术进行探索和研究。比如梁斌对区块链中共识算法的研究，张立钧和刘德林对区块链中智能合约的研究。

2016 年中国人民银行多批次发表了多篇关于中国法定数字货币的论文论证中国法定数字货币的可行性和奠定了中国法定数字货币的基本理论基础。范一飞提出了中国法定数字货币的理论依据和架构选择前构想了中国法定数字货币的原型。在数字货币的基础上，一些学者对基于中国法定数字货币的数字票据进行了探索性的研究。比如徐忠对中国数字票据交易平台初步方案的设计，无论从业务场景、技术架构、逻辑流程，徐忠都进行了系统性的阐述。聂舒从区块链的角度讨论了智能数字票据系统的概念验证原型。除了中国人民银行的学者和研究人员对数字票据的理论研究以外，任安军等学者也对区块链对原有票据体系的推动进行了研究。

狭义上的区块链虽然只是一种特殊的数据结构，但是广义上的区块链涵括了点对点通信、共识机制、分布式存储、加密算法等各类计算机技术，因此区块链是一个全面的计算机技术的综合体系，因此很多学者对区块链的相关技术也进行了研究和探讨。

在拜占庭共识机制的研究中，范捷等学者对拜占庭系统技术的定义和特点进行了深入的研究和讨论，范捷认为拜占庭将军问题和分布式系统是相似的。分布式系统的每一个服务器可以类比成将军，服务器之间的消息传递可以类比成信使，服务器可能会发生错误而产生错误的信息传达给其他服务器，同时范捷还对目前常用的拜占庭共识算法的优化方法进行了分析和比较。杨磊等学者对拜占庭共识机制在 P2P 存储系统中的容错率、稳定性等方面进行了全面剖析和讨论，概述了 P2P 存储系统容错的要求与技术，对现有拜占庭错误冗余技术进行了总结；详细分析对比了目前各种典型拜占庭容错系统的容错方式。探讨了 P2P 存储系统中拜占庭容错技术需要改进的关键问题。

与区块链相比，分布式存储研究在国内已经非常成熟了，特别是随着大数据、云计算等新兴技术飞速发展，分布式存储在理论研究和实际应用两方面都明显比区块链丰富。宫婧和李晓辉分别在大数据和云计算中分布式存储的应用和研究进行了深入的研究和总结。李晓辉指出云计算是“以互联网为载体,利用虚拟化等手段整合大规模分布式可配置的计算资源,使其以服务的方式提供给用户,满足用户按需使用的计算模式”。宫婧对大数据存储中容错技术进行详细分析和深入讨论，认为不断增长的海量数据需要被可靠存储,而分布式存储系统庞大的节点规

模和数据规模,大大提升了发生节点失效的概率,容错技术成为大数据存储中不可忽视的关键技术。虽然目前还没有学者把区块链与大数据、云计算等技术的结合起来进行研究和分析，但是随着区块链技术的普及，一定会涌现出很多学者对区块链与大数据和云计算统一起来展开研究。因为大数据和云计算都是在现在数据量和信息量爆发式增长的互联网时代诞生的计算机技术，而区块链最初的目的是为了追求数据的精准和明确，两者可以互补。

(2) 国外研究现状

与国内相比，国外关于区块链的研究时间比较早，研究的程度比较深，研究的方向比较全面，而且由于各个国家之间社会环境和文化上的不同，各个国家的学者研究区块链的角度也有所不同。

区块链因比特币而被世人熟知，国外对区块链研究最热的领域还是在金融领域。Kurt Fanning 全面分析了区块链在比特币中的作用，Kurt Fanning 认为区块链将对包括银行在内的金融机构的运营和交易模式产生巨大的改革和冲击。著名全球资讯公司埃森哲咨询公司在 M2 Presswire 中刊登了一篇文章，该文章的作者与 Kurt Fanning 相比对区块链持乐观和开放的态度，文章中指出区块链技术是对目前金融领域某些效率较低大大增加了时间和经济成本，特别是在跨国交易频繁的现代商业社会中。Kurt Fanning 和埃森哲咨询公司对区块链的不同态度也代表了现在国内外金融领域对区块链的两种态度，一种是对区块链充满危机感，认为区块链未来可能会对金融行业造成革命性的改变，对行业进行重新洗牌；而另一种态度就是认为区块链是能够解决现在金融领域一些传统技术无法解决的顽疾的良方。

除了在金融领域以外，国外很多研究人员认为区块链的价值绝不仅仅体现在金融领域中。Zyskind 等人着重于研究区块链在个人数据隐私保护，Zyskind 认为比特币验证了区块链去中心化的特点在金融领域中较好的保护了交易双方的隐私，因此区块链可以应用到第三方机构的个人数据隐私保护当中，Zyskind 还提出了一种不局限于金融领域的区块链应用模式，该模式能够在不存在第三方机构的情况下保证数据使用权限的可控管理。Patrick Nelson 在 Network World 上发表的文章用了大量的实例分析了区块链在总统选举中的应用前景，区块链改变目前美国大选投票站一人一票的模式，每个选举人在日常生活中与选举相关的一举一动都会通过区块链被记录下来，这样就规避了一人一票非黑即白的投票模式，避免投票人因为一时冲动错误投出选票的情况。Irving Grg 和他的同事认为区块链可以以较低的成本纠正药物科学研究中的实验过程和实验数据的造假等问题，Irving Grg 设计了一种基于区块链的科学实验校正和确认的原型机。

上述内容都是从行业应用的角度介绍区块链在国外的研究现状，国外也有很

多研究人员和学者对区块链本身的一些性质和特点进行了深入研究和讨论，还有Daniel Kraft 从时间复杂度的角度对比特币区块链生长速度进行研究分析和Sunny King 对区块链中常用的共识算法——PoS 和 PoW 进行了系统性的研究分析，对两种共识算法的性能、特点进行了比较分析。与国内相比较，国外对数字票据的研究进度与国内相似，都处于初级阶段，相关文献较少。不过国外在数字货币方面的研究成果比较丰富，本文借鉴了一些国外学者在数字货币方面的经验到数字票据的研究当中。在法定数字货币的研究当中，最具代表性的是 RScoin 和 BitMint 两种。两种数字货币的设计中都包含了法定货币从发行、流通、回笼完整的生命周期，更重要的是两种数字货币都考虑到了中央银行在货币体系中的地位和作用。

1.5 论文创新点

本文设计的基于区块链的扶贫资金管理平台具有以下三个创新点。

(1) 脱贫攻坚+区块链

区块链是一个新兴技术，本文系统性的对区块链在扶贫场景的应用进行了探索、研究、设计和实现。具有较强的创新意义和探索意义，为区块链技术在中国的落地实际应用提供了借鉴经验。

(2) 区块链共识机制创新

共识机制是区块链系统的核心与灵魂所在，在传统的区块链技术中，如比特币、以太坊等采用 PoW 共识机制，虽然 PoW 共识机制可以有效的保证区块链的可信性，并且很好的实现了去中心化，但是该算法依然存在诸如性能低下、高耗能、弱一致性等问题。针对以上问题，本论文提出了基于信用评分的主节点切换协议的 CBFT 共识算法，在保障区块链系统的一致性的前提下，提升了区块链的 TPS，降低了区块共识所需消耗的资源，提高了区块链系统的安全性。

(3) 区块链系统架构创新

区块链的性能一直是制约区块链发展的重要瓶颈。提高区块链系统的吞吐量，提高区块链对其上层业务的处理能力，才能应对更多的应用场景。本文经过研究，对区块链系统架构进行了优化和改进，设计多链架构，对请求进行并行处理，结合优化后的共识机制提升了区块链的 TPS。

1.6 论文结构

本文共有七个章节，具体章节安排如下：

第一章，介绍了论文的研究背景、研究问题、研究意义、国内外对区块链的研究现状和存在的问题、论文创新点以及论文结构。

第二章，介绍了区块链的设计思想、类型、特征和核心技术，并分析对比了当前主流的区块链技术。

第三章，分析当前区块链共识机制存在的问题，提出了基于信用评分的主节点切换协议的 CBFT 共识算法，在保障区块链系统一致性的前提下，降低了区块共识所需消耗的资源，提高了区块链系统的安全性。

第四章，对底层区块链系统架构进行了优化和改进，设计多链架构，对请求进行并行处理，结合优化后的共识机制进一步提升区块链的性能。

第五章，对改进后的共识算法和多链架构进行 TPS 测试。

第六章，详细分析了“脱贫攻坚+区块链”的实现方式，并详细介绍了该平台的技术架构、技术路线、技术选型、系统全貌。

第七章，对全文工作进行总结，并给出下一步的工作计划与前景展望。

第2章 区块链相关技术

2.1 概述

区块链技术起源于化名为“中本聪”（Satoshi Nakamoto）的学者在 2008 年发表的奠基性论文《比特币：一种点对点电子现金系统》。狭义来讲，区块链是一种按照时间顺序将数据区块一顺序相连的方式结合成的一种链式数据结构，并以密码学方式保证的不可篡改和不可伪造的分布式账本。广义来讲，区块链技术是利用块链式数据结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学的方式保证数据传输和访问的安全、利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算范式。

目前，区块链技术被很多大型机构称为是彻底改变业务乃至机构运作方式的重大突破性技术。同时，就像云计算、大数据、物联网等新一代信息技术一样，区块链技术并不是单一信息技术，而是依托于现有技术，加以独创性的组合及创新，从而实现以前未实现的功能。

至今为止，区块链技术大致经历了 3 个发展阶段，如图 2.1 所示。

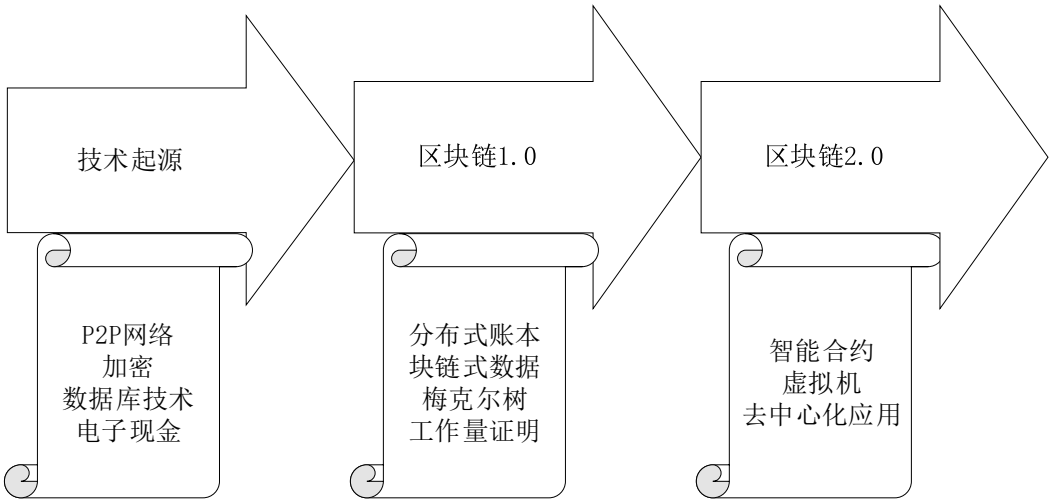

图 2.1 区块链发展阶段

价值交互的基础是双方信任的建立。区块链技术的革命性在于它实现了一种全新的信任方式，通过在技术层面的设计创新，使得价值交互过程中人与人的信任关系能够转换为人与技术的信任，甚至于由程序自动化执行某些环节，商业活动得以更低成本的实现。

(1) 经济层面的设计思想

降低成本，是区块链技术的一个重要的设计思路。在区块链体系中，参与者可以不需要了解对方基本信息的情况进行交易，实现了“无需信任的信任”，改变了传统模式中以第三方为中心的信任模式。

这种设计模式有许多创新性，其中两项值得关注：

第一，交易信任由机器和算法确定。区块链通过构建一个信赖于机器和算法信任的交易体系，解决在匿名交易过程中的互相信任问题。所有参与者将在无需建立信任关系的环境中，通过密码学原理确定身份，依靠共识机制实现相互间的信任。

第二，交易过程可以由程序自动执行。区块链通过可编程的智能合约，自动执行双方所达成的契约，排除了认为的干扰因素，从制度上防止任何一方的抵赖。从而推动经济社会进入一种智能的状态，实现当前经济交易系统的质的飞跃。

基于区块链技术的“弱中心化”特征，现有的经济体系可以脱离当前通过制度约束或第三方机构背书，双方直接实现价值交付。这种“弱中心化”特征可以有效降低交易成本，提高交易效率，减少因交易一致性所引发的摩擦。

(2) 技术层面的设计思想

通俗的说，区块链可以看成是一套由多方参与的、可靠的分布式数据存储系统，其独特之处在于：一是记录行为的多方参与，即各方可参与记录；二是数据存储的多方参与、共同维护，即各方均参与数据的存储和维护；三是通过链式存储与合约，并且只能读取和写入，不可篡改。

在应用实践中，这种系统能够实现所有参与者信息共享、共识、共担，可以成为各种商业行为和组织机构的基础技术架构。具体与传统中心式系统对比如下表所示：

表 2.1 区块链与传统技术对比

关键点 系统分类		传统技术系统		区块链技术系统	
		特点	中心化的实现方式	特点	去中心化的实现方式
记录行为的多方参与	网络架构	中心化	主从式的 B/S 网络	去中心化	P2P 分布式网络
	记录权及记录方式	中心节点进行	中心节点记录及维护所有交易数据	所有节点参与	共识算法确定记录权，共同维护交互数据
	交易方	每笔交易需中	中心节点监督	点对点交易	所有节点集体

	式	心节点确认	和维护		监督和见证
	信任关系	中心节点见证	中心节点为所有节点进行信任背书	节点自证其信	非对称加密技术验证身份，零知识证明等方式验证信息
	交易一致性	中心节点保障交易数据的一致性	中心节点的一本账，保障交易数据的一致性	所有节点共同参与解决数据交易的一致性	所有节点通过共识算法保障交易一致性，解决双花现象
账数据存储的多方维护	交易有无欺诈	存在欺诈和造假的可能	中心节点主动欺诈的可能	不可欺诈、不可造假	分布式存储、共识算法
	信息被篡改	存在数据被篡改和抵赖的可能性	中心节点存在被攻击、数据被篡改等可能性	不可篡改、不可抵赖	分布式存储、链式数据结构、哈希算法、时间戳及数字签名
	数据存储的可靠性	中	依靠中心节点进行交易信息系统的存储和容灾备份	高	任意单个节点故障或者少数节点故障，系统能正常运行，并且故障节点数据可以恢复
	隐私保护	交易双方身份信息存在泄漏的可能性	所有参与交易者需提供身份信息，且都由中心节点保存，中心节点存在被攻击、盗取等可能，导致交易者的隐私泄漏	交易双方的身份信息不会被泄漏	所有参与方在区块链中通过加密后的 ID 进行标识。 1.需要所有交易者提供身份隐私信息，保障交易者的隐私不被泄漏。 2.同一个交易者可通过多个 ID 进行的多次交

					易来达到隐私保护的目的。

2.2 区块链的类型

根据区块链的开放程度，可以将区块链分为公有链、联盟链和私有链。但是随着区块链技术的快速发展，各种类型的链之间的界限慢慢也将变得模糊，特别是随着节点上所运行的智能合约所包含业务逻辑越来越复杂，私有链上的部分节点必须对外开放才能执行完整的业务逻辑，而部分共识及记账节点则会约束仅向许可节点开放保证效率和可控性，各种链之间的业务界限会逐渐模糊。三种链之间的对比，如表 2.2 所示。

表 2.2 三种区块链对比

	公有链	联盟链	私有链
参与者	任何人	授权的公司和组织	个体或一个公司内
记账人	任何人	参与者协调授权控制	自定
信任机制	工作量证明等	集体背书	自行背书
中心化程度	去中心化	多中心化	中心化
突出优势	信用的自建立	效率、成本优化	透明、可追溯
典型应用场景	比特币	清算	审计

2.3 区块链的特征

(1) 去中心化

去中心化是区块链最基本的特征，意味着区块链应用不依赖于中心化的机构，实现了数据的分布式记录、存储与更新。在传统的中心化网络中，业务运行高度依赖中心节点的稳健性与可信性，黑客若对单一的中心节点进行攻击即可破坏整个系统。而区块链的分布式架构中全网节点的权利和义务均等，系统中的数据是由全网节点共同基于密码学规则进行维护的，具有点对点、多冗余等特性，不存在单点失效的问题，因此其应对拒绝服务攻击的方式比中心化系统要灵活得多。即使一个节点失效，其他节点不受影响。

(2) 透明性

区块链系统的数据记录对全网节点是透明的，数据记录的更新操作对全网也是透明的，这是区块链系统值得信任的基础。由于区块链系统使用开源的程序、开放的规则和高参与度，区块链的数据记录和运行规则可以被全网节点审查、追溯，具有很高的透明度。

(3) 开放性

区块链的开放性是指，除数据直接相关各方的私有信息被加密外，区块链的所有数据对所有人公开（具有特殊权限要求的区块链系统除外）。任何人或参与节点都可以通过公开的接口查询区块链的数据记录或者开发相关应用，因此整个系统是开放的。

(4) 自治性

区块链采用基于协商一致的规范和协议，使整个系统中的所有节点能够在去信任的环境下自由安全地交换、记录以及更新数据，把对个人或机构的信任改成对体系的信任，任何人为的干预都将不起作用。

(5) 不可篡改性

区块链中有两套加密机制防止记录篡改，第一是采用默克尔树的方式加密交易记录，当底层数据发生改动时，必会导致默克尔树的根哈希值发生变化；第二是在创建新的区块时放入了前一区块的哈希值，这样区块之间形成链接关系，若想改动之前区块的交易数据，必须将该区块之前的所有区块的交易记录和哈希值进行重构，这是很难达到的，除非能够同时控制系统中超过 51%的节点，否则单个节点上对区块中记录的修改是无效的，因此区块链的数据的稳定性和可靠性极高。

(6) 匿名性

区块链系统中虽然所有数据记录和更新操作过程都是对全网节点公开的，但其交易者的私有信息仍是通过哈希加密处理的，即数据交换和交易都是在匿名的情况下进行的。由于节点之间的数据交换遵循固定且预知的算法，因而其数据的交互无需双方存在相互信任的前提，可以通过双方地址而非身份的方式进行，因此交易双方无须通过公开身份的方式让对方产生信任。

2.4 区块链的核心技术

2.4.1 共识机制

共识机制是区块链技术的一个核心问题，它决定了区块链中区块的生成法则，保证了各节点的诚实性、账本的容错性和系统的稳健性。常用的共识机制主

要有 PoW、PoS、DPoS 等。基于区块链技术的不同应用场景，以及各种共识机制的特性，主要可以从性能效率、资源消耗、容错性、监管水平等几个方面进行评价和比较。

(1) PoW

PoW 的定义简单来说就是工作端提交已知难于计算但易于验证的计算结果，而其他任何人都能够通过验证这个答案就确信工作端为了求得结果已经完成大量的计算工作。PoW 工作量证明的主要特征是计算的不对称性。根据机器的运算资源来分配记账权，由于参与运算的不同节点根据自身的运算资源获取记账权，所以这些节点在竞争结束前都要一直进行哈希运算，资源消耗较高。而众多参与节点中最终只会产生一名记账者，性能效率比较低。其典型应用为比特币。

(2) PoS

PoS 指的是所有权证明，节点通过拥有的所有权的证明获得产生新区块的权利。根据节点持有的所有权的数量和时间来等比例地降低挖矿难度，这样节点记账权的获得难度与节点持有的权益成反比，与 PoW 所有机器同等挖矿难度相比，这种方法在一定程度减少了数学运算难度，各节点资源消耗减少，性能也得到了一些提升。但由于在挖矿时仍是基于哈希运算竞争的方式，可监管性弱，共识机制容错性也和 PoW 相同。典型应用为点点币（Peercoin）。

(3) DPoS

PoW 与 PoS 机制都能有效的解决记账行为的一致性共识问题，但 PoW 中拥有巨大算力的一方容易成为另一个中心，而 PoS 机制中会产生所有权比例越大的账户拥有的权力更大。DPoS 机制致力于解决 PoW 机制和 PoS 机制的这类不足。DPoS 机制中，可由区块链网络主体投票产生 N 个见证人来对区块进行签名，其根本特性是权益所有者保留了控制权从而使系统去中心化。通过信任少量诚信节点减少了确认要求，提高了交易速度，因此，性能、资源消耗都要优于 PoS。其合规监管、容错性与 PoS 相似。其典型应用为比特股（BitShares）。

2.4.2 智能合约

智能合约（Smart Contract）由尼克·萨博（Nick Szabo）于 1995 年提出，他给出的定义是：“一个智能合约是一套以数字形式定义的承诺，包括合约参与方可以在上面执行这些承诺的协议。”

区块链中的智能合约可视作一段部署在区块链上由事件驱动，具有状态的，获得多方承认的，可自动运行、无须人工干预，且能够根据预设条件自动处理资产的程序，从本质上讲，智能合约的工作原理类似于计算机程序中的 if-then 语句，当一个预先编好的条件被触发时，智能合约执行便相应的条款程序。由于智

能合约运行在图灵完备的虚拟机上，因此智能合约的具体条款可以根据应用场景由开发人员编写，其具体的技术细节又包括编程语言、编译器、虚拟机、事件、状态机、容错机制等。但由于智能合约本质上是一段程序，存在出错的可能性，因此需要做好充分的容错机制，通过系统化的手段，结合运行环境隔离，确保合约的正确执行。

2.4.3 安全技术

(1) 哈希算法

哈希算法也叫数据摘要或者散列算法，其原理是将一段信息映射成一个固定长度的二进制值，该二进制值称为哈希值。哈希值具有以下特点：

✧ 若某两段信息相同，则他们经过哈希运算得到的哈希值也相同。

✧ 若两段信息不同，即使只是相差一个字符，他们产生的哈希值也会不同且杂乱无章毫无关联。

要找到哈希值为同一值得两个不同输入，在计算上是不可能的，因此数据的哈希值可以被用以检验数据的完整性，可以把给定数据的哈希值理解为该数据的“指纹信息”。本质上，散列算法的目的不是为了“加密”而是为了抽取“数据特征”。

典型的哈希算法有 MD5（Message Digest Algorithm，消息摘要算法第五版）、SHA1/SHA256 和 SM3（SM3 密码杂凑算法）等，各算法特点的对比，如表 2.3 所示。

目前区块链主要使用 SHA256，国内某些特定业务场景使用国密 SM3，亦是比较符合国家安全和监管的选择。SHA256 和 SM3 这两种算法的效率和安全性大致相当，但由于不同业务场景的安全性标准有别，未来不排除仍需探索更优算法的可能性。

表 2.3 典型哈希算法的特点

加密算法	安全性	运算速度	输出大小（位）
MD5	低	快	128
SHA1	中	中	160
SHA256	高	比 SHA1 略低	256
SM3	高	比 SHA1 略低	256

(2) 非对称加密算法

非对称加密算法是区块链基础技术之一，区块链中使用非对称加密的公私钥对来构建节点间信任。非对称加密算法由对应的一对唯一的密钥（即公开密钥和私有密钥）组成，任何获悉用户公钥的人都可用用户的公钥对信息进行加密与用户实现安全信息交互。由于公钥与私钥之间存在依存关系，只有持有私钥的用户本身才能解密该信息，任何未经授权的用户甚至信息的发送者都无法将此信息解密。

常用的非对称加密算法主要有 RSA、ECC 以及 SM3，其特点比较如表 2.4 所示。具体算法的技术细节将在本书后续章节进行讨论。

表 2.4 常用非对称加密算法的特点

加密算法	成熟度	安全性	运算速度	资源消耗
RSA	高	低	慢	高
ECC	高	高	中	中
SM3	高	高	中	中

2.4.4 分布式存储

(1) 区块数据结构

在区块链中，数据以区块的方式永久储存。区块链的时间戳解决了区块的排序问题，新区块生成时便记录着上一个区块通过哈希计算得到的哈希值，实现了区块密码学链接。每一个区块记录了其创建期间发生的所有交易信息。区块的数据结构一般分为区块头和区块体，其中，区块头部结构记录了版本号、前一个区块的哈希值、默克尔树的根值、时间戳、目标特征值和随机数值；区块体部分则包含了经过验证的、区块创建过程中产生的所有交易信息。区块主标识符是它的加密哈希值，一个通过 SHA256 算法对区块头进行二次哈希计算而得到的数字指纹，产生的 32 字节哈希值被称为区块头哈希值。第二种识别区块的方式是按照该区块在区块链中的位置，即“区块高度”，如第一个区块，其区块高度为 0。区块链的数据结构，如图 2.2 所示。

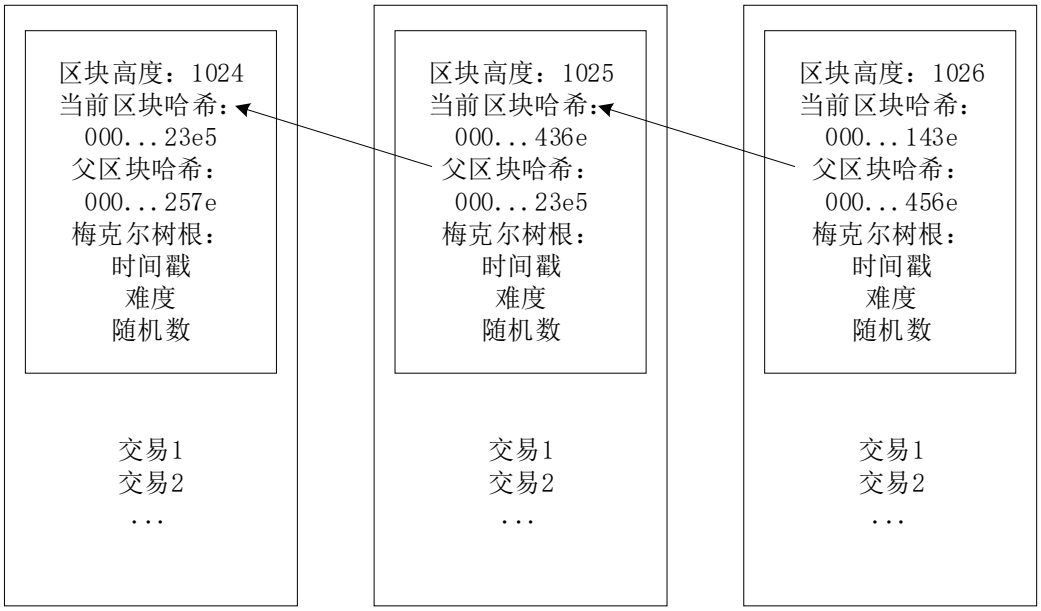

图 2.2 区块链数据结构

(2) 数据库

区块链中关系型和非关系型两种数据库均可采用。其中，关系型数据库采用关系模型来组织数据，支持各种 SQL（Structured Query Language，结构化查询语言）功能，功能性强，支持事务性，读写性能一般，可扩展性弱，在数据存在海量并发情况下表现较差。而非关系型数据库中键值对数据库的数据结构组织形式简单，读写性能很高，支持海量并发读写请求，可扩展性强，操作接口简单，支持一些基本的读、写、修改、删除等功能，但不支持复杂的 SQL 功能和事务。

根据数据库的部署形式，可分为单机型和分布式两种。其中，单机型数据库保证强一致性和较好的可用性。分布式数据库在物理部署上遵循了分布式架构，能提供高并发的读写性能和容错，有很强的可用性和分区容错性，但由于需要进行数据同步，分布式架构的数据一致性较弱，只能保证最终一致性。

在区块链中，如果待存储的是一些字符串、json 对象，可以使用扩展账本结构链存储；如果是图片、视频等较大的多媒体文件，可以将文件的哈希值存储在链上，而原文件可使用云存储存储到云端。

2.5 主流区块链技术介绍

2.5.1 比特币

2.5.1.1 重要概念

(1) 账户/地址

比特币采用了非对称的加密算法，用户自己保留私钥，对自己发出的交易进行签名请确认，并公开公钥。

比特币的账户地址其实就是用户公钥经过一系列 Hash（Hash160，或先进行 SHA256，然后进行 RIPEMD160）及编码运算后生成 160 位（20 字节）的字符串。

一般地，对账户地址串进行 Base58Check 编码，并添加前导字节（表明支持哪种脚本）和 4 字节校验字节，以提高可读性和准确性。

(2) 交易

交易是完成比特币功能的核心概念，一条交易可能包括如下信息：

✧ 付款人地址：合法的地址，公钥经过 SHA256 和 RIPEMD160 两次 Hash，得到 160 位 Hash 串。

✧ 付款人对交易的签名确认：确保交易内容不被篡改。

✧ 付款人资金的来源交易 ID：哪个交易的输出作为本次交易的输入。

✧ 交易金额：多少钱，与输入的差额为交易的服务费。

✧ 收款人地址：合法的地址。

✧ 收款人公钥：收款人的公钥。

✧ 时间戳：交易何时能生效。

✧ 网络中节点收到交易信息后，将进行如下检查：

✧ 交易是否已经处理过。

✧ 交易是否合法，包括地址是否合法、发起交易者是否输入地址的合法拥有者、是否是 UTXO。

✧ 交易的输入之和是否大于输入之和。

如果检查都通过，则将交易标记为合法的未确认交易，并在网络内进行广播。

(3) 交易脚本

脚本（script）是保障交易完成（主要用于检验交易是否合法）的核心机制，当所依附的交易发生时被触发。通过脚本机制而非写死交易过程，比特币网络实现了一定的可扩展性。比特币脚本语言是一种非图灵完备的语言，类似于 Forth

语言。

一般每个交易都会包括两个脚本：输入脚本（scriptPubKey）和认领脚本（scriptSig）。输出脚本一般由付款方对交易设置锁定，用来对能动用这笔交易输出（例如，要花费交易的输出）的对象（收款方）进行权限控制，例如限制必须是某个公钥的拥有者才能花费这笔交易。认领脚本则用来证明自己可以满足交易输出脚本的锁定条件，即对某个交易的输出（比特币）的拥有权。

(4) 区块

比特币区块链的一个区块主要包括如下内容：

表 2.5 比特币区块内容

字段名称		字段说明
神奇数		神奇数是一个等于 0xD9B4BEF9 的常数，用于区分区块间的间隔，长度为 4 字节。
区块大小		区块大小是指从区块开始到区块结束的字节数，长度为 4 字节。
区块头部信息	版本号	版本号是区块的版本号，长度为 4 字节。
	前一个区块地址	前一个区块 HASH 值，长度为 32 字节。
	Merkle 树根节点	记录了当前区块中所有交易 Merkle 树的根节点的 HASH 值，长度为 32 字节。
	时间戳	记录了当前区块生成的时间，按照 UNIX 时间格式，长度为 4 字节。
	目标值	当前区块生成所达成目标值的特征，用于挖矿时的工作量证明和比特币的“发行”，长度为 4 字节。
	随机数	当前区块工作量证明的参数，长度为 4 字节。
交易计数		当前区块所记录的交易数，长度为 1 至 9 字节。
交易详情		记录了当前区块保存的所有交易细节，长度不确定。

可见，要对区块链的完整性进行检查，只需要检查各个区块头信息即可，无需获取具体的交易内容，这也是简单交易验证（simple payment verification,SPV）的基本原理。另外，通过头部的链接，提供时序关系的同时加大了对区块中数据进行篡改的难度。

2.5.1.2 基本交易过程

每次发生交易，用户需要将新交易记录写到比特币区块链网络中，等网络确

认后即可认为交易完成。每个交易包括一些输入和一些输出，未经使用的交易的输出（unspent transaction output,UTXO）可以被新的交易引用作为合法的输入，被使用过的交易的输出（spent transaction output,STO）则无法被引用作为合法输入。

一笔合法的交易，即引用某些已存在的交易的 UTXO 作为交易的输入，并生成新的输入的过程。

在交易过程中，转账方需要通过签名脚本来证明自己是 UTXO 的合法使用者，并且指定输出脚本来限制未来本交易的使用者（为收款方）。对每笔交易，转款方需要进行签名确认。并且，对每一笔交易来说，总输入不能小于总输出。总输入相比总输出多余的部分称为交易费用（transac fee），为生成包含该交易区块的矿工所获得。目前规定每笔交易的交易费用不能小于 0.0001BTC，交易费用越高，越多矿工愿意包含该交易，也就越早被放到网络中。交易费用在奖励矿工的同时，也避免了网络受到大量攻击。

2.5.1.3 创新设计

(1) 避免作恶

避免作恶基于经济博弈原理。在一个开放的网络中，无法通过技术手段来保证每个人都是合作的。单可以通过经济博弈来让合作者得到利益，让非合作者遭受损失和风险。

比特币网络中所有试图参与者（矿工）都首先要付出挖矿的代价，进行算力小号，越想拿到新区块的决定权，意味着抵押的算力越多。一旦失败，这些算力都会被没收掉，称为沉没成本。当网络中存在众多参与者时，个体试图拿到新区块决定权要付出的算力成本是巨大的，意味着进行一次作恶付出的代价已经超过可能带来的好处。

(2) 负反馈调节

比特币网络中矿工越多，系统就越稳定，比特币价值就越高，但挖到矿的概率会越低。反之，网络中矿工减少，会让系统更容易被攻击，比特币价值降低，但挖到矿的概率提高。

因此，比特币的价格理论上应该稳定在一个合适的值（网络稳定性也会稳定在响应的值），这个价格乘以挖到矿的概率，恰好达到矿工的收益预期。

从长远角度看，硬件成本是下降的，但每个区块的比特币奖励每隔 4 年减半，最终将在 2140 年达到 2100 万枚，之后将完全依靠交易的服务费来奖励矿工对网络的维护。

(3) 共识机制

传统共识问题往往是考虑在一个相对封闭的分布式系统中，允许同时存在正常节点、故障如何快速达成一致。

对于比特币网络来说，它是完全开放的，可能面对各种攻击情况，同时基于 Internet 的网络质量只能保证“尽力而为”，导致问题更为复杂，传统的一致性算法在这种场景下难以使用。

因此，比特币网络不得不对共识的目标和过程进行一系列限制，提出了基于 proof of work 的共识机制。

首先是不实现面向最终确认的共识，而是基于概率、随时间逐步增强确认的共识。现有达成的结果在理论上可能被推翻，只是攻击者要付出的代价随时间而指数级上升，被推翻的可能性随之指数级下降。

此外，考虑到 Internet 的尺度，达成共识的时间相对比较长，因此按照区块来进行阶段性的确认（快照），从而提高网络整体的可用性。

最后，限制网络中共识的噪音。通过进行大量的 Hash 计算和少数的合法结果来限制合法提案的个数，进一步提高网络中共识的稳定性。

2.5.2 以太坊

作为公有区块链平台，以太坊将比特币针对数字货币交易的功能进一步进行了拓展，面向更为复杂和灵活的应用场景，支持了智能合约这一重要特性。

从此，区块链技术的应用场景，从单一基于 UTXO 的数字货币交易，延伸到图灵完备的通用计算领域。用户不在受限于仅能使用比特币脚本所支持的简单逻辑，而是可以自行设计任意复杂的合约逻辑。这就为构建各种多样化的上层应用开启了大门，意义重大。

2.5.2.1 主要特点

以太坊区块链底层也是一个类似比特币网络的 P2P 网络平台，智能合约运行在网络中的以太坊虚拟机里。网络自身是公开可接入的，任何人都可以接入并参与网络中数据的维护，提供运行以太坊虚拟机的资源。

与比特币项目相比，以太坊区块链的技术特点主要包括：

✧ 支持图灵完备的智能合约，设计了变成语言 Solidity 和虚拟机 EVM。

✧ 选用了内存需求较高的哈希函数，避免出现强算力矿机、矿池攻击。

✧ 叔块激励机制，降低矿池的优势，并减少了区块产生间隔（10 分钟降低到 15 秒左右）。

✧ 采用账户系统和世界状态，而不是 UTXO，容易支持更复杂的逻辑。

✧ 通过 Gas 限制代码执行指令数，避免循环执行攻击。

✧ 支持 PoW 共识算法，并计划支持效率更高的 PoS 算法。

2.5.2.2 重要概念

(1) 智能合约

智能合约是以太坊中最为重要的一个概念，即以计算机程序的方式来缔结和运行各种合约。最早在上世纪 90 年代，Nick Szabo 等人就提出过类似的概念，但一直因为缺乏可靠执行智能合约的环境，而被当做一种理论设计。区块链技术的出现，恰好补充了这一缺陷。

以太坊支持通过图灵完备的高级语言（包括 Solidity、Serpent、Viper）等来开发智能合约。智能合约作为运行在 EVM 中的应用，可以接受来自外部的交易请求和事件，通过触发运行提前编写好的代码逻辑，进一步生成新的交易和事件，可以进一步调用其他智能合约。

智能合约的执行结果可能对以太坊网络上的账本状态进行更新。这些修改由于通过了以太坊网络中的共识，一旦确认后无法被伪造和篡改。

(2) 账户

相对于比特币采用了 UTXO 模型记录整个系统的状态，任何人都可以通过交易历史来推算出用户的余额信息。而以太坊直接用账户来记录系统状态。每个账户余额信息、智能合约代码和内部数据存储等。以太坊支持在不同账户之间转移数据，以实现更为复杂的逻辑。

具体来看，以太坊账户分为两种类型：合约账户（contracts accounts）和外部账户（externally owned accounts,EOA）:

✧ 合约账户：存储执行的智能合约代码，只能被外部账户来调用激活。

✧ 外部账户：以太币拥有者账户，对应到某公钥。

当合约账户被调用时，存储其中的智能合约会在矿工处的虚拟机中自动执行，并消耗一定的燃料。燃料通过外部账户中的以太币进行购买。

(3) 交易

交易在以太坊中是指从一个账户到另一个账户的消息数据。消息数据可以是以太币或者合约执行参数。

以太坊采用交易作为执行操作的最小单位。每个交易包括如下字段：

✧ to：目标账户地址。

✧ value：可以指定转移的以太币数量。

✧ nonce：交易相关的字串。

✧ gasPrice：执行交易需要消耗的 Gas 价格。

✧ startgas：交易消耗的最大 gas 值。

✧ signature：签名信息。

类似于比特币网络，在发送交易时，用户需要交纳一定的交易费用，通过以太币方式进行支付和消耗。

(4) 以太币

以太币（Ether）是以太坊网络中的货币。

以太币主要用于购买燃料，支付给矿工，以维护以太坊网络运行智能合约的费用。以太币最小单位是 wei，一个以太币等于 10^18 个 wei。

以太币同样可以通过挖矿来生成，成功生成新区快的以太坊矿工可以获得 5 个以太币的奖励，以及包含在区块内交易的燃料费用。

(5) 燃料

燃料（gas），控制某次交易执行指令的上限。每执行一条合约指令会消耗固定的燃料，当某个交易还未执行结束，而燃料消耗完时，合约执行终止并回滚状态。

gas 可以跟以太币进行兑换。需要注意的是，以太币的价格是波动的，单运行某段智能合约的燃料费用是固定的，通过设定 gas 价格等进行调节。

2.5.2.3 创新设计

(1) 智能合约

以太坊采用 EVM 作为智能合约的运行环境。EVM 是一个隔离的轻量级虚拟机环境，运行在其中的智能合约代码无法访问本地网络、文件系统或其他进程。

对同一个智能合约来说，往往需要在多个 EVM 中同时运行多份，以确保整个区块链数据的一致性和高度的容错性。

智能合约编写完毕后，用编译器编译为 EVM 专用的二进制格式（EVM bytecode），由客户端上传到区块链中，之后在矿工的 EVM 中执行。

(2) 共识

以太坊目前采用了基于成熟的 PoW 共识的变种算法 Ethash 协议作为共识机制。

为了防止 ASIC 矿机矿池的算力攻击，跟原始 PoW 的计算密集型 Hash 运算不同，Ethash 在执行时候需要消耗大量内存，反而跟计算效率关系不大。这意味着很难制造出专门针对 Ethash 的新票。

以太坊有计划在未来采用更搞笑的 PoS 作为共识机制。相对于 PoW 机制来讲，PoS 机制无需消耗大量无用 Hash 计算，但其共识过程的复杂度要更高。

(3) 降低攻击

由于以太坊网络中的交易更加多样化，也就更容易受到攻击。

以太坊网络在降低攻击方面的核心设计思想仍是通过经济激励机制防止少数作恶：

✧ 所有交易都要提供交易费用，避免 DDoS 攻击；

✧ 程序运行指令数通过 gas 来限制，所消耗的费用超过设定上限时就会被取消，避免出现恶意合约。

这就确保了攻击者试图消耗网络中虚拟机的计算资源时，需要付出经济代价；同时难以通过构造恶意的循环或不稳定合约代码来对网络造成破坏。

2.5.3 超级账本

超级账本（hyperledger）是 Linux 基金会于 2015 年发起的首个面向企业应用场景的开源分布式账本平台。

如果说以比特币为代表的数字货币提供了区块链技术应用的原型，以太坊为代表的智能合约平台延伸了区块链技术的功能，那么进一步引入权限控制和安全保障的超级账本项目则开拓了区块链技术的全新领域。超级账本首次将区块链技术引入到了分布式联盟账本的应用场景，这就为未来基于区块链技术打造高效率的商业网络打下了坚实的基础。

2.5.3.1 核心特性

超级账本 Fabric 架构的核心特性主要包括：

✧ 解耦了原子排序环节与其他复杂处理环节，消除了网络处理瓶颈，提高可扩展性。

✧ 解耦交易处理节点的逻辑角色为背书节点、确认节点，可以根据负载进行灵活部署。

✧ 加强了身份证书管理服务，作为单独的 Fabric CA 项目，提供更多功能。

✧ 支持多通道特性，不同通道之间的数据彼此隔离，提高隔离安全性。

✧ 支持可插拔的架构，包括共识、权限管理、加解密、账本机制等模块，支持多种类型。

✧ 引入系统链码来实现区块链系统的处理，支持可编程和第三方实现。

2.5.3.2 重要概念

(1) 节点

节点（Peer）的概念最早来自于 P2P 分布式网络，意味着在网络中担任一定职能的服务或软件。节点功能可能是对等一致的，也可能是分工合作的。

在超级账本 Fabric 网络中，Peer 意味着在网络中负责接收交易请求、维护一致账本的各个 fabric-peer 实例。这些实例可能运行在裸机、虚拟机甚至容器中。节点之间彼此通过 gRPC 消息进行通信。

按照功能角色划分，Peer 可以包括三种类型：

✧ 背书节点（endorser）：负责对来自客户端的交易提案进行检查和背书。

✧ 确认节点（committer）：负责检查交易请求，执行交易并维护区块链和账本结构。

✧ 提交节点（submitter）：负责接收交易，转发给排序者。

(2) 排序者

排序者（orderer）也称为排序节点，负责对所收到的交易在网络中进行全局排序。

Orderer 主要提供了 Broadcast 和 Deliver 两个接口。前者代表客户端将数据（交易）发送给 Orderer，后者代表从 Orderer 获取排序后构造的区块结构。

(3) 成员身份管理

CA 节点负责对 Fabric 网络中的成员身份进行管理。

Fabric 网络目前采用数字证书机制来实现对身份的鉴别和权限控制，CA 节点则实现了 PKI 服务，主要负责对身份证书进行管理，包括生成、撤销等。

2.5.3.3 整体架构

超级账本 Fabric 的整体框架如图 2.3 所示

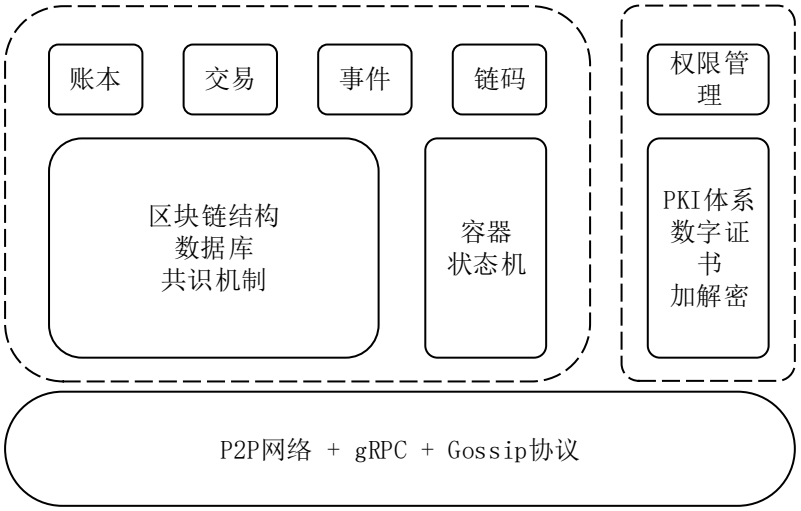

图 2.3 Fabric 整体架构图

其中账本是最核心的结构，负责记录应用信息，应用则通过发起交易来向账本中记录数据。交易执行的逻辑通过链码来承载。整个网络运行中发生的时间可以被应用访问，以触发外部流程甚至其他系统。权限管理则负责整个过程中的访问控制。

账本和交易进一步地依赖核心的区块链结构、数据库、共识机制等技术；链码则依赖容器、状态机等技术；权限管理利用已有的 KPI 体系、数字证书、加解密算法等诸多安全技术。

底层由多个节点组成 P2P 网络，通过 gRPC 通道进行交互，利用 Gossip 协议进行同步。

2.5.3.4 典型工作流程

典型的交易处理过程示例如图 2.4 所示

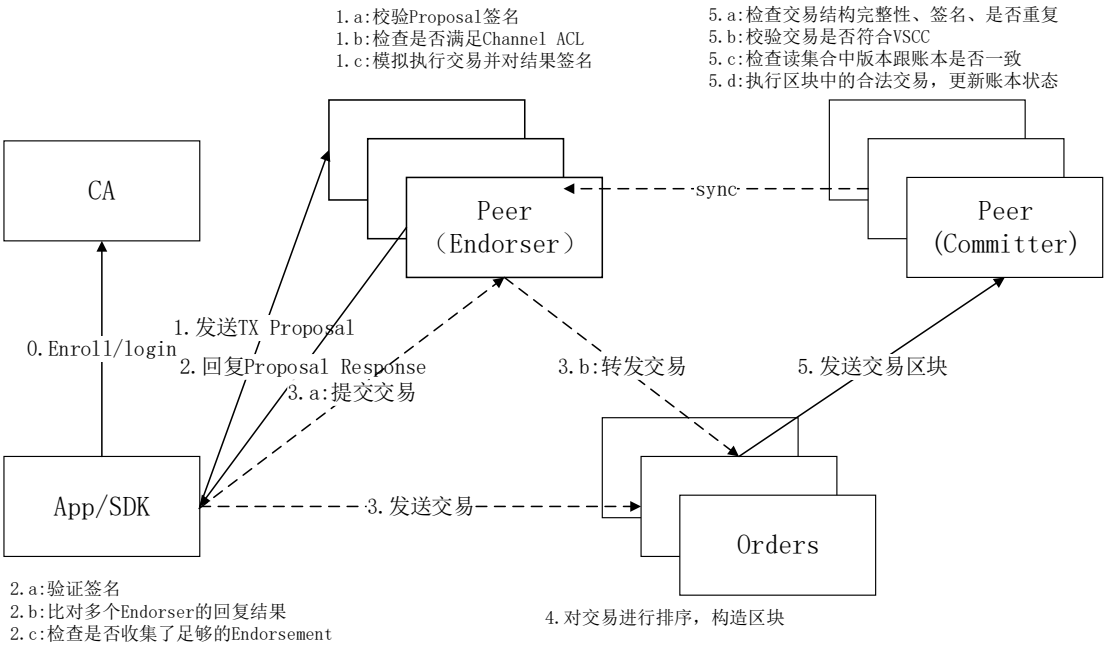

图 2.4 Fabric 交易处理流程

在整个交易过程中，各个组件的主要功能如下：

(1) 客户端（App）

客户端应用使用 SDK 来跟 Fabric 网络打交道。首先，客户端从 CA 获取合法的身份证书来加入网络内的应用通道。发起正式交易前，需要先构造交易提案提交给 Endorser 进行背书，客户端收集到足够的背书支持后可以利用背书构造一个合法的交易请求，发给 Orderer 进行排序处理。

(2) Endorser 节点

主要提供 ProcessProposal 方法供客户端调用，完成对交易提案的背书处理。收到来自客户端的交易提案后，首先进行合法性和 ACL 权限检查，检查通过则模拟运行交易，对交易导致的状态变化（以读写集形式记录，包括所读状态的键和版本，所写状态的键值）进行背书并返回结果给客户端。

(3) Committer 节点

负责维护区块链和账本结构（包括状态 DB、历史 DB、索引 DB 等）。该节点会定期地从 Orderer 获取排序后的批量交易区块结构，对这些交易进行落盘前的最终检查（包括交易消息结构、签名完整性、是否重复、读写集合版本是否匹配等）。检查通过后执行合法的交易，将结果写入账本，同时构造新的区块，更新区块中的 BlockMetadata[2]（TRANSACTIONS_FILTER）记录交易是否合法等信息。同一个物理节点可以仅作为 Committer 角色运行，也可以同时担任 Endorser 和 Committer 这两种角色。

(4) Orderer

仅负责排序。为网络中所有合法交易进行全局排序，并将一批排序后的交易组合生成区块结构。

(5) CA

负责网络中所有证书的管理（分发、撤销等），实现标准的 PKI 架构。

第3章 共识机制的研究与优化

3.1 痛点分析

共识机制是区块链系统的核心与灵魂所在，在传统的区块链技术中，如比特币、以太坊等采用 PoW 共识机制，虽然 PoW 共识机制可以有效的保证区块链的可信性，并且很好的实现了去中心化，但是该算法依然存在如下几类问题：

(1) PoW 共识机制需要进行大量的计算来证明工作量，算力的竞争会造成大量算力的浪费和资源的消耗。

(2) PoW 共识机制是一种基于概率的共识机制，是一种弱一致性的达成，只要某一节点算力足够强大，依然能够对之前的共识结果进行篡改。即便没有恶意节点的存在，依然会有分叉现象的出现。

(3) TPS 过低，比特币每 10 分钟一个区块，以太坊每 15 秒一个区块，这样低下的交易速度无法满足绝大多数的业务场景。

基于区块链的扶贫资金管理平台是基于联盟链场景。联盟链往往是由一些有着共同的利益的商业联盟体所组成的区块链，并且由这些商业联盟体共同进行区块链系统的搭建与维护。然而，这些商业联盟之间并没有完全相互信任，因此作为联盟中的成员都有义务去对区块链中其他成员进行监督，维持区块链系统正确的运行。因此就涉及到“拜占庭将军问题”。拜占庭将军问题是对现实世界的模型化，由于硬件错误、网络拥塞或断开以及遭到恶意攻击，计算机和网络可能出现不可预料的行为。

针对以上问题，本论文提出了改进的共识算法，在保障区块链系统的一致性的前提下，提升了区块链的 TPS，降低了区块共识所需消耗的资源，提高了区块链系统的安全性。

3.2 算法设计

3.2.1 系统模型

本文提出的算法保证了在一个由 N 个节点组成的分布式系统中，当存在 f 个（ $N>3f$ ）失效节点时，所有的正常节点都能达成一致性。这里， N 和 f 的关系证明如下：

在一个分布式系统中，为了达成一致性，需要满足以下两个必要条件：

(1) 活性，即一定能在有限的时间内做出判断。

(2) 安全性，即做出的判断一定要保证其正确性。

针对以上两点，考虑到如下最极端恶劣情况，可以做出如下判断：

极端恶劣情况 1： f 个拜占庭节点在收到消息后，都选择不回复。

在这种情况下，非拜占庭节点最多只会收到 $N-f$ 个回复，那么为了保证系统的活性，节点就必须要求在收到 $N-f$ 个回复的时候做出判断。如果非要等到 $N-f+1$ 或者更多个回复，如 N 个，那么拜占庭节点就可以采用集体不回复的方式来破坏系统，使得系统一直堵塞在该阶段，无法达成系统的一致性。

极端恶劣情况 2：考虑到回复的时间先后顺序问题，在率先收到的 $N-f$ 个回复中，存在 f 个回复是来自拜占庭节点。

在这种情况下，系统仍旧需要足够数量的非拜占庭节点的响应，并且这些非拜占庭节点的响应数量必须超过时效节点的响应数量，即 $N-f-f>f$ ，因此得到 $N>3f$ 。

3.2.2 模型假设

本文提出的算法有如下假设：

(1) 系统中允许拜占庭节点的出现，即该节点会无视规则对系统进行破坏，妨碍系统一致性的达成。而非拜占庭节点会按照规则运行，在给定状态和参数相同的情况下，操作执行的结果一定相同。

(2) 系统是一个由多个节点组成的分布式网络，节点之间的通信可能会因为网络故障、网络抖动等原因导致传输的消息产生丢失、延迟、重复或者乱序等现象，这类现象不归结为拜占庭错误。

(3) 使用非对称加密算法对消息进行签名、加密。保证了消息的真实性和身份的可验证性，防止消息被篡改和伪造。

3.2.3 算法定义

本文提出的算法有如下定义：

定义 1. Quorum

Quorum 是由系统节点组成的集合，并且任意两个 Quorum 的交集不为空。假设系统节点集合为 U ，$\delta=\{Q_1,Q_2,Q_3,...,Q_n\}$，且 $Q_i \subseteq U$,满足公式（3.1）则称 Q 为一个 Quorum。

$$\forall Q_i,Q_j \in \delta 且 Q_i \cap Q_j \neq \Phi \qquad (3.1)$$

Quorum 有如下性质：

(1) 任意两个 Quorum 至少有一个共同的并且正确的节点。

(2) 一定存在着没有错误的 Quorum。

其中本文定义$2f+1$个节点为一个 Quorum，这样可以保证在一个 Quorum 至少有 $f+1$个节点没有发生错误，其中 f 是该系统中出现允许最大错误节点数。

定义 2.View

算法在执行一次共识时，所有节点都在一个相同的环境中执行操作，这个环境称之为视图（view）。每次共识完成（失败或者成功）都将进行视图的变更。视图编号是连续的整数。

定义 3.Primary 和 backups

系统是一个由 N 个节点组成的分布式网络，这 N 个节点中，有一个称之为主节点（primary），其余节点称之为备份节点（backups）。主节点由公式（3.2）计算得到。

$$p = v \bmod N \tag{3.2}$$

当主节点失效的时候，就需要启动视图切换过程。视图切换协议用于解决良性容错，主节点切换协议用于解决恶性容错。

3.2.4 符号说明

本文提出的算法有如下符号：

p：主节点编号。

v：视图编号，从 0 开始的整数，每次视图变更$v+1$。

o：操作请求。

t：时间戳。

n：主节点对打包的交易组成的区块所分配的区块编号。

d：区块信息的摘要。

i：节点的编号。

f：拜占庭节点的个数。

h：区块链高度。

TX：客户端发送的交易请求。

$REPLY$：节点经过共识后回复给客户端的消息。

$PRE-PREPARE$：Pre-prepare 阶段，主节点向备份节点发送的消息。

$PREPARE$：Prepare 阶段，节点向其他节点发送的消息。

$COMMIT$：Commit 阶段，节点向其他节点发送的消息。

3.2.5 算法流程

本算法是一种状态机副本复制算法，即服务作为状态机进行建模，状态机在分布式系统的不同节点进行副本复制。每个状态机的副本都保存了服务的状态，同时也实现了服务的操作。算法采用三阶段协议来广播请求给节点，分别为 Pre-prepare、Prepare、Commit 阶段，下面详细说明每个阶段算法的流程。

Pre-prepare 阶段

主节点收集当前区块链网络中未被共识确认的交易 $<TX,o,t,s>$。t 时间戳，用来保证客户端请求只会执行一次，客户端发出请求的时间戳是全序排列的，或许发出的请求比早先发出的请求拥有更高的时间戳；s 是客户端的签名，采用非对称加密算法，用来保证客户端发送的交易不被篡改，不被伪造。

主节点将收集到的交易按照交易发出的时间进行排序，打包成一个区块，并分配一个序号 n 给这个区块，然后向所有的备份节点广播预准备消息，预准备消息的格式为 $<<PRE-PREPARE,v,b,d>,m>$。

备份节点收到 $PRE-PREPARE$ 信息后会对信息的合法性进行检查，检查一共有 4 项，分别是：

(1) 交易和预准备消息的签名是否正确，即交易是否来自真实存在的客户端，预准备消息是否来自真正的主节点，而非伪造。

(2) d 与 m 的摘要是否一致。

(3) 视图编号是否一致。

(4) 该备份节点从未在视图 v 中接收过序号为 n 但是摘要 d 不同的消息 m。

如果通过上述检查，备份节点接收这条 $PRE-PREPARE$，进入下面的 Prepare 阶段。

Prepare 阶段

备份节点向所有节点（包括主节点）发送准备消息 $<PREPARE,v,n,d,i>$，并且将预准备消息和准备消息写入自己的消息日志。

节点收到 $PREPARE$ 信息后会对信息的合法性进行检查，检查一共有 2 项，分别是：

(1) 准备消息的签名是否正确，即验证是否是来自节点 i 的消息。

(2) 视图编号是否一致。

如果验证通过，这将这个准备消息写入消息日志中。

定义，准备阶段完成的标识是副本节点 i 收到了大于或等于 $2f$ 个从不同节点发来的，与自己收到的 $PRE-PREPARE$ 消息一致的 $PREPARE$ 消息。验证预准备消息和准备消息一致性主要检查 3 项，分别是：

(1) 视图编号v是否一致。

(2) 消息序号n是否一致。

(3) 摘要d是否一致

准备阶段和预准备阶段确保所有非拜占庭节点对同一视图中的请求序号达成一致，即都收到了一致的请求。那我们是不是就可以说至此共识工作已经完成，全网节点都达成了一个一致的请求，每一个节点开始照着这个序列执行就可以了吗？这是有漏洞的，设想一下，在$t1$时刻只有节点一把请求m（编号为n）带到了准备状态，其他两个备份节点节点二、节点三还没有来得及收集完来自其它节点的*PREPARE*信息进行判断，那么这时发生了视图切换进入到了一个新的视图中，节点一还认为给m分配的编号n已经得到了一个 Quorum 同意，可以执行了，但对于节点二来说，它来到了新的视图中，它失去了对请求m的判断，甚至在上个视图中它还有收集全其他节点发出的*PREPARE*信息，所以对于节点二来说，给请求m分配的编号n将不作数，同理节点三也是一样。那么节点一一个节点认为作数不足以让全网都认同，所以在新的视图中，请求m的编号n将作废，需要重新发起提案。所以就有了下面的 Commit 阶段。

Commit 阶段

备份节点向所有节点（包括主节点）发送提交消息$<COMMIT,v,n,d,i>$。

节点收到*COMMIT*信息后会对信息的合法性进行检查，检查一共有 2 项，分别是：

(1) 提交消息的签名是否正确，即验证是否是来自节点i的消息。

(2) 视图编号v是否一致。

如果验证通过，这将这个验证消息写入消息日志中。

定义，提交阶段完成的标识是副本节点i收到了大于或等于$2f$个从不同节点发来的，与自己收到的*PRE − PREPARE*消息一致的*COMMIT*消息。验证预准备消息和准备消息一致性主要检查 3 项，分别是：

(1) 视图编号v是否一致。

(2) 消息序号n是否一致。

(3) 摘要d是否一致。

如果验证通过，节点就会运行相应智能合约，执行相应请求。经过 Commit 阶段，保证了所有非拜占庭节点以同样的顺序执行相同的请求，保证了算法的正确性。

每个节点都向客户端发送回复消息$<REPLY,v,t,s,i,r>$，客户端等待$f+1$个从不同节点得到的同样响应，同样响应需要保证签名正确，并且具有同样的时间戳和执行结果。这样客户端才能把r作为正确的执行结果。

3.2.6 主节点切换协议

因为系统中允许拜占庭节点的出现，因此，系统会受到拜占庭节点各种不同方式的攻击。假设在一个由四个节点组成的系统中，最多允许有一个拜占庭节点。此时的算法可以很好的避免拜占庭节点的各种诸如多播、不播、伪造等破坏手段，但是有一种破坏方式却无法避免。即当拜占庭节点为主节点时，该节点故意不打包某个特定交易，这样的区块仍然是合法的区块，因为区块信息并没有涉及到伪造、篡改或违规操作。因此，这个区块可以经过三阶段的检验，被全网所认可。这样一来，只要该主节点不发生变化，那么那条特定交易就永远不会被确认。本论文针对这种拜占庭作恶方式，提出主节点切换协议，从最大程度上降低该作恶方式的出现，维护系统的安全性和活性。

本论文采用结合区块高度的轮流更换主节点的方式避免上述作恶方式，改进后的主节点由公式（3.3）确定：

$$p = (h - v) \bmod N \tag{3.3}$$

h 为当前区块高度，v 为视图编号，N 为节点数量。每成功完成一次共识，区块高度就会加一，同时，主节点也会因此随之改变。这种方式类似于联合国轮值主席制度，系统中的每个节点轮流担任主节点。这样，即便有拜占庭节点担任主节点时采用了上述作恶方式，那么，在下一次共识时，新任的主节点就会将上一轮共识时未被打包的交易重新打包到区块中，进行确认。

但是，这种方式任然存在一个问题。每一轮，拜占庭节点必然会成为一次主节点，只要它成为主节点，依然可以使用上述作恶方式，破坏系统的正常运行。因此，针对于此本问对算法进行又一次改进。

在算法中，引入评价机制，对每次节点担任主节点时的表现进行评价打分，评价指标有两个：

(1) 共识是否成功。

如果共识顺利完成，给该共识过程担任主节点的节点评价 10 分，否则给该主节点评价 1 分。共识失败很大的原因是主节点为拜占庭节点，该节点在 Pre-prepare 阶段，发给每个备份节点的 *PREPARE* 信息编制了不同的消息编号 n，这样在 Prepare 阶段，因为 n 的不一致，将会导致共识失败。但是，也不能一言以蔽之，共识失败也可能因为网络延迟、网络孤岛等良性错误导致。因此，共识失败任然给主节点 1 分而非 0 分。

(2) 当前区块中是否有比上一个区块打包时间更早的交易。

该举措是在新一轮共识时，对上一轮共识效果的又一次评价。如果在新一轮共识，新的区块中存在一笔或几笔交易，该交易的发生时间早于上一个区块的打

包时间，则给上一轮共识时的主节点的评分降到 1 分。同时也是考虑到网络延迟、网络孤岛等良性错误导致的该情况的出现。因此，任然给主节点留有 1 分。

每完成一次共识，不论成功还是失败，全网进行一次的主节点的切换。为了保证主节点选择上的公平性和安全性，选择算子参考 GA 算法中最经典的选择算子——轮盘赌选择。每个节点被选中为主节点的概率与其评价函数大小成正比。具体操作如下：

(1) 计算每个节点的评价函数：

$$S_i = \frac{S_i \times (c-1) + S_i'}{c} \tag{3.4}$$

(2) 计算出每个节点被选中的概率：

$$P_i = \frac{S_i}{\sum_{j=1}^{N} S_j} \tag{3.5}$$

(3) 计算出每个节点的累积概率：

$$q_i = \sum_{j=1}^{i} P_j \tag{3.6}$$

(4) 在[0,1]区间内产生一个均匀分布的随机数 $random$，若 $random < q_1$，则选择节点 1 位下一阶段共识的主节点，否则，选择节点 k，使得 $q_{k-1} < random \leq q_k$ 成立。

分数高的节点，被选中的概率大，分数高则代表了这个节点一直按照算法的规则在运行。而正如上面所述，即便评价指标不达标，仍然给予 1 分，这样做避免非拜占庭节点因为网络延迟、网络孤岛等非自身原因而被永远认定为拜占庭节点，减少非拜占庭节点的数量，将会对系统的鲁棒性造成破坏。同时，这种主节点的选择方式，随着系统运行的时间的推移，系统的鲁棒性、安全性将会更加稳固。

3.3 本章小结

本章主要讨论区块链系统的共识机制。本文通过分析当前区块链共识机制存在的问题，提出了基于信用评分的主节点切换协议的 CBFT(Credit-based Byzantine Fault Tolerance)共识算法，保障了区块链系统的安全性和活性。可以较为有效的避免主节点作恶，从原来的无法察觉主节点作恶到现在可以察觉到主节点的作恶行为，并且将主节点作恶的概率降低到 10%。

第4章 区块链架构的研究与设计

4.1 痛点分析

目前区块链技术发展飞快并日趋成熟，但仍有不少企业对应用区块链还有些顾虑，主要因为传统区块链技术要落地到商业应用特别是金融应用，仍有比较多的问题，其中最大的一个问题是 TPS(Transactions Per Second)的限制。对于商业应用来看，TPS 是企业非常关心的交易性能指标。类似比特币区块链交易速率约 6.67 次/秒，每笔交易需要 6 个区块确认，10 分钟才能产生一个区块，全网确认一次交易需要 1 个小时。显然，这样的交易性能无法满足金融机构所涉及的高频交易。

4.2 现有方案对比

为了提升性能，工业界提出了一些如闪电网络、分片处理等创新的设计构想，下面简述现阶段具有代表性的方案。

(1) Ethereum

可扩展性是以太坊网络承接更多业务量的最大限制。以太坊项目未来希望通过分片（sharding）机制来提高整个网络的扩展性。分片是一组维护和执行同一批智能合约的节点组成的子网络，是整个网络的子集。

支持分片功能前，以太坊整个网络中的每个节点都需要处理所有的智能合约，这就造成了网络的最大处理能力受制于单个节点的处理能力。

分片后，同一片内的智能合约处理是同步的，彼此达成共识，不同分片之间则可以是异步的，这样就可以提高网络的可扩展性。

(2) Bitcoin

为了提升性能，Bitcoin 社区提出了闪电网络的创新设计。闪电网络的主要思路十分简单——将大量交易放到比特币区块链之外进行，只把关键环节放到链上进行确认。

闪电网络主要通过引入智能合约的思想来完善链下的交易渠道。核心的概念主要两个：RSMC（recoverable sequence maturity contract），即“可撤销的顺序成熟度合同”，其原理类似于资金池机制。首先假定交易双方之间存在一个“微支付通道”（资金池）。交易双方先预存一部分资金到“微支付通道”里，初始

情况下双方的分配方案等于预存的金额。每次发生交易，需要对交易后产生资金的分配结果共同进行确认，同时签字把旧版本的分配方案作废。任何一方需要提现时，可以将他受众双方签署过的交易结果写到区块链网络中，从而被确认。另一个概念是 HTLC（hashed time lock contract），这其实就是限时转账。通过智能合约，双方约定转账方先冻结一笔钱，并提供一个哈希值，如果在一定时间内有人能提出一个字符串，使得它哈希后的值与已知值匹配，则这笔钱转给接收方。

RSMC 保障了两个人之间的直接交易可以在链下完成，HTLC 保障了任意两个人之间的转账都可以通过一条“支付”通道来完成。闪电网络整合这两种截止，实现任意两个人之间的交易都是在链下完成。

(3) Hyperledger

Hyperledger Fabric 针对之前 Peer 节点承担了太多的功能，从而带来了扩展性差、交易性能低的问题，针对上述问题，做出很大的改进和重构：

✧ 解耦了原子排序环节与其他复杂处理环节，消除了网络处理瓶颈，提高可扩展性。

✧ 解耦交易处理节点的逻辑角色为背书节点、确认节点、可根据负载进行灵活部署。

综合上述方案，为了提高区块链系统的 TPS，大家一致都采用分布式的处理方法以优化其系统架构。这一变革也恰恰迎合了当前金融领域去 IOE（IBM 大型机、Oracle 数据库、EMC 数据存储设备）取而代之上 XML（x86 小型机、MySQL 数据库、Linux 操作系统）的趋势。在未来的应用环境中，单台处理器的处理能力必定是有限的，但服务集群必然越来越大，在这样的情况下，乘势而行，因势利导通过适配单位机器的处理能力，解耦节点功能，特定节点做特定的工作，并结合服务集群的数量红利，从而提高区块链的 TPS，应该是一个可行的方案。

4.3 解决方案

本文通过研究工业界的设计构想，同时结合政府主导下的联盟链场景的特点，设计了多链并行计算的系统架构。

4.3.1 方案架构

在区块链层与业务层之间增加中继层，中继层向上负责接收业务层的请求，向下根据中继规则向多条区块链进行消息转发，多条链协同处理，并行计算，中继层相对独立于区块链系统，因此中继层处理请求的能力不会受制于区块链本身

的 TPS 瓶颈，因此提升了整个系统的 TPS；同时中继层可以根据所链接的每个区块链处理载荷的实时情况，对请求进行负载均衡，提升了系统的鲁棒性。

为了保障系统的安全，业务层与中继层的通信采用 Https 通信协议，中继层与区块链层的通信采用 SSL 通信协议。

中继层又非完全独立于区块链系统，中继路层的路由规则来源于区块链，在多条区块链中，独立设置一条路由链，路由链上运行着与路由规则相关的智能合约，中继层通过安全的 SSL 通信协议与路由链通信，获取路由规则，对业务层发送过来的请求进行相应路由。所有规则来源于区块链，又服务于区块链，保障了整个系统任然是以一种分布式的方式运行，保障了系统的安全和规则的透明。

同时，中继路由模块的设计，也提高了系统的扩展性，实现了可插拔、模块化。只需要在路由链上编写不同规则的智能合约，中继路由模块即可实现不同的功能。

具体的方案架构如图 4.1 所示：

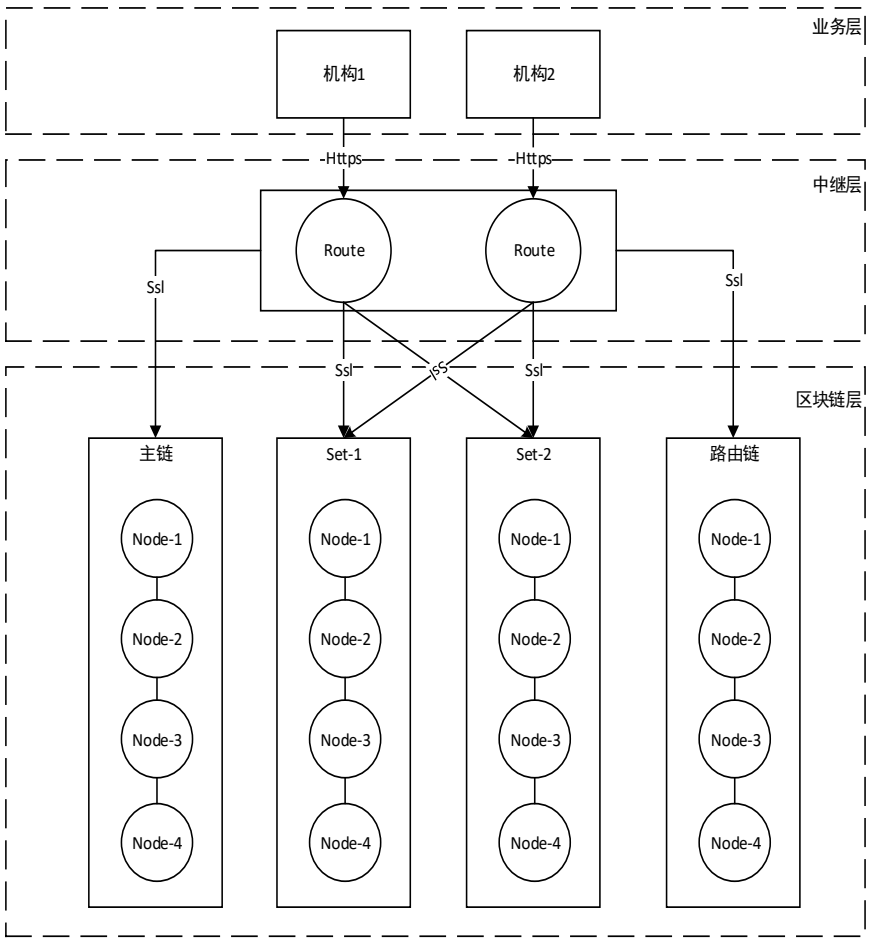

图 4.1 多链并行计算系统架构图

4.3.2 执行流程

该架构对交易的执行流程如下：

(1) 步骤 1

中继层接收客户端的请求，根据路由规则将交易请求转发到相应业务链进行处理。

(2) 步骤 2

当业务链收到该交易请求后返回该交易请求的摘要，中继层缓存该摘要。为了提高运行效率，该系统采用异步的方式对数据进行处理，中继层根据交易请求的摘要判断异步回调的关系。

(3) 步骤 3

当业务链处理完该交易请求后，转发交易请求的摘要和处理结果到路由模块（路由模块可以设置多个，以增加系统的运行效率）。

(4) 步骤 4

路由模块收到回复后，根据交易请求的摘要，寻找对应的回调。一方面，向客户端返回请求处理结果，另一方面向主链更新数据。

4.3.3 关键模块

该架构主要包括两个关键模块，分别为中继层的路由模块和区块链层的路由链，下面详细介绍每个模块的功能和作用。

4.3.3.1 区块链层的路由链

路由链与区块链层的其他区块链一样，为一条完整独立的区块链。路由链与业务链的区别在于链上智能合约的不同。业务链部署与业务相关的智能合约，而路由链用于制定多链并行计算架构中中继层路由模块的路由规则，在该条区块链上部署了路由规则相关的路由管理合约、集群合约和节点合约。

三种合约之间是有相互依赖关系的，如图 4.2 所示，自上而下属于 1 对 N 的关系，层层嵌套，路由管理合约只有一个，集群合约根据有几条业务链对应几个集群合约，节点合约根据每条链上有几个节点对应几个节点合约。

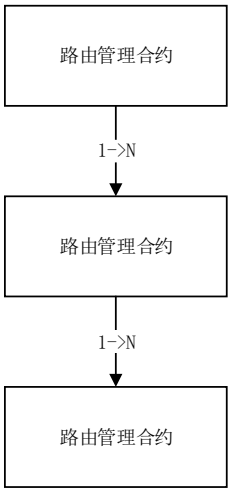

图 4.2 合约关系图

下面详细介绍每种智能合约的数据结构和方法接口：

(1) 路由管理合约

路由管理合约用于事务编号与集群之间的关系，路由通过事务编号进行路由，简单以用户编号为例，每个集群（即每个业务链）处理特定用户编号的请求，路由管理合约根据用户编号对用户分配到响应的集群。支持注册新集群路由、注册新事务、事务编号对应集群的查询、集群信息的查询等功能。

表 4.1 路由管理合约存储数据

存储数据	说明
Array<集群合约地址>	数组结构，存储所有集群合约的地址
Map<用户 ID,集群序号>	Map 结构，集群合约和事务 ID 的映射，即该 ID 的事务的数据请求应该由哪个集群处理
Uint 业务 ID	
Uint 当前空闲集群序号	递增

表 4.2 路由管理合约接口

接口	输入	输出	说明
registerSet	集群合约地址		注册新集群，即将新的集群合约的地址加入到数组中

registerRoute	事务 ID	Boole	注册新事务路由，即分配新事务的数据请求交由哪个集群处理
getRoute	事务 ID	集群序号	获取当前事务是由那个集群处理

(2) 集群合约

集群合约用于管理该集群的事务集和节点集。每个集群规定了管理事务的数量上限。在部署时，接收来自路由管理合约的事务分配请求，如果当前事务数量未满，接收并管理该事务。提供事务查询接口，用于在路由分配时，确定事务的路由规则，即分发方向。同时，管理该集群下的所有节点，包括增加、删除、查询节点等功能。

表 4.3 集群合约存储数据

存储数据	说明
Array<用户 ID>	数组结构，存储当前集群需要处理的事务列表
Array<节点合约地址>	数组结构，存储属于该集群的所有节点合约的地址
Uint SET 序号	
Uint maxNum	最大集群数
Uint warnNum	告警集群数

表 4.4 集群合约接口

接口	输入	输出	说明
registerRoute	事务 ID		注册事务路由
getNodeList		节点信息列表	获取集群的节点列表
addNode	节点信息		增加节点
removeNode	节点信息		删除节点

IsFull		布尔	返回当前集群是否已满，如果以已满则不允许继续注册用户

(3) 节点合约

节点合约用于存储节点的各类信息，如节点 ID、IP 地址等。

表 4.5 节点合约存储数据

存储数据	说明
String NodeId	节点 ID
String ListenIp	P2P 网络监听端口 IP 地址
Uint P2PPort	P2P 网络端口
Uint RpcPort	RPC 端口
Uint NodeType	节点类型
String Desc	节点描述
String CAHash	CA 摘要
String agencyinfo	节点信息

4.3.3.2 中继层路由模块

为了提高中继层的运行效率，该分布使用 Node.js 实现高并发接入，实现内存缓存路由信息，提高路由速度。

中继层的路由模块主要功能如下：

表 4.6 中继路由模块主要功能项

功能项	说明
接入准入	控制请求的接入授权管理。
路由链请求转发	将路由相关的请求转发至路由链
业务链请求转发	判定业务路由规则并对请求进行业务链内的分发
回调模块	添加支持对交易成功后进行回调

下面，结合流程图，详细介绍该模块的功能与实现原理。

(1) 接入准入

业务层的客户端向中继层发送请求前，需要先建立连接。中继层读取客户端的 IP 地址，与区块链中保存的 IP 配置白名单进行对比，比对失败则断开连接，拒绝服务。这一步充分体现了联盟链的准入机制，只有实现被联盟所认可的一方才能接入并参与服务。这一点也大大提高了系统的安全性。

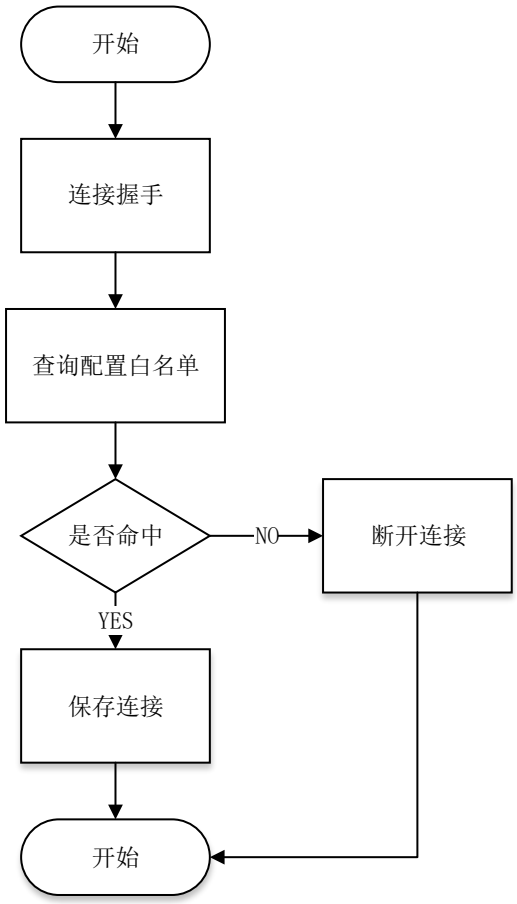

图 4.3 接入准入流程图

(2) 请求转发

客户端身份验证通过之后，中继层的路由模块对客户端发送的请求进行解析，读取其中的事务 ID，如果该事务在之前进行过路由注册，为了提高运行效率，会将该事务对应的路由规则存储在 cache 中。读取路由缓存，如果未命中，即说明该事务未进行路由注册。否则，将该请求分发至路由分发器，路由分发器会再次判断与集群的连接是否正常，正常情况下，会将该信息发送至集群中的节点。为了保障安全性，一般会要求发送节点的数量至少有两个。

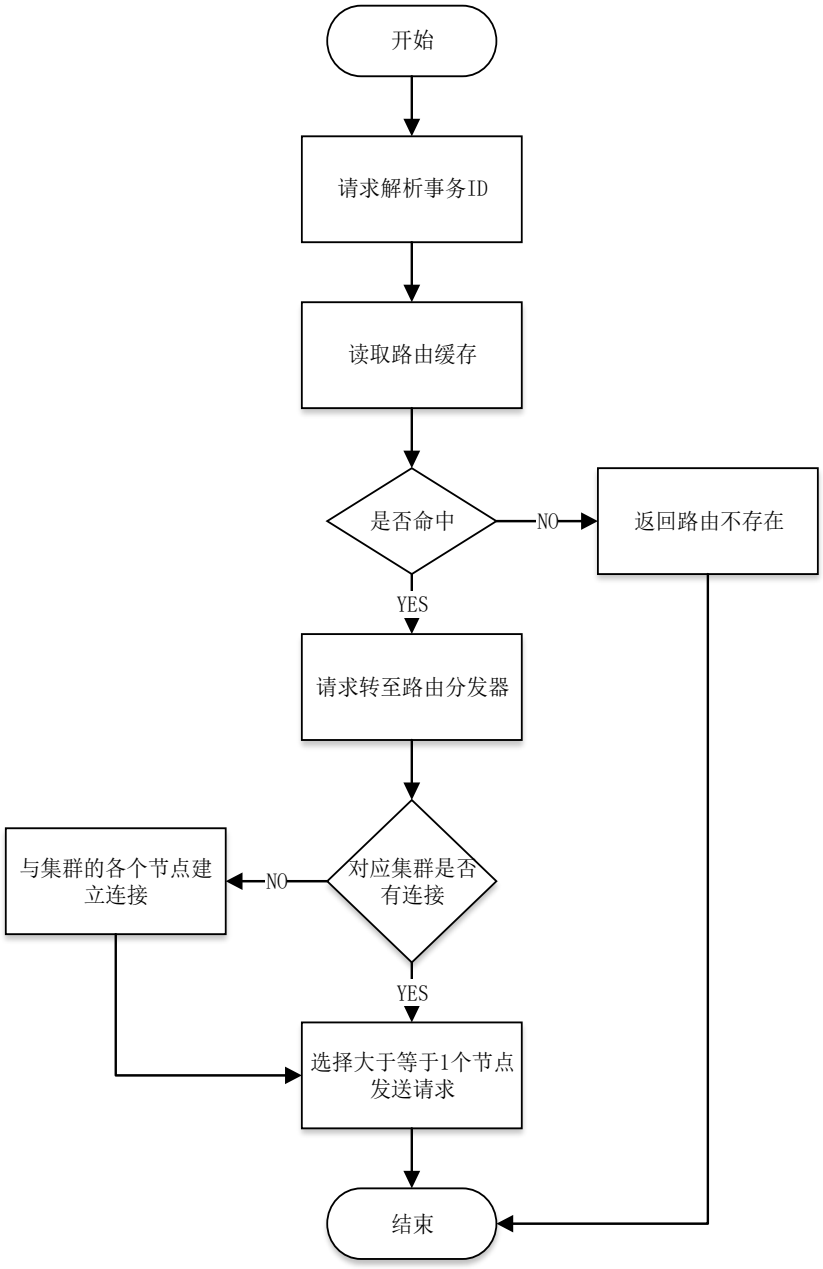

图 4.4 请求转发流程图

(3) 路由分配策略

为新事务注册路由，首先解析请求，读取事务 ID，如果该事务已经有路由存在，则返回路由已经存在，直接结束。否则，运行路由管理合约，读取当前空闲集群的集群合约地址。调用集群合约 isFull 接口，如果当前集群管理的事务数量超过了警戒值，会提示告警，并进一步检查当前集群管理的事务数量满员，如果满员，就会在路由管理合约的集群合约数组中选取下一个集群地址，如果存在下一个集群地址，则回过头调用集群合约 isFull 接口，否则注册失败。如果 isFull 接口的检查都通过，则调用集群合约 registeRoute 接口，返回注册集群序号，注

册成功！

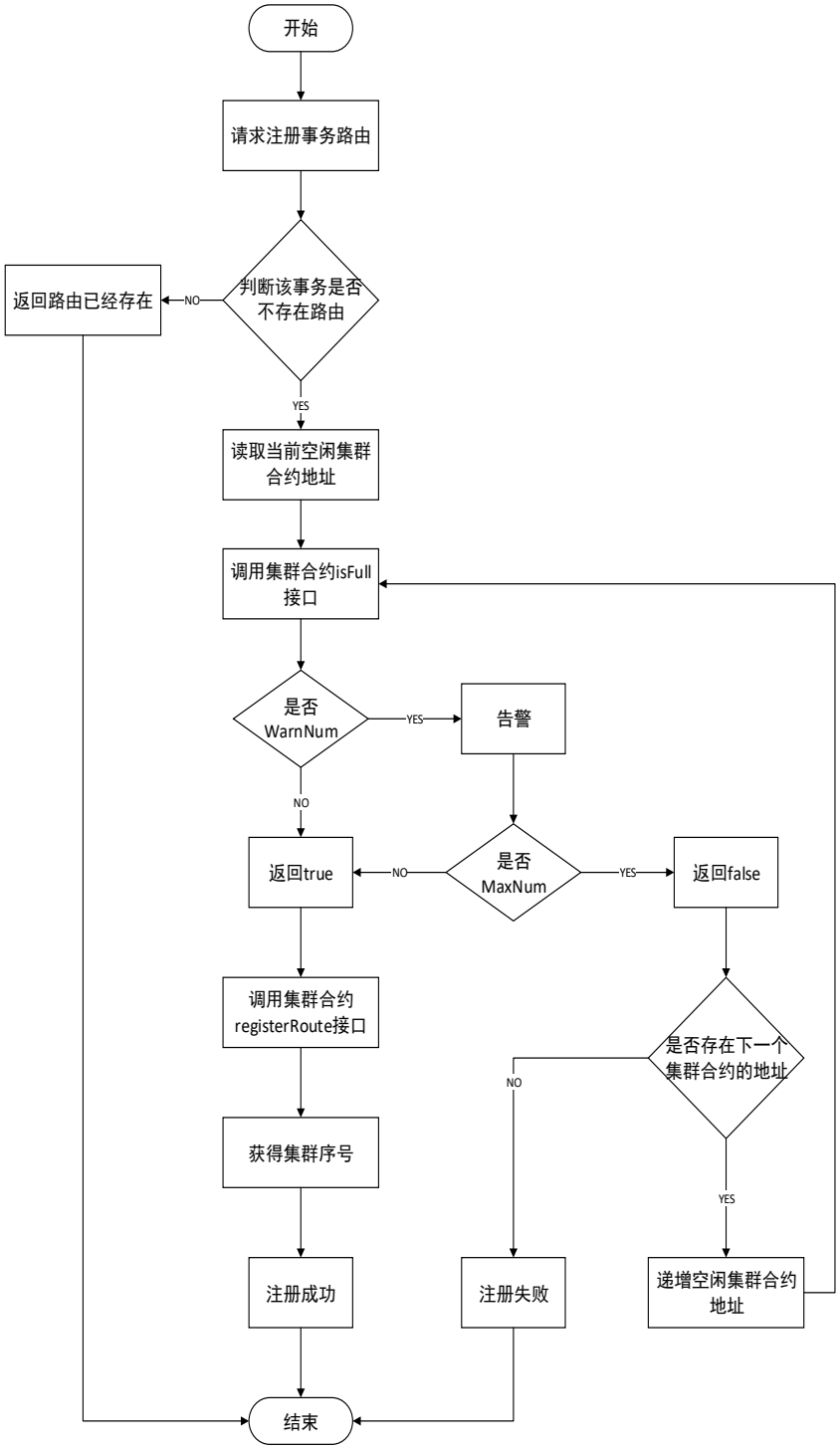

图 4.5 路由分配策略流程图

4.4 本章小结

本章主要讨论区块链系统的性能问题，从系统架构着手，设计多链并行计算

架构。该架构秉承从区块链中来到区块链中去的思想，将保证了效率的同时，又不失安全性。同时，模块化的设计使得多链并行计算架构具有较强的灵活性，可以根据需求对架构进行调整，以达到资源利用的最优化。

第5章 系统测试

5.1 性能测试

5.1.1 测试环境

(1) 硬件环境

本文实验硬件采用 4 核 8 线程，Intel(R) Core(TM) i7-4790 CPU @ 3.60GHz 处理器，8G 内存的服务器。

(2) 软件环境

- Docker - v18.02.0
- Docker Compose - v1.16.1
- Node.js - v6.9.5
- Linux - v3.10.0-514.6.1.el7.x86_64

(3) 区块链配置

区块配置如下：

- BatchTimeout: 2s
- MaxMessageCount: 10
- AbsoluteMaxBytes: 98 MB
- PreferredMaxBytes: 512 KB

网络配置如下：

本文实验的区块链网络由 4 个 peer 节点组成。为了提高测试的精度，4 个 peer 节点都以 docker 容器的形式部署在同一台机器中，这样保证了不同节点都在相同的环境下运行。

(4) 合约配置

每个节点部署相同的 pressureMeasureCC.go 智能合约。该合约初始化一个账户 A，账户初始金额为 100，设置有 add 接口，每次调用智能合约的 add 接口，账户 A 资金加 1。

5.1.2 测试算法

区块链的 TPS（Transaction Per Second），即每秒钟处理的交易笔数。TPS

的计算公式如下：

$$TPS = \frac{1}{t_{end} - t_{start}} \tag{5.1}$$

t_{end} 为一笔交易结束的时间，t_{start} 为一笔交易开始的时间。这个算法简单易懂，但是问题也很突出。好比计算一页纸的厚度，完成一笔交易的时间相对很短，一点点网络抖动都有可能导致这个时间的巨大变化。同时，加上区块链交易池和区块结构的特殊性，即客户端先将交易请求发送到区块链网络（交易池）中，然后再由节点打包成块，批量共识、落盘。为了修正上述算法的不准确性，本文将 TPS 的计算方法修改如下：

$$TPS = \frac{\sum_{i=0}^{n} N_i}{t_n - t_0} \tag{5.2}$$

N_i 为第 i 个区块中交易的笔数，t_i 为第 i 个区块的时间戳。n 的值越大，即统计越多的区块，TPS 的计算准确性就会越高。这里 n 取值 100。

5.1.3 TPS 测试

TPS 和每秒交易请求速度是相关的，经过测试，shell 单进程请求速率是有瓶颈的，如下图所示：

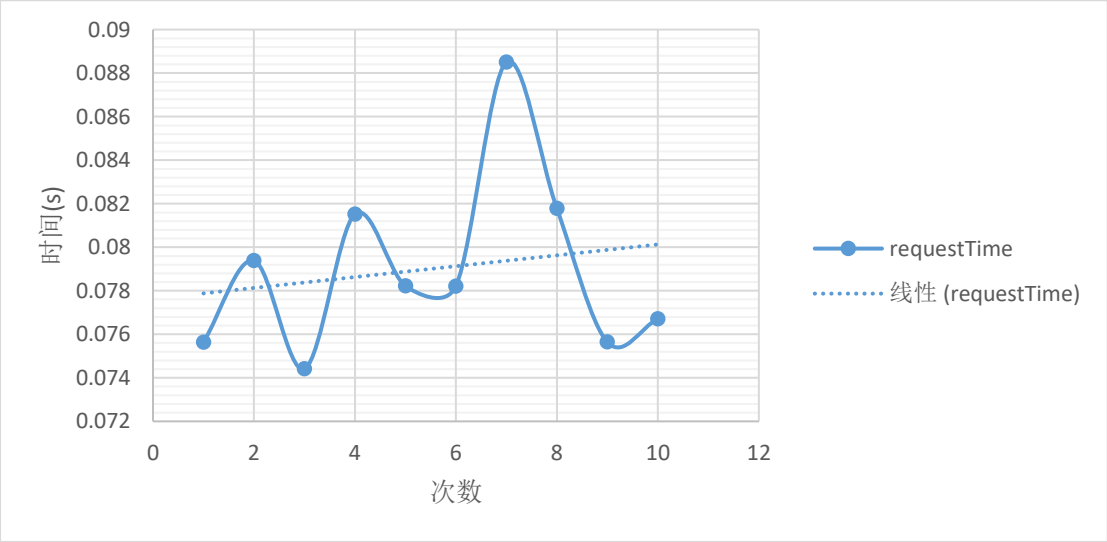

图 5.1 shell单进程请求时间统计图

表 5.1 shell单进程请求时间统计表

Number	RequestTIme

1	0.075638632
2	0.079388702
3	0.074410545
4	0.081524101
5	0.0782242
6	0.078217538
7	0.08850884
8	0.081778304
9	0.075644207
10	0.076710529
Average	0.07900456

在这样的情况下，请求的速率最高只能达到12.65822笔/S。为了克服发送请求速度的瓶颈问题，本文在这个基础上进行改进，通过多进程请求的方式，增加交易请求速度，通过验证，方法有效。

(1) 单链TPS测试

测试的结果如下：

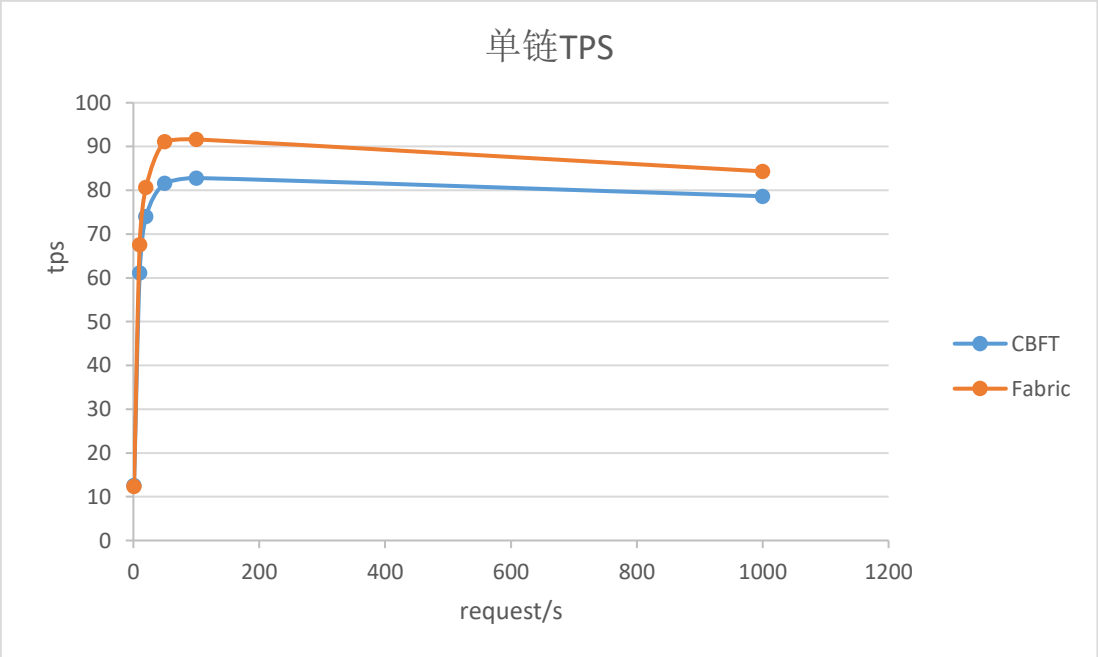

图 5.2 单链TPS测试

表 5.2 单链 TPS 统计数据表

开进程 bash 个数	CBFT TPS	Fabric TPS
1	12.54721623	12.35146578
10	61.14271127	67.54263225
20	74.02828005	80.65223214
50	81.61117806	91.12574523
100	82.80057674	91.62341125
1000	78.64186596	84.32514452
峰值	82.80057674	91.62341125

当进程开到1000个的时候，CPU满负荷运行，具体情况如下：

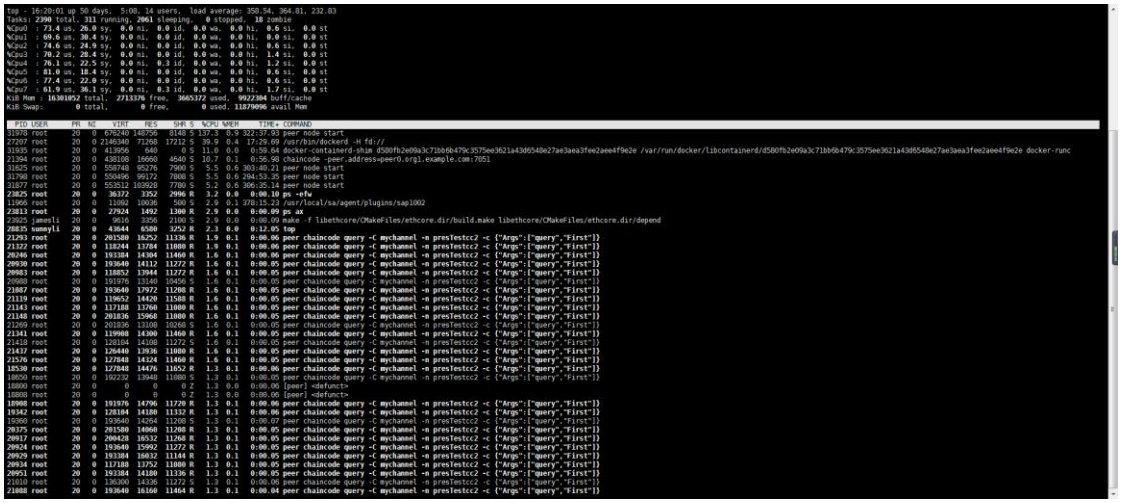

图 5.3 单链TPS测试时进程状态

(2) 多链 TPS 测试

多链由 1 个 Route 模块，2 个 Set 链，1 个路由链，1 个全节点链组成，每条链采用单链相同的区块和网络配置。

测试结果如下：

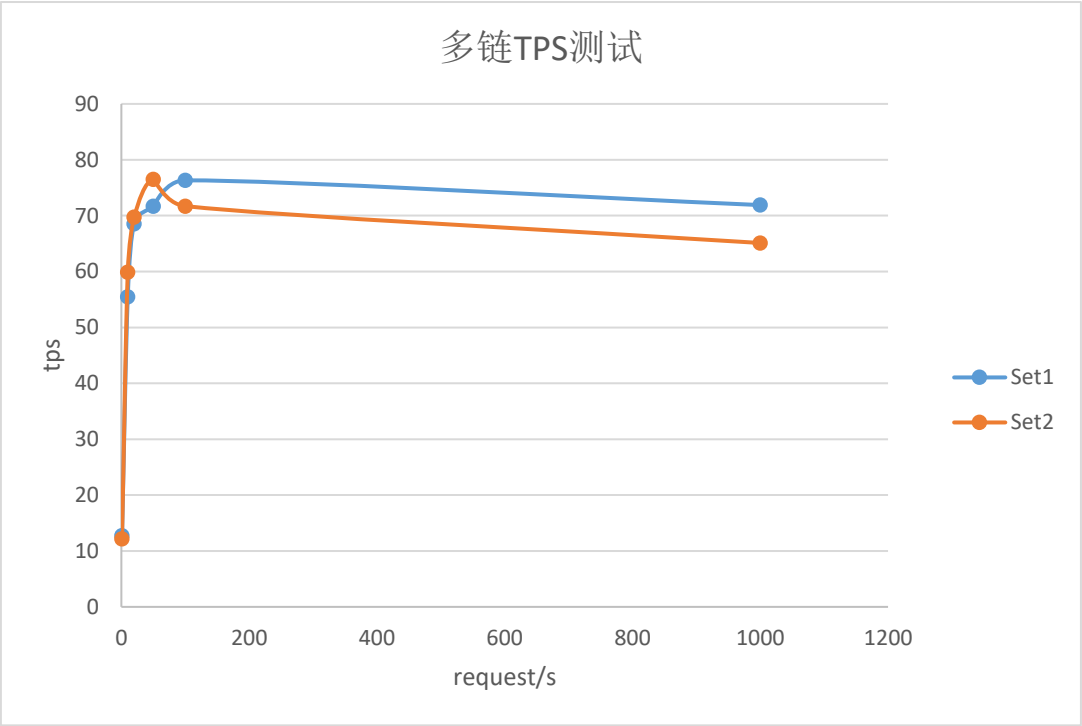

图 5.4 多链 TPS 测试

表 5.3 多链 TPS 统计数据表

开进程 bash 个数	Set1 TPS	Set2 TPS
1	12.75283591	12.14488894
10	55.49323704	59.86487837
20	68.55851301	69.72854058
50	71.68280337	76.4947125
100	76.32345686	71.70960609
1000	71.89624145	65.11471285
峰值	76.32345686	76.4947125

当进程开到1000个的时候，CPU满负荷运行，具体情况如下：

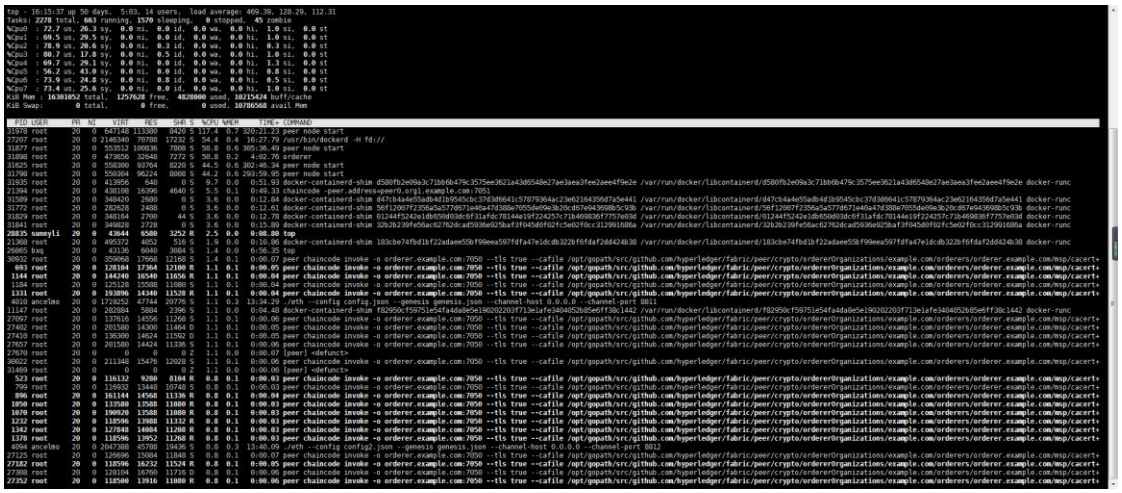

图 5.5 单链 TPS 测试时进程状态

5.2 本章小结

经过测试，在一个由 4 个节点组成的基于改进的 CBFT 共识算法的区块链网络中，其 TPS 峰值约为 80 笔/s。与基于 PBFT 共识算法的 BCOS 区块链拥有相当的 TPS，同时一定程度上解决了主节点作恶的问题。多链测试，两条 Set 链的 TPS 峰值都约为 75 笔/s，整个系统最高可以承受 150 笔/s 的交易，相对性能得到了一定的提高。

第6章 平台的设计与实现

6.1 业务介绍

贵州省政府根据《贵州脱贫攻坚投资基金设立方案》，设立贵州脱贫攻坚投资基金扶贫产业子基金（以下简称“扶贫基金”）。扶贫基金遵循“政府主导、企业主体、市场运作、风险可控”的原则，按照“强龙头、创品牌、带农户”的思路组织实施。政府通过财政出资、明确投资方向、界定投资范围、提供风险增信服务等方式发挥主导作用。从而撬动社会资金投入到脱贫攻坚事业中去。其业务参与主体如图 6.1 所示：

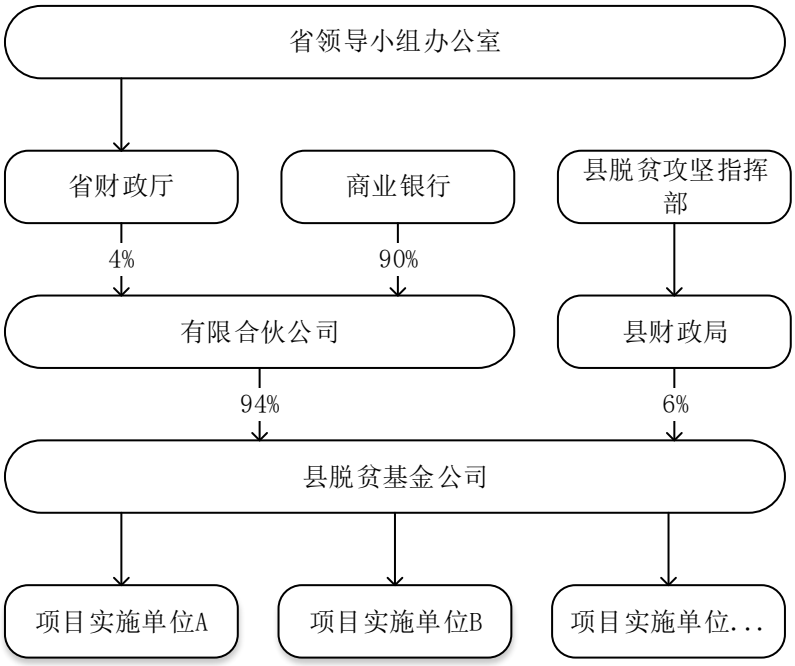

图 6.1 业务主体图

扶贫基金总规模 3000 亿元，财政性资金和金融机构按 10%:90%比例出资，即：财政性资金出资 300 亿元，银行等金融机构出资 2700 亿元。其中，财政性资金省市出资比例为：4:6，即省财政厅资金出资 120 亿元，20 个极贫乡镇所在市的财政局出资 180 亿元。

产业基金采取募投制，投资项目成熟一个投放一个。投资项目获批后由脱贫基金公司发起募集，其对应的 10%财政募集资金到位后，90%的金融机构募集资金同步到位。然后再逐级下拨，直到款项到达施工单位。

6.2 业务痛点分析

扶贫基金业务涉及的资金总体规模巨大，为了强化对资金的管理，达到提高使用效率，降低资金风险的目标，传统的做法是增加中间层级，级级加码，层层沉淀。但是，人心不古，虽然有行政层级上的上下关系，但是从每级的角度上讲，其需求是不一样的，从最高级省政府来讲，是想看到资金能更好的被利用，更多的贫困人口能够受到帮扶；往下中间层，更多的是想能不能把这笔扶贫资金留在他这里，做一些对自己有利的事情，比如弥补财政的赤字，做一些投资等；在最下层，这些钱是天上掉下来的馅饼，能不能真正用到扶贫上，另当别论。因此，虽然在行政上看是至上而下的，但是在需求上分析，是对立的。总结问题如下：

- ✧ 信用可达性和管理有效性随着层级的增加而逐渐衰减。
- ✧ 无法实时、全面的了解扶贫资金的使用情况和项目的开展情况。

6.3 解决方案

为了解决以上存在的问题，本文提出了基于区块链的解决方案，区块链是一种新型的信息共享模式，将同一业务（生态）体系下的不同实体建立一个安全可靠、可追溯、不可篡改、低成本和利于多方协同的系统。这正是省政府最想看到的，同时也给下级徇私舞弊敲响了警钟。全网信息共同记录、共同检查、共同维护，体现了平等与开放，每一个参与者都是主人翁，提高了下级参与者的积极性和责任意识。区块链的使用，为消除上下层级之间约束和限制，简化组织结构提供了可能的实现方式，信息的传递也因此更加流畅。

该方案由两个子系统组成，分别为基于区块链的数字汇票系统和基于区块链的实时对账系统，前者为解决信用可达性和管理有效性随着层级的增加而逐渐衰减的问题提供了可行的解决方案，后者为实时、全面的了解扶贫资金的使用情况和项目的开展情况提供了可行的解决方案。

6.3.1 基于区块链的数字汇票系统

在系统内，通过省政府的强信用背书发行“数字汇票”。

“数字汇票”实质上是运行在区块链上的根据资金划拨、流转业务需求定制化的智能合约，具有如下特点：

- ✧ 发行时，约定使用条件，确定资金用途、流转路径、兑现范围等约束条件，固化资金的使用方向。
- ✧ 流通时，按照发行时约定的约束条件使用，且流通过程受参与各方共同

监督。

✧ 承兑时，采用以链上信息为准的原则（区块链上信息更安全，更透明），当使用场景符合要求时，由对应的银行账户向受付对象发起现金转账。

✧ 数字汇票只在扶贫资金管理平台体系内部闭环流转。

相关流程如图 6.2 所示：

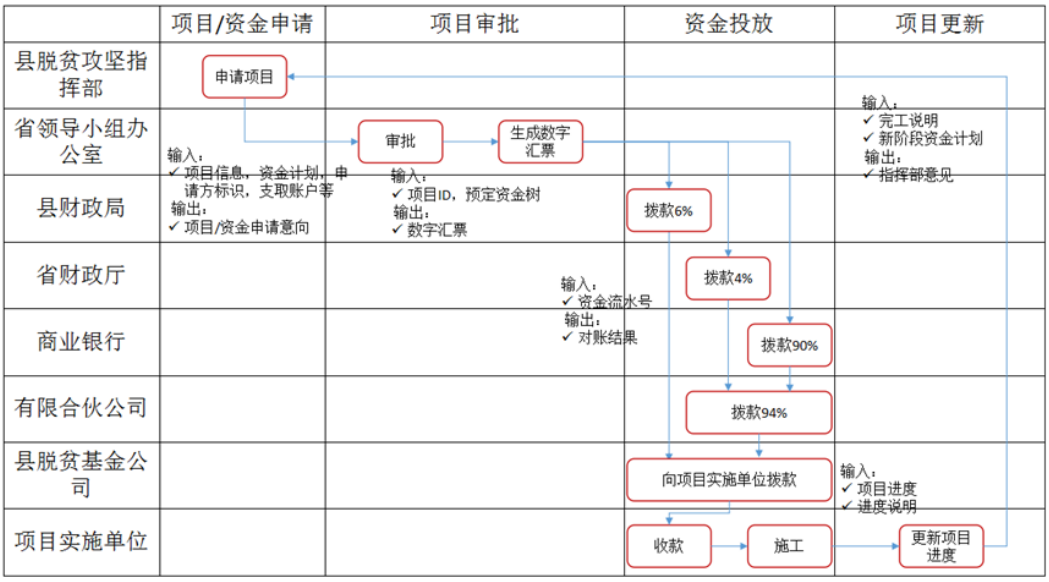

图 6.2 数字汇票生成及流转

6.3.1.1 系统框架

系统架构如图 6.3 所示：

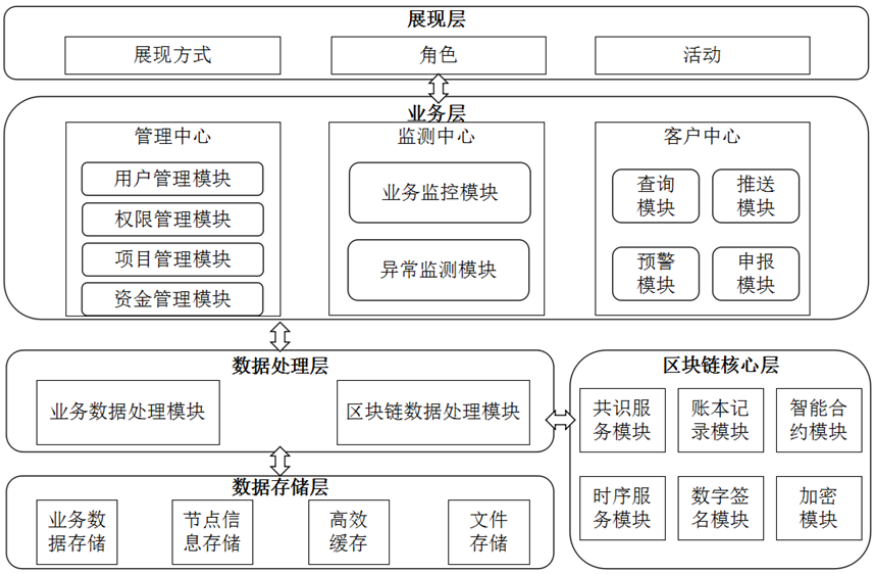

图 6.3 系统架构图

(1) 展现层：

a) 展现方式：基于区块链的脱贫攻坚应用管理平台以 web 应用形式呈现。

b) 角色：角色有管理员、贵州脱贫攻坚投资基金管理领导小组办公室、省财政厅、县脱贫攻坚指挥部、县财政局、商业银行、有限合伙公司、县脱贫基金公司，项目实施单位。共计 9 种角色。

c) 活动：活动有身份注册与认证、项目申请、项目审批、资金拨付、项目进度查询、资金进度查询、项目进度更新等活动

(2) 业务层：

a) 管理中心

✧ 用户管理：处理 LP，GP 和项目实施单位等用户的加入/退出区块链系统。

✧ 权限管理：对角色所拥有的权限进行管理。

✧ 项目管理：对项目信息进行管理。

✧ 资金管理：对资金的申请、拨付、使用等进行管理。

b) 监控中心

✧ 业务监控：监控业务流程中的用户行为。

✧ 异常监控：监测项目或者资金的异常信息。

c) 客户中心

✧ 查询：LP，GP 和项目实施单位根据自己的权限查询响应的信息，包括项目进度，资金流向等。

✧ 推送：LP，GP 和项目实施单位个性化订制信息推送，免去查询环节，订制推送信息一有变化，第一时间向其推送。

✧ 预警：项目、资金如发生异常，发送系统预警。

✧ 申报：对发现存在的且系统未预警的问题进行申报。

(3) 数据处理层：

a) 业务数据模块：对业务层产生的数据进行处理和转换，将需要存储的数据输出到数据存储层，将需要上链的数据输出到区块链数据处理模块，并根据数据流进行负载均衡。

b) 区块链数据处理模块：对输入的数据按照区块链和智能合约的要求进行处理和转换并输出到区块链系统中。

(4) 数据存储层：

a) 系统数据存储：存储平台系统数据，包括用户信息、区块链节点信息等。

b) 节点信息存储：存储区块链网络节点即区块链网络部署信息。

c) 文件存储：存储平台所有文件信息数据，包括大型文本文件、视频文件、

音像文件等非结构化的数据。

d) 高效缓存：应对超高业务流量对系统的冲击。

(5) 区块链层：

a) 共识服务：区块链网络中各节点对在区块链系统中进行事务或状态的验证、记录、修改等行为达成一致确认的方法。

b) 账本记录：负责区块间 P2P 通讯以及分布式存储。

c) 智能合约：智能合约是一套以计算机代码形式定义的承诺，以及合约参与方可执行承诺的协议，即：用计算机代码形式编写合约参与方达成的条件型协议，当条件被触发时区块链系统自动执行该协议。根据应用场景的不同需求，区块链系统可有选择性地提供智能合约功能。

d) 时序服务：对于区块链系统中的行为或数据需记录相应的一致性的时序。

e) 数字签名：数字签名功能被接收者用以确认数据单元的完整性以及不可伪造性，即确定消息确实是由签发方签署的。

f) 加密：加密功能一般具体包括加密和解密两个操作：加密操作是把明文数据转化为密文数据，解密操作是把密文数据还原为明文数据。

6.3.1.2 智能合约设计

(1) 实现功能

在区块链网络中发行数字汇票，力求解决信用可达性和管理有效性随着层级的增加而逐渐衰减的问题。

(2) 触发时机

省领导小组办公室审批项目成功即触发发行数字汇票接口，每个参与方拨款对账成功后触发流转数字汇票接口，项目实施单位接收款项时触发承兑数字汇票接口。

(3) 运行逻辑

“数字汇票”和智能合约相结合，相应设定资金用途、流转路径、收款方等约束条件。发行时约定使用条件，确定资金用途、流转路径、兑现范围。按约定流通，流通过程受参与各方共同监督。按约定兑现支付，当使用场景符合要求时，由对应的银行账户向受付对象发起资金转账。

(4) 数据结构及接口

表 6.1 数字汇票智能合约存储数据

存储数据	说明
DraftID	数字汇票编号
ProjectID	对应项目编号
InstructionID	发行机构编号
InstructionSign	发行机构签名
Status	数字汇票状态
CreateAt	数字汇票生成时间
Amount	数字汇票金额
PlanPath	计划路径
ActualPath	实际路径
SpecialRule	特殊规则

表 6.2 数字汇票智能合约接口

接口	输入	输出	说明
create	数字汇票信息	数字汇票编号和发行结果信息	发行数字汇票。如果发行数字汇票失败，会将失败信息输出。
transfer	数字汇票编号，对账信息		结合实时对账系统，对账成功，对账合约自动调用该接口，更新数字汇票信息。
accept	数字汇票编号	承兑结果	
query	数字汇票编号	数字汇票信息	

6.3.2 基于区块链的实时对账系统

“数字汇票”就好比一部严格完善的法典，规定了方方面面。但是，如何让

人们都按照它规定的去做呢？即如何保证每级部门都如实、按时的将相关款项下拨下去呢？也就是如何保证上链数据的真实性问题。比特币、以太坊等公有区块链大多采用经济制衡的手段，囚徒困境的策略，即作恶的获利要远远低于遵守规则的获利。但是，这样往往会造成资源的浪费和弱一致性的达成，即还是会导致作恶，只是作恶的成本较高。结合扶贫基金业务的特点——“政府主导、企业主体、市场运作、风险可控”，即这是一个在政府管制下的系统，因此，要想做好对中间环节的管控，就要充分发挥强信用单位的作用。在入口处，使用省政府的强信用对“数字汇票”的真实性进行背书。由此及彼，中间环节，使用商业银行的强信用对拨款信息的真实性进行背书。

具体的做法如图 6.4 所示：

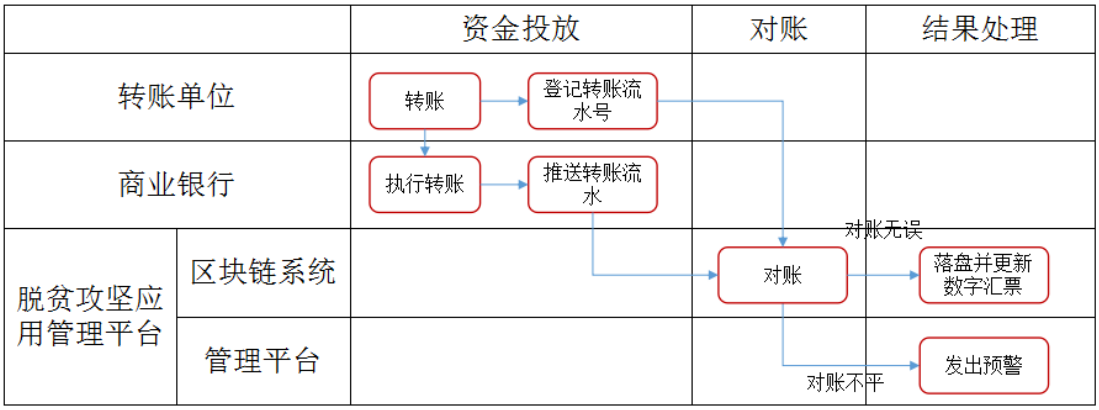

图 6.4 实时对账流程

(1) 转账单位根据“数字汇票”上的信息（转账金额、拨款账户、收款账户、转账截止时间）在规定的时间内向规定的收款账户转账。转账完成后，根据银行转账回执，在扶贫资金管理平台上登记转账流水号，转账流水号直接发送到区块链系统的对账智能合约。

(2) 商业银行执行转账，并将转账流水推送到平台，转账流水直接发送到区块链系统的对账智能合约。

区块链系统的对账智能合约根据转账部门登记的转账流水号，获取商业银行推送过来的转账流水，根据“数字汇票”的信息，核对转账金额、拨款账户、收款账户、转账截止时间等信息是否合规，如果有不合规之处，将不合规信息推送到管理平台，发出预警。如果对账无误，则落盘数据，并更新“数字汇票”。

6.3.2.1 系统框架

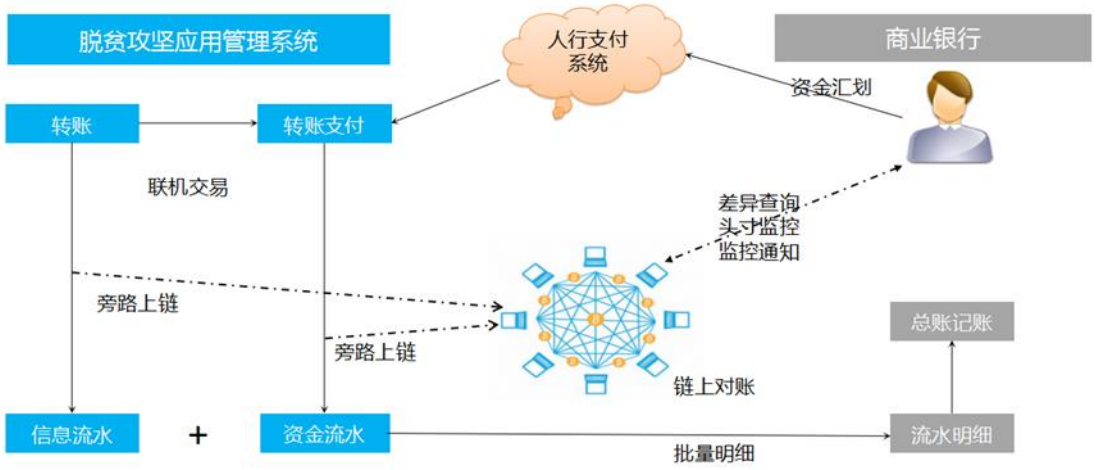

图 6.5 实时对账系统架构图

6.3.2.2 智能合约设计

(1) 实现功能

实时流水对账，及时发现对账差异。

(2) 触发时机

每条交易流水和资金流水上报都会调用该合约的接口。

(3) 运行逻辑

流水对账智能合约每收集到一条流水就会存储并执行对账逻辑(根据业务流水号、转账金额、拨款账户、收款账户、转账截止时间进行对账)，对平的流水就会实时清除，不平的流水根据发生时间判断，超过一定阈值，就认为是对账差异，需要进行告警和后续处理。

(4) 数据结构

表 6.3 对账智能合约存储数据

存储数据	说明
Account	银行账户
Amount	拨款金额
ActualAmount	实际拨款金额
DeadLine	拨款截止时间
ActualTimeOfRemit	实际拨款时间

SerialNumber	银行汇款流水号

表 6.4 对账智能合约接口

接口	输入	输出	说明
checking	银行汇款流水号	对账结果	如果对账没有问题，自动更新数字汇票中的相关字段，否则，将错误信息输出

6.4 技术路线

基于区块链的脱贫攻坚应用管理平台以 web 应用形式呈现，设计 MVCB 的软件架构。

MVCB(Model-View-Controller-Blockchain)，即把每一个应用的输入、处理、输出流程按照 Model、View、Controller、Blockchain 的方式进行分离，这样应用被分成四个层——模型层、视图层、控制层、区块链层。

视图(View)：代表用户交互界面，对于 Web 应用来说，可以概括为 HTML 界面。随着应用的复杂性和规模性，界面的处理也变得具有挑战性。一个应用可能有很多不同的视图，MVCB 设计模式对于视图的处理仅限于视图上数据的采集和处理，以及用户的请求，而不包括在视图上的业务流程的处理。业务流程的处理交予模型(Model)处理。比如一个 form 表单的视图只接受来自模型的数据并显示给用户，以及将用户界面的输入数据和请求传递给控制和模型。

模型(Model)：是业务流程/状态的处理以及业务规则的制定。业务流程的处理过程对其它层来说是黑箱操作，模型接受视图请求的数据，并返回最终的处理结果。业务模型的设计可以说是 MVCB 最主要的核心，它从应用技术实现的角度对模型做了进一步的划分，以便充分利用现有的组件，但它不能作为应用设计模型的框架。MVCB 设计模式把应用的模型按一定的规则抽取出来，应该组织管理这些模型，以便于模型的重构和提高模型的重用性。

业务模型还有一个很重要的模型那就是数据模型。数据模型主要指实体对象的数据保存（持续化）。从数据库获取数据表单信息，并将这个模型单独列出，所有有关数据库的操作只限制在该模型中。

控制(Controller)：可以理解为从用户接收请求, 将模型与视图匹配在一起，共同完成用户的请求。划分控制层的作用也很明显，它清楚地告诉你，它就是一

个分发器，选择什么样的模型，选择什么样的视图，可以完成什么样的用户请求。控制层并不做任何的数据处理。

区块链（Blockchain）：是应用程序中区块链部分，提供透明、不可篡改的分布式存储功能，并使用智能合约完成业务逻辑功能。

模型、视图与控制器的分离，使得一个模型可以具有多个显示视图。如果用户通过某个视图的控制器改变了模型的数据，所有其它依赖于这些数据的视图都应反映到这些变化。因此，无论何时发生了何种数据变化，控制器都会将变化通知所有的视图，导致显示的更新。这实际上是一种模型的变化-传播机制。模型、视图、控制器三者之间的关系和各自的主要功能，如图 6.6 所示。

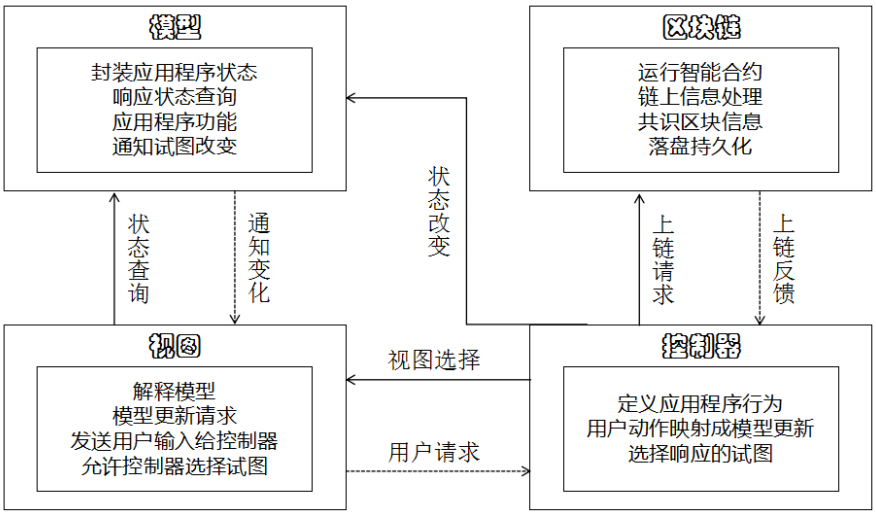

图 6.6 技术路线图

6.5 技术选型

图 6.7 技术选型图

(1) 后端技术：

整个后端是由 Node.JS 来驱动的，在这个基础之上使用 express 框架来快速

搭建 web 应用。数据库采用 mongoDB，以及对 mongoDB 快速建模的工具 mongoose。后端的模板引擎使用 jade。关于日期的格式化使用 Moment.js。

(2) 前端技术：

我们将使用符合规范的HTML5页面作为基于区块链的脱贫攻坚应用管理平台的前端展示技术，选用 jQuery 类库，以及 Bootstrap 样式框架，它们都是网站前端的静态资源。

(3) 区块链技术：

区块链底层基础平台采超级账本 fabric 的应用框架。

超级账本是 Linux 基金会于 2015 年发起的首个面向企业应用场景的开源分布式账本平台。如果说以比特币为代表的数字货币提供了区块链技术应用的原型，以太坊为代表的智能合约平台延伸了区块链技术的功能，那么进一步引入权限控制和安全保障的超级账本项目则开拓了区块链技术的全新领域。超级账本首次将区块链技术引入到了分布式联盟账本的应用场景，这就为未来基于区块链技术打造高效率的商业网络打下了坚实的基础。

6.6 系统展示

基于区块链的扶贫资金管理平台的首页如下图所示，首页起到了一个全局总览的作用，所有重要信息一目了然。在首页最显眼的位置，呈现了系统最关键的信息——区块链运行情况和扶贫资金使用情况。区块链运行情况展示区域展示了当前区块高度和正在运行的智能合约的个数；扶贫资金使用情况展示区域展示了当前扶贫资金累积投放金额、帮扶乡镇个数和资金安全运行时间的信息。区块链的使用保障了资金的安全、多方高效地协同和有效的监管。

联盟链相对于公有链最大的一个区别就在于联盟链具有严格的资格审查机制和用户权限划分，不同的用户具有不同的访问权限。平台根据扶贫业务严格划分用户权限。

图 6.8 平台首页

下面按照业务流程对系统进行详细展示，首先是项目申请，项目的申请由当地县政府办公室登录平台进行项目的录入申请，如下图所示为雷山县政府办公室相关工作人员任鹏登录平台，进入项目申请页面，发起了项目名为“农村种植产业扶贫项目”的申请，在该页面需要录入诸如县责任部门、项目建设预算、项目承接单位等重要信息。项目信息登记完成之后点击申报，将触发项目申请智能合约，经过多方共识之后，将该项目信息成功上链。

图 6.9 平台项目申请页

项目申请之后，项目将处于待审批状态。审批将由省脱贫攻坚指挥部完成，如下图所示，脱贫攻坚指挥部相关工作人员胥月登录平台，进入项目查询页面，在该页面列出了当前所有项目，项目的状态一目了然。选择将要审批的项目，点击进入后将会看到该项目的详细信息。进入项目审核页，根据项目资料对项目的

合规性进行判断，完成项目的审批工作。这一步将触发项目审批智能合约和数字汇票智能合约，根据审批意见完成项目状态的变更，并生成数字汇票。

图 6.10 平台项目列表页

图 6.11 平台项目详情页

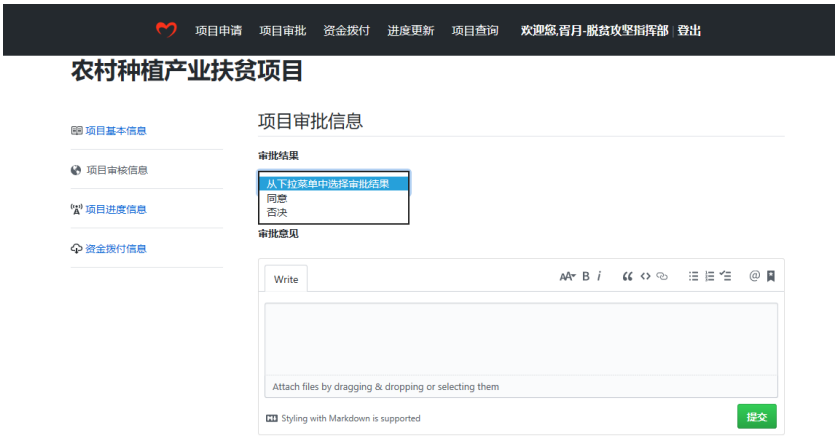

图 6.12 平台项目审批页

数字汇票生成后将进入区块链网络中进行流转，相关方登录后将会在资金拨付页面看到与自己相关的数字汇票信息。微众银行相关工作人员李一鸣收到相关通知后登录平台，进入资金拨付页面，就可以看到与自己相关的拨款信息，按照信息完成拨款之后，登记银行转账流水号。此时，将会触发实时对账智能合约，将对资金、收付款账号等信息进行验证。验证通过之后数字汇票向预先设定的下一级流转。

图 6.13 平台资金拨付页

当所有资金到位后，项目实施单位使用数字汇票进行承兑，进行项目实施。为了

保障资金的高效实用，资金的拨付采用按需拨付的方式。项目实施单位按照预先商定的时间完成相关工作，并登记上链。如下图所示，农科所相关工作人员杜明晓登录平台后进入项目进度页面，将当前进度信息和进度证明登记上链。

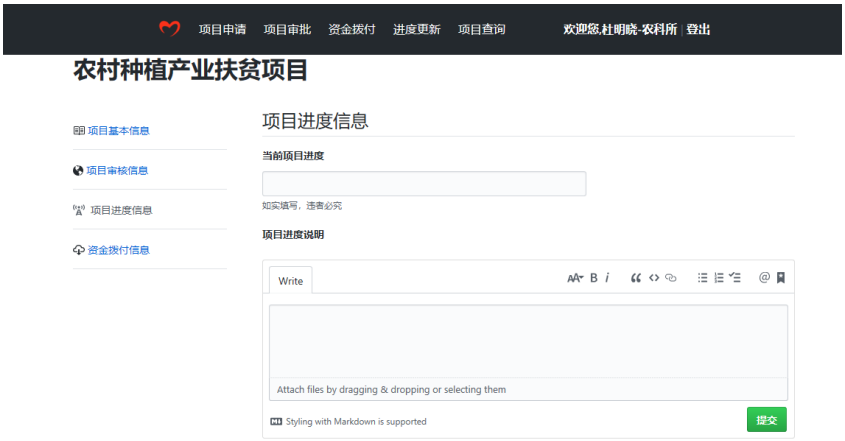

图 6.14 平台项目进度更新页

6.7 本章小结

通过使用区块链技术，将原来单方管理变为“可视化”公开管理，全程穿透，公开透明，实时监管，一定程度上解决了原来因为层层加码、层层沉淀所造成的信用可达性和管理有效性随着层级的增加而逐渐衰减的问题。通过“数字票据”的形式对资金进行数字化处理，两头见“钱”，中间采取“数字汇票”+智能合约的流通模式，即中间步骤“有数无钱”，开端使用省政府的强信用对“数字票据”背书，保证“数字票据”的真实性，中端使用商业银行的强信用对转账背书，保证转账上链信息的真实性，同时区块链为“数字票据”提供了安全、可信的运行流转环境。一定程度上解决了无法实时、全面的了解扶贫资金的使用情况和项目的开展情况的问题。在这样一个结合了完善规章制度和先进科学技术的闭环系统中，扶贫资金将得到更大的保障。

第7章 总结与展望

7.1 总结

脱贫攻坚是“第一民生工程”，是普惠千万贫困百姓的举措。新技术的发展为扶贫工作提供了全新的解决方案。区块链技术具有安全可靠、可追溯、不可篡改、透明性高、利于多方协同等特点。因此，区块链技术的运用，为实时、全面的了解扶贫资金的使用情况和项目的开展情况，保障数据的可追踪和不可篡改，实现精准的资金管控提供了可能的实现手段。

根据实际项目需求，提出了“脱贫攻坚+区块链”的解决方案。设计并实现了基于区块链技术的扶贫资金管理平台，设计了基于区块链技术的链上“数字汇票”和实时对账系统，双管齐下，做到了对扶贫资金从发行、流转到最终使用的全流程闭环监控。

基于实际项目需求，本论文对区块链技术现阶段存在的相关问题进行研究，对共识机制和系统架构做出了分析并改进。本文通过分析当前区块链共识机制存在的问题，提出了基于信用评分的主节点切换协议的 CBFT 共识算法，保障了区块链系统的安全性和活性。在系统架构方面，本文设计了多链架构，对请求进行并行处理，从而提升了区块链系统的 TPS。

本文一方面探索了区块链在扶贫场景的应用模式。另一方面，研究并设计了新的共识算法和系统架构，经过实验验证，提高了区块链系统的安全性和 TPS。本论文是国内较早探索区块链在扶贫场景应用的研究，为区块链技术在中国的实际落地应用提供了借鉴经验。

7.2 展望

经过研究生近三年的学习与研究，对区块链这项新兴技术由陌生到熟悉再到像对自己孩子一样，对它拥有一份寄托和希望。但是，在它真正长大之前，仍然有许多问题亟待解决，区块链技术尚处于发展初期，还有许多技术需要突破，还有很多应用场景需要拓展。简述如下，望能够起到抛砖引玉之用。

(1) 技术的突破

现阶段区块链技术有三大方面需要突破，分别是性能的提高，异构区块链的通信和存储空间的裁剪。当前区块链的性能只能应用在一些低频交易的场景，对

于诸如证券交易、电子商务等场景只能望洋兴叹；异构区块链的通信是下一代区块链的一个方向，是区块链世界互联的一个必经之路；随着时间的推移，存储空间的限制必将显现，数据的爆炸也将是亟待解决的重要问题之一。

(2) 应用的拓展

现阶段，除了比特币以外，尚未有第二个杀手级应用出现，一方面是技术的不完善限制了杀手级应用的出现，另一面，尚有许多场景有待开发。本文认为，区块链之核心基于两点，安全与协同，于此相关，本文相信，区块链在监管领域并将有所作为。

展望未来，区块链技术必将大有所为！

致谢

时光飞逝，转眼间三年的硕士生涯即将画上句号。我要由衷感谢我挚爱的母校同济大学，提供给我们优质的学习、生活条件以及顶级的师资队伍；感谢老师们，提供给我的教育以及学术指导；感谢班上的同学，和我一起为未来拼搏、奋斗。

由衷感谢我的导师马小峰教授。您严谨求实的学术思想以及宽厚儒雅的人格魅力，一直都是我的榜样。三年的研究生学术生涯，您不但以丰富的学术经验以及工程经验帮助我解决一个又一个的学术难题，而且还时常关心我的生活、给予我鼓励。感谢您在课题研究过程中，从论文选题、实验设计以及论文写作，均耐心地给予我指导；同时，也正因为您的支持，我才有幸多次参加重要项目，拓宽自己的视野。谢谢老师，是您让我实现了蜕变、成长。

感谢同实验室的胥月、侯玉娇、陈杰樱、任鹏、王意、徐晶晶、刘烈彤和王铎，三年间，我们一起做项目、一起外出开会、一起组织实验室聚餐等等，由衷感谢你们这三年的陪伴，也衷心祝愿你们在以后的工作学习中一帆风顺。

最后，我要把最为真挚的谢意以及最为深沉的爱留给我的父母。感谢父母总是无条件的信任我、支持我，从进入大学到现在，你们总是我最坚强的后盾。于我而言，你们始终是我人生中最为重要的部分，今后我一定会更加努力，争取好的成绩来回报你们。

2018.03.13

参考文献

[1] 姚前. 中国法定数字货币原型构想[J]. 中国金融,2016,17:13-15.

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

[3] Zyskind, Guy,Nathan, Oz,Pentland, Alex et al.Decentralizing Privacy: Using Blockchain to Protect Personal Data[C].//2015 IEEE Security and Privacy Workshops: 2015 IEEE Security and Privacy Workshops (SPW 2015), 21 May, 2015, San Jose, CA, USA.2015:180-184.

[4] Kraft D. Difficulty control for blockchain-based consensus systems[J]. Peer-to-Peer Networking and Applications, 2016, 9(2):397-413.

[5] 杨晓晨,张明.比特币：运行原理、典型特征与前景展望[J].金融评论,2014,(1):38-53.

[6] 陈道富,王刚.比特币的发展现状、风险特征和监管建议[J].学习与探索,2014,(4):88-92.DOI:10.3969/j.issn.1002-462X.2014.04.018.

[7] 黄永刚.基于区块链技术的电子健康档案安全建设[J].中华医学图书情报杂志,2016,25(10):38-40,46.DOI:10.3969/j.issn.1671-3982.2016.10.008.

[8] 张立钧.未来区块链应用更多向智能合约发展[J].金卡工程,2016,(8):20-21.

[9] 刘德林.区块链智能合约技术在金融领域的研发应用现状、问题及建议[J].海南金融,2016,(10):27-31.DOI:10.3969/j.issn.1003-9031.2016.10.05.

[10] 范一飞. 中国法定数字货币的理论依据和架构选择[J]. 中国金融,2016,17:10-12.

[11] Nine out of 10 Major Banks in North America and Europe are Exploring the use of Blockchain Technology for Payments, Accenture Survey Finds[J]. M2 Presswire,2016

[12] 聂舒,张一锋. 从SDDS看区块链技术的应用[J]. 中国金融,2016,17:35-36.

[13] 任安军. 运用区块链改造我国票据市场的思考[J]. 南方金融,2016,03:39-42.

[14] 中国区块链技术和应用发展白皮书（2016）

[15] Lamport L, Shostak R, Pease M. The Byzantine generals problem. ACM Trans. on Programming Languages and Systems,1982,4(3):382–401.[doi:10.1145/357172. 357176]

[16] Castro M, Liskov B. Practical Byzantine fault tolerance and proactive recovery. ACM Trans. on Computer Systems,2002,20(4):398–461.[doi:10. 1145/571637. 571640]

[17] 基于区块链构建数字票据[J].上海国资,2016,(3):80-81.decimal

[18] King S, Nadal S. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake[J]. 2012.

[19] Kurt Fanning,David P. Centers. Blockchain and Its Coming Impact on Financial Services[J]. J. Corp. Acct. Fin,2016,27(5):.

[20] H, e, g, et al. Analysis of Present Day Election Processes vis-à-vis Elections Through Blockchain Technology[J]. Social Science Electronic Publishing, 2017.

[21] 中国人民银行上海总部金融服务一部课题组,季家友. 关于建设全国电子票据交易平台的研究[J]. 金融电子化,2015,(03):67-69.

[22] 王宏,孔劼,王魁生等.可追溯实名防伪票据系统的设计与实现[J].现代电子技术,2016,39(6):127-131.DOI:10.16652/j.issn.1004-373x.2016.06.034.

[23] David Wigan.Microsoft clicks on blockchain[J].International financing review: IFR,2015,(Nov.14 TN.2109):66-67.

[24] Michele Spagnuolo,Federico Maggi,Stefano Zanero et al.BitIodine: Extracting Intelligence

from the Bitcoin Network[C].//Financial cryptography and data security: 18th International conference on financial cryptography and data security (FC 2014), March 3-7, 2014, Christ Church, Barbados.2014:457-468.

[25] Chris Rose.The Evolution Of Digital Currencies: Bitcoin, A Cryptocurrency Causing A Monetary Revolution[J].International business & economics research journal,2015,14(4):617-621.

[26] Dev, Jega Anish.Bitcoin mining acceleration and performance quantification[C].//2014 IEEE 27th Canadian Conference on Electrical and Computer Engineering: 2014 IEEE 27th Canadian Conference on Electrical and Computer Engineering (CCECE), 4-7 May 2014, Toronto, ON, Canada.2014:1-6.

[27] Moser, Malte,Bohme, Rainer,Breuker, Dominic et al.An inquiry into money laundering tools in the Bitcoin ecosystem[C].//2013 eCrime Researchers Summit: 2013 eCrime Researchers Summit (eCRS), 17-18 Sept. 2013, San Francisco, CA, USA.2013:1-14.

[28] Beikverdi, Alireza,Song, JooSeok.Trend of centralization in Bitcoin's distributed network[C].//Software engineering, artificial intelligence, networking and parallel/distributed computing: 2015 IEEE/ACIS 16th international conference on software engineering, artificial intelligence, networking and parallel/distributed computing (SNPD 2015), June 1-3, 2015, Takamatsu, Japan.2015:1-6.

[29] 俞佳佳.数字货币支付功能探索及思考[J].海南金融,2016,(3):79-83.DOI:10.3969/j.issn.1003-9031.2016.03.17.

[30] 李根.论数字货币的现状影响因素及发展趋势[J].商,2016,(10):173-173,163.

[31] 朱阁.数字货币的概念辨析与问题争议[J].价值工程,2015,34(31):163-167.

[32] 黄锐.金融区块链技术的监管研究[J].学术论坛,2016,39(10):53-59.DOI:10.3969/j.issn.1004-4434.2016.10.012.

[33] 何明星,李鹏程,李虓等.高效的可证明安全的无证书数字签名方案[J].电子科技大学学报,2015,(6):887-891.DOI:10.3969/j.issn.1001-0548.2015.06.016.

[34] Swan M. Blockchain: Blueprint for a New Economy[M]. O'Reilly Media, Inc. 2015.

[35] Pazaitis A, De Filippi P, Kostakis V. Blockchain and Value Systems in the Sharing Economy: The Illustrative Case of Backfeed[J]. Social Science Electronic Publishing, 2018, 125.

[36] Hancock M. Digital transformation in government and blockchain technology[Z].

[37] Lemieux V L. Trusting records: is Blockchain technology the answer?[J]. Records Management Journal, 2016(2).

[38] Cohen L, Tyler R, Contreiras D, et al. Blockchain's three capital markets innovations explained[J]. International Financial Law Review. 2016, 35.

[39] Greg I, John H. How blockchain-timestamped protocols could improve the trustworthiness of medical science:[J]. F1000 Research. 2016, 5.

[40] Zyskind G, Nathan O, Pentland A S. Decentralizing Privacy: Using Blockchain to Protect Personal Data[C]. IEEE Security and Privacy Workshops, 2015. 2015: 180-184.

[41] Malinova K, Park A. Market Design for Trading with Blockchain Technology[J]. Social Science Electronic Publishing. 2016.

[42] Huckle S, White M. Socialism and the Blockchain[J]. 2016.

[43] Peters G W, Panayi E, Chapelle A. Trends in Crypto-Currencies and Blockchain

Technologies: A Monetary Theory and Regulation Perspective[J]. Social Science Electronic Publishing, 2015, 3.

[44] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[J]. Consulted, 2008.

[45] 刘肖飞. 基于动态授权的拜占庭容错共识算法的区块链性能改进研究[D]. 浙江大学, 2017.

[46] 黄秋波, 安庆文, 苏厚勤. 一种改进PBFT算法作为以太坊共识机制的研究与实现[J]. 计算机应用与软件, 2017, 34(10).

[47] 黄洁华, 高灵超, 许玉壮,等. 众筹区块链上的智能合约设计[J]. 信息安全研究, 2017, 3(3):211-219.

[48] Milutinovic M, He W, Wu H, et al. Proof of Luck: an Efficient Blockchain Consensus Protocol[J]. 2017.

[49] Technical report by the UK government chief scientiflc adviser[Online], available: HTTPs://www.gov.uk/government/uploads/system/uploads/attachment data/flle/492972/gs-16-1 -distributed-ledger-technology.pdf, February 21, 2016

[50] Huckle S, Bhattacharya R, White M, et al. Internet of Things, Blockchain and Shared Economy Applications ☆[J]. Procedia Computer Science, 2016, 98(C):461-466.

[51] 薛腾飞, 傅群超, 王枞,等. 基于区块链的医疗数据共享模型研究[J]. 自动化学报, 2017, 43(9):1555-1562.

[52] 安庆文. 基于区块链的去中心化交易关键技术研究及应用[D]. 东华大学, 2017.

[53] 张俊, 高文忠, 张应晨,等. 运行于区块链上的智能分布式电力能源系统:需求、概念、方法以及展望[J]. 自动化学报, 2017, 43(9):1544-1554.

[54] 胥月, 马小峰. 基于区块链的学生行为综合评价体系的研究与实现[J]. 信息技术与信息化, 2016(12):131-133.

[55] Underwood S. Blockchain Beyond Bitcoin[J]. Communications of the Acm, 2016, 59(11):15-17.

[56] Rizzo P. World Economic Forum Survey Projects Blockchain 'Tipping Point' by 2023[Z]. 2015.

[57] 安瑞, 何德彪, 张韵茹,等. 基于区块链技术的防伪系统的设计与实现[J]. 密码学报, 2017, 4(2):199-208.

[58] 张宁, 王毅, 康重庆,等. 能源互联网中的区块链技术:研究框架与典型应用初探[J]. 中国电机工程学报, 2016, 36(15):4011-4022.

[59] Allayannis G, Fernstrom A. An Introduction to Blockchain[J]. Social Science Electronic Publishing, 1969, 20(4):568.

[60] Pilkington M. Blockchain Technology: Principles and Applications[J]. Social Science Electronic Publishing, 2016.

[61] García-Bañuelos L, Ponomarev A, Dumas M, et al. Optimized Execution of Business Processes on Blockchain[M]// Business Process Management. 2017.

[62] Irving G, Holden J. How blockchain-timestamped protocols could improve the trustworthiness of medical science[J]. F1000research, 2016, 5:222.

[63] Sharples M, Domingue J. The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward[C]// European Conference on Technology Enhanced Learning. Springer, Cham, 2016:490-496.

[64] Pazaitis A, De Filippi P, Kostakis V. Blockchain and Value Systems in the Sharing Economy: The Illustrative Case of Backfeed[J]. Social Science Electronic Publishing, 2018, 125.
[65] 廖建桥, 张万山. 论中文的阅读速度[J]. 人类工效学, 1996(1):38-41.
[66] 王振亚. 阅读理解的准确性与阅读速度[J]. 外语界, 1989(3):30-34.
[67] Kraft D. Difficulty control for blockchain-based consensus systems[J]. Peer-to-Peer Networking and Applications, 2016, 9(2):397-413.
[68] Gramoli V. From blockchain consensus back to Byzantine consensus[J]. Future Generation Computer Systems, 2017.
[69] Lee B, Lee J H. Blockchain-based secure firmware update for embedded devices in an Internet of Things environment[J]. Journal of Supercomputing, 2017, 73(3):1-16.
[70] Lee J H. BIDaaS: Blockchain based ID as a Service[J]. IEEE Access, 2017, PP(99):1-1.

个人简历、在读期间发表的学术论文与研究成果

个人简历：

李一鸣，男，1993年3月生。

2015年6月毕业于西安邮电大学 广播电视工程专业，获学士学位。

2015年9月入同济大学 控制科学与工程系 控制理论与控制工程专业，攻读硕士学位。

待授权发明专利：

[1] 马小峰，李一鸣.基于区块链的信用兼职平台（已受理）