* 1. 研究背景

//大大大！背景（中央）

精准扶贫是“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，举全社会之力精准扶贫。2013年，习近平在湖南调研时，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。“扶贫开发要贵在精准，重在精准，成败之举在于精准。”

//背景（贵州省的战略）

为加快贵州省极贫乡（镇）脱贫步伐，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，

//脱贫攻坚投资基金介绍

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。

//痛点：

由于传统的组织架构和管理方式的限制，全省财政扶贫开发投入资金虽然总体规模大，但资金“碎片化”，“各自为政、条块分割”，项目多头申报、资金重复安排。随着资金的下发，可信程度逐渐衰减。为了解决这一问题，目前往往采用增加管理层级的方式，这又带来了管理成本急剧上升、资金沉淀比例增加等问题。具体到极贫乡镇业务，领导小组需要能实时、全面的了解到极贫乡镇基金的管理使用和项目动态信息；贵民集团和商业银行需要能实时了解到资金流转和使用情况，并根据不可篡改的项目进度资料等信息进行资金的监控。

//为什么用区块链

新技术的发展为扶贫工作实现精准化提供了全新的解决方案，其中区块链技术的运用，为实时了解项目进展和资金流转信息、资料和数据的可追踪和不可篡改、精准的资金控制（专款专用）等穿透式管理的需求，提供了前所未有的实现手段。

//理由1：智能合约

区块链的重要功能之一，智能合约，能够让参与各方按照事先约定好的规则，在工作流程中自动进行数据、资产和资金的转移，整个过程透明、可控、不受人为干扰。通过智能合约，在资金划拨阶段就可规定好其用途、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。

//理由2：透明性，安全性

区块链具有分布式存储、非对称加密、共识认证和智能合约等技术特征，在适当（监管和保密的平衡）保护隐私的前提下，为数据和信息的传递提供前所未有的透明性、公开性和安全性。基于区块链技术形成的数据拥有完整性、可靠性、连续性、永久性、可追溯性、不可篡改、与透明性等特点。

//理由3：可信数据

区块链扶贫体系是现有信息基础设施建设的进一步延伸。区块链以其信任性、安全性、不可篡改性的特征，在块数据、流数据的融合中解放数据孤岛、条块的束缚，让数据真正“放心”的流动起来，释放更大的数据潜能。经过区块链交换、融合的数据信息，在区块链的技术保障下，成为大数据分析系统可信任的数据来源，从而充分体现数据挖掘分析效果，为科学预测和规划的根据。这对于实现大扶贫战略具有十分重要的意义。

//意思是这个意思，但是要换个好一点的语言表达

本论文取材于真实案例，以贵州省脱贫攻坚子项目——贵州脱贫攻坚投资极贫乡（镇）基金项目为依托，提出了基于区块链技术的精准扶贫新模式。

* 1. 研究问题

新技术的发展为扶贫工作实现精准化提供了全新的解决方案，其中区块链技术的运用，为实时了解项目进展和资金流转信息、资料和数据的可追踪和不可篡改、精准的资金控制（专款专用）等穿透式管理的需求，提供了前所未有的实现手段，本文将对以下两个问题进行研究。

1. 智能合约的研究和设计。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）基金业务完美结合，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，使得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。
2. 区块链性能的的研究和优化。区块链的性能一直是制约区块链发展的最重要瓶颈，如何提高区块链的性能，提高区块链对其上层业务的处理能力，本篇论文将从两个方面进行研究。一是架构的优化和改进，传统的区块链的架构都为单链，数据处理能力低，且可扩展性差，本论文将对架构进行优化和改进，采用多链架构，结合跨链技术可对数据进行并行处理，从而大大提高区块链系统的性能；二是共识算法的优化和改进，影响区块链性能的另一个关键因素——共识算法。因此为了提高区块链的性能，本论文将对共识算法进行优化和改进，定制化适合脱贫攻坚投资极贫乡（镇）基金应用场景的拜占庭一致性算法。
   1. 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、及时、准确的用在最需要的地方而不是被挪用、延误或浪费。本论文提出的基于区块链的精准扶贫应用平台（贵阳市大扶贫区块链应用系统工程），提供了对扶贫资金有效管理和使用的途径。通过智能合约，在资金划拨阶段就规定好其用途、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，改“大水漫灌”为“精准滴灌”，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，区块链系统为未来对接央行法定数字货币提供了基础，实现资金更为精准的投放和审计跟踪。在数字货币可以发放到农户并由农户自由使用后，可结合农村电商等实现资金的高效实用和数字货币应用的闭环场景

综上所述，基于区块链的精准扶贫应用平台的设计与实现对于解决脱贫攻坚中存在的问题是一个非常积极的研究和探索，因此本论文的研究课题具有重要的实践意义。

本课题的研究为未来数字货币的实际应用场景提供了一种思路和方向，同时也为区块链技术在中国的落地实际应用提供了借鉴经验，因此，本论文的研究课题具有重要的理论意义。

* 1. 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[5]。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[6]，陈道富等对比特币风险特征、监管建议的研究[7]，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[8]，荣希对区块链在资产证券化中的应用的研究[9]，黄永刚对区块链在电子健康档案安全建设中应用的研究[10]。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[11]，张立钧[12]和刘德林[13]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[14]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[15]。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[16]。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[18]。

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[26]，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[27]。

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”[28]。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[29]。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。

* + 1. 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[30]。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[31]。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[39]。

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[23]。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[32]。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[40]。

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[24]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[43,44,45]。

* 1. 论文难点和创新点

通过查阅文献和实际调查，本论文认为在基于区块链的精准扶贫应用平台设计和实现过程中有以下几个难点。

1. 智能合约研究与设计。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）基金业务完美结合，智能合约的设计至关重要，设计智能合约是本文的核心之一和难点之一。智能合约不仅需要满足脱贫攻坚投资极贫乡（镇）基金业务需求，还需要达到一定的安全要求和性能要求。本文在设计数字票据的数据结构的过程中，本文研究并总结了RScoin和BitMint在数字货币中的设计思路和成功经验，并且借鉴了国内一些电子票据交易平台的设计原理和系统架构，预期设计的智能合约能够满足脱贫攻坚投资极贫乡（镇）基金业务的功能要求、安全性要求和性能要求。
2. 区块链技术架构的选型。目前区块链技术架构主要包括比特币、以太坊、超级账本、Ripple等，不同的区块链技术架构功能和特性不同，且各自侧重于不同的业务场景。目前，虽然每个区块链技术架构都发布了自己的白皮书和技术文档，许多技术人员也对这些区块链技术架构的特点、使用方法做了详细介绍和解读，但是没有学者或者技术人员把几种主流的区块链技术架构进行全方位的比较和分析，因此本文需要对不同的区块链技术架构进行分析和分类，根据数字票据的特性选择本文设计的数字票据交易平台的区块链技术架构。
3. 拜占庭一致性算法的性能测试与提升。虽然很多学者对区块链的应用前景非常乐观，但是同时也指出了区块链的一些缺陷，其中最大的缺陷在于基于区块链的系统单位时间内的交易或者活动数量远远不如现在成熟的应对高频交易或者海量数据的技术解决方案。区块链由于其分布式账本和共识机制使得区块链难以应付高频交易的场景。但是在特定场景下，可以对共识算法进行改进和完善。从应对高频交易、共识速度、节点安全三个维度来分析定制化适合脱贫攻坚投资极贫乡（镇）基金应用场景的拜占庭一致性算法。
4. 跨链并行计算方案的研究与设计。区块链技术是一种分布式账本技术，但是受吞吐量、网络孤立性、监管、伸缩性等因素的制约，目前的区块链项目并不能很好的服务于商业应用。在区块链所面临的诸多问题中，网络孤立性阻碍了不同区块链之间的协同操作，极大程度的限制了区块链的发挥空间。本文对跨链并行计算方面的探索与研究，打破区块链的信息孤岛，构建互联、互通、互信的通信网络，让区块链技术的潜能得到更大的释放。

区块链虽然是一个新兴技术，但是目前国内关于区块链的研究发展迅猛，本文对区块链在精准扶贫场景的研究和实践是具有创新意义和探索意义，可以为后来者提供丰富的借鉴经验和理论基础。本文设计的基于区块链的精准扶贫应用平台具有以下两个创新点。

1. 系统性的对区块链在精准扶贫场景的应用进行了探索、研究、设计和实现。本文借鉴了我国法定数字货币的设计思路，结合区块链技术的优点，在实践中尝试构建基于区块链的精准扶贫应用平台。本文的研究成果和设计方案可以为之后希望在精准扶贫与区块链相结合的研究领域的研究人员提供研究经验和理论基础，为未来数字货币的实际应用场景提供了一种思路和方向，同时也为区块链技术在中国的落地实际应用提供了借鉴经验。
2. 拜占庭共识算法进行了量化分析和研究。针对拜占庭共识算法的特点和精准扶贫应用场景的特点，对低频交易和存在强信用节点的区块链网络中的拜占庭共识算法进行优化和改进。现在国内关于拜占庭容错机制的研究比较丰富，但是大多都是对大数据、云计算、分布式计算等领域的研究，区块链中共识机制是一个非常重要的部分，本文对区块链中共识机制的量化分析以及优化改进可以为以后对区块链中共识机制这一部分的深入研究提供切入点和新思路。
3. 跨链并行计算方案的研究与设计。如果说共识机制是区块链的灵魂核心，那么对于区块链特别是联盟链及私链来看，跨链技术就是实现价值网络的关键，它是把联盟链从分散单独的孤岛中拯救出来的良药，是区块链向外拓展和连接的桥梁。同时，跨链技术的使用将进一步提高区块链系统的性能，正所谓“众人拾材火焰高”。本文从性能、安全、可扩展性三个维度，结合脱贫攻坚投资极贫乡（镇）基金应用场景实际需求，参考webank的基于DCN的分布式架构，Polkadot、Cosmos等区块链平台的跨链技术研究并设计一种基于proxy的跨链并行计算方案，本文的跨链技术研究为跨链技术的发展与研究提供了一种新颖的思路和方向。
   1. 论文结构

本论文包括三个部分。

第一部分包括第2章，主要内容是分析传统扶贫资金的管理中存在的缺陷和问题；同时对区块链进行了简要介绍，并重点分析了目前常用的区块链技术架构的特点。最后根据扶贫资金管理中存在的缺陷和问题选择合适的区块链技术架构并阐述了选型依据，提出本文基于区块链的扶贫资金管理的解决方案。

第二部分包括第3章，主要内容是介绍本文设计的基于区块链的精准扶贫应用平台的系统架构、数据结构、业务流程、智能合约设计和实现原理等。

第三部分包括第4章、第5章、第6章，主要内容是本文中三个创新点——业务创新、架构创新、算法创新。并设计了一套完整的区块链一致性协议的测试体系和方法，在该方法的基础上对本文设计和实现的区块链系统进行评测并分析测试结果。