各位老师同学们，你们好。我是杜治国老师的学生苏锐佳，我的开题报告内容是《区块链共识机制的研究与开发》。

这是目录，我们先研究背景和国内外研究现状切入本课题提出的新的共识机制以及一些问题，然后则是拟完成工作。

区块链首先是一个分布式系统，因此在区块链技术框架的工作流程中，共识机制是一个核心问题。在进入3.0联盟链时代以来，区块链已应用于各种商业场景，当然，其中也包括区块链溯源这一个方向。但是，目前还没有针对这一个方向进行的共识算法的优化研究，因此，借助Fabric框架的诸多特性，我们将在区块链溯源这一方向上对共识机制进行优化。

这是国内外研究现状，主要介绍几种目前主流的共识算法，比如大家都很熟悉的比特币所使用的工作量证明的共识算法，还有在联盟链中比较出名的瑞波共识算法和拜占庭容错算法。

接下来是本课题的主要内容，基于Fabric框架设计的新共识机制。选择Fabric框架的原因在于它提供了身份管理服务，这意味着节点只有被认可才能加入网络。这是我们优化的一个重要前提。

下面我们来讲解本课题提出的共识算法它的共识过程是怎么样的。首先，网络中每个节点都处于无请求状态、单请求状态和多请求状态这三种状态中的一种，默认是无请求状态。在节点发送了交易请求并在交易最终加入区块链这期间属于单请求状态。而多请求状态表示节点将有大批数据要加入区块链中。我们假设网络中有一个节点，暂时称为节点A，它有大批数据导入系统中。那么首先，节点A的状态由无请求状态转变成多请求状态，并在第一轮共识中，将第一次的交易请求和状态向全网进行广播，等待接收其他节点的状态信息。节点A将收到的其他节点及其状态加入一个状态列表中，这个列表中的节点数必须占全网节点80%以上，若没有，则从新生成。节点A的状态列表生成后，通过Fabric框架的通道服务将这个列表发送给列表中的所有节点，这样就形成了一个这样的网络。由于网络中只有节点A在发送交易请求，因此我们无需像瑞波共识算法等算法一样执行交易打包共识这一步。

接下来就是区块打包，共识过程。每一个节点将如下信息整合在一起计算成一个哈希并向状态列表重点节点广播。节点A收集哈希，计算比例，若超过80%，则区块哈希共识成功，然后如果这个哈希与自己生成的哈希相同，则说明自己打包的区块得到了确认，是新的被共识过的区块，直接存到本地，并且更新状态。如果自己的哈希与共识通过的哈希不同，那么重新开始共识过程，直到满足条件。至此，一个区块的共识过程结束，开启下一轮共识过程。从第二轮共识开始，继续使用第一轮的状态列表，并直接进行区块打包共识。

然后我们再看看这个算法可能出现的问题

前两种情况都将导致状态列表失效，因此我们需要重新生成状态列表。

第3种情况，假设节点B由无请求状态变成单请求状态，首先，我们让节点B向状态列表中的其他节点广播自己的交易，其他节点将收到的交易暂时缓存起来，等待这一轮节点A的区块共识结束。在下一轮中再将节点A和节点B的交易打包在一起。我们让节点B在广播了自己的交易后不进行任何等待反馈，而是在交易打包后直接进行区块打包并共识，如果成功，则进入下一轮共识，如果失败，则节点B继续向状态列表的其他节点发送自己的交易，直到成功为止。成功后，节点B的状态从单请求状态变成无请求状态。

第4中情况，在节点A进行完本轮的共识过程后，可将改变状态的节点加入状态列表中，形成新的状态网络，再按照上述第2种情况的解决方法去处理。

第5、6中情况，则只需恢复交易打包共识即可