各位老师同学们，你们好。我是杜治国老师的学生苏锐佳，我的开题报告题目是《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到即将提出的新的共识机制，还有新共识机制的一些问题，最后则是拟完成工作。

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，目前还确实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，我们在区块链溯源这一方向上对共识机制进行优化。

我们先来说一下这个题目是基于怎么样的场景下产生的。请看，数据录入区块链溯源系统时，区块的生成步骤大致如图所示。企业录入溯源数据，然后通过客户端应用发送交易请求。网络中的节点则尽可能多的接收交易，打包交易，然后进行区块共识。这两块组成了共识机制模块，目前主流的拜占庭容错算法大致都是分成这样两步走。共识模块一般几秒生成一个区块，在数据量少的时候对系统的性能影响不大，然而但有大量数据同时录入时，则会导致性能瓶颈，因此本课题要优化此场景下的共识机制。

在提出优化方案之前，我们先大致了解基于Fabric的茶叶产业链溯源系统的架构，因为共识机制的优化需要新利用到新系统的诸多功能特性。

首先是茶叶产业链溯源系统的架构和业务流程，这块和传统的溯源系统没太大区别，我们就不过多地讲。然后是Fabric框架，网络中存在两种节点，Peer节点和Orderer节点，Peer节点可充当多种角色，如Endorser节点和Committer节点。一个Fabric交易流程大致如下：客户端发送交易给一个或多个Peer节点。背书节点endorser收到后，验证权限并返回结果。然后客户端验证把收到的各个背书节点的应答打包到一起组成一个交易并签名、发送给Orderers节点。Orderers对接收到的交易进行共识排序，然后按照区块生成策略将一批交易打包到一起生成新的区块。

下面是Fabric框架与溯源系统的结合：

企业对溯源数据的增删改操作（未生成区块前）依旧在溯源平台上进行。Fabric则通过智能合约的方式对产品当前担责节点开放权限，防止非相关节点违规操作。被授予权限的参与者（企业）维护信息时需以私钥连接到网络中，而一旦参与者发起产品转移，系统通过内嵌的智能合约进行相关的审核，通过后将参与者之前提供的信息打包录入区块链中。

为什么选择Fabric框架？因为Fabric框架提供身份管理服务，成员必须被许可才能加入网络，这是我设计的新共识机制的一个基础前提。