各位评委老师，你们好，我是来自计算机科学与技术专业电计1604的徐富，我的指导老师是吴迪老师。论文的题目是，基于区块链的医疗记录存储系统研究与开发。

我的答辩将由以下几部分展开

首先是 系统概述

传统的医疗机构以纸质版的形式保存患者的医疗数据，形式单一且检索困难。随着互联网技术的飞速发展，医疗行业也呈现出信息化的发展趋势，但目前的电子病历大都采用中心化的存储方式，面临数据泄露的风险，而且数据由各个医院单方面保管，无法实现共享。区块链具有去中心化和防篡改特性，应用到医疗系统中，能够实现数据安全共享，提高医疗行业服务质量，具有一定实际价值。

为推动区块链技术和产业发展，国务院工业和信息化部软件服务业开展区块链专题研究，发布了《中国区块链技术和应用发展白皮书》。目前区块链的应用主要有金融科技、物流溯源以及供应链领域等，在医疗方面的应用研究相对较少。国外有学者利用以太坊平台，开发了一个医疗区块链与大数据相结合的信息共享系统 MedicalRecord，但以太坊采用的是POW共识算法，造成了一定的算力浪费。为了避免资源浪费，国内有学者提出将医疗机构根据信用积分划分等级，配合改进的股份授权证明机制实现共识，适用于解决各医疗机构共享数据的难题，但此模型启动时至少需要121 所医院的同时参与。针对其启动代价大的缺点，有学者使用实用拜占庭容错算法, 构建了一种既能以较少节点来启动运行，又不需要大量算力来维护的联盟式医疗区块链系统模型，具有较好的适用性。通过梳理国内外医疗区块链研究案例，可以发现，医疗领域的区块链应用场景尚不明确，本着探索的想法，本课题设计并实现一个基于hyperledger fabric的医疗数据存储系统。

系统参与方为，管理员，医生和患者，每个节点都是对等的，不再依赖中央机构。区块链网络中，大多数诚实节点通过共识机制建立信任，共同维护一个分布式大账本，记录不可篡改，可以保证数据在链上的真实性与安全性；同时，病历数据上链前和传输过程中都必须经过签名加密来保证数据隐私性，患者拥有病历数据控制权，医生或研究人员需要向患者申请授权才能访问病历数据。在保证隐私安全性的前提下，授权管理使得病人对于就诊记录有更灵活的调度，防止病历数据被第三方机构恶意托管和出售。为跨医院就诊和远程医疗提供一种技术支持。

系统架构，使用fabric 框架维护世界状态，并存储患者的隐私数据。使用Go语言开发链代码，为java后端提供接口服务，访问区块链数据库。后端使用SSM开源框架实现业务逻辑，框架成熟，运行稳定；

这个图展示了响应用户的请求的一次完整流程，简单来说就是前端请求后端，后端将数据发给区块链。再将处理的结果逐级返回

第二部分，fabric环境搭建

首先介绍区块链的技术特点。去中心化。区块链底层采用P2P网络架构，可以直接进行点对点的价值传输。不可篡改。区块首尾相接，形成链状结构，全网广播的数据公开透明可溯源。节点通过共识机制建立互联网上的信任，确保区块数据的有效性达成一致。智能合约，是由程序员编写的存储在区块链上的计算机程序，满足条件就会自动执行。

Hyperledger fabric是联盟链中的优秀代表，具有很高的灵活性和可扩展性。成员管理服务MSP，提供通道成员身份管理、身份认证等服务，链码运行在Docker容器上，客户端通过SDK提供的API调用链码访问区块链数据库。Fabric共识过程也可以看做是一次交易的三个步骤，其中排序节点使用Etcdraft算法对交易进行排序。

设计的网络拓扑结构为，一个 orderer节点，两个peer节点属于两个组织，一个通道mychannel负责通信。通过cli客户端执行命令，fabric网络启动主要包括生成证书文件、生成创始区块、创建通道和部署合约等内容，环境搭建成功后，查看docker容器状态就是下面的图片显示的那样。

在fabric2.0中，对链码的安装和升级也要通过共识策略，例如在本系统中，必须得到两个组织的同时批准才允许修改链码。

下面是 后端架构设计

后端整体实现根据用户分类分为，管理员功能，通用功能，医生和患者功能模块

管理员不能干涉具体业务流程，主要任务就是维持系统的正常运行。用户模块是医生和患者的通用功能。管理员与用户通用功能不是系统核心部分，在一个真正的去中心化系统中，并非必要实现，这里只是起到辅助作用。下面介绍系统的核心功能

为了保证数据在存储与共享过程中的隐私安全性，系统引入RSA非对称加密算法。其中加密解密和签名验证的过程就是图中展示的这样。

这是新建病历流程，首先医生填写相关病历信息，签名加密后发送给患者，患者接收验证，如果签名和内容都正确就可以上传病历，存储到区块链上。

下面这张图是测试新建病历的截图，左面的图是医生新建的病历，右面的图是患者确认上传后又查询区块链获得的最新数据，可以看到，与医生新建病历内容一致

申请授权实现流程，医生向患者发出授权请求，患者查看待授权列表，如果同意，则获得授权的医生可以查询到病历数据

下面这张图是申请授权流程测试，左面是患者操作，result=0表示同意授权成功，右面这张图是医生根据自己的私钥查询到的病历数据，如果私钥错误或者没授权，得到的数据就都是null，

最后，总结 与 收获

整体上，系统使用区块链结合密码学技术实现医疗数据的安全存储和授权共享，区块链平均响应时间在1000ms的可接受范围内，证明了区块链在医疗领域的可行性，各个模块功能解耦，可扩展性强

下一步计划，首先是开发前端页面，使系统看起来更加完整；另外系统目前专注于医疗数据的存储和共享，可以看做医疗系统的一个子系统，如果想要实用，还要结合现实场景处理复杂的就诊流程。现在系统可以看作是一个半中心化系统，因为后端代码运行在服务器上，真正的去中心化应用应该是类似于比特币的DAPP客户端模式。不只医疗记录，只要遵守统一的协议，任何需要隐私保护的数据都可以存储到区块链上，我认为，区块链在存储系统的应用前景非常广阔。

我的答辩到此结束，欢迎评委老师批评指正

RSA 是目前应用最广泛的数字加密和签名技术，它的安全程度取决于秘钥的长度，目前主流可选秘钥长度为 1024位、2048位、4096位等（64的整数倍），RSA算法的安全性基于RSA问题的困难性，也就是基于大整数因子分解的困难性上，理论上秘钥越长越难于破解，当然更长的秘钥更安全，但也意味着会产生更大的性能开销。

DSA：和 RSA 不同的是 DSA 仅能用于数字签名，不能进行数据加密解密，其安全性和RSA相当，但其性能要比RSA快。

ECDSA：椭圆曲线签名算法，是ECC（椭圆曲线密码学）和 DSA 的结合，相比于RSA算法，ECC 可以使用更小的秘钥，更高的效率，提供更高的安全保障，据称256位的ECC秘钥的安全性等同于3072位的RSA秘钥，