厦门大学“大学生创新创业训练计划”
创新训练项目申报书

学　　院：	信息学院
项目名称：	基于智能合约的区块链系统
负 责 人：	庄震丰
联系方式：	18959211260
指导教师：	刘昆宏
职称：	教授
学历：	
E-mail：	lkhqz@xmu.edu.cn
项目申请日期：	2019 年 11 月 06 日
项目起止年月：	2019 年 11 月 06 日至 2021 年 11 月 06 日

厦门大学教务处

二〇一三年十一月

填 写 说 明

1、本申请书所列各项内容均须实事求是，认真填写，表达明确严谨，简明扼要，申报书请按顺序逐项填写，填写内容必须实事求是，空缺项要填“无”。

2、申请人可以是个人，也可为创新团队，首页只填主持人。

3、本申请书为大16开本（A4），左侧装订成册。可网上下载、自行复印或加页，但格式、内容、大小均须与原件一致。填写完后用A4纸张双面打印，不得随意涂改。

4、主持人所在学院认真审核，经初评和答辩，签署意见后，将申请书（一式两份）报送教务处。

一、基本情况

项目名称	基于智能合约的医疗区块链系统						
所属学科	计算机科学						
申请金额	60700 元		起止年月	2019 年 11 月 06 日至 2021 年 11 月 06 日			
主持人姓名	庄震丰	性别	男	民族	汉	出生年月	2000 年 05 月 27 日
学号	22920182204393	联系电话	18959211260				
指导教师	刘昆宏	联系电话	13159265652				

主持人曾经参与科研的情况	学习成绩在年级前列 加入了 ACM 队 参加数模大赛和各级 ACM 编程比赛
指导教师承担科研课题情况	1. 厦门大学-新加坡 Cellnetwork 区块链联合研究中心， 2. 国家自然科学基金面上项目，“基于输出纠错编码的开集多类数据挖掘算法研究” 3. 福建省自然科学基金面上项目，“基于输出纠错编码的多类基因微阵列数据挖掘方法研究” 4. 福建小知大数科技公司，“基于深度学习的智能音乐评分模型研究与核心功能模块开发”
指导教师对本项目的支持情况	提供区块链相关理论分析与编程实验方面的指导，并在论文写作、投稿等方面提供全面指导。

项目组主要成员	姓 名	学号	专业班级	所在学院	项目中的分工
	庄震丰	22920182204393	计算机系	信息学院	项目负责人
	林正昊	22920182204238	计算机系	信息学院	项目成员
	黄国文	22920182204190	计算机系	信息学院	项目成员
	张晶瑾	22920182204359	计算机系	信息学院	项目成员

	张泽锴	17420182201050	会计系	管理学院	项目成员

二、项目简介（限 50 字以内）

大创小组前期已经明确树立对以太坊大创项目的基本认识，每个成员均一定程度上了解了以太坊产生的背景，了解区块链的基本背景。为解决当前医疗系统医疗数据造假、篡改医疗记录等事件的发生，团队利用区块链技术和智能合约的特点，使用区块链技术的安全性处理 EMA 和利用区块链属性实现数据共享。在信息化和万物互联时代，涉及个人的敏感隐私资料，如身份信息、疾病情况、治疗方案以及社保医保等信息，几乎是完全公开并被商家无偿使用的,出现医疗纠纷则完全依靠医疗机构的公信力，这种状态对所有人都非常危险。本项目以医疗系统中医疗设备和药品的医院和患者的流通为切入点。而以太坊通过智能合约可以对单项信息数据分配多把私钥，通过区块链多私钥权限保管模式确保个人敏感资料数据在全网络使用中的规范性和安全性。这个规则是基于密码学算法而非信任，数据是透明的，任何人都无法篡改，只有授权的人或机构才能访问数据的具体内容。

三、立项依据（可加页）

（一） 研究目的

在日常生活中交易一般会选择一个两方共同信任的交易平台交易，而在区块链中消去这个平台的效力。而正因为这个去中心化，区块链期望被大力应用与生活。

本项目旨在建设一个基于以太坊的区块链系统。为解决当前医疗系统医疗数据造假、篡改医疗记录等事件的发生，利用区块链技术和智能合约的特点，使用区块链技术的安全性处理 EMA 和利用区块链属性实现数据共享。在信息化和万物互联时代，涉及个人的敏感隐私资料，如身份信息、支付消费情况、疾病情况、治疗方案以及社保医保等信息，几乎是完全公开并被商家无偿使用的，患者的医疗信息在诊疗过程中患者是没有任何发言权的，出现医疗纠纷则完全依靠医疗机构的公信力，这种状态对所有人都非常危险。而以太坊通过智能合约可以对单项信息数据分配多把私钥，通过区块链多私钥权限保管模式确保个人敏感资料数据在全网络使用中的规范性和安全性[3]。这个规则是基于密码学算法而非信任，数据是透明的，任何人都无法篡改，只有授权的人或机构才能访问数据的具体内容。

（二） 研究内容

团队会研发出以区块链为基础的智能合约系统，届时可以确保各个环节在交互时的安全性和完整性，从而保证了医疗信息的闭环操作。但是，对于一个界面友好的应用程序来说，还需要构造一个去中心化的应用来提供操作智能合约的用户接口，这就需要这些应用能很好地与以太坊进行交互。为了达到此目的，以太坊规定了每一个信息环节都需要实现的 JSON RPC API，通过这个 API 可以采用各种通信机制来操作以太坊节点。因此，JSON RPC API 的协议细节至关重要，通常用特定的语言做成封装库，以便于开发人员直接用此封装库开发出以太坊之上的去中心化应用。这些都是我们团队需要解决的问题。

智能合约确保了各个环节在交互时的安全性和完整性，从而保证了医疗信息的闭环操作。但是，对于一个界面友好的应用程序来说，还需要

构造一个去中心化的应用来提供操作智能合约的用户接口，这就需要这些应用能很好地与以太坊进行交互。为了达到此目的，以太坊规定了每一个信息环节都需要实现的 JSON RPC API，通过这个 API 可以采用各种通信机制来操作以太坊节点。因此，JSON RPC API 的协议细节至关重要，通常用特定的语言做成封装库，以便于开发人员直接用此封装库开发出以太坊之上的去中心化应用

（三） 国、内外研究现状和发展动态

目前，世界上已经有多家初创公司提前布局医疗行业区块链应用。Gem Health 公司与菲利普公司合作成立一家医疗健康区块链公司，初步构建了一个网络基础设施，致力于构建一个全球化的医疗健康平台，从而为全人类提供更加私有化的医疗健康服务。目前已经初步具有完善的医疗数据、保险理赔和药品供应链、基因数据等方面的区块链数据节点。Healthnautica 公司在 Factom 公司提供的区块链技术基础上，实现了医疗信息记录，大大方便了医院、医生和病人之间的沟通和信息共享，保证了医疗信息使用的规范性。BitHealth 公司发明了解决诸如数据复制、医疗数据分散化等问题的区块链实现，可安全地在全球网络上传送和存在医疗健康数据，实现了患者可以保护个人隐私数据，医生在授权下可以调取和记录医疗信息。美国科学院和工程院双料院士 George Church 创建的 Nebula 公司运用区块链实现了基因、健康和疾病等数据追踪和共享机制，通过分权、秘钥结合区块链技术实现了数据保护。

而本项目可以在区块链技术的基础上实现医疗器械、药品的监管和实时查询监控，根据上述方案中的合约算法。并且具有隐私保护、不可修改、存取和存取流程简化的特点。

1、 基于区块链的特性，每个患者的个人信息都会被唯一的哈希值表示，而不是医疗系统中的使用用户姓名和 ID 等，基于密码学的非对称加密技术可以在每次重新生成密钥时实现用户对文件的唯一标识，文件访问权在用户自己手中。

2、 不可修改性

基于区块链设计，上传导私有网络的文件都带有时间戳，任何记录都会被同步到所有节点。而修改请求需要超过 50%的节点通过，所以任何文件的改变都会显示

在跨域网络中，保证了其不可修改性。

3、 存取流程简化

在本方案中，基于私有区块链的数据在分析中保证了不可修改的特性，存储中只要一次便可以随地访问。基于哈希算法的重复检查机制使得重复文件上传到私有区块，实现上传永久保存。这样节约了传统医疗保存方案中的时间成本，彻底实现了“精准定位”节约了人力成本、时间成本、提高了检索文件的精确度。

4、 存储效率高

EMR 文件大小约在 1-5MB，上传与下载一般在 100ms 时间级别。一个医院可能同时存在上百上千份 EMR 文件，如果在高并发条件下存取同时进行，同时考虑到实际情况，在实验中基于 POW 共识机制中，打包合约节点少，交易缓慢，因此理论上可以将实验布置到公网上可以将效率进一步优化。

（四） 创新点与项目特色

区块链是一个非常新兴的领域。医疗信息系统和基于区块链的智能合约天生具有较高的匹配度，两者结合，可大大降低各种医疗环节的成本，对医疗系统进行完善，大幅度改变医疗现状，实现医疗卫生行业更好的突破。

此处引用 SWOT 模型中的 S 模块来对区块链及智能合约系统进行分析：

Strengness(优势)：

1）高效的实时更新：由于智能合约的执行不需要人为的第三方权威或中　　心化代理服务的参与，其能够在任何时候响应用户的请求，大大提升了交易进行的效率。用户不需要等待银行开门就可以办理相关的业务，只要通过网络一切都可以方便快捷地解决。

2）准确执行：智能合约的所有条款和执行过程是提前制定好的，并在计算机的绝对控制下进行。因此所有执行的结果都是准确无误的，不会出现不可预料的结果。这也是传统合约制定和执行过程中所期望的。现今，智能合约的准确执行得益于密码学的发展和区块链技术的发明。

3）较低的人为干预风险：在智能合约部署之后，合约的所有内容都将无法修改，合约中的任何一方都不能干预合约的执行，也就是说任何合约人都不能为了自己的利益恶意毁约，即使发生毁约事件，事件的责任人也会受到相应的处罚，这种处罚也是在合约制定之初就已经决定好的，在合约生效之后无法更改。

4）去中心化权威：一般来说，智能合约不需要中心化的权威来仲裁合约是否按规定执行，合约的监督和仲裁都由计算机来完成。在区块链上的智能合约更具有这一特性，在一个区块链网络中一般不存在一个绝对的权威来监督合约的执行，而是由该网络中绝大部分的用户来判断合约是否按规定执行，这种大多数人监督的方式是由 PoW 或 PoS 技术来实现的。如果将这种情况搬到现实世界中，或许现在的所有法官都要失业了，而与此同时我们每个人都是法官，都参与监督和仲裁。

5）较低的运行成本：正因为智能合约具有去人为干预的特点，其能够大大减少合约履行、裁决和强制执行所产生的人力成本，但要求合约制定人能够将合约的各个细节在合约建立之初就确定下来。这可能会使在传统行业（如银行）工作的部分员工面临失业，但从长远来说会促进行业的转型，向更新更好的领域发展。

（五） 技术路线、拟解决的问题及预期成果

- 基于区块链网络的医疗记录安全储存访问方案

1. 应用场景

传统的医疗记录解决方案在储存和实时查看记录方面有限于效率的影响。医疗记录生成也需要医生授权，由于我国某些医院的就医人数常年处于处于饱和水平，所以医疗过程常常处于无记录的状态，包括一些医疗设备和医药用品的流通，并且也储存了医院和患者的不同隐私信息，所以需要保证存放在医院数据库的 EMR 信息不被窃取。

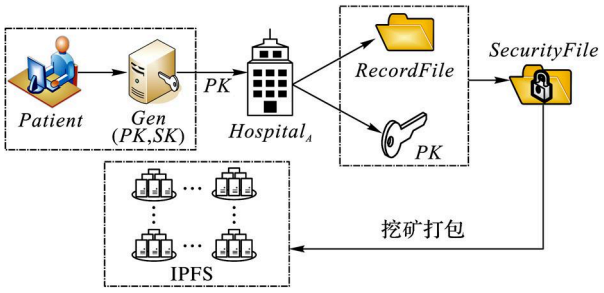
本方案这对医疗记录 EMR 的四大核心问题：1、如何安全有效存储患者的 EMR 2、如何实时上传 EMR 3、如何设置访问过滤非法访问者。4、如何方便跨域。由此设计了三个基于 Ethereum 的以太坊智能合约：文件同步、授权和跨域获取合约。

- 首先设计不可更新的智能合约，然后形成一个可更新的策略；这似乎是一个有实践意义的方式，也是理想的方式。在合约的基础上嵌入医疗信息加以数据库管理。采用区块链结构，把隐私数据和区块链分离，保证数据的隐私和数据的真实性，并利用区块链的不可篡改的特性保证医疗数据和流通过程的安全可靠，进行交易的同时可以看到交易流程，同时也可以保护技术隐私，减少有关医疗研发对工艺和科技泄露的担忧等。
- 智能合约算法：

1、 文件同步合约

在加密层采一种非对称的加密算法（ECC）用于给患者的 EMR 加密。在方案中，用户在医院注册给患者保存一个经过哈希算法 SHA-256 加密后的 ID 和加密的公私密钥 PK、SK。另外就是 IPNS 经过哈希加密后医疗记录的地址 FolderAddress。整个用户数据可以根据上述地址和密钥表示。

上述哈希算法加密后的 ID 用于唯一识别患者的身份。整个过程如图表示：



算法实现：

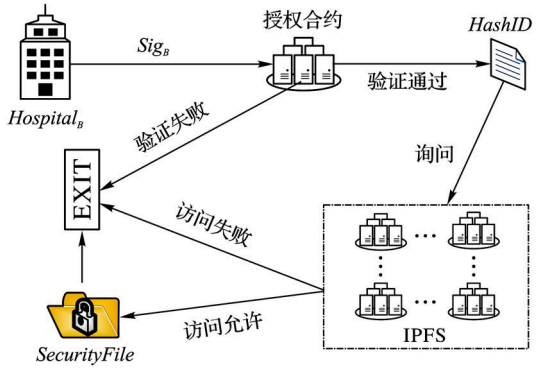
```
1)  Input: PK , RecordFile
2)  Output: SecurityFile
3)  begin
4)  while( 用户第一次使用 RSMR 系统)
5)    if ( 患者符合使用条件)
6)      { 为患者创建结构体数据:
7)       Patient{ ID ,PK ,SK ,FolderAddress} }
8)      if ( 创建 FoldAddress 成功 && 得到医疗记录文件 EMR)
9)            { 用 SHA256( PK ,EMR) = HashID 加密得
              SecurityFile}
10)     reture SecurityFile;
11)   if ( SecurityFile 的哈希值重复性检查通过)
12)     { 上传 SecurityFile 到 IPFS 网络上 ,并且副本同时同步
        在私有网络的不同网络位置}
13)   else
14)     { 文件已经上传过 ,不需要重复上传 ,节约带宽}
15)   else

16)       医院分配具有 IPFS 服务的虚拟机供患者使用
17)   end
```

2、 授权合约

授权合约解决一个自动智行的合约在以太坊网络上传输的过程。

（1） 加密输出唯一的 ID 与加密文件 SecurityFile。合约收到传输过来自动将文件传到私用 IPFSS 协议网络 MPN 上，上传之前 IPFS 会自动检验加密文件是否重复以节约带宽。经过加密后得到该文件的唯一文件 ID。但一份完整的 EMR 文件包括不同的文件。

（2） 经过校验和上传后文件将分为不同的序列储存在患者计算机项链的机器上，即使某个主极关机或不可预错误发生，都不会影响患者拿到储存在其他地方的副本。如图所示：

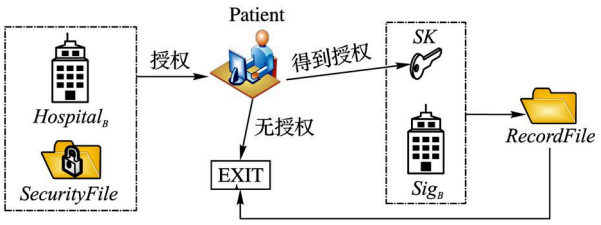


（授权合约）

Initialization: getHashvalue , VerificationSig , Download
Ensure: 用户的 EMR 文件在本地计算机同步完成
func(getHashvalue)
func(VerificationSig)
func(Download)
AccessControl: 用户在 $Hospital_B$ 需要 EMR 文件
do VerificationSig(Sig_B) 验证 $Hospital_B$ 签名
if(验证通过) {
Allow acess
do getHashvalue( )
得到文件哈希 $Hospital_A$($HashID_1$ $HashID_2$ ···HashI
do download($Hospital_A$($HashID_1$ $HashID_2$ ···HashID
下载得到密文文件 *SecurityFile*
$Hospital_B$ 查看完成 ,合约结束
else { Access denied}
end

3、 跨域合约

针对不同的场景，当患者在不同 Hospital 就医后，医生需要获得文件夹和 Premission，医生可以在 Folder 下进行医疗设备的记录和访问患者信息，并在调用医疗器械和药品的时候自动记录合约。但是下载后的文件医生没法解密，所以采用一种非对称的加密形式：（获取跨域合约）



算法实现:

```
1)  Input: SK , SecurityFile
2)  Output: RecordFile
3)  while( 用户到达 Hospital_B 满足使用条件)
4)    if( Hospital_B 得到下载权限)
5)      { 利 用 FolderAddress 哈 希 下 载 EMR 记 录 文 件
        SecurityFile}
6)    while( 用户输入 PrivateKey 与初始分配一致)
7)      { 执行算法 Unlock( SK ,SecutyFile ,Sig_B) = RecordFile
        得到历史病历 RecordFile}
8)    else
9)      患者需授权 Hospital_B; continue;
10)   合约结束
11) end
```

- 安全性分析

若盗取者能够通过某种手段得到的患者在 RSMR，但是在 RSMR 中的数据不会被查看，也不会被删除或修改，因此数据也是安全的。除非有区块链（51%以上的算力），这几乎是不可能的。另外在 RSMR 中储存的数据 SecurityFile 被分为序列储存相连的计算机上，但是数据并按照一定序列才能拼成源文件，但是概率非常小。

在跨域合约中算法中，经过加密文件被存储在区块链。因此，在得不到患者密钥的加密文件一样也无法解密文件，窃取者并不可查看真实内容，从而保证患者的隐私。

而在授权合约中，对执行合约的文件会对 SecurityFile 的哈希值进行重复性检查，盗取者会进入一个虚假的文件执行合约，通过哈希算法得到的 HashM 与源文件不同，所以合约总是不同执行，这个机制可以保证不同用户的源文件不能被篡改。

方案部署

在实验方案中，采用 Ubuntu 系统作为硬件载体不同模拟结点的功能，软件方案使用之前所述的协议分布在每个硬件载体。为解决拓扑中拜占庭问题，实验部分采用结点管理工具解决，分为服务端和管理端（配置在使用部门中心的服务器）可以用于管理 EMR 文件在不同结点执行相同的操作。

智能合约部分：使用 Remix-IDE 作为以太坊智能合约系统开发工具，用 Solidity 编写，部署以太坊测试网 Ropesten Test Network 上测试运行。

节点对象：医疗机构的所有参与对象，包医生电脑、患者电脑或者医疗记录的一台 PC 机

模型节点：

A：同步医生记录的医疗用品信息的计算机

B：患者要保留的医疗药品器械使用记录的计算机

C：和患者有关的亲邻计算机

D：医院服务器上的虚拟机镜像

同步流程：

1. 生成密钥
2. 启动节点
3. 上传 EMR
4. 确认交易
5. 文件溯源

（六） 项目研究进度安排

前期工作：学习了解有关前端，数据库，solidity 语言等知识

1、 分组学习前端开发、数据库处理、交互框架搭建等知识。

2、 利用 Remix IDE 学习以太坊编程语言（solidity）

3、 利用 Django 建立后台管理。

4、 调研智能合约系统在预期选定应用方向的应用环境，并作出必要修改。

中期：在调研讨论得出结果后进行平台搭建

1、 先搭建好底层架构，后面利用接口进行前端开发，同时完善数据库。

后期：项目完善并进行商业策划

（七） 已有基础

1. 与本项目有关的研究积累和已取得的成绩

我们大创小组前期已经明确树立对以太坊大创项目的基本认识，每个成员均一定程度上了解了以太坊产生的背景，了解区块链的基本背景，成功尝试搭建智能合约开发环境 Remix IDE 并初步使用。本小组已与指导老师联系，进行小型的会议探讨和有关方面学术上的交流，在会后我们明确该大创

项目的具体流程和大致方向，根据这些信息，小组曾多次组织开会，并且逐步确定了每个人的分工和大致需要的学习内容。有关书籍文献我们已经从各种渠道获得，并且我们小组正在努力申报校长基金，力求为本次大创项目实践争取更多的支持和机会。在空闲之余，我们小组还会定期参加一些相关方面的讲座，在增加见识，拓宽眼界的同时，也加深了对于该项目的理解程度，从而使我们能更好地投入到本次项目开发当中;指导老师也会不定期分配一些专业技术指导人员辅助项目的实施开发，帮助我们解决一些在项目开发中遇到的问题。由于本大创小组成立不久，尚处于知识储备阶段，具体大的项目成果还没有完全落地，但是我们相信通过我们小组每个成员的不懈努力，一定能在将来取得丰硕的成果。

2. 已具备的条件，尚缺少的条件及解决方法

已具备条件：已经搭建好虚拟机和各种 IDE 准备进行合作项目编程，有关数据、资料已经得到，项目调研已经在各个行业展开。

缺少条件：大创小组成立不久，尚处于知识储备阶段，具体大的项目成果还没有完全落地。

解决办法：自主学习，与老师合作交流意见，通过我们小组每个成员的不懈努力，一定能在将来取得丰硕的成果。

四、经费预算

开支科目	预算金费（元）	主要用途	预计使用时间
（1）计算、分析、测试费	5000	上机费，设计费等	2019 年
（2）能源动力费	500	水电费等	2019-2020 年
（3）会议、差旅费	20000	参加有关学术会议和论坛费用、项目调研	2019-2020 年
（4）文献检索费	1000	文献费、查重费	2020-2021 年
（5）论文出版费	1200	论文、文印费、	2020-2021 年

2.仪器设备购置费	15000	购置设备测试机、服务器搭建等等	2019-2020 年
3.实验装置试制费	15000	设备维修、装置调试和实验零器件购置等	2019-2020 年
4.材料费	3000	电子、纸质书籍资料费	2019-2020 年
预算经费总额	60700		
学校批准经费	0		

五、指导教师意见

1.项目研究的选题意义

a.应用意义
在无信任的环境下，在整个网络中的任意节点建立起共识机制，而无需担心数据被篡改。
b.战略意义
基于创建信任的机器，促进价值的全球流动。把各个机构和个人，映射到虚拟世界，基于数学这种人类文明的最大公约数，汇集世界上不同人群、不同权利群体的共识，实现了价值，资产的全球实时流动
c.社会意义
区块链就是构建了不依赖第三方的、自运行的社会信任网络，推动整个社会开始了价值互联。不仅仅是让今天的资产更好地体现价值，还可以让无法简单计价和量化的关系，逐步成为可以计价和量化的社会资产，全方位地推动了社会生产力的发展，推动人类社会迈上新的台阶。

2.项目研究方案的科学性

a．以太坊是一个开源的有智能合约功能的公共区块链平台。通过其专用加密以太币去中心化的虚拟机来处理点对点合约。
b．以太坊是一个开源的区块链底层系统，就像安卓，供应了非常丰厚的 API 和接口，让许多人在上面能够快速开宣告各种区块链运用，同时以太坊有很大的特色就是能够完结智能合约。

3.项目研究方案的可行性

a．区块链在金融领域十分火爆，具有研究潜力
b.区块链中不可篡改信息的去中心化，实现解决交易中选择一个两方共同信任的交易平台交易问题，消去平台效力。可以使得交易进行的更加便捷。
c．区块链中同时使用密码学加密，能够进一步保护人们隐私，从一定程度上提高人们交易安全应用。

导师（签章）：

六、院系大学生创新训练计划专家组意见

专家组组长（签章）：

七、校大学生创新训练计划专家组意见

负责人（签章）：

八、大学生创新创业训练计划领导小组审批意见

负责人（签章）：