厦门大学校长基金项目申报书

学　　院：	信息学院
项目名称：	基于以太坊的智能合约系统
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 12 日
项目起止年月：	2019 年 11 月 12 日至 2019 年 11 月 12 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。

<table>
<tr><td colspan="2">学
院</td><td colspan="8">信息学院</td></tr>
<tr><td colspan="2">项目名称</td><td colspan="8">基于智能合约的医疗区块链系统</td></tr>
<tr><td rowspan="3">项
目
负
责
人</td><td>姓名</td><td colspan="2">庄震丰</td><td>学
号</td><td colspan="2">22920182204393</td><td>院系</td><td colspan="2">信息学院计算机系</td></tr>
<tr><td>专业</td><td colspan="4">计算机科学与技术</td><td>年级</td><td colspan="2">2018 级本</td></tr>
<tr><td>邮箱</td><td colspan="2">22920182204393@stu.xmu.edu.cn</td><td>手机</td><td colspan="2">18959211260</td><td>电话</td><td></td></tr>
<tr><td rowspan="5">项
目
组
成
员</td><td>学
生
姓
名</td><td>性
别</td><td>出生年月</td><td>学院/系
别</td><td>所在专
业/年级</td><td colspan="2">学号</td><td>签字</td></tr>
<tr><td>林
正
昊</td><td>男</td><td>2000.8</td><td>信息学院</td><td>计算机</td><td colspan="2">22920182204238</td><td></td></tr>
<tr><td>黄
国
文</td><td>男</td><td>2000.5</td><td>信息学院</td><td>计算机</td><td colspan="2">22920182204190</td><td></td></tr>
<tr><td>张
晶
瑾</td><td>女</td><td>2000.9</td><td>信息学院</td><td>计算机</td><td colspan="2">22920182204359</td><td></td></tr>
</table>

	张泽锴	男	2000.8	管理学院	会计	17420182201050	
指导教师	姓名	刘昆宏		出生年月		职称/学位	教授
	研究方向	机器学习、区块链		联系电话	13159265652	邮箱	lkhqz@xmu.edu.cn
导师组	姓名	职称/学位		研究方向	联系电话	邮箱	

一、前期基础（500 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。

二、项目实施思路（2000 字以内）

1．研究意义

区块链技术最早是以比特币的底层基础技术框架形式出现，其概念由“中本聪”学者在2008年所撰写的论文《Bitcoin:A Peer-to-Peer Electronic Cash System》中首次提出，目的是为了解决数字系统中出现的双重支付问题。基于以太坊的智能合约系统是一次新的产业革命，区块链技术应用于各类系统的底层中，使系统具有安全、可信赖和普适性等优势。本课题基于上述思考，提出以区块链为基础，使用智能合约技术应用到相关领域中，实现一个去中心化的系统，有如下优点：

1） 用智能合约技术可以解决协议规则被不法节点中断的问题。

2） 存储到区块链的数据不可以被更改，无法作假。

3） 降低了因第三方参与维护而产生的不必要成本，系统可信度高。

4）丰富交易与外界状态的交互。

2．研究目标、主要内容、成效

研究目标：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，论文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

研究主要内容：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。

成效：对于医疗机构来说，药品的采购及使用、医生的从业资质、对患者的健康管理、临床试验的各个环节都需要做到可回溯、可监管和可防伪，基于区块链的智能合约能自然的提供解决方案。建立在区块链基础上的药物一致性的物流配送和管理体系，做到药品数据即时更新共享，数据链上的药店、患者、药厂、医院甚至监管机构都能实时的观察数据流动。更进一步，智能合约

还可以构建医疗从业人员的验证平台，同样允许从医人员、医疗单位等对信息进行验证，从而实验多点执业。在不久的未来，患者、医疗机构、医师、药企、保险商、监管机构等都可以在区块链上构建完整而独立的数据架构，在智能合约的基础上实现共享。

3．研究方案

- 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。

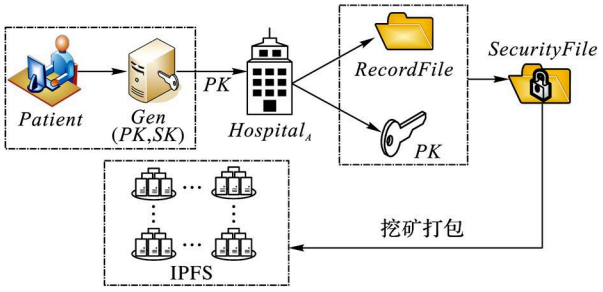
本方案这对医疗记录 EMR 的四大核心问题：1、如何安全有效存储患者的 EMR 2、如何实时上传 EMR 3、如何设置访问过滤非法访问者。4、如何方便跨域。由此设计了三个基于 Ethereum 的以太坊智能合约：文件同步、授权和跨域获取合约。

- 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：

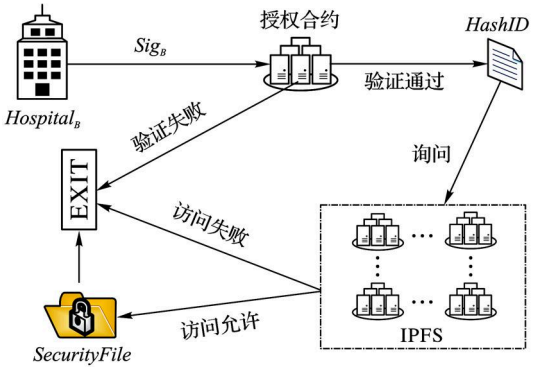
```
1)  Input: PK , RecordFile
2)  Output: SecurityFile
3)  begin
4)  while( 用户第一次使用 RSMR 系统)
5)    if ( 患者符合使用条件)
6)      { 为患者创建结构体数据:
7)       Patient{ ID ,PK ,SK ,FolderAddress} }
8)      if ( 创建 FoldAddress 成功 && 得到医疗记录文件 EMR)
9)            { 用 SHA256( PK ,EMR)  =  HashID 加密得
              SecurityFile}
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。

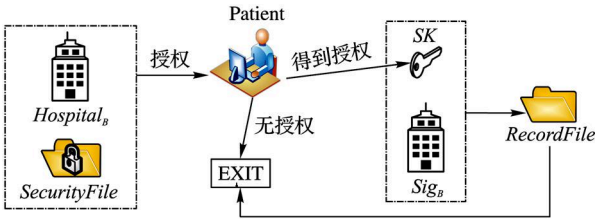
（2） 经过校验和上传后文件将分为不同的序列储存在患者计算机项链的机器上，即使某个主极关机或不可预错误发生，都不会影响患者拿到储存在其他地方的副本。如图所示：（授权合约）



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 $Hospital_A$($HashID_1 HashID_2 \cdots HashID_n$) }
do download($Hospital_A$($HashID_1 HashID_2 \cdots HashID_n$))
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

4. 可行性分析

以往案例：

以太坊用去中心化的应用程序 (DApp) 来实现智能合约的应用，用来实现提交交易

数据到区块链并且从区块链中读取数据。

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。

5．特色与创新

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。

在基于区块链技术的特定医疗环境重点 应用场景实现医疗药品器材的跨域分享和溯源，并具有保护、存取效率、安全、部署复杂、易用的优点。

区块链作为一种多方参与、多方监管的技术、可以保证交易记录随时记录，利用密码学的属性加密、同态加密和代理等复杂加密技术可以保证其正常隐私保护和运行。

6．研究支持条件

现我们团队有一名富有经验的带队老师，同时每周都会有研究区块链的公司派来的专家给我们做技术支持，除此之外，我们还有专属的创客空间，供团队平日做科研用。

三、项目管理（400 字以内）

1．**项目人员组成及分工**

人员组成：林正昊，庄震丰，黄国文，张泽锴，张晶瑾

团队分工：

1. 底层 solidity 搭建,并且在一些方面补充前端开发网页 app 设计，接口、协议技术所需要人力支持（林正昊，张泽锴）
2. 负责该项目的商业规划设计,并对该项目进行市场化分析，负责各类文案及项目展示。（张泽锴）
3. 利用 php 和 js 进行前端开发。（庄震丰）
4. 网页 app 设计，接口、协议技术，数据库分析（黄国文，张晶瑾）

2. **项目研究时间安排**

（1）明确树立对以太坊大创项目的基本认识，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。

（2）购买相关设备，并做好各项申请工作。

（3）根据分工开始学习所负责的内容，学习途径包括从书店购买相关专业书籍，查阅国内各大高校的文献资料和研究成果，以及定期到学校的实验科研室进行实践学习等。

（4）定期进行小型的会议探讨和有关方面学术上的交流，并不断根据实际需求灵活应变，交流所学内容以及经验便于日后正式开发的时候各方面合作更加顺畅。

2.中期建立系统阶段（2019-2020 学年下）

（1）在以太坊公共平台上，利用计算机学科的相关编程知识和能力，独立编写一整套数字化的，存储在区块链中，并使用加密代码强制执行协议。

（2）预编写一个独立属于本系统自身的，功能强大的数据库进行信息存储并进行维护

（3）学习较前沿的密码学，使用户信息能够进一步加密

（4）设置系统 app，建立前端小程序，设计小程序

3.后期完善阶段（2020-2021 学年）

（1）检测数据库的最大使用限制

（2）检测智能协议的运行

（3）通过部分调试 app 中能否与后端系统更好结合，并通过修改去取得前端与后端最优的配合方法。

（4)努力将产品完善并与商业化需求结合，并将所开发产品参加各级全国大学生创新创业大赛。

3.经费预算及经费使用

开支科目	预算金费（元）	主要用途	预计使用时间
1.设备费	15000	购置设备测试机等	2019 年
2.材料费	3000	电子、纸质书籍资料费	2019-2020 年
3.测试化验加工费	500	上机费，购置服务器、设计费等	2019 年
4.燃料动力费	500	水电费等	2019-2020 年
5.差旅费	5000	项目调研	2020 年
6.会议费	10000	参加有关学术会议和论坛费用	2020-2021 年
7.国际合作与交流费	5000	参加国际学术交流费用	2020-2021 年
8.出版/文献/信息传播/知识产权事务费	2200	发表论文、文印费、文献费、查重费	2020-2021 年
9.劳务费	500	设备维修等	2019-2021 年
10.专家咨询费	0		
11.其他支出	0		

四、申请者承诺
我保证上述填报内容真实，如果获得项目资助，我将严格遵守学校有关规定，切实保证研究工作时间，按计划认真开展研究工作，按时报送有关材料，按时完成研究项目。若填报失实或违反规定，本人将承担全部责任。 申请人签字： 年　　月　　日

五、导师意见（600 字以内）
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。 导师承诺
我遵守学术道德，切实负起项目指导教师责任。加强项目的指导和监管，认真组织和指导项目的实施工作，保证项目质量，按预期目标完成研究任务。严格执行财务制度，本着实事求是、节约开支的原则，规范使用研究经费，根据有关制度报销费用，不将专项资金用于与完成项目研究无关

的开支。
导师签字： 年　　月　　日

六．学院初审意见
学院领导/学院项目领导签字：　　**学院盖章：** **年　　月　　日**

七、学校专家评审意见
1．学校专家评审意见 专家组组长签字： 年　月　日

2．学校教务处意见   教务处（盖章） 年　　月　　日