智能合约设计文档

1.产品概要

新冠肺炎疫情爆发，疫情蔓延迅速。随着 2020 年 1 月 20 日武汉宣布“封城”， 武汉协和医院等当地多家医院防疫物资紧缺、在网络上请求防疫物资捐赠。当地政府指定 省、市红十字会和慈善总会作为接受捐助的专责机构，正当国内外人民群众纷纷捐款捐物、 助力武汉抗击疫情时，网友发现湖北省红十字会和武汉市红十字会未及时合理地将防疫口 罩分配到承担救助任务的一线医院，而不接诊肺炎患者的仁爱医院却获得了大量的口罩。 一时争议四起，把湖北省红十字会、武汉市红十字会推上了舆论的风口浪尖，引发了民众 对官方公益组织披露信息透明程度、分配物资的公平性和效率的质疑，更激发了民众长期 以来对公益慈善机构的不信任情绪、对社会监管缺失的担忧。

回首过往，善款的去向不明一直以来都是公益慈善的痛点之一，一来不断的激发受众对慈善机构怀疑的情绪，二来给了不法人员可趁的机会。但如若借助区块链为捐赠溯源， 便可快速解决此类问题。具体来看，区块链技术具有分布储存的特点，天然具有记账和信息追溯的功能，在慈善捐赠领域中，通过使用分布式账本来跟踪捐赠信息，确保每笔捐赠款项都清晰透明。 早在 2017 年，我国就针对区块链技术进行物资公益捐赠流程追溯进行过尝试，9 月由美丽中国支教项目发起的“守梦天使寻找之旅”公益项目在京东公益物爱相连平台上线。 通过区块链技术与物联网相结合，不仅实现捐赠物资的全程流转信息上链，保证物资流转信息的透明可追溯，还大大改善了网上捐赠者的用户体验。面对此次疫情，中国雄安集团开通了慈善捐赠管理溯源平台，以区块链技术特性提高捐赠信息的透明度与公信力。

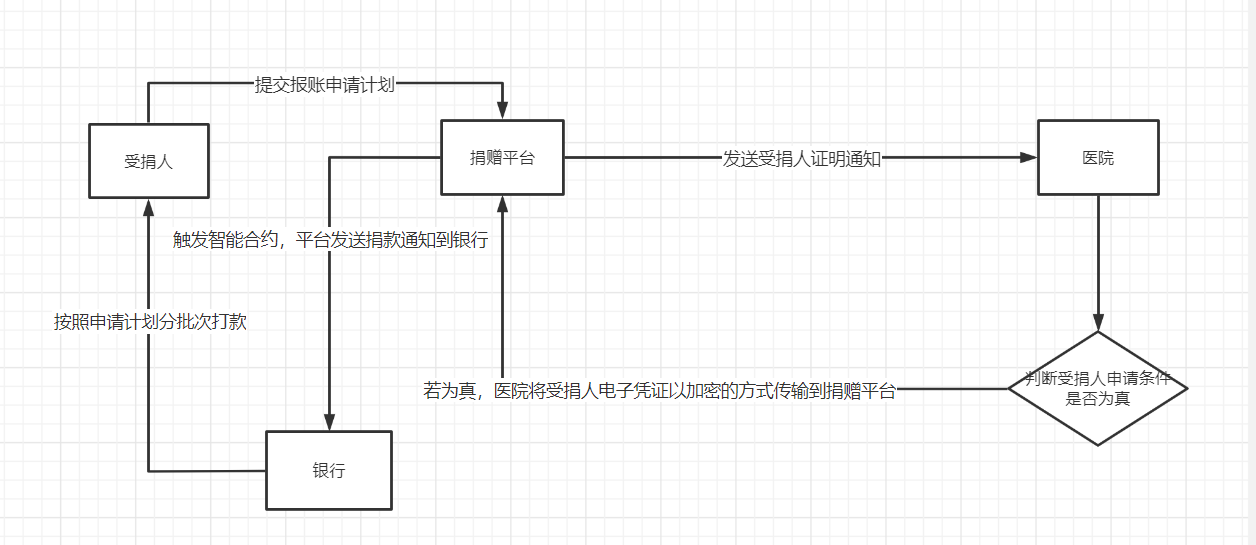
为了解决善款不明的问题，我们小组设计一款应用于市面上捐赠平台的区块链插件，该产品以智能合约为基础，使用非对称算法，哈希算法，数字签名等技术，解决大众对受捐人救助信息是否真实的问题，当使用该产品时，平台会向医院发送受捐人救助申请的证明，医院使用PSA加密算法，MD5算法以及数字签名等加密技术将电子凭证传输到捐赠平台，平台接收到医院的证明后触发智能合约，银行收到信息后自动打款给受捐人。产品也打破了医院，银行，平台用户三方之间的不信任问题，同时区块链技术特性提高了善款的透明性以及增强了大众对于捐赠平台的信任度。解决了捐赠平台，受捐人，捐赠人三方信任问题。

2.总体设计

**2.1总体框架**

**业务过程中共有两次触发智能合约的情况**

受捐人向平台提交报账认证申请，平台向医院发送申请信息真假性的通知，如果申请是真实的，则医院使用PSA加密算法，MD5算法以及数字签名等方式将受捐人获赠的电子凭证以加密的方式传输到捐赠平台，平台接收到医院的证明后触发智能合约，银行收到信息后自动打款给受捐人。



图一 该软件主要业务流程图

**2.2密钥说明：**

密钥的使用对象是获得国家公立医院和捐赠平台受助人。

该产品包含以下两种密钥：

**权限密钥（auth\_map）**：用于账户发送正常交易时使用的签名密钥，支持多个密钥，按权重分配实现多签名，是区块链节点判断交易是否有效授权的依据。

**加密密钥（encryption\_key）**：用于隐私保护场景下的数据加密密钥，可被交易参与方获取并用于隐私数据的加密。

合约平台采用将账户与密钥解耦的方式来实现，从一定程度上防止因为密钥丢失带来的链上数据丢失等安全隐患。

密钥使用方式以及产生机制如下：

当平台收到报账申请信息时，平台立刻产生受捐人和医院的公钥，私钥；医院使用受捐人的公钥对电子证明进行加密并使用MD5算法得到摘要，使用医院的私钥对摘要进行签名，将加密后的电子证明同签名一起传输到捐赠平台，平台收到加密文件后，使用受助人的私钥进行解密得到证明，再对电子证明使用MD5算法得到摘要，同时平台收到数字签名，对其使用医院的公钥进行解密得到摘要，如果解密后的数字签名和对解密后的电子证明使用哈希算法得到的摘要是一致的话，则触发系统的智能合约。

3.智能合约详细设计

本智能合约调用前提条件为：受捐人已在慈善平台通过受捐信息认证，且医院已通过正规认证。受捐人向平台提交报账认证申请，触发智能合约的“报账申请”。同时，医院收到是否确认的信息。医院的电子凭证触发智能合约，完成智能合约流程中的“自动汇款”。

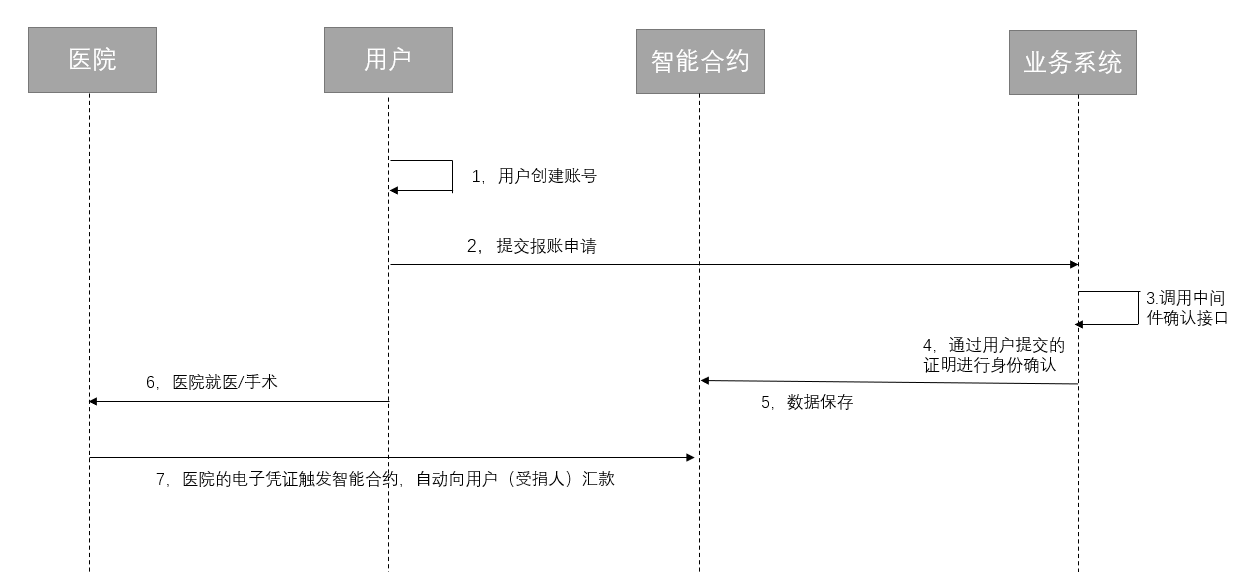
权限：受捐人只能提交申请，医院只能上传电子凭证而不能直接控制捐助资金的流向。

合约数据简单，包括：报账申请Quest即主检索ID，电子凭证Proof，汇款Fund即主key。用于数据的重复性验证、查询及溯源。

协议流程图：

*示例：*

|  |  |
| --- | --- |
| 合约名称 | 医院开销认证 |
| 合约描述 | 确认受捐人医疗信息，执行相关校验并记链 |
| 业务规则 | R1：单个受捐人在区块链上仅具有唯一档案信息；  R2：不同的正规医院完成注册，会生成不同的账户地址。 |
| 调用前提 | 受捐人通过核验后提交报销申请，且医院通过注册认证。 |



**说明：**

1、用户登录业务系统，创建账号；

2、用户提交创建信息，进行用户创建信息；

3、业务平台调用中间件完成认证；

4、通过用户提交的证明进行身份确认；

5、数据保存；

6、用户（受捐人）就医；

7、医院的电子凭证触发智能合约，自动向用户汇款。

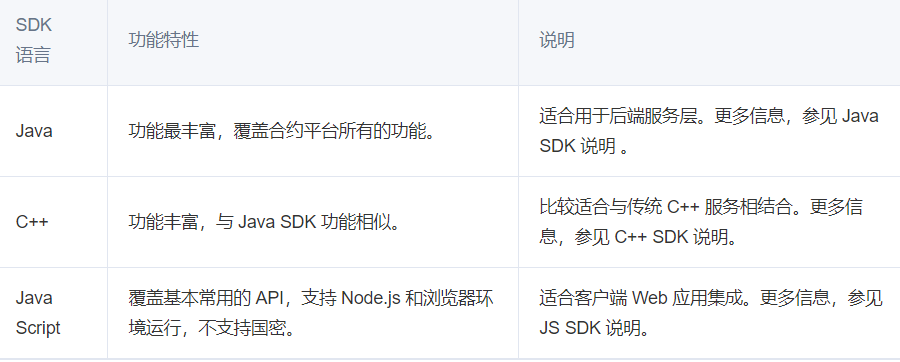
4.SDK接口设计

**4.1总体接口介绍**

1. 面向医院的接口：接收医院传递来的电子凭证
2. 面向银行的接口：在触发合约后向银行发出汇款信息
3. 公开的接口：所有人民群众可以查阅智能合约的源代码等信息
4. 面向开发者的接口：用于开发者的维护、升级工作

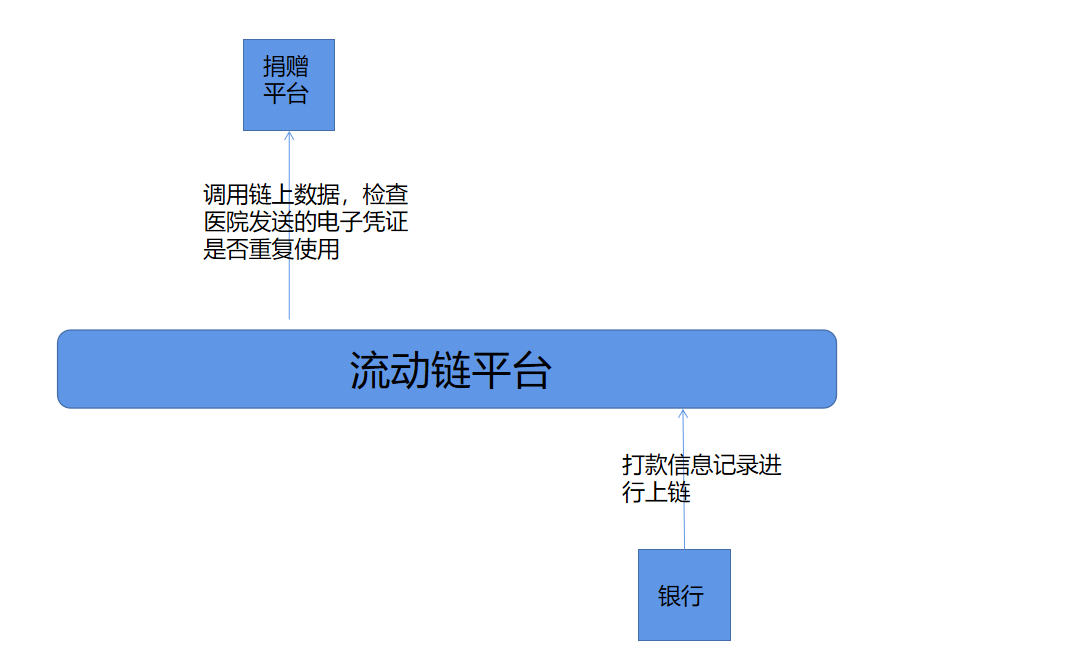
**4.2详细接口设计**

合约平台提供多语言 SDK 支持，如下：



5.界面设计

**5.1业务系统改造**

****