区块链期末 project 题目

陈铭涛

16340024

软件题目：CryptoChat

选题背景：当前大部分的聊天应用如微信、WhatsApp 等都需要通过中心化的服务器来实现各个用户之间的通信，这带来了聊天信息可能被监视、篡改的风险。即使是以 Telegram 这类以安全的加密通信为主要特点的聊天应用，也无法避免发起 P2P 通信时需要从中心化的服务器获取聊天对象的基本信息，从而可能导致 IP 地址等信息泄露的风险。利用区块链技术，将聊天数据保存至区块链上，可以使聊天应用实现去中心化，利用 RSA 或 ECC 等非对称加密算法，可以使保存在区块链上的聊天信息数据的明文信息只能被发送者或接收者所看到，区块链的特征也使得数据极难以被篡改或删除，实现一定的安全性。

应用构思：使用 Solidity 编写智能合约，使用 JavaScript 编写 Web 端客户端，使用 web3 来进行浏览器上应用与区块链的交互，由用户定义或随机生成用于加解密的私钥，生成公钥后将用户地址与公钥的映射存入区块链，其他用户向该地址发送信息时使用发送者和接受者的公钥分别进行加密，将加密后的数据存入区块链，在使用应用时取出数据进行解密。通过这种方法可以保证只有发送者和接收者可以读取到原信息的明文。用户可以通过该应用发送文本消息至其他用户地址，可以将其他用户的地址添加至自身的通讯录中以便快速再次进行消息发送。此外，用户还可以直接对选择的地址进行以太币转账操作。

在最开始的构思中，数据的加解密使用的是用户账户的公钥与私钥进行的，

然而在查找网络资料后发现在浏览器中使用 MetaMask 并无获得账户私钥或直接利用账户的公私钥加密消息的方法。因此选择了使用用户定义或随机生成的密钥搭配非对称加密算法对信息进行加密。这种方法带来的一点局限是对于尚未设置密钥的账户将无法发送信息。