基于区块链的保险系统

李泓睿 16340114

系统简述

该保险系统是基于区块链的智能合约建立的，系统中有三种角色：公司、判定机构、客户。公司可以部署保险智能合约，从合约中收取利益；判定机构负责审核客户是否满足赔付条件；客户可以购买合约、自助索赔。

系统中的智能合约由保险公司创建，指定并公开合约价钱、合约赔款、合约期限、以及第三方仲裁机构(一个账户地址)。用户可通过调用合约函数购买保险，经过第三方仲裁机构认定事故发生后，可调用函数直接领取保险赔款，无须向保险公司再度申请。

该系统的理想应用情景为：该系统搭建在一条官方实名制区块链上。区块链上的每一个地址都被实名认证过，每个公民只有唯一的一个地址。虽然现在政府不支持具有匿名性的区块链，但有基于区块链的电子发票先例，推测政府很可能在未来推出基于公民身份ID的实名制区块链，在该链上的地址即为公民的ID，公民可以在该链上办理电政事务。而保险的赔付与否判定由智能设备进行，现阶段还需要第三方权威机构进行判定。

选题背景

长期以来，保险行业存在着不少痛点：重复索赔、恶意多次投保等欺诈行为层出不穷，保险索赔过程繁琐，消耗大量人力物力。将保险合约部署在区块链上，能解决不少行业痛点。

选题依据

- 用户可以通过客户端接口调用智能合约函数，进而自助购买保险，免去纸质合同的签署过程 ，大大提高效率。与此同时，保险公司不再需要雇佣推销员，节省大量资金。
- 区块链具有不可篡改性和可审计性。用户可以看到保险合约的价格、赔款金额等信息，避免基于大数据分析的价格歧视现象的发生。记录在区块链上的保险合同是不可篡改的，可以杜绝同一事件多次投保、多次索赔的诈骗现象，减少保险双方的争议。
- 合约赔付的判定由第三方机构或智能设备进行，一方面极大程度上保护了用户的隐私信息，另一方面也简化了索赔流程 。
- 保险公司在合约中存储一定数额的金钱，用于支付赔款。保险公司可以通过调用智能合约函数进行资金调度。一个智能合约对应了所有购买了这个合约的用户，并非为每一个用户都准备一份赔付金，所以保险公司无需将大量资金存储到合约中，从而可以将资金进行周转，符合商业运作模式。

系统设计

- 合约的设计符合solidity官方要求，函数编写遵循“Checks-Effects-Interaction ”原则。
- 该系统使用了truffle框架，是基于truffle官方例子“pet-shop”改写而成。证书在项目目录中给出。
- 该系统的服务器使用lite-server部署。
- 在安全性方面，使用了合约、前端双重检测。如果用户调用了错误的函数，如重复调用购买函数，合约会反馈一个错误信息。但仅有合约检测的情况下，用户需要花费手续费调用函数后才能收到结果，这显然是不合理的。于是加入js前端检测，虽然有时会因为同步问题没能提前发现错

误，但能在很大程度上帮助用户节省交易手续费，提高用户体验。即使恶意用户绕过js前端检测，合约检测也会将恶意攻击拒之门外。

心得

不得不感叹，现阶段关于智能合约的文章还是太少了，找到一个好教程都要找很久。

好在有solidity的官方网站和我找到的一篇很好的dApp开发教程，我的整个开发流程，从合约编写、部署到最终dApp完工，都没有遇到多少困难，总体来说还是比较顺利的。

编写合约时要牢记一些安全准则，安全性才是最重要的。这一点可以从solidity官网的例子上学到不少。

使用truffle框架和可视化测试链Ganache，合约的部署简直无比轻松。truffle还提供了一个dApp框架的例子，将这个例子中的合约、前端（html、css、js）等替换成自己的内容，就可以很方便地做出一个client-server结构的dApp。参考dApp 开发，只要掌握了前端获取智能合约实例、调用智能合约函数等方法，前端就可以很快完工了。

开发过程中最难的应该就是前端界面的样式开发了，仿照着前端界面，做了个还算能看的页面。总体感觉还是不错的。

参考网站

- dApp 开发
- 前端界面
- 合约编写