基于区块链的车险智能合约应用的研究

张瑜颖，赵星辉，华昕豪，李晓蕾*

（宁波财经学院，浙江 宁波 315327）

摘 要 针对传统车险行业存在的复杂流程，且理赔周期长、效率低等问题，本文将智能合约技术引入车辆保险中，基于区块链的数据安全性和不可篡改性特点设计一个基于区块链的车险智能合约系统，利用区块链中的智能合约代码来自动完成区块链中的每笔交易，高效率完成车险中的各个环节，通过java编程搭建测试环境和以太坊智能合约交互工具对设计方案进行验证。实验结果表明，车险智能合约具有高效性和安全性。

关键词 车险；区块链；智能合约技术

中图分类号：F840.6 **文献标识码**：A **文章编号**：1007-0745(2023)05-0010-03

传统车险[1]流程复杂繁冗，造成保险公司营运人力的大量耗费，而车险智能合约[2]的应用可以提升人为工作效率，改善客户体验。区块链技术[3]的兴起帮助保险公司更加便捷地获取车辆运行、驾驶员行为等参数，并运用于车辆保险理赔等方面，这有助于减少保险欺诈，实现自动理赔。区块链技术对保障保险交易环节信息的安全性有较大帮助。

1 相关知识

区块链技术是一种革命性的分布式数据库存储技术，具有数据不可篡改、数据安全、可信赖性以及全局可见性等优点。因此，区块链技术可以用于构建车险智能合约，提高车险的效率、透明度和可信性。

智能合约是能够自动执行合约条款的计算机程序，并由代码强制执行，一旦启动就会自动运行，不需要它的发起者进行任何干预。基于区块链技术的智能合约不仅可以发挥智能合约在成本效率方面的优势，而且可以避免恶意行为对合约正常执行的干扰。

2 共享系统的模型

区块链共享系统[4]包含的主要角色如下。

2.1 用户

注册用户信息提交到区块链，每个用户都有属于本人的唯一认证合约，绑定公钥地址，负责授权或取消案件信息给保险公司。

2.2 勘察审核员

在区块链上提交或审核用户信息，一个案件对应一份案件合约，生成的案件信息和用户公钥地址绑定。

2.3 保险公司

维护绑定自己公钥的访问控制列表，发送查询共享案件信息的申请指令，在用户授权后可以利用查询函数在案件库中搜寻信息进行比对。

2.4 区块链

基于智能合约的数据存储平台，实时判断合约生效可能，判定成功后自动开始智能合约过程。整个执行过程无人工参与，提高了案件信息的透明化。

基于区块链的车险智能合约技术可以优化车险理赔流程，利用区块链上的信息有效改善骗保问题，区块链上的各个角色因数据库的去中心化特点都是对等的，每一笔交易记录都不可修改且可查询，因此无论对于用户还是保险公司，平台都是可管理且安全透明的。

3 车险智能合约的模型

3.1 数据结构和函数定义

数据结构：用户注册信息、保险公司信息和电子保单合约信息，皆存放在车险智能合约系统区块链数据库之中

函数定义：区块链中各角色及其功能需要定义函数来实现，函数定义如下：

1.getKey() 定义非对称性密钥[5]，利用加密算法而生成公私钥，用于处理对信息的加密和解密，通过发送信息来加密公钥，收到信息后用私钥解密；与此同

★基金项目：项目名称：国家级大学生创新创业训练计划《基于区块链的车险智能合约应用的研究》，项目编号：202213001019。

*本文通讯作者，E-mail：lixiaolei@nbufe.edu.cn。

时公钥作为区块链的地。

2.send(a,b) 发送消息 b 给 a 对象，b 是公钥地址，a 可发送加密消息、操作指令。比如 X 发送自己的公钥给 Y，可表示为 X.send(YPK,XPK)。

3.Initial(address) 用于初始化地址 address，进行合约与第三方绑定。比如 G 保险公司的访问控制使得列表初始化 Initial(address)

4.UserAddcase(SL_addr) 增加一个用户信息的对应关系，用户可检索车辆信息对应表查看自己的车辆证件信息。这里只保存与车辆信息库的一对一对应关系，不保存具体信息内容。

5.UserUpdateInf(hash(Content),Rsig) 用户对信息进行上传更新，参数包括更新的信息，以及判断更新信息的有效性。

6.UserAddOpear(hash(Content_1),Ysig,SL_addr) 保险公司的数据审核系统审核用户上传的保单信息，生成电子保单以及电子签名，并添加到区块链网络中。此函数用于生成区块链中新生成的保单号库地址和患者公钥的关联对应。

7.CaseShare(RPK,SL_addr) 保险公司申请共享用户 R 的保单信息，SL_addr 为申请的保单的地址映射。

8.CompAdd(address) 保险公司通过该函数添加用户对所选购保险的授权，address 参数为保险公司的地址。

9.CompDele(address) 保险公司使用该函数取消用户对所选购保险的授权。

10.CaseSelect(address) 检索请求命令，根据地址 address 在保险单号库中进行检索，返回所需索引号。

11.GetData(Content_2) 根据索引好获取保险信息列表，并返回给保险公司和用户查看使用。

3.2 密钥信息的公布

智能合约区块链中保险公司、用户和管理员（勘察员和审核员）分别生成密钥对，各环节的所在之处是公钥，各个端之间首先进行公钥 PK 的公布交换，分别对提交的信息的进行加密保留再传向下一环节，提取者需利用个人私钥进行解锁提取。实现如下：

```
(RPK,RSK):=R.get_key();
(YPK,YSK):=Y.get_key();
(GPK,GSK):=G.get_key();
R.send(YPK,RPK); R.send(GRK,RPK);
Y.send(BPK,YPK); Y.send(GPK,YPK);
G.send(RPK,GPK); G.send(YPK,GPK);
```

3.3 用户注册个人信息

用户提交个人和车辆基本信息上传到系统，区块链上触发注册信息合约初始化绑定用户，添加并更新一个新用户的个人信息。注册信息合约实现如下：

```
Procedure Contract Reg(Content,RPK,SL_addr)
Init(RPK);
If(msg.send==RPK) then
UserAddCase(Sl_addr);
UserUpdateinf(hash(content),Rsig);
End procedure
```

3.4 保险公司提交保险合同

保险公司发布自己公司对应的保险并且分类，保险自动执行一次后，将更新合约，并根据保险公司给出的公钥地址该保险将对应绑定，方便第三方公司对自己的保险进行管理授权。更新的合约实现如下：

```
Procedure Contract Opeartion(Content_3,RPK)
RPK=msg.sender
UserAddOpear(Content_3,Rsig,RPK);
End procedure
```

3.5 用户签订智能合约，生成电子保单

用户对想要签订的合约公司发起授权，授权成功签订完成后，产生电子版保单，保单合约将开始执行。合约实现如下：

```
Procedure Contract CompAlter(RPK,InstAddress,operat
ion)
If (msg.send==RPK and operation==add) then
CompAdd(InstAddress);
End if
If (msg.send==RPK and operation==delete) then
CompDele(InstAddress);
End procedure
```

3.6 用户申请理赔

用户发生事故之后，个人申请报案，上交理赔材料，申请理赔，勘察员和审核员对此进行实地勘察和审核，若发现骗保可能则返回用户。若无则发生授权给保险公司进行赔偿。实现代码如下：

```
Procedure Contract InstSearch(InstAddress,RPK,Content)
Init(InstAddress);
If(msg.send==InstAddress) then
CaseQuery(RPK);
GetData(content);
```

表1 用户注册信息

字段	第n个区块
RPK	$2a$10$HQscb2n46SWWOEnhQWtpGO
UserId	12345678
Prevblock_hash	$2a$10$FuIEnMzVJD6llGk4tMl4eu6cNj2Taumsmr3rcWdIJjWktwWeDJUS2
Content2	“小明，27岁”
Case_mapping	0
Hash(content2)	$2a$10$VnqpSZOmZvNREv2L0yMuEu61kxBkropqQUJGDpPgt0ppiuNspguza
Signature	T.
Self_hash	$2a$10$40ry9UaUehFaVdVgUFZg8e

End procedure

4 设计实现

4.1 用户实现过程

用户注册个人信息并上传至区块链中，授权区块链访问个人信息和每日行程情况，获取该车辆以及车辆使用人在常规情况下的行驶情况，成为申请理赔时进行审核与判断的依据。初始化后用户暂未生成案件信息映射，用户地址为$2a$10$HQscb2n46SWWOEnhQWtpGO，如表1所示。

用户在购买保险界面选择心仪的险类后，依照各个保险公司给出报价，确认并授权个人信息、每日行程及之后可能发生的案件信息后，签订智能合约，并将现有材料上传到区块链中。办理保险成功后，保险公司将反馈电子保单给用户并上传到区块链。保险公司用户地址为$2a$10$GCgOCFj7TuaPLOiigTfj7。

用户在发生事故后，可通过app报案并申请理赔，在查勘员确认可以进行索赔后，上传并确认相关理赔材料，整个过程可通过app跟踪进度。在通过审核员审核确认无骗保可能后，在一定期限内获得赔偿。

4.2 勘察员、审核员实现过程

查勘员和审核员可从区块链上获取了解所需案件信息。查勘员在了解案件信息后上传定损详情至区块链并确认索赔内容，上传部分索赔材料，若有用户申诉则需重新定损。审核员则需要在确认案件信息无误且没有骗保可能时，确认案件真实性。

4.3 工作人员实现过程

工作人员可查看和管理用户列表，查看、增加、修改、删除用户基本信息。可修改管理勘察员和审核员身份，查看其基本信息及工作情况，选择是否授予相应权限。在理赔管理中，首先进行报案录入，对用户提交的报案信息输出为表格进行管理。然后进行查勘定损并上传材料，对勘察员现场勘察的结果提交的数据生成查勘定损表进行管理，对用户提交的验证材料生成材料统计表进行管理。审核员对用户提交的信息材料和勘察员提交的信息进行分析生成骗保分析表，并对其进行管理；在保险和合约管理中工作人员对保险公司发表的现有保险进行分析之后分类管理，并把用户签订智能合约后生成的电子保单上传区块链进行管理。

5 结语

传统车险存在的理赔周期较长且效率低下弊端，随着区块链技术和智能合约技术的不断深入研究，车险智能合约的实施将更加安全、高效、可靠，更适应信息时代人类的需求，能有效解决传统车险耗时长、效率低、处理事故本人必在等问题，对车险行业的改革有很大的意义，后续我们将对设计方案进一步测试来验证其可靠性和高效性。未来，可以考虑把车险智能合约应用于其他领域，以实现安全、高效的车辆管理和安全保障。

参考文献：

[1] 杨世东.我国汽车保险理赔中存在问题及对策研究[J].现代经济信息,2011,319(09):185-188.
[2] 贺海武,延安,陈泽华.基于区块链的智能合约技术与应用综述[J].计算机研究与发展,2018,55(11):2452-2466.
[3] 袁勇,王飞跃.区块链技术发展现状与展望[J].自动化学报,2016,42(04):481-494.
[4] 徐鑫垚.共享单车App后台管理系统的优化[J].电子技术与软件工程,2017,102(04):80-81.
[5] 刘艳华.非对称密钥算法在区块链专利中的应用分析[J].中国科技信息,2020,639(21):18-20.