计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2019,28(1):61−68 [doi: 10.15888/j.cnki.csa.006745]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

基于区块链的保险产品推荐模型①

杨　立[1,2], 左　春[1,2,3], 梁　赓[1,2]

[1](中国科学院 软件研究所 区块链技术与应用联合实验室, 北京 100190)
[2](中国科学院 软件研究所 精准计算联合实验室, 北京 100190)
[3](中科软科技股份有限公司, 北京 100190)
通讯作者: 杨　立, E-mail: yangli2017@iscas.ac.cn

摘　要: 我国的保险市场正在经历快速发展时期, 客户、保险主体和产品的多样性使得产品推荐成为一个热点问题. 然而, 精准的产品推荐面临着隐私保护问题和可信问题带来的技术挑战. 本文首先对客户与保险公司的需求匹配问题进行了分析, 然后基于区块链技术提出了一个新的保险产品推荐模型, 客户和保险公司可以将对方需要的隐私信息安全地提交给推荐模型进行需求匹配, 从而实现了更为精准的产品推荐. 实验表明该模型可以在保护隐私的同时, 实现产品推荐过程的安全可信和透明公正.

关键词: 保险; 产品推荐模型; 区块链; 隐私保护

引用格式: 杨立,左春,梁赓.基于区块链的保险产品推荐模型.计算机系统应用,2019,28(1):61–68. http://www.c-s-a.org.cn/1003-3254/6745.html

Insurance Product Recommendation Model Based on Blockchain

YANG Li[1,2], ZUO Chun[1,2,3], LIANG Geng[1,2]

[1](Laboratory of Blockchain Technology & Application, Institute of Software, Chinese Academy of Sciences, Beijing 100190, China)
[2](Laboratory of Precise Computing, Institute of Software, Chinese Academy of Sciences, Beijing 100190, China)
[3](SinoSoft Co. Ltd., Beijing 100190, China)

Abstract: Chinese insurance market is experiencing the rapid development period, the variety of customer, insurance stakeholder, and product makes the product recommendation become a hot issue. However, accurate product recommendation faces the technical challenge brought by privacy-preserving and trustworthy problem. Firstly, this study analyzes the matching problem of customer demand and insurance company. Then based on blockchain technology, a new insurance product recommendation model is proposed, customer and insurance company can submit the privacy information needed by the other party to the recommendation model for requirement matching, thus more accurate product recommendation result can be achieved. The experiment shows that the model can achieve the security and transparency of the product recommendation process while preserving the privacy of participants.

Key words: insurance; product recommendation model; blockchain; privacy-preserving

2017 年 1~10 月, 中国保费收入 3.2 万亿元, 同比增长 20%, 即将成为全球第二大保险市场. 但是, 中国的保险深度、保险密度分别为全球平均水平的 66%、53%, 还有很大的发展空间[1]. 目前, 我国保险市场的经营主体有 100 多家, 产品更是多达上万种, 每一个保险产品的保障范围和免责条款都相对较为复杂, 客户在选择保险产品时往往无所适从, 非常需要推荐模型来进行产品推荐. 文献[2]提出了一个基于用户分群的保

① 基金项目: 中国科学院 A 类战略性先导科技专项 (XDA20080200); 广州市科技计划项目 (201802020015)
Foundation item: Strategy Priority Research Program of Chinese Academy of Sciences (XDA20080200); Science and Technology Plan of Guangzhou Municipality (201802020015)
收稿时间: 2018-07-22; 修改时间: 2018-08-21; 采用时间: 2018-08-29; csa 在线出版时间: 2018-12-26

险产品推荐模型, 文献[3]提出了基于贝叶斯网络的推荐方法, 文献[4]对健康险的保险计划进行了分解, 重点探讨了产品与需求的逐项匹配问题. 以上方法的实质上都是假设同类用户具有类似的需求, 对用户的各类属性进行相似性计算来达到推荐的目的. 而在实际环境中, 一是这样的假设未必成立, 二是用于推荐模型训练的数据一般都是涉及到隐私问题, 往往并不容易获取. 本文归纳现有的保险产品推荐方法主要存在以下问题.

(1) 信任问题

客户和保险公司存在着双向信任问题, 一方面, 保险公司或者第三方销售对客户具体情况不够了解, 特别是保险关键因素如健康状况, 驾驶习惯等等, 难以提供精准的保险产品推荐; 另一方面, 由于电销、网销特别是第三方机构的销售方式普遍存在的夸大宣传问题, 客户对保险公司也存在着信任危机, 一般来说, 对退保、理赔的条件和过程疑问较大, 需要了解详细可信的实际过程才愿意达成保险交易. 客户在选择保险公司和保险产品时只能简单地通过规模或者舆论来做决策, 对预期结果存在着较大的不确定性, 从而极大地影响了购买意愿.

(2) 隐私问题

客户在和保险公司协商的过程中, 通常不愿意将自己的个人资料完全提供给保险公司, 比如个人健康状况, 家庭住址等隐私信息, 而保险公司也不愿意轻易将真实详细的历史退保、理赔记录展示给尚未确认购买意愿的普通客户, 在当今环境下, 一个单一的隐私泄露可能导致的结果是相当严重的, 因为攻击者可以从一个点揭示更多的相关信息. 因此需要一种精确的授权机制, 保证各类隐私信息在严密受控的情况下进行传递, 并不被用于其他用途.

(3) 精准问题

现有人为推荐的模式受中介主体 (包括代理人、电销、网销和第三方机构) 因素影响较大, 往往会因为中介主体自身的利益导向而向用户推荐并非是最符合用户要求的产品, 同时也受困于信任问题和隐私问题导致的信息不对称, 文献[3]提到通过这类方法进行保险产品推荐的实际转化率仅有 12% 左右; 有些学者提出了利用同类用户数据进行推断等方式实现的推荐模型[2–4], 在实际应用中由于难以获得高质量的训练数据, 制约了其使用效果.

区块链[5]是一种分布式数据库技术, 是数据全网分布式共享存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式. 这种模式具有以下特点:

(1) 去中心化: 区块链所形成的账本呈现去中心化特点, 即没有中介机构, 所有节点具有相同的权利和义务, 任意节点停止工作都不影响系统整体的运作;

(2) 去信任: 基于区块链的系统中所有节点之间无需信任也可以进行交易, 因为数据库和整个系统的运作是公开透明的, 交易双方的信任关系是建立在全网共识基础上的, 只要符合系统规则, 节点之间无法欺骗彼此;

(3) 可编程: 区块链上的交易双方可以通过共同制定智能合约, 实现交易自动化;

(4) 集体维护: 基于区块链的系统是由全网节点共同参与维护, 系统中每一个节点都将同步最新的共识结果, 基于共识的记账机制保证数据经过少数人的篡改是无效的.

由于区块链技术的以上特点, 目前业界已经成功将该技术应用在数字资产交易[6], 医疗数据共享[7], 电子证照共享[8]等领域.

本文对区块链在保险产品推荐领域内的应用模式开展研究, 提出一种基于区块链的保险产品推荐模型, 试图解决以上问题, 该模型通过区块链的安全存储和授权机制管理客户和保险公司的完整信息, 并通过推荐算法精准推荐符合客户需求的保险产品.

本文的贡献主要如下:

(1) 对保险产品推荐问题进行了形式化定义, 提出了一个保险客户决策参考信息模型, 讨论了其中涉及到的隐私问题, 并说明该问题的解决可以提高保险产品推荐的转化率.

(2) 提出了基于区块链的保险产品推荐模型, 该模型首先利用区块链技术存储和管理客户和公司隐私信息, 然后设计了两阶段的需求匹配方法, 首先将用户信息和产品的免责范围进行匹配, 缩小了有效的产品选择范围, 然后在有效产品选择范围内, 通过计算需求与产品之间的加权距离有效计算出最满足用户需求的候选产品推荐给用户.

(3) 为该模型设计了实验, 模拟结果证明了该模型在推荐转化率、存储可扩展性及相关安全性方面达到了设计要求, 为安全高效地解决保险产品推荐问题提供了一种新方案, 也为产品合同签订和后续理赔流程

奠定了可信的证据基础.

1 背景知识

1.1 相关定义和说明

定义保险公司的集合为 I, 每一个保险公司 $i \in \{1,\cdots,|I|\}$, 公司i的公司信息集合为K_i, 产品集合为 P_i, 产品$p \in \{1,\cdots,|P_i|\}$, 其中, $R_{i,p}$是产品的保障范围. 比如“安联环游四海全球旅行-马哥波罗计划”产品的保障范围包含个人及宠物责任, 而其他保险产品的保障范围一般不包含宠物责任.$C_{i,p}$是产品的免责范围, 免责范围是指保险公司不承担赔偿责任的风险范围. 比如某保险公司健康险的免责范围包含遗传性疾病, 即当客户个人信息中包含此项内容时, 无论客户产生何种风险, 承保的保险公司都不承担赔偿责任; 而一般的同类产品免责范围不包含这一项, 由此可以看出, 由于不同保险公司的经验理念和精算模型不同, 对具体产品的定义和风险保障都有着自己的特点. 如果客户不了解这一点, 极容易造成不必要的损失. 而是否有遗传性疾病属于个人隐私信息, 很难在传统的推荐过程中被利用.

本文将客户μ的信息记作H_μ, 其对保险产品的需求可以分为两部分, 一部分是对公司的需求, 记为RI_μ, 另一部分是对产品保障范围等的需求, 记为RC_μ.

如果$H_\mu \cap C_{i,p} \neq \emptyset$, 意味着客户$\mu$即使购买了保险公司$i$的产品$p$, 保险公司也不承担保障责任, 这显然不是客户所需要的产品, 所以不构成有效的匹配.

定义 1. 有效匹配

如果$H_\mu \cap C_{i,p} = \emptyset$, 则$(p,i)$是客户$\mu$的一个有效匹配.

定义 2. 目标函数

假设(p,i)是客户μ的有效匹配, 推荐系统的目标是找到最符合客户需求的保险公司i及其产品p, 满足需求的程度可以用需求信息与目标信息之间的加权距离来表示, 形式上表达如下: 保险产品推荐模型的目标是找到满足如下条件的(p^*,i^*), 使得加权距离 $\omega_i \| RI_\mu - K_i \| + \omega_c \| RC_\mu - R_{i,p} \|$取值最小, 其中$\omega_i$, ω_c分别为客户对公司需求和产品需求的权重.

不失一般性, 为简化描述, 假定$\omega_i = \omega_c = 1$, 即:

$$\arg\min_{p,i}(\| RI_\mu - K_i \| + \| RC_\mu - R_{i,p} \|) := (p^*,i^*)$$

1.2 保险客户决策参考信息模型

参照文献[4]中提出的健康险保障计划模型, 我们提出一个通用的客户决策参考信息模型, 如图 1 所示. 其中公司信息部分在很多第三方网站上有部分展示, 但是其公信力和信息完整性都存在疑问, 难以作为真实有效的决策依据. 显然, 只有由公司自身才能为本公司提供真实可信并且完整的数据, 并且有大部分信息是不公开的, 需要系统进行隐私保护; 而产品信息一般是公开的, 不需要进行隐私保护. 由于目前市场竞争日益激烈, 公开的产品特性有日益趋同的趋势, 而反映公司服务实力的内在属性信息成为客户做出购买决策的重要因素. 相反, 该部分信息的缺失或者不可信会严重影响客户的购买意愿.

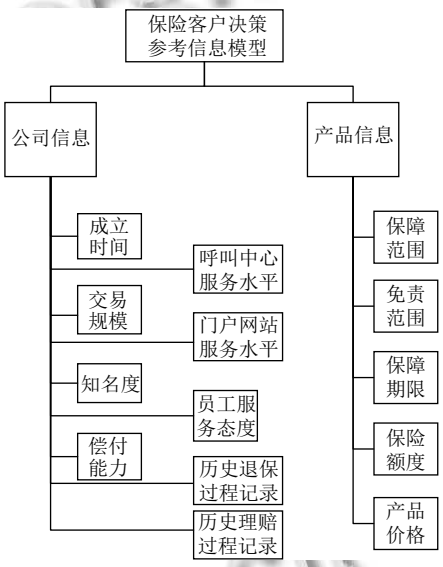

图 1 保险客户决策参考信息模型

2 系统设计

2.1 安全需求分析

本文将模型安全需求定义如下:

定义 3. 隐私保护

如果没有一个成员知道除预先定义功能以外的数据信息, 我们说该模型是支持隐私保护的, 比如在进行产品推荐时, 参与的公司都不应了解客户的健康隐私, 而客户也不应了解公司的内部隐私信息.

定义 4. 透明性

所有的计算对于交易双方都是透明的, 这可以防止竞争对手对匹配结果进行伪造, 也可以防止保险公司对他们的产品模型进行计算过程之后的修改.

定义 5. 可验证性

所有的计算过程和结果, 都可以让每一个参与方进行验证, 以保证确实是按照预定计算规则和参数计

算出来的最优解.

定义 6. 可信性

计算过程不依赖于任何单独一方, 每一个参与方都可以有能力发起匹配的过程, 从而实现去中心化的容错过程.

2.2 模型框架

本文提出的模型框架如图 2 所示, 该模型的流程可以分为如下几个阶段.

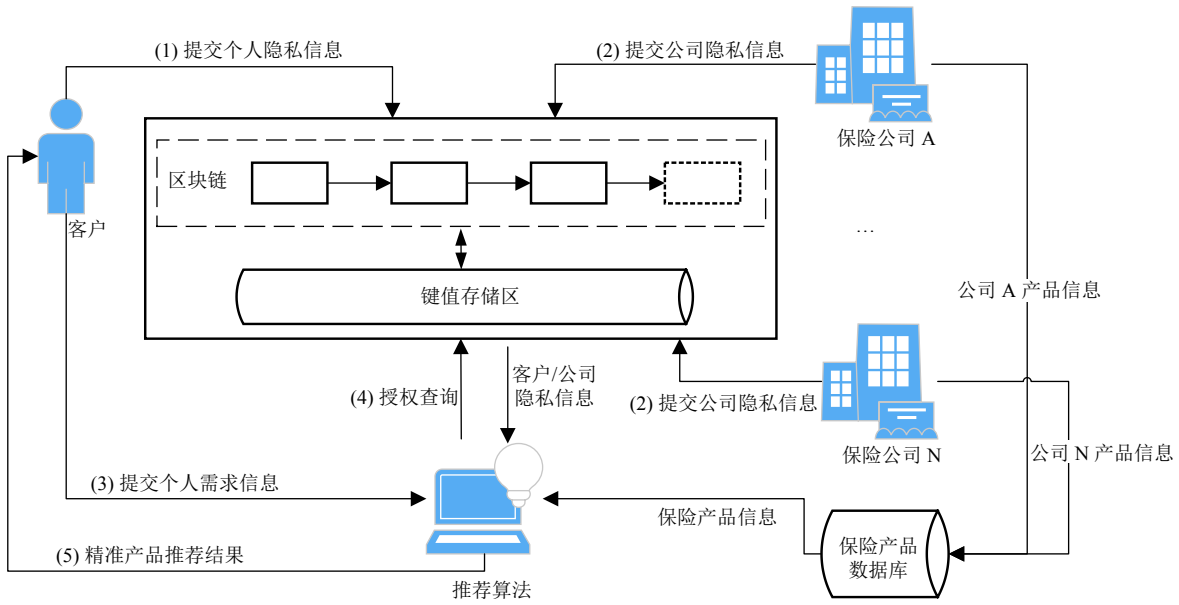

图 2 模型总体框架图

(1) 信息提交阶段

如图 2 中的步骤 (1)、(2), 客户μ和保险公司i将各自的信息H_μ和K_i提交给区块链进行加密存储并对推荐算法进行授权, 为了避免客户和保险公司的具体信息在区块链上被泄露, 同时也为了降低链上存储的数据量, 本文采取的方案是在区块链上只存储数据信息的存储地址, 具体信息以 key-value 方式存储在单独的键值存储区中, 基于文献[8]改进的数据提交流程如图 3 所示. 模型的事务处理流程和智能合约结构在 2.3 节做详细说明.

(2) 需求初步匹配阶段

在这个阶段, 如图 2 中的步骤 (3), 客户μ将自己对保险产品的需求RC_μ和对公司的需求RI_μ提交给推荐算法, 推荐算法首先根据客户μ的授权向区块链查询客户信息H_μ, 然后根据保险公司i的授权向区块链查询公司信息K_i, 数据查询的流程图如图 4 所示. 同时推荐算法从保险产品数据库中获取各个产品的免责范围, 根据有效匹配的定义得到客户μ的有效匹配产品集合, 记为$\tilde{P}$.

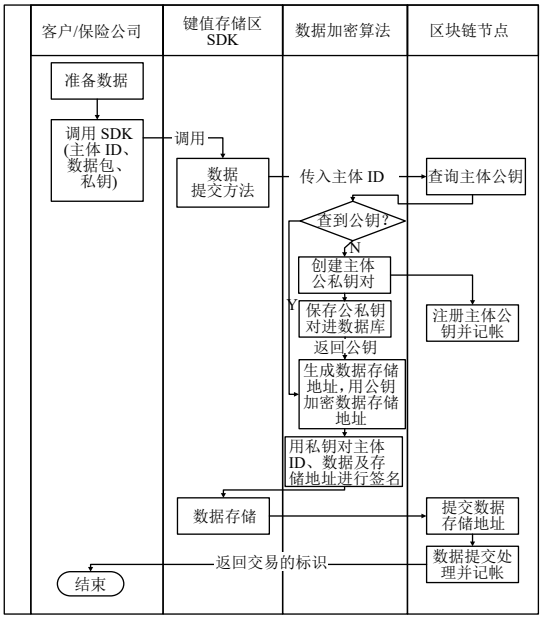

图 3 数据提交流程图

(3) 精准计算阶段

在这个阶段, 模型将根据客户需求对产品的匹配程度进行计算, 首先对RI_μ, RC_μ进行必要的预处理, 比

如对公司理赔的要求进行数值化处理, 如理赔响应时间<30 分钟, 理赔办结时间<3 天. 推荐算法的伪代码如算法 1 所示.

算法 1. 保险产品推荐算法

输入: 客户μ的需求RI_μ, RC_μ及有效匹配产品集合$\tilde{P}$
输出: 产品推荐结果(p^*,i^*)

```
s=0
for each p∈P̃ do
j=getcompany(p)
Retrieve K_j from blockchain
Retrieve R_{j,p} from product database
distance=||RI_μ−K_j||+||RC_μ−R_{j,p}||
if s=0 then
s=distance + 1
end if
if distance<s then
s=distance
p* = p
i* = j
end if
end for
return (p*,i*)
```

算法执行完毕后, 如图 2 中的步骤 (5) 所示, 模型将产品推荐结果(p^*,i^*)展示给用户.

2.3 区块链运行机制

在本节中, 我们描述如何对区块链中的信息主体、存取权限及其映射关系进行管理.

本文模型中的区块链包含两种事务类型, 一种用于信息存储和检索, 记作 T_r; 另一种用于访问控制管理, 记作 T_a; 当用户首次进行签名时, 将生成一个新的共享标识, 包含用户标识和对外服务标识, 并连同相关的权限一起发送到区块链的 T_a 事务中. 主体准备的隐私信息 (例如某遗传性疾病) 使用共享加密密钥进行加密, 并将其发送到区块链的 T_r 事务, 随后将其路由到键值存储区 (本文采用 MongoDB 来实现), 同时只保留指向公共分类帐上信息地址的 SHA-256 哈希指针.

主体 (如客户或保险公司) 和服务都可以通过 T_r 事务对指针关联的信息进行检索, 区块链会验证数字签名属于某主体还是服务. 对于服务, 还将通过 T_a 检查其访问信息的权限. 最后, 用户可以通过更新 T_a 事务随时更改授予服务的权限, 包括撤消对以前存储信息的访问.

在信息写入或者读取之前, 每一个信息区块对应智能合约的条件必须被满足, 下面说明主要的两种合约结构.

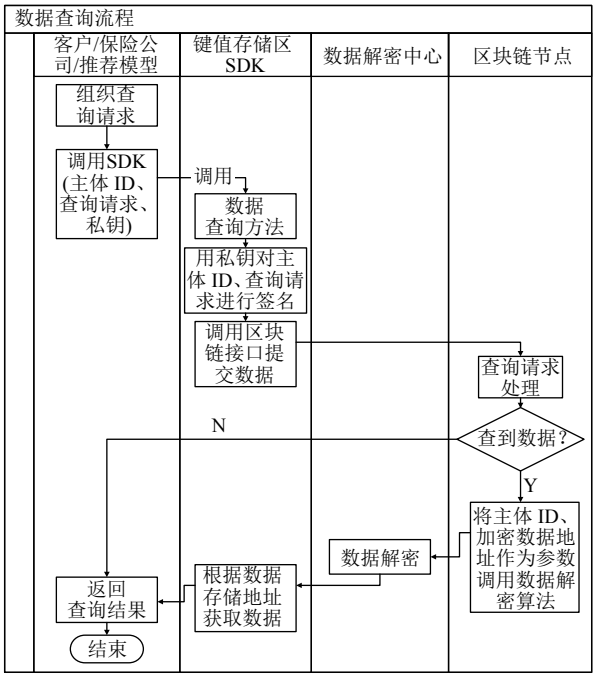

图 4 数据查询流程图

2.3.1 信息提供者注册合约

该合约控制客户或者保险公司如何成为区块链的合格信息提供者. 在约定的初始成员加入后, 对于新的成员加入申请, 基本的判断逻辑是区块链中的现有成员是否都同意新成员的加入. 如图 5 所示, 这种判断逻辑可以在智能合约中用代码的方式进行控制.

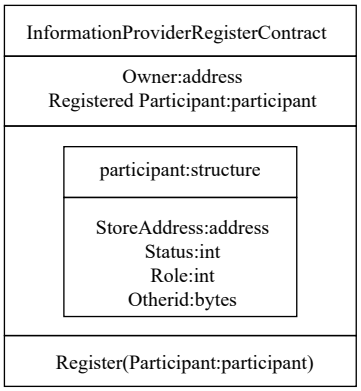

图 5 信息提供者注册合约结构

2.3.2 信息存取合约

该合约被用来执行区块链上信息存取的权限控制, 主要的信息内容包括信息所有者、信息在键值存储区

的地址、权限认证参数、保证数据未被篡改的 Merkle 树哈希值等, 结构如图 6 所示, 这些信息内容保证了信息是严格按照授权进行访问的.

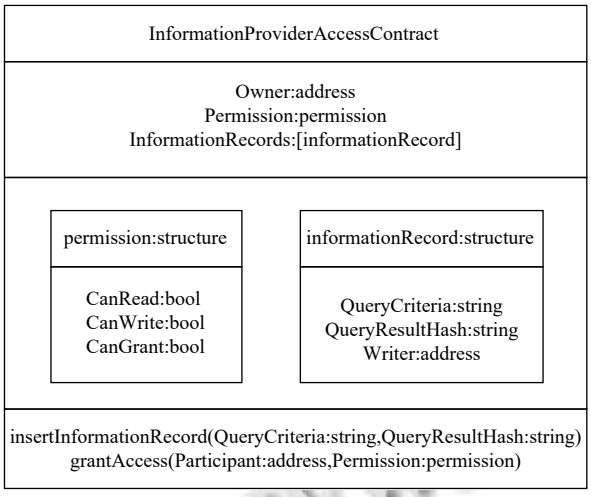

图 6 信息存取合约结构

2.3.3 实例分析

如图 7 所示, 客户 1、客户 2、公司 1、公司 2、算法 1 分别通过信息提供者注册合约加入到区块链中, 假设客户 1 的隐私信息为“遗传病=哮喘”, 公司 2 的隐私信息为“理赔时长=1 天”. 在信息存取合约中, 通过 insertInformationRecord(“遗传病”, “哮喘”) 和 insertInformationRecord(“理赔时长”, “1 天”) 加入到对应主体的信息存储地址队列中, 同时均通过 grantAccess (地址 5, “Y, N, N”) 将读取权限授权给算法 1.

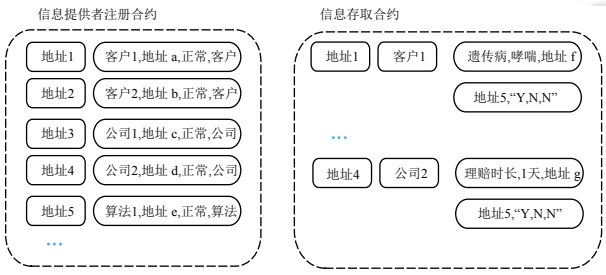

图 7 合约实例

本文中基于智能合约的模型实现过程具有如下特点:

(1) 灵活权限授权: 主体可以随时批准或撤销数据访问请求, 一旦授权立即生效. 如当整个保险产品推荐过程完成以后, 客户或者保险公司可以随时关闭对自己隐私数据的读取, 也可以对新算法进行随时授权.

(2) 细粒度访问控制: 模型可以对所选数据块 (而不是主体的所有数据) 授予更细粒度的访问权限, 这也提高了数据的可读性.

3 实验

为了评价本文提出的模型, 我们基于中国科学院软件研究所自主开发的区块链基础组件 RepChain[9]实现了该模型, 实验环境为 4 台服务器组成的节点网络, 服务器配置为 8 GB 内存, 600 GB 硬盘, 处理器为 Intel Xeon 2.4 GB 双核.

3.1 推荐性能分析

为了评价本模型在实际推荐过程中的效果, 我们选取了某第三方平台[1] 上 30 家保险公司的 836 种保险产品, 分为健康险、意外险和旅游险三个险类, 将本文模型与文献[3]中的算法进行比较, 并引用文献[3]中定义传统方式的产品推荐转化率 12% 为基线. 假设模型推荐的产品与用户需求的差距在 20% 之内, 则认为是一个成功的推荐, 定义如下:

$$Rsuc_{\mu}=\begin{cases}1, & \text{if}\ \dfrac{\|RI_{\mu}-K_j\|+\|RC_{\mu}-R_{j,p}\|}{\|RI_{\mu}\|+\|RC_{\mu}\|}\leqslant 20\%\\ 0, & \text{if}\ \dfrac{\|RI_{\mu}-K_j\|+\|RC_{\mu}-R_{j,p}\|}{\|RI_{\mu}\|+\|RC_{\mu}\|}>20\%\end{cases}$$

假设试验用户数量为 N, 则转化率 *conversion* 定义为:

$$conversion=\frac{\sum_{\mu=1}^{N}Rsuc_{\mu}}{N}$$

我们模拟了 100 个用户的需求, 实验结果如图 8 所示, 本文模型在三个险类的推荐成功率均优于文献[3]中模型和基线模型, 这是由于本文模型引入了基于区块链的隐私保护机制, 增加了推荐过程的信息量, 从而实现了更为精准的计算过程. 从不同险类的推荐效果看, 产品和隐私信息关联更为密切的健康险和旅游险推荐效果要优于意外险, 而文献[3]采用的贝叶斯网络方法没有考虑隐私信息因素的影响, 其推荐效果在不同险种上的表现基本上是一致的.

3.2 存储策略分析

为了保证隐私数据不被泄露, 本文中采用的数据

[1]http://www.huize.com

存储策略是在区块链上只存储数据信息的地址, 而将具体数据存储在链下的键值数据库中. 同时这样的设计也使得模型在链上空间存储上具有良好的可扩展性, 假设所交换的原始数据的大小为λ, 其引用指针的大小为ξ. 这样, 按空间复杂度存储在链上的数据总量为$O(hash(\lambda)+\xi)$. 而采取传统模型直接将数据信息存储在区块链的方式, 其存储在区块链上的数据总量为$O(\lambda)$. 而一般来说, 数据信息占用空间大于其哈希值与数据指针共同占用的存储空间.

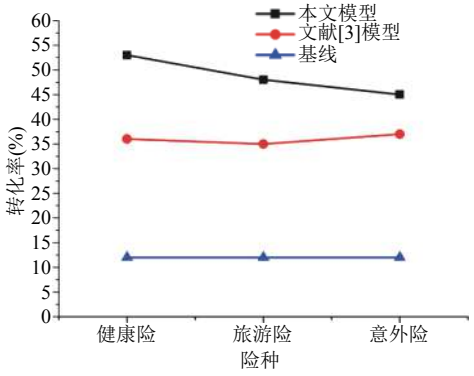

图 8 推荐转化率比较

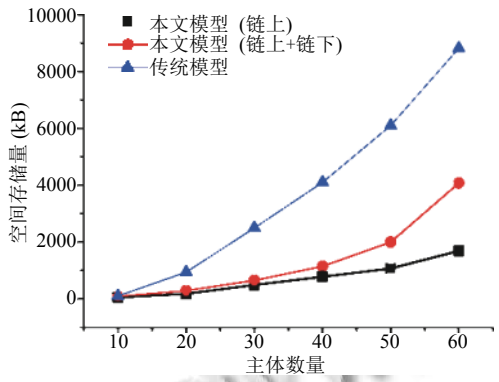

图 9 空间存储量比较

为了验证以上分析, 实验中将主体数量从 10 个逐步增加到 60 个, 以此来验证模型存储策略在可扩展性方面的表现. 实验结果如图 9 所示, 相对于传统区块链模型, 本模型实现的存储策略不仅使得链上存储量较小, 而且链上+链下的共同存储总量也显著低于传统模型的空间存储量, 随着主体数量的增加, 优势更为明显, 从而证明本文的存储策略具有良好的可扩展性.

本文中的数据存储方法可以有效解决链上数据安全和数据存储开销过大的问题, 弊端是这种存储方法只适合做原始数据的存储和整体查询, 而不适合对数据进行语义查询或者做进一步的处理, 例如对数据进行模糊查询等操作. 因此对于需要利用区块链上数据进行复杂处理的场景, 本模型还有待进一步改进, 这也是我们未来的工作方向之一.

3.3 安全性能分析

本文模型的隐私保护要求是:

(1) 没有一个客户了解公司的确切信息; (2) 没有一个公司了解客户的确切信息.

首先, 所有参与者都是匿名的, 即他们都是通过模型中的 ID 来参与计算的.

攻击者可能试图通过链接与同一匿名用户关联的不同数据段来对用户进行去匿名化, 此攻击称为链接攻击, 危及用户的隐私. 为了防止此攻击, 每个用户在不同推荐请求的每个交互中都使用一个新密钥.

在信息提交阶段, 区块链中的每个事务都包含确保完整性的数据哈希. 所有事务都使用不对称加密方法进行加密, 从而提供保密性. T_a 维护一个密钥列表, 为主体成员或服务提供访问控制, 只有嵌入私钥与区块链中的密钥列表匹配的事务才能转发给其他成员.

在需求初步匹配和精准计算阶段, 只有经客户和保险公司授权过的推荐算法才可能获取到客户和公司信息, 客户无需向任何参与的公司授权, 公司也无需向任何参与的客户进行授权, 因此该阶段不存在隐私泄露问题.

根据以上分析, 在本文的模型运行过程中, 没有一个客户了解公司的确切信息, 也没有一个公司了解客户的确切信息. 因此, 本模型实现了 2.1 节定义的隐私保护原则.

由于目标函数是公开的, 客户和保险公司作为主体都可以申请进行公开验证, 在匿名的情况下获得对方的授权, 取得计算过程所需要的信息, 独立发起计算过程进行结果验证. 经过模拟实验, 我们分别验证了本文的模型符合 2.1 节定义的透明性、可验证性和可信性.

4 结语

保险市场存在的双向信任缺失和隐私保护是保险产品销售过程中面临的实际问题, 本文提出了一个基于区块链的保险产品推荐模型. 该模型首先扩展了传统的保险要素, 加入个人健康记录、理赔历史记录等

隐私信息; 然后利用区块链的加密存储机制和智能合约技术实现了对个人、公司隐私信息的可扩展安全存取管理, 在隐私保护的前提下实现了个人信息和除外责任对应的产品有效性筛选; 最后提出了基于多要素特征匹配的精准保险产品推荐算法. 对本模型设计了实验, 结果表明, 该模型可在隐私保护的前提下, 提高产品推荐的转化率, 并实现计算过程的安全有效和透明公正. 在未来的工作中, 我们将采用形式化方法进一步验证和分析模型的特性, 并将该模型延伸到后续的产品成交和理赔过程.

参考文献

1 黄洪. 黄洪副主席在亚金协•中东欧金融前沿问题论坛上的开幕致辞. http://bxjg.circ.gov.cn//web/site0/tab5207/info4090860.htm, 2017-11-28.

2 Xu W, Wang JJ, Zhao ZQ, *et al*. A novel intelligence recommendation model for insurance products with consumer segmentation. Journal of Systems Science and Information, 2014, 2(1): 16–28.

3 Qazi M, Fung GM, Meissner KJ, *et al*. An insurance recommendation system using Bayesian networks. Proceedings of the Eleventh ACM Conference on Recommender Systems. Como, Italy. 2017. 274–278. [doi: 10.1145/3109859.3109907]

4 Abbas A, Bilal K, Zhang LM, *et al*. A cloud based health insurance plan recommendation system: A user centered approach. Future Generation Computer Systems, 2015, 43–44: 99–109. [doi: 10.1016/j.future.2014.08.010]

5 袁勇, 王飞跃. 区块链技术发展现状与展望. 自动化学报, 2016, 42(4): 481–494. [doi: 10.16383/j.aas.2016.c160158]

6 韩爽, 蒲宝明, 李顺喜, 等. 区块链技术在数字资产安全交易中的应用. 计算机系统应用, 2018, 27(3): 205–209. [doi: 10.15888/j.cnki.csa.006247]

7 薛腾飞, 傅群超, 王枞, 等. 基于区块链的医疗数据共享模型研究. 自动化学报, 2017, 43(9): 1555–1562. [doi: 10.16383/j.aas.2017.c160661]

8 闵旭蓉, 杜葵, 戴逸聪. 基于区块链技术的电子证照共享平台设计. 指挥信息系统与技术, 2017, 8(2): 47–51. [doi: 10.15908/j.cnki.cist.2017.02.009]

9 区块链技术与应用联合实验室. 响应式许可链基础组件 RepChain. https://gitee.com/BTAJL/repchain. [2018-07-11].