Journal of Computer Applications
计算机应用,2017,37(10):2787-2793
ISSN 1001-9081
CODEN JYIIDU
2017-10-10
http://www.joca.cn

文章编号:1001-9081(2017)10-2787-07
DOI:10.11772/j.issn.1001-9081.2017.10.2787

# 基于区块链的个人隐私保护机制

章　宁,钟　珊*
(中央财经大学 信息学院,北京 100081)
(*通信作者电子邮箱 shakira0909@163.com)

**摘　要**:针对互联网租车场景中个人隐私保护问题,提出一种基于区块链的个人隐私保护机制。首先,针对互联网租车中暴露的个人隐私问题提出一个基于区块链的个人隐私保护解决方案框架;然后,通过参与者简介、数据库设计以及性能分析给出模型的设计和定义,并从授予权限、写入数据、读取数据和撤销权限等方面阐述该模型的框架和实现;最后,通过基于区块链的系统开发表明了该机制的可实现性。

**关键词**:个人隐私保护;区块链;互联网租车;数据交互审计平台
**中图分类号**:TP311;TP393.08　　**文献标志码**:A

# Mechanism of personal privacy protection based on blockchain

ZHANG Ning, ZHONG Shan*
(*School of Information, Central University of Finance and Economics, Beijing* 100081, *China*)

**Abstract:** Aiming at the problem of personal privacy protection in Internet car rental scenario, a personal privacy protection mechanism based on blockchain was proposed. Firstly, a framework for personal privacy protection based on blockchain was proposed for solving personal privacy issues exposed in the Internet car rental. Secondly, the design and definition of the model were given by participant profile, database design and performance analysis, and the framework and implementation of the model were expounded from the aspects of granting authority, writing data, reading data and revoking authority. Finally, the realizability of the mechanism was proved by the system development based on blockchain.

**Key words:** personal privacy protection; blockchain; Internet car rental; data interactive audit platform

## 0　引言

随着计算机和网络的普及,个人隐私保护逐渐成为人们关注和担心的问题。如果忽视个人隐私保护问题或者对其处理不当,可能会给人们带来经济名誉损失甚至阻碍网络创新等后果。个人隐私保护问题可以通过法律和技术两条途径进行解决,而当前出现的区块链技术正好可以成为个人隐私保护问题的有效解决方案。区块链是一个分布式的账本,记录了每个交易发送和验证的历史,同时也记录了交易中包含的额外信息[1]。区块链中所有的区块都按照时间先后顺序排列,由矿工不断地创造添加,并且每个节点都有一份区块链信息的备份。区块链技术由于具有去中心化、永久记录和便于审计等特点[2],刚好可用于满足隐私数据的完整性、可限制性以及可审计性等数据安全需求,因此可以作为个人隐私保护问题的有效解决方案。

国内外关于区块链技术的文献不多,其中关于区块链技术在个人隐私保护问题上应用的文献更是凤毛麟角。在区块链技术对于个人隐私保护问题的应用领域方面,Swan[3]提到健康隐私问题的严重性,认为区块链技术可以提供一个保护个人健康隐私数据不受侵犯的机制,但是却没有给出区块链对于个人隐私保护问题的应用场景实现细节。在使用区块链技术解决实际问题并提供具体实现细节方面,Zyskind 等[4]提出了一种去中心化的个人信息管理系统,通过某种协议,可以在该系统中使用比特币来传递存储、询问和数据分析等指令,从而确保用户拥有和控制他们自己的信息;但是该文并没有提出具体的案例应用,也没有关于个人隐私理论问题的阐述。Kosba 等[5]认为当前的区块链交易环境缺乏交易的隐私保护,虚拟地址之间的金钱流动完全暴露在区块链环境中,因此提出了一个叫作 Hawk 的去中心化智能合约系统,通过避免在区块链上存储财务交易的明文形式来保障交易的隐私性;但是该方法只能保障交易信息的隐私性,缺乏更加广阔的实际生活领域应用空间。Lazarovich[6]详细给出了如何使用区块链技术来保护个人隐私,提出了基于分布式存储的第三方数据库 escrow 以及基于区块链审计的隐形墨水系统,并以医疗信息个人隐私保护为例来阐明区块链技术在个人隐私问题上的应用;但是缺乏对个人隐私问题的探讨以及区块链应用细节的展示。综上所述,国内外学者对区块链在个人隐私保护问题上应用的研究还十分有限。因此,本文将通过代入具体应用场景,将区块链技术个人隐私保护机制的应用细节进行逐一阐述,为进一步研究个人隐私保护问题提供机制参考。

刘雅辉等[7]提出,个人隐私保护问题的技术层面解决方案需要考虑匿名、数据访问控制、审计、在线社会网络隐私保护、移动定位隐私保护以及数据库个人隐私保护等方面的问题和需求。广受社会关注的互联网租车场景刚好贴合上述需求,具有一定的普遍性和代表性,因此本文将其作为区块链技术个人隐私保护机制的应用场景。

**收稿日期**:2017-03-13;**修回日期**:2017-05-31。　**基金项目**:国家社会科学基金资助项目(13AXW010)。
**作者简介**:章宁(1975—),女,江西临川人,教授,博士,主要研究方向:个人信息保护、互联网金融、服务外包;　钟珊(1992—),女,重庆人,硕士研究生,主要研究方向:区块链、个人信息保护。

## 1 互联网租车及其个人隐私问题

### 1.1 互联网租车场景及流程

互联网租车以“租车+代驾”为基本模式为乘客提供了一种新型的城市出行方式[8]，我国的“滴滴出行”等互联网租车软件平台已经受到了民众的欢迎。但是随着互联网租车的逐渐盛行，个人隐私问题也暴露无遗，并引起了社会的广泛关注。

考虑这样一个场景：乘客想要通过互联网租车软件出行去公司上班。首先，乘客在互联网租车软件中输入目的地；然后由互联网租车软件自动获取乘客出发地，推荐一定范围内的司机，并将乘客出发地信息发送给司机；司机接收到后决定是否抢单，而抢单成功的司机有优先权完成本次交易。

### 1.2 该流程暴露的问题

乘客每天都使用该软件，出行路线也比较固定。在此过程中，乘客遇到了一些个人隐私方面的问题：

问题1 乘客无法保证互联网租车平台会对自己的个人信息进行保密，上传的行程路线信息可能会被互联网租车平台盗用于推销广告以及获取其他商业价值。

问题2 平台及各个司机可以随意查看乘客行驶路线信息，使得乘客难以有效掌控自己的个人隐私信息。

问题3 当乘客想要停止使用该互联网租车软件时，之前保存于该软件上的信息却无法清空。

问题4 假如乘客已经成功要求该互联网租车软件删除自己的个人信息，若之后该软件受到黑客攻击，乘客发现泄漏名单中竟然有自己的名字，也没有任何证据对其进行诉讼。

### 1.3 解决方案

为了解决上述四个隐私保护问题，本文使用基于区块链的第三方数据库和数据交互审计平台来进行个人隐私保护。

第三方数据库是指用户可以选择自己信任的数据库来实现个人隐私数据的托管。第三方数据库是一种开源的数据库，只要提供一个链接便可使用。由于其存放的是用户隐私数据的加密形式，因此看不见隐私数据具体内容。不同用户可选择不同的第三方数据库，通过这样的分布式存储可以增强数据安全性以及减少互联网租车软件服务器的数据存储量。

数据交互审计平台是一种建构在区块链之上并对所有数据操作行为进行审计的系统。数据交互审计平台使用区块链来记录互联网租车平台、司机以及其他团体对用户数据的每一次操作，包括读数据、写数据、更新数据以及许可管理。数据交互审计平台可保证所有相关数据操作都被记录在区块链中，从而加强了互联网租车软件平台等各方的操作合规性，同时能够让用户真正控制和掌握自己的数据。

本文解决机制框架如图1所示。首先，乘客、第三方数据库和数据交互审计平台之间进行初始密钥交换，并由乘客授予数据交互审计平台权限。为了租车，乘客将上传自己的行程路线隐私信息。通过第三方数据库及区块链审计方法，回避互联网租车软件平台，使得其无法获取用户的整个行程路线，问题1将得到解决。

其次，在互联网租车软件平台和司机读取乘客行程路线的过程中，两者通过数据交互审计平台获取用户数据，其所有操作都记录在区块链上；再加上第三方数据库无法看到用户数据明文形式，其分布式存储可保障用户数据安全。上述均增强了乘客对个人隐私信息的掌控感，问题2将得到解决。

然后，乘客可以读取访问者记录，不仅增强了对自身数据的掌控感，同时假如平台泄露隐私，乘客还可以有证据状告该平台的违规操作，问题4将得到解决。

最后，当用户不想继续使用该互联网租车软件平台时，可以撤销该平台所在数据交互审计平台的操作权限，从而保障自身隐私免受侵害，问题3得到解决。

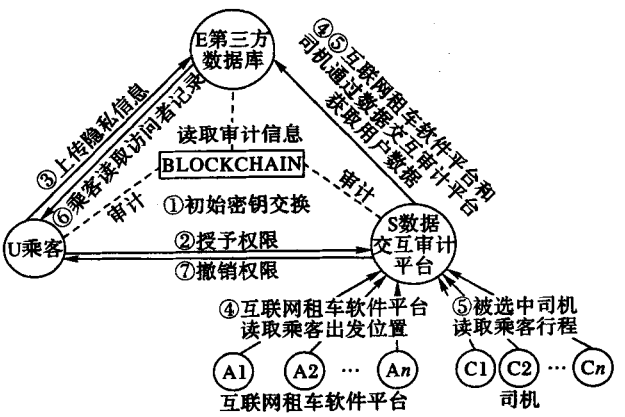


图1 基于区块链的个人隐私保护解决方案

Fig. 1 Personal privacy protection solution based on blockchain

## 2 模型设计和定义

### 2.1 参与者

模型中包括以下参与者：

1)乘客移动终端(本文用U表示)。乘客移动终端可以是下载了互联网租车平台APP的用户手机，代表了用户身份。

2)数据交互审计平台(本文用S表示)和第三方数据库server(本文用E表示)。

3)互联网租车软件平台(本文用A表示)。互联网租车软件平台即常见的打车软件。A需要获取乘客出发地点，以此来提供可匹配的最佳司机源(比如一定范围内的司机)。

4)互联网租车软件司机(本文用C表示)。互联网租车软件司机可以是下载了互联网租车平台(司机版)的司机移动终端。当A提供了若干个可匹配的最佳司机C后，会将乘客出发地发送给C。C申请查看乘客行程路线后决定是否抢单。

### 2.2 数据库

#### 2.2.1 区块链数据库

对于区块链数据库的设计来说，首先要提到区块链交易的说明书定制。Herbert等[9]在解决授权问题时提到了两种方法：一种是Master bitcoin模型，另外一种是Bespoke模型。Herbert等想要解决的问题是如何通过区块链来完成对软件使用的授权，以及如何保障软件完整、防止软件盗版、实现软件更新。在Master bitcoin模型中，软件厂商通过区块链，在特定的区块链钱包地址中向用户钱包地址转移1单位的Master bitcoin，以此来代表厂商对用户授予软件的使用权。用户手中欲购买的软件将自动读取交易，若验证得到用户地址中的

Master bitcoin 确实来自于厂商的特定地址,则自动启动安装;否则用户将无法安装软件。而 Bespoke 模型则使用了一种具有特殊说明书(specification)的区块链,将一些额外的域成分包含在说明书中。这些额外的域成分是为软件授权的灵活要求量身定制的,比如可以在说明书中加入 token、license、software Hash 以及 signature 等域,来进一步实现软件的所有权转移和完整性检查等高级功能。另外,区块链说明书对于不同的加密货币是不同的,有时候可以根据自己的需要来构筑这种说明书,从而满足特定的应用需求。

Herbert 方法[9]对于本文的互联网租车案例也有一定的启发。本文可以通过实现不同个体在区块链上发送交易来达到对交易内容的审计,因此本文也需要使用一种特别定制说明书的区块链。也就是说,本文可以根据特定的目的来构造一种更为独特的区块链说明书。本文的交易说明书如图 2 所示。

| TRANSACTION SPECIFICATION | | | |
|---|---|---|---|
| tx-id | Hash(meta-data) | token | signature |

图 2　交易说明书(specification)中域的特别定义

Fig. 2　Special definition of specification fields

图 2 中 Hash(meta-data)是该交易所需要传达的某个消息 meta-data 的哈希值,目的是为了以一种较短字节的方式来存储较长的消息 meta-data;token 用来记录是谁查看或者操作了乘客 U 的信息;signature 则用来记录发送者的签名,主要是为了验证发送者的身份,从而能够确定该交易的真实性; tx-id 是特定的交易号,起到区块链当中的唯一标识作用。

在本文的定制交易中,发送者使用接收者的公钥对消息进行加密生成 Hash,接收者使用自己的私钥进行解密;发送者使用自己的私钥进行签名生成 signature,接收者使用发送者的公钥进行签名验证。

### 2.2.2　第三方数据库

第三方数据库 E 需要有能力为每一个"用户-数据交互审计平台"组合建立和维护一张表 the chain of title,以此来记录它曾验证过的所有区块链交易号 tx-id 以及其对应交易的详细信息(比如 token 和 signature)。该表构造如图 3 所示。

| The chain of title | | | | |
|---|---|---|---|---|
| tx-id | Hash(meta-data1) | token | signature | Encrypt(meta-data2) |

图 3　第三方数据库的表

Fig. 3　Table of the third database

图 3 中 Hash(meta-data1)是某个消息 meta-data1 的哈希值,对 E 不可见。token 存放乘客隐私信息的数据操作动作,对 E 可见,且 E 可根据 token 具体内容采取相应措施。signature 是 E 需要使用相应发送者的公钥进行验证的部分。Encrypt(meta-data2)是用户个人隐私数据的加密形式,E 无法看到其明文形式。

### 2.2.3　数据交互审计平台数据库

数据交互审计平台数据库存放了各参与者(如 U、E、A、S)进行数据交互时所需的一些必要信息,包括区块链地址(如 U 的区块链地址 UAddress)、非区块链 ID 号码(如 U 的非区块链 ID 号码 UID)等,其角色类图、角色属性、角色方法如图 4 和表 1 所示。

该数据库有如下几种角色方法。

1)send(X;Y)。向 X 发送内容 Y。发送方式包括发送到区块链地址和非区块链地址两种。发送到区块链地址是指将相应交易发送到某角色所在区块链的钱包地址当中。由于区块链定制域中包含了 meta-data 等定制内容,通过该交易刚好能实现对所装载信息的审计。以参与者 U 为例,一般的发送形式为 U. send(XAddress; Hash(meta-data, token, signature)。发送到非区块链地址是指将相应内容通过电子邮件等方式进行发送。以参与者 U 为例,一般的发送形式为 U. send(X; Y)。其中接收者具有辨识内容 Y 并且由此触发相应动作的能力,而内容 Y 包括普通信息、授权指令等类型。

2)read(X)。读取区块链上的交易 X。一般由 E 通过 tx-id 将区块链上相应的交易查找出来,比如根据一个 tx-id "002"找到区块链上的相应交易并提取出来。读取所有交易(如读取 all-token),则是将对应参与者的所有交易依次遍历提取出来。

3)generate(X)。生成密钥 X。本模型中,生成密钥主要包括生成非对称密钥和生成对称密钥两种类型。生成非对称密钥是指系统将用户鼠标或触屏的滑动路线数据作为输入,采用椭圆曲线密码体制(Elliptic Curve Cryptography, ECC)生成公钥和私钥。而生成对称密钥是指系统将用户鼠标或触屏的滑动路线数据作为输入,采用高级加密标准(Advanced Encryption Standard, AES)算法生成对称密钥作为双方共享密钥。

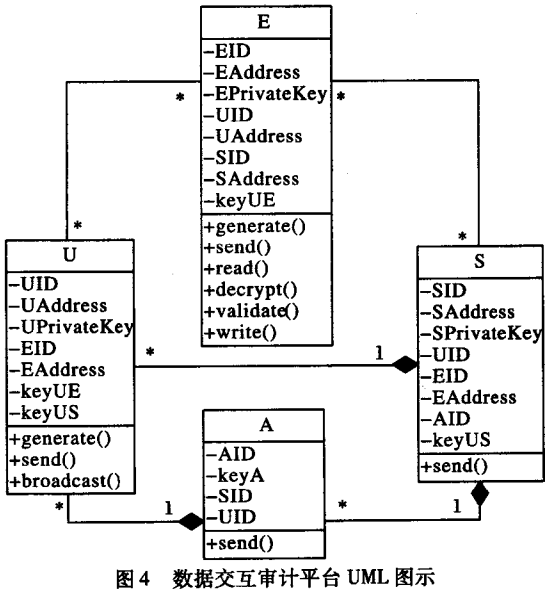


图 4　数据交互审计平台 UML 图示

Fig. 4　UML diagram of data interactive audit platform

表 1　各角色属性释义

Tab. 1　Attribute definitions of roles

| 属性名 | 属性释义 |
|---|---|
| XID | X 的非区块链地址,仅用于传递普通的明文或加密信息,比如 U 的邮箱地址 |
| XAddress | X 的区块链地址,也是 X 的公钥。一般不是唯一标识,因为每个参与者 X 可以有多个区块链地址 |
| XPrivateKey | X 的私钥。对于某个 X 来说,一个私钥便对应了一个区块链地址(公钥) |
| keyXY | X 和 Y 之间的对称密钥 |

4) decrypt(X)。解密X。解密是指E将相应交易读取出来,使用自己的私钥得到交易的具体内容,包括tx-id、Hash(meta-data)、token,以及signature等部分。以E. decrypt(EAddress. transaction)为例,其伪代码为:

```
token = DecryptEAddress(transaction). token
        //用E的公钥EAddress来解密交易得到token部分
signature = DecryptEAddress(transaction). signature
        //用E的公钥EAddress来解密交易得到signature部分
```

5) validate(X)。验证X。验证一般指E使用相应发送者的公钥对解密出来的token和signature进行验证。验证完毕后,E将提取出来的token和signature等信息存储在它自己所维护的the chain of title表中。针对E. validate(token)而言,一般流程的伪代码如下:

```
E. read(token);                          //E读取当前的token
E. check(U. the_chain_of_title);
    //E在the chain of title表中,找出属于该乘客U的那张表
test = true                              //设定测试变量为true
For(tx_id = 1;tx_id <= tx_id. max;tx_id ++)
    //循环,依次遍历U的the chain of title表中的tx_id
  {if (U. token = "U撤销S操作其数据的权限")
    {test = false;break;}}
  /*若该条tx_id对应的token内容为撤销权限,则测试变量
    test变为false;若没有出现撤销权限,则测试变量test仍然
    为true*/
  if (test = true)          //循环结束之后检查测试变量test的值
    {Insert token into U1. the_chain_of_title; Execute(token)}
    /*若test为true,则将该条token插入到the chain of title表
    的末尾(从细节上说,应该是同tx-id、token、signature等内容
    一起插入),然后执行token中所交代的内容*/
  Else refuse.                           //若test为false,则拒绝执行
```

6) write(X)。将内容X写入数据库。当E收到其他参与者发送到E非区块链地址中的交易号tx-id及其对应内容X后,会将该信息写入tx-id对应条目中。举例,当E收到U发送的交易号为002且对应信息为encryptkeyUS(meta-data2)的消息后,E将会把该消息写入002对应的条目中。

7) broadcast(X)。将内容X在区块链上进行广播。所谓广播是指用户将交易发送到区块链上,然后由各个节点进行验证,从而能够获知X的具体内容,使得X内容得到公开。

#### 2.2.4 互联网租车软件平台数据库

互联网租车软件平台数据库是由互联网租车软件平台自身维护的数据库。本文将该数据库进行简化处理,只留下区块链交互等关键部分进行数据库展示。其角色类如图5,属性释义及方法释义见表1。

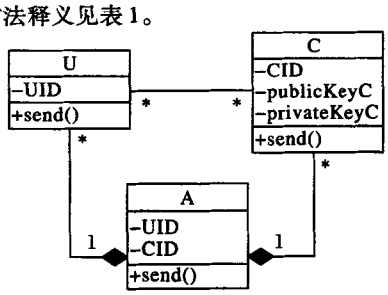


图5 互联网租车软件平台UML图示

Fig. 5 UML diagram of Internet car rental platform

### 2.3 加密算法及性能分析

#### 2.3.1 加密算法

2.2.3节提到本模型生成密钥(generate(X))所使用的加密算法包括两种类型:第一种为区块链上对较短数据量进行加密时所使用的ECC椭圆曲线加密算法;第二种为非区块链部分进行个人隐私信息较长数据传递时所使用的AES对称加密算法。

对于非对称加密算法而言,本模型区块链中生成公私钥

$$privateKey = \mathrm{SHA256}(message) \tag{1}$$

$$publicKey = \mathrm{Secp256k1}(privateKey) \tag{2}$$

其中:*message*为用户鼠标或触屏的滑动路线数据作为输入的随机值;*privateKey*是生成的私钥;*publicKey*是生成的公钥;SHA256是一种常见的哈希算法;Secp256k1是区块链中常用的ECC椭圆曲线算法。

对于对称加密算法而言,当前使用较多的是AES的Rijndael算法。由于Rijndael具有密钥安装速度快、未提出已知攻击方法和安全性高的优点,因此非常适用于本模型非区块链部分的对称加密。

#### 2.3.2 性能分析

区块链的安全性与每轮区块生成率(block generation rate per round,简记为f)相关[10]。每轮区块生成率$f$是指信息传递过程中每轮所用的工作量证明(Proof-Of-Work,POW)解决方案的期望值。区块链的安全性与$f$之间成反比关系,因此区块链的安全性可用$1/f$来表示。$f$与区块链中其他相关性能变量之间的关系如下所示:

$$transactionProcessingSpeed \propto \frac{blockSize \times f}{roundDuration} \tag{3}$$

其中:*transactionProcessingSpeed*是区块链上的交易传播速率;*blockSize*是区块大小;*roundDuration*是每轮持续时间。由于每轮持续时间与区块生成时间间隔(*blockInterval*)成正比,即$roundDuration \propto blockInterval$,因此可以将式(3)改写为:

$$transactionProcessingSpeed \propto \frac{blockSize}{blockInterval \times (1/f)} \tag{4}$$

可见区块链的安全性与区块大小(*blockSize*)、区块生成时间间隔(*blockInterval*)以及交易传播速率(*transactionProcessingSpeed*)有一定的相互制约关系。另外,区块大小和区块生成时间间隔之间还有如下关系:

$$blockSize = m \times Q \times blockInterval \tag{5}$$

其中:$m$是每个交易数据的平均大小;$Q$是每秒上传的交易数量。可见,在$m$和$Q$给定的情况下,*blockSize*和*blockInterval*之间也存在制约关系。

对比特币区块链而言,*blockSize*为1 MB,*blockInterval*为10 min。但是在本模型基于区块链的互联网租车场景中,由于第三方数据库需查验审计后才能进行写入数据和读取数据操作,对审计及时性的要求较高,所以*blockInterval*较低;但由于互联网租车平台每秒上传的订单交易量$Q$较大,所以*blockSize*可以基本保持不变。因此,在*blockInterval*较低而*blockSize*保持不变的情况下,根据式(4),为了使得区块链安全性(用$1/f$表示)保持稳定,需要在一定程度上提升交易传播速率(*transactionProcessingSpeed*)。

## 3　模型框架和实现

该模型主要包括初始密钥交换、授予权限、上传隐私信息等 7 个流程板块。流程中部分参考数据标识定义如表 2 所示。

表 2　参考数据标识及内容

Tab. 2　Reference data identification and content

| 数据标识 | 内容 |
|---|---|
| token | 为空 |
| token1 | U 授予 S 操作其数据的权限 |
| token2 | U 授权 A 读取其初始位置 |
| token3 | U 授权 C 获取 U 的行程路线 |
| token4 | U 想要撤销 S 对 U 数据的操作权限 |
| meta-data1 | U 的行程路线等私人信息 |
| meta-data2 | A 想要获取 U 的初始位置 |
| meta-data3 | U 的初始位置 |
| meta-data4 | C 想要获取 U 的行程路线信息 |
| meta-data5 | U 的行程路线 |
| meta-data6 | U 想要读取其访问者记录 |
| meta-data7 | U 请求撤销 S 对其数据的操作权限 |
| E. check-permission | E. read( EAddress. transaction) ;<br>E. decrypt( EAddress. transaction) ;<br>E. validate( signature) ; E. validate( token) |

### 3.1　初始密钥交换

乘客、数据交互审计平台、第三方数据库之间首先要进行密钥交换,具体流程如图 6 所示。

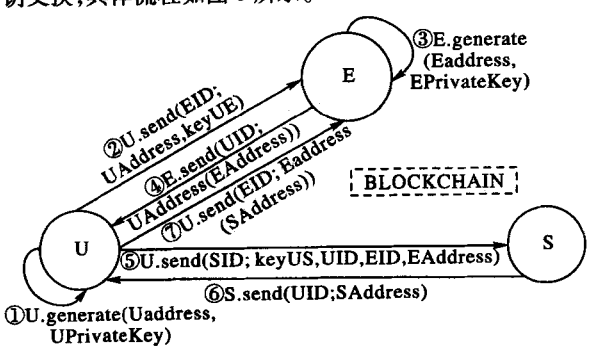


图 6　初始密钥交换

Fig. 6　Initial key exchange

### 3.2　授予权限

乘客申请使用数据交互审计平台,并授予其在区块链审计前提下操作乘客数据的权限,如图 7 所示。

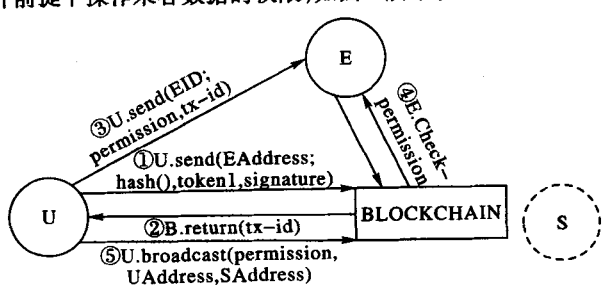


图 7　授予权限

Fig. 7　Grant permissions

### 3.3　上传隐私信息

乘客要进行互联网租车,应当首先提供自己的出发地和目的地等个人隐私信息,并且上传至第三方数据库并审计在区块链中。由于区块链大小有限,上传的审计信息都是长度较短的哈希值。乘客上传出发地和目的地信息到第三方数据库之后,将自动触发互联网租车软件平台进行司机推荐等一系列动作(将在 3.4 节详细阐述)。该自动触发机制由乘客向互联网租车软件平台发送打车请求 request 来实现。

由此,本文解决了问题 1,从而互联网租车软件平台无法获取用户的整个行程路线隐私并售卖给其他团体,并且上传至第三方数据库并审计在区块链中,如图 8 所示。

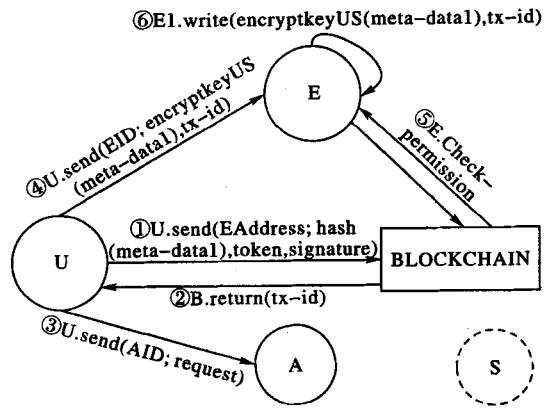


图 8　上传隐私信息

Fig. 8　Upload privacy information

### 3.4　平台读取乘客位置及推荐司机

互联网租车软件平台要读取乘客的出发位置,并以此为基础给乘客提供可推荐的司机。数据交互审计平台是互联网租车软件平台所选择使用的隐私保护系统,所以互联网租车软件平台若是想要获取乘客的出发位置,仍然需要通过数据交互审计平台来向第三方数据库申请,如图 9 所示。

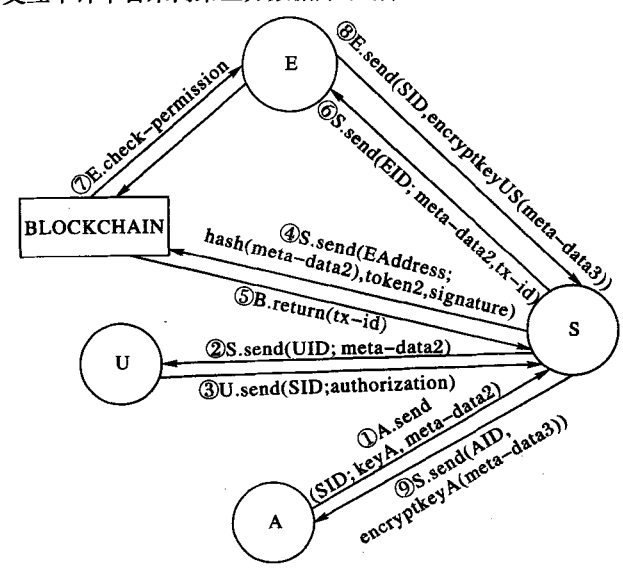


图 9　互联网租车软件平台读取乘客出发位置

Fig. 9　Internet car rental platform reads passenger's departure location

### 3.5　司机读取乘客行程路线

互联网租车软件已读取乘客出发位置,由此通过系统匹配出最佳位置司机,并将乘客的出发地发送给司机。司机将自动申请查看行程路线,并决定是否抢单。整个过程如图 10 所示,避免了互联网租车软件平台对用户行程路线隐私的获

取。抢单成功后,该司机将有机会向该用户提供打车服务。

由此,通过本节和3.4节本文解决了问题2,从而互联网租车软件平台和司机的所有操作都会记录在区块链上,使得乘客能够拥有掌控自己个人隐私信息的能力。

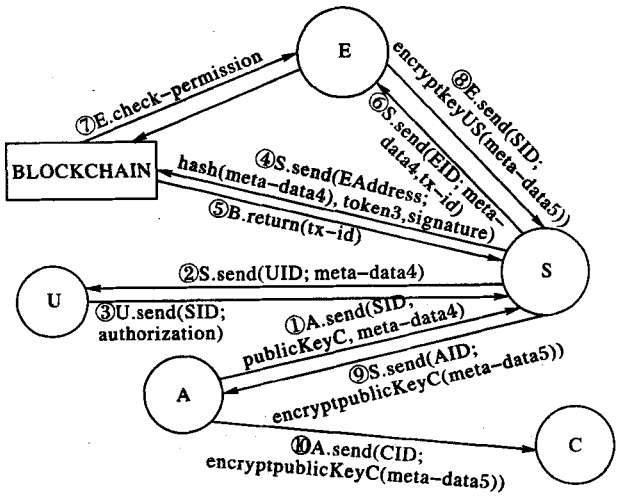


图10 被选中的司机读取乘客行程路线的操作流程

Fig. 10 Selected driver reads passenger's itinerary

### 3.6 乘客读取访问者记录

乘客可通过token值读取访问者记录,因为token中含有乘客的授权记录,即授权何种角色团体查看乘客的何种信息,如图11所示。

由此,本文解决了问题4,乘客不仅能够看到所有的访问者记录,增强对自己数据的掌控感,还可以有证据状告隐私泄露平台的违规操作(未及时清空乘客信息)。

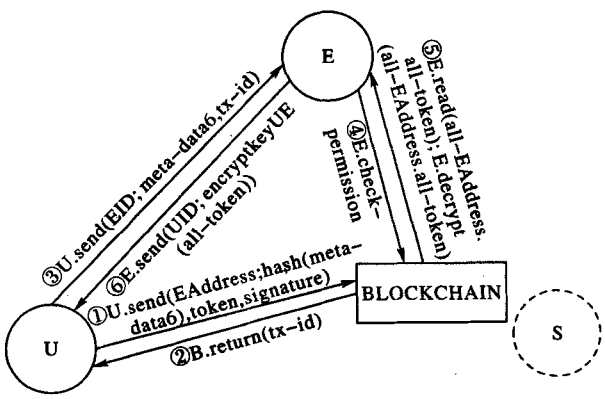


图11 乘客读取访问者记录

Fig. 11 Passenger reads visitors' records

### 3.7 撤销权限

乘客可能因为某些原因想终止使用当前互联网租车软件平台,并希望通过撤销其数据交互审计平台的权限来终止互联网租车软件平台对自己数据的读取,如图12所示。另一方面,乘客也可以放弃当前的第三方数据库而选择其他的第三方数据库。但由于第三方数据库对乘客隐私信息完全不可见,所以事实上乘客没有必要改变当前的第三方数据库。

由此,本文解决了问题3,从而一旦乘客决定停止使用该互联网租车软件,可以马上撤销数据交互审计平台对自己数据的访问权,以保障自身隐私免受侵害。

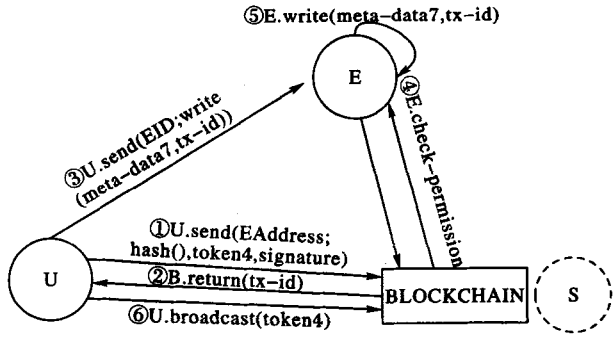


图12 撤销权限

Fig. 12 Revoke permissions

## 4 系统设计与实现

本文采用Gcoin进行系统实现。Gcoin是一种能够支持安全性、效率性和低维护成本的区块链交易平台,可实现各类金融资产永久性记录保存。就参与者和数据库而言,首先,本系统的数据交互审计平台主要由python连接Gcoin平台进行操作,可将各参与者提供的数据操作动作以字符串的方式插入和审计到区块链中。而第三方数据库server可根据交易号tx-id来查验某个数据操作动作是否在区块链上进行了审计,采用的方法是判断给定字符串与审计在区块链当中的字符串是否相同。其次,由于资源限制,本系统采用MySQL数据库对第三方数据库the chain of title表进行模拟,能够在形式上存储该表中应有的信息并完整记录所有数据操作动作。最后,对于互联网租车平台和司机,主要呈现了其与数据交互审计平台之间的交互行为。剔除次要功能之后,本系统主要功能框架布局如图13所示。

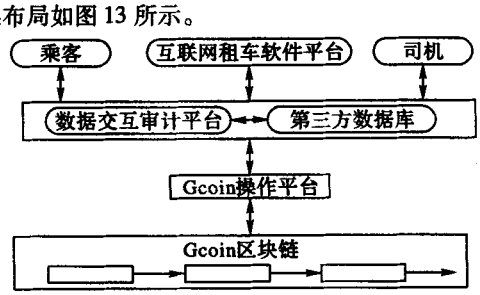


图13 系统底层框架布局

Fig. 13 Layout of system bottom framework

就系统操作流程而言,以写入隐私数据和读取隐私数据为例,首先由乘客U上传行程路线信息至第三方数据库。互联网租车平台A向数据交互审计平台S申请获取用户初始位置。S将该数据操作动作审计在区块链上,并将生成的交易号和数据操作动作一起通过邮件发送给第三方数据库server E。然后,E通过S提供的交易号和数据操作动作,在区块链中查验其是否审计成功。若审计成功,则E将该数据操作动作和相应交易号信息放入the chain of title表中;反之则拒绝完成此动作。最后,E将对应的用户行程位置个人隐私数据的加密形式发送给S,S将该信息返回给A,并由A返回给相应匹配司机C。

就系统关键步骤而言,可由表3所示(部分过长数据未完全显示)。对于步骤"S将该数据操作动作审计在区块链上",当S将数据操作动作审计入区块链后,系统将自动返回审计后的关键信息值,包括原始信息的加密值(raw_tx)、签名

(sig)、区块链交易号(tx_id),以及数据操作动作信息字符串的加密转化值(op_return)。其中,sig 由原始信息加密值和接收者私钥共同作用生成,tx_id 来自交易插入区块链后的自动返回信息。

表 3　审计过程关键信息值举例

Tab. 3　Critical value of audit process

| 类型 | 标识 | 操作内容举例 |
|---|---|---|
| 审计前输入信息值 | S 区块链地址(from_address) | 1C9UtVyqTsCzbwh5BfhEfgXikZA2gSNi7P |
| | E 区块链地址(to_address) | 1BD5v4RbFiij9QKLCpuydksyp53QnMU9qi |
| | S 区块链私钥(privateKey) | 6932e11206c5ece7ae48636160f526aae62b5e82899ae5c82891fa59b9973d6d |
| | 数据操作动作(op_return_data) | A1ReadDepartureOfU1InU_ordernumber01-20170514074951 |
| 审计后得到关键信息值 | 原始信息加密值(raw_tx) | 010000000108c9b7e6a1bf5f1c357595d0e52fe16840d651a… |
| | 签名(sig) | 01000000008c9b7e6a1bf5f1c357595d0e52fe16840d651ab… |
| | 区块链交易号(tx_id) | dd1f1b8f33edc577e8386dba79571316b1cc09703381457ef9b48fc677897769 |
| | 审计信息加密转化值(op_return) | 0472998f3f4e45e8a8c2ba8318c068b0245c6178ace6cdffc… |

## 5　结语

互联网租车个人隐私保护问题一直没有得到有效解决,除了民众隐私保护意识淡薄致使互联网租车软件平台缺乏改善动力之外,当前隐私保护技术的不足也使得互联网租车软件平台缺乏改善能力,而区块链技术的应用刚好为互联网租车提供了一种个人隐私保护的有效解决机制。通过上述基于区块链的解决机制,首先,互联网租车软件平台无法获取用户的行程路线隐私,从而无法将用户行程路线售卖给其他团体;其次,用户可看到所有的访问者记录,从而增强对自己数据的掌控感;再者,一旦用户决定停止使用该互联网租车软件,可以撤销其数据交互审计平台对自身数据的访问权;最后,假如撤销权限后该互联网租车软件平台遭受黑客入侵使得用户信息泄露,用户可将访问者记录作为证据状告互联网租车软件平台不及时清空用户信息的违规行为。

本文将区块链技术创新性地运用于解决个人隐私保护问题,选取当前流行的互联网租车作为应用场景。首先从流程概貌到实现细节,全面刻画了授予权限、写入数据、读取数据、撤销权限等方面的区块链个人隐私保护应用细节,并对加密算法和方案性能进行了分析。最后通过基于区块链的系统开发证明了该机制的可实现性。由于区块链是一种新兴的技术,目前的应用还主要在实验阶段,因此本文的研究还存在一定的局限性,未来可以尝试通过模拟仿真等方法对该机制进行更进一步的论证,并尝试推广到其他应用场景。

**参考文献**(References)


[1] CLAASSEN R A. An introduction to bitcoin and blockchain technology [EB/OL]. [2017-01-10]. https://zh.scribd.com/document/332585285/Intro-to-Bitcoin-and-Blockchain-Kaye-Scholer-pdf.

[2] PILKINGTON M. Blockchain technology: principles and applications [EB/OL]. [2017-01-10]. https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2662660.

[3] SWAN M. Blockchain thinking: the brain as a decentralized autonomous corporation [commentary] [J]. IEEE Technology & Society Magazine, 2015, 34(4): 41-52.

[4] ZYSKIND G, NATHAN O, PENTLAND A. Decentralizing privacy: using blockchain to protect personal data [C]// Proceedings of the 2015 IEEE Security and Privacy Workshops. Washington, DC: IEEE Computer Society, 2015: 180-184.

[5] KOSBA A, MILLER A, SHI E, et al. Hawk: the blockchain model of cryptography and privacy-preserving smart contracts [C]// Proceedings of the 2016 IEEE Symposium on Security and Privacy. Washington, DC: IEEE Computer Society, 2016: 839-858.

[6] LAZAROVICH A. Invisible ink: blockchain for data privacy [D]. Massachusetts: Massachusetts Institute of Technology, 2015: 36-40.

[7] 刘雅辉, 张铁赢, 靳小龙, 等. 大数据时代的个人隐私保护[J]. 计算机研究与发展, 2015, 52(1): 229-247. (LIU Y H, ZHANG T Y, JIN X L, et al. Personal privacy protection in the era of big data [J]. Journal of Computer Research and Development, 2015, 52(1): 229-247.)

[8] 程絮森, 朱润格, 傅诗轩. 中国情境下互联网约租车发展模式探究[J]. 中国软科学, 2015(10): 36-46. (CHENG X S, ZHU R G, FU S X. A study on the development approach of Internet tailored taxi in Chinese context [J]. China Soft Science, 2015(10): 36-46.)

[9] HERBERT J, LITCHFIELD A. A novel method for decentralised peer-to-peer software license validation using cryptocurrency blockchain technology [EB/OL]. [2017-01-10]. http://pdfs.semanticscholar.org/ff56/173b83c4b6d2b02687f82bd4da56337c97ec.pdf.

[10] KIAYIAS A, PANAGIOTAKOS G. Speed-security tradeoffs in blockchain protocols [EB/OL]. [2017-01-10]. https://eprint.iacr.org/2015/1019.pdf.

[11] FORTE P, ROMANO D, SCHMID G. Beyond bitcoin, part 1: a critical look at blockchain-based systems [EB/OL]. [2017-01-04]. http://eprint.iacr.org/2015/1164.pdf.

[12] SHULTZ B L. Certification of witness: mitigating blockchain fork attacks [D]. New York: Columbia University, 2015: 1-24.

[13] SWAN M. Blockchain: Blueprint for a New Economy [M]. Sebastopol: O'Reilly Media, 2015: 1-67.

[14] WRIGHT A, DE FILIPPI P. Decentralized blockchain technology and the rise of lex cryptographia [EB/OL]. [2017-01-10]. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664.


This work is partially supported by the National Social Science Foundation of China (13AXW010).

**ZHANG Ning**, born in 1975, Ph. D., professor. Her research interests include personal information protection, Internet finance, service outsourcing.

**ZHONG Shan**, born in 1992, M. S. candidate. Her research interests include blockchain, personal information protection.