一种基于智能合约的新型校园外卖体系探索

张三，李四，王五
(电子科技大学，四川 成都)

摘 要：如今外卖业务和物流业务都伴随着电子信息技术的发展而不断提升，两者实质上都是一种资源传递的行为，而本文设计并提出了一个采用EOS底层区块链技术的一种同时支持长途、短途的“人人可送”的智能货物运输平台。这个平台的目的是提高物流等平台的可靠性、数据安全性，同时结合推荐算法为用户、司机提供一种匹配模型，减少订单之间的等待时间，一定程度上避免“空车返回”的现象发生，进而提升资源的传递效率。最后我们提出采用星际文件系统以期避免分布式系统的造成的在节点设备上的存储限制问题。

关键词：物流，区块链，智能合约，星际文件系统，效率

0 引言

随着互联网时代的到来，不论是城市内短途的“跑腿”“外卖”服务还是跨市、跨省的长途运输服务都在迅速发展，而我国在这方面的需求量更是巨大。但同时，在一些高峰期“人找好车难”“车找货难”“空车返回”的现象也数见不鲜，这些都会产生资源闲置和运输费用成倍增加的问题。

为了解决用户与送货者之间的信任问题，从而缓解“人找好车难”的问题，我们决定采用区块链技术。在2016年12月在国务院发布的《国务院关于印发“十三五”国家信息化规划通知》中第一次将区块链作为颠覆性技术、战略性前沿技术列入国家通知中。而区块链技术由于其特有的不易篡改、数据透明的特点，无疑可以很好地作用在物流方向上。以此缓解用户对于运货途中对于货物安全、运输时效的担忧。在这个分布式系统中，每个用户和运输者的终端设备就相当于一个参与节点，在其中共享数据。但是我们难以让每一个用户的设备都存储下链上的每一条数据，这样的成本是巨大的，因而我们打算采用星际文件系统（IPFS）来降低主链的数据存储成本。

而为了提高资源利用率，减少“车找货难”“空车返回”等问题，我们决定设计一个推荐算法，用于匹配运货者（的车）与用户的传运需求。这里，我们希望采用一个——[一种基于车辆推荐的画像数据可用性判断方法]——，不仅可以让用户与运货者之间做出快速且符合要求的相互选择，同时可以在上一次运输的目的地周围寻找以此为起点且以原出发地附近为终点的订单，从而减少“空车返回”现象的发生，减少在能源、时间上产生的无谓损失。

本文将在第一章描述……；第二章……

1 新型平台模式设计与介绍

1.1 区块链技术

目前区块链技术的开源项目如雨后春笋般有十分多的类型，这里比较了5种目前较流行的区块链项目(Bitcoin、Ethereum、Hyperledger、EOS、Corda)进行对比。

由于我们的算法需要建立在智能合约的基础上，并且为了方便交易，我们也需要用到代币功能，且其交易速度应该够快以满足平台的计算和交

表 1: 目前主流区块链项目对比

项目名称	共识算法	去中心化程度	代币功能	智能合约	速度
Bitcoin	PoW	高	有	不支持	慢
Ethereum	PoW/PoS	高	有	支持	较慢
HyperledgerFabric	RAFT/BFT	中	无	支持	快
EOS	DPoS	中	有	支持	快
Corda	Raft/BFT	低	无	支持	快

易需求。同时为了更好地保证平台数据安全性，我们也希望其具有较高的去中心化水平。综合以上需求，采用EOS项目可以很好的实现这个平台。

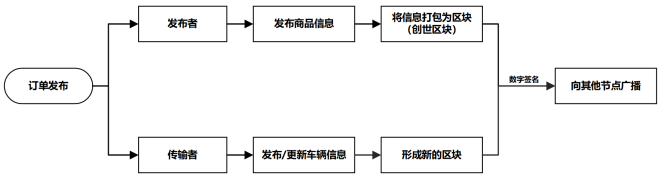

图 1: 订单发布示意图

1.2 功能性需求

我们将每一次订单发布到实现的过程分为3个部分：订单发布与接受部分、运输与信息共享部分、交易与评分模块。下面将分别详细描述这三个部分。

1.2.1 订单发布

订单发布又可以细分为有送货需求的用户发布订单和传输者（司机）发布订单。

有送货需求的用户发布订单需要上传货物信息，包括货物的重量、体积、材质种类、货物价格、起点终点的地址等等。在上传信息之后，系统自动将这笔订单信息打包成一个区块，这个区块便是这个订单的创世区块，同时在用户进行数字签名后对其他节点进行广播，其他节点验证该区块信息正确性后将在自身节点上同步该订单信息。

而传输者同时也可以发布或更改自己的车辆信息，从而在系统推荐算法中找到更适合自己的订单（或者让别人更快的找到自己）。由于链上的信息已经不可修改，所以每一次的信息发布或更改都会产生一个新的区块，而这也将在数字签名后想其他节点进行广播。

在订单发布后，系统后台自动运行车货匹配推荐算法。发布者可以看到根据推荐算法计算出的匹配程度由高到低的可用车主信息[1]。司机可向订单发布者发送接单申请，订单发布者也可以向司机发送接单申请。当另一方同意了接单申请后即进行双方即进行数字签名，将该成交订单向其他节点广播。

1.2.2 运输部分

运输部分建立在订单发布后司机已经接单的前提下，这部分可以对订单部分进行实时更新，包括检查订单状态、检查实时位置等操作。该部分流程如下。

1、司机到订单指定起点位置，将要运输的货物装载。装载完成后，司机对该区块链上的运输信息进行数字签名，广播到其它节点。一旦检测到该过程结束，系统便会会这个订单生成一个用户的查询接口。

2、在运输过程中，定位模块将对货物的位置信息（实质上是司机的终端设备的位置信息）进行实时更新，每一次的位置操作也都将更新到区块中，形成不可更改的货物位置追踪记录。

[1]这里的可用也可能指在马上执行完上一次任务的司机，且上一次任务的终点处于本次任务的起点。

3、当司机将货物送至指定地点时，让收货人进行验收，若验收成功，则对该订单信息进行数字签名，发布并等待其他节点验证。当上述操作完成之后，该订单确认送达，进入转账操作。

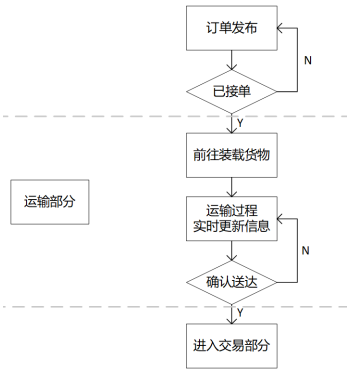

图 2: 运输部分流程示意图

1.2.3 交易部分

当用户确认物品已经安全送达后，系统会向发布用户提交转账申请。

首先系统会判定发布者的对应的地址余额是否充足，当用户同意进行转账操作并且余额充足后，转账操作进行，订单发布者与司机账户对应余额减少或增加相应数量。转账操作结束后两个账户对此次操作进行数字签名并广播到其它节点。

1.3 推荐算法部分

该部分目的在于快速匹配与需要运送货物相符的车辆或为车辆匹配与之对应的货物订单。因此我们决定采用一种在优先满足硬性条件前提下的的基于车辆推荐的画像数据可用性判断方法[引用]结合[引用]中提出的匹配中的四种“软性条件匹配”模型——“路线匹配模型”“意愿衰减模型”“车辆靠近趋势模型”“熟车关系模型”。这些推荐算法与模型将在后文中详细说明。

2 区块链技术在该平台中的应用

如上文所说，基于EOS项目免费试用、轻松调试、低延迟、串并行性能高的特点，我们在该平台中决定使用EOS进行智能合约的部署。该部分详细介绍了该项目在如何区块链上的部署与执行。

2.1 EOS介绍

EOS和ETH的愿景大致相似[引用-白皮书]，都是一个操作系统的底层。其中我们可以构建各种各样的智能合约应用。而EOS通过并行链和DPoS的方式解决了延迟大，和数据吞吐量小的难题。EOS的数据吞吐量理论可以达到百万TPS的数量级。该区块链不需要通过费用来加入与执行合约，大大降低了部署与运行的成本。

2.2 EOS账户

EOS自带基于角色权限管理和账户恢复功能的账户体系，是一种更加灵活的组织和管理账户的方式。EOS.IO软件允许帐户可被长度多达12个字符的唯一可读名称所引用。该名称由帐户的创建者选择。帐户创建者必须保留存储新帐户所需的RAM，直至新帐户存储令牌以保留其自己的RAM。[引用-白皮书]EOS没有采用地址的形式而是采用账户的形式，这是EOS相对于以太坊和比特币的不同之处。每一个账户都为长度为12位[1]，包含了英文字符'a'～'z'以及数字1～5，这样的优点在于将原来没有固定格式的长地址形式转换为人们容易记住的形式。

重新回到考虑如何在我们设计的平台中使用EOS的优势来进行部署的问题。EOS账户中自带两个权限：owner与active[2]。两者实质上都是私钥的形式。Owner权限代表了用户对账户的所有权，可以对账户进行任何修改。而active权限一般用于转移资金、执行智能合约、为DPoS机制中的区块生产者投票等等操作。事实上在EOS系统中

[1]事实上可以存在小于12位的账号，但长度小于12位的账号属于高级账号，系统每天进行只会进行最多一次高级账号的拍卖。如第一个拍卖的账户名"eos"价格高达50000EOS，现在价格已超过百万人民币

[2]还存在一个账户被盗后用于恢复账户的Recovery权限与用户自定义的权限，我们在这里不做考虑

智能合约也有类似的权限，我们在实现该运输平台的合约时便可运用这一特点。具体的说，我们可以在合约权限中设置阈值，每当有新的订单发布或转账操作要进行，我们就让该系统中所有账号进行验证，只有当最后认可该信息的节点数量大于事先设定的阈值时，该信息才最终会被更新到作业链上。通过这样的方式，我们可以确保数据的安全性以及真实性。

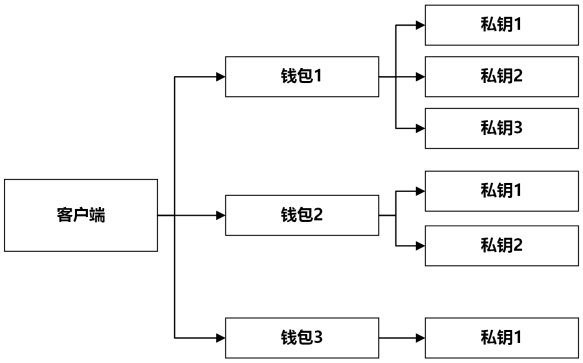

图 3: 钱包-私钥对应关系

2.3 数字签名

在上文提到了其他节点用于验证信息真实性、确定身份、确定责任的方法便是数字签名，几乎全部区块链项目都采用了数字签名这一方法，EOS也不例外。在我们的系统中并不需要我们自己来构建数字签名的加密算法，但其作为几乎作业链中每一个流程都需要用到的东西，我们决定在这里介绍一下EOS中数字签名的过程。

在上一小节中提到了EOS账户，而这一节中我们则介绍与之相对应的“钱包”。在EOS系统中，钱包与账户并不一一对应，相反它们可以存在一对多的关系，即一个钱包中可以管理许多账户，而这里账户的表现形式形式便为私钥。其关系可参照下图3。

而数字签名的工作流程如图4所示[引用]。发送方对原始数据通过哈希计算数字摘要，接着使用非对称加密[1]中的私钥对其进行加密，然后将加密后的数据向其他节点广播。当接收方进行验证时，首先使用发送者公钥对数字签名进行解密，将原始信息的散列值与解密出的散列值对比，只有两者相同时签名验证才算通过。

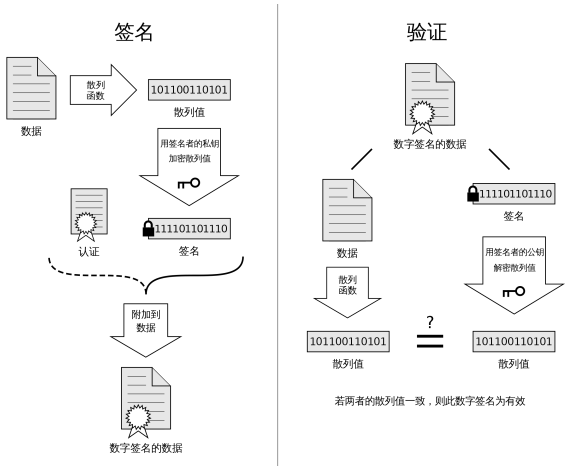

图 4: 签名及签名验证的流程示意图

[1]EOS中采用了椭圆曲线加密方式