计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.200700210

智能合约定义路由目录服务器

王向宇[1]　杨　挺[2]
1 电子科技大学计算机科学与工程学院　成都 611731
2 电子科技大学网络空间安全学院　成都 611731
(909732311@qq.com)

摘　要　路由目录服务器是匿名网络中的重要组成部分,路由目录服务器的中心化特性导致了匿名网络在系统的可扩展性、数据的安全性和网络的弹性等方面受限。为了从根本上改善这些问题,文中构建了去中心化目录服务方案 DCSM(Decentralized Contents Service Model),以智能合约替代中心化的目录服务器,将路由目录服务器应用在区块链上,从而达到路由交易去中心化的目的。为实现路由目录服务器的功能,用 3 个智能合约分别定义了以下规则:用户注册授权、路由信息拍卖、路由信息加解密。实验结果证明,提出的智能合约在功能上能够替代原有的路由目录服务器,完成路由信息的交易过程,并在性能上具有较好的安全性。智能合约的加入将目录服务器的功能在去中心化的区块链上实现,该方案提高了系统的可扩展性、数据的安全性和网络的弹性,有更多人维护的匿名网络也将变得更加有活力。

关键词:匿名网络;路由目录服务器;智能合约;授权认证;拍卖
中图法分类号　TP393

Routing Directory Server Defined by Smart Contract

WANG Xiang-yu[1] and YANG Ting[2]
1 School of Computer Science and Engineering,Electronic Science and Technology of China,Chengdu 611731,China
2 School of Computer Science and Engineering,Electronic Science and Technology of China,Chengdu 611731,China

Abstract　The routing directory server plays an important role in the anonymous network,which is restricted by its centralization. Currently,the main problems are reflected in the scalability of the system,the security of the data,and the flexibility of the network. According to the characteristics of the directory server,the following three functions are implemented by smart contracts:user registration authorization,routing information auction,and the routing information encryption with decryption. Experiments prove that the smart contract proposed in this paper can replace the interconnected routing directory server in function. The smart contract can not only complete the transaction process of routing information,but also perform a good security in performance. The addition of smart contracts implements the function of the directory server on a decentralized blockchain. The solution improves the scalability of the network,data security and network flexibility. In addition,the solution means more energetic.

Keywords　Anonymous network,Routing directory server,Smart contract,Authorized authentication,Auction

1　引言

1.1　路由目录服务器

随着整个社会隐私意识的增强,匿名网络受到了社会各界的高度重视。在匿名访问过程中,路由目录服务器负责对网络中的路由节点进行存储和分配。当用户需要匿名访问 Internet 网络时[1],路由目录服务器提供全球活动中继节点信息,并随机选择节点构建节点网络,用户通过访问节点网络将层层加密的信息发送到 Internet 网络,大致过程如图 1 所示。

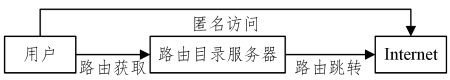

图 1　访问匿名网络

Fig. 1　Access to the anonymous network

随着业务量的增大,路由目录服务器显示出了一些问题。首先,系统可扩展性受限,目录服务器是中心化的服务模式,当前全球所有的数据完整地存储在少数中心目录服务器中[2],数据量的增加对网络访问的速度造成了影响;其次,网络可靠性较低且网络弹性欠佳[3],由于数据较集中,路由目录服务器存在单点故障和资源浪费的问题;最后,安全性存在隐患,路由目录服务器有特定的选择偏好[4],如更大带宽的路由节点,一方面提高了网络访问的速度,另一方面降低了攻击者伪造特定节点的难度。

针对以上问题,研究一套去中心化的路由目录服务器的工作亟待开展。

1.2　智能合约去中心化认证机制

关于去中心化机制的研究已有众多成果,早在 1999 年,Shawn Fanning 设计了用于音乐共享的 Napster 网络,是第一

基金项目:自然科学基金项目:基于电子标签的航空旅客行李全程跟踪技术研究(U2033212)
This work was supported by the NSFC:Research on Airline Passenger Luggage Tracking Technology Based on Electronic Tag(U2033212).
通信作者:杨挺(yting@uestc.edu.cn)

个点对点(P2P)的音乐共享服务。Napster 网络提供一个分布在各个节点间的 MP3 目录,网络中每个用户节点都能成为服务器,用户节点在提供音乐文件的同时,也向其他节点取用。作为 Napster 网络的改进,Kazaa 使用混合架构进行文件索引,性能高的节点被提升为"超级节点",追踪其他用户共享的文献,协助处理搜索请求。2005 年,BitTorrent 取代 Kazaa 成为 P2P 文件共享的顶级协议,用户之间相互连接,进行数据传输。

这一系列 P2P 技术的发展为区块链提供了基础,作为一个分布式的共享账本和数据库,相比上述的去中心化机制,区块链不仅具有去中心化的特性,还具有匿名性、不可篡改性和不可逆等特性[5],而智能合约能够将交易部署在区块链上。参与智能合约的双方或多方接受网络共识的认证,行为一旦确认,就无法被伪造和篡改[6],因此合约双方做出的所有决定公开且不可撤销。

除了 P2P 技术的运用,智能合约对用户身份的认证以及行为的监测,能够保证去中心化的交易在多数节点可信的环境下顺利执行。智能合约实现以来被广泛用于构建去中心化的解决方案[7]。以物联网行业为代表,社会各界纷纷在智能合约的基础上实现去中心化方案,如智能电网交易[8]、分布式的边缘计算框架[9]以及分散式资源交换[10]等。

智能合约为路由目录服务器的重构提供了可操作性。本文以智能合约取代路由目录服务器机制,由智能合约定义路由目录服务器的功能,将匿名网络中的路由交换过程部署在区块链上,从而达到将路由目录服务器去中心化的目的。

1.3 去中心化目录服务方案 DCSM

本文采取去中心化目录服务方案 DCSM 来替代路由目录服务器,通过定义智能合约,用户不再通过路由目录服务器获取路由信息,而是通过智能合约与网络中的其他用户进行路由交易。本文通过增价拍卖的规则来确定路由交易的双方,由路由信息的卖方发起拍卖,以最高竞价者作为路由交易的买方。

路由目录服务器的基本功能由 3 个智能合约共同实现。智能合约 $Contract_R$ 注册授权功能,卖方 Seller 和买方 Buyer 在 $Contract_R$ 中进行注册,分别申请路由信息的加密和解密权限;智能合约 $Contract_{Auct}$ 定义拍卖功能,经过 Buyer 竞价,确定本次路由信息交易的买卖双方;智能合约 $Contract_{EDU}$ 定义加解密功能,Seller 在拍卖开始前,将路由信息用特定加密密钥加密后上传,Buyer 在拍卖成功结束后,下载并使用对应的加密密钥对路由信息进行解密,自行使用解密的路由信息进行匿名访问,具体的访问过程本文不再叙述。

在 DCSM 方案下,匿名网络的访问过程如图 2 所示。

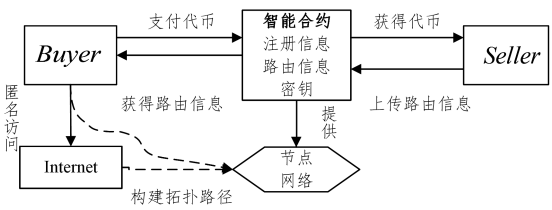

图 2 DCSM 方案下的匿名访问

Fig. 2 Access with DCSM

运用 DCSM 方案后,中心化的路由目录服务器被替换,交易类型由 P2C 转换为 P2P。DCSM 方案能够增加系统的可扩展性、数据的安全性和网络的弹性。

2 相关工作

路由目录服务器存储着大量路由信息,具有中心化的特性[11],在网络攻击中容易成为被攻击的对象。相关的攻击包括蜜罐攻击、空间资源探测和流量确认攻击等[12]。关于防御的研究主要致力于在原方案中添加新的机制,如改进的路由选择算法、流量伪装技术[13]等,少有涉及底层架构的改进。这些研究一定程度上增加了网络的安全性,而服务器过于中心化这一根本问题尚未得到解决,数据的可扩展性和网络的弹性仍有较大进步空间。

具有去中心化特性的区块链是近年来的研究热点。自以太坊平台将智能合约与区块链结合以来,规则和合同能够被编码为程序,部署在区块链上,条件触发后程序即可自动执行[14]。智能合约的加入大大增强了区块链的可移植性,智能合约被应用于信息追溯、物联网数据共享等多个方面[15]。上述研究为本文方案提供了技术基础和实验平台,本文方案的解决思路是将路由目录服务器去中心化。本文将利用智能合约定义路由目录服务器的规则,来实现一个去中心化的路由目录服务器模型。

路由目录服务器在大型路由交易中起着重要的作用,中心化特性带来的数据安全隐患不可忽视。本文以智能合约为工具将路由信息的交易过程构建在区块链上,是具有突破性的尝试,而目前在路由目录服务器研究领域还鲜有类似尝试。

3 具体方案

3.1 智能合约运行机制

以 DCSM 方案替代路由目录服务器后,对应 1.3 节中引入的 3 个智能合约,将用户获取路由信息的过程分为 3 步:以拍卖方式确定路由信息交易对象、交易双方授权认证、路由信息加解密。3 个智能合约之间的交互如图 3 所示。

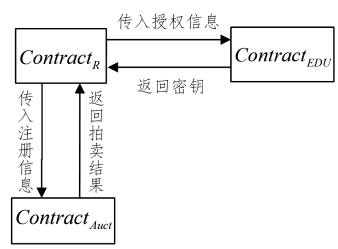

图 3 智能合约交互

Fig. 3 Interaction in smart contracts

在 DCSM 方案的智能合约运行机制中,交易的发起者是路由信息的卖方 Seller,以竞拍方式加入交易的是路由信息的买方 Buyer。

为保证 Buyer 具有支付能力且最大限度上不会违约,Buyer 需要在拍卖阶段支付全额代币,智能合约会在每一轮拍卖后退还竞拍失败者的代币 token。

DCSM 定义的路由信息交易流程如图 4 所示,时间轴上方对应 Seller 在拍卖过程中的行为,下方对应 Buyer 在拍卖中的行为。拍卖的不同阶段,由不同的智能合约定义。

如图 4 所示,路由信息交易的步骤如下:

(1)在交易编号 $ID_{transaction}$ 为 i 的交易中,卖方 $seller_i$ 通过 $Contract_R$ 进行注册并申请加密授权,成功注册后会得到

$Contract_{EDU}$随机分发的加密密钥key_i，$seller_i$使用key_i加密路由信息$Info_i$，并将解密后的路由信息$Info_i'$上传，调用$Contract_{EDU}$发起拍卖；

(2)买方$buyer_j$进行注册，并提前申请解密授权，成功注册后加入竞拍；

(3)在$Contract_{Auct}$规定的拍卖结束时间t后停止竞价，确认竞拍成功的买方$buyer_j$为本次交易的最终买方，并进行解密授权，$buyer_j$使用交易i的解密权限$authority_{i_D}$获得对应的解密密钥key_i'；

(4)$buyer_j$下载$Info_i'$，使用key_i'解密[16]得到$Info_i$，$Info_i$将用于构建匿名网络。

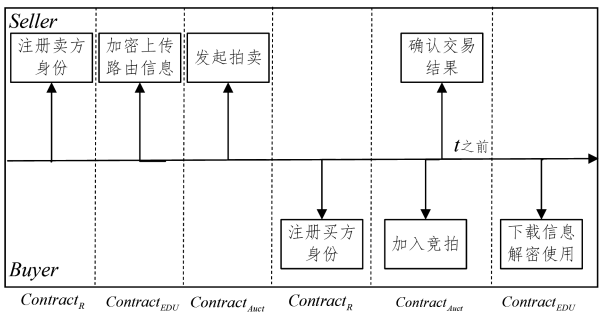

图4 路由信息交易流程图

Fig. 4 Process of transaction

3.2 智能合约原理

3.2.1 $Contract_R$：注册授权

申请开启拍卖的卖方需要注册卖方身份*Seller*，并获得路由信息的加密授权；参加竞拍的买方需要注册买方身份*Buyer*，并在拍卖成功后获得对应路由信息的解密授权。

如表1所列，注册需要提供自己的地址*address*、密码*password*以及所申请的权限*authority*，卖方申请加密权限$authority_E$，买方申请解密权限$authority_D$。由于*address*具有唯一性，因此将*address*作为该用户的唯一识别码，每个用户可以对应多个交易编号$ID_{transaction}$。$Contract_R$的功能主要由表2所列的两种方法来实现。

表1 $Contract_R$：注册授权

Table 1 $Contract_R$: Registration authorization

Feature	register and authorize
Input	$address$、$password$、$authority$
Output	$ID_{transaction}$、$authority_D$/$authority_E$

表2 $Contract_R$包含的方法

Table 2 Functions in $Contract_R$

Founction	Feature
Register	register
Authorize	authorize

设交易编号为i，在拍卖开始前，$seller_i$注册该交易，并获得路由信息的加密权限$authority_{i_E}$。$seller_i$调用$Contract_{EDU}$获得随机分发的加密密钥key_i，把需要拍卖的路由信息$Info_i$加密上传为$Info_i'$；参加交易i的买方注册买方身份为$buyer_j$，其中j为交易i过程中的买方编号。$buyer_j$成功完成$Contract_{Auct}$规定的拍卖流程后，获得$Info_i$的解密权限$authority_{i_D}$。

$authority_{i_D}$用于获取key_i'：

$$key_j=(authority_j==authority_{i\_E})?\ key_i':null$$

key_i'用于获取$Info_i$：

$$Info_j=(Info_i'\ \&\&\ Checked(key_i')==1)Info_i:null$$

买方$buyer_j$通过解密权限$authority_{i_D}$，能够取得路由信息$Info_i$。

3.2.2 $Contract_{Auct}$：拍卖

$seller_i$完成注册授权并上传加密后的路由信息$Info_i'$后发起拍卖，$buyer_j$在$Contract_{Auct}$统一规定的时间t之前参与竞价，由$seller_i$作为发起人制定基本规则。

$seller_i Contract_{Auct}$包含的买卖双方的输入和输出如表3所列。

表3 $Contract_{Auct}$：拍卖

Table 3 $Contract_{Auct}$: Auction

Feature	auction
Seller Input	$quality$、$price_{Initial}$、$rate$
Buyer Input	$token$
Seller Output	$token_{Max}$
Buyer Output	$refund/authority_{i\_D}$

$Contract_{Auct}$的功能主要由表4所列的3种方法来实现。

表4 $Contract_{Auct}$包含的方法

Table 4 Function in $Contract_{Auct}$

Function	Feature
Bid	bidding
Withdraw	refund
AuctionEnd	end the auction

拍卖的具体步骤有：

(1)卖方$seller_i$设定路由质量$quality$、起价$price_{Initial}$、加价率$rate$[17]，其中$quality$由固定公式计算而来，这里不再详述。开启拍卖后，卖家为参与拍卖的买家创建一个开放式最大交易$transaction_{Max}$[18]，买方竞拍的同时，需要将相应数额代币支付至交易区。

(2)$buyer_j$投标，同时支付代币$Token_j$，如果$Token_j$已经存在，则更新$Token_j$。如果$Token_j$大于当前最高价格$Token_{Max}$加上加价，将$Token_{Max}$数额的代币退还至原账户，并更新$Token_{Max}$为$Token_j$，否则直接将$Token_j$退还给$buyer_j$，具体表达式如下：

$$Token_{Max}=Token_j*(1+rate)>Token_{Max}?\ Token_{Max}:Token_j$$

若$Token_j$被接受，本轮$buyer_j$的优先级$level_j$将更新为1，其余买方优先级为0。

(3)严格控制拍卖在时间t之前结束，智能合约中设置互斥锁$lock$[19]，$lock$为真时买方能够竞价：

$$lock=t_{current}<t?\ \text{true}:\text{false}$$

即上个步骤进行前需要保证拍卖的时效性。

(4)拍卖结束后，根据竞拍是否成功来确认$buyer_j$是否获得解密路由信息的权限：

$$authority_j=(level_j==high\ \&\&\ t_{current}>t)?\ authorize_{i\_d}:null$$

权限不足则返回空值。

3.2.3 $Contract_{EDU}$：加解密

在$seller_i$注册的同时，*Contract*3为交易生成密钥对，根据$Contract_R$提供的$ID_{transaction}$记录key_i和key_i'密钥对。

如表5所列，拍卖成功结束后，系统将根据交易$ID_{transaction}$找到对应key_i，$buyer_j$申请key_i'需要满足的条件是：

$authority_j = authority_{i\_D}$

权限有效则返回 key_i' 给 $buyer_j$，用于最终的解密。解密函数如下：

$Info = Dec(key', Info')$

$Contract_{EDU}$ 的功能主要由表 6 所列的两种方法来实现。

表 5 $Contract_{EDU}$：加解密

Table 5 $Contract_{EDU}$: Encryption and decryption

Feature	Encryption and decryption
Seller Input	$address$、$ID_{transaction}$、$authority_{i\_E}$
Buyer Input	$address$、$ID_{transaction}$、$authority_{i\_D}$
Seller Output	key_i
Buyer Output	key_i'

表 6 $Contract_{EDU}$ 包含的方法

Table 6 Function in $Contract_{EDU}$

Function	Feature
Geberatekey	generate pairs of keys
Search	search for keys

每次合约发起，对应一对密钥的生成，密钥存储在数据库中。加解密算法统一采用国产 SM2 方法[20]，密钥对生成的原理是，使用随机数发生器产生 key_i'，key_i' 为整数，且 $key_i' \in [1, n-2]$。

以 G 为基点，计算点 key_i：

$key_i = (x_p, y_p) = [d]G$

生成的密钥对存储在数据库中。

4 实验验证

本文使用 Truffle 4.0、Geth 1.7.2、TestRPC 在私有链上搭建智能合约。实验过程中合约定义了 10 个步骤：

(1)部署合同；

(2)$Seller_1$ 注册后，上传加密后的路由信息，路由信息暂存在数据库中，$Seller_1$ 将起拍价定为 100 英镑；

(3)－(7)一些 *Buyer* 账户出价更改当前最高价格，一些出价成功，一些失败，记录下每个出价的价格和这些出价的结果；

(8)竞标超时的情况下，*lock* 变为 *false*，拍卖结果得到确认，*Buyer* 不能继续出价；

(9)$Seller_1$ 获得 $Token_{\mathrm{Max}}$，$Buyer_3$ 获得解密权限以及经 $Seller_1$ 加密后的路由信息，通过调用 *Contract*3，获得 key_i' 并解密路由信息。

实验结果表明，3 个智能合约各自的运作及交互正常，共同实现了文中设置的路由信息交易的功能。

5 安全性分析

本系统依托于区块链，在多数节点为可信节点的情况下，能够顺利运行。在本系统特定的场景下，针对小部分恶意节点，本系统也对交易中常见的恶意操作做了预防。

5.1 不可抵赖性证明

定理 1 $seller_i$ 不上传路由信息或 $buyer_j$ 不付代币都不符合经济人的社会本能。

证明：在传统的交易设定中，如果没有第三方，互不信任的双方将面临囚徒困境，繁琐的流程商议会成为交易的阻碍[21]。而本文的设置是：$buyer_j$ 在竞拍时直接付款，首先避免了 $buyer_j$ 不付款的问题。同时该设置的前提是，$seller_i$ 在拍卖开始前上传加密后的路由信息。只有在上传加密后的路由信息且成功完成拍卖后，$seller_i$ 才能够获得代币，即 $seller_i$ 的获利条件是：

$Info' \&\& endAction == 1$

在这个设置中，$buyer_j$ 拍得的是解密权限，拍卖结束后不需要等待卖家发送 $Info_i$，只需要从 $Contract_{EDU}$ 获取 key_i'，即可解密卖家拍卖前已上传的 $Info_i'$：

$Info_j = (Info_i' \&\& Checked(key_i') == 1)\, Info_i : null$

因此，为了获利，$seller_i$ 不上传路由信息或 $buyer_j$ 不付代币的情况都不会出现。

5.2 交易有效性证明

定理 2 $seller_i$ 无法挪用代币或拖延时间。

证明：在本系统的设置中，$seller_i$ 不断获得代币又自动退回，虽然该过程能够保证买方的代币可退回，但是如果 $seller_i$ 迟迟拖延，恶意拖延拍卖结束的时间，则 $seller_i$ 能不断使用买方的代币，而 $buyer_j$ 迟迟得不到需要的路由信息[22]。

针对该攻击，本系统有两个应对措施：

首先，在交易过程中，限定 $seller_i$ 账户的代币先出后进，即先返还上一个买方 $buyer_k$ 的代币，后接收当前买方的代币。如果 $seller_i$ 账户余额不足以返还 $buyer_k$ 的代币，就直接终止拍卖，把解密权限 $authority_{i\_D}$ 授予 $Buyer_k$：

$authorize_k = authority_{i\_D}$

其次，设定拍卖时间上限 t，使用 *lock*：

$lock = t_{current} < t$ true:false

一旦 *lock* 为 false 则终止拍卖，把解密权限授予 *level* 为 1 的买家。

因此，$seller_i$ 挪用代币等行为会给自己造成损失，这个时间机制保证了交易的有效性。

结束语 在数据量不断增长的今天，由于路由目录服务器的中心化，系统的可扩展性受限、网络可靠性较低、网络弹性欠佳、目录服务器本身的选择偏好使得攻击者更容易伪造信息。采用 DCSM 后，智能合约替代路由目录服务器，服务器增加去中心化特性，上述问题迎刃而解，网络将变得更加安全和活跃。实验结果证明，本文提出的智能合约基本功能完备，功能上能够替代原有的路由目录服务器，并且对该交易场景下常见的攻击做出了预防，具有较好的安全性。

本文方案目前仍存在不足之处，由于缺少前端界面，方案的可操作性有待改善。在后续研究中将增加前端构建，添加更详细的使用规则，致力于构建更加完善和健全的网络匿名访问方案。

参 考 文 献

[1] HE D, ZEADALLY S, KUMAR N, et al. Anonymous Authentication for Wireless Body Area Networks With Provable Security [J]. IEEE Systems Journal, 2017, 11(4): 2590-2601.

[2] CATALANO D, FIORE D, GENNARO R. A certificateless approach to onion routing[J]. International Journal of Information Security, 2017, 16(3): 327-343.

[3] LIU X, WANG N. An overview of anonymous communication [J]. Computer Applications, 2010, 30(3): 719-722.

[4] TAN Q, GAO Y, SHI J, et al. Toward a Comprehensive Insight Into the Eclipse Attacks of Tor Hidden Services[J]. IEEE Internet of Things Journal, 2019, 6(2): 1584-1593.

[5] CHRISTIDIS K, DEVETSIKIOTIS M. Blockchains and Smart Contracts for the Internet of Things[J]. IEEE Access, 2016, 4: 2292-2303.

[6] HAMOUID K, ADI K. Secure and reliable certification management scheme for large-scale MANETs based on a distributed anonymous authority[J]. Peer-to-Peer Networking and Applications, 2019, 12(5): 1137-1155.

[7] HAGHIGHI M S, AZIMINEJAD Z. Highly Anonymous Mobility-Tolerant Location-Based Onion Routing for VANETs[J]. IEEE Internet of Things Journal, 2020, 7(4): 2582-2590.

[8] TSAI J L, LO N W. Secure Anonymous Key Distribution Scheme for Smart Grid[J]. IEEE Transactions on Smart Grid, 2016, 7(2): 906-914.

[9] RAHMAN M A, HOSSAIN M S, LOUKAS G, et al. Blockchain-based Mobile Edge Computing Framework for Secure Therapy Applications[J]. IEEE Access, 2018(99): 1-1.

[10] ZHUMABEKULY AITZHAN N, SVETINOVIC D. Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams[J]. IEEE Transactions on Dependable and Secure Computing, 2018, 15(5): 840-852.

[11] WAN S. Topology hiding routing based on learning with errors [J]. Concurrency and Computation: Practice and Experience, 2020, e5740.

[12] SAKAI K, SUN M T, KU W S, et al. On Anonymous Routing in Delay Tolerant Networks[J]. IEEE Transactions on Mobile Computing, 2019, 18(12): 2926-2940.

[13] ZHAO K, XING Y H. Overview of research on security of the Internet of Things driven by blockchain technology [J]. Information Network Security, 2017(5): 1-6.

[14] KANG J, YU R, HUANG X, et al. Enabling Localized Peer-to-Peer Electricity Trading Among Plug-in Hybrid Electric Vehicles Using Consortium Blockchains[J]. IEEE Transactions on Industrial Informatics, 2017(6): 1-1.

[15] LEI A, CRUICKSHANK H, CAO Y, et al. Blockchain-Based Dynamic Key Management for Heterogeneous Intelligent Transportation Systems[J]. IEEE Internet of Things Journal, 2017 (99): 1-1.

[16] MAXWELL G, POELSTRA A, SEURIN Y, et al. Simple Schnorr multi-signatures with applications to Bitcoin[J]. Designs, Codes and Cryptography, 2019, 87(9).

[17] ZOU B. Summary of Auction Theory[J]. Science Consulting (Technology · Management), 2013(11): 19-20.

[18] LEI A, CRUICKSHANK H, CAO Y, et al. Blockchain-Based Dynamic Key Management for Heterogeneous Intelligent Transportation Systems[J]. IEEE Internet of Things Journal, 2017 (99): 1-1.

[19] MESHRAM C, LEE C C, LI C T, et al. A secure key authentication scheme for cryptosystems based on GDLP and IFP[J]. Soft Computing, 2016, 21(24): 7285-7291.

[20] CHEN Z, QI F, YE C Y. Research on a cloud data encryption scheme based on national secret algorithm[J]. Information Security Research, 2018, 4(7): 646-651.

[21] HE D, ZEADALLY S, KUMAR N, et al. Efficient and Anonymous Mobile User Authentication Protocol Using Self-Certified Public Key Cryptography for Multi-Server Architectures[J]. IEEE Transactions on Information Forensics & Security, 2016, 11(9): 2052-2064.

[22] YAGHMAEE M H, BARABADI B, ALISHAHI S, et al. Incentive cloud-based demand response program using game theory in smart grid[C]// Electrical Power Distribution Networks Conference. IEEE, 2016.

WANG Xiang-yu, born in 1996, postgraduate, is a member of China Computer Federation. Her main research interests include blockchain and cryptography.

YANG Ting, born in 1975, associate professor. His main research interests include blockchain and cyber security.