计算机应用研究
Application Research of Computers
ISSN 1001-3695,CN 51-1196/TP

《计算机应用研究》网络首发论文

题目：基于区块链的共享充电桩安全监管方案
作者：刘会霞，李玲玲
DOI：10.19734/j.issn.1001-3695.2021.10.0425
收稿日期：2021-10-08
网络首发日期：2021-12-20
引用格式：刘会霞，李玲玲．基于区块链的共享充电桩安全监管方案[J/OL]．计算机应用研究. https://doi.org/10.19734/j.issn.1001-3695.2021.10.0425

网络首发时间：2021-12-20 11:18:45
网络首发地址：https://kns.cnki.net/kcms/detail/51.1196.TP.20211216.2049.006.html

基于区块链的共享充电桩安全监管方案

刘会霞，李玲玲

(河南警察学院，郑州 450046)

摘 要：共享充电桩可缓解当前电车充电难的现状。然而，基于第三方平台的共享充电桩平台面临着信任问题；而基于区块链的共享充电桩平台虽可提供信任环境，但缺乏对用户、桩主、充电量等信息核查。为解决以上问题，提出了一种基于区块链的共享充电桩安全监管方案。该方案通过基于双链的共享充电信任模型，安全地存储用户、桩主或运营商的关键信息；并在该模型上设计穿透式监管方案，向上核查用户、桩主或运营商的身份，向下核查充电量、充电速度等信息正确性。实验评估表明，本方案能够以不大的开销提高平台的安全性。

关键词：区块链；智能合约；共享充电；穿透式监管；层次分析法

中图分类号：TP393 doi: 10.19734/j.issn.1001-3695.2021.10.0425

Security supervision scheme of shared charging pile based on blockchain

Liu Huixia, Li Lingling

(*Henan Police College*, *Zhengzhou Henan* 450046, *China*)

Abstract: Sharing charging piles can alleviate the current situation of difficult charging of electric vehicles. However, the shared charging pile platforms based on the third-party platform face the problem of trust; although shared charging pile platforms based on the blockchain can provide a trust environment, these platforms lack verification of users, pile owners, charging capacity and other information. In order to solve the above problems, a security supervision scheme of shared charging pile based on blockchain is proposed. The scheme can securely store the key information of users, pile owners or operators through the shared charging trust model based on double chain; a penetrating supervision scheme is designed on the model to check the identity of users, pile owners or operators upward and the correctness of information such as charging capacity and charging speed downward. Experimental evaluation shows that this scheme can improve the security of the platform with a small overhead.

Key words: blockchain; smart contract; shared charging; penetrating supervision; analytic hierarchy process

0 引言

随着人口增加和空气污染日益严重，电动汽车作为出行工具被认为是减少车辆交通对环境污染的战略选择。中共中央《“十四五”规划建议》中也提出了统筹推进基础设施建设和加快推动绿色低碳发展的建议，表明了国家对发展相关产业的大力支持。2020 年，中央明确提出将充电桩作为国家“新基建”七大领域之一，预计政府将投资 100 亿元左右建设充电桩。据国际能源署测算，2030 年全球私人充电桩保有量预计达到 12800-24500 万台；全球公共充电桩保有量预计达1000-2000 万台[2]。

电动汽车在高速发展的同时，充电难的现象也层出不穷[1]。按照公安部统计数据，截至 2019 年底，目前桩车比约为 1：3，充电桩的缺口仍旧很大。电动汽车用户存在找桩难的问题，用户 APP 无法获得充电桩的动态信息，难以搜索到分属各个企业或多个充电运营商的充电桩，不同运营商有不同的 APP，行业内没有实现信息的互联互通；私人充电桩难以“落户”，必须征得物业的同意，即使安装私人充电桩，也存在充电车位被燃油车长时间占用的情况。私人充电桩闲置率很高，一般白天充电桩和车位均属于闲置状态。

综上来看，如何有效提高充电桩的使用效率，是面临的一个重要问题。共享充电桩提升充电桩利用率，可缓解当前电车充电难的现状。然而，现有第三方平台实现信息共享或计价时，面临着充电桩运营商或用户对第三方平台的信任问题，例如第三方平台计价不透明，收取高比例的交易佣金，或被攻击造成充电运营商和用户的利益损失等问题[3]。

区块链作为一个分布式可信账本，涉及不同利益体之间的交互，适合于解决不同利益体之间的信任问题，或者作为一个第三方可信平台用来解决用户对平台的信任问题[4~6]。目前，区块链主要用于解决公平计价[7~9]、电车认证[10~12]问题，较少考虑使用区块链构建私桩桩主、公共充电桩、各充电运营商、电车用户等多方共建的信息共享方案。即使采用区块链提供多方信任的共享充电环境，但现有区块链的交易方案大多只能核查交易记录，缺乏对用户、桩主等信息核查，以及对充电量、充电速度等交易详情核查，而导致当前的充电体系安全性不高，给充电用户带来利益方面的损失[13]。

针对以上问题，本文提出了一种基于区块链的共享充电桩安全监管方案。该监管方案通过基于双链的共享充电模型，安全地存储用户、桩主或运营商的关键信息，通过认证合约构建交易双方的信任关系；并在该共享充电模型上设计穿透式监管方案，向上核查用户、充电桩、桩主或运营商的身份，向下核查充电交易中充电量、充电速度和价格详情信息正确性。本文的贡献如下：

1)提出一种基于区块链的共享充电桩安全监管方案，能够安全地存储用户、桩主或运营商的关键信息，并实现充电交易向上和向下的穿透式监管；

2)提出一种基于模糊层次分析法的共享充电平台安全性评估方法，能够实现平台安全性的量化分析；

收稿日期：2021-10-08；**修回日期：**2021-12-06

作者简介：刘会霞，女，副教授，硕士研究生，主要研究方向为物联网安全、区块链(liu_huixia668@163.com)；李玲玲，女，副教授，硕士研究生，主要研究方向为物联网安全、区块链.

3)通过实验验证，本文的监管方案能够以不大的开销下提高共享充电桩平台的安全性。

1　相关工作

区块链技术应用到电车充电已经成为热点，主要集中在充电定价、电车认证方面。在充电定价方面，Schwieters 等人[7]提出利用区块链技术实现公用充电桩计费的透明化和信任化。Pustišek 等人[8]针对多充电服务提供商问题，提出了根据电车到充电站距离和充电价格来自动选择充电站，同时保证可信性和隐私性。Kang 等人[9]使用联盟链设计了电动汽车之间的充放电交易，采用迭代双拍卖机制确定电动汽车的电价和交易电量，设立了本地聚合器来充当服务节点。

另一些研究人员开展了电车认证的研究。Huang 等人[10]提出基于区块链技术的电动车和充电桩安全管理模型，利用区块链生态中的闪电网络和智能合约构建安全模型，该安全模型与现有的调度机制来增强认证和交易过程的安全性。Jeong 等人[11]提出了一种基于区块链的电动汽车认证计费系统，通过使用区块链智能合约防止当前不信任的基于硬件的计费仪表出现问题。Su 等人[12]提出了一种基于智能合约的能源区块链，通过执行智能合约设置电动汽车用户与分布式能源运营商进行交易，并实现电动汽车的安全充电服务。

区块链监管的研究也逐渐受到关注。Sun 等人[14]提出了一种针对数字货币的区块链模型，通过设计链内、跨链等多种协议来实现对交易过程的监管；Pan 等人[15]提出在区块链中建立多人通道，并引入监管节点处理通道内的交易，通过缴纳保证金及惩罚机制来实现交易的监管；葛钟慧等人[16]将多人通道交易扩展至跨通道交易，有效降低了网络时延，实现了监管下安全的链下支付。以上研究大多考虑交易的监管，没有对参与方、交易物品或服务的监管，也没有针对电车充电的监管方案。

关于平台安全性评估也有一些的研究工作。李伟明等人[17]对网络中的威胁、攻击进行实时动态的评估分析，通过使用隐马尔可夫模型阐述了系统的可靠性、可生存性和安全性；Dreyling 等人[18]针对电子服务领域的风险，通过建立信息风险因素评估模型，来实施了安全性评估；雷柯楠等人[19]建立了全面的评估系统，运用层次分析法实现了漏洞类型的分析量化。虽然以上工作可以对平台进行定性定量的分析，但缺少适用于区块链平台安全性的评估方案。

本文与以上工作不同，本文给出了基于区块链的平台的穿透式监管方案，并能够对平台的安全性进行量化评估。

2　基于区块链的共享充电模型

针对当前情况下汽车共享充电体系中存在的一些问题，如私有充电桩资源浪费严重、运营商与充电桩桩主无序竞争等一系列问题。本文提出了一套基于双链的共享充电模型，联盟链作为整个模型的核心，加密存储充电过程中产生的信息并部署认证合约、监管合约等一系列智能合约；公有链作为模型的底层，链上保存联盟链数据的信息摘要，对涉及到的信息作进一步存储。监管过程主要针对联盟链。

2.1　模型设计

区块链按照参与节点数量及结构可分为公有链、私有链和联盟链三种。其中，私有链完全私有，只适用于特定的群体内部进行交易，与面向大众的共享充电体系相差较大。公有链则完全公开，虽然其匿名性在一定程度上可以保护用户隐私等问题，但针对公有链进行监管却十分困难。因此，联盟链与共享充电体系的相容性最好。

设计双链结构，联盟链中加密存储完整的用户和桩主信息、充电交易记录、服务质量评价信息、充电请求和竞价承诺等信息。联盟链用户为有限的第三方用户，实现了交易的私密性。链上保存的数据经加密后实现了保密性，同时也为追溯环节提供了可能性。联盟链内部节点间的通信使用加密信道，防止通信明文传输完整交易时造成信息的泄露。为了充分发挥区块链去中心化的优势，同时弥补联盟链可信性不足的问题，特引入公有链，建立联盟链-公有链的双链体系。

将联盟链区块摘要存储在公有链中，作为公开可信的验证交易的凭据，扩大了共享充电体系参与程度，也增加了交易的见证群体，保证了联盟链中数据的可信性。另外，联盟链将数据摘要存储在公有链中，还能防止联盟链成员串通对消息进行窜改。这里充分利用了公有链在结构方面的优点，方便了系统的扩展，促使多方参与到共享充电体系的维护中。

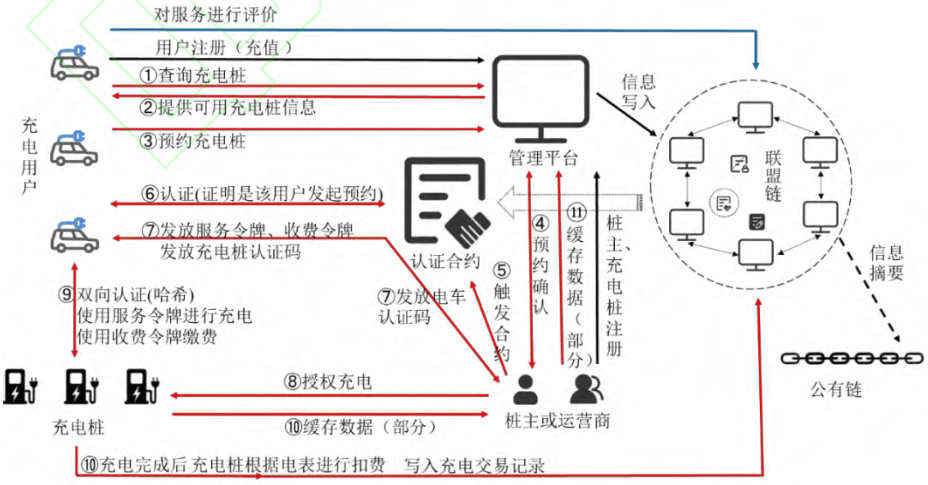

图 1　共享充电模型

Fig. 1　Shared charging model

如模型图 1 所示，在此汽车共享充电体系开始时，用户和桩主要先在管理平台上进行注册。同时用户可以选择进行充值操作，桩主注册时要同时将充电桩信息一并登记。管理平台再将这些信息整理后写入联盟链中。

充电流程如下：首先用户向共享充电平台发出查询充电桩的请求，平台接收到该请求后与自身缓存的充电桩信息进行对比，为用户提供可用的充电桩信息。用户从这些信息中筛选出最优的充电桩，向管理平台发起预约，以保证充电桩独占。平台与桩主通信，实现预约确认。桩主触发认证合约，合约运行，同时给桩主发放电车认证码，给充电用户发放充电桩认证码和服务令牌、收费令牌。桩主将电车认证码发送给充电桩授权充电。充电桩通过电车用户提供的充电桩认证

码来确认充电用户即充电交易发起者、预约者；同理，充电用户也通过充电桩反馈的电车认证码来确定该充电桩即为预约的充电桩。二者进行双向的哈希认证后，正式开始充电过程。充电结束后，充电桩根据自身电表进行扣费，同时将自身部分缓存数据(电量记录)发回给桩主，将此次充电交易记录写入联盟链。桩主确认信息无误后将信息发回给管理平台留作备用。

评价流程如下：充电用户在结束充电后，可以将此次充电的评价信息发布至联盟链。最后，联盟链定期将数据摘要写入公有链中。

2.2　存在的问题

本文提出的共享充电体系可以有效避免私桩浪费、无序竞争等一系列问题。同时，仍存在着一些问题是充电体系本身无法解决的，如：冒充充电用户进行充电、伪造虚假充电记录、系统显示充电量虚高、不同用户间差别化定价等。这些问题可以通过有效的监管来避免或解决。

3　穿透式监管方案

区块链因其匿名性、低成本的特性得到了飞速的发展，但任何科学技术都是双刃剑，缺乏必要的监管必然导致难以想象的后果。这就要求监管机构不断探索新的监管方案对现有的区块链体系进行监管。

穿透式监管这一方法源自金融领域，最初指证监机构对项目资产管理的一种方法，包括对资产和资金两方面的监管。将此方法引入到对区块链的监管之中，是因为两者之间存在着相似之处。两者都有实体，即为向上穿透监管的对象；同时，区块链上数据与金融资金都是海量冗杂的。如果缺少必要的监管，将会产生难以想象的后果。

本文以架设在区块链双链结构上的一个汽车共享充电体系为例，提出了一种监管区块链交易的解决方案：使用穿透式监管对汽车共享充电的参与各方和具体的交易数据进行有效监管。穿透式监管分为向上穿透核查和向下穿透核查两部分，这两部分分别对整个共享充电体系的实体和数据内容进行监管，以达到监管效果的完整性和全面性。下面分别介绍这两部分。

3.1　向上穿透核查交易参与者

如图 2 所示，由监管机构触发监管合约，主要目的是核查参与共享充电各方的信息情况。针对充电用户，对比用户注册时管理平台写入联盟链的信息和充电交易记录中对应的用户信息，以核实确保用户信息真实性。针对私桩桩主或运营商，对比注册时管理平台写入联盟链的信息和充电交易记录中对应的身份信息，以核实确保私桩桩主或运营商信息的真实性。针对充电桩，同样将管理平台写入的信息与链上具体记录中的编号进行对比，以确定该次充电交易是否真实发生。

编写向上穿透式监管合约，用来实现向上穿透式监管中对充电用户、桩主或运营商以及充电桩的核查，包括信息的对比，其伪代码如算法 1 所示。算法 1 中的第 1~3 行描述了监管合约调用区块链平台接口，第 4~10 行描述了读取链上的用户身份信息进行核查的过程；第 11~17 行描述了读取链上的桩主身份信息进行核查的过程；第 18~24 行描述了读取链上的充电桩信息进行核查的过程。

Algorithm 1 SupervisionInformation

Input: Register user id *register_uid*; Register user id *register_oid*; Register point id *register_pid*; Record charging num *num*; Get chain *CHARGE*;

Output: Return the result of upward supervision *result*

```
1: chain ← ChainFactory.openChain(CHARGE)
2: entry ← Chain.EQ(num)
3: num ← entry.getString(num)
4: record_uid ← num.getUid(uid)
5: if register_uid == record_uid then
6:     user information is correct
7: else
8:     user information is wrong
9:     return
10: end if
11: record_oid ← num.getOid(oid)
12: if register_oid == record_oid then
13:     owner information is correct
14: else
15:     owner information is wrong
16:     return
17: end if
18: record_pid ← num.getPid(pid)
19: if register_pid == record_pid then
20:     point information is correct
21: else
22:     point information is wrong
23:     return
24: end if
```

3.2　向下穿透核查交易数据

如图 3 所示，向下穿透，主要为了监管充电交易过程中发生的具体数据信息，包括充电量、充电速度以及充电价格等。本方案采用对比与计算相结合的方法，针对充电量，合约通过对比充电交易记录中记录的充电量与实际发生的充电量进行对比，以监管确保充电量信息真实可靠。针对充电速度，合约通过审查充电交易记录中的充电量数据和充电时长，经过简单计算可以得出充电速度大小，将此速度与管理平台中记录的标准充电速度相比，得出最后的核查结果。针对充电价格，合约主要审查两方面内容，第一是该充电桩定价是否过高，高于市场平均价格。第二则是差别化定价问题，能够在一定程度上保证充电价格稳定。要核查充电价格，合约需要核查充电交易记录中的充电量数据和用户所缴费用，简单计算后可得出充电价格。与管理平台上记录的标准充电价格对比，即可判定该充电桩是否定价过高。多条充电交易记录中的信息之间互相对比，则可以得出是否差别化定价。

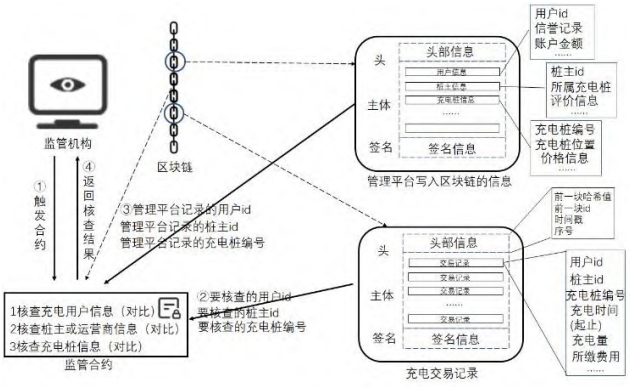

图 2　向上穿透监管

Fig. 2　Upward penetration regulation

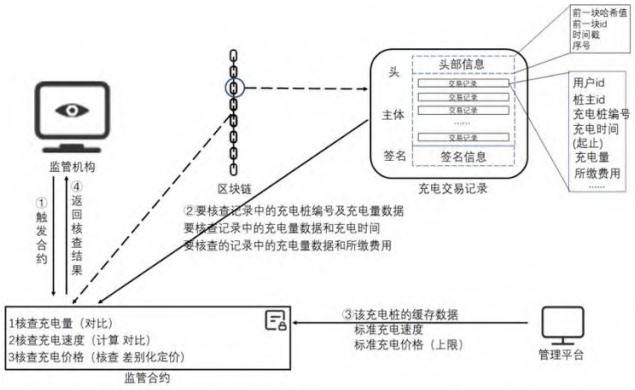

图 3　向下穿透监管

Fig. 3　Downward penetration regulation

编写向下穿透式监管合约，用来实现向下穿透式监管中对充电量、充电速度以及充电价格的核查，包括数据的简单计算与对比，其伪代码如算法 2 所示。算法 2 中的第 1~3 行描述了监管合约调用区块链平台接口，第 4~14 行描述了读取交易记录中的充电量信息进行核查的过程；第 15~22 行描述了读取充电时长计算出充电速度、再核查充电速度的正确性的过程；第 23~33 行描述了读取交易金额信息计算出单位时间的充电价格、再核查充电价格是否高于标准价格的过程。

Algorithm 2 SupervisionCharging

Input: Record charging num *num*; Register point id *register_pid*; Register charging capacity *register_capacity*; Register charging speed *register_speed*; Register charging price *register_price*; Get chain *CHARGE*;

Output: Return the result of downward supervision *result*

```
1: chain ← ChainFactory.openChain(CHARGE)
2: entry ← Chain.EQ(num)
3: num ← entry.getString(num)
4: record_pid ← num.getPid(pid)
5: record_capacity ← num.getCapacity(capacity)
6: if register_pid == record_pid then
7:     if register_capacity == record_capacity then
8:         capacity is correct
9:     else
10:        capacity is wrong
11:        return
12:    end if
13:    return
14: end if
15: record_time ← num.getTime(time)
16: if register_pid == record_pid then
17:    if register_speed > (record_capacity ÷ record_time)
   then
18:        charging speed is lower than standard
19:        return
20:    end if
21:    return
22: end if
23: record_cost ← num.getCost(cost)
24: if register_pid == record_pid then
25:    if register_price < (record_capacity÷record_time) then
26:        charging price is more expensive than standard
27:        return
28:    end if
29:    return
30: end if
31: if the price of different user is obvious different then differ-
   entiated pricing exists
32:    return
33: end if
```

3.3　追溯环节

除了对区块链进行实时的监管，增加对区块链的追溯环节也是监管的一种有效方法。

追溯发起时，由联盟链参与者发起对某项交易的追溯请求，全体成员投票决定是否执行。同意发起追溯的节点将保存的秘密共享信息发送给联盟链中的监管节点，根据提供的的交易编号，查找联盟链中相匹配的交易，对交易进行追溯，得到交易者的身份．同时，当完成对一次完整交易的追溯，就会得到与其相关的完整交易记录，因此可以通过逐步递进完成对所有交易信息的揭示．交易追溯结束后，监管节点会诚实的完成对相关信息的删除．交易追溯的结果并不直接作用到区块链系统中，不会发生系统内对系统状态的修改，如果要撤销交易或者封禁账户均由系统外的监管机构完成。

3.4　监管评价

穿透式监管对共享充电体系的监管是方方面面的，很难从单独一个方面来描述整个监管方案的好坏，因此本方案采用模糊层次分析法(AHP 法)对监管效果进行简单评价。层次分析法是将问题的各种要素依次分类成目标、准则、方案几个层次，在此基础之上进行定性和定量的分析方法。完美契合穿透式监管方案多角度、多方面的特点。

对评价对象采用 1-9 标注法，依次建立一级、二级评价矩阵。判断矩阵标度定义如表 1 所示。

表 1　判断矩阵的标度定义

Tab. 1　Scale definition of judgment matrix

标度	含义
1	表示两个因素相比，具有相同重要性
3	表示两个因素相比，前者比后者稍重要
5	表示两个因素相比，前者比后者明显重要
7	表示两个因素相比，前者比后者强烈重要
9	表示两个因素相比，前者比后者极端重要
2，4，6，8	表示上述相邻判断矩阵的中间值
倒数	若因素 i 与因素 j 的重要性之比为 a_{ij}，那么因素 j 与因素 i 的重要性之比为 $a_{ji}=1/a_{ij}$

本次评估监管结果时采用特征向量法计算权重。计算方法如下：

$$AW=\lambda_{\max}W \tag{1}$$

其中，W 为权重，A 为判断矩阵，$\lambda_{\max}$ 为对应判断矩阵的最大特征值，存在且唯一。

根据计算得出的权重与专家评估得出的结果计算一级指标主因素评价矩阵 R，然后根据公式 $B=A^2\cdot R$ 计算可以得到最终结果 B，即为评价结果。

4　实验评估

4.1　测量智能合约 gas 消耗情况

设计实验分别测量穿透式监管合约向上核查和向下核查时在区块链中的表现情况如何。同时测量其他合约的 gas 值消耗情况。

实验使用 FISCO BCOS 联盟链作为区块链底层，系统环境为 CentOS7。编译器为 WeBASE IDE。语言为 Solidity ^0.4.24(0.4.24 向上兼容至 0.5 版本以下)。在区块链存储了电车用户、桩主、充电桩信息和交易信息，然后根据算法 1 和算法 2 描述在 Solidity 语言上进行编写、部署和执行合约。图 4 是对向上穿透监管合约部署上链消耗的 gas 值的测量；图 5 是对向下穿透监管合约部署上链消耗的 gas 值的测量；图 6 是对用户信息、充电桩信息和桩主信息上链和充电交易打包上链的 gas 值开销。

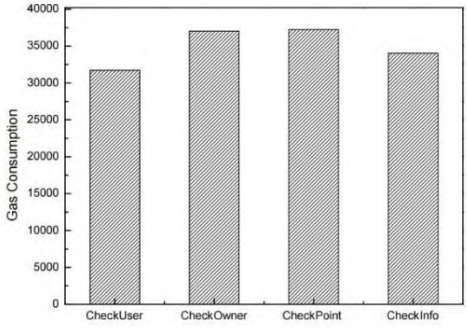

图 4　向上穿透监管合约部署上链需要消耗的 gas 值

Fig. 4　Gas consumption of upward penetration regulatory contracts

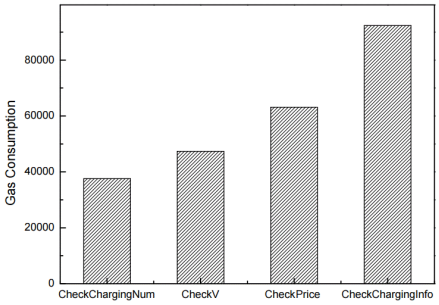

图 5　向下穿透监管合约部署上链需要消耗的 gas 值

Fig. 5　Gas consumption of downward penetration regulatory contracts

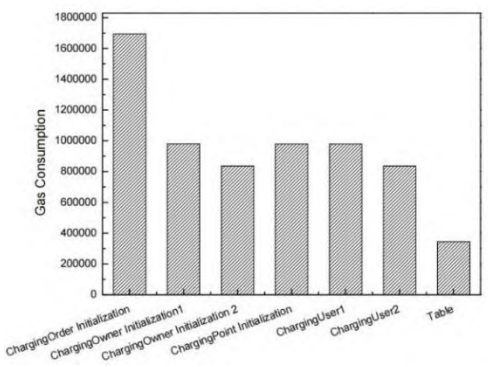

图 6　其他合约部署上链需要消耗的 gas 值

Fig. 6　Gas consumption of the other regulatory contracts

简单分析实验结果，可以得出结论：1)从图 4 中可以看出，核查用户、桩主或运营商、充电桩的 gas 消耗值相近，说明了三者的核查难度相近。2)从图 5 中可以看出，核查充电量、充电速度、充电价格的 gas 消耗值依次递增，说明 gas 消耗值与监管难度是成正比的；3)对比图 4 和图 5，穿透式监管中向上核查过程之中的 gas 消耗值要远远小于向下核查的 gas 消耗值，说明对充电交易参与者的监管难度要小于对交易的数据监管；4)从以上三张图的 gas 消耗值中，可以得出本方案的 gas 开销在可以接受的范围内，满足应用需求。

4.2　层次分析法评价安全性

在本次评估中，层次分析法将与汽车共享充电有关的各种要素分类成目标、准则、方案几个层次，在此基础之上进行定性和定量的分析方法。分类如表 2 所示。

表 2　汽车共享充电指标

Tab. 2　Index of car sharing charging

目标层	准则层	指标层
汽车共享充电	交易操作参与者	充电电车用户信息认证
		桩主或运营商信息认证
		充电桩信息认证
	交易数据	充电量数据
		充电速度
		充电价格
	智能合约与共识协议	认证合约执行情况
		监管合约执行情况
		共识协议漏洞
	隐私保护	电车用户隐私
		桩主隐私

为了对迁移结果进行一定程度上的评价，根据 AHP 理论，采用 1-9 标注法。构建出一级指标判断矩阵 A，如下：

$$A=\begin{bmatrix}1 & 5 & 3 & 4\\ 1/5 & 1 & 2 & 3\\ 1/3 & 1/2 & 1 & 5\\ 1/4 & 1/3 & 1/5 & 1\end{bmatrix} \tag{2}$$

同时，构建出 4 个二级判断矩阵 A_1,A_2,A_3,A_4 如下：

$$A_1=\begin{bmatrix}1 & 1/5 & 1/3\\ 5 & 1 & 1/7\\ 3 & 7 & 1\end{bmatrix} \tag{3}$$

$$A_2=\begin{bmatrix}1 & 1/7 & 1\\ 7 & 1 & 6\\ 1 & 1/6 & 1\end{bmatrix} \tag{4}$$

$$A_3=\begin{bmatrix}1 & 7 & 8\\ 1/7 & 1 & 1/3\\ 1/8 & 3 & 1\end{bmatrix} \tag{5}$$

$$A_4=\begin{bmatrix}1 & 1/3\\ 3 & 1\end{bmatrix} \tag{6}$$

可以得到每个矩阵的最大特征值对应的特征向量。该向量中每一分量的 2 次幂都代表相应元素的权重。因此，每一元素的相对重要性即可求得，以此来判断其影响程度。根据 3.4 节中的计算公式，可以得到这几个矩阵的计算结果，如表 3 所示。

表 3　矩阵计算结果

Tab. 3　Matrix calculation results

矩阵	最大特征值	对应特征向量的平方
A	4.408	0.886^2, 0.331^2, 0.303^2, 0.115^2
A_1	3.702	0.138^2, 0.305^2, 0.942^2
A_2	3.004	0.147^2, 0.977^2, 0.155^2
A_3	3.17	0.978^2, 0.093^2, 0.184^2
A_4	2	0.351^2, 0.936^2

从表 3 中可以看出，在该共享充电体系中，交易操作参与者、交易数据、智能合约与共识协议及隐私保护分别对应的权重为 0.886^2, 0.331^2, 0.303^2, 0.115^2。可以得出交易操作参与者的权重最高，对整个共享充电体系的也最重要，交易数据和智能合约与共识协议权重则相近，均为三分之一左右。隐私保护环节的权重则最小。

将计算得到的数据与汽车共享充电指标表结合，引入专家对整个体系的评价结果，可以得出表 4 的结果。

从表 4 以及专家对风格迁移的评价结果，可以得到一级指标主因素评价矩阵 R 如下：

$$A=\begin{bmatrix}0.468 & 0.143 & 0.389\\ 0.311 & 0.307 & 0.382\\ 0.398 & 0.496 & 0.105\\ 0.624 & 0.200 & 0.175\end{bmatrix} \tag{7}$$

模糊层次分析法的评价结果可以由一级指标主因素评价矩阵 R 和一级指标向量 A^2 计算得到。由公式 $B=A^2\cdot R$ 计算得知，层次分析法评价的最终结果 B 为 (0.367　0.016　0.036)。其中最大数值为 0.367，表明未经本方法监管时，汽车共享充电体系运行一般。

表 4　单因素评价结果(监管前)

Tab. 4　Single factor evaluation results(before the regulation)

目标层	准则层	指标层	专家的评价结果		
			高	中	低
汽车共享充电(监管前)	交易操作参与者(0.886²)	充电电车用户信息认证(0.138²)	0.3	0.4	0.3
		桩主或运营商信息认证(0.305²)	0.2	0.5	0.3
		充电桩信息认证(0.942²)	0.5	0.1	0.4
	交易数据(0.331²)	充电量数据(0.147²)	0.6	0.4	0
		充电速度(0.977²)	0.3	0.3	0.4
		充电价格(0.155²)	0.5	0.5	0
	智能合约与共识协议(0.303²)	认证合约执行情况(0.978²)	0.4	0.5	0.1
		监管合约执行情况(0.093²)	0.6	0.1	0.3
		共识协议(Rapidchain)漏洞(0.184²)	0.3	0.5	0.2
	隐私保护(0.115²)	电车用户隐私(0.351²)	0.8	0.2	0
		桩主隐私(0.936²)	0.6	0.2	0.2

使用本文提出的穿透式监管方法后，再次统计专家对整个共享充电体系的评价，可以得到表 5。

从上表以及专家对风格迁移的评价结果，本文可以得到一级指标主因素评价矩阵 R 如下：

$$R=\begin{bmatrix}0.871 & 0.115 & 0.013\\ 0.795 & 0.012 & 0.193\\ 0.593 & 0.394 & 0.105\\ 0.636 & 0.287 & 0.088\end{bmatrix} \tag{8}$$

由公式 $B=A^2\cdot R$ 计算得知，层次分析法的最终结果 B 为 (0.684　0.013　0.012)。其中最大数值为 0.684，与未经监管时结果进行对比，可以得出简单结论：经过本方法进行穿透式监

管，汽车共享充电体系安全性表现大大提升。

表 5　单因素评价结果(监管后)

Tab. 5　Single factor evaluation results(after the regulation)

目标层	准则层	指标层	专家的评价结果		
			高	中	低
汽车共享充电(监管后)	交易操作参与者(0.886²)	充电电车用户信息认证(0.138²)	0.4	0.4	0.2
		桩主或运营商信息认证(0.305²)	0.7	0.2	0.1
		充电桩信息认证(0.942²)	0.9	0.1	0
	交易数据(0.331²)	充电量数据(0.147²)	0.8	0.1	0.1
		充电速度(0.977²)	0.8	0	0.2
		充电价格(0.155²)	0.6	0.4	0
	智能合约与共识协议(0.303²)	认证合约执行情况(0.978²)	0.6	0.4	0.1
		监管合约执行情况(0.093²)	0.7	0.1	0.2
		共识协议(Rapidchain)漏洞(0.184²)	0.4	0.3	0.3
	隐私保护(0.115²)	电车用户隐私(0.351²)	0.9	0.2	0
		桩主隐私(0.936²)	0.6	0.3	0.1

5　结束语

本文首先分析了目前汽车共享充电现状和区块链监管现状，然后提出了一种区块链穿透式监管方案，并针对一个基于联盟链-公有链双链结构的汽车共享充电模型的整个充电交易过程和评价流程进行监管。运用模糊层次分析法对整个模型进行评价，得出简单的结论：运用穿透式监管的方法进行监管之后，整个共享充电体系的安全性和有序性得到了一定程度的提高。未来的区块链监管实践还需在以下几个方面展开研究：进一步提高监管的方法水平；进一步扩大监管的对象；在监管过程中加强隐私保护等。

参考文献：

[1] Qarebagh A J, Sabahi F and Nazarpour D. Optimized Scheduling for Solving Position Allocation Problem in Electric Vehicle Charging Stations [C] Proc of the 27th Iranian Conference on Electrical Engineering (ICEE) . Piscataway, NJ: IEEE Press, 2019: 593-597.

[2] 任泽平, 连一席, 郭双桃. 充电桩新基建: 迈向新能源汽车时代 [J]. 中国工业和信息化, 2020 (04): 74-79. (Ren Zeping, Lian Yixi, Guo Shuangtao. New infrastructure of charging piles: towards the era of new energy vehicles [J]. China Industry and Information Technology, 2020 (04): 74-79.)

[3] Chen Q A, Yin Yucheng, Feng Yiheng, *et al.* Exposing Congestion Attack on Emerging Connected Vehicle based Traffic Signal Control [C]// Proc of the Network and Distributed System Security Symposium (NDSS) . California: ISOC Press, 2018: 1-15.

[4] 刘明达, 陈左宁, 拾以娟, 等. 区块链在数据安全领域的研究进展 [J]. 计算机学报, 2021, 44 (01): 1-27. (Liu Mingda, Chen Zuoning, Shi Yijuan, *et al.* Research progress of blockchain in the field of data security [J]. Chinese Journal of Computers, 2021, 44 (01): 1-27)

[5] Gorenflo C, Golab L, and Keshav S. Mitigating Trust Issues in Electric Vehicle Charging using a Blockchain [C]// Prof of the 10th International Conference on Future Energy Systems (e-Energy'19) . New York: ACM Press, 2019: 160–164.

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

[7] Kotsiuba I, Velykzhanin A, Biloborodov O, *et al.* Blockchain evolution: from bitcoin to forensic in smart grids [C]// Prof of the IEEE international conference on big data (big data) . Piscataway, NJ: IEEE Press, 2018: 3100-3106.

[8] Pustisek M, Kos A, Sedlar U. Blockchain based autonomous selection of electric vehicle charging station [C]// Proc of the international conference on identification, information and knowledge in the Internet of Things (IIKI) . Piscataway, NJ: IEEE Press, 2016: 217-222.

[9] Kang J, Yu R, Huang X, *et al.* Enabling Localized Peer-to-Peer Electricity Trading Among Plug-in Hybrid Electric Vehicles Using Consortium Blockchains. IEEE Trans on Industrial Informatics, 2017, 13 (6): 3154-3164.

[10] Huang X, Xu C, Wang P, *et al.* LNSC: A security model for electric vehicle and charging pile management based on blockchain ecosystem [J]. IEEE Access, 2018, 6: 13565-13574.

[11] Jeong S, Dao N N, Lee Y, *et al.* Blockchain based billing system for electric vehicle and charging station [C]// Prof of the 10th International Conference on Ubiquitous and Future Networks (ICUFN) . Piscataway, NJ: IEEE Press, 2018: 308-310.

[12] Su Z, Wang Y, Xu Q, *et al.* A secure charging scheme for electric vehicles with smart communities in energy blockchain [J]. IEEE Internet of Things Journal, 2018, 6 (3): 4601-4613.

[13] Choi H, Lee W C, Aafer Y, *et al.* Detecting attacks against robotic vehicles: A control invariant approach [C]// Proceedings of the ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2018: 801–816.

[14] Sun H, Mao H, Bai X, *et al.* Multi-blockchain model for central bank digital currency [C]// Prof of 18th International conference on parallel and distributed computing, applications and technologies (PDCAT) . Piscataway, NJ: IEEE Press, 2017: 360–367.

[15] Pan C, Tang S, Ge Z, *et al.* Gnocchi: Multiplexed Payment Channels for Cryptocurrencies [C]// Proc of International Conference on Network and System Security. Berlin: Springer, 2019: 488–503.

[16] 葛钟慧, 张奕, 龙宇, 等. 一种支持高并发的多人链下支付方案 [J]. 计算机学报, 2021, 44 (01): 132-146. (Ge Zhonghui, Zhang Yi, Long Yu, *et al.* A multi-person off-chain payment scheme supporting high concurrency [J]. Chinese Journal of Computers, 2021, 44 (01): 132-146.)

[17] 李伟明, 雷杰, 董静, 等. 一种优化的实时网络安全风险量化方法 [J]. 计算机学报, 2009, 32 (04): 793-804. (Li Weiming, Lei Jie, Dong Jing, etc. An optimized real-time network security risk quantification method [J]. Chinese Journal of Computers, 2009, 32 (04): 793-804.)

[18] Dreyling R, Jackson E, Pappel I. Cyber Security Risk Analysis for a Virtual Assistant G2C Digital Service Using FAIR Model [C]// Prof of the 8th International Conference on eDemocracy & eGovernment (ICEDEG) . Piscataway, NJ: IEEE Press, 2021: 33-40.

[19] 雷柯楠, 张玉清, 吴晨思, 等. 基于漏洞类型的漏洞可利用性量化评估系统 [J]. 计算机研究与发展, 2017, 54 (10): 2296-2309. (Lei Kenan, Zhang Yuqing, Wu Chensi, *et al.* A Quantitative Evaluation System for Vulnerability Exploitability Based on Vulnerability Types [J]. Computer Research and Development, 2017, 54 (10): 2296-2309.)