计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2023,32(2):119−127 [doi: 10.15888/j.cnki.csa.008984]

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

基于联盟区块链的电动汽车可信充电模型①

穆　蕾, 安毅生, 肖玉坤

(长安大学 信息工程学院, 西安 710064)
通信作者: 穆　蕾, E-mail: 18729274217@163.com

摘　要: 基于中央服务器的传统架构是过去后台服务搭建的重要解决方案, 但随着用户数与应用需求的爆发式增长, 该架构对中心节点的计算与存储能力提出了更高的要求, 同时也带来了信任危机. 分布式系统的一个典型代表-区块链, 作为比特币的核心技术, 它的不可篡改, 可追溯, 不可伪造数据等特性使得它在近几年受到广大研究者的广泛关注. 本文提出将联盟区块链应用到电动车, 充电桩, 智能电表, 传输电网所组成的充电网络中, 利用区块链技术来管理充电记录, 以此来保护每一方的利益, 为交易纠纷的解决提出一种数据层面的支撑. 本文在提出专用联盟区块链的同时, 也提出了一种新的适用于电动汽车可信充电模型的共识机制和对应的查询智能合约. 实验结果表明所设计的共识机制能在该可信充电网络模型中安全高效的运行, 同时也能够满足用户快速查询交易的需求.

关键词: 联盟区块链; 智能合约; 共识机制; 电动车 (EVs); 充电记录管理

引用格式: 穆蕾,安毅生,肖玉坤.基于联盟区块链的电动汽车可信充电模型.计算机系统应用,2023,32(2):119–127. http://www.c-s-a.org.cn/1003-3254/8984.html

Trusted Charging Model for Electric Vehicles Based on Consortium Blockchain

MU Lei, AN Yi-Sheng, XIAO Yu-Kun

(School of Information Engineering, Chang'an University, Xi'an 710064, China)

Abstract: The traditional architecture based on a central server is an important solution for the construction of background services in the past. However, with the explosive growth of the number of users and application requirements, this architecture has put forward higher requirements for the computing and storage capabilities of the central node and brought a crisis of confidence. A typical representative of distributed systems, namely, blockchain, is the core technology of Bitcoin, and it has been widely concerned by researchers in recent years due to its characteristics such as tampering prohibition, traceability, and forgery data prohibition. This study aims to apply the consortium blockchain to the charging network composed of electric vehicles, charging piles, smart electric meters, and transmission networks and use blockchain technology to manage charging records, so as to protect the interests of each party and provide transaction disputes with data-level support. In addition to a dedicated consortium blockchain, this study also proposes a new consensus mechanism and a corresponding smart query contract suitable for the trusted charging model of electric vehicles. The experimental results show that the designed consensus mechanism can operate safely and efficiently in this trusted charging network model and can make users quickly search for transactions.

Key words: consortium blockchain; smart contracts; consensus mechanism; electric vehicles (EVs); charging record management

① 基金项目: 国家自然科学基金 (52172325)
收稿时间: 2022-07-06; 修改时间: 2022-08-15; 采用时间: 2022-09-21; csa 在线出版时间: 2022-11-29
CNKI 网络首发时间: 2022-11-30

随着城市化的不断发展, 能源互联网极大地改变了人们的生活, 电动汽车作为智能交通系统中新兴的重要组成部分, 不仅使人们的出行更加便捷, 而且极大降低了碳排放与噪音污染. 然而, 电动汽车的不断普及对供电的需求提出了新的挑战, 因此需要大量布设充电桩来解决该问题. Jochem 等[1] 和 Jung 等[2] 研究如何寻找一种最优部署方案来设置充电桩以满足用户的动态需求. Qin 等[3] 和 Lu 等[4] 研究如何通过优化电动汽车充电顺序来减少充电等待时间, 以满足大量电动车的充电请求. 文献 [5] 研究了利用区块链保证车辆通信数据传输安全与用户隐私, 同时利用网联电动车辆的群体智能辅助智能驾驶. 文献 [6] 研究了利用区块链记录网联车辆之间的交易信息以鼓励资源共享. 文献 [7] 研究了一种存储电动车充电交易记录的最优代价存储模型, 文献 [8] 研究了将区块链与物联网相结合保障智能交通系统中的数据安全性与隐私保护. 如上所述, 对于区块链在智能交通领域的应用, 现有研究主要围绕车辆社交网络 (vehicular social network, VSN) 展开, 利用区块链来存储车辆间共享数据的交易记录以及车辆在途数据, 构建一个安全的, 可靠的, 协同工作的, 隐私保护型的 VSN. 然而, 很少有工作针对电动车在充电过程所发生的潜在交易问题进行研究, 例如:

(1) 传输的电量全由充电桩一方计量, 电动车处于被动接受的地位. 有存在电动汽车充满电的情况下, 充电桩恶意放电, 提高充电金额的可能性[9]. 同时, 也存在因电动车电池老化, 充满电会消耗更多电量, 引发车主与充电站纠纷的可能性.

(2) 电动汽车用户的重要隐私数据存储在多个第三方平台上, 数据容易受人为或者设备故障而泄露.

(3) 传统中心式存储机制相对于分布式存储, 其数据集中存放, 中心节点发生故障会导致大规模业务瘫痪, 无法响应用户的请求.

(4) 由于充电桩设备工作状态异常, 在充电过程中会对电动车造成损坏, 若日后电动车出现问题, 难以追溯责任源头.

针对以上问题, 在电动汽车充电业务中急需一种技术方案来确保交易数据可信, 其核心在于确保充电交易数据被安全的, 不可更改的, 可多方验证的存储.

1 相关工作

区块链是一种不依赖于中心机构的分布式账本技术, 由各方验证, 在异构、不可信的网络环境中实现各个节点交易数据的一致性. 区块链涉及到诸多领域, 例如密码学[10], 分布式存储[11], 端对端传输[12], 以及共识机制[13] 等. 在一个区块中, 数据按照时间戳顺序被封装, 经由多方验证后被添加到区块链中. 区块链主要解决两个问题: 1) 如何使上链的数据不可篡改, 不可伪造, 可追溯; 2) 如何在去中心化的环境中达成交易数据的一致性. 前者使用密码学技术如公钥, 私钥, 数字签名等保证. 后者使用共识机制保证, 例如工作量证明 (proof of work, PoW)[14], 权益证明 (proof of stake, PoS)[15], 实用拜占庭容错协议 (practical Byzantine fault tolerance, PBFT)[16] 等共识机制. 比特币采用 PoW 实现共识, 每一个记账员节点要想夺取记账权, 必须不断修改区块的 nonce 值 (即区块头中的随机数) 以使该区块的 SHA256 摘要满足以一定数目的零开头. 由于在夺取记账权的过程中会消耗大量算力和时间, 因此 PoW 不适合于商业应用场景. PoS 共识机制规定一个记账员节点要想夺取记账权, 必须要将一定数量的货币作为筹码存入网络, 筹码的多少决定选择该记账员节点生成区块的可能性. PBFT 共识机制可以容忍小于等于 $(N-1)/3$ 个恶意节点 (N 为网络节点个数), 但该共识机制通信复杂度高, 安全性与活跃度高依赖于网络质量[17]. 这 3 类共识机制的对比见表 1.

表 1 常用共识算法的优点与缺点

共识算法	优点	缺点
PoW	完全去中心化	消耗大量算力与时间
PoS	节能, 带宽利用率高, 比PoW效率高	单个节点容易统治整个网络, 威胁整个系统的安全[18]
PBFT	高效率, 高安全性	通信复杂度高, 严重依赖于网络质量

比特币是区块链的一个重要应用, 为其他区块链产品奠定了理论基础. 区块链中的区块由区块头与区块体构成, 区块体存储全部的交易信息, 交易数据每两两进行哈希运算生成 Merkle 根存于区块头中. 区块头中存储前驱区块的哈希值, 时间戳, Merkle 根, 难度系数, 随机数等. 区块链网络中的每个节点都在努力改变随机数, 使其整个区块的哈希值前缀满足规定个数连续的零. 满足要求的节点有资格将区块加入到区块链中从而获得收益. 在比特币网络中如果恶意节点想要篡改, 接管整个区块链, 那么它必须拥有一半以上的算力, 由于代价是非常大的, 所以这就迫使每个节点按规定工作.

区块链按照公开化程度分为公共区块链 (public

blockchain), 私有区块链 (private blockchain) 和联盟区块链 (consortium blockchain)[13]. 在公共区块链中, 任何节点都有权力参与到共识流程中, 获得建块权力得到奖励, 且所有公众对区块链都有读权限, 比特币是公共区块链的典型代表. 不同于公有区块链, 联盟区块链的共识流程是由挑选出的特殊节点参与, 由多个组织组成一个联盟, 只有加入到这个联盟才可以参与区块链服务, 实现部分去中心化. 而私有区块链的共识则是由一个特定组织来确认, 已经不具备去中心化的特点. 所以联盟区块链是半去中心的, 私有区块链则是全中心的.

对于上述电动汽车与充电桩运营商之间可能存在的交易问题, 综合考虑到系统的安全性和效率, 本文采用联盟区块链技术来实现, 这将限定只有经过合法注册的用户才可以加入到区块链网络, 并且只有符合特定要求的节点才可以参与到共识过程中, 以此来保证该架构的安全运行. 之所以使用区块链而不使用其他数据存储方式的原因如下.

1) 区块链可以确保电动车与充电桩交易数据真实, 不会存在造假的可能, 确保交易双方的权益.

2) 分布式特性使交易信息更加安全, 同时使充电网络具有更高的容错性、可拓展性与灵活性.

3) 经过加密的数据可以防止用户隐私的泄露.

4) 交易记录可追溯, 每笔交易都要接受双端确认, 形成有效交易并加入区块链, 使用户明确知道每笔花费的详细信息, 给交易纠纷提供了一个可能解.

2 基于区块链的可信充电模型

如前所述, 为了降低构建该区块链可信充电网络模型的成本且使网络更加可控, 将采用联盟区块链用以实现分布式数据存储与数据的安全访问. 不同于传统的公有区块链, 联盟区块链所有实体加入该网络必须得到认证. 充电交易数据在得到电动车与充电桩的签名后, 由智能电表发往离它最近的区块链记账员 (data aggregator, DAG)[19] 经共识机制确认后加入区块链. 本文提出的基于区块链的电动汽车可信充电模型如图 1 所示, 模型及后文中使用的符号见表 2.

可信充电模型中区块生成过程如下所示.

步骤 1. 电动车, 充电桩, 智能电表, 以及区块链中的记账员进行注册获取密钥和证书, 该过程应用椭圆数字签名算法和非对称加密技术. 这 4 类实体要想成为合法实体加入到该区块链网络中, 必须在权威证书颁发机构 (CA) 进行注册[20].

步骤 2. 假设电动车可以找到一个合法注册的充电桩, 并且智能电表安装无误. 当用户连接扫码, 智能电表确认电动车证书 ($Cert_{vi}$) 无误后, 允许充电桩给电动车充电, 若出错则拒绝.

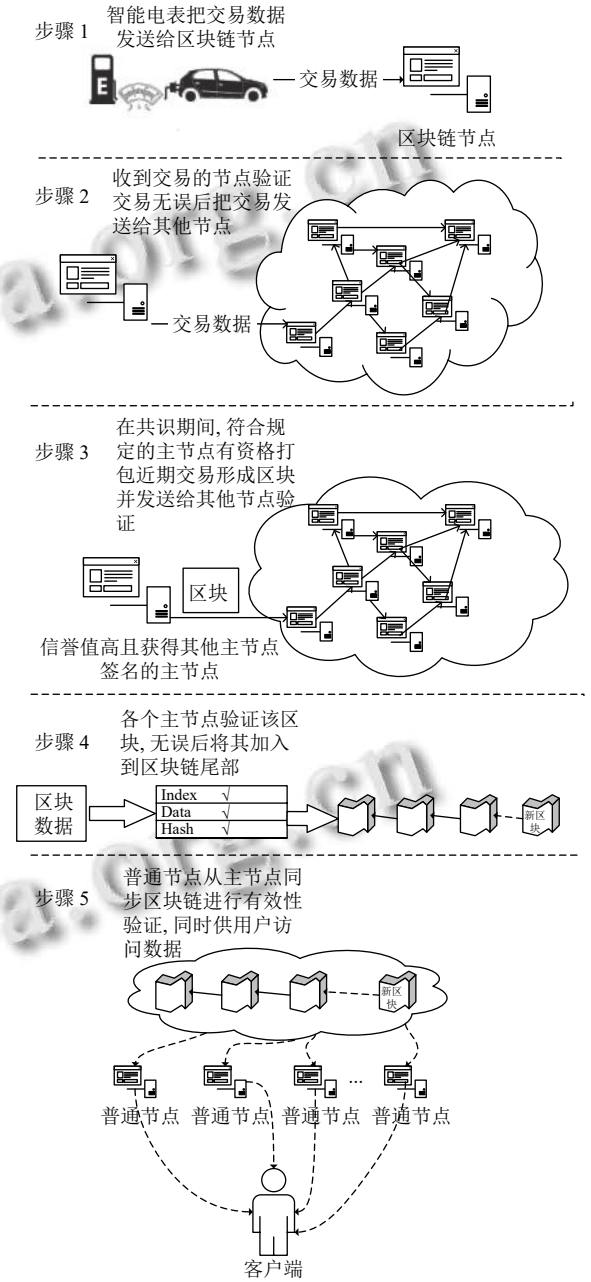

图 1 区块生成过程

步骤 3. 在充电过程中, 为了使充电过程可追溯, 本文规定智能电表检测到每充一度电 (可以根据实际情况更改), 则需要将其充电信息 (例如, 电动车标识, 充电桩标识, 电表标识, 电表所记电量 (我们只记录两次

上传电量的差值, 而不是总电量, 这将允许用少量存储空间就可以记录耗电量), 时间戳, 电池状态, 以及一切相关信息) 打包, 经由充电桩, 智能电表, 电动汽车签名确认无误后形成交易记录发送到区块链节点, 这个请求消息格式如下所示:

$$M_k \rightarrow DAG_j : Transaction = E_{pk_{DAG_j}}(Data1||Sign_{SK_{M_k}}(hash(Data1))||Cert_{m_k}||timestamp)$$
$$\text{where } Data1 = (Data\_1||Data\_2||timestamp||Data)$$
$$\&\&Data\_1 = (Sign_{SK_{v_i}}(hash(Data))||Cert_{v_i})$$
$$\&\&Data\_2 = (Sign_{SKC_p}(hash(Data))||Cert_{C_p})$$

表 2 符号集合

符号	描述
V_i	区块链网络中第i个电动车
PID_i	第i个电动车的假名
C_p	第p个充电桩
DAG_j	区块链网络中第j个的记账员
$i \rightarrow j$	实体i发送消息给实体j
M_k	区块链网络中第k块智能电表
PK_i, SK_i, $Cert_i$	实体i的公钥, 私钥及其证书
$E_{pkx}(m)$	用实体x的公钥加密信息m
$Sign_{skx}(m)$	实体x在信息m上进行签名
$timestamp$	时间戳
$x\|\|y$	消息x连接消息y

步骤 4. 记账员节点在收集到交易信息后, 会将验证无误的交易信息扩散到其他指定节点, 该节点将会验证交易的合法性, 在收集到一定的合法交易后, 符合规定的主节点会生成一个区块, 经由共识过程确认无误后将其添加到区块链尾端.

步骤 5. 普通节点可以下载区块链数据供电动车用户和充电桩运营商查询, 用以解决可能发生的经济纠纷问题.

可信充电模型中的区块链主要由两部分组成: 区块头与区块体. 区块头主要包括前驱区块的哈希值, 时间戳, 建块节点标识符, 区块体则包括若干个交易即电动车交易信息. 整体结构如图 2 所示, 不同于传统比特币的区块结构, 由于我们的共识机制不涉及“挖矿”操作, 所以我们的区块头部只存储少量信息, 用以减轻节点存储负担.

2.1 基于信誉值的众签名共识机制

由于区块链是去中心化的结构, 没有一个中心的节点对其进行控制与管理, 因此会遇到数据一致性问题. 为了确保数据一致性, 区块链中的节点必须要遵循相同的协议, 也就是共识算法[21]. 共识算法必须满足:

1) 一致性: 所有诚实节点保存的区块数据必须是相同的.

2) 有效性: 诚实节点发布的信息最终被其他节点有效记录在各自的区块链中.

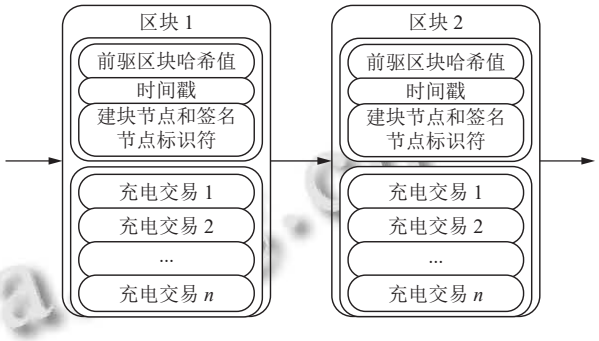

图 2 区块链结构

针对本文可信充电模型所对应的联盟区块链结构, 需要为其设计一种快速、公平、高效率的共识机制. 本文将信誉值引入共识机制. 有研究表明高信誉值的节点会为区块链网络带来更高质量的数据同时也能促进网络的平稳运行[22]. 信誉值的计算依赖于记账员节点在加入该网络后的具体行为. 恶意的行为比如篡改交易, 伪造交易, 攻击区块链网络会降低该节点的信誉值, 善意的行为比如参与区块链共识获得建块权力, 探测举报恶意节点, 为区块链的安全运行做出贡献会增加其信誉值. 所以, 需要一种度量机制来根据节点的行为量化其信誉值.

在共识期间, 所有记账员节点按其信誉值大小进行竞争, 挑选出信誉值 top α 的节点形成共识节点列表 (consensus node list, CNL) 也叫做主节点列表, 这些节点参与块生成与块验证, 用以提高吞吐率. 为了防止 PoS 中出现的极端问题, 当一个主节点生成块以后, 它需要其他 β 个主节点进行签名来证明该块的有效性, 用以防止某个节点因信誉值太大而统治整个网络. 当符合要求后, 该节点将其发送到其他节点进行验证, 若检查无误, 则添加到区块链中. 若出错则抛弃, 然后更新该节点及其签名节点的信誉. 为了加快块生成速度, 防止恶意节点恢复信誉值过快, 必须设计一种简洁的, 满足该区块链网络的信誉值更新函数来维护该系统的安全. 根据文献 [23] 中提出的一种针对路测单元 RSU 的一种信誉更新函数, 本文将拓展该函数以使其满足恶意节点信誉值恢复速度比诚实节点增加信誉值慢, 同时细分了节点的具体行为. 在此基础上提出一种新

的信誉值更新函数, 来维护该系统的安全性与高效性, 如式 (1) 所示, 此式将作为记账员节点的信誉值更新函数. 根据数学关系, 它满足: 1) 恶意节点的信誉值会快速降低, 阻碍其参与共识过程, 有助于维护该联盟区块链的安全. 2) $R_i(t)$ 随善意行为增加缓慢, 阻止恶意节点恢复速度快, 进而威胁到该网络. 上述两条可以确保该联盟区块链可以避免因恶意节点的存在而威胁到整个联盟网络的安全.

$$R_i(t)=\frac{1}{1+\mathrm{e}^{\frac{\zeta}{F_j^p}+\gamma F_j^N}} \tag{1}$$

式 (1) 的信誉值计算依赖于 DAG_j 的具体行为, 其值在 (0, 1) 之间. 其中, $R_i(t)$ 表示 DAG_j 节点的信誉值, 此外, F_j^N 为该节点加入该区块链网络以来所有的不合法行为数, 比如伪造交易, 篡改区块数据等做出危害区块链网络安全的举动, 每发生一次该值每次加一, 与 $R_i(t)$ 负相关. F_j^p 记录了该节点加入区块链网络以来所有的合法行为数, 比如参与信誉值评比获得建块权力或者为合法区块签名, 排查恶意节点等为维护区块链网络的安全做出贡献的行为, 该值每次加一, 它与 $R_i(t)$ 正相关. ζ 与 γ 是协调因子, 会根据加入的节点总数随区块链网络动态更改其值. 初始时, F_j^p 取为 1, F_j^N 取为 0.

重要的是为了在所有的 DAG_j 平衡信誉值, 生成区块不仅需要自己的信誉值尽量高, 而且需要获得其他 β 个主节点的签名, 只有经过其他主节点签名的区块才是一个有效的区块, 才会被其他节点接受和验证, 确认无误后才会被加入到区块链中. 配合相应的激励机制, 不仅建块节点可以获得奖励, 而且相应的签名节点也可获得相应比例的奖励, 因此该机制可以提高其他区块链节点的积极性, 共同维护该区块链系统的平稳运行, 这是该共识机制不同于其他共识机制的地方.

2.2 基于索引的查询智能合约

该可信充电网络所涉及的是数据密集型交易, 区块链网络将会存储大量交易信息. 相比于传统关系型数据库, 区块链并没有主键和外键的概念用于快速定位交易信息. 相反, 区块链需要搜索每一个区块来找到目标数据, 这将是非常耗时的, 特别是在区块链数据不断增长的情况下. 本文将设计一种用于查找操作的智能合约来方便用户根据特定索引查找数据. 智能合约定义了一组存储并运行在区块链中的数字承诺, 用以实现事务的自动化, 该过程不能被人为干预, 具有高度的自执行能力. 我们采用文献 [24] 中提出的分类方法为本文可信充电网络模型设计查询智能合约.

在该联盟链中, 为了快速检索到相应用户的所有交易, 本文将采用字典结构来存储加入到区块链中的数据. 该字典结构记录了键值对的关系, 根据相应的键得到值的时间复杂度为 O(1), 这大大降低了查找相应用户所有交易的时间, 不需要对整个区块链进行暴力迭代, 进而得以优化查询. 具体方法为在把合法区块加入到区块链时, 抽取出区块体中的交易, 然后以用户的假名也就是公钥的哈希值作为键, 整个交易为值加入到以该键对应的交易集合中, 这样就形成了一一对应关系. 当用户想要查询属于自己的交易数据时, 后台根据用户公钥哈希值获取到该用户交易池, 由于交易已经按照时间戳排序, 然后根据时间段进行二分查找获取交易信息然后序列化返回, 整个查询过程的时间复杂度为 O(log(N)), N 为该交易池大小, 具体请求过程如图 3 所示.

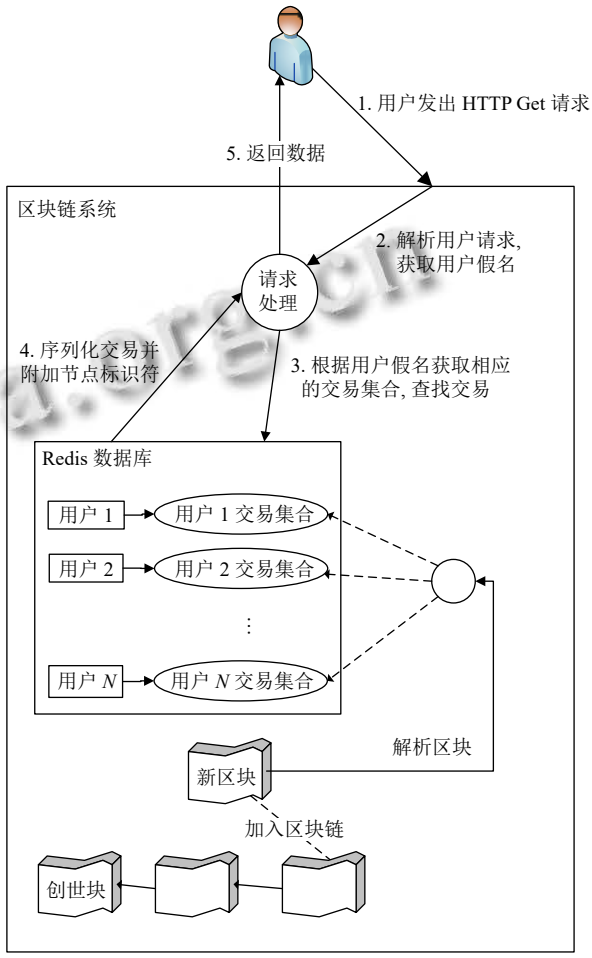

图 3 用户查询过程

为了确保返回数据的可靠性, 真实性, 客户端发出的查询请求被普通节点获取到之后, 返回给客户端之前, 需要得到高信誉值节点的签名. 交易加入所属集合的具体过程如图 4 所示.

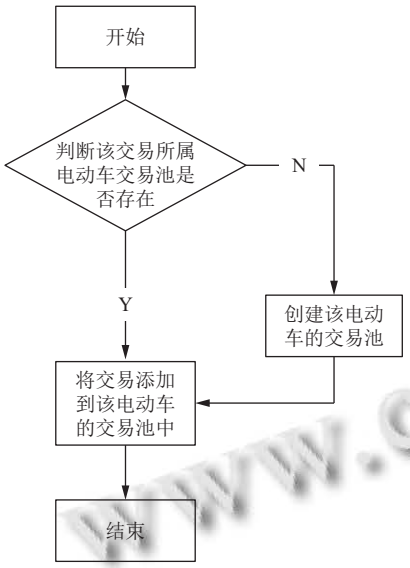

图 4 添加交易过程

用户从浏览器输入的数据格式内容及输出格式内容如表 3 所示.

表 3 数据输入输出格式

数据输入	数据查询结果
[uid, startTime, endTime]	[[uid, pileid, meterid, blockid, timestamp, cost, signuser, signpile, signmeter, [voltage, current, temperature, power]], …]

如表 3 所示, 用户输入自己的公钥 SHA256 编码, 交易起始时间, 结束时间, 联盟区块链网络将会返回该时间段内的相关交易信息, 如电表标识符, 充电桩标识符, 电动车标识符, 上述三者的签名, 所属区块哈希值, 充电金额, 和相应的电动车电池信息, 如平均电压, 平均电流, 平均功率, 温度相关信息. 查询智能合约将上述交易信息集合序列化成 JSON 后返回给用户.

3 安全分析与实验结果

不同于传统的通信模型与隐私保障机制, 本文设计的区块链网络使用联盟区块链与智能合约技术来保障在交易上传至区块链时的安全性与快速查找能力. 联盟区块链确保数据不可篡改, 不可伪造, 自执行的智能合约确保数据的快速查询, 并且该充电网络分布式的特性相比于集中式可以保障数据的安全存储[25]. 交易上传与查询过程中使用数字假名进行操作, 为交易双方带来隐私保护. 更多的关于本区块链网络的安全性能分析如下[26].

1) 数据不可伪造与篡改: 由于使用联盟区块链, 所有节点必须经过认证才可以加入该区块链网络, 只要节点不丢失自己的私钥, 就不会有恶意节点伪造交易签名来攻击该区块链网络.

2) 去除中心节点: 在应用联盟区块链的情况下, 节点之间通过 P2P 的方式进行通讯, 交易经由共识机制确认. 中央可信节点不会参与到该过程中, 这样不会因为中心节点被攻击而造成整个网络的瘫痪, 分布式的特性确保了这一点.

3) 自执行的智能合约: 本文提出的查找智能合约运行在该联盟区块链上, 是自治的, 自我运行和自我维护的[18], 一旦生效就不会被人为因素所干扰.

所以, 对于一个区块链网络来说, 共识机制与智能合约是两个不可缺少的重要组成部分. 前者决定了区块链系统的交易数据一致性, 后者自动化、不被人为干预的机制可以确保区块链系统的事务不会被外界影响而造成交易数据不一致错误.

为了验证上述提出的基于信誉值的共识机制与查询智能合约, 本文在 Win10, 16 GB 内存, 4 核 8 线程的电脑上进行实验. 后台服务器采用 Go 语言编写, 创建 10 个 Goroutine 来模拟节点进行共识, 加入区块链中的交易以聚簇分类, 也就是以键值对的方式进行存储, 并根据需要存入 Redis 数据库并持久化. 客户端模拟用户上传交易信息, 同时也可利用浏览器查询各个用户的某个时间段内的交易信息.

3.1 共识机制的实验

在该实验中, 将对比本文提出的基于信誉值众签名的共识机制与传统 PoS 机制之间的不同. 不同于传统 PoS 共识机制, 本文设计的共识机制可以确保参与共识的每个节点都可以公平竞争, 不会存在某个高信誉值节点统治整个区块链网络的现象. 为了简化设计, 每 10 笔交易建立一个区块, 设计 10 个 Goroutine 来模拟共识节点, 同时设置式 (1) 中的 ζ 与 γ 为 1, 每个节点随机获得其他节点的签名. 令 α 为 5, β 为 3, 实验将统计每 100 次共识过程中每个节点参与区块生成的次数, 并计算每笔数据的标准差. 实验结果如图 5 所示, 随着共识次数的增加, 采用信誉值的众签名模式的节点平均建块次数标准差要小于传统 PoS, 即表明本文提出的基于信誉值的众签名模式可以确保每一个记账员节点都可以公平获得建块权力从而得到奖励, 同时防止单个节点统治整个网络.

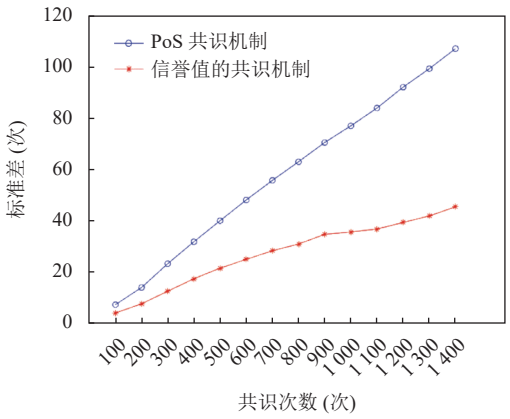

图 5 共识机制对比图

该可信充电网络属于交易密集型网络, 在确保每个节点公平参与共识过程的条件下, 也必须保证该系统的吞吐量足够高, 即单位时间内能处理更多的交易. 实验将通过计算平均共识时间来评价吞吐率, 将对比 PoS 与本文所提出的基于信誉值的共识机制的吞吐量. 分别以每 1 024 笔交易为一个区块, 2 048 笔交易为一个区块, 4 096 笔交易为一个区块, 8 192 笔交易为一个区块, 以及 16 384 笔交易一个区块, 计算当共识节点数目一定时达成共识的平均时间. 如图 6 所示, 实验表明在共识节点数目一定时, 随着单位区块中交易数量的增加, 基于信誉值的共识机制的共识时延与传统共识机制 PoS 基本相同, 可以看出在该共识机制下每个区块的交易数量不是限制该网络共识时延的瓶颈.

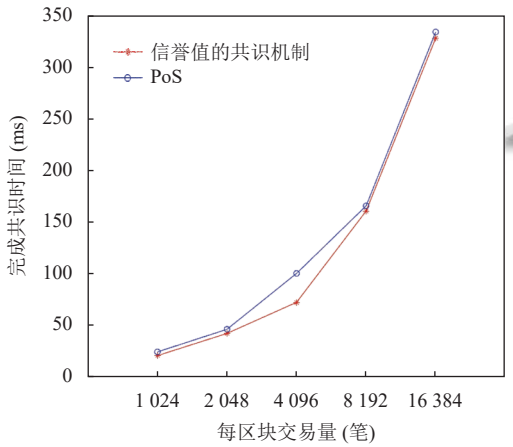

图 6 平均共识时间 (节点数目一定)

同时, 为了分析节点数目对共识时间的影响. 规定每区块打包 4 096 笔交易, 分别在 10 个节点, 15 个节点, 20 个节点, 25 个节点, 30 个节点中的网络中, 计算共识过程所需时间, 如图 7 所示.

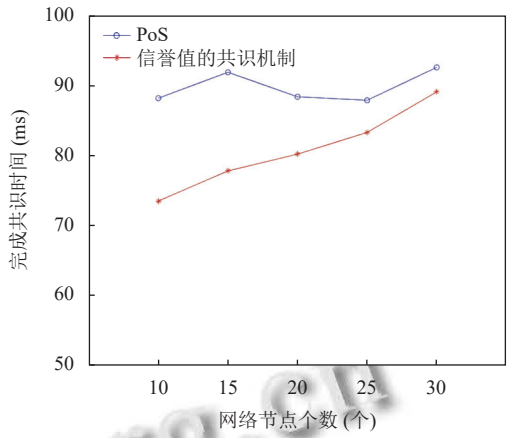

图 7 平均共识时间 (每区块交易数目一定)

可以看出, 随着节点数目的增多, 该基于信誉值的共识机制所需要共识时间会优于传统 PoS 机制接近 10%, 排除网络时延的原因可能是由于该信誉值机制不需要复杂的计算. 同时如图 5 所示, 在保障共识时间的同时, 也能够保证每个共识节点能公平地参与共识, 保证整个区块链网络节点参与共识过程的积极性, 即每个节点都有机会获得建块权力来获得奖励以更新自己的软硬件.

3.2 查询智能合约的实验

随着电动车与充电桩的不断部署, 交易数量会不断增加, 区块链的长度也会不断增长, 因此在一条较长的区块链中快速查找交易是区块链应用的一个关键技术. 当用户从浏览器访问区块链服务时, 区块链网络内部的智能合约将会处理用户的请求并返回.

传统的区块链查询算法如算法 1 所示.

算法1. Traditional query method of blockchain

Input: Hash H of transaction T

Output: Result (details of transaction T)

```
1.  FLAG = false
2.  For Block in blockchain
3.    For Transaction in Block.Transactions
4.      IF H = Transaction.Hash Then
5.        Result = Transaction
6.        FLAG = true
7.        Break
8.      EndIF
9.    EndFor
10. EndFor
11. IF FLAG = true Then
12.   Return Result
13. EndIF
14.   Return NULL
```

传统区块链查询方式类似于链表查找, 首先定义一个标志位 flag, 初始为 false, 遍历区块链得到一个区块, 然后遍历其中的交易信息, 通过匹配待查询交易与 Transaction 的哈希值, 如果匹配失败则继续遍历, 匹配成功则结束查询. 这种查询方式在区块链长度较短, 交易数量少的情况下可以满足用户的需求, 但不适用于该数据密集型网络, 否则会造成很大的查询延迟. 第 3.2 节提出的基于索引的查找智能合约所对应的查找算法如算法 2 所述.

算法2. Smart contract algorithm based on classification search

Input: Transaction StartTime st and EndTime et and hash of public key of user uid

Output: Details of transaction set

```
1. Pool = FindTransactionPool(uid)
2. Txs = BinarySearchTransactionsByTime(st, et)
3. RETURN SerializeTransaction(Txs)
```

为了对比上述的两种查询算法的性能, 实验规定每 1024 笔交易生成一个区块. 在每上传 1024 笔交易, 2048 笔交易, 4096 笔交易, 8192 笔交易, 16384 笔交易时随机查找一位用户某个时间段内的交易信息. 实验结果如图 8 所示, 本文提出的基于索引的分类查询的搜索效率比传统迭代查询有明显优势.

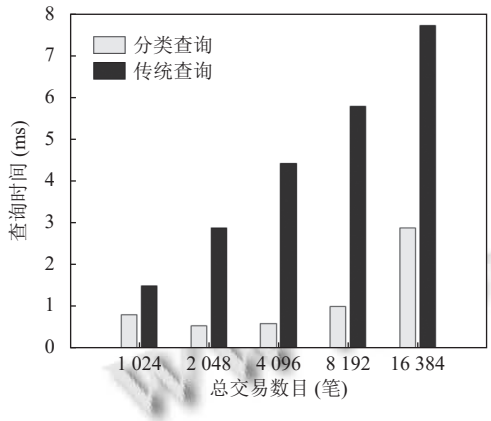

图 8 交易搜索对比图

4 结论与展望

本论文利用区块链技术来解决电动车在充电过程中遇到的经济纠纷问题, 本文设计了一种满足该区块链网络的共识机制以用来弥补传统 PoS, PoW, PBFT 共识机制的不足, 本文所设计的基于信誉值的众签名共识机制在保证共识速度的同时也能够维护每个节点参与共识的公平性. 然而, 该信誉值机制更需要合理地与区块链激励机制相结合, 确保每个节点可以定期凭借信誉值来换取存储空间与计算能力更强的硬件, 以用来鼓励每个节点参与该系统共识过程, 共同来维护整个系统的安全性与可靠性. 除此之外, 对于该数据密集型网络, 也设计了一种基于索引的查询智能合约来满足用户查询交易的需求, 虽然该索引机制可以满足用户快速查询的要求, 但也对节点的存储能力有很大的挑战, 例如, 可以设计压缩智能合约来定期压缩数据, 将历史数据压缩后保存在云端, 节点只存储摘要信息, 进而降低记账员节点的存储压力, 这些都噬需今后的工作来解决.

参考文献

1 Jochem P, Brendel C, Reuter-Oppermann M, *et al*. Optimizing the allocation of fast charging infrastructure along the German autobahn. Journal of Business Economics, 2016, 86(5): 513–535. [doi: 10.1007/s11573-015-0781-5]

2 Jung J, Chow JYJ, Jayakrishnan R, *et al*. Stochastic dynamic itinerary interception refueling location problem with queue delay for electric taxi charging stations. Transportation Research Part C: Emerging Technologies, 2014, 40: 123–142. [doi: 10.1016/j.trc.2014.01.008]

3 Qin H, Zhang WS. Charging scheduling with minimal waiting in a network of electric vehicles and charging stations. Proceedings of the 8th ACM International Workshop on Vehicular Inter-networking. Las Vegas: ACM, 2011. 51–60.

4 Lu JL, Yeh MY, Hsu YC, *et al*. Operating electric taxi fleets: A new dispatching strategy with charging plans. Proceedings of the 2012 IEEE International Electric Vehicle Conference. Greenville: IEEE, 2012. 1–8.

5 Fu YC, Yu FR, Li CL, *et al*. Vehicular blockchain-based collective learning for connected and autonomous vehicles. IEEE Wireless Communications, 2020, 27(2): 197–203. [doi: 10.1109/MNET.001.1900310]

6 Astarita V, Pasquale Giofrè V, Guido G, *et al*. The use of a blockchain-based system in traffic operations to promote cooperation among connected vehicles. Procedia Computer Science, 2020, 177: 220–226. [doi: 10.1016/j.procs.2020.10.031]

7 Qian LP, Wu Y, Xu X, *et al*. Distributed charging-record management for electric vehicle networks via blockchain. IEEE Internet of Things Journal, 2021, 8(4): 2150–2162. [doi: 10.1109/JIOT.2020.3027482]

8 Manjunath P, Soman R, Shah PG. IoT and block chain driven

intelligent transportation system. Proceedings of the 2018 2nd International Conference on Green Computing and Internet of Things. Bangalore: IEEE, 2018. 290–293.

9 马晓蕾. 黑客盯上了充电桩. 经营者 (汽车商业评论), 2022, (6): 101–102.

10 Cao ZF. New development of cryptography. Journal of Sichuan University (Engineering Science Edition), 2015, 47(1): 1–12.

11 Hao K, Xin J, Huang D, *et al*. Decentralized model for distributed storage system. Computer Engineering and Applications, 2017, 53(24): 1–7, 22.

12 Yang M, Yang YY. An efficient hybrid peer-to-peer system for distributed data sharing. IEEE Transactions on Computers, 2010, 59(9): 1158–1171. [doi: 10.1109/TC.2009.175]

13 韩璇, 袁勇, 王飞跃. 区块链安全问题: 研究现状与展望. 自动化学报, 2019, 45(1): 206–225.

14 Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. https://nakamotoinstitute.org/bitcoin/. (2008-10-31).

15 King S, Nadal S. PPCoin: Peer-to-peer crypto-currency with proof-of-stake. http://people.cs.georgetown.edu/~clay/classes/fall2017/835/papers/peercoin-paper.pdf. (2012-08-19).

16 Castro M, Liskov B. Practical byzantine fault tolerance. Proceedings of the 3rd Symposium on Operating Systems Design and Implementation. New Orleans: USENIX Association, 1999. 173–186.

17 Qiao L, Dang SP, Shihada B, *et al*. Can blockchain link the future? Digital Communications and Networks, 2021. [doi: 10.1016/j.dcan.2021.07.004]

18 Xiao Y, Zhang N, Lou WJ, *et al*. A survey of distributed consensus protocols for blockchain networks. IEEE Communications Surveys & Tutorials, 2020, 22(2): 1432–1465.

19 Kang JW, Yu R, Huang XM, *et al*. blockchain for secure and efficient data sharing in vehicular edge computing and networks. IEEE Internet of Things Journal, 2019, 6(3): 4660–4670. [doi: 10.1109/JIOT.2018.2875542]

20 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]

21 Zheng ZB, Xie SA, Dai HN, *et al*. blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 2018, 14(4): 352–375. [doi: 10.1504/IJWGS.2018.095647]

22 Delgado-Segura S, Tanas C, Herrera-Joancomartí J. Reputation and reward: Two sides of the same bitcoin. Sensors, 2016, 16(6): 776. [doi: 10.3390/s16060776]

23 Wang YT, Su Z, Zhang K, *et al*. Challenges and solutions in autonomous driving: A blockchain approach. IEEE Network, 2020, 34(4): 218–226. [doi: 10.1109/MNET.001.1900504]

24 Abuhashim A, Tan CC. Smart contract designs on blockchain applications. 2020 IEEE Symposium on Computers and Communications (ISCC). Rennes: IEEE, 2020. 1–4.

25 Yue L, Huang JQ, Qin SZ, *et al*. Big data model of security sharing based on blockchain. 2017 3rd International Conference on Big Data Computing and Communications. Chengdu: IEEE, 2017. 117–121.

26 Zyskind G, Nathan O, Pentland AS. Decentralizing privacy: Using blockchain to protect personal data. 2015 IEEE Security and Privacy Workshops. San Jose: IEEE, 2015: 180–184.

(校对责编: 牛欣悦)