计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2017,26(12):43−50 [doi: 10.15888/j.cnki.csa.006109]
©中国科学院软件研究所版权所有.
E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

基于区块链的电力市场交易结算智能合约①

鲁　静[1,2], 宋　斌[1], 向万红[1], 周志明[1]

[1](远光软件股份有限公司, 珠海 519085)
[2](湖北第二师范学院, 武汉 430205)

摘　要: 本文针对未来“放开两端”的电力交易市场多主体、多模式、多规则的特点, 设计了电力市场交易结算智能合约, 同时分析了关键技术难点, 并有针对性的给出了解决方案. 利用运行在区块链上的智能合约降低电力市场交易的信任成本, 提高清结算效率, 同时推动能源零售市场的智能化. 通过在由 4000 个节点构成的 P2P 网络中运行一个购售电合同的智能合约实例, 验证了本文方法的成功率约为 99.38%, 每笔交易的平均确认时间约为 16 秒. 如果本文方法得到应用, 将帮助能源交易双方共同制定因需求而动态变化的能源价格, 保证不同能源市场的互联互通, 促进智慧能源价值互联.

关键词: 区块链; 智能合约; 电力交易; 电费结算; 电力市场

引用格式: 鲁静,宋斌,向万红,周志明.基于区块链的电力市场交易结算智能合约.计算机系统应用,2017,26(12):43–50. http://www.c-s-a.org.cn/1003-3254/6109.html

Smart Contract for Electricity Transaction and Charge Settlement Based on Blockchain

LU Jing[1,2], SONG Bin[1], XIANG Wan-Hong[1], ZHOU Zhi-Ming[1]

[1](YGSoft Inc., Zhuhai 519085, China)
[2](University of Education, Wuhan 420205, China)

Abstract: In this paper, aimed at the complicated characteristics, patterns and rules of the future “let go” electricity market, smart contracts of electricity transaction based on the blockchain platform are proposed. Then the key technological difficulties are analyzed and solutions are given. By running a smart contract instance in a peer-to-peer network composed of 4000 nodes, the success rate is 99.38% and the average time consumption for each transaction is proven to be 16s. If our method is applied, we can in the field of electric power market transaction settlement through different systems, reduce the trust of the electric power market transaction cost, reduce the friction in the process of liquidation, improve the efficiency of the clearing and settlement.

Key words: blockchain; smart contract; electricity transaction; electricity charge settlement; electricity market

电力体制改革背景下, 国家电改配套文件《关于推进售电侧改革的实施意见》[1]第四条“电网企业负责收费、结算, 负责归集交叉补贴, 代收政府性基金, 并按规定及时向有关发电公司和售电公司支付电费”; 第八条“电网企业按照交易中心出具的结算依据, 承担市场主体的电费结算责任, 保障交易电费资金安全”, 明确了电网公司承担电力市场结算职能. 为适应电力体制改革、支撑及促进电力市场建设, 电网公司需要建设高效便捷的市场电费结算系统, 建立与之相适的业财结算业务处理规则与工作流程, 为电力市场主体提供安全、快捷、高效的电费清分和资金结算服务, 做好电费结算信息的披露工作, 进一步巩固公司统一电费结算核心优势.

然而, 相比电改前的传统电费结算, 电改后的市场

① 基金项目: 广东省科技计划项目 (2014B010117006); 湖北省教育厅科学研究计划重点项目 (D20163002)
收稿时间: 2017-03-09; 采用时间: 2017-04-07

© 中国科学院软件研究所 http://www.c-s-a.org.cn

化结算在市场成员、交易合同和交易品种等方面对应用和系统提了新的要求. 成员增多、交易品种多样化, 合同规则复杂化, 要求结算系统能灵活拓展, 按照市场价结算; 同时允许购、售电端自主协商、集中竞价, 导致最终市场价格、电量都不统一, 这些都对交易结算管理及风险防范都提出了更高要求.

区块链 (Blockchain)[2]是一种目前受到各国战略性关注的革命性技术, 被《经济学人》杂志誉为“信任的机器”, 是继蒸汽机、电力、信息和互联网科技之后最有潜力触发第五轮颠覆性革命浪潮的核心技术. 区块链综合采用分布式安全存储、一致性验证和密码技术, 提供了一种新型的分布式资源存储、数据保护和历史追溯的解决方案. 这种基于区块链的分布式管理架构所解决的正是交易信用与安全问题, 具有广阔的应用领域和重要的应用价值, 将区块链技术应用于交易结算业务领域中, 可以有效解决财务数据安全、数据篡改、历史追溯、有效监管、交易信任等方面存在的问题.

在国外, 区块链技术已在清算结算领域崭露头角. 2015 年, 美国证券交易巨头联手区块链初创公司 Chain.com 正式上线了用于私有股权交易的 Linq 平台[3]. Linq 基于区块链技术, 将股权交易市场 3 天的标准结算时间直接缩短到 10 分钟, 几乎就在交易完成的瞬间进行完成结算工作, 同时让结算风险降低了 99%. 2015 年 7 月, Overstock 创建了 T0 区块链交易平台[4]销售首个加密债券, 使得结算和交易发生在同一时间, 被评述为“交易即结算”. 2015 年底, 高盛以比特币区块链为蓝本, 开发了通过加密货币进行交易结算的系统 SETLcoin[5], 保证了几乎瞬时的执行和结算. Ripple 专注于跨境支付领域, 基于区块链开发的 InterLedger 协议项目[6]在保持银行等金融机构的各自不同的记账系统基础上建立了一个全球分布式清算结算体系. 2015 年, 金融领域代表性组织 R3CEV 和巴克啥莱银行, 蒙特利尔银行 (BMO), 瑞信银行, 汇丰银行等 11 家银行组成了金融科技创新公司来研究区块链技术应用[7], 目前已经有四十多家世界著名的银行成为 R3 CEV 的会员; 此外, 西班牙的 Santander 银行认为, 到 2022 年, 区块链技术帮助金融行业降低 200 亿美元的记账成本, 因为支付系统目前仍然是中心化的, 货币的转移要通过中央银行, 当金融公司彼此生意往来时, 同步内部的账簿是个耗时几天的繁重任务, 桎梏住了资本并带来了风险.

在国内, 区块链的应用开发实践在以金融科技为代表的领域逐渐展开, 金融企业、互联网企业、IT 企业和制造企业积极投入区块链技术研发和应用推广, 发展势头迅猛. 区块链的应用已延伸到物联网、智能制造、供应链管理、数字资产交易等多个领域. 2016 年国务院印发《“十三五”国家信息化规划》[8], 区块链与量子通信、类脑计算、虚拟现实等被并列为新技术基础研发和前沿布局. 2016 年工信部发布《中国区块链技术和应用发展白皮书》[9], 为各级产业主管部门、从业机构提供指导和参考. 2017 年初, 中国人民银行推动的基于区块链的数字票据交易平台[10]已测试成功, 央行旗下的数字货币研究所也正式挂牌. 区块链技术的意义在于它将成为互联网金融的基础设施, 如果说 TCP/IP 建立了机器之间数据传输的可达、可信和可靠, 那么区块链技术则首次在机器之间建立了“信任”. 互联网被区块链划分出一个“信任”的连接层, 可以记载、验证和转移经济价值.

本文针对未来“放开两端”的电力交易市场多主体、多模式、多规则的特点, 开展基于区块链技术的分布式账本、共识机制、以及购售电智能合约的研究. 利用区块链技术构建的分布式账本, 对电力市场的前端交易、营销数据实现分布式的记账存储, 将交易中心提供的结算依据数据、营销部门提供的用户用电数据保存在区块链共享账本上, 从而打通从支付计划、记账、付款、结算、清分到核算、纰漏、分析、预测的各个财务业务处理环节, 实现购电费、售电公司服务费的安全、高效结算, 提高财务数据的透明度和可审计性; 利用区块链自动共享、不可篡改的记录保管方式, 简化数据记录、存储环节, 规避因人为操作造成的错误; 通过智能合约将清算业务结构化, 减少清算过程中的摩擦, 同时实现“交易即结算”, 提高清算、结算的效率.

1 区块链与电力交易结算的匹配度分析

从电改 9 号文[11]相关内容以及国外的改革经验来看, 市场的开放不可能一步到位, 必然要经过一个过渡期才会进入全面推广. 因此, 未来电力交易市场化改革将是一个逐步推进的过程, 很长一段时间内会存在多种业务模式并存的局面, 包含输配售一体、输配一体售电分开、输配分离等模式, 如图 1. 输配售一体的业务模式相对传统; 输配一体售电分开模式中, 允许电源

© 中国科学院软件研究所 http://www.c-s-a.org.cn

与售电公司协商定价, 结算主体为电网公司, 需要根据市场用户的销售收入和电源结算购电费, 与售电公司结算服务费, 与政府结算政府基金, 与管制用户结算交叉补贴等等; 输配分离模式的结算主体为配售电公司, 通过与市场用户协商定价结算销售收入, 通过与电源协商定价结算购电费, 与电网公司结算输配电服务费, 与政府结算政府基金等等. 由此可见, 市场化结算模式在市场成员、交易合同和交易品种等方面对应用和系统提了新的要求: 市场成员增多、交易品种逐步发展, 要求结算系统能够灵活拓展, 要能根据电能计量系统提供的有效电能数据、现货交易和实时交易中的电价数据、运行考核系统中记录的考核数据、交易合同中签定的相关数据 (包括电价、电量、计量点等) 及电力市场运行相关规则进行电能量结算和电费结算.

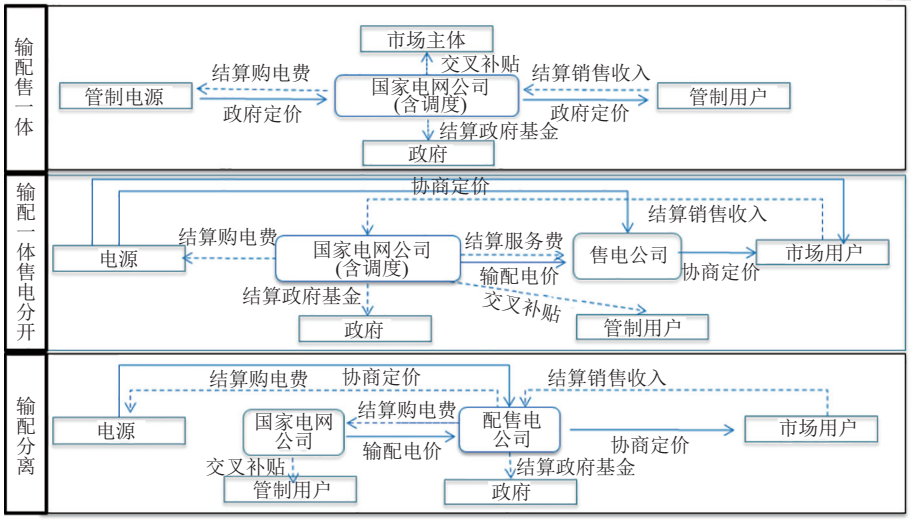

图 1 电改进程中的三种核心结算业务模式

区块链共享、可信、可追溯的特点, 使其在清、结算等领域具备显著的优势. 运行在区块链上的智能合约能将合同规则代码化, 并构造一个去中心化的可信履约环境. 区块链与电力市场交易结算的匹配度分析如下:

(1) 区块链是一个共享式的公共账本, 可打通不同的系统, 从而提升沟通效率, 降低成本;

(2) 区块链实现交易的时候, 基于区块链网络的共识机制实际上可以同时实现清算和结算, 提高清算、结算的效率;

(3) 区块链能完整记录每一笔历史交易记录, 并且可追溯, 更能可靠地登记各种信息, 具有高审计性[12];

(4) 利用区块链的智能合约[13], 能将原有的繁琐、耗时长、业务手续繁杂的清算用计算机代码的方式保存在区块链上, 自动触发执行, 使得结算过程变得简单、结构化, 能减少清算过程中的摩擦; 同时将原有的电子表格存储方式以及手动记录的操作方式变为分布式、不对称加密的账本, 通过自动共享不可篡改的交易记录提高透明度和可审计性.

区块链技术对现有的电力交易结算系统带来的改变如图 2.

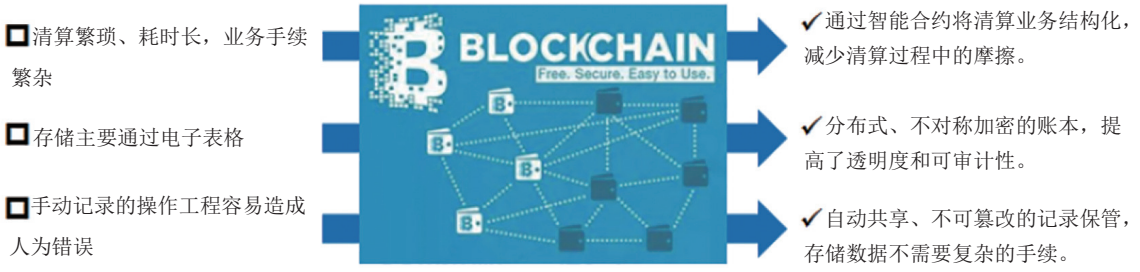

图 2 区块链对现有结算系统的革新

© 中国科学院软件研究所 http://www.c-s-a.org.cn

2 电力市场交易结算智能合约的方案设计

由图 1 可见, 未来的电力市场包括电厂、售电公司、电网、用户、交易中心等交易主体, 在区块链上这些交易主体之间可以自由地定制交易智能合约, 在合约中写入购售电交易的清算、结算规则; 利用会员制身份管理判断交易双方的市场身份, 并匹配对应的智能合约; 用户通过区块链平台自定义智能合约, 实现高效率的电费清算、结算.

如图 3, 将购售电交易电费结算模型用计算机代码表示为智能合约, 并事先写入到区块链的分布式网络体系中; 当合约中的某一事项发生时, 智能合约就会被触发并自动执行相应的合约条款; 会员制服务负责管理网络上的身份识别、隐私与机密. 在合约发生前, 会员制身份管理首先识别交易双方的市场身份, 并匹配对应的智能合约; 同时, 会员机制也保证未授权的第三方不能获悉有关身份、交易模式、交易内容等机密信息.

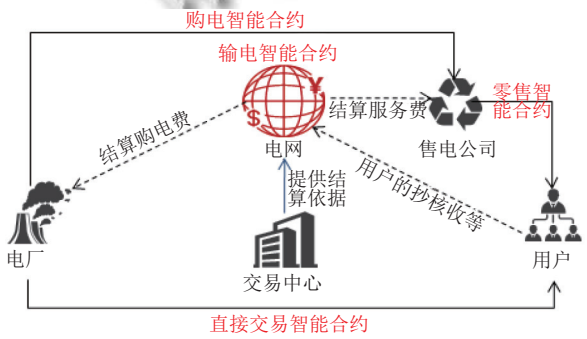

图 3 基于智能合约的电力市场交易模型

2.1 以电网为结算主体的电力市场私有链

由于电能并不是一个普通的数字化商品, 其发电、输电、用电过程需要在平衡供需关系的前提下由电网统一调配. 因此在电网的智能化水平尚未达到一定程度之前, 区块链在电力市场中的应用不可能做到完全的去中心化. 未来随着电网智能化水平的不断提升, 以用户为代表的市场主体去中心化诉求逐步凸显, 区块链的去中心化程度才会逐步提高. 因此笔者认为在输配售一体、输配一体售电分开两种业务模式下, 区块链应用于电力市场首先是电网财务部门内的私有链[14], 逐步向各市场主体渗透形成联盟链, 最终形成分布于各用电终端的公有链[15].

在私有链阶段, 应用区块链对前端交易、营销数据实现分布式的记账存储, 打通财务业务处理各个环节, 实现透明、高效、高审计性的电费清结算. 如图 4, 将交易中心提供的结算依据数据保存在购电费结算区块链, 营销部门提供的用户用电数据保存在售电公司服务费结算区块链, 它们之间通过侧链技术[16]锚定, 从而打通财务业务处理的计划、记账、结算、清分、支付、审计、披露、预测等各个环节, 提高财务数据的透明度和可审计性; 利用区块链自动共享、不可篡改的记录保管方式, 简化数据记录、存储环节, 规避因人为操作造成的错误; 通过智能合约将清算业务结构化, 减少清算过程中的摩擦, 同时实现清算即结算, 提高清算、结算的效率.

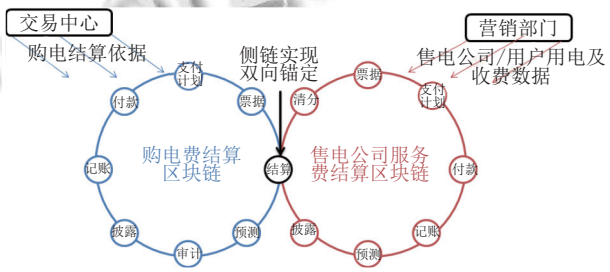

图 4 电费结算的私有链设计

2.2 以电网为结算主体的电力市场联盟链

随着市场对区块链的接受程度、区块链价值的认可程度的提高, 区块链逐步向电力市场的各个主体渗透, 形成电力市场联盟链. 如图 5, 区块链以分布式点对点对等网的方式将电力市场的交易主体 (电厂、售电公司、电网、用户) 连接起来; 用数字化编码将清算结算规则写入区块链, 交易双方可在区块链平台的基础上自定义智能合约; 从达成合约协议开始, 合约中约定的条件事项的发生将自动触发合约的执行程序; 点对点对等网上大部分都是轻量级节点, 保存与合约相关的交易哈希以及简要支付验证所必须的时间戳邻近的交易数据. 这样做的好处是为了保留账本存储容量, 提高处理性能; 全节点类似于一个中心化的数据库, 它保存从第一个区块开始的所有结构化的合约基础数据与交易数据, 同时通过 hash 映射保护用户隐私与交易的机密信息, 保证了数据的不可篡改性. 需要注意的是, 这样的设计保留了中心化数据库, 并没有做到完全的去中心化, 但带来的好处有两个: (1) 提高链上的共识效率; (2) 便于查询、统计、审计等中心化的操作.

2.3 售电平台上的零售智能合约

在新电改配售分离模式下, 以配售电公司为电费结算主体的电力交易将更加灵活、自由. 如图 1 所示的输配分离结算业务模式, 配售电公司通过客户负荷

© 中国科学院软件研究所 http://www.c-s-a.org.cn

预测制定售电计划, 与发电企业、电网公司签订三方购电合同. 由于现货交易、实时交易的存在, 很多情况下难以以纸质形式签约, 而多以电子合同存在. 然而, 电子合同的法律效应、公信力的缺失容易引起分歧. 区块链上的智能合约以代码方式撰写、执行, 一旦签约必然履行, 且区块链的可溯源、不可篡改性可以避免合约纷争, 是配售电公司购电合同的一个良好解决方案.

在售电侧, 配售电公司在区块链售电平台上发布零售智能合约 (如图 6), 电力用户与售电公司在区块链上签署智能合约, 明确电量、协议电价、违约责任等要素. 建立在区块链基础上的智能电表直接把电量记录在分布式账本上, 自动抄表、自动计量、自动计费, 自动履行智能合约, 便于市场交换. 区块链可以使零售电合同透明化、去信度化, 帮助配售电公司提升售电平台的公信力, 提升智能电表抄表的公信力; 同时由于售电平台属于售电公司自己搭建、管理, 因此落地的可能性很大.

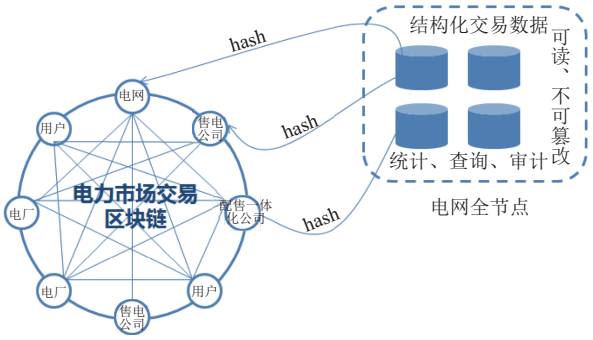

图 5 电力市场交易的联盟链设计

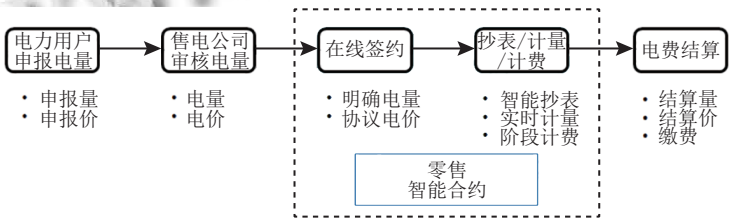

图 6 配售电公司的零售智能合约

3 关键技术难点与实现

智能合约是由尼克萨博早在 1994 年提出的, 但由于缺少可信的执行环境并没有得到应用. 直到 2009 年比特币[2]诞生后, 人们意识到其底层区块链技术可以为智能合约提供可信的执行环境. 然而, 比特币的区块链架构主要围绕去中心化的数字货币, 用来支撑智能合约还非常局限. 例如比特币的区块链平台使用工作量证明共识算法 (Proof of Work, PoW), 在执行时需要每个旷工计算随机数以争夺记账权, 这需要消耗大量的算力, 并且一笔交易的确认至少需要 10 分钟, 达不到商用要求.

近年来, 以以太坊[17]、hyperledger [18]为代表的区块链 2.0 技术的长足发展, 保证了智能合约的高效运行. 本文提出的电费结算智能合约就是基于以太坊开源平台开发的, 与比特币系统比较起来, 在节点的准入机制、传输协议、hash 算法、加密方法、共识机制等方面上有诸多不同, 表 1 给出了主要技术实现上的改进.

3.1 权益证明共识算法 (Proof of Stake, PoS)

比特币采用 PoW, 不仅耗费大量算力, 而且每秒最多只支持 7 笔交易, 效率低下. 本智能合约系统采用 PoW+PoS 的共识机制, 将区块分为 PoW 区块和 PoS 区块两种. 权益 (Stake) 体现为区块链节点对特定数量货币的所有权, 称为币龄或币天数 (Coin age). 在 PoS 区块中, 旷工通过向自己支付并消耗掉特定数量的币龄来获取区块记账权. 整个过程如图 7, 左边第一个输入称为内核 (Kernel), 本质上是一条达成哈希目标的协议, 要求币龄>哈希目标, 其中哈希目标由区块平均权益、未被花费的输出 (Unspent transaction output, UTXO) 和当前时刻共同决定, 而币龄=当前拥有的币数量×最后一次交易的时间.

表 1 技术实现上的改进

	比特币系统	本文的智能合约系统
共识机制	PoW	PoW+PoS
脚本引擎	非图灵完备	图灵完备
存储策略	全节点	全节点+云存储
哈希算法	SHA256+RIPEMD160	SHA3
交易长度	60字节	30字节
支付验证方法	Merkle tree	Merkle Patricia tree
交易平均确认时间	10 min	16 s
安全策略	UTXO	会员制账户

© 中国科学院软件研究所 http://www.c-s-a.org.cn

由此可见, 在生成内核的过程中消耗的币龄越多, 越容易满足哈希目标. PoS 共识过程仅依靠内部币龄和权益而不需要消耗外部算力和资源, 从根本上解决了 PoW 共识算力浪费的问题, 并且能够在一定程度上缩短达成共识的时间.

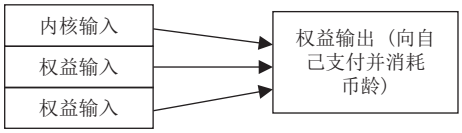

图 7 PoS 的交易结构

3.2 图灵完备计算环境

比特币系统从安全角度出发, 其脚本引擎非图灵完备, 因此目前能通行的比特币脚本指令不多, 应用场景仅限于数字货币. 本文的智能合约系统基于图灵完备的 256 位计算环境-以太坊虚拟机 (EVM), 可以进行任何种类的计算, 从而支持智能合约的运行.

EVM 中运行智能合约需要消耗 Gas(即执行的代码受参数 Gas 的严格限制), 规定了可运行计算指令的上限, 从而避免无限循环. 假设整个网络状态为 σ, 合约运算剩余的 Gas 为 g, 区块链运行环境中的重要信息保存在元组 I(当前合约地址, 合约发起者地址, 本次交易的 Gas 价格, 交易输入数据, 执行合约的账户地址, 合约账户余额, 当前区块头, 当前 CALL 操作和 CREATE 操作数) 内, 系统状态转移函数记为ψ, σ'为系统运行后状态, g'为运行后剩余 Gas, s 为执行终止操作的合约列表, l 为记录序列, r 为运行后返还的 Gas, o 为合约产生的输出, 则整个状态转换可表示为:

$$(\sigma', g', s, l, r, o) = \psi(\sigma, g, l) \quad (1)$$

在大多数情况下, ψ被定义为不断迭代系统临时状态和虚拟机临时状态的过程, 迭代的终止由以下两个条件决定:

(1) 系统状态出现异常使得 EVM 停止工作, 例如 Gas 不足、指令无效、虚拟机堆栈不足等情况;

(2) EVM 执行完所有指令并返回结果, 正常停止.

在每一次迭代过程中, 智能合约的指令被压入堆栈, EVM 按堆栈索引执行指令. 每执行一条指令就支付相应的的 Gas, 直到所有指令执行完毕, 堆栈被清空; 若遇到异常, EVM 则停止工作并逐层向上返回.

3.3 P2P 网络上的 Whisper 协议

智能合约运行在一个点对点对等 (P2P) 网络上, DApp 间采用 Whisper 通信协议. Whisper 结合了 DHT 和数据包消息系统, 是一个纯标志消息系统, 提供低层次但易用的 API, 不需要记忆底层硬件属性[19]. 另外, 有一个每条可配置的生存时间以及签名/加密规则, 提供多索引、非单一的记录.

Whisper 不是一个典型的通信系统, 其主要目标是给新型的应用开发模式提供一个新的通信协议, 而非简单地在两个节点间传输数据. Whisper 使用多播和和广播场景协议, 采用低层次部分异步通信, 降低低价值流量与延迟, 从而支持大规模多对多数据发现和完全的隐私保护. Whisper 的运行机理如下:

(1) DApp 发布合约内容, 广播至 P2P 网络;

(2) DApp 发信号给其他 DApp, 希望它们参与对某个交易的协同 (如签署智能合约);

(3) DApp 提供非实时的通信内容;

(4) 除了交易双方的哈希地址, Whisper 协议隐藏其他交易信息.

3.4 并行存储策略与数据上链方法

电力市场交易结算智能合约的设计思路是在不改变原有业务架构的前提下并行一个区块链账本, 因此需要解决数据库到区块链的数据同步问题. 从交易中心数据库到购电费结算区块链的数据同步有两种, 一种是采用 ETL 方式连接交易中心数据库与区块链, 在 ETL 工具上实现交易数据采集脚本, 由 ETL 工具定时从交易中心数据库抽取购电费结算数据, 完成数据抽取之后, 将抽取数据进行一定的清洗, 通过区块链 RPC 接口以交易的方式实时提交到区块链上; 另一种方式是, 通过 ETL 工具对接交易中心数据库的日志系统, 实现实时日志分析, 根据 ETL 上预设的采集规则对需要采集的数据进行实时抽取, 将抽取数据进行一定的清洗之后, 组装成区块链交易单, 放入区块链前端消息队列, 通过区块链 RPC 接口提交到区块链上.

基于 ETL 工具的数据同步流程如图 8.

4 实验与结论

本部分通过在区块链上发布一个购售电合同的智能合约实例, 分析区块链系统运行的正确性、稳定性和效率. 该合同根据约定的购售电量和实际实施的购、发电量之间的关系, 做出如下约定:

约定 1. 甲方年度实际购电量高于年度合同约定电量的 105% 时, 直接交易结算电量为甲方年度合同约

© 中国科学院软件研究所 http://www.c-s-a.org.cn

定电量×105%, 超出部分按照对应电压等级的大工业目录电价×110% 结算.

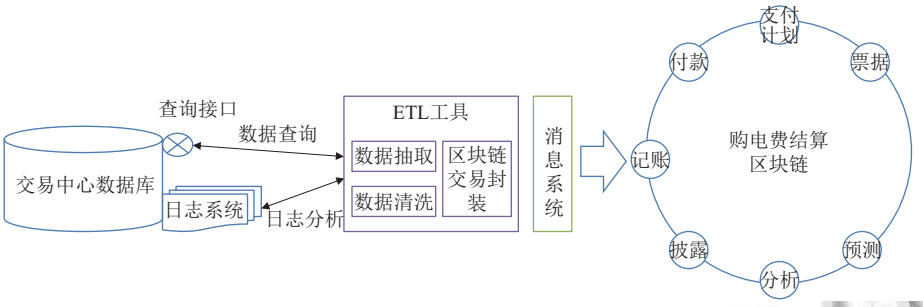

图 8 数据写入与同步方法

约定 2. 甲方年度实际购电量低于年度合同约定电量的 95% 时, 直接交易结算电量为甲方年度实际购电量. 对低于年度约定购电量×95% 的差额电量, 甲方按电量差额乘以 2 分/千瓦时 (含税, 下同) 的标准向乙方支付违约金, 违约金计算式为: (月度约定购电量×95%-当月实际购电量)×2 分/千瓦时.

约定 3. 如果乙方因设备故障等原因导致当月全部上网电量低于约定直接交易电量的 95%, 低于部分电量由乙方按甲方相应的目录电价与直接交易到户电度电价的差价向丙方支付补偿金. 补偿金计算式为: (甲方月度约定购电量×95%-乙方当月实际上网电量)×(甲方目录电价-甲方直接交易到户电度电价).

图 9 是用 solidity 语言编写的智能合约实例, 其中图 9(a) 是约定 1、约定 2 的智能合约实例, 图 9(b) 是约定 3 的智能合约实例. 由图可见对于售电方发电充足、售电方发电不足、购电方的购电量上下浮动等多种情况都用计算机编码写成了规则, 并存放在区块链上. 购售双方一旦在区块链上签名, 该合约就会根据智能电表的抄表情况自动履行.

表 2 是在一个由 4000 个结点构成的 P2P 网络中执行该智能合约的结果. 在一周时间内, 共签署了 7129 个智能合约, 其中顺利履约的由 7085 个, 失效的合约有 44 个, 成功率约为 99.38%. 合约失效的原因主要是购电方的保证金不足或合约发布方的 Gas 耗尽. 同时, 合约履行时每笔支付的平均交易确认时间约为 16 秒.

与原来的双边合同相比, 由分布式记账本管理的能源零售市场增加了配售电公司和用电用户的选择权, 合约内的多余电量不仅可以存于电池备用, 或返回给电网, 还可以出售给网络里出价最高的买家, 甚至异地赎回 (如给在行驶的电动车充电) 等. 通过建立在区块链上的智能合约, 可以数字化、智能化地完成售电公司的切换, 用电用户只需在电脑或手机上点击几次, 就可以便捷地完成供应商的更换. 由此可见, 区块链技术能推动能源零售市场的智能化, 使得公民在能源零售市场中发挥更大的作用. 利用区块链技术, 用电成本和需求数据能及时地反映在一体化的能源市场上, 帮助公民做出正确的决策, 鼓励公民积极参与能源市场, 简化能源供应合同的切换. 区块链技术帮助能源生产者和能源消费者共同制定因需求而动态变化的能源价格, 保证不同市场的互联互通性, 使电网中的能源用户真正获得收益. 通过分布式发电、智能电网和储能技术, 居民可以通过区块链参与能源的生产和销售, 降低电费开支.

5 结束语

本文研究了区块链技术在能源互联网尤其是电力行业的应用, 包括市场电费结算与区块链技术的匹配度分析、区块链技术应用于电力市场电费结算、购售电智能合约的解决方案以及关键技术难点与实现. 通过在由 4000 个节点构成的 P2P 网络中运行一个购售电合同的智能合约实例, 验证了本文方法的成功率约为 99.38%, 每笔交易的平均确认时间约为 16 秒. 利用运行在区块链上的智能合约降低电力市场交易的信任成本, 提高清结算效率, 同时推动能源零售市场的智能化. 如果本文方法得到应用, 将帮助能源交易双方共同制定因需求而动态变化的能源价格, 保证不同能源市场的互联互通, 促进智慧能源价值互联.

今后的工作应聚焦于如何改善共识算法的效率、如何建立一套逻辑严密、可定制的智能合约, 以适应电网结算业务流程规则复杂, 结算合同类型多的特点, 以及当区块链上有异常行为发生时如何快速、有效地熔断, 以保护用户利益不被侵犯. 只有在解决了高冗余

© 中国科学院软件研究所 http://www.c-s-a.org.cn

数据的资源占用、共识的算力与时间耗费、政策与法律等问题之后, 区块链技术才能得到大规模的应用.

```
contract PurchasingElectricity
{
    //售电方数据结构
    struct Saler
    {
        address sale   //售电方地址
        uint plan_quantity;  // 计划购电量
    }

    uint public value_1; // 目录电价
    uint public value_2; // 用户电价
    address public punchase;  // 购电方地址
    address public transport; // 传输方地址

    mapping(address => Saler) public salers; //售电方


    function PurchasingElectricity(address _sale, uint _plan_value; uint _plan_quantity,
                                   address _transport, uint _value1, uint _value2)
    {
        punchase = msg.sender;
        salers[_sale].sale = _sale;
        salers[_sale].plan_quantity = _plan_quantity;

        transport = _transport;

        value_1 = _value1;
        value_2 = _value2;
    }
```

(a) 约定1、约定2的智能合约实例

```
    //售电方发电足额的情况
    function payment_a(address sale, uint actual)
    {
        if(actual > salers[sale].plan_quantity*1.05)  // 甲方年度实际购电量高于年度合同约定电量的105%时
        {
            value = (actual - salers[sale].plan_quantity*1.05)*(value_1*1.10);
            Send(punchase, sale, value);
        }
        if(actual < salers[sale].plan_quantity*0.95) // 甲方年度实际购电量低于年度合同约定电量的95%时
        {
            value = (salers[sale].plan_quantity*0.95 - actual)*2;  //（月度约定购电量×95%-当月实际购电量）×2分/千瓦时
            Send(punchase, sale, value);
        }

    }

    //售电方发电不足额的情况
    function payment_b(address sale, uint actual)
    {
        if(actual < salers[sale].plan_quantity*0.95) //乙方因设备故障等原因导致当月全部上网电量低于约定直接交易电量的95%时
        {
            value = (salers[sale].plan_quantity*0.95 - actual)*(value_1 - value_2);
            Send(sale, transport, value);
        }
    }
}
```

(b) 约定3的智能合约实例

图 9　一个购售电合同的智能合约

表 2　智能合约执行情况

日期	合约签署数	合约执行数	合约失效数
2017.3.1	1339	1334	5
2017.3.2	2113	2097	16
2017.3.3	1337	1326	11
2017.3.4	727	725	2
2017.3.5	308	308	0
2017.3.6	1215	1206	9
2017.3.7	90	89	1
合计	7129	7085	44

参考文献

1 国家发改委, 国家能源局. 《关于推进售电侧改革的实施意见》节录. 大众用电, 2016, (4): 5–6.

2 Nakamoto S. Bitcoin: A Peer-to-peer Electronic Cash System. Satoshi Nakamoto Institute, 2008.

3 龚鸣. 详解纳斯达克区块链私人股权市场 Linq. http://mt.sohu.com/20151122/n427544175.shtml. [2015-11-22/2015-11-25].

4 Mattke S. Overstock.com macht Ernst: Erste Blockchain-Anleihe Emittiert, Weitere Sollen Folgen. Preisvergleich, 2015.

5 Marinelli G. Goldman sachs moves to Blockchain: SETLcoin. http://themarketmogul.com/goldman-sachs-moves-to-blockchain-setlcoin/. [2016-09-06/2016-12-30].

6 Ripple. Consensus whitepaper: A novel consensus algorithm| Ripple. https://ripple.com/consensus-whitepaper/. [2017-08-29].

7 龚鸣. 从 R3 区块链联盟看欧美金融巨头的区块链探索之路. 当代金融家, 2016, (6): 101–105.

8 国务院. 国务院关于印发“十三五”国家信息化规划的通知. http://www.gov.cn/zhengce/content/2016-12/27/content_5153411.htm. [2016-12-27].

9 工业和信息化部. 中国区块链技术和应用发展白皮书(2016 版). https://img2.btc123.com/file/0/chinabolckchaindevwhitepage2016.pdf. [2016-10-18].

10 任安军. 运用区块链改造我国票据市场的思考. 南方金融, 2016, 1(3): 39–42.

11 国务院办公厅. 关于进一步深化电力体制改革的若干意见. https://wenku.baidu.com/view/7a04cf8cf61fb7360a4c6538.html. [2015-03-23].

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

13 Watanabe H, Fujimura S, Nakadaira A, *et al*. Blockchain contract: Securing a blockchain applied to smart contracts. 2016 IEEE International Conference on Consumer Electronics. Las Vegas, NV, USA. 2016. 467–468.

14 Morrison A. Blockchain and smart contract automation: Private blockchains, public, or both? http://www.pwc.com/us/en/technology-forecast/2016/blockchain/pwc-smart-contract-automation-private-public.pdf. [2016-12-01/2016-12-30].

15 Walch A. Open source operational risk: should public blockchains serve as financial market infrastructures. Handbook of Digital Banking &Internet Finance, http://works.bepress.com/angela-walch/3/, 2016.

16 Back A, Corallo M, Dashjr L, *et al*. Enabling blockchain innovations with pegged sidechains. https://www.blockstream.com/sidechains.pdf. [2014-10-22].

17 Buterin V. Ethereum White Paper. https://ethereum.org/pdfs/EthereumWhitePaper.pdf. [2013].

18 Hull R, Batra VS, Chen YM, *et al*. Towards a shared ledger business collaboration language based on data-aware processes. International Conference on Service-Oriented Computing 2016: Service-Oriented Computing. Cham. 2016. 18–36.

19 邹均, 张海宁, 唐屹, 等. 区块链技术指南. 北京: 机械工业出版社, 2016: 102–103.

© 中国科学院软件研究所 http://www.c-s-a.org.cn