清　华　大　学

博 士 后 研 究 工 作 报 告

区块链在能源互联网中的应用研究

Research on the Applications of Blockchain in Energy Internet

艾　崧　溥

工作完成日期　2019 年 7 月—2021 年 10 月

报告提交日期　2021 年 10 月

清　华　大　学　（北京）

2021 年 10 月

区块链在能源互联网中的应用研究

Research on the Applications of Blockchain in Energy Internet

博　士　后　姓　名:　　艾崧溥

流动站（一级学科）名称:　　计算机科学与技术

专　业（二级学科）名称:　　计算机软件与理论

合　　作　　导　　师:　　邢春晓（研究员）

研究工作起始时间　2019 年　7 月　9 日

研究工作期满时间　2021 年 10 月 31 日

摘要

本研究报告主要在分析讨论能源互联网中区块链的研究现状的基础上，以能源互联网分布式电力交易为场景进行应用研究。研究工作从现有电力系统出发，逐步探索实现能源互联网分布式电力交易所需的区块链技术并开展针对性研究。

本报告的主要研究结果如下：

1. 提出基于区块链的能源互联网分布式电力交易系统的架构及功能模块，并构建链上异步结算存证方案，采用链下签约，链上自动化记录交易与结算的形式，适配现有中心化交易基础设施，实现在中心化交易所监管下的分布式自动交易与结算。
2. 使用 K-prototypes 聚类的相异度算法，提出一种考虑多因素的分布式电力交易撮合机制及相应交易系统，基于智能合约设计自动匹配、签名确认等功能，为售、购双方提供自动化撮合与可控匹配；基于零知识证明和同态加密方法设计电力交易的隐私保护方法和算法实现，实现去中心/多中心场景下的分布式电力匹配与交易。
3. 基于线性多目标优化方法提出一种支持拆分买卖需求的多属性偏好电力撮合机制，更加灵活地对分布式电力交易售、购需求提供撮合服务；设计电力交易全流程区块链链上实现的交易方案，实现分布式场景下的电力自动撮合、交易与结算。
4. 围绕能源互联网分布式电力交易区块链对共识机制的需求，提出耦合业务场景设计共识机制的研究思路，设计面向未来能源互联网分布式电力交易场景的分级异步共识架构，以 PBFT 结合声誉机制为例，针对设定场景进行具体共识机制的设计与验证。

关键词：能源互联网，区块链，分布式电力交易，交易匹配，共识机制

Abstract

Mainly based on the survey of the current research status of blockchain in the energy Internet, the application research conducted in this report is focused on the applications of blockchain in energy Internet, adopting the energy Internet distributed electricity trading as a scenario. The research is gradually explored and realized the blockchain technologies from the existing electricity system towards energy Internet to realize distributed electricity trading.

Solutions presented in this report can be summarized as follows:

1. The architecture and functional modules of a blockchain-based energy Internet distributed electricity trading system is proposed. An on-chain asynchronous settlement scheme is designed, adopting the form of signing off-chain and automatically recording transactions and settlements on-chain. The proposed system suits for the existing centralized trading infrastructure to realize distributed automatic trading and settlement based on the supervision of centralized exchanges.

2. Using the dissimilarity algorithm of K-prototypes clustering, a distributed electricity transaction matching mechanism considering multiple factors and corresponding trading system are proposed. Based on smart contract, automatic matching, signature confirmation and other functions are provided for both sellers and purchasers for automated matching and controllable matching. Privacy protection methods and algorithm implementations for power transactions are designed based on zero-knowledge proof and homomorphic encryption methods. Distributed electricity matching and trading in decentralized/multi-center scenarios are realized.

3. Based on the linear multi-objective optimization method, a multi-attribute preferential power matching mechanism that supports splitted buying and selling needs is proposed. It is more flexible to provide matching services for distributed electricity selling and buying needs. The whole process of on-chain electricity trading is designed. The automatic matching, trading and settlement in distributed scenario are realized.

4. Focusing on the demand for consensus mechanism of distributed electricity transaction blockchain of energy Internet, the research idea of designing consensus mechanism to couple business scenarios is put forward. A hierarchical asynchronous consensus architecture for future energy Internet distributed electricity trading scenarios

is proposed. A specific consensus mechanism combining reputation mechanism with PBFT is designed and verified as an instance.

Keywords: Energy Internet, Blockchain, Distributed Electricity Trading, Transaction Matching, Consensus Mechanism

目录

英 文 缩 写 表

EI	Energy Internet.	能源互联网
REI	Regional Energy Internet	区域能源互联网
ER	Energy Router	能量路由器
MG	Microgrid	微网
P2P	Peer-to-peer	点对点
PoW	Proof of Work	工作量证明
PoS	Proof of Stake	权益证明
DPoS	Delegated Proof of Stake	委托权益证明
PBFT	Practical Byzantine Fault Tolerance	实用拜占庭容错
MBT	Maximum Block Batch Time	最大区块批处理时间
MMC	Maximum Message Capacity	最大消息容量
DA	Double Auction	双重拍卖
APET	Actual Unit Price of Electricity of The Single Transaction	单笔交易电力实际单价
CMAP-Matching	Transaction Matching Mechanism that Considering Multi-Attribute Preferences	考虑多属性偏好的交易匹配机制
HFPI-Matching	Two-Side Matching Decision-Making Model with Hesitant Fuzzy Preference Information	具有犹豫模糊偏好信息的双边匹配决策模型

第一章 绪论

1.1 能源互联网区块链中的关键技术

1.1.1 引言

近年来，能源行业形势日趋复杂，光、风、热等清洁可再生能源迅速发展，现有的能源架构难以满足不断增长的能源消耗和多样化的能源产销需求，一场能源行业的革新势在必行。能源互联网作为“第三次工业革命”的重要标志之一[1]，通过融合互联网技术和分布式可再生能源技术来构建新型能源供需架构，获得了广泛的关注。

能源互联网是一个学术与工业界看好的下一代能源基础设施的发展方向[2-5]，其开放、互联、对等、分享的基本特征及蕴含的全新能源生产、使用理念和商业模式，对能源和信息的互联、共享提出了更高的要求。然而，现有的能源运营体系与成熟的技术堆栈难以满足全面实现能源互联网的设计思想。特别地，我国的能源，尤其是电力体系架构一直以来以中心化为主轴的设计思路难以为丰富的清洁能源分布式接入与多样化产销耦合提供灵活地架构支撑，随着用电负荷加大，在冬夏季高峰时可能出现故障甚至停运[6]。引入新的设计思路与技术堆栈，在现有能源体质下进行场景、业务、价值创新，建设分层级分区域，多元接入的能源互联网架构成为当下学界与工业界研究的热点方向之一[7]。

区块链作为一种具有去中心化、点对点传输、可追溯、集体维护、可编程和安全可信等特点的技术堆栈，其设计思想核心即为区块链网络中各节点平等，网络中节点在互联的基础上相互合作、制约，共享信息，而整个架构由区块链网络中的节点共同维护的。可以发现，区块链技术与能源互联网的设计思想高度契合，很有可能会成为能源互联网真正落地的关键技术。区块链技术在能源互联网大量的用户之间建立安全自主的能源交易渠道，实现一个自组织、自调节的能源系统，将极大地提高能源使用效率、降低管理成本[8]，实现能源互联网的高效运行。

在电力交易场景中，利用与场景耦合的区块链共识机制、智能合约技术，通过点对点交易，可有效解决电力交易双方信息不对称导致的信任缺失问题[9]。同

时，基于区块链的电力交易可从交易侧解决多方信息不对称带来的信任危机，构建多层级公平公开的电力交易市场化交易环境，提升电力交易市场主体的参与水平，实现市场交易效率的最大化。目前,已有一些文献对当前能源电力交易相关的区块链研究进行了综述[10-13]。然而，很多已有的综述文献多聚焦于能源互联网电力交易区块链的应用场景，对于电力交易区块链中的关键技术缺乏系统的分析和讨论，难以从技术的角度对电力交易区块链研究与发展提出有效的建议。于是，本节面向电力交易场景，通过定位电力交易区块链中的关键技术，对电力交易区块链共识机制、交易与智能合约设计、安全机制和其他领域技术等方面的研究进展进行综述，并结合发展现状进行深入地讨论与分析，探讨目前各项技术领域存在的问题，以及未来可能的研究方向，为能源区块链的进一步研究与落地提供参考。

1.1.2 相关背景

能源互联网

能源互联网的概念由美国学者杰里米·里夫金于 2011 年在其著作《第三次工业革命》中提出[1]。能源互联网是以互联网理念为基础构建的新型信息—能源融合网络体系，它以大电网为“主干网”，以微电网、分布式能源、智能小区等为“局域网”[14]，以开放对等的信息——能源一体化架构为基础实现能源的双向按需传输和动态平衡使用，可以最大限度的适应新能源的接入。

构建开放、互联、对等、分享的能源互联网基础设施，各个设施主体在局域网和广域网的范围内广泛连接，能量自治单元之间地位平等，施行分散化的调度和管理，形成价值驱动、用户中心的能源互联网应用模式，是能源互联网的基本要求。能源互联网的组成如图 1.1 所示。在能源互联网的场景中，信息与能量的高度流通，也催生了价值的流动。通过在分布式能源、局域微电网和公共电网等主体之间，建立起自由、灵活的能源市场，以满足能源的合理化配置；利用智能电表、能量路由器[15]等传感通信设备实现智能计量和实时决策，提升用户数据精确度和用户业务效率；采用自动化需求响应、线路阻塞管理和潮流约束等手段维持网络平稳运行；同时，结合大数据、人工智能等技术对能源交易数据进行分析，进一步发掘能源互联网的深层价值[16-18]。

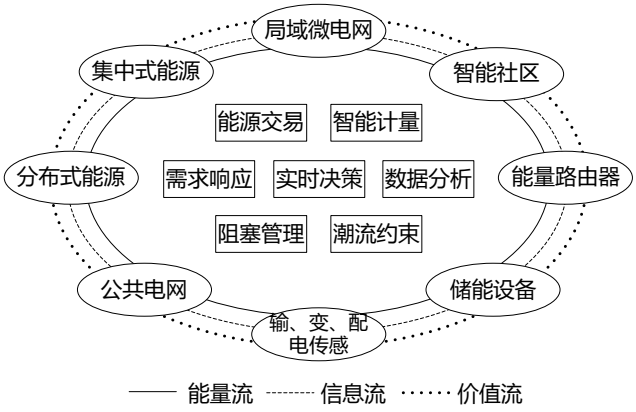


图 1.1.　能源互联网组成示意图

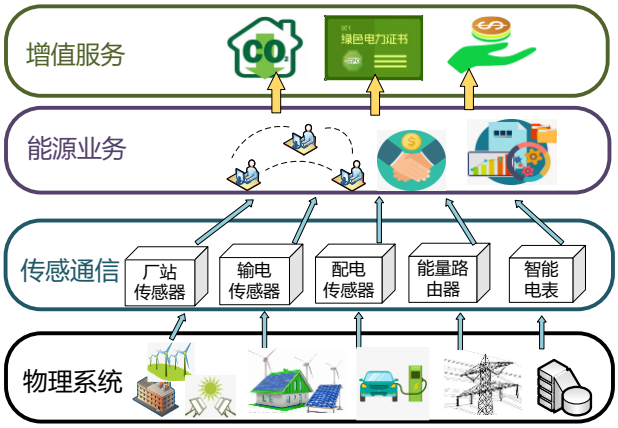


图 1.2.　能源互联网层次功能图

如图 1.2 所示，从层次功能来讲，能源互联网一般可以分为 4 个层次：第一层为物理系统层，主要包括组成能源互联网的基础设施，例如电厂、清洁能源发电设备、输变电设备、充电桩、储能装置和用电负荷，以及服务器、移动设备和基站等；第二层为传感通信层，主要包括厂站传感器、输电传感器、配电传感器、能量路由器和智能电表等设备，负责采集和传输物理系统层的数据与信息；第三层为能源业务层，该层运行在各能量自治单元的终端之上，主要负责执行分散化的自治决策，满足用户产能、用能和交易的业务需求；第四层为增值服务层，主要为用户提供绿证、碳排放权等用能增值服务，以及能源金融产品等。

区块链

区块链是一种去中心化的分布式数据账本的技术[19]。区块链网络由多个对等节点组成，所有节点共同维护一个公开的数据账本，账本中的记录由区块间的链式结构按时序严格排列，每个节点都可以完全拥有该账本，账本数据通过共识机制达成一致。

去中心化是区块链最主要的特征。在合理机制的支持下，区块链系统比中心化系统更加稳定可靠，单一节点的故障问题不影响整个系统的平稳运行。高冗余度的分布式存储使得区块链具有防篡改、可追溯的特性，再结合数字签名等密码学算法，使得数据更加安全可信。区块链集成了一系列的关键技术，包括共识算法、智能合约、密码学算法等，此外还包含激励机制、数据库和 P2P 通信等技术，是多个领域技术结合的产物。

根据侧重点不同，区块链发展出了多种类型，包括公链、联盟链和私链等。公链是区块链最早的形态，其对应的场景中用户之间完全没有信任，奉行完全去中心化、节点完全对等的原则，对节点数量也没有要求；联盟链是为具有一定是信任基础的应用场景而设计的，共识过程由可信的、数量确定的一组节点完成，由于存在信任差距，内部的节点往往会在权限上有所区别，并非完全对等；私链则是某个单位或组织内部应用的系统，系统内所有节点均受同一个单位或组织的控制。

基于去中心化的设计理念和成熟的技术手段，区块链在数字资产、数据存储、数据鉴证、金融交易和可信计算等方面具有显著的作用[20]，可以帮助各行业解决相关问题，尤其是涉及到价值流动的应用场景，比如能源交易、供应链金融、版权认证和保险评定等。应用于能源互联网电力交易场景的区块链技术——电力交易区块链，是本节综述的主要内容。

1.1.3 电力交易区块链

欧盟工业界认为，能源区块链是区块链技术的一个重要应用场景[21]。能源互联网与区块链都具有分布式、去中心化的特征，能源互联网强调的开放、互联、对等和分享的设计理念与区块链去中心化、共同维护、地位平等和数据共享的特性高度契合。基于区块链技术的技术架构可以保证能源互联网中个体用户的地位平等，并实现用户之间的 P2P 能源及能源相关信息交易，从而实现能源互联网的价值驱动，建立新的能源价值体系。

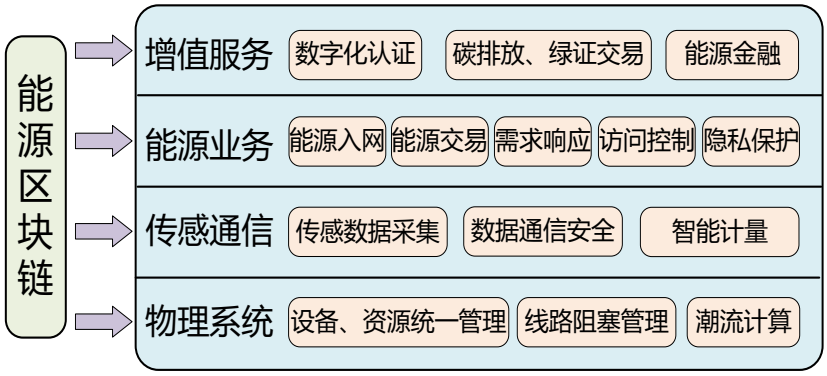


图 1.3.　能源区块链应用层次图

本报告认为，区块链可以帮助能源互联网的各个层次构建相关的应用，分别或联合地构建能源区块链，具体应用场景如图 1.3 所示。

物理系统层：区块链可以辅助能源互联网进行物理设备和其他资源的统一管理，保障设备资源的安全稳定；区块链还可以通过智能合约对电力传输进行安全校核与阻塞管理，保障传输线路的优化畅通；区块链能够根据电力网络的拓扑结构和各设备的参数指标，实时地进行潮流计算，保障电力物理系统的安全。

传感通信层：针对能源传感数据的采集制定对应的智能合约，使得能量路由器可以定期自动化采集传感数据并上传到区块链；区块链节点之间采用加密算法对数据进行加密通信，保证了数据通信的安全性；针对能源的生产和消费过程，区块链与智能电表等设备相结合，根据各个终端的能源生产、消费状况进行智能化计量，保障了计量数据准确、不被篡改。

能源业务层：智能合约可以自动化准确地执行能源入网、能源交易等复杂的系统流程；在需求侧管理方面，区块链能够辅助完成自动化的需求响应，对分布式的能源用户来讲更加快捷简便；区块链安全特性可以用于能源系统的身份认证和访问控制，以及保护用户的隐私。

增值服务层：区块链可以为用户在能源互联网中的行为提供数字化认证，以满足各方需要；应用区块链可以更好地推行绿证和碳排放权等政策实施，甚至实现绿证和碳排放权的自由交易；区块链可以对能源产品的生产、购买过程进行担保，从而促进能源产品的金融化。

作为能源区块链场景之一，电力交易属于能源互联网架构的第三层级——能源业务层。在绿色能源广泛去中心化接入电网，电动车反向供电等技术逐步成熟的趋势中，区域点对点交易需求日渐增多，构建去中心化点对点可信安全的区域

交易平台是电力交易区块链的发展方向。同时，随着物联网技术传感通信控制技术的发展，电力系统在时间、空间维度上进行监管控制的粒度逐渐细化，将物联网、大数据、人工智能等技术以适当的方式嵌入电力交易区块链堆栈可以自动化、批量化地快速执行电力系统监管与控制，提升效率。从能源互联网的角度思考，电力交易需要用到传感通信层提供的数据，且需要使用区块链交易结果对物理系统层进行精细化管控制，在不同电网物理架构下，交易需求、特征复杂，为研究提供了丰富的场景。

在电力交易场景，已有不少与区块链相关的应用与研究。早期，LO3 Energy(New York, USA)和西门子(Munich, Germany)合作开发了基于区块链的交易型网格微电网交易平台[22]，用户可以在平台上自由地进行能源交易而不依赖于第三方机构，但是该平台没有适合交易方的竞价策略模型和基于区块链数据的直接结算功能。文献[23]介绍了区块链技术在提高能源交易处理效率方面的新进展，以及结合了区块链技术的分布式能源交易理论研究与实际应用；分析了国内外区块链技术在能源交易方面的研究现状，并给出了中国在区块链参与消纳分布式能源、建设需求响应管理等方面的建议。Luo 等人基于区块链技术提出了一种代理者联盟机制[24]，能源生产者形成电力交易联盟进行电力交易谈判，电力交易数据通过智能合约技术将电力交易数据上链存储，并基于区块链中的电力交易数据进行交易结算。这些项目和研究工作对于区块链技术在能源行业中应用来讲，无疑具有巨大的示范和推进作用，然而这些项目大多还处于理论和试验阶段，如何构建完善的能源区块链体系，还需要对实际应用中的问题进行深层次的考虑和研究。

现阶段，我国能源电力部门正在在电力交易区块链技术路线方向上逐步达成共识，基于电力交易对参与者准入，数据、信息、交易安全性等方面的特性，联盟链作为一种可实名、可监管的技术路线方向逐渐成为主流。

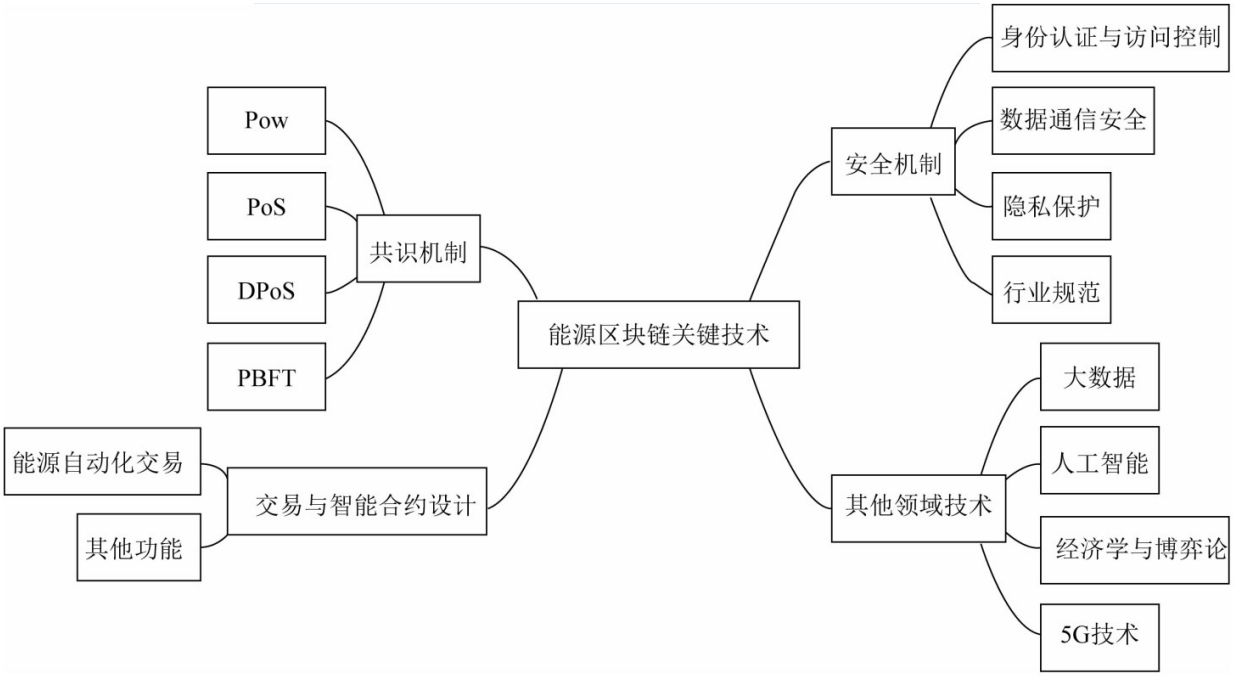


图 1.4. 能源区块链关键技术构成

总体来讲，目前已有的电力交易区块链技术研究，既包含区块链技术应用模式的探索，也包含面向应用过场景的对区块链技术的深入研究[8]。这反映出当前区块链技术堆栈在电力交易领域研究的阶段性特征，即具体应用业务场景还需明确，特征性价值框架还未建立，且区块链作为一个技术堆栈本身还需要丰富并需要针对电力交易场景进行针对性创新。

本节从区块链的技术特征角度出发，结合当前的研究现况，认为目前电力交易区块链堆栈的关键技术探索主要有以下四个方向：共识机制，交易与智能合约设计，安全机制和其他领域技术，具体技术要点如图 1.4 所示，共识机制主要包括 PoW、PoS、DPoS 和 PBFT 等 4 种，交易与智能合约设计主要包括能源自动化交易和其他功能等 2 方面，安全机制主要包括身份认证与访问控制、数据通信安全、隐私保护和行业规范等 4 方面，其他领域技术主要包括大数据、人工智能、经济学与博弈论和 5G 技术等 4 方面。接下来本节将从这四个方向出发，分析当前能源区块链的发展现状和问题，以及探讨各技术领域下一步的研究趋势。

1.1.4 能源区块链中的共识机制

基于分布式的特性，能源互联网经历了从最初的中心化系统到去中心化系统的发展，根据特征性场景针对性设计，又衍生出微电网、区域能源互联网等能源

网络。区块链作为分布式账本，与能源互联网分散化的拓扑结构高度契合，各能源主体可通过共识机制来保证能源交易数据的一致性。

共识机制作为区块链技术的一部分，也符合能源互联网的发展脉络。目前基于区块链的能源项目研究所采用的共识机制主要包括 PoW、PoS、DPoS 和 PBFT 等几种，以及在其基础上改进的共识机制。针对能源互联网的发展，目前共识机制相关按研究可主要分为 3 个阶段，（1）针对能源互联网去中心化的特征，采用 PoW、PoS、DPoS 等通用性的共识机制，保证了各能源节点中交易数据的一致性；（2）针对电网特性，采用 PBFT 及其改进的共识机制，在抵抗拜占庭攻击的同时，提高了共识效率；（3）针对不同的能源网络场景，制定针对性共识机制，以保证能源交易的共识效率和存储准确性。

PoW

在能源区块链中共识机制研究的第一阶段，共识机制的重点在于保证分布式场景中节点数据的一致性，多采用通用性的共识机制。例如：文献[25-27]采用 PoW 共识能源交易数据，保证各节点记账的平等性和节点数据的一致性，但是 PoW 耗费大量算力，造成能耗问题。针对 PoW 的能耗问题，部分研究通过转移算力计算目标[28]或减少共识节点[29]的方式来解决，前者中未获得记账权的节点依旧会消耗大量算力，并没有从根本上解决 PoW 的能耗问题；后者降低了系统的去中心化程度，少数节点保存能源交易数据，不适用于未来特定能源网络的场景。

PoS 与 DPoS

针对 PoW 的能耗问题，部分研究采用 PoS 共识机制来解决。例如：文献[30]基于 PoS 提出了 ESCA、ETCA 和 EICA 三种共识机制，分别对应存储三种不同能源交易数据的区块链；文献[31]基于 PoS 将交易量和交易金额作为“权益”代替币龄，由调度中心节点进行共识；文献[32]基于交易模式的不同，提出了适用于综合能源服务场景的权益分享证明（PoSS）共识机制。针对 PoW 的共识效率问题，部分研究采用 DPoS 共识机制牺牲部分去中心化程度以换取共识效率[33][34]，例如：文献[35]将能源交易量作为“权益”，选取交易量大的账户轮流担任记账节点；文献[36]将碳排放权或绿证作为“权益”，选取超级节点进行记账。

以上共识机制，虽然避免了 PoW 的能耗问题，但是，交易数据分散共识、分链存储，增大了存储空间和数据溯源的难度。此外，“权益”积累降低了系统的

去中心化程度，易形成超级节点，易造成节点间权利不对等，削弱了能源互联网的去中心化程度，可能导致能源互联网退化为中心化系统。

PBFT

针对某些特定的能源应用场景，例如微电网等，其中能源主体数量较少且无监管中心[37][38]，能源交易量较少，选用 PBFT 共识机制，在所有能源节点地位平等的前提下，提高了能源交易的共识效率；某些微电网中可能存在默认可信节点，例如：需要能源监管主体[38]对能源交易进行监管，或通过数据中心[39]总览数据，则其对应的节点必然是可信节点，部分研究针对此类微电网场景[40]，将可信节点作为共识节点，基于 PBFT 机制对能源交易数据进行共识，该方式减少了共识节点的数量，极大地提高了能源交易数据的共识效率。

在无默认可信节点的微电网中，随着能源接入主体的增多，因 PBFT 机制 3 段式的频繁交互，导致共识效率的显著下降，因此，PBFT 机制的应用仅局限于节点数量较少的微电网场景。

在具有默认可信节点的微电网中，选取定量可信节点参与共识，在一定程度上减缓了因节点数量增加导致的 PBFT 共识效率降低的问题，但是，公开确定的节点易成为被攻击的目标，并且预先指定共识节点的方法，不仅牺牲了能源互联网去中心化的特性，也难以保证共识节点的长期可信。

针对 PBFT 机制中节点的可信性问题，文献[41]采用 BP 神经网络构建区块链节点信用模型并选举信用最高的节点作为主节点，降低了拜占庭节点作为主节点的概率，但是该方法同样面临节点增多导致共识效率降低的问题。

区域能源互联网共识机制研究

针对能源互联网分布式电力交易实际落地的场景，共识机制的设计应考虑节点数目、去中心化程度、数据一致性和共识效率等因素，现阶段迫切需要一种在能源主体增多时，能保证共识效率的去中心化共识机制，并且同时能够保证共识结果的一致性。例如，在笔者的研究[41]中，耦合场景特点针对性设计共识机制，借鉴信誉模型的方法，结合随机值对共识节点进行全局选取，所有信誉值合格节点均可能被选为共识节点，在保证去中心化特性的同时，减少了共识节点的数量，保证能源交易数据的共识效率。可依据交易场景的不同，更改共识节点的选举范围，使得能源交易由相关节点共识决定，并且支持多组共识节点同时进行共识，

降低了共识节点被攻击的可能性，缓解了固定共识节点的共识压力。同时，快速概率共识协议(FPC)等其他类型的共识机制也可以结合业务特点进行针对性设计，满足不同场景下的区域能源互联网共识需求。

1.1.5 能源区块链中的智能合约

现阶段在能源互联网中，如何进行满足用户需求的能源相关信息交互是重中之重。一方面，大量个体发电用户涌现并加入能源互联网，电力能源类型逐渐增多，能源相关信息的交互逐渐从单一的集中交易、集中管控发展为多元化的综合能源交易[42]；另一方面，需要考虑各种类型能源的特点，如传输成本和环保标准等，尽可能实现能源就近消纳，降低传输成本，增加清洁能源的使用比例。此外，还需考虑能源数据溯源、自动化结算、偏差/损耗处理等问题，使得能源区块链中的信息记录及交互能够更好地满足能源互联网中各类角色的不同需求。

智能合约能够使区块链系统完成更加复杂的程序和计算，并保证程序运行的自动化和正确性，能够很好地实现能源互联网中复杂的多元化综合能源交易。智能合约在能源交易中应用的研究主要分为 3 个阶段，（1）针对能源交易结果制定智能合约，将交易结果上链存储，保证交易结果的不可篡改；（2）针对能源交易的阶段结果制定智能合约，将价格制定、交易结果和资金转账等数据上链存储，保证阶段数据的准确溯源；（3）针对能源交易双方需求制定智能合约，为交易双方提供需求信息发布、电力匹配、电力结算和偏差处理等一体化服务，保证了交易流程的自动化执行，避免了人为因素对电力交易过程的干扰。

能源自动化交易

目前，已有较多采用智能合约实现能源互联网电力自动化交易的研究[31,43-47]，交易过程主要包括价格制定、需求信息发布、电力匹配、资金结算和偏差处理等环节。

针对电力交易价格的制定，主要有三种方法：自由制定价格[48]、通过智能合约自动化调整价格[35][46]、密封售价机制[49][50]。方法一：用户可以自由定价，但是能源市场价格波动频繁，恒定的价格不利于电力的售卖。方法二：依据市场行情，通过智能合约实时调整电价，有利于电力售卖。因电价是影响电力匹配的重要因素之一，公开的电价易被竞争者作为参考。方法三：通过智能合约保

证电价在匹配之前的密封性，有效防止了电价被作为参考的问题。未来电价制定，既要保证其密封性，又要充分参考市场行情，为卖家获取最大化的利益。

为满足买卖双方需求，应为用户提供自主发布需求信息的功能。现阶段，部分研究采用智能合约已实现用户需求信息的自动化发布[31][43][44]。例如：文献[51]设计了电力多边交易的智能合约，合约第一步便是交易信息投标。在市场中，交易者依据自身喜好和实际需求，发布符合自身需求的购电、售电信息，能够更好地进行电力匹配，激发用户参与电力交易的积极性，促进电力市场的蓬勃发展，同时，用户在发布需求信息时应充分参考市场行情，避免电力供需失衡。

针对复杂的多元化综合能源交易场景，多种电力交易匹配机制被提出，大致可以总结为 P2P 撮合匹配[47][48]、双边拍卖匹配[1,50-54]和多因素电力交易匹配等三种。

文献[55]提出了一种基于用户偏好的去中心化匹配方法，采用智能合约实现了基于用户偏好的 P2P 能源撮合匹配，但是在交易数量大、匹配要求多的能源交易场景下，单个用户的匹配方式匹配效率较低。针对大量的电力交易，现阶段多采用双边拍卖匹配能源交易。例如：文献[56]采用双边拍卖匹配机制为社区用户进行电力匹配，有效减少了整体社区的高峰需求；文献[57]提出了一种综合能源交易机制，将匹配过程分为集中匹配和双边拍卖两个阶段。双边拍卖匹配主要参考电力价格，缺少对能源类型、传输损耗等因素的考虑，不利于清洁能源的售卖，并且远距离传输易造成不必要的传输损耗，增大传输成本。

针对电力交易匹配，应充分考虑电价、交易量、传输损耗、能源类型和环保指标等多种因素，侧重用户具体需求进行匹配，有利于为用户匹配相对最合适的电力交易。例如：文献[58]提出了一种基于区块链的分布式多因素电力交易匹配机制，并在文献[59]实现应用，实验结果表明该机制在满足用户需求的同时，还提高了清洁能源的消售比例，并降低了电力传输损耗，是较为适合多元化综合能源交易场景的一种匹配机制。

针对电力交易结算，现有研究主要采用以下两种方式：依据交易计划的同步结算[35,43,45,48,49,51]和依据实际数据的异步结算[60]。前者是先付款后用电，依据交易计划中的购电量等信息利用智能合约进行自动结算；后者是先用电后付款，通过智能电表等设备获取实际的电力供耗数据，并采用智能合约实现异步结

算。前者在结算的同时也导致了计划电量偏差处理的问题，后者有效避免了电力偏差浪费和费用预支的问题，较为适合分布式电力交易结算。

针对电力交易中的偏差，主要分为计划电量偏差处理和实际传输偏差处理。前者指的是实际需求量与计划交易量的偏差处理，可通过智能合约向周边用户提交偏差电量交易申请，周边用户更改计划量，进而消除偏差量[49][51]，该偏差大多因计划交易量不够准确造成，不存在经济处罚；后者指的是实际传输电量与购买电量的偏差处理，造成原因主要是不良卖家少供电，通过对比智能电表采集的实际电量传输数据与区块链中的计划交易数据，得出偏差量，并依据奖惩机制，对违规者进行处罚[48][50]。

其他功能

智能合约技术在电力交易过程中除以上功能之外，还包括能源主体注册[50][61]、密钥遗忘处理[35]、计量监管碳排放权[11][43]、电力交易确权溯源等功能。计量监管碳排放权功能在一定程度上限制了化石燃料的使用，有利于促进清洁能源的推广；电力交易确权溯源主要包括售电和购电信息[26][35][55]、电力匹配记录[1,58-60]、结算记录[51,58,59]以及碳排放权和绿证交易记录[43]的确权和溯源，通过智能合约实现以上信息的自动化上链存储，保证了交易数据的不可篡改和可溯源查询，此外，也为电力结算提供了准确的参考数据，推动了自动化结算功能的实现。

现阶段，应用于能源互联网区块链应用的框架主要基于 Hyperledger Fabric[62]，多采用联盟链的方式部署能源互联网网络，智能合约多采用 Golang 语言编写，智能合约能够保证程序的自动化运行，避免人为因素对电力交易过程的干扰，区块链技术具体细节过于琐碎，在此不进行细节描述。未来，智能合约技术完善能源交易的自动化执行，可能面临的问题主要包括：自动化运算存储效率、轻量化运行、大批量交易等几方面。

1.1.6 能源区块链中的安全机制

能源区块链的一个重要的作用就是为能源互联网提供安全保障，因此能源区块链的安全机制也倍受关注。文献[63][64]讨论了区块链所面临的安全风险，并对当前存在的一些改进手段进行评价。这些研究更加侧重于对区块链本身进行分析

和讨论，然而能源互联网面临的问题更加复杂，包括身份认证与访问控制、数据通信安全、隐私保护和行业规范等。

身份认证与访问控制

身份认证可以保证系统内的交易、数据等更加公开透明，提升用户和系统的可信度；而访问控制是系统通过对用户进行认证，从而控制用户访问系统内资源的手段，防止用户非法使用系统资源。能源互联网中用户参与交易或其他业务一般是通过真实身份来进行，而能源系统中也存在多种类型的用户，如管理员用户、电厂用户、分布式能源用户等，他们各自所有拥有的权限是不同的，需要进行严格的控制。

能源互联网中的用户入网往往需要满足一定的注册条件，比如真实身份、信用状况等，而单纯使用公私钥难以保证这一点。此外，由于用户之间没有权限分别，系统难以进行访问控制。

有研究通过单独构造身份链的方式进行身份认证[65]，但该方案实际上是将受攻击的风险转移到了另一条链，而没有缩减这种风险。

如何在尽可能去中心化的情况下，完善身份认证和访问控制机制，是解决能源区块链身份认证和访问控制问题的重要方向。此外，对于能源互联网内基础设施来说，则应尽可能地控制其权限，防止产生漏洞或被恶意攻击。文献[66]通过智能合约实现物联网中设备的访问控制，对能源区块链也具有一定的参考价值。该方案中设定了访问控制合约、注册合约和判定合约，对设备进行严格的管理，并能够诊断设备的非法操作，当然在效率上相对于中心化的管理会有所下降。

数据通信安全

能源区块链的通信安全要求包括保密性、完整性和可用性三个要素[26]，其中保密性指的是通信数据不被破译，完整性表示发送与接收数据一致，没有受到篡改，而可用性要求系统可以持续正常运行。

区块链使用 P2P 通信协议在节点之间进行通信，节点与节点之间直接建立连接传输数据，节点广播的信息也会通过泛洪机制传播到整个网络。P2P 网络往往缺少身份认证、数据验证、网络安全管理等机制，使攻击者有机会发送非法内容对网络进行攻击[67]，如日蚀攻击、女巫攻击、DDoS 攻击等。文献[26]提出将数据分发服务（DDS）作为区块链的底层数据传播技术，结合智能合约对数据进行

校验，防御虚假数据攻击。DDS 采用发布/订阅体系架构，并提供服务质量策略，各个节点在逻辑上无主从关系，与区块链的架构相类似，提高了通信数据的质量，但也没能解决底层节点的验证和授权问题。

Fabric 基于自身严格的身份认证和访问控制机制，使用安全传输层协议（TLS）进行节点之间的安全通信。TLS 会在两个节点之间建立安全连接，包括身份确认和数据加密传输，避免了伪造节点和虚假数据的问题。当然，TLS 的安全性也是由 CA 机构进行保证的。

总的来讲，数据通信安全与系统内身份认证机制紧密相关，身份认证较强的联盟链网络中，通信安全更容易得到保障；而身份认证较弱的公链系统容易遭受攻击。在讨论解决方案时，研究者对于这两方面的安全问题应当一起考虑。

隐私保护

能源互联网中包含了大量的用户交易数据，随之带来的是用户的隐私保护问题。区块链去中心化的结构不仅提升了整个系统的安全保障，也让用户隐私保护成为可能。P2P 网络结构和去中心化特征在隐私保护上具有一定的优势，但也面临着一些问题[68]，这些问题主要分为数据隐私问题和身份隐私问题。

a. 数据隐私

区块链中的数据是公开透明的，攻击者能够通过分析交易记录获得有价值的信息，例如资金流向和交易内容等，而用户往往不希望这些信息被其他人探知。

基于 UTXO 模型的区块链系统具有一定的匿名性，用户可以选择使用多个账户来隐藏自己的交易行为。但仅仅通过多重账户的方法是不够的，攻击者依然可以通过交易溯源和账户聚类等技术获取到有用信息。文献[25] [69]试图通过动态随机数、相邻账户隐藏和账户映射算法等手段完善多重账户机制，以避免数据挖掘算法的攻击。然而多重账户机制会给审计和监管带来不便，增加系统的不可控性。

通过多链结构来保护数据隐私也是一种常见的手段。多链结构是区块链的一种独特的结构，多个区块链各自拥有一部分节点群体，且链与链之间存在节点交集。例如一个多链结构可以包括账户链和交易链[35]，分别存储不同类型的数据，只有参与其中的账户有权查询。文献[65]将交易分为了公有交易和私有交易，私有交易不进行全网共识，而是由一组可信任的监管节点进行验证和记录，因此可

以实现对部分隐私数据的保护。这在本质上还是一种包含了 “私有交易链”和“公有交易链”的多链。多链结构实质上是通过分割用户群体来保护部分数据的隐私，但难以作用于所有用户都参与的数据集。

此外，鉴于能源区块链中大多数据将会频繁参与计算，保护能源数据在计算过程中的隐私也将会是一项重要的课题。目前已经有研究提出将 SGX[70][71]、安全多方计算[72][73]和同态加密[74]等技术与区块链相结合，使得区块链中的数据在参与某些处理和计算仍能够保证隐私，可以为能源区块链提供改进思路。

b. 身份隐私

区块链去中心化的网络分布结构难以阻断交易数据的传播和外泄，隐私保护更加侧重于保障用户的匿名性，也就是身份隐私。

目前关于能源区块链匿名性的研究比较稀缺。文献[75]使用多重签名结合匿名信息流实现匿名的能源交易。该方案的难点在于快速验证，如何提高匿名信息流的处理效率是一个不小的难题。此外，像结合群签名[76]、环签名[77]、零知识证明[78]等密码学技术来保障区块链匿名性的相关研究已有很多，下一步需要考虑结合能源交易中的匿名需求做出更多的尝试。

行业规范

在全世界范围内，区块链拥有庞大的开发社区和众多的开源项目，而能源区块链的相关研究也都会基于这些开源项目进行实验和试运行。能源区块链要想在我国真正落地并发挥作用，还需要遵守相应的行业规范。

区块链中包含了大量的密码学算法，大多数开源项目使用的是主流密码学算法，比如 SHA256、secp256k1 等。而我国密码行业技术委员会颁布了一套密码行业推荐标准，包括各类算法以及使用规范，这些国密算法经过专业的设计和证明，相较于主流算法而言具有更好的安全性和适用性。目前其他领域已经存在国密算法相关的区块链设计[79][80]，可以为能源行业提供参考。

监管也是能源区块链所面临的重要问题。当前能源区块链相关法律法规尚未健全[81]，导致国内外的能源区块链项目普遍规模较小且应用场景过于理想，无法进行广泛地应用[13]。文献[65]和[39]都通过在系统中设置监管节点的方式完成系统的监管；文献[30]采用实时监听的方式，获取用户节点的交易行为；而文献[35]在多链体系中设置了监管区块链，对用户的诚信和违规行为进行记录，达到

以链治链的效果。对于监管问题，一方面相关部门应该继续严格相关法律法规，引导能源行业对区块链技术进行正确地使用；另一方面研究者应当积极探索更多的技术监管手段，例如节点追踪、穿透式监管、主动探测和以链治链等。

1.1.7 能源区块链中的其他领域技术

在能源互联网的相关研究中，许多其他领域的技术例如大数据、人工智能、经济学与博弈论、5G 技术等，被用于促进能源互联网的进一步提升。这些其他领域的技术与区块链技术相互促进、相互融合，从而发挥出“1+1>2”的效果。目前许多研究都在尝试着将其他领域的技术与区块链进行结合，以构建出更符合实际需求的能源区块链体系。

大数据

大数据技术可以有效地提升能源互联网的数据整合与分析能力，在能源互联网领域具有广泛的应用[16]，包括负荷预测、分布式能源接入、系统安全和态势感知等方面。

主流的大数据技术都采用分布式存储的方式，与能源区块链的结构较为符合。区块链能够为大数据提供安全可靠的数据来源，也可以对大数据分析的结果进行认证[82]。此外，应用大数据技术可以为能源互联网数据的处理提供更丰富的选择，例如结合边缘计算[83]可以为本地用户提供高吞吐量、及时的数据处理服务等。

人工智能

人工智能算法如神经网络、深度学习等为能源互联网的设计、模拟、优化和用户分类等提供了强大的工具[18]，而区块链可以为人工智能技术提供安全的执行平台，以保护这些关键的能源数据。

文献[84][85][86]探讨了区块链和人工智能技术在实现能源互联网的自动化和现代化的作用。人工智能支持的区块链可以更好地分析和处理包含数千个变量（频率、负载和电压变化等）的数据集，来实现传输路径优化、入侵检测和交易数据识别等功能。由于计算量过大不适合直接使用智能合约，这些方案大多采用“链上结合链下”的手段，人工智能分析系统与区块链系统往往各自独立运行。

群体智能算法则能够与智能合约更好地进行融合，例如蚁群优化（ACO）算

法。ACO 算法与区块链技术共同存在的去中心化特征，通过个体间的沟通协作可实现整体寻优。文献[44]利用改进的 ACO 算法来处理各能源市场主体竞争的多目标优化问题，还将该优化算法与其他类型的优化进行比对，以证明该算法的全局搜索能力和收敛能力更强、求解效率更高。

此外，还可以考虑将人工智能技术与区块链进行深度融合，例如利用深度学习等对能源区块链底层结构进行分析，辅助能源互联网中设施的调整和优化，如分析各个节点的数据吞吐量，以实现节点之间的快速响应和分布式系统负载均衡[87][88]等。

经济学与博弈论

区块链本身蕴含着一定的经济学原理，例如激励机制和代币发行，而能源市场情况更加复杂和多样化，电网能够通过调整电价对用户施加影响，还能通过发放补贴[44]、绿证等行为促进用户参与能源交易。

文献[34][89]都提到了使用代币来作为用户参与能源区块链记账的奖励，而单一的挖矿激励机制却无法起到促进用户参与能源市场的作用。文献[44]根据可再生能源利用率设计了新的激励机制，即以可再生能源利用率高于平均的程度来发放奖励，甚至还设计了碳排放相关的惩罚机制，对于用户多余的碳排放量给予惩罚。

能源市场常常会涉及到各方之间的博弈，区块链和智能合约能够帮助用户自动化地获取市场信息并执行最优策略，从而在能源交易中获益。根据场景设定的不同，许多研究采用合作博弈模型[39]或非合作博弈模型[44][52][90]来预测市场的形式和均衡问题。博弈模型首先要考虑的问题就是是否存在均衡状态，文献[52]采用势博弈保证了纯策略均衡解的存在，不需要讨论均衡的存在性，有利于推进博弈模型的进一步应用。文献[44]分析了微电网运营商、大用户和分布式聚合商的市场需求，建立了市场竞争博弈模型，并验证了在三者获益区域内并不存在帕累托最优点，说明电力市场各方主体之间具有明显的竞争关系。

此外，用户制定市场策略时除了考虑参与交易所带来的收益最大化之外，还有可能考虑行为偏好、环保效益等，以及能源市场的附加产品所带来的额外收益，这些也需要在设计博弈模型时加以考虑，进行定量的分析。

5G 技术

区块链本身存在一定的效率和性能缺陷，而 5G 通信技术包含了 5 个方面的基本特征，即高速率、高容量、高可靠性、低时延与低能耗[91]，能有效提升能源区块链的综合效率，创新能源区块链的应用模式。

5G 能够连接海量设备，每平方公里可以支撑 100 万个移动终端，使得能源区块链可以将更多的基础设施纳入管理范围，实现能源互联网中更加精确、密集的信息互联。

5G 高速率、低时延的特性可以显著提升能源区块链中交易广播和区块同步的效率，从而能够在根本上提升共识机制的效率，有利于能源区块链选取可靠性更高的共识机制和数据传输手段。

5G 支持网络切片技术[92]，可以根据能源互联网中不同业务的差异性选择不同的网络，比如超高可靠性超低时延、海量机器通信接入和增强带宽等。

对于层次式的能源区块链结构来说，5G 技术能够帮助区块链系统更加快速、精准地从传感设备收集数据，以实现对电网内物理设施的有效控制。凭借在物联网通信中的巨大优势，5G 技术将会促进电力系统更好地与物联网融合，形成“5G+物联网+区块链”的能源区块链一体化格局。

当然 5G 技术目前也存在一些不足，例如通信能效问题。5G 时代的通信基站密度将会达到 4G 时代的 10 倍以上，大容量、高速率、低时延的代价将会是能效的降低。因此，如何能在更加节能环保的基础上融合 5G 技术，是能源互联网未来将要面对的问题。此外，区块链模式在 5G 通信中的深度结合也是一个值得讨论的话题，与当前 5G 技术提升区块链性能和效率的结合方式不同，区块链有助于在底层机制上实现点对点的安全高效通信。

1.1.8 能源区块链未来研究方向

能源区块链正处在一个飞速发展的阶段，然而目前存在诸多因素制约能源区块链的发展。一方面，现今关于能源区块链的研究中，缺少对区块链前沿技术的深入探究与应用；另一方面，多数能源区块链方案停留在设计和原型阶段，缺少有效的实践反馈。基于现有的研究状况和问题，未来能源区块链设计的研究重心可能会集中在高性能、高安全、高可扩展和可监管等几个方面。

高性能

能源区块链想要真正落地，必须要解决性能问题，区块链自身性能瓶颈和在能源场景应用产生的额外性能需求是当前制约能源区块链性能提升的主要因素。

针对区块链自身的性能瓶颈，需从区块链底层的设计机制出发，提升现有的性能水平。例如，共识机制可靠性与效率之间的矛盾尚未解决，需要设计出满足能源区块链节点场景，且具有良好的容错性的高效共识算法；智能合约的效率难以支撑复杂的人工智能算法或数据分析，需要从合约底层的执行引擎入手提升计算效率；去中心化账本中的冗余数据太多导致存储效率低下，可以尝试结合分布式存储方案，如 IPFS[93][94]等，更高效地存储海量数据。

而针对区块链具体应用时产生的额外需求，需要考虑具体应用的影响采取相应的措施。例如，应用密码学技术保护系统安全和隐私的同时，也会降低系统业务的处理速度，需要设计信息冗余度更小、更加简洁的安全和隐私保护机制；能源互联网大规模物理设备接入和海量数据搜集，会涉及到硬件设施的性能瓶颈问题，需要广泛应用 5G、大数据等技术来有效地管理能源设备与数据。

高安全

针对现有的能源区块链关于安全机制的研究，可以做到的提升有以下几方面：

进一步加强对用户的身份认证和访问控制，继续探究去中心化的公钥认证机制和权限控制机制，同时依靠有效的身份认证机制来提升节点间数据通信安全，避免系统因验证和管理缺失而遭受攻击；充分考虑能源场景的隐私保护需求，防止因隐私泄露而造成安全问题，结合可信执行环境 SGX、安全多方计算和同态加密等技术保障数据的私密性，结合群签名、环签名和零知识证明等技术保障分布式能源用户在交易中的匿名性；采用更加安全可控的密码学标准，如在能源区块链的构建中使用国密算法代替主流密码学算法，以从基础上获取更可靠的安全保障。

高可扩展

良好的可扩展性对于能源区块链的可用性、易用性等方面具有重要影响。随着未来能源互联网的发展，势必会对能源区块链的可扩展性提出更高的要求。

首先是对规模可扩展的要求，需要积极探索高可扩展的共识算法，发展区块链分片、跨链、多链等技术，以保证更大规模区块链网络的事务处理能力，满足更广泛的能源—信息互联需求。

此外还有对于能源互联网业务和应用的扩展要求，一方面需要完善能源区块链的平台化建设，构建整个能源互联网应用的社区和生态；另一方面可以考虑对智能合约引擎的扩展功能进行改进，支持更多种类的编程语言。

可监管

能源是关系到国计民生的重要领域，能源区块链在设计上必须做到严格监管，能够保证事前能预防、事中可止损、事后要追责。一方面要通过技术手段加强对能源互联网内各主体的监管，明确各个主体的权责问题，积极探索节点追踪、穿透式监管、主动探测和以链治链等监管技术；另一方面要加强对能源市场的审计和监管，尤其是在对用户的隐私进行保护的同时，要为市场监管留有余地，严格遵守相关的信息管理规定。

1.1.9 总结

本节通过定位能源互联网中电力交易区块链中的关键技术，从共识机制、交易与智能合约设计、安全机制和其他领域技术等四个角度，详细地综述现今电力交易区块链在各项技术方面的研究进展，并结合发展现状进行更加深入地讨论与分析，指出目前各项技术领域存在的问题，以及未来可能的研究方向，以期为能源互联网电力交易区块链的进一步研究提供参考。

可以看出，区块链对于能源互联网的提升是全方位、多维度的，构成电力交易区块链的多种关键技术能够自底向上的发挥其作用，有望从根本上解决目前电力交易面临的种种挑战。不过，目前能源互联网电力交易区块链仍然有很长一段路要走，要想真正地实现落地应用，除了从技术理论方面展开更加深入的研究，还需要在行业中进行更加广泛的实践。

1.2 研究报告概要

本节对本报告中后续章节的主要研究内容及贡献进行简要介绍。

第二章分析传统集中式电力交易方案在能源互联网发展中面临的挑战，中心化方案难以适应广泛分布式能源交易的需求。针对现有电力交易区块链信息不统一、信任体系难以建立、电力预售造成的电力偏差浪费和成本超前等问题及能源互联网点对点分布式电力交易的需求，提出一种基于区块链技术的微电网电力交

易系统，基于业务特点，设计所需架构和模块，将交易与结算流程上链，自动化执行交易匹配与异步结算。本章面向我国现有微电网交易场景进行系统仿真，实现良好的性能，具有实际应用前景。

第三章基于 K-prototypes 聚类的相异度算法，综合计算和比较电价、交易量、传输距离、能源类型等影响电力匹配的因素的总相异度。选择相异度最小的电力记录进行撮合。此外，系统架构设计较第二章更为独立并简化模块间的信息沟通，减弱区块链共识周期对于撮合与结算的影响。基于智能合约设计相应的自动匹配、私钥签名确认和交易结算功能，实现区块链上单笔交易的自动撮合，匹配结果由电力交易双方控制，并基于零知识证明和同态加密方法设计电力交易的隐私保护方法和算法实现。共识机制基于进一步分布式的交易及区块链基础设施架构设计。实验验证本节提出的方法提升清洁能源交易比例与价格，降低能源互联网输电损耗，提升撮合成功率。

为了更广泛地适应基于区块链的分布式电力交易特点与优势，在第四章中进一步地基于线性多目标优化方法提出一种支持拆分买卖需求的多属性偏好电力交易系统，并设计电力交易全流程在区块链上实现的交易方案。该系统提供的包含交易双方对交易的多种匹配需求的交易撮合机制，保证能源交易的公平性和可靠性。交易匹配结果可控并最大化买卖多方的匹配满意度，更灵活地实现多属性偏好的双边匹配算法，更好地满足买卖双方的匹配需求。实验结果表明，该方法在匹配成功电量、匹配满意度、传输损耗、清洁能源占比等方面均具有良好的表现。因此，匹配机制产生良好的匹配结果，基于区块链的实现也适用于微电网能源交易场景。

第五章围绕现有电力交易区块链共识机制性能与快速成规模电力分布式链上交易需求的差距，提出耦合业务场景设计共识机制的研究思路；设计面向能源互联网分布式电力交易场景的分级异步共识架构，以 PBFT 结合声誉机制为例，对区域能源互联网分布式电力交易共识机制进行设计，提高区域能源互联网场景下微电网的可扩展性。实验结果证实所提出机制的有效性。

第六章总结了本研究报告的主要成果，并对未来能源互联网中区块链的应用研究做出适当展望。

第二章 基于区块链的分布式电力交易系统及异步结算交易方案研究

2.1 介绍

分布式能源是指连接到配电网为终端用户提供灵活负荷的分布式发电和储能[95]。分布式能源并网有利于实现多种形式的能源互补，可以提高能源效率，扩大可再生能源利用规模。随着相关领域技术的发展和可再生能源发展政策的支持，分布式能源发展迅速[96]。鼓励分布式能源参与市场化交易，可以进一步推动电力体制改革和交易模式转变，其普及和快速发展已成为大势所趋。

能源互联网是基于互联网概念构建的一种新型信息能源综合网络[14]。微电网是能源互联网的重要组成部分[31]。它是一种新型的能源联网供应和管理技术，既可以满足当地电力用户的需求，又可以保证极端条件下的供电稳定性，提高能源效率。能源互联网微电网的主要研究对象包括各种分布式能量收集和存储设备、负载和能源路由器[15]。能源路由器是一种可以从电力设备收集数据并调度能源的设备。它不仅与电气设备相连，还与其他能源路由器互连，传输能源和能源数据，有效地调度和控制微电网内部和微电网之间的能源。典型的微电网结构如图2.1 所示，是本章的主要研究对象。

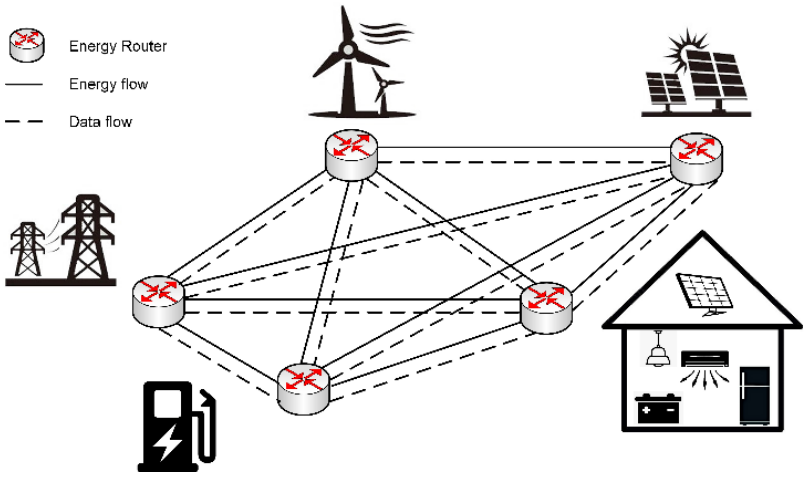


图 2.1. 一个典型的能源互联网微电网的结构。

传统的微电网交易系统采用集中结算方案[97]。计量采集模块处理电费收缴业务，结算模块处理电费结算业务，存在交易信息不一致、信用体系建立困难等

问题[98]。虽然智能电表基础设施可以准确记录用户用电量[99]，但计划电力交易不可避免地存在合同电力偏差。尽管市场交易可以按月结算、按年结算来结算这种偏差，但在一定程度上仍可能造成供电资源的浪费和用电资金的流失。

区块链作为一种分布式账本，通过区块哈希值的单向连接实现链式存储。它采用非对称加密、默克尔树等技术保证链上信息不可篡改，很好地保证了数据的安全性[19, 100-101]。区块链技术具有去中心化、交易透明、可信、不可篡改等特点，与能源互联网的理念高度契合：区块链中记录的可靠数据可以为能源互联网内的能源交易提供可靠的记录；分布式账本存储对应分布式能源主体，避免中心组织失效带来的问题；区块链各方信息公开透明，有利于能源灵活调配。

目前，将区块链技术应用于微电网的探索并不多，大多停留在理论和实验阶段。在理论方面，文献[102]提出了能源集成区块链模型，文献[103]建立了基于区块链的能源互联网安全共享网络体系。尝试验证区块链可以很好地应用在微电网电力交易系统中，解决电网结算信息不对称、信用体系难以建立的问题。文献[104]研究了一种以智能合约形式存储电力交易信息并自动进行资金划转的电力交易方案。 文献[105]描述了智能合约技术与电力拍卖相结合解决合约控制难问题的应用研究。

作为一个初期的典型项目，布鲁克林微电网开发商 LO3 Energy 和区块链技术开发商 ConsenSys 共同开发并运营了一个微电网项目[22]，参与用户可以通过连接到区块链的智能电表跟踪和记录用电量和电力交易。智能能源电网交易比传统的自上而下的能源分配系统更高效，允许用户自己进行电力交易，而无需国家电力公司参与。欧盟 Scanergy 项目[106] 旨在基于区块链系统实现小用户绿色能源的直接交易。该项目设想在交易系统中每 15 分钟检测一次网络的生产和消费状态，并向能源供应商提供类似于比特币的 NRGCoin 作为能源生产的奖励。然而，这两个项目的试点规模有限，只是为了证明小规模微电网进行分散式电力交易的可行性，还需要在更大范围内进一步验证，其能源交易结算设计具有仍然有很大的改进空间。

本章针对微电网信息不一致、信任体系难以建立、预售造成的电力浪费和成本垫付等问题，结合区块链的良好特性，提出用于微电网电力交易系统架构，并初步设计了其中的异步结算交易方案。该系统的设计有效地避免了功率偏离造成

的损失。第二节给出了交易系统的总体结构和模块功能。电力交易异步结算方案的具体步骤描述在第三节。系统性能的实验设计和结果在第四节说明。第五节对本章内容中进行了总结。

2.2 基于区块链的能源互联网微网电力交易系统

2.2.1 系统框架

我们提出并设计了一个基于区块链的微电网交易异步结算系统。该系统与 Hyperledger Fabric [107] 项目相结合，实现能源互联网微电网中的能源路由器之间的交易实施交易的系统。系统总体架构如图 2.2 所示，主要包括数据采集模块、区块链节点模块、用户管理模块、智能合约模块和合约管理模块。

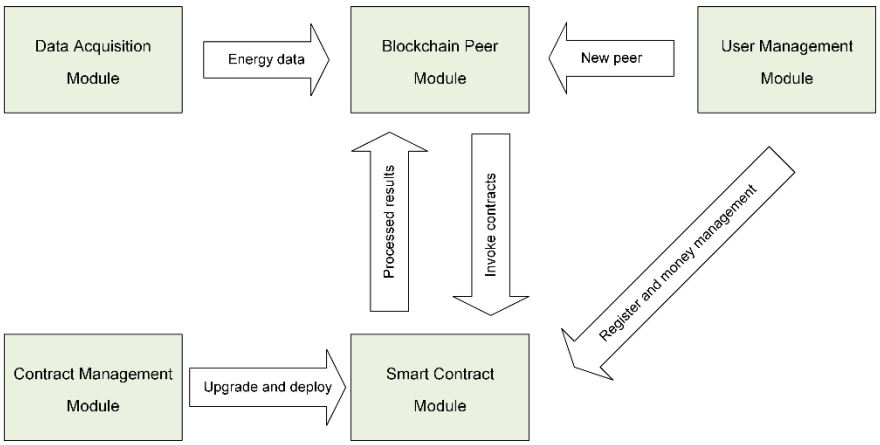


图 2.2. 能源互联网微网电力交易系统的整体架构。

2.2.2 系统模块

a. 用户管理模块：该模块用于根据用户注册信息进行身份认证注册和管理其他用户相关的东西，如用户资金管理和节点状态管理，也可以根据用户数量和用户发起新用户注册用户获取能源路由器后的身份信息。智能合约验证注册信息后，会为用户分配一个用户节点，用户通过该节点参与系统中的交易业务。

b. 数据采集模块：该模块通过能源路由器对能源主体进行监控，收集这些主体的供电和用电数据，并组织成区块链交易。最后，这些区块链交易通过使用节点发送到区块链网络。

c. 区块链节点模块：该模块用于整个区块链网络对应的区块链节点之间进行

特定的数据传输和通信。主要包括用户节点、系统管理员节点、排序节点、背书节点。每个节点通过调用智能合约实现链下数据的上传和链上数据的查询。它是用户与区块链网络交互的窗口。

d. 智能合约模块：该模块用于为各个模块提供具有相应功能的各类智能合约，并处理各个模块的智能合约调用请求。主要包括用户注册合约、数据上传合约、异步结算合约、资金管理合约、违规处罚合约。

e. 合约管理模块：该模块用于远程升级和部署新版本的智能合约。系统会根据用户的不同需求进行相应的功能合约研发。新合约获得用户认可后，模块将进行远程升级和部署。

2.3 电力交易方案

我们提出的电力交易及异步结算方式主要包括交易计划制定、能源价格匹配、能源数据采集、能源数据上传、异步结算五个部分。 本章主要介绍这五个部分的流程和相关知识。 图 2.3 是所有过程的概览。

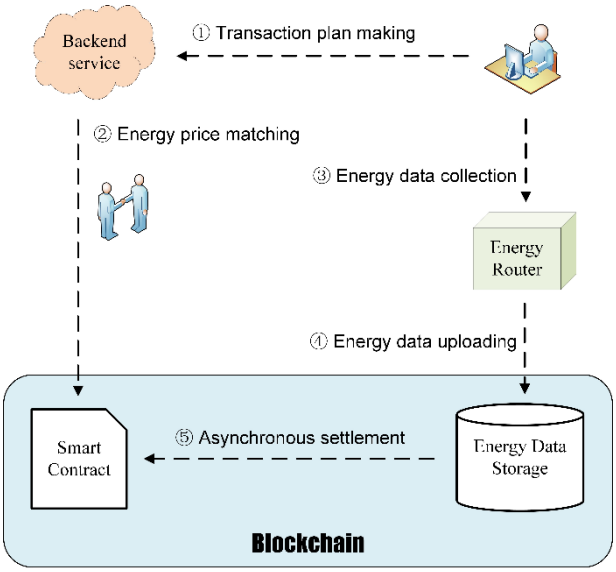


图 2.3. 电力交易及异步结算方案的步骤。

2.3.1 交易计划制定

该系统中的用户可以自由设定他们生产的能源的价格。用户可以根据自己的情况设定合理的能源供应价格，并在网上公布能源供应价格。本系统所有用户都可以看到该用户发布的能源供应计划。同时，需要使用能源的用户也可以自行设

定能源采购价格，发布能源采购计划。

2.3.2 能源交易匹配

该系统中的所有能源买卖双方都可以自由匹配。经过协商和确认后，一对用户将他们的能源交易价格记录在一个价格表中，最后以价格矩阵的形式保存在区块链中。此外，一个用户可以与多个用户设置不同的能源交易价格，并且可以设置购买优先级。例如，用户 A 可以同时与用户 B 和 C 协商交易价格，A 可以选择先向 C 供应能源。优先级的设置也记录在价格矩阵中。表 2.1 是具有四个用户的价格矩阵的示例。

表 2.1. 一个能源价格矩阵的例子

Buyer / **Seller**	User A	User B	User C	User D	Grid
User A		(1, 0.3)	(2, 0.4)	(3, 0.5)	0.5
User B	(3, 0.5)		(1, 0.2)	(2, 0.4)	
User C	(3, 0.4)	(2, 0.3)		(1, 0.3)	
User D	(1, 0.2)	(2, 0.4)	(3, 0.4)		
Grid	0.5				

表中的元素是购买策略，它是一个二维向量。第一个元素代表购买优先级，第二个元素代表相应的购买价格。例如，第二行代表卖方为用户 A，第三列代表买方为用户 B。那么第三列第二行的元素代表用户 B 向用户 A 购买能源的策略。该策略为 B 从 A 购买能源，优先级为 1，即第一购买者，购买价格为 0.2 元/kW·h。如果 A 可以提供 10kW·h 的电力，B 需要 7kW·h，C 需要 5kW·h，A 先向 B 供电 7kW·h，然后再向 C 供电剩余的 3kW·h。用户 C 需要匹配下一个供应商以获得足够的电力。

表格的最后一列和最后一行是主网格价格。当用户有剩余能源不出售或部分能源需求无法满足时，系统将与主电网进行交易，剩余交易按电网价格结算。

2.3.3 能源数据收集

在本系统中，能量上传周期设置为 T。能量路由器连接各种供用电设备，准确检测供用电数据。数据一个周期收集一次，并传送到相应的用户节点——Peer。用电数据包括用户 ID、电量、时间戳等。每个能源路由器可以注册一个用户并连接到多个访问代理。换句话说，一个用户可以被多个家庭或公司使用。电量表示一周内接入能源路由器的所有接入主体的供电和消耗之和。正值代表供电，负值代表功耗。时间戳表示能源路由器收集能源数据的时间点。

2.3.4 能源数据上链

Peer 在接收到能源数据时，根据能源数据生成区块链交易。然后交易调用数据上传合约将这些数据上传到区块链，包含数据的交易将通过共识存储在区块链上。我们在本章系统中讨论微网中存在可信共识基础设施或存在可信第三方负责共识的场景进行设计和验证，这种场景可能存在于国家电网完全可控的分布式电力交易环境中。这种场景下，可以采用 Kafka 机制模拟共识过程，具体流程如图 2.4 所示。Peer 将交易发送给背书节点（其他 Peer）进行背书；背书节点验证此交易并将验证后的交易返回给 Peer； Peer 将经过验证的交易发送到排序节点 Orderer，该节点收集交易并将其发送到 Kafka 组。所有的 Orderer 都会收到 Kafka 组返回的一致的交易序列，并生成相同的区块。

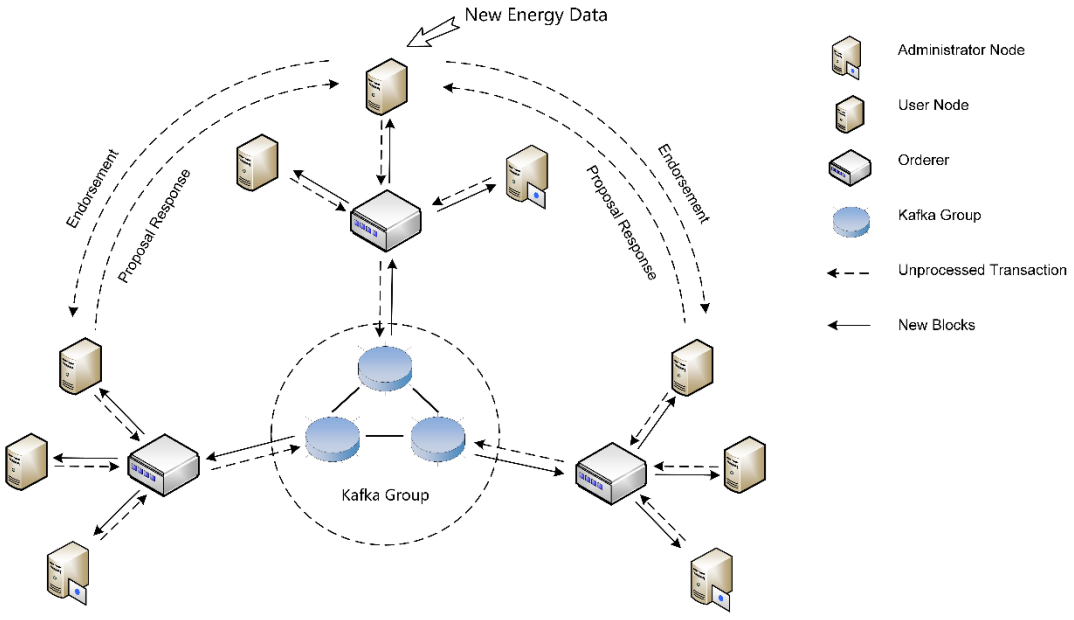


图 2.4. 区块链交易共识过程。

2.3.5 异步结算

链上数据的异步结算是指使用存储在区块链上的能源数据进行结算，与这些数据的上传异步执行。异步结算基于准确的能源数据，可有效解决因预售造成的电力偏差浪费和成本预付款问题。由于区块链网络中可能存在节点宕机，可能导致数据丢失，因此结算分为正常周期结算和异常周期结算。

正常周期结算是指所有节点按时上传能源数据，周期内所有节点的交易记录到区块链后触发异步结算合约的情况。合同根据这些供用能数据和价格矩阵完成结算。异常周期结算是指由于节点宕机或网络问题，部分用户的交易无法按时上传到区块链，该周期被标记为未结算周期。 n 是延迟的容限，如果在下一个（$i<n$）周期上传那些缺失的数据，则在本周期完成一次正常的结算；否则，异步结算合约将在第 n 个周期触发，进行不完全结算，网格将处理所有剩余交易。同时触发违规处罚合约，对不按时上传数据甚至冻结账户的用户进行处罚。

具体的结算算法如图 2.5 所示。**SL** 代表周期内所有供应数据的列表； **CL** 表示该期间所有消费数据的列表； **PM** 代表一个二维表，记录了每两个用户之间的价格和优先级； *systemPrice* 表示主电网的电价。 **UL** 代表一个记录能源和资本变化的用户账户列表，其元素由交易数量、交易价格、买方和卖方组成。这些记录存储在区块链中，以提供能源供应和消耗的有效证明。

Algorithm 1 Asynchronous Settlement

Input: **SL**, **CL**, **PM**, *systemPrice*
Output: **RL**

```
For each s in SL:
    While s.value > 0:
        Choose a buyer of s by priority;
        If there is no one to choose from:
                Set amount = s.value × systemPrice;
                Generate a record r(s.value, amount, s.user, "Grid");
                Add r into RL;
                Set c.value = 0;
        Get c in CL that belong to buyer;
        If c.value != 0:
                If c.value > s.value:
                        Set amount = s.value × PM[s.user][c.user];
                        Generate a record r(s.value, amount, c.user,
s.user);
                        Add r into RL;
                        Set c.value = c.value - s.value;
                        Set s.value = 0;
                Else:
                        Set amount = c.value × PM[s.user][c.user];
                        Generate a record r(c.value, amount, c.user,
s.user);
                        Add r into RL;
                        Set s.value = s.value - c.value;
                        Set c.value = 0;
For each c in CL:
    If c.value > 0:
        Set amount = c.value × systemPrice;
        Generate a record r(c.value, amount, c.user, "Grid");
        Add r into RL;
        Set c.value = 0;
```

图 2.5. 异步结算算法。

2.4 实施和性能评估

本节首先介绍该系统的实现，随后通过实验结果验证系统性能。此外，基于本节及后续章节研究成果在青岛国际院士港对交易系统进行了实例化试点部署，详情见附录。

2.4.1 实施

本系统基于 Hyperledger Fabric v1.4.4 实现。实验设备为华为 2288H V5 服务器，40 核 64GB 内存，分配 30 台 1 核 2GB 虚拟机。虚拟机上的操作系统是 CentOS Linux release 7.7.1908。每个虚拟机部署一个或多个 Peers，它分为几个组织。每个 Peer 可以承载一个或多个用户。

共识机制采用趋近于中心化的 Kafka，它符合我国现有微网电力交易场景，并且 Kafka 在实际生产环境中有很好的表现，适用于由多个组织组成的区块链网

络。 Peers 和用户的管理是基于组织的。为了将用户发送的数据保存在区块链网络中，每个组织至少应有一名成员对其进行背书。

在这个系统中，区块生成规定了两个条件：

1) 超时条件：等待时间达到最大区块批处理时间（MBT）；

2）容量条件：一个区块中的交易数量达到最大消息容量（MMC）。

两种情况下的参数都可以在网络正常运行时修改。

2.4.2 系统性能评估

本节设计了一系列实验来评估系统的性能。测试数据集是通过对现有微电网环境的模拟获得的，包括微光伏、分布式存储、电动汽车桩、电力照明负载等。首先测试平均数据批处理时间随用户数量增长的变化趋势。各实验参数设置如下：组织数量设置为 5，Peer 数量设置为 10，MBT 设置为 2s，MMC 设置为 10，数据上链周期 T 设置为 20s，用户数量逐步增加，我们得到的实验结果如图 2.6 所示。开始时，随着用户数量的增加，平均时间减少。原因可能是系统中的用户越多，交易数量就越容易达到一个区块的最大容量并减少等待时间。随后，平均批处理时间增加，这是由于交易数量增加，导致部分交易处理缓慢，影响平均处理时间。

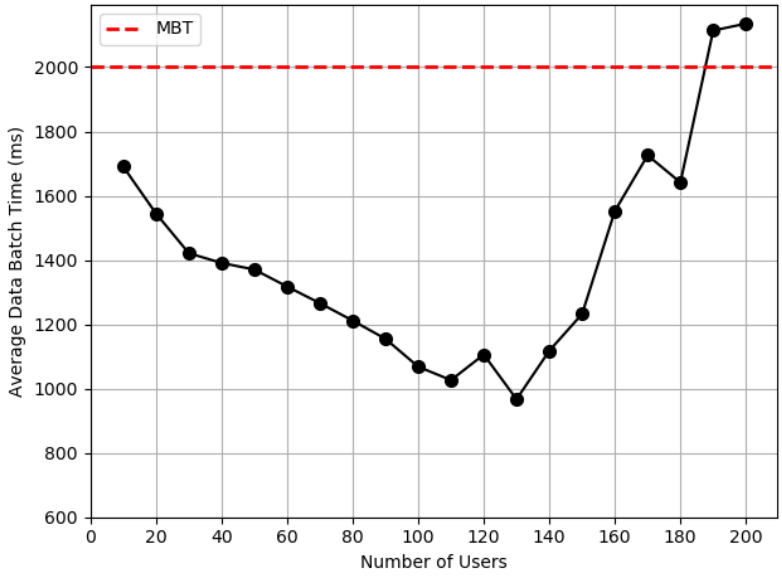
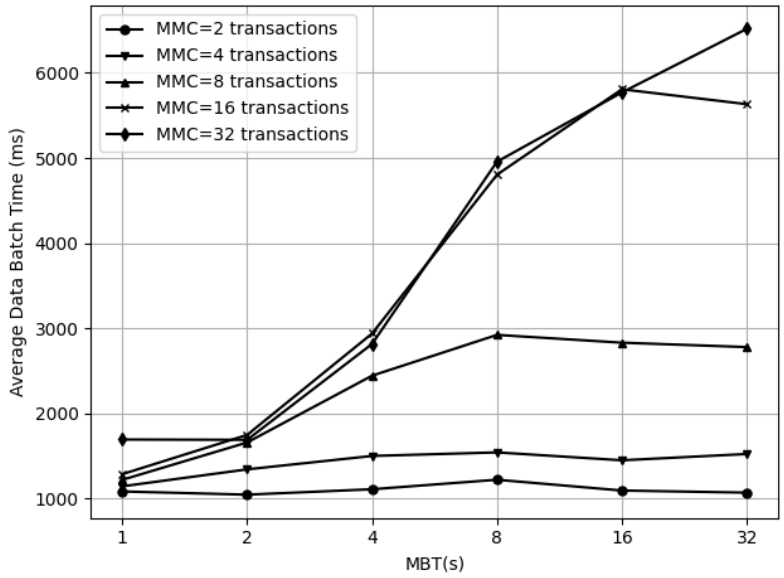


图 2.6. 用户数增长下的系统性能。

然后测试平均数据批处理时间随着 MBT 和 MMC 的增长而变化的趋势。实验参数设置为：组织的数量设置为 5，Peer 和用户数量设置为 30，数据上传周期

T 设置为 20s，MBT 和 MMC 呈指数型增长。我们得到的实验结果如图 2.7 所示。我们可以看到，随着 MBT 和 MMC 的增长，平均数据批处理时间也在增长。在图 2.7(a)中，当 MMC 较大时，MBT 的增长趋势类似指数型增长，这种现象可能是由于每个周期的交易数量有限，很难在短时间内满足可用容量。当 MBT 较大时，超时条件比容量条件更难满足，因此类似的情况出现在图 2.7(b)。但是，当 MBT=32 时，数据批处理时间几乎停止增长，原因可能是一个周期内的消息数量不足以满足 MMC 条件，MMC 的大小不再影响数据批处理时间。



(a)

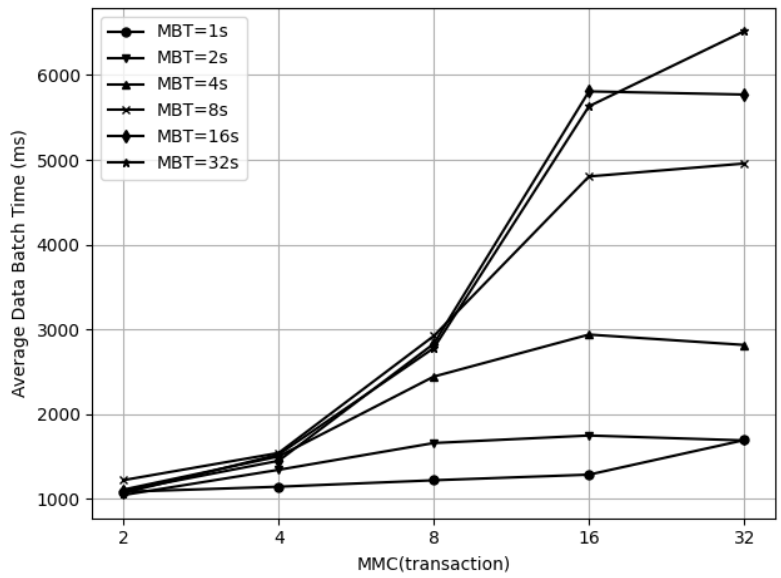


图 2.7. MBT 和 MMC 增长下的系统性能。

对于平均数据批处理时间，分别测试组织数为 2、5、10 时的性能。Peer 数

设置为 10，MBT 设置为 2s，MMC 设置为 10 个，数据上传周期 T 设置为 20s，并且系统中的用户数量逐渐增加。实验结果如图 2.8 所示。可以看出，组织数量的增加会略微减慢系统的数据批处理时间。原因可能是组织数量的增加导致每笔交易所需的背书数量相应增加。不过，与用户增长相比，组织增长的影响是可以接受的。

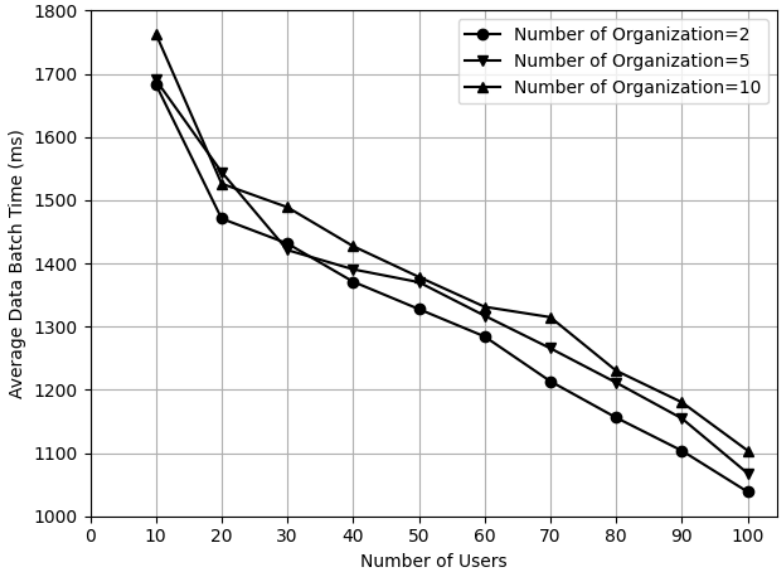


图 2.8. 不同组织数量下的系统性能。

2.5 结论

本章分析了传统集中式电力交易方案在能源互联网发展中面临的挑战，中心化方案难以适应广泛分布式能源交易的需求。针对现有电力交易区块链信息不统一、信任体系难以建立、电力预售造成的电力偏差浪费和成本超前等问题及能源互联网点对点分布式电力交易的需求，提出一种基于区块链技术的微电网电力交易系统，基于业务特点，设计所需架构和模块，将交易与结算流程上链，并面向我国现有微电网交易场景进行系统仿真，实现良好的性能，具有实际应用前景。

第三章 基于 K-prototypes 算法的电力交易区块链多因素撮合机制研究

3.1 介绍

随着分布式可再生能源和储能的广泛接入，以及电力电子和互联网技术的不断进步，区域能源互联网（REI）的概念被提出[108-111]。从地理角度来看，REI 的规模跨度可以是灵活的。它可以覆盖多个微电网的集合，甚至城市。或者它可以是一个社区的微电网。 REI 是许多国家应对城市化进程中高耗能、高污染问题的重要手段之一[3,112]。此外，DRE 发电技术的推广使更多的生产者和消费者能够访问 REI 参与电力交易。文献[113]对基于用户能源需求类型对面向用户的 REI 框架和应用进行了详细分析，为面向用户的 REI 应用提供了技术支持。一方面，REI 为用户提供满足其偏好的可再生能源；另一方面，让更多种类的绿色清洁能源（如风能、水能、太阳能、生物能等）积极参与市场交易。电力交易已从传统的单一能源集中交易逐步演变为多元化综合能源交易[114]。交易匹配、撮合过程更复杂，集中管理难度更大。

在传统电力市场中，消费者通过第三方中心化机构间接与可再生能源供应商打交道[115-117]。这种机制虽然解决了消费者之间的信任问题，但第三方中心化组织的加入，增加了输电损耗和交易成本，并存在信息安全风险[22]。因此，传统的机制可能无法胜任 REI 多元化综合能源交易的场景。

区块链作为比特币的底层技术[19]，利用非对称加密、默克尔树等技术保证链上信息不可篡改[118-119]，并利用数字签名、共识算法等技术实现 P2P 交易.利用区块链技术在 REI 中实现多元化综合能源交易，不需要第三方机构为用户建立信用体系。生产者和消费者可以自由地进行 P2P 交易以减少传输损失[120]；并且通过使用分布式加密存储来保证交易信息的安全[121]。因此，区块链可能是适合在 REI 中进行电力交易撮合的有能力的技术之一。

大量的生产者和消费者接入 REI，产生大量的分布式电力交易撮合需求。目前，电力互联网撮合多采用双重拍卖（DA）等传统匹配机制，容易造成清洁能源

难以撮合、输电浪费等问题。因此，为 REI 设计合适的电撮合机制至关重要。文献[23]从点对点交易、集体竞价和连续 DA 三个方面分析了国内外区块链电力交易撮合研究现状，并对我国区块链能源交易的建设提出建议。然而，它未给出一个可用的系统。文献[122]提出了一个基于区块链的去中心化市场交易平台，允许生产者和消费者进行双重交易，实时消耗市场上的可再生能源。但平台并未针对可再生能源与化石能源的价格差距设计相应的撮合机制。文献[56]提出了一个基于区块链的点对点社区能源交易市场平台，并采用 DA 机制为社区用户提供电力匹配，有效降低了整个社区的用电高峰。然而，并没有针对不同类型的能量设计相应的撮合机制。文献[47]使用智能合约技术实现基于区块链的智能能源交易平台，允许交易者通过代币完成电力交易，无需第三方干预，但未设计交易的全流程，特别是撮合、匹配过程。LO3 Energy 和西门子联合开发的基于区块链的交易网格微电网交易平台[22]设计了 DA 的撮合机制。但是，该平台没有竞价策略模型且没有基于区块链的直接结算。文献[54]为能源互联网分布式电力交易模型提出了一种基于区块链的连续 DA 机制，但该模式主要侧重于根据市场变化及时调整报价，采用区块链将数字电力交易凭证传输给用户进行电力结算。文献[57]基于电力交易撮合的原理，提出了一种基于区块链的综合能源交易机制，将撮合过程分为集中撮合和连续 DA 撮合两个阶段。前者通过第三方机构集中撮合，不适用于多节点自由交易，后者主要依靠价格进行排名和撮合。由于缺乏对能源类型、输电损耗等因素的考虑，该阶段从机制上不利于清洁能源的销售，可能会发生造成更多的输电损失，增加长距离输电的输电成本。

本章针对 REI 电力交易匹配提出了一种基于区块链的多因素电力交易撮合机制。基于区块链技术，为产消者建立分布式信任体系。基于 K-prototypes 聚类算法的相异度距离，综合计算并比较电价、交易量、传输距离、能源类型等影响电力匹配的因素的总相异度。选择相异度最小的电力买卖需求进行交易匹配。此外，基于智能合约设计了相应的自动匹配、私钥签名确认和交易结算，并基于零知识证明和同态加密对交易撮合、匹配、结算过程进行隐私保护设计；面向 REI 分布式交易场景对交易平台进行针对性设计。

本章的其余部分组织如下。第二节描述了多因素电力交易撮合机制的应用场景和总体框架。第三节详细介绍了基于区块链的多因素电力交易撮合机制以及该

机制的系统实现。基于 REI 的场景，对所提出的机制进行了实验测试，测试结果在第四节中进行了分析。论文在第五节中进行了总结。

3.2 分布式电力交易系统设计

3.2.1 应用场景

本章提出的多因素电力交易撮合机制是为 REI 场景设计的，如图 3.1 所示。一个 REI 由多个微电网组成，每个微电网包含许多生产者、消费者和产消者。每个微电网拥有一个微电网能量路由器以及许多子路由器。每个能源路由器和子路由器也是一个区块链节点。区块链节点用于数据流传输，能量路由器用于能量流传输。与单个微电网相比，一个 REI 可能包含更多的售电者，可以为购电者提供更全面、更个性化的电力供应选择。与现有的许多机制相比，本章提出的机制采用智能合约技术，根据链上购电记录的先后顺序自动完成电力交易撮合，同时也采用智能合约技术，根据链上的电力交易撮合记录，自动完成资金转账。上链，避免人为因素对电力交易的干扰，采用区块链技术将所有电力交易信息完整存储，确保电力交易信息的安全性和可追溯性。

该机制设置电力按周期交易。交易采用计划交易，即本周期交易的能量为下一个周期的能量。在一个周期结束前，如果周期可用电量为正，则该周期可用电量低价转售给电网公司。该机制根据链上购电记录的先后顺序，对购电者进行电力匹配，避免售电记录并行匹配导致的双花问题。

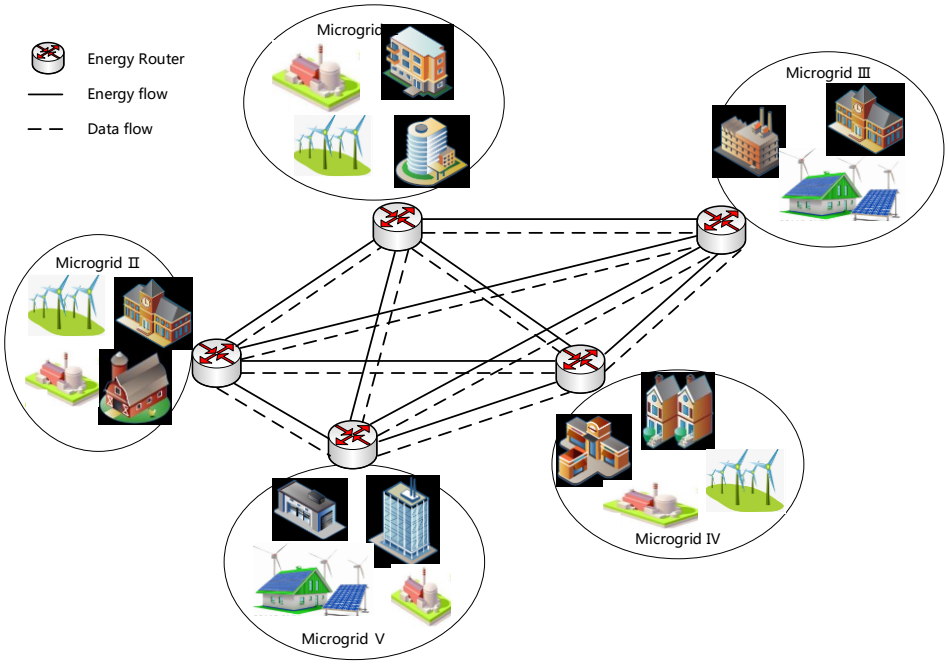


图 3.1. 系统应用场景图。

3.2.2 系统框架介绍

该机制的总体架构如图 3.2 所示，主要包括用户管理模块、电力交易获取模块、区块链节点模块和智能合约模块。基于第二章设计对模块功能进一步独立并简化模块间的信息沟通，使得交易平台可以支持基于智能合约的链上匹配、交易存证，更好地适应区域能源互联网分布式电力交易场景需求。

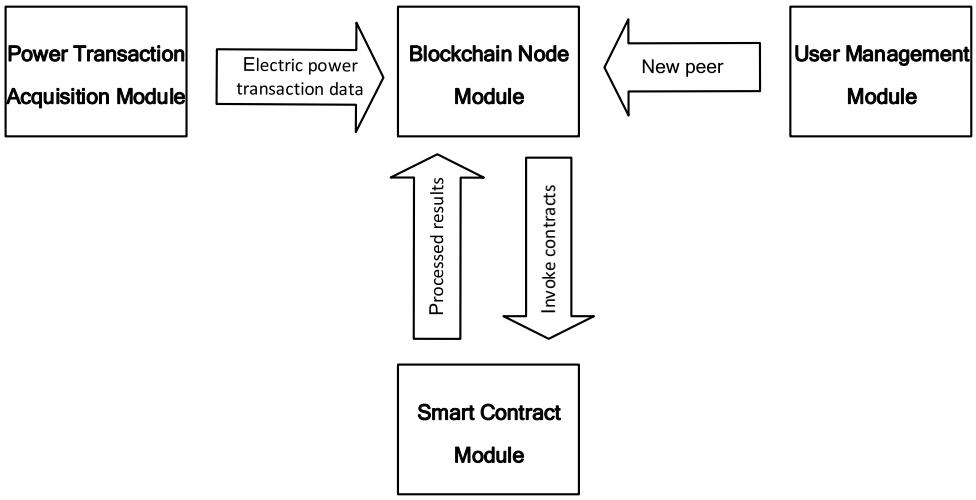


图 3.2. 基于区块链的分布式电力交易系统。

用户管理模块：该模块主要是为新用户完成身份认证注册，注册成功后为用户分配一个公私钥对。用户可以根据自己的喜好，使用智能合约技术进行自动电

力交易撮合。为保证区块链系统的共识效率，用户和区块链节点可以采用一对多的方式。

电力交易获取模块：该模块主要是用户根据自己的喜好向区块链节点提交售电信息或购电信息，进而触发智能合约根据提交的信息自动生成相应的区块链交易并存储在区块链。最后通过智能合约自动完成电力交易撮合，为用户提供最合适的电力撮合。

区块链节点模块：该模块主要供用户通过区块链节点与区块链网络进行特定的数据传输和通信。区块链节点主要包括用户节点、系统管理员节点和排序节点。用户节点主要分为售电节点和购电节点，供用户完成电力交易；系统管理员节点主要用于售电节点和购电节点的远程合约部署或升级；排序节点主要用于对区块链交易的共识排序。区块链节点通过调用智能合约实现链下数据上传和链上数据查询，是用户与区块链网络交互的窗口。

智能合约模块：该模块主要用于区块链节点调用具有相应功能的智能合约，处理各节点的合约调用请求，主要包括基于售电信息的售电记录销售记录并存储在链上；交易撮合结算合约主要用于购电节点调用，根据购电信息生成购电记录并存储在链上。之后，根据用户在购电记录中的偏好完成电力匹配，并根据匹配记录完成资产转移及异步结算。

3.3 多因素电力交易撮合机制

3.3.1 机制流程

本章提出的基于区块链的多因素电力交易撮合机制的具体流程如图 3.3 所示，主要包括以下 7 个阶段和 15 个步骤。

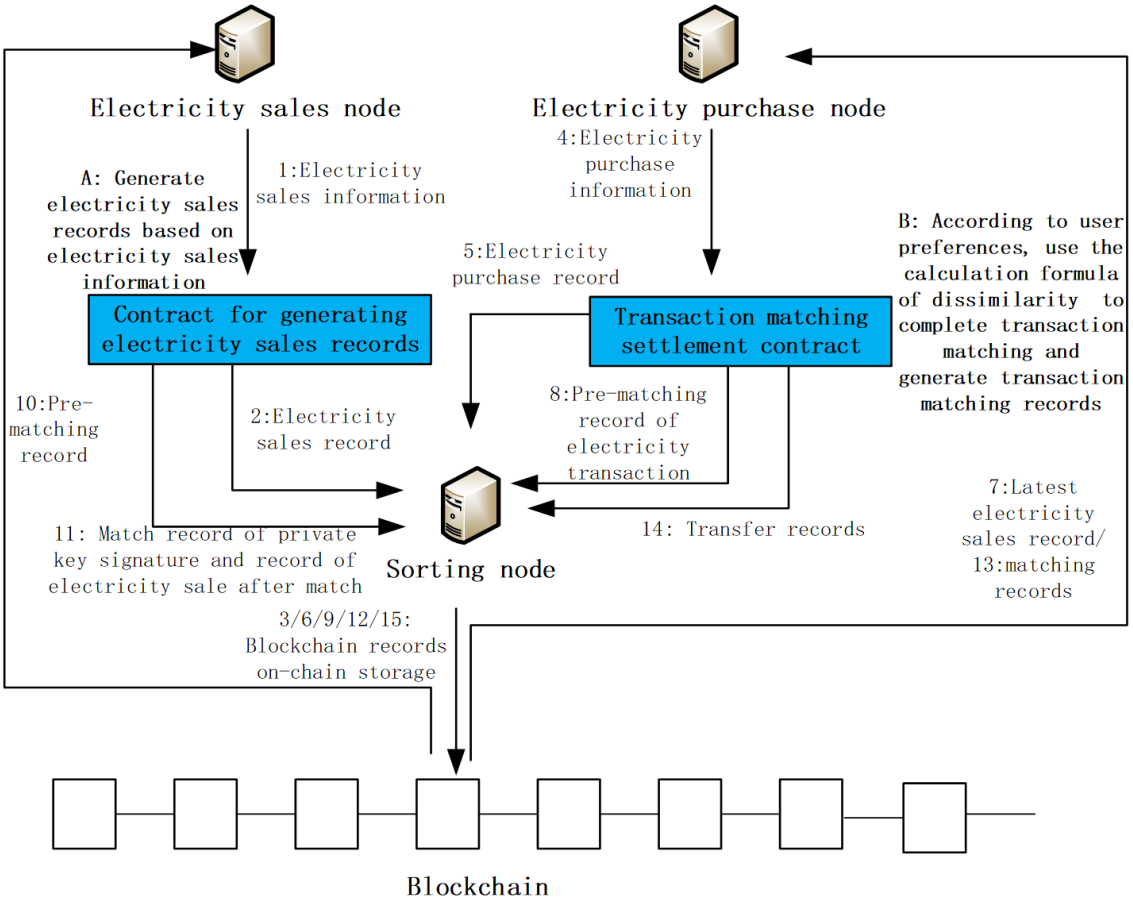


图 3.3. 基于多因素的电力交易撮合过程。

阶段一：售电者通过售电节点提交下一周期的售电信息。

本阶段对应于图 3.3 中的步骤 1。售电者是指 REI 中的主要发电商和普通独立发电商用户。具体售电情况见表 3.1。

表 3.1. 电力销售信息

User ID	Energy Type	Electricity Selling Price	Cycle Total Electricity Supply	Cycle Available Electricity	Electricity Supply Location

表中能源类型主要包括风能、水能、化石能源、太阳能、生物质能等；售电价是指售电单位定制的单位售电价，即每千瓦时的售价； Cycle Total Electricity Supply 指售电单位下一个周期的总发电量；周期可用电量是指当期售电单位本周期总电量供应中未售出的剩余电量。

阶段二：生成售电记录合约根据售电信息自动生成售电记录并存储在链上。

本阶段对应图 3.3 中的步骤 2-3，售电记录的具体信息如表 3.2 所示。

表 3.2. 电力销售记录

Electricity Sales Records ID	User ID	Environmental Protection Index	Electricity Selling Price	Cycle Total Electricity Supply	Cycle Available Electricity	Energy Type	Credit Value of Electricity Seller	Electricity Supply Location

表中环保指数是指按能源种类计算的清洁能源供给比例，风能、水能、太阳能、生物能均为清洁能源；售电者信用值是指根据售电者最近 100 次电力交易的匹配记录得出的电力销售者信用值，信用值计算方法：完成一次电力交易后信用值增加 1；被处罚一次信用值减少 10 次。它的初始值可设为 100，达到 100 后不会增加。

阶段三：购电者通过购电节点提交下一个周期的购电信息。

该部分对应图 3.3 中的步骤 4，具体购电信息见表 3.3。

表 3.3. 电力采购信息

User ID	Environmental Protection Index	Electricity Purchase Price	Cycle Demand of Electricity	Estimated Transmission Loss	Energy Type	Electricity Demand Location

表中购电价是指购电单位定制的购电单价，即每千瓦时的预期购电价；Cycle Demand of Electricity 指购电者下一个周期的用电需求；估计输电损失是指购电者可以接受的输电距离所造成的估计输电损失。

阶段四：交易撮合结算合约根据购电信息生成购电记录并存储在链上。

该部分对应图 3.3 中的步骤 5-6，购电记录的具体信息如表 3.4 所示，预期环保指数是指购电者预期的电力环保指数，由购电者根据自己的喜好设定；能源类型是指购电者希望首先购买的发电能源类型；购电者信用值与售电者信用值的理论相同，在第（2）节已经详细描述，此处不再赘述。

表 3.4. 电力采购记录

Electricity Purchase Record ID	User ID	Expected Environmental Protection Index	Electricity Purchase Price	Cycle Demand of Electricity	Energy Type	Credit Value of Electricity Purchasers	Electricity Demand Location

阶段五：交易撮合结算合约从区块链中获取下一周期的售电记录并进行撮合。

根据购电记录，采用 K-prototypes 聚类算法中的相异度计算公式撮合售电记录。最后，生成电力交易的撮合记录并存储在链上。

本节对应图 3.3 中的步骤 7-9，相异度的计算如公式（3.1）所示。为了保证每个属性对最终相异度的影响相同，需要对每个属性的相异度计算结果进行数字尺度转换。

$$d(X_j, Z_i) = d_m(X_j, Z_i) + d_n(X_j, Z_i) \qquad (3.1)$$

公式中，$d(X_j, Z_i)$为购电记录 X_j与售电记录 Z_i的相异度，相异度最小的购电记录与售电记录为最优匹配，X_j为 第 j 个购电记录，Z_i 是第 i 个售电记录。

$d_m(X_j,Z_i)$为单价、电量、环保指数、用户信用值、传输损耗等数值属性的相异度。具体计算方法如公式(3.2)所示，公式中 P 表示数值属性的个数，α_p 表示属性 p 的权重，则$(X_{jp}-Z_{ip})^2$ 为属性 p 的购电记录和售电记录的欧氏距离的平方。

$$d_m(X_j, Z_i) = \sum_{l=1}^{P} \alpha_l (X_{jl} - Z_{il})^2 \qquad (3.2)$$

$d_n(X_j,Z_i)$为能量类型等非数值属性的相异度，计算方法如公式（3.3）和公式（3.4）所示，公式（3.3）中，Q 表示非数值属性个数，β_q 表示属性 q 的权重。

$$d_n(X_j, Z_i) = \sum_{q=1}^{Q} \beta_q \delta(X_{jq}, Z_{iq}) \qquad (3.3)$$

如公式(3.4)所示，当购电记录 X_{jq} 和售电记录 Z_{iq} 的属性 q 不相同时，相异度为 1，相同为 0。

$$\delta(X_{jq}, Z_{iq}) = \begin{cases} 1, X_{jq} \neq Z_{iq} \\ 0, X_{jq} = Z_{iq} \end{cases} \qquad (3.4)$$

电力交易撮合记录的具体信息如表 3.5 所示，交易价格为售电记录中的售电价格； 输电损耗是指根据供电地点与购电地点的距离计算的实际电力传输损耗；售电记录 ID 和购电记录 ID 主要用于追溯电力交易记录的来源。

表 3.5. 电力交易撮合记录

Pre-matching Record ID	Electricity seller ID	Private Key Signature of Electricity Purchaser	Trading Price	Electricity for Periodic Trading	Environmental Protection Index	Transmission Loss	Electricity Sales Records ID	Electricity Purchase Record ID

阶段六：售电者从区块链获取电力交易撮合记录并签署授权，完成撮合后生成电

力交易撮合记录和售电记录，并存储在链上。

该部分对应图 3.3 中的步骤 10-12，电力交易匹配记录的具体信息如表 3.6 所示。表中售电方私钥签名表示售电方对电力交易的许可，没有售电方私钥签名的匹配记录不视为有效记录。售电者有权否决交易。如果他不同意售电，他可以不使用他的私钥签署售电匹配记录。

表 3.6. 电力交易撮合记录

Matching Record ID	Electricity seller ID	Private Key Signature of Electricity seller	Private Key Signature of Electricity Purchaser	Trading Price	Electricity for Periodic Trading	Environmental Protection Index	Transmission Loss	Electricity Sales Records ID	Electricity Purchase Record ID

新售电记录中的 Cycle Available Electricity 为完成本次交易后的剩余电量。如果剩余电量为 0，则不会产生新的销售记录。

阶段七：交易撮合结算合约通过电力交易撮合记录中的公钥解密技术验证售电者的私钥签名。验证成功后，电力交易完成，生成电力交易记录并存储在链上。

该部分对应图 3.3 中的步骤 13-15，电力交易记录的具体信息如表 3.7 所示。表中，电力交易匹配记录 ID 主要用于追溯交易记录的来源。

表 3.7. 电力交易记录

Transfer ID	Electricity seller ID	Matching Record ID	Private Key Signature of Electricity Purchaser	Trading Price	Electricity for Periodic Trading	Transfer Amount

3.3.2 其他系统设计

本章研究结合 Hyperledger Fabric 项目[62]开发并实现了一个基于多因素电力交易撮合机制的系统。其中售电节点、购电节点和监管节点是 Hyperledger Fabric 项目中的 Peer 节点，方便用户进行数据上链操作；排序节点为 Orderer 节点，主要用于收集 Peer 组织中的区块链交易。针对能源微网中存在多个区块链基础服务节点（即 Orderer 节点）的场景。在这个场景下，共识过程中不会出现节点主动作恶，普通用户（Peer 节点）可能在交易撮合匹配、交易合同签订和执行过程中作恶。基于上述场景特点，本章采用 Raft 共识进行设计与实施。具体数据流程

如图 3.4 所示，Raft 共识流程如图 3.5 所示。

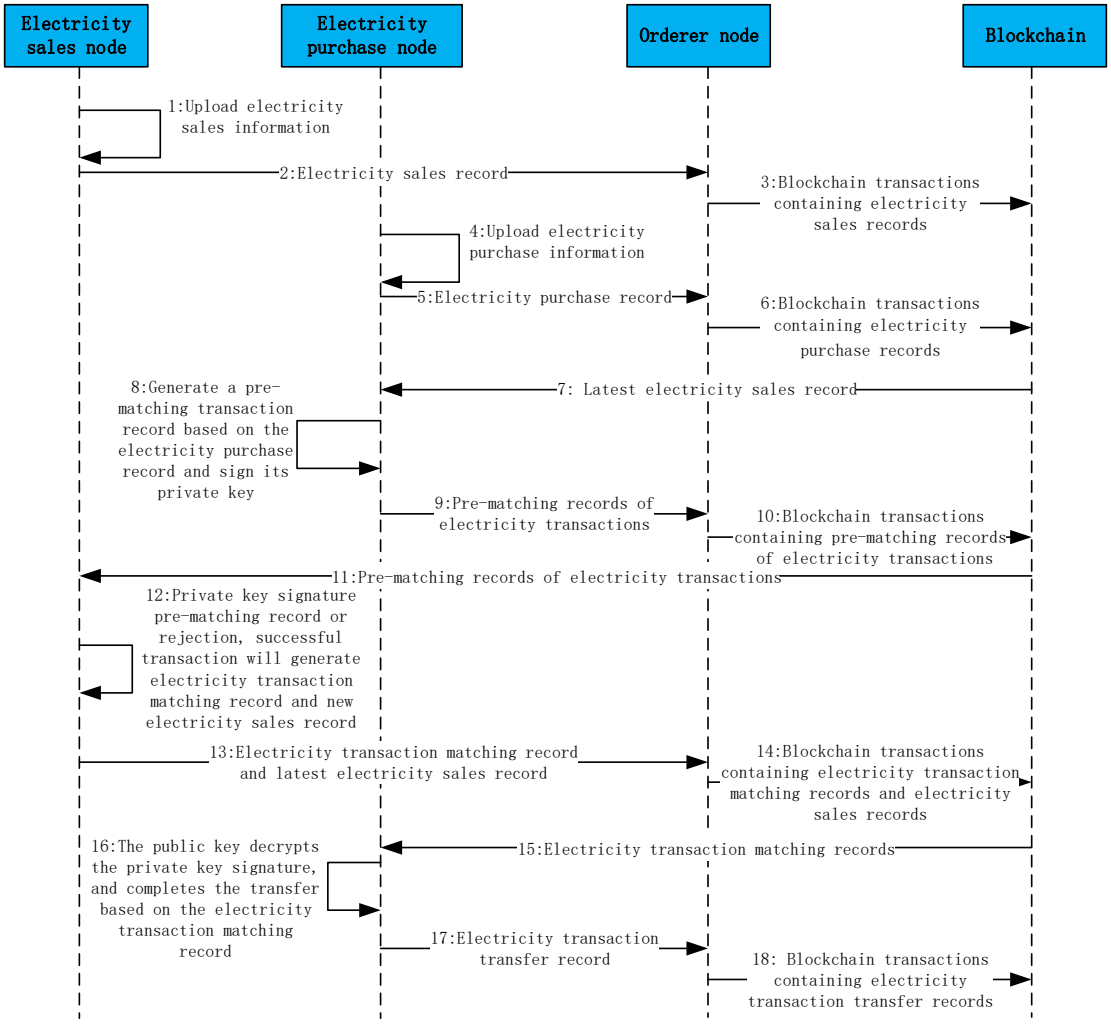


图 3.4. 多因素电力交易撮合机制流程序列图。

在为 REI 构建区块链网络时，首先需要完成系统管理员 Peer 节点和 Orderer 节点的部署。新用户 Peer 节点加入区块链网络后，系统管理员 Peer 节点远程实例化并安装智能合约，完成 REI 的区块链网络建设。

如图 3.5 所示，普通用户上传购电信息后，对应的 Peer 节点将其封装成区块链交易发送给特定的 Orderer 节点； Orderer 节点将区块链交易发送给 Orderer 节点作为 Leader； Leader 节点将区块链交易发送给所有属于 Follower 身份的 Orderer 节点；Follower 节点确认区块链交易并将确认信息返回给 Leader 节点；Leader 节点收到大部分 Follower 节点的确认信息后，将区块链交易的确认信息发送给所有 Follower 节点；所有 Follower 节点完成区块链交易的链上存储；所有 Peer 节点通过 Orderer 节点完成新区块的同步链上存储。

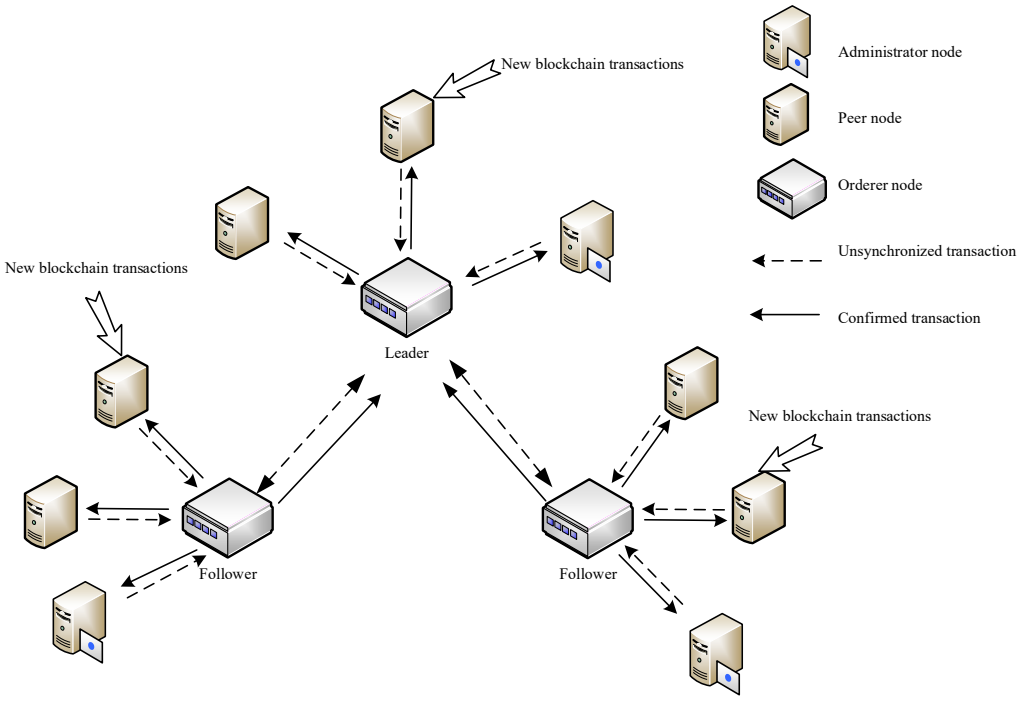


图 3.5. 系统 Raft 共识过程。

3.4 电力交易的隐私保护

区块链中的用户交易数据公开透明，随之带来的是用户的隐私保护问题。攻击者能够通过分析交易记录获得有价值的信息，例如资金流向和交易内容等，而用户往往不希望这些信息被其他人探知。在某些交易流程中，攻击者甚至可以探知交易计划和撮合匹配记录，进而掌握用户交易动向，破坏市场秩序。此外，区块链去中心化的网络分布结构，难以阻断交易数据的传播和外泄，因此，用户的匿名性也就是身份隐私也需要考虑在内。

由此，对应上节中的电力交易及异步结算方案设计，本节提出一种基于区块链的能源交易隐私保护方法，利用零知识证明算法以及同态加密算法，解决现有的区块链能源交易中存在的数据隐私泄露问题以及用户身份暴露的技术问题。

具体地，本节设计的方法使用同态加密算法，在实现保护用户身份隐私的情况下对区块链能源交易中各个流程进行验证，在实现保护数据隐私的同时支持用户之间的撮合计算，在不泄露具体数值的情况下完成最优匹配；通过以上两种算法的结合，既保证用户在区块链中存储的数据不被探知和分析，又能够保护能源交易过程中双方用户的身份隐私，实现了对区块链能源交易中用户身份隐私和数据隐私的双重保护。

3.4.1 零知识证明和同态加密算法

零知识证明技术是一种用于隐私保护的密码学技术，证明者可以证明一组数据满足某种关系，而不透露该数据的具体内容。零知识证明技术可以用来实现私密状态下的数据验证，以实现隐私保护。本节中设定要证明的关系等式的证明密钥为 gk，验证密钥为 vk。使用 gk 生成证明 proof，使用 vk 验证 proof 的正确性；生成函数用 ***Gen***(gk, data)表示；验证函数用 ***Ver***(vk, data)表示。生成函数需要使用关系等式中包含的所有参数生成 proof，而验证 proof 只能使用公开的参数进行证明。

同态加密技术，即非对称同态加密，是基于数学难题的计算复杂性理论的密码学技术。对经过同态加密的数据进行处理得到一个输出，将这一输出进行解密，其解密后的结果与用同一方法处理未加密的原始数据得到的输出结果是一样的。本节中，设使用公钥 pk 进行加密，使用私钥 sk 进行解密。加密函数用 ***Enc***(pk, data)表示；解密函数用 ***Dec***(sk, data)表示。

本节使用零知识证明和同态加密算法对能源用户在区块链中的匿名信息以及匿名交易计划提供隐私保护。

匿名信息即利用零知识证明技术实现的链上数据，包括本章提到的各种单方申明上链存证的信息，包括售、购电计划等。这些信息将在链上不直接标明所有者的身份，所有者通过持有秘钥来控制该数据，并通过生成零知识证明来对外验证数据的所有权。匿名信息没有明确的身份标记，可以保护电力交易双方的隐私。

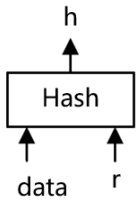


图 3.6. 匿名信息的实现原理图

匿名信息的实现原理如图 3.6 所示，上链的信息被隐藏在一个哈希值当中。匿名信息用 h 表示，h 的计算方法为：h = ***H*** (data || r)。

data 指的是需要上链的数据，例如该信息为发电计划等；r 为一个随机的私密值，其作用为防止数据被暴力破解。

由于匿名信息不带有身份标识，因此除所有者以外的用户无法从链上得知数据的归属。

匿名信息的使用规则为：

a. 用户根据数据中包含的数据生成零知识证明 proof；

b. 在使用过程中附带该 proof 用于验证，共识过程中，其他用户将会计算该 proof 是否满足验证需要，满足则可以证明该用户拥有该项数据。

例如，用户要证明其发电能力，则该用户用自己发电能力的记录 G、发电能力 v、私密值 r 生成零知识证明 proof，证明其满足的关系为：$G = \boldsymbol{H}(v \| r)$。

所有参数中可以公开的仅仅为 G 和 proof，其他用户在对该事务进行共识时，只需要使用 G 来验证 proof 的正确性，即可承认该用户对该匿名信息使用的合法性。

考虑到一些数据使用后会有新数据产生，则新数据仍以该形式表示，用户需要为新数据生成新的私密值，该新数据同样需要证明。

例如某用户结算账户余额 B 的数值为 b，使用部分余额 b_n 进行结算后，剩余的余额 B'的数值为 b'，则该用户应当为剩余余额提供一个新的私密值 r'，且证明这些数据满足如下关系：

1）$B = \boldsymbol{H}(b \| r)$；

2）$B' = \boldsymbol{H}(b' \| r')$；

3）$b - b_n = b'$；

对于该关系下生成的 proof，其他用户可以用公开的 B 和 B'来验证 proof 的正确性。

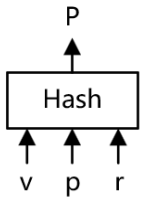


图 3.7 匿名交易计划的实现原理图

匿名交易计划的实现原理如图 3.7 所示，主要有售电计划和购电计划两种类型，其结构是相似的，可以用 P 来表示，P 的计算方法为：

$P = (v \| p \| r)$；其中，v 表示计划售/购电量；p 表示计划售/购电价格及其他

匹配参数；r 为一个随机的私密值，其作用为防止信息被暴力破解。

对于售电计划来说，其售电量不能超过该用户所拥有的发电能力。售电用户要制定一个售电计划时，需要构造上述参数并生成零知识证明，证明其满足如下关系：

1）$G = \boldsymbol{H}(v_g \| r_g)$；

2）$P_s = \boldsymbol{H}(v_s \| p_s \| r_s)$；

3）$v_g >= v_s$；

其中公开用于验证的参数为发电能力 G 和售电计划 P_s。

对于购电计划来说，其购电计划的总费用不能超过该用户所拥有的余额。购电用户要制定一个购电计划，需要构造上述参数并生成零知识证明，证明其满足如下关系：

1）$B = \boldsymbol{H}(b \| r_b)$；

2）$P_p = \boldsymbol{H}(v_p \| p_p \| r_p)$；

3）$b >= v_p \times p_p$；

其中，公开用于验证的参数为账户余额 B 和购电计划 P_p。

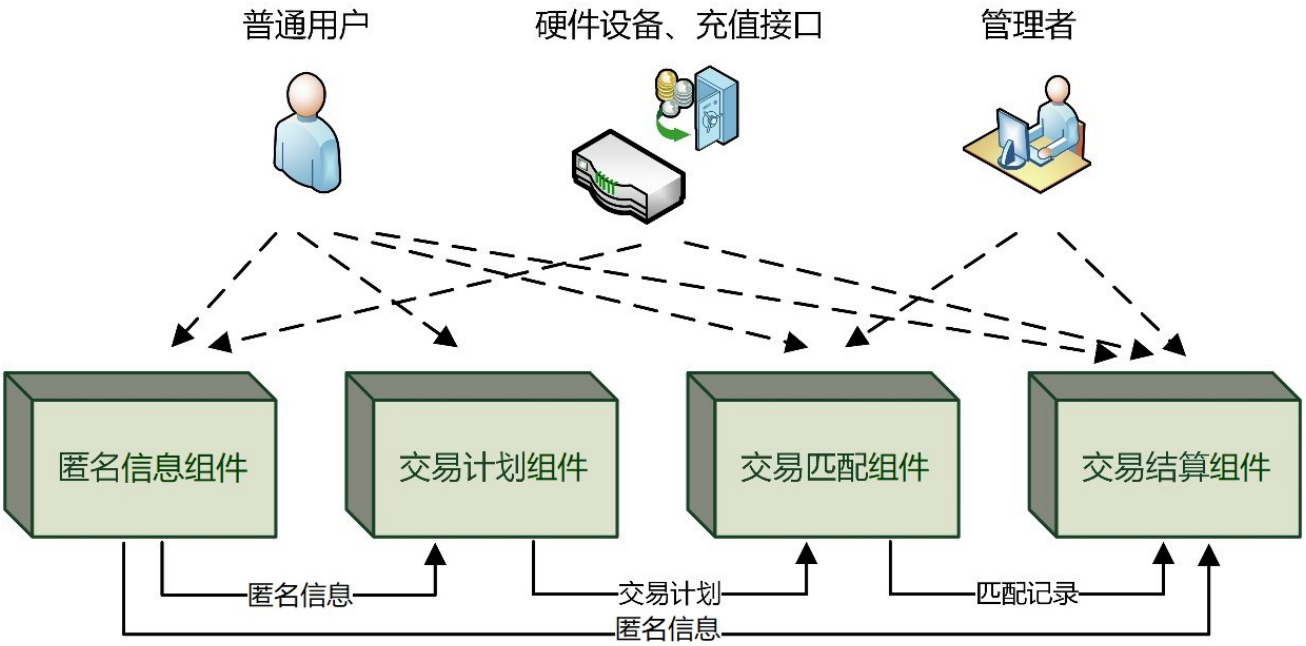


图 3.8 基于区块链的能源交易隐私保护方法中参与用户的示意图

如图 3.8 所示，本节设计的基于区块链的能源交易隐私保护方法中的用户分为四类：

第一类是普通用户，普通用户可以作为售电用户或者购电用户参与能源交易；

第二类是监管节点，负责管理系统的密钥和参与隐私保护交易的监督；

第三类是能量路由器硬件设备、充值接口，负责提供可靠的数据记录和资产；

第四类是区块链基础服务节点，负责区块链交易的处理；

其中，普通用户拥有 gk、vk 和 pk；监管节点拥有全部类型的密钥，包括 gk、vk、pk 和 sk，能够与普通用户进行数据分享与监管；能量路由器硬件设备、充值接口拥有 pk，能够与普通用户进行数据分享。

3.4.2 电力交易隐私保护方法

本节提出的能源交易隐私保护方法包括如下步骤：

1. 售电用户结合自身的发电记录，制定售电计划，并根据发电记录和售电计划生成零知识证明，同时使用同态加密算法生成售电计划密文；将发电记录、售电计划、零知识证明和售电计划密文发送到区块链中进行验证并存储。

具体地，售电用户使用同态加密算法将售电计划中的出售电量、售电价格以及用于匹配计算的参数进行加密，生成售电计划密文，售电计划密文与售电计划一起存储。

发电记录至少包括发电量以及私密值。其中，发电记录在区块链中的存储形式为发电量和私密值合并生成的哈希值。

售电计划至少包括售电量、售电价格以及私密值。其中，售电计划在区块链中的存储形式为售电量、售电价格、私密值合并生成的哈希值。

2. 购电用户结合自身需求制定购电计划，并根据购电用户的账户余额和购电计划生成零知识证明，同时使用同态加密算法生成购电计划密文；将账户余额、购电计划、零知识证明和购电计划密文发送到区块链中进行验证并存储。

购电用户使用同态加密算法将购电计划中的购买电量、购电价格以及用于匹配计算的参数进行加密，生成购电计划密文，购电计划密文与购电计划一起存储。

账户余额至少包括余额数量以及私密值。其中，账户余额在区块链中的存储形式为余额数量、私密值合并生成的哈希值。

购电计划至少包括购电量、购电价格以及私密值。

其中，购电计划在区块链中的存储形式为购电量、购电价格、私密值合并生

成的哈希值。

3. 区块链基础服务节点依据现有的售电计划，使用上节中提到的撮合方法为购电计划进行匹配计算，将生成的撮合记录上传到区块链中进行存储，并将撮合记录参数 P2P 地告知匹配双方。匹配计算使用购电计划和售电计划中的密文以本报告提到的撮合算法进行计算得出的撮合结果。

区块链基础服务节点进行匹配计算的具体过程如下：

a. 对于一个购电计划，从现有的售电计划中取一个售电计划，利用该购电计划对应的购电计划密文与当前售电计划对应的售电计划密文进行匹配计算；

b. 重复以上匹配计算过程，直到现有的售电计划中所有售电计划均与该购电计划完成匹配计算，然后选取最优进行撮合，得到撮合记录。

其中，撮合记录参数至少包括售电计划、购电计划、交易电量、交易价格以及私密值。撮合记录参数在区块链中的存储形式为以上信息合并生成的哈希值。区块链基础服务节点使用同态加密算法将撮合记录参数中的交易电量进行加密处理，生成交易电量密文；将生成的交易电量密文与撮合记录一起存储。

4. 匹配双方分别生成零知识证明，并上传到区块链中验证并存储，确认为匹配记录。确认为匹配记录的具体过程如下：

对于撮合记录参数中的售电计划，售电用户需要生成零知识证明，证明该售电用户是撮合记录中的售电方，验证通过后，售电确认完成；

同时，对于撮合记录参数中的购电计划，购电用户需要生成零知识证明，证明该购电用户是撮合记录中的购电方，验证通过后，购电确认完成。

5. 匹配双方分别按照经过确认后形成的匹配记录进行供电和用电，进而得到实际供/用电记录，实际供/用电记录由能量路由器硬件设备接口提供并上传。实际供/用电记录至少应包括匹配记录、实际供/用电量、私密值。实际供/用电记录在区块链中的存储形式为匹配记录、实际供/用电量、私密值合并生成的哈希值。能量路由器硬件设备接口使用同态加密算法将实际供/用电量加密，生成实际供/用电量密文。

区块链基础服务节点基于生成的交易电量密文与实际供/用电量密文，利用偏差计算函数，计算交易电量与实际供/用电量之间的偏差，根据偏差是否合理，确

定结算定量。判断偏差是否合理的具体过程为：

设定容忍偏差，判断偏差值是否小于容忍偏差值；

经过判断，若偏差小于容忍偏差，则按照匹配记录中的交易电量进行结算；若偏差不小于容忍偏差，则按照实际供/用电量进行结算；得到结算电量。

6. 匹配双方分别生成零知识证明，发送到区块链中验证，确认参与交易并完成结算。具体过程为：

购电用户依据实际供/用电记录，从其账户余额中减去交易费用；购电用户生成的零知识证明，需要证明其对账户余额的更新，还要证明该购电用户参与了交易过程；

售电用户依据实际供/用电记录，在其账户余额中加上交易费用；售电用户生成的零知识证明，需要证明其对账户余额的更新，还要证明该售电用户参与了交易过程；

另外，售电用户需要在区块链中减去交易电量，同时售电用户的发电记录也需要更新。

如上所述，本方法述及了一种基于区块链的能源交易隐私保护方法。其中，该方法使用零知识证明算法，在实现保护用户身份隐私的情况下对区块链能源交易中各个流程进行验证；同时，该方法还使用同态加密算法，在实现保护数据隐私的同时支持用户之间的匹配计算，能够在不泄露具体数值的情况下完成最优匹配；本方法基于零知识证明算法与同态加密算法，既保证用户在区块链中存储的数据不被探知和分析，又能够保护能源交易过程中双方用户的身份隐私，实现了对区块链能源交易中用户身份隐私和数据隐私的双重保护。

能源交易隐私保护方法位于电力交易系统的智能合约模块中，涵盖以下四个功能组件：

a. 匿名信息组件：

用于记录所有用户的匿名信息，参与者为普通用户和能量路由器硬件设备、充值接口。

所述匿名信息，至少应包括发电记录和账户余额，对于某项匿名信息，只有该资产的所有者知道其明确数值且具有使用权，区块链中的其他用户则无法得知。

该匿名信息组件的功能为：

新增一项资产记录；查找某个特定的资产记录；删除使用过的资产记录。

其中，匿名信息包括发电记录和账户余额，发电记录由相应的能量路由器硬件设备接口上传存储；账户余额可以通过相关充值接口获取，也可以通过交易获取。

b. 交易计划组件：

用于用户制定并记录交易计划，参与者为售/购电用户。

该交易计划组件的功能为：依据发电记录制定售电计划；依据账户余额制定购电计划。

c. 交易撮合匹配组件：

其功能为对系统中存在的售/购电计划执行匹配计算，进行撮合，生成撮合记录；交易双方对撮合记录进行确认形成匹配记录。参与者为区块链基础服务节点、售/购电用户。

d. 交易结算组件：

用于完成购电用户与售电用户间的结算，其中购电用户根据实际用电记录支付费用，并生成支付记录，售电用户将支付费用转入自己的账户；

交易结算组件的参与者为区块链基础服务节点、售/购电用户、能量路由器硬件设备接口。

该交易结算组件的功能为：上传实际供/用电记录；计算实际供/用电量与匹配记录中电量的偏差；购电用户支付费用；售电用户收取费用。

特别地，本节中区块链指的是一般意义下的区块链技术，不限于本章所提出的机制及系统。出于隐私保护需要的需要，方法流程中未提及使用数字签名的步骤中可不包含数字签名。

该基于区块链的能源交易隐私保护方法中所使用到的参数，除非直接说明其公开或存储于区块链中，默认只有操作者知晓，且使用过程不被区块链所记录。

3.4.3 电力交易的隐私保护算法实现

下面对利用零知识证明算法以及同态加密算法以实现本方法的具体算法过程进行说明：

a. 售电用户结合自身的发电记录，制定售电计划，并根据发电记录和售电计

划生成零知识证明，发送到区块链中进行验证并存储。

售电用户拥有的发电量为 v_g，其发电记录 G 表示为：

$G = \boldsymbol{H}(v_g \| r_g)$；

其中，r_g 表示一个随机的私密值；

售电用户计划的出售电量为 v_s，售电价格为 p_s，其售电计划 P_s 表示为：

$P_s = \boldsymbol{H}(v_s \| p_s \| r_s)$

其中，r_s 表示一个随机的私密值；

售电用户使用参数 G、v_g、r_g、P_s、v_s、p_s、r_s 生成零知识证明 $proof_s$，其生成方法为：

$proof_s = \boldsymbol{Gen}_s(gk, G, v_g, r_g, P_s, v_s, p_s, r_s)$；

其中，gk 表示证明秘钥；

售电用户将发电记录 G、售电计划 P_s 以及零知识证明 $proof_s$ 发送到区块链中验证并存储，区块链中其他用户验证该售电计划 P_s 是否合法的方法为：

1）发电记录 G 为区块链中存在的发电记录；

2）$r = \boldsymbol{Ver}_s(vk, G, P_s, proof_s)$ 且 r 为真；

其中，vk 表示验证秘钥；验证通过后该售电计划 P_s 合法，并存储到区块链中。

同时，售电用户还要使用同态加密算法将出售电量 v_s、售电价格 p_s 以及其他用于匹配计算的参数 $para_s$ 加密生成密文，密文的生成方法为：

$CT_s = \boldsymbol{Enc}(pk, v_s, p_s, para_s)$

其中，pk 表示公钥，CT_s 表示售电计划密文；

将生成的售电计划密文 CT_s 与售电计划 P_s 放在一起存储。

b. 购电用户结合自身需求制定购电计划，并根据账户余额和购电计划生成零知识证明，发送到区块链中进行验证并存储。

购电用户的账户余额 B 表示为：

$B = \boldsymbol{H}(b \| r_b)$；

其中，b 表示账户余额 B 的数值，r_b 表示一个随机的私密值；

购电用户计划的购买电量为 v_p，购电价格为 p_p，其购电计划 P_p 表示为：

$P_p = \boldsymbol{H}(v_p \| p_p \| r_p)$；

其中，r_p 表示一个随机的私密值；

购电用户使用参数 B、b、r_b、P_p、v_p、p_p、r_p 生成零知识证明 $proof_p$，其生成方法为：

$proof_p = \boldsymbol{Gen}_p(gk, B, b, r_b, P_p, v_p, p_p, r_p)$；

其中，gk 表示证明秘钥；

购电用户将账户余额 B、购电计划 P_p 以及零知识证明 $proof_p$ 发送到区块链中验证并存储，区块链中其他用户验证该购电计划 P_p 是否合法的方法为：

1）账户余额 B 为区块链中存在的账户余额；

2）$r = \boldsymbol{Ver}_p(vk, B, P_p, proof_p)$ 且 r 为真；

其中，vk 表示验证秘钥；验证通过后该购电计划合法，并存储到区块链中；

同时，购电用户还要使用同态加密算法将购买电量 v_p、购电价格 p_p 以及其他用于匹配计算的参数 $para_p$ 加密生成购电计划密文，密文的生成方法为：

$CT_s = \boldsymbol{Enc}(pk, v_p, p_p, para_p)$

其中，pk 表示公钥，CT_s 表示购电计划密文；

将生成的购电计划密文 CT_p 与购电计划 P_p 放在一起存储。

c. 区块链基础服务节点依据现有的售电计划和购电计划进行匹配计算，将加密的撮合结果上传到区块链中进行存储，并将解密后的结果由链下告知双方。

区块链基础服务节点进行匹配计算的方法为：

对于一个购电计划 P_p，取一个售电计划 P_s，使用购电计划密文 CT_p 和售电计划密文 CT_s 进行安全计算，交易撮合算法表示为 F，则匹配计算的方法为：

1）$CT_r = F(CT_p, CT_s)$；

2）$t = \boldsymbol{Dec}(sk, CT_r)$；

其中，CT_r 为加密的匹配结果，t 为解密后的匹配结果，sk 表示私钥；

区块链基础服务节点重复以上匹配计算过程，直到所有售电计划均与该购电计划完成匹配计算，然后选取匹配结果最优的售电计划与该购电计划进行撮合；

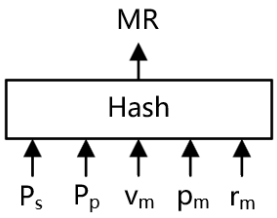


图 3.9 撮合记录的表示示意图

如图 3.9 所示，撮合记录 MR 表示为：$MR = \boldsymbol{H}(P_s \| P_p \| v_m \| p_m \| r_m)$；

其中，v_m 为交易电量，p_m 为交易价格，r_m 为私密值；

区块链基础服务节点将撮合记录 MR 发送到区块链中存储，并将撮合记录的参数通过链下告知双方；

区块链基础服务节点使用同态加密算法将交易电量 v_m 加密生成密文，密文的生成方法为：

$CT_m = \boldsymbol{Enc}(pk, v_m)$；

其中，pk 表示公钥，CT_m 表示交易电量密文；

将生成的交易电量密文 CT_m 与撮合记录 MR 放在一起存储。

d. 售电和购电用户分别生成零知识证明确认撮合记录形成匹配记录，并上传到区块链中进行存储。

撮合记录生成后不会立即生效，需要等待售、购双方进行确认，任何一方不进行确认，交易都不会进行下去。

售电用户进行确认时需要证明自己是该撮合记录的售电方，而拥有售电计划的证明是拥有全部参数 v_s、p_s、r_s，因此：

对于撮合记录中的售电计划 P_s，售电用户需要生成零知识证明 $proof_{ms}$ 证明如下关系：

1）$MR = \boldsymbol{H}(P_s \| P_p \| v_m \| p_m \| r_m)$；

2）$P_s = \boldsymbol{H}(v_s \| p_s \| r_s)$；

其中，MR 和 P_s 公开用于验证；零知识证明 $proof_{ms}$ 的生成方法为：

$proof_{ms} = \boldsymbol{Gen}_{ms}(gk, MR, P_s, P_p, v_m, p_m, r_m, v_s, p_s, r_s)$；

其他用户验证该确认操作是否合法的方法为：

1）撮合记录 MR 为区块链中存在的撮合记录；

2）$r = \boldsymbol{Ver}_{ms}(vk, MR, P_s, proof_{ms})$ 且 r 为真；

验证通过后，售电用户售电确认完成。

购电用户进行确认时需要证明自己是该撮合记录的购电方，而拥有购电计划的证明是拥有全部参数 v_p、p_p、r_p，因此：

对于撮合记录中的购电计划 P_p，购电用户需要生成零知识证明 $proof_{mp}$ 证明

如下关系：

1）$MR = \boldsymbol{H}(P_s \| P_p \| v_m \| p_m \| r_m)$；

2）$P_p = \boldsymbol{H}(v_p \| p_p \| r_p)$；

其中，MR 和 P_p 公开用于验证；零知识证明 $proof_{mp}$ 的生成方法为：

$proof_{mp} = \boldsymbol{Gen}_{mp}(gk, MR, P_s, P_p, v_m, p_m, r_m, v_p, p_p, r_p)$；

其他用户验证该确认操作是否合法的方法为：

1）撮合记录 MR 为区块链中存在的撮合记录；

2）$r = \boldsymbol{Ver}_{mp}(vk, MR, P_p, proof_{mp})$ 且 r 为真；

验证通过后，购电用户购电确认完成，该记录成为匹配记录。

e. 售电用户和购电用户分别按照经双方确认的匹配记录进行供电和用电，得到实际供/用电记录，并与匹配记录进行比对，确定结算电量。

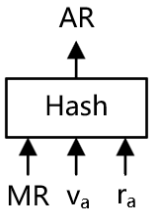


图 3.10 实际供/用电记录的表示示意图

实际供/用电记录由能量路由器硬件设备接口提供并上传，如图 3.10 所示，实际供/用电记录 AR 表示为：

$AR = \boldsymbol{H}(MR \| v_a \| r_a)$；

其中，v_a 为实际供/用电量，r_a 为私密值，v_a 和 r_a 与售电用户和购电用户共享；能量路由器硬件设备接口使用同态加密算法将实际供/用电量 v_a 加密生成密文，密文的生成方法为：

$CT_a = \boldsymbol{Enc}(pk, v_a)$；

其中，CT_a 表示实际供/用电量密文；

考虑到实际情况下用户用电很难与计划完全一致，区块链基础服务节点将实际供/用电量 v_a 与匹配记录中的交易电量 v_m 进行比对，以确定实际传输中的偏差是否在合理的范围内。

偏差计算函数表示为 ***Dev***，该偏差计算方法为：

1）$CT_d = \boldsymbol{Dev}(CT_a, CT_m)$；

2）$d = \boldsymbol{Dec}(sk, CT_d)$；

其中，CT_d 表示加密的偏差结果，d 表示解密的偏差结果；

判断偏差是否在合理的范围内的方式为：

设定容忍偏差 σ，判断偏差 d 是否小于容忍偏差 σ；经过判断：

若偏差 d 小于容忍偏差 σ，则按照匹配记录中的交易电量 v_m 进行结算；若偏差 d 不小于容忍偏差 σ，则按照实际供/用电量 v_a 进行结算，并对实际交易过程中违规的一方进行处罚；

最终，结算电量用 v_f 表示。

f. 双方生成零知识证明，并发送到区块链中进行验证，证明参与交易，并完成结算。

购电用户依据实际供/用电记录，从自己的账户余额中减去交易费用；购电用户不仅需要证明其对账户余额的更新，还要证明购电用户参与了交易过程。

其中，交易费用即结算电量 v_f 与交易价格 p_m 的乘积。

因此，购电用户需要生成零知识证明 $proof_{fp}$，证明如下关系：

1）$B_p = \boldsymbol{H}(b_p \| r_{bp})$；

2）$B_p' = \boldsymbol{H}(b_p' \| r_{bp}')$；

3）$b_p' = b_p - v_f \times p_m$；

4）$MR = \boldsymbol{H}(P_s \| P_p \| v_m \| p_m \| r_m)$；

5）$AR = \boldsymbol{H}(MR \| v_a \| r_a)$；

6）$v_f = v_m$ 或 v_a；

其中，b_p 表示账户余额 B_p 的数值，b_p'表示表示账户余额 B_p' 的数值；r_{bp}、r_{bp}'分别表示一个随机私密值；参数 B_p、B_p'、MR、AR 公开用于验证；

区块链中其他用户验证该确认操作是否合法的方法为：

1）B_p 为区块链中存在的账户余额；

2）AR 为区块链中存在的实际供/用电记录；

3）$r = \boldsymbol{Ver}_{fp}(vk, B_p, MR, AR, B_p', proof_{fp})$ 且 r 为真；

验证通过后账户余额 B_p 更新为账户余额 B_p'，购电用户付款完成；

售电用户依据实际供/用电记录，在自己的账户余额中加上交易费用；售电用户不仅需要证明其对账户余额的更新，还要证明其参与了交易过程；

此外，售电用户需要在区块链中减去交易的电量，发电记录也需要更新；

因此，售电用户需要生成零知识证明 $proof_{fs}$，证明如下关系：

1）$B_s = \boldsymbol{H}(b_s \| r_{bs})$ ；

2）$B_s' = \boldsymbol{H}(b_s' \| r_{bs}')$；

3）$b_s' = b_s + v_f \times p_m$；

4）$MR = \boldsymbol{H}(P_s \| P_p \| v_m \| p_m \| r_m)$；

5）$AR = \boldsymbol{H}(MR \| v_a \| r_a)$；

6）$v_f = v_m$ 或 v_a；

7）$G = \boldsymbol{H}(v_g \| r_g)$；

8）$G' = \boldsymbol{H}(v_g' \| r_g')$；

9）$v_g' = v_g - v_f$；

其中，b_s 表示表示账户余额 B_s 的数值，b_s'表示账户余额 B_s' 的数值；r_{bs}、r_{bs}' 分别表示一个随机私密值；参数 B_s、B_s'、MR、AR、G、G'公开用于验证；

区块链中其他用户验证该确认操作是否合法的方法为：

1）B_s 为区块链中存在的账户余额；

2）AR 为区块链中存在的实际供/用电记录；

3）G 为区块链中存在的发电记录；

4）$r = \boldsymbol{Ver}fs(vk, B_s, B_s', MR, AR, G, G', proof_{fs})$ 且 r 为真；

验证通过后，账户余额 B_s 更新为 B_s'，发电记录 G 更新为 G'，售电用户收款完成。

由以上算法过程不难看出，本方法使用零知识证明算法，能够在实现保护用户身份隐私的情况下，对区块链能源交易中各个流程进行验证；

同时，本方法还使用同态加密算法，能够在实现保护数据隐私的同时，支持用户之间的撮合，在不泄露具体数值的情况下由第三方进行撮合；

本方法通过以上零知识证明算法与同态加密算法的组合，既保证用户在区块链中存储的数据不被探知和分析，又能够保护能源交易过程中双方用户的身份隐私。

3.5 实施和性能评估

3.5.1 实验测试环境

该机制基于 Hyperledger Fabric v1.4.4 实现。实验设备由 5 台 1 核 2GB 虚拟机组成。虚拟机上的操作系统是 CentOS Linux release 7.7.1908/ Ubuntu 18.04.4 LTS。每个虚拟机部署一个 Peer 节点，每个 Peer 连接到微电网中的一个或多个用户。

该机制基于 REI 的应用场景。根据实际情况设置了一系列实验参数。在我们的实验中，REI 包含 5 个微电网，每个微电网对应一个区块链节点，用户通过区块链节点并发提交电力交易信息。每个微电网设置为在 10 分钟内有约 200 个电力用户购买电力。本次 REI 每个周期约有 1000 条售电记录可供购买。本次 REI 用户之间的最大距离为 10000 米，用户可接受的电力传输损耗百分比在 10% 以内，实际电力传输损耗百分比为每 1 公里 1%。电力销售者每个周期总电力供应范围为 10-50kwh，电力购买者一个周期内电力需求范围为 10-20kwh。清洁能源电价区间为 0.5-0.6 元，非清洁能源电价区间为 0.4-0.5 元，购电者预期购电价区间为 0.4-0.6 元。能源有 5 种类型：风能、水能、化石能源、太阳能和生物能源。多因素电力交易中各因素的匹配权重范围为 0-1。实验测试数据基于以上设置随机生成，设置测试周期为 10 分钟。在本章实验中，MBT 设为 2 秒，MMC 设为 50。

3.5.2 结果分析

a. 绿色清洁能源供给比例

为推广绿色清洁能源，采用多因素电力交易撮合机制和 DA 等传统机制进行电力交易撮合，检验两种撮合机制的绿色清洁能源供给比例。清洁能源供给比例的计算方法如公式（3.5）所示。该比率越高，绿色清洁能源的销售越好，越有利于减少环境污染。相关数据从区块链中的匹配记录中获取，统计 1000 笔交易中绿色能源的供应比例。 10 次测试后的结果如图 3.11 所示。

$$\text{Supply ratio of green clean energy} = \frac{\text{Total supply of green and clean energy}}{\text{Total energy supply}} \quad (3.5)$$

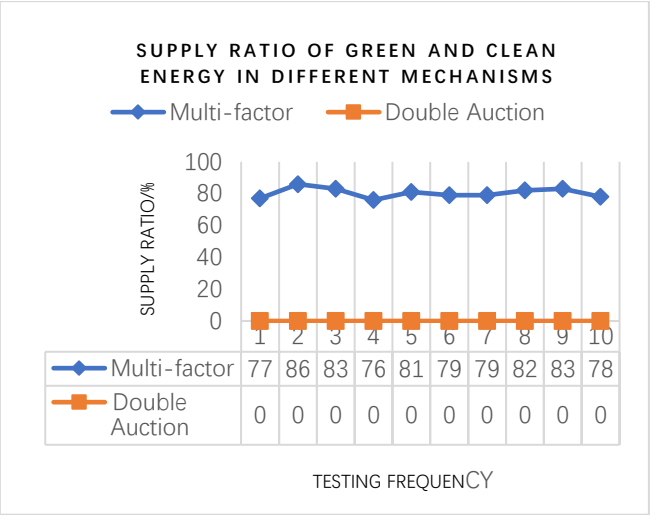


图 3.11. 绿色清洁能源供给比例。

从图 3.11 可以看出，多因素撮合机制匹配的绿色清洁能源约占总能源的 80%，而 DA 匹配机制匹配的绿色清洁能源为 0。因此，这种机制有利于推动小规模清洁能源生产用户积极参与 REI 能源交易，促进绿色清洁能源发展，保护环境。

b. 交易实际单价

根据购电者的利益，采用多因素电力交易撮合机制和 DA 等传统机制进行电力交易撮合，对两种撮合机制的单笔交易电力实际单价（APET）进行检验。单笔交易的实际电价定义为单个用户购买的可用电量的单价。计算方法如公式(3.6)所示。该值越小，传输损耗越低，用户购买成本越低。相关数据从区块链中的匹配记录中获取，统计 1000 笔交易的平均实际单价。 10 次测试后的结果如图 3.12 所示。

$$\mathrm{APET} = \frac{\text{Total purchase of single transaction}}{\text{Total energy of single transaction - Loss energy of single transaction}} \qquad (3.6)$$

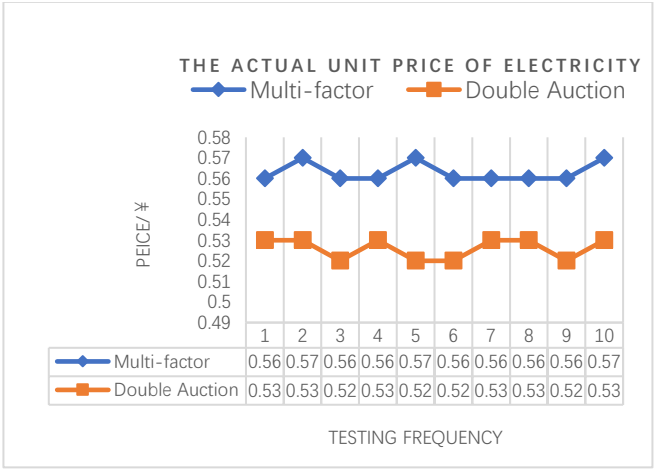


图 3.12. 实际单价对比。

从图 3.12 可以看出，在每次测试 1000 笔购电交易的情况下，经过 10 次测试，多因素撮合机制的实际单价为 0.563 元，DA 匹配的实际单价 0.526 元，实际单位电价差 0.037 元。从实验 a 可以看出，DA 匹配机制匹配的绿色清洁能源供给比例为 0，因此 0.526 元只是非清洁能源的实际单价。从实验测试数据设置可以看出，绿色清洁能源与非清洁能源的价格差距为 0.1 元，0.037 元相比 0.1 元明显缩小。因此，通过这一机制，绿色清洁能源与非清洁能源的实际单价差距缩小了 63%，有效促进了绿色清洁能源的销售。

c. 撮合成交量

根据电力销售商的利益，撮合通常成功更高的利润。采用多因素电力交易撮合机制和 DA 等传统机制进行电力交易撮合，统计测试期内采用两种撮合机制的销售商撮合成功的电量。相关数据从区块链中的匹配记录中获取，统计 1000 笔购电交易的撮合成交量。10 次测试后的结果如图 3.13 所示。

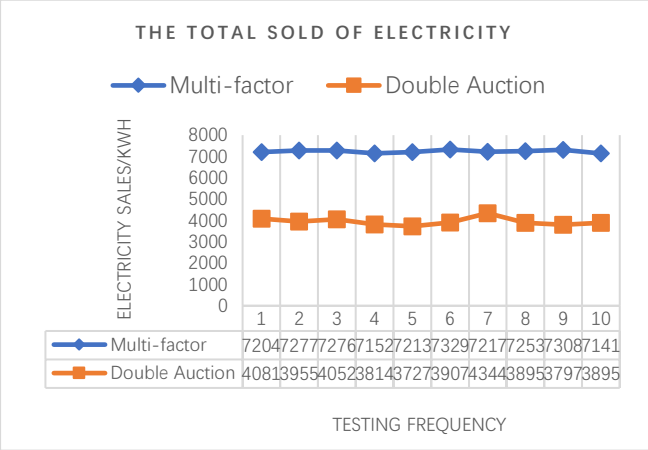


图 3.13. 整体电力销售量。

从图 3.13 可以看出，多因素撮合机制的撮合成交量的平均值为 7237kwh，DA 匹配机制的撮合成交量平均值为 3946.7kwh。该机制使撮合成交量提高了 83%，保证了售电者能够以高于电网收购的价格向购电者出售更多的电力，避免以较低的价格向国家电网公司出售更多的剩余电力，为售电者带来更大的经济效益。

d. 电力交易撮合速度

为证明系统具有一定的实用性，对系统的电力交易匹配速度进行了测试。不同数量的用户通过 5 个区块链节点同时提交用电信息。测试了系统处理每笔交易的平均时间。测试结果如图 3.14 所示。

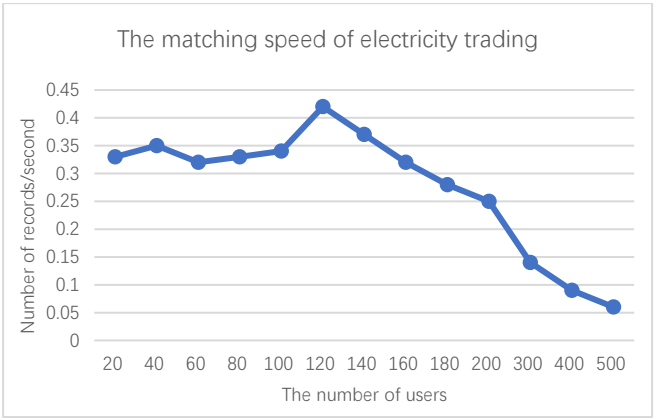


图 3.14. 电力交易撮合速度。

从图 3.14 可以看出，当总用户数在 160 以下时，系统每秒可以完成约 0.35 场电匹配，即完成一场比赛大约需要 2.86 秒。当总用户数在 160 以上时，匹配速度逐渐降低。当总用户数为 120，每个节点对应 24 个用户时，系统匹配速度最快，一次购电需求匹配完成时间约为 2.38 秒。该系统的多因素撮合机制依赖于所有售电需求。在区块高度相同的状态下，每个 Peer 背书通过的匹配请求是互斥的。因此，当每个 Peer 节点对应的用户数量过多时，匹配速度会显着降低。

e. 清洁能源供给比例

对于清洁能源的推广，采用 DA 等传统机制对相同的电力交易实验数据进行匹配，比较两种匹配机制的清洁能源供给比例。结果如图 3.15 所示。

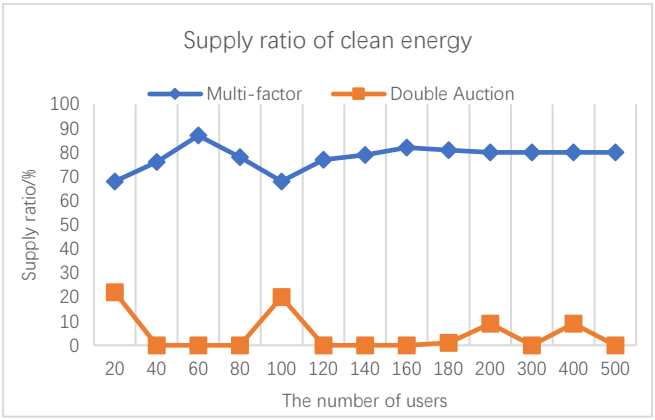


图 3.15. 清洁能源供给占比例。

从图 3.15 可以看出，在不同用户量的各种测试用例中，该系统清洁能源的供应比例约为 78.15%，而传统集中匹配机制的清洁能源供应比例约为 4.69%比如 DA。这一结果充分证明该系统有利于促进清洁能源的销售和发展，保护环境。

f. 总传输损耗

对于远距离传输造成的传输损耗，采用 DA 等传统机制对相同的电力交易实

验数据进行匹配，比较两种匹配机制的总传输损耗。结果如图 3.16 所示。

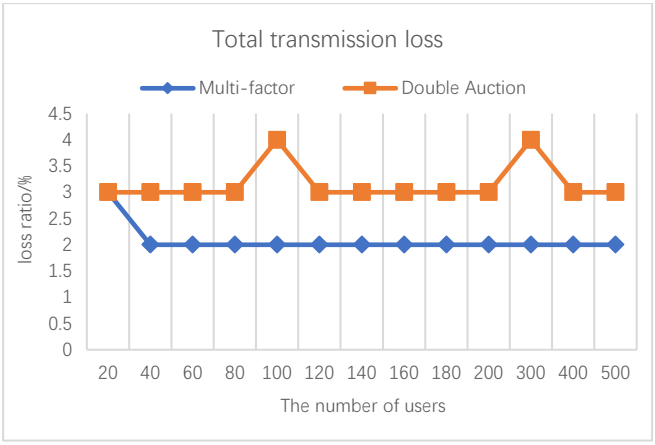


图 3.16. REI 的总传输损耗。

从图 3.16 可以看出，在不同用户量的各种测试用例中，本系统匹配总能量的平均传输损耗率为 2.07%，而总匹配能量的平均传输损耗率为 3.15 % 通过传统的集中匹配机制，例如 DA。因此，减少了 REI 中能量的传输损耗。该系统为整个 REI 节省了 1.08% 的能源。

3.6 总结

本章基于 K-prototypes 聚类的相异度算法，综合计算和比较电价、交易量、传输距离、能源类型等影响电力匹配的因素的总相异度。选择相异度最小的电力记录作为匹配记录。此外，交易平台系统架构设计较第二章更为独立并简化模块间的信息沟通，减弱区块链共识周期对于撮合与结算的影响。基于智能合约设计了相应的自动匹配、私钥签名确认和交易结算功能，实现区块链上单笔交易的自动撮合，匹配结果由电力交易双方控制，并基于零知识证明和同态加密方法设计了电力交易的隐私保护方法和算法实现。共识机制基于进一步分布式的交易及区块链基础设施架构设计。实验验证本节提出的方法与传统方法相比提升了清洁能源交易比例与价格，降低了能源互联网输电损耗，提升了撮合成功率。

第四章 基于线性多目标优化的电力交易区块链多属性偏好撮合机制研究

4.1 介绍

为了更广泛地适应基于区块链的分布式电力交易特点与优势，更充分地进行分布式电力交易供需匹配，本章进一步地基于线性多目标优化方法提出了一种支持拆分买卖需求的多属性偏好能源交易撮合机制以及相应的满意度评估方法，并在交易匹配流程中较第三章细化设计了相应的拒绝机制和循环撮合机制，使交易匹配结果可控并最大化买卖多方的匹配满意度，更灵活地实现多属性偏好的双边匹配算法，更好地满足买卖双方灵活个性化的匹配需求。

在本章讨论的能源互联网微网场景下，能源交易方案的设计可分为交易系统设计和匹配机制设计两个层次。在基于区块链的交易系统设计方面，微电网能源市场允许小规模生产者和消费者就近参与能源交易，促进分布式清洁能源就近消费。 LO3 Energy 运营的 BMG 项目是世界上第一个在区块链上推动 P2P 能源交易的项目 [22]。该项目包括纽约布鲁克林的微电网能源市场 [123]，在 TransActive Grid 私有区块链协议上实施。但是，平台并没有建立比较完善的交易撮合机制。文献[124] 提出了一种使用微电网之间非合作投标的点对点能源交易机制。竞价策略的设计考虑了多维意愿，并在基于区块链的并行交易框架下实现。但多维意愿是指特定时间压力、实时供需关系等因素，不包括用户关心的输电损耗、能源类型等因素。而其多维意愿的计算方法是将多个因素相乘，不按照各个意愿之间的关系进行合并。文献[125]设计了一个 P2P 能源交易平台，并使用博弈论模拟了 P2P 能源交易。但博弈论方法如何在利益最大化的前提下，获得各方都能接受的均衡点是一个非常具有挑战性的问题。而目前的博弈论模型只是一个简单的价格或数量博弈，没有考虑用户行为和偏好。

从撮合机制设计来看，电力交易市场广泛采用双边撮合、连续双重拍卖（CDA）等一大批注重价格属性的撮合机制。文献[126]提出了一种基于区块链和 CDA 的微电网机制，主要关注交易中的报价策略。该机制提供了自适应进取策略，允许

交易者根据市场变化及时调整报价，然后利用 CDA 匹配交易。但是，该机制更侧重于投标策略。文献[127] 提出了一种新的博弈论模型，用于社区中产消者之间的 P2P 能源交易。卖家之间的价格竞争被建模为非合作博弈。该机制在匹配时也不考虑多属性偏好。文献[128]在 P2P 能源交易中提出了一个双边合同网络。发电商、供应商和生产商之间的 P2P 能源交易可以通过网络中的多个中间代理来实现。但不是去中心化的设计。文献[24]为电力交易系统设计了代理联盟机制，使生产者可以联合进行电力交易谈判。但是，设计方案也没有包括很多影响交易形成的属性。文献[129]考虑了能源交易过程中的传输损耗，设计了分布式解决方案。文献[130] 提出了一种使用原始对偶梯度法的新算法，并在事务中考虑了流量限制，以避免系统中的电路过载或拥塞。这两种设计方案考虑了价格以外的属性，但还考虑了一个附加属性。

总的来说，本章的研究做出了以下贡献：

a. 尊重买卖双方的多元交易偏好，分布式设计并实现多属性偏好的双边匹配算法。自由拆分买卖需求以达到更个性化的撮合方案，满足用户的匹配需求。

b. 建立多属性偏好评价方法，计算各属性的匹配满意度，为构建线性多目标优化模型提供了合适的评价基础。

c. 设计拒绝机制和循环匹配机制，使交易匹配结果可控并最大化满意度。

本章的其余部分安排如下。在第二节中，描述了基于区块链的电力交易系统的方案和架构。在第三节中，详细描述了交易双方具有多种匹配需求的双边匹配机制，并建立了基于匹配满意度的优化模型。实验部署和结果分析在第四节讨论。第五节对本章进行总结。

4.2 系统架构和全流程链上交易工作流程

在本章讨论的 REI 微电网范围内，设计具有多属性偏好的基于区块链的能源交易系统，实现 P2P 能源交易。本章中讨论的微电网可以是在该地区具有多个分布式发电机和多个能源需求者的工业园区或社区级电网。微电网能源交易从发起购售电请求到匹配交易再到实现电力结算的整个工作流程应该是安全可靠的。所提出的链上设计可以真正实现每笔交易的公平性和可靠性。此外，尊重微电网中购电者和售电者的多元交易偏好。系统架构如图 4.1 所示。

从图 4.1 可以看出，系统中提供了自动电力交易流程。区块链、分布式发电设备、智能电表、分布式储能设备、能源路由器共同构成了系统的物理架构。区块链除了提供底层数据存储服务外，还利用智能合约进行交易匹配计算。从提交买卖请求到完成交易撮合和结算，整个流程都在区块链上执行，而不仅仅是使用区块链进行安全存储。

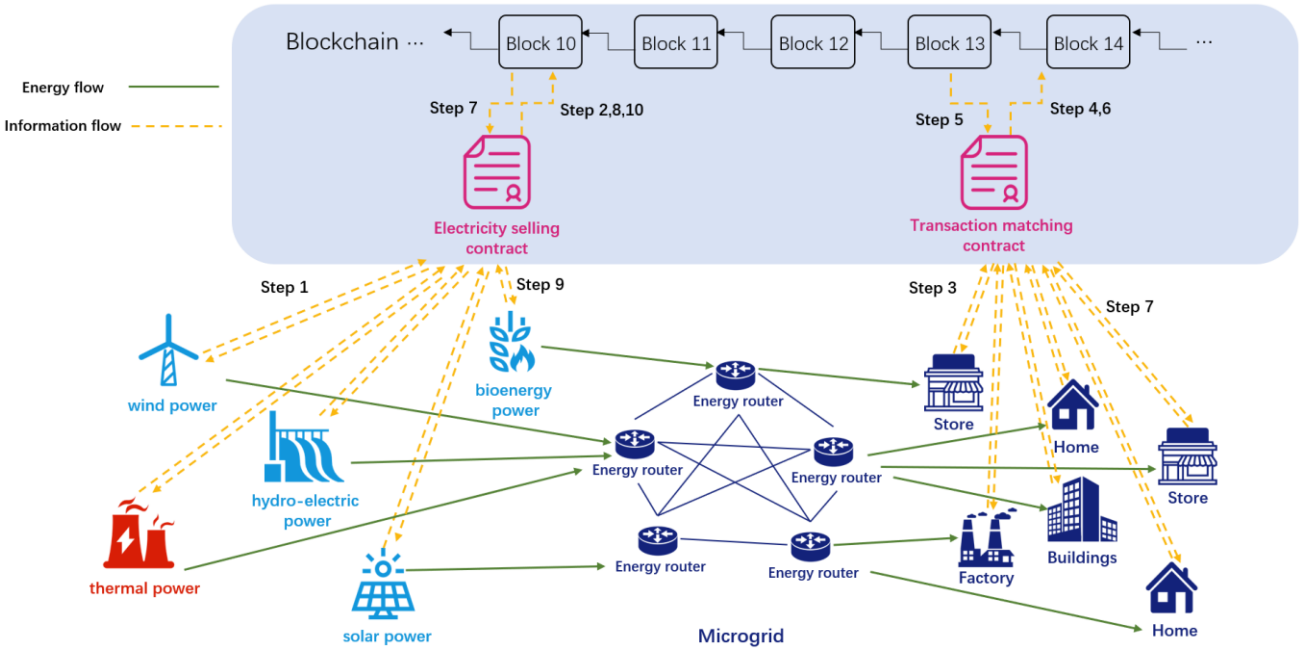


图 4.1 系统架构。

微电网中的多个能源路由器承载多向能量流。售电者是指具有分布式发电能力的实体。发电方式包括风能、水力发电、热能、太阳能和生物能发电。电力购买者是指家庭、商店、建筑物、工厂和其他需要电能的消费者。

微电网中的每个购电者和售电者都维护一个其可达节点列表，包括到可达节点的距离，从而为第四节构建一个加权有向图来估计传输损耗。当一个电力买家或卖家加入基于区块链的微电网时，所有相关节点的可达列表同时更新。

交易流程主要包括以下几个步骤：

第一步，售电者提交售电信息及匹配要求。

在本章讨论的微电网范围内，与主电网相比，用户规模小得多，分布式发电设备多样化，不同的位置会产生不同的输电损耗。这允许每个发电机生成不同的售电信息。对于售电者来说，除了根据实际发电情况提供电价和电力供应外，还可以根据微电网的输电网络估算输电损耗，根据发电方式提供能源类型和环保指标，并提供区块链记录的信誉值。对于购电者，还可以提供购电价格、需求、传

输损耗、信誉值等供售电者匹配。

交易双方的匹配需求的示例见表 4.1、表 4.2。

表 4.1. 售电匹配参数示例。

Selling price	*Supply*	*sTransmission loss*	*Energy type*	*Environment-Protection Index*	*sReputation value*

表 4.2. 购电匹配参数示例。

Purchasing price	*Demand*	*pTransmission loss*	*pReputation value*

售电前，售电者首先向区块链提交其售电信息和要求（为尊重售电者的偏好，本章提出的匹配机制还包括售电者的交易匹配要求）。除 *sTransmission loss*（电源的传输损耗）外，售电者须提供所售电的匹配参数，例如表 4.1 所示的所有售电参数；以及对匹配的购电方的需求，例如表 4.2 中的一个或多个参数。本章中限定售电者可任选示例中的三项作为其偏好。能源类型是指发电类型，包括火电、风电、水电、太阳能和生物能发电；环保指数是指能源类型是否为清洁能源。其中，风电、水电、太阳能、生物质能都是清洁能源； *sReputation* value 由每笔交易累计，总分为 100 分，基值为 60。 信誉值的具体计算方法在步骤 10 中详细说明。

第二步，售电合约生成售电信息并存储在链上。

售电信息中包含售电者的匹配要求。交易如有隐私保护相关需求可采用 3.4 节中所述零知识证明及同态加密方法对交易信息进行加密。

第三步，购电者提交购电信息及配套要求。

购电者在购电前先向区块链提交购电信息及参数和对售电方的匹配偏好。例如表 4.2 所示的所有购电参数，及表 4.1 中一个或多个售电匹配参数。本章中限定购电者任选三个作为其购电偏好。若选择 *pTransmission loss*（购电的传输损耗）则其损耗参数由双方确认。若选择能量类型，应输入所需的能量类型。*pReputation value* 由每笔交易累计，总分 100，基值 60。，

第四步，交易撮合合约生成购电信息并存储在链上。

购电信息中包含对购电者的匹配要求。

第五步，随着购电信息上链，售电者交易撮合合约被触发，则售电者从区块链中读取最新的售、购电信息，根据撮合机制进行交易撮合并上链共识。

第六步，若购电者对撮合结果满意则授权确认撮合结果，并生成交易撮合信息并存储在链上。

第七步，售电者从区块链中获取交易撮合信息，若对匹配结果满意则进行授权。生成电力交易匹配信息和新的售电信息。

新售电信息中记录的电量为本次交易完成后的剩余售电量。如果没有剩余电量，则不会生成新的售电信息。

第八步，售电者将电力交易匹配信息和新的售、购电信息存储在链上。

第九步，购电者从区块链中获取交易撮合信息和售电者私钥签名的电力交易匹配信息，生成新的购电信息。

新购电信息中的电量为本次交易完成后的剩余购电量。如果没有剩余购电量，则不会生成新的购电信息。

交易价格是电力买卖双方所报的平均价格。如果售购电者售出的电量在一场比赛中没有售、购完成，剩余的电量将在下一轮比赛中进行匹配。本章中的循环撮合机制将在多个撮合后电力仍未平衡时，由上级电网兜底购、售。

第十步，异步结算并更新交易双方的信誉值。

声誉值的计算方法是：交易正常完成后，声誉值加 1，否则会受到惩罚，声誉值减 10。初始声誉值为 60，最高为 100，最低的是 0。

4.3 支持拆分买卖需求的多属性偏好撮合机制

能源互联网微网与主电网相比，用户规模小得多，分布式发电设备多样化。这使得每个售电者/购买者能够生成不同的电力销售/购买信息。在这种情况下，在匹配中考虑他们对能源属性（价格、传输损耗、能源类型等）的偏好，可以更好地满足双方对交易的匹配要求，从而提供更加个性化的服务。

本章提出一种基于匹配满意度的双边撮合决策算法，在影响匹配结果的属性中包含了来自交易双方的多个匹配需求。构建基于匹配满意度的多目标优化模型，求解线性规划模型。区块链网络中的所有节点均采用考虑多属性偏好的交易匹配机制（CMAP-Matching）。交易撮合算法流程如图 4.2 所示。

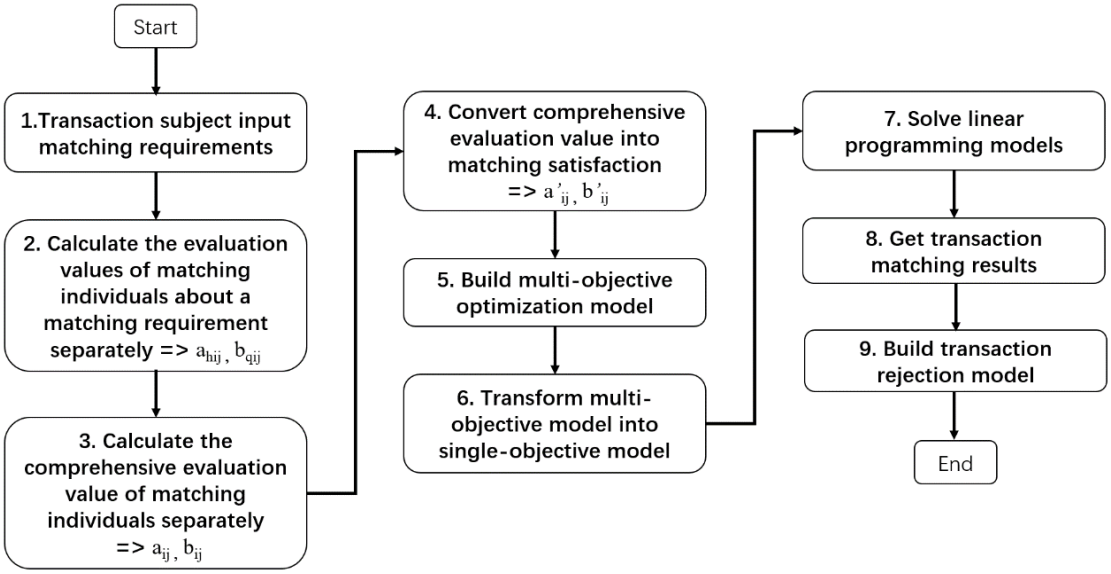


图 4.2. 交易撮合算法流程图

为方便下文对交易撮合机制的详细说明，相关符号定义，如表 4.3 所示。

表 4.3. 本章的符号

Content	Symbol	Description
collection of electricity purchasers	$P=\{P_1,P_2,P_3,\ldots,P_m\}$	A total of m electricity purchasers, P_i represents the i-th electricity purchasers
collection of electricity sellers	$S=\{S_1,S_2,S_3,\ldots,S_n\}$	A total of n electricity sellers, S_j represents the j-th electricity sellers
collection of matching requirements of the electricity purchaser to the electricity seller	$Q=\{Q_1,Q_2,Q_3,\ldots,Q_f\}$	A total of f matching requirements, of which Q_h represents the h-th matching requirement (h=1,2,...,f)
Weight vector corresponding to matching requirement Q	$w=\{w_1,w_2,w_3,\ldots,w_f\}$	Where w_h represents the weight of the indicator Q_h; $0\le w_h\le 1$, $\sum_{h=1}^{f} w_h=1$
collection of matching requirements of the electricity seller to the electricity purchaser	$I=\{I_1,I_2,I_3,\ldots,I_k\}$	A total of k matching requirements, of which I_q represents the q-th matching requirement (1=1,2,...,k)
Weight vector corresponding to matching requirement I	$v=\{v_1,v_2,v_3,\ldots,v_k\}$	Where v_q represents the weight of the indicator I_q; $0\le v_q\le 1$, $\sum_{q=1}^{k} v_q=1$;
Matching satisfaction of electricity purchaser P_i to electricity saler S_j	a_{hij}	It's about matching requirements Q_h's matching satisfaction
Matching satisfaction of electricity saler S_j to electricity purchaser P_i	b_{qij}	It's about matching requirements I_q's matching satisfaction
The comprehensive matching satisfaction of the electricity purchaser P_i to the electricity seller S_j	a_{ij}	$0\le a_{ij}\le 1$,
The comprehensive matching satisfaction of electricity saler S_j to electricity purchaser P_i	b_{ij}	$0\le b_{ij}\le 1$,
The amount of electricity that the purchaser P_i needs to purchase	PE_i	$\sum_{j=1}^{n} SE_j \ge \sum_{i=1}^{m} PE_i$
The amount of electricity that the saler S_j can sale	SE_j	$\sum_{j=1}^{n} SE_j \ge \sum_{i=1}^{m} PE_i$
Trading electricity between P_i and S_j	x_{ij}	Decision variables in matching models

步骤 1. 交易参与者输入匹配要求。

双方信息的输入和撮合需求已在第三节进行描述。

步骤 2. 分别计算匹配个体对匹配需求的评价值。

交易双方对对方的匹配满意度进行评价。对于每一个购电者 P_i，计算每一个售电者 S_j 的 P_i 在某个匹配需求 Q_h 上的匹配满意度：a_{hij}；对于每个售电者 S_j，计算每个购电者 P_i 在某个匹配要求 I_q 上的匹配满意度：b_{qij}。本章将 a_{hij} 和 b_{qij} 设置为 0-10 之间的评价值。评价值为 10 时表示满意度最高，0 表示满意度最低。上一节列出购、售方的几种匹配需求的匹配满意度的计算方法可由如下方法求出：

购电方的匹配满意度评价值：

a. 售价

理想的电力购买/销售价格设置为 $pPrice$ 和 $sPrice$。 $Price_{min}$ 被设置为代表

现实中的最低电价。售电价格满意度的计算方法如下：

如果 $sPrice \le pPrice$，则表示购电者可以以满意的价格进行交易，$a_{hij}=10$；如果 $Price_{min} \le pPrice < sPrice$，则购电价格与售电价格的相似度表示购电者对售电者的满意度。比率越接近，对购买者越好。满意度评价值定义为：

$$a_{hij} = \frac{pPrice}{sPrice} \times 10 \qquad (4.1)$$

如果 $sPrice < Price_{min}$，则被认定为售电者恶意报价以提高售电价格满意度，$a_{hij}=0$。这个设计是为了提醒售电者对自己的报价负责。

b. 供应

若需求为 x_{need}，供给为 x_{supply}，则供给满意评价值的计算方法如下：

若 $x_{need} \le x_{supply}$，则表示售电者的供给完全满足购电者的需求，$a_{hij}=10$；如果 $x_{need} > x_{supply}$，则表示供给不能满足需求。满意度评价值如下：

$$a_{hij} = \frac{x_{supply}}{x_{need}} \times 10 \qquad (4.2)$$

c. *sTransmission loss*

传输损耗包括线路传输损耗和 ER（能源路由器）转换损耗。改进的 Dijkstra 算法用于计算从某个售电者到所有购电者的最短路径。改进的 Dijkstra 算法在计算线路损耗的同时，加上线路上的能量路由器的转换损耗，不仅包含了两个节点之间的最短路径，还显示了更准确的传输损耗 L。

包括 ER 在内的整个微电网抽象为一个带权有向图 $G=(V,E,W)$，边的方向代表能量流动的方向。售电节点、购电节点和 ER 构成图 G 的节点集 V。传输线用于连接售电节点和 ER，ER 之间的互连，ER 和购买节点构成边图 G 的集合 E。线(i,j)的传输损耗 $w(i,j)$和作为边权重的 ERj 的转换损耗 w_j 共同构成图 G 的权重集合 W。其中，线路传输损耗 $w(i,j)$ 是路径长度和线路损耗率 η 的乘积。

在本章讨论的微电网范围内，设置最大传输损耗为 $L_{max}=R_{max} \times \eta$，其中 R_{max} 表示最大供电线路长度。R_{max} 的设置可参考《工业与民用配电设计手册》[131]。*sTransmission loss* 的满意度评价值计算方法如下：

如果 $L > L_{max}$，则认为传输损耗过大，$a_{hij}=0$；如果 $L \le L_{max}$，传输损耗与 L_{max} 的比值代表了它们之间的接近程度。更大的比率意味着更大的传输损失。满意度评价值定义为公式（4.4）：

$$a_{hij} = (1 - \frac{L}{L_{max}}) \times 10 \quad (4.4)$$

d. 能量类型

能源类型包括火电、风电、水电、太阳能和生物能源。 此匹配要求用于允许电力购买者指定他们想要的能源类型。 如果售电者提交的能源类型是购电者选择的能源类型，则 a_{hij}=10，否则 a_{hij}=0。

e. 环保指数

根据能源类型对是否为清洁能源进行分类。除了火电，其他都是清洁能源。

热功率：$a_{hij} = 0$； 否则 $a_{hij} = 10$。

f. *sReputation value*

信誉值最低为 0，最高为 100。将信誉值设为 *sRepVal*，同样利用线性方程来评估信誉值的满意度：

$$a_{hij} = \frac{sRepVal}{100} \times 10 \quad (4.5)$$

售电方匹配满意评价：

a. 采购价格

理想的售电/购电价格设置为 *sPrice* 和 *pPrice*。$Price_{max}$ 被设置为代表现实中的最高电价。 采购价格满意度评价值计算方法如下：

如果 *pPrice*＜*sPrice*，则表示此时售电者没有交易意愿，b_{qij}=0；

若 *sPrice*≤*pPrice*＜$Price_{max}$ ，则表示购买者出价较高，符合售电者的预期，则满意度评价值为：

$$b_{qij} = (1 - \frac{sPrice}{pPrice}) \times 10 \quad (4.6)$$

如果 *pPrice*≥ $Price_{max}$，则认为购电者为了更高的满意度而恶意报价，b_{qij} = 0。

b. 需求

如果需求为 x_{need}，供给为 x_{supply}，则需求满意度评价值的计算方法如下：

如果 $x_{supply} \leq x_{need}$，则表示需求大于供给，b_{qij} = 10；

如果 $x_{need} < x_{supply}$，则用一个线性方程来表达需求的满意度评价：

$$b_{qij} = \frac{x_{need}}{x_{supply}} \times 10 \quad (4.7)$$

c. *pTransmission loss*

pTransmission loss 的满意度评价值的计算与 *sTransmission loss* 的计算相同。

d. *pReputation value*

信誉值设置为 *pRepVal*，信誉值满意度评价值的计算方法如下：

$$b_{qij} = \frac{pRepVal}{100} \times 10 \tag{4.8}$$

步骤 3. 分别计算匹配个体的综合评价

参与撮合的双方选择任意个匹配要求并允许输入权重。匹配购售电的权重集合分别为 w 和 v。 本章中以三个匹配需求为例，w 和 v 的三个权重值均默认设置为 0.5、0.3、0.2，表示对每个匹配需求的关注程度不同。

购电者 P_i 对售电者 S_j 的综合评价值：

$$a_{ij} = \sum_{h=1}^{f'} w_h \times a_{hij} \tag{4.9}$$

售电者 S_j 对购电者 P_i 的综合评价值：

$$b_{ij} = \sum_{q=1}^{k'} v_q \times b_{qij} \tag{4.10}$$

步骤 4. 综合评价转化为匹配满意度

本步骤对数据进行标准化，将综合评价值转化为 0-1 区间内的匹配满意度。使用最小-最大标准化方法。

购电者 P_i 对售电者 S_j 的匹配满意度：

$$a'_{ij} = \frac{a_{ij} - \min_i \min_j a_{ij}}{\max_i \max_j a_{ij} - \min_i \min_j a_{ij}}, i = 1,2,\dots,m;\ j = 1,2,\dots,n \tag{4.11}$$

售电者 S_j 对购电者 P_i 的匹配满意度：

$$b'_{ij} = \frac{b_{ij} - \min_i \min_j b_{ij}}{\max_i \max_j b_{ij} - \min_i \min_j b_{ij}}, i = 1,2,\dots,m;\ j = 1,2,\dots,n \tag{4.12}$$

其中，$0 \leqslant a'_{ij} \leqslant 1$, $0 \leqslant b'_{ij} \leqslant 1$。

步骤 5. 构建多目标优化模型

基于匹配满意度，构建多目标优化模型，最大化交易双方的整体匹配满意度：

$$\begin{cases} \mathrm{Max}Z_1 = \sum_{j=1}^{n} \sum_{i=1}^{m} a'_{ij}\, x_{ij} & (4.13) \\ \mathrm{Max}Z_2 = \sum_{j=1}^{n} \sum_{i=1}^{m} b'_{ij}\, x_{ij} & (4.14) \end{cases}$$

$$\textbf{s. t.} \quad \begin{cases} \sum_{i=1}^{m} x_{ij} \leq SE_j,\ j = 1,2,\dots,n & (4.15) \\ \sum_{j=1}^{n} x_{ij} = PE_i,\ i = 1,2,\dots,m & (4.16) \\ \sum_{i=1}^{m} PE_i \leq \sum_{j=1}^{n} SE_j & (4.17) \end{cases}$$

公式（4.13）和（4.14）是目标函数，即尽可能最大化交易双方的匹配满意度。公式（4.15）、（4.16）和（4.17）是约束条件。 公式(4.15)表明所有购买者从 S_j 购买的电力总和不大于 S_j 出售的电力。 许多具有多个匹配要求的现有优化模型[132,133]具有以下公式：

$$\sum_{i=1}^{m} x_{ij} = 1,\ j = 1,2,\dots,n \qquad (4.18)$$

$$\text{or} \quad \sum_{i=1}^{m} x_{ij} \leqslant 1,\ j = 1,2,\dots,n \qquad (4.19)$$

这意味着每个售电者最多只能匹配一个购买者，这很容易导致在有剩余电量的情况下，出售者无法出售给其他购买者。 CMAP-Matching 中的约束修改为公式（4.15），这意味着卖方可以向多个买方出售电力，只要售电量的总和不超过其可用电力。

公式（4.16）表明 P_i 购买的电力总和必须等于 P_i 的电力需求（PE_i），即满足 P_i 的电力购买需求。 许多具有多个匹配要求的现有优化模型 [132,133] 具有以下公式：

$$\sum_{j=1}^{n} x_{ij} \leqslant 1,\ i = 1,2,\dots,m \qquad (4.20)$$

这意味着每个购电者最多只能匹配一个售电者，这容易导致匹配的售电者可能无法满足购买需求，也无法从其他售电者那里购买。为满足购买需求，将 CMAP-Matching 中的约束修改为公式（4.16），即每个购买者可以从多个销售者处购买电力，满足购买需求。此外，在满足采购需求时，为了避免匹配结果满意度低的交易，设计了匹配流程末端的拒绝模型。当用户对匹配结果不满意时，可以拒绝交易。实验结果表明，当匹配用户数量较多时（购电者和售电者各 500 人），产生的匹配结果较为理想：在所有匹配结果中，满意度最低的 10%仍达到 0.43。另外，与简单的双边匹配相比，在满足采购需求的情况下，CMAP-Matching 在传输损耗和清洁能源比方面具有优势。

公式（4.17）表明，售电的总和应该大于购买的电的总和，以确保可以实现公式（4.16）。

步骤 6. 将多目标模型转化为单目标模型

目标函数转化为隶属度函数。Z_1^{max} 和 Z_2^{max} 设置为分别考虑目标 Z_1 和目标 Z_2 时获得的单目标优化的最优值。 Z_1^{min} 和 Z_2^{min} 是对应的单目标最小值，那么两个隶属函数 $\mu(Z_1)$ 和 $\mu(Z_2)$ 可以定义为：

$$\mu(Z_1) = \frac{Z_1^{max} - Z_1}{Z_1^{max} - Z_1^{min}} \tag{4.21}$$

$$\mu(Z_2) = \frac{Z_2^{max} - Z_2}{Z_2^{max} - Z_2^{min}} \tag{4.22}$$

其中，$0 \le \mu(Z_1) \le 1$，$0 \le \mu(Z_2) \le 1$。 w_1 和 w_2 分别设置为目标 Z_1 和 Z_2 的权重。在这个匹配机制中，双方的匹配满意度同等重要，所以 w_1 和 w_2 都设置为 1/2。新的目标函数如下：

$$\text{MaxZ} = w_1 \mu(Z_1) + w_2 \mu(Z_2) \tag{4.23}$$

公式（4.13）和（4.14）被公式（4.23）代替，原来的多目标问题转化为单目标问题。

步骤 7. 求解线性规划模型

因为优化模型的目标函数和约束都是线性的，所以优化模型是一个线性规划问题。 Big M 方法（一种使用 Simplex 算法解决线性规划问题的方法）用于解决线性规划问题。

步骤 8. 获取交易匹配结果

交易匹配结果为 $x_{ij}=value$ 的形式，其中表示 P_i 和 S_j 之间的交易电量为 $value$。

步骤 9. 构建交易拒绝模型

由于交易撮合模型的建立是为了最大限度地提高交易双方的撮合满意度，因此撮合结果可能会损害某些个人的利益。基于此考虑，本章中的匹配方具有选择权。当他们对匹配结果不满意时，可以拒绝交易。具体的拒绝模型由用户根据自己的期望定义。交易被拒绝后，购电者可以在下一轮重新匹配，卖方可以选择是否将电力出售给上级电网。

4.4 仿真实验

本章所涉及的电力交易系统在 Hyperledger Fabric 上被实现 [62]。区块链系

统基于 Fabric 框架开发，每个售电者、购电者、监管者对应一个 Peer+Orderer 节点。节点负责收集信息并将其封装成区块链交易进行 Raft 共识。 Peer 节点的交易撮合合约中存在撮合机制。

实验设备为华为 2288H V5 服务器，40 核 64GB 内存，分配 5 台 1 核 2GB 虚拟机。挂载在虚拟机上的系统是 CentOS Linux release 7.7.1908。每个虚拟机上部署一个 Peer 节点。每个 Peer 节点可以连接一个或多个用户。

设置电力买卖双方各有 500 个。执行交易匹配所需的最长时间设置为 15 分钟。该系统被设计为每 15 分钟对电力购买和销售请求进行一次交易匹配。匹配由购买者在提交购买请求时触发。触发条件是提交时间距离上次匹配开始时间超过 15 分钟，谁先提交购买需求谁触发撮合及后续步骤。

4.4.1 仿真设置

分别生成 500 个不同的购电者和售电者，在设定的时间间隔内随机生成购电者/售电者的每一个信息。在微电网场景中，实验数据设置如表 4.4 和表 4.5 所示。

表 4.4. 售电信息数据设置

Selling price	*Supply*	*sTransmission loss*	*Energy type*	*Environment-Protection Index*	*sReputation value*
0.3023 -1.4167	48.96 - 453.62	*Longitude*: 116.1038574 -116.7040686 *Latitude*: 39.685167-40.145071	Thermal power/ wind power/ hydropower /solar power/ bioenergy power	whether it is clean energy	60 - 100

表 4.5 购电信息数据设置

Purchasing price	*Demand*	*pTransmission loss*	*pReputation value*
0.3023-1.4167	48.96 - 453.62	*Longitude*: 116.1038574 -116.7040686 *Latitude*: 39.685167- 0.145071	60-100

本章的应用场景包括一般工商业用电，其价格区间较广，故以其价格作为设定价格区间的依据。据了解，北京城区一般工商业用电 1-10kv 电压等级的低电价

和高峰电价分别为 0.3023 元/kW·h 和 1.4167 元/kW·h[134]。因此，为实验设置 $Price_{min}$ = 0.3023 CNY/kW·h 和 $Price_{max}$ = 1.4167 CNY/kW·h。购电价和售电价在区间 $Price_{min}$ - $Price_{max}$ 内随机生成。

根据国家能源局发布的文献[135]，2019 年非城乡居民用电量占全社会用电量的比重较大。因此，非城镇居民月人均用电量以农村居民最高月（12 月）和城乡居民最低月（5 月）作为需求区间的上下限，需求区间为 48.96-453.62kW·h。目前，电力市场采用负荷预测、计划发电等形式来平衡供需。因此，电力供需范围是相同的。

在传输损耗的模拟中，由于随机生成可达节点的不确定性，某些节点可能不可达。因此，本章采用两点之间的直线距离来模拟传输线。虽然无法准确模拟购电者和售电者双方的能量传输路径，但也可以在一定程度上体现两个参与者之间的距离所造成的传输损耗。买卖节点在一定范围内随机生成自己的经纬度，然后根据经纬度计算两点之间的直线距离。随机生成的经纬度范围设置方法如下：根据北京市行政区划[136]，北京市 16 个区平均面积为 1026.66 平方公里。如果抽象成一个圆圈，半径约为 25.55km。以天安门广场（116.403963、39.915119）为中心，以 25.55km 为半径，经纬度范围分别为 116.403963°±0.3001056°和 39.915119°±0.229952°值得注意的是，经纬度范围形成一个正方形区域，因此两点之间的距离有时会超过 25.55km。

4.4.2 与包含多个匹配需求的双边匹配机制比较

本实验的目的是为了证明本章提出的具有多重匹配需求的双边匹配机制，产生了满意度更高、经济效益更高的匹配结果。据了解，现有的交易撮合方式很多是简单的双边撮合，即根据双方报价按高低撮合原则进行撮合。作为简单双边匹配的改进，文献[126]采用连续双拍来持续满足采购需求。这种匹配机制无法提供个性化的匹配服务，容易出现传输损耗过大、清洁能源匹配困难等问题。目前具有多重匹配需求的双边匹配机制仍然有限，文献[132]提出了一种具有犹豫模糊偏好信息的双边匹配决策模型（为描述方便，称为“HFPI-Matching”）。这个方法也包含了双方的多个匹配属性，所以选择比较。每个实验产生 500 个不同的购电者和 500 个不同的售电者，相同数据下两种机制的匹配成功电量对比如图 4.3 所示。

因为在 HFPI 匹配中使用的约束是公式 (4.18) 和 (4.20)，所以存在以下缺点： a)。不保证与买家匹配的卖家能满足需求； b)。对于售电者来说，如果有剩余电量，就无法匹配其他购买者，造成浪费。根据图 4.3 匹配成功电量对比结果，在满足购电者多重匹配需求和购电需求的前提下，CMAP-Matching 匹配成功电量比 HFPI-Matching 匹配成功电量高 25.34% .产生这种结果的原因是将约束修改为公式（4.15）和（4.16），从而可以满足购买需求，并且买方/卖方可以匹配多个卖方/买方。

由公式（4.13）可知，当售电量一定时，满意度为 1 时得到目标值的最大值，为理想情况。以理想的客观值为参考，相同数据下两种方法的客观值（无单位）对比如图 4.4 所示。

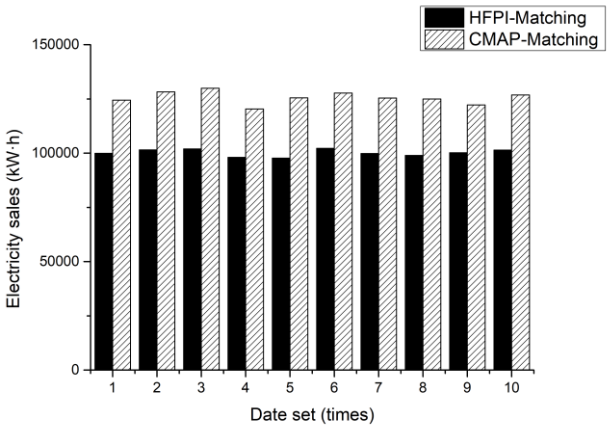


图 4.3. 匹配成功电量的比较。

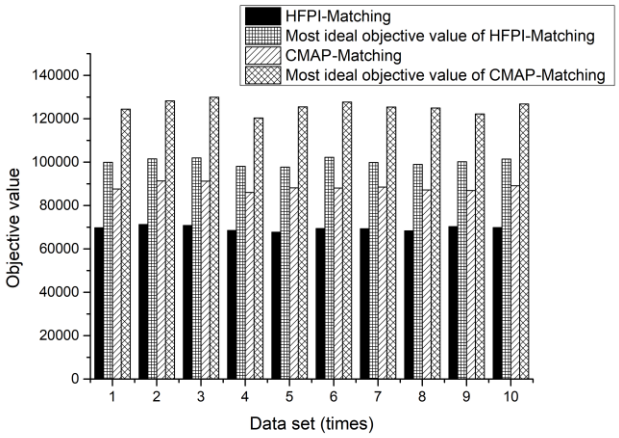


图 4.4. 客观值的比较。

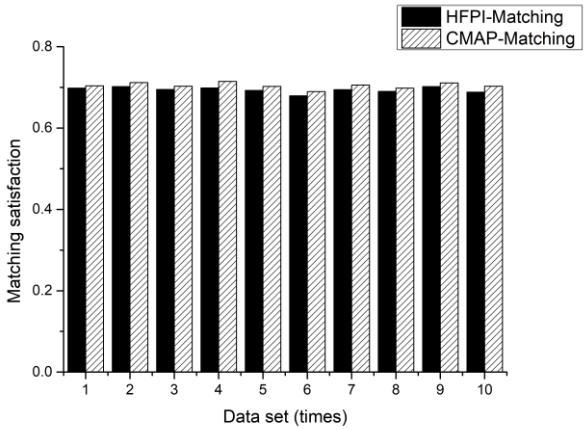


图 4.5. 匹配满意度比较。

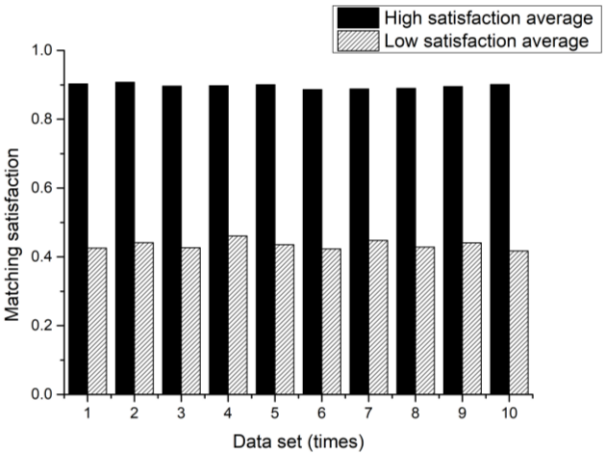


图 4.6. CMAP-Matching 高/低满意度平均值比较。

从图 4.4 中可以看出，CMAP-Matching 的目标值比 HFPI-Matching 的目标值平均高 27.18%，一个显而易见的原因之一是图 4.3 中 CMAP-Matching 结果有更高的销售电量。为研究匹配满意度对目标值的影响，本实验分别计算了两种匹配方式的匹配满意度平均值，如图 4.5 所示。从图中可以看出，两种匹配方式的匹配满意度方法基本相同（CMAP-Matching 往往稍高一些），都在 0.70 左右（匹配满意度是 0-1 之间的一个值）。因此，在满足采购需求、售出更多电量的前提下，CMAP-Matching 的匹配满意度并没有下降，反而略有上升。匹配满意度和匹配成功电量的增加，使得 CMAP-Matching 获得了更大的客观价值。其中，匹配成功电量增加是主要原因。 CMAP-Matching 的匹配结果更好。

图 4.5 展示了匹配满意度的平均值。为了研究匹配结果中的高满意度和低满意度，CMAP-Matching 的高满意度平均值和低满意度平均值定义为：将匹配结果从高到低排序，则高/低满意度平均值为匹配结果排序后的最高 10%/最低 10%的

平均值，如图 4.6 所示。从图中可以看出，高满意度平均值在 0.90 左右，最低满意度的平均值在 0.43 左右。 并且在 CMAP-Matching 中设置了拒绝机制，当用户对匹配结果不满意时可以选择拒绝。

4.4.3 整体最优对一方的损害程度

本实验的目的是解释整体最优与个体最优之间的关系。个体最优性可以定义为单目标最优性：考虑电力销售商或购买者的最佳选择。因为客观值是包括满意度和交易量的整体表现，通过比较客观值可以观察追求整体最优对追求单目标最优的影响程度。计算总体最优结果中购电者和售电者的客观值（分别用 Overall-Purchaser 和 Overall-Seller 表示）。然后与单目标最优性的结果进行比较（分别以最优买方和最优卖方为代表）。每个实验产生 500 个不同的购电者和 500 个不同的购电者。如图 4.7 和图 4.8 所示，目标值没有单位。

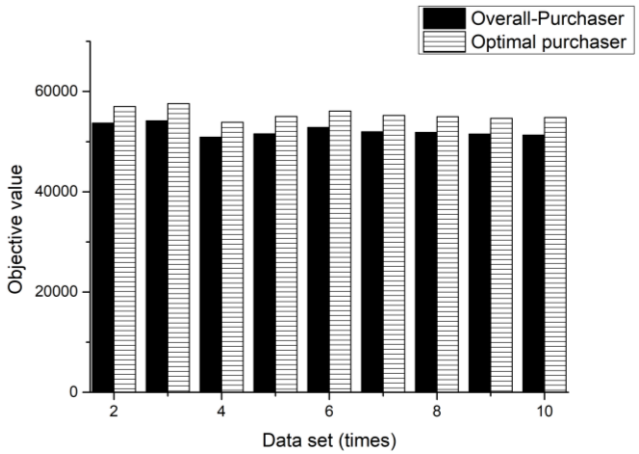


图 4.7. 购电者客观值比较。

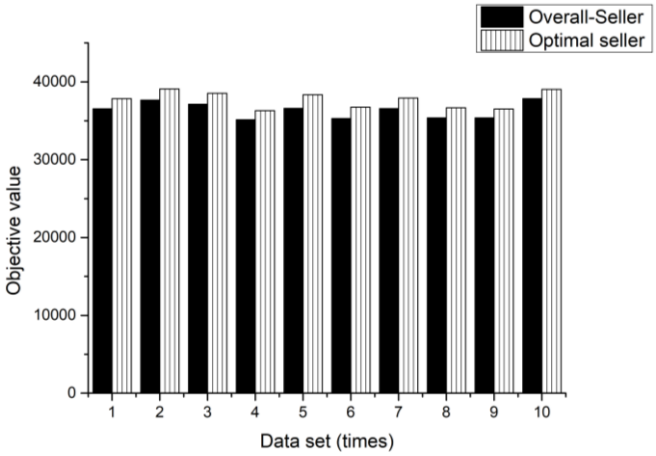


图 4.8. 售电商客观值比较。

从图 4.7 和图 4.8 可以看出，总体最优匹配结果得到的购电者客观值与购电者最优匹配结果相差不大；总体最优匹配结果得到的售电者客观值与售电者最优匹配结果也相差不大。数据的波动是由不同的匹配对象产生不同的匹配满意度引起的。经计算，整体买家目标值达到最优买家目标值的 94.24%；整体卖家目标值达到最优卖家目标值的 96.44%。因此，在基于整体最优目标的匹配结果中，对个体满意度的损害很小，基本可以达到单目标最优结果。

4.4.4 与简单的双边匹配机制比较

本实验的目的是说明 CMAP-Matching 与简单双边匹配的比较，主要侧重于交易价格、传输损耗和清洁能源比例方面的价格属性。本实验中的简单双边撮合是利用以双方报价为基础的高低撮合原则来确定交易主体，并根据边际成交价格进行清算。由于本次实验比较项目为交易价格、输电损耗、清洁能源占比，因此购电者均选择销售价格、*sTransmission loss*、环保指数作为匹配要求。需要说明的是，高低匹配方式中两条价格曲线相交后的交易对象不会形成匹配，因此单纯的双边匹配无法完成所有的买卖请求。本章提出的匹配机制可以满足所有的购电需求。因此，为了使结果尽可能公平，本实验定义了拒绝模型，使得交易对象在不满足匹配结果的情况下可以选择拒绝交易。拒绝模型本身是匹配机制的一部分。为了仿真，本实验中的拒绝模型统一定义如下：

当匹配结果的满意度小于低满意度平均值（0.43）时，交易对象拒绝匹配结果。

每个实验产生 500 个不同的购电者和 500 个不同的购电者。相同数据下两种匹配机制的匹配结果数（无单位）对比如图 4.9 所示。

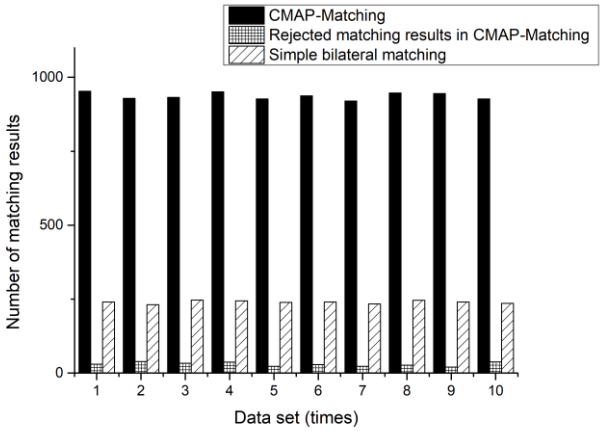


图 4.9. 匹配结果数量比较。

如图 4.9 所示，CMAP-Matching 的匹配结果数量远高于简单双边匹配。原因之一是 CMAP-Matching 允许多对多匹配。在所有购电者都能购买到所需电力的情况下，CMAP-Matching 在一次交易匹配中的平均匹配结果数为 937 个，人均匹配结果数为 1.87 个，这意味着每个购电者平均从大约 2 售电者购电。 CMAP-Matching 中被拒绝的交易占 3.00%，这进一步证明了满意度低于 Low 满意度平均值的匹配结果很少。简单双边匹配的平均匹配结果数为 239，这意味着大约 52.00%的用户没有匹配到交易对象。下面的比较都是基于这个匹配结果。

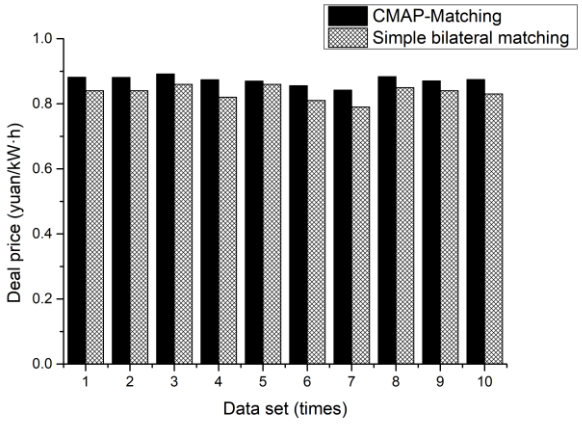


图 4.10. 成交价格比较。

交易价格对比见图 4.10。 CMAP-Matching 和简单双边匹配的成交价格基本相同。成交价之所以在 0.85 元/kW·h 左右，是因为实验中的售/购价在 0.3023-1.4167 元/kW·h 区间内随机产生。两种匹配机制的平均交易价格分别为 0.87 元/kW·h 和 0.84 元/kW·h。 CMAP-Matching 比简单的双边匹配略高，但差异很小，约为 0.03 CNY/kW·h。可能有两个原因

这种细微的价格差异：首先，在用于比较的匹配结果方面，CMAP-Matching 使用的匹配结果数量占所有匹配结果的 97.00%，满足所有购电需求。在简单的双边匹配中，48.00%的用户成功匹配了交易对象，因此匹配结果的完整性较弱。其次，CMAP-Matching 包含多种匹配属性，而不是单纯的与价格的双边匹配。

传输损耗用交易双方之间的距离来表示。如图 4.11 所示，CMAP-Matching 的传输距离远低于简单双边匹配的传输距离。经计算，两种机制的平均传输距离分别为 5.0km 和 26.4km，简单双边匹配的传输距离是 CMAP-Matching 的 5 倍以上。因此，在满足购电需求且交易价格波动不大的情况下，CMAP-Matching 的传输损耗比单纯双边匹配降低了 81.06%。

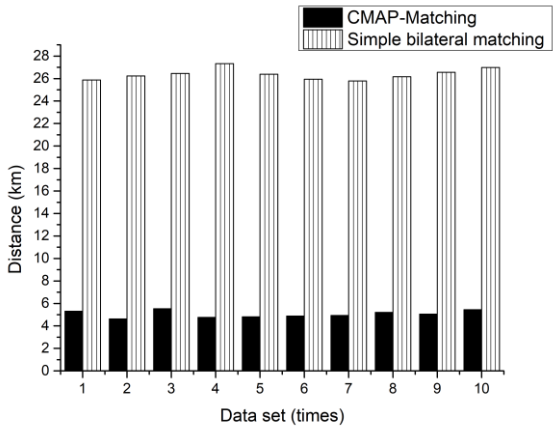


图 4.11. 传输损耗比较。

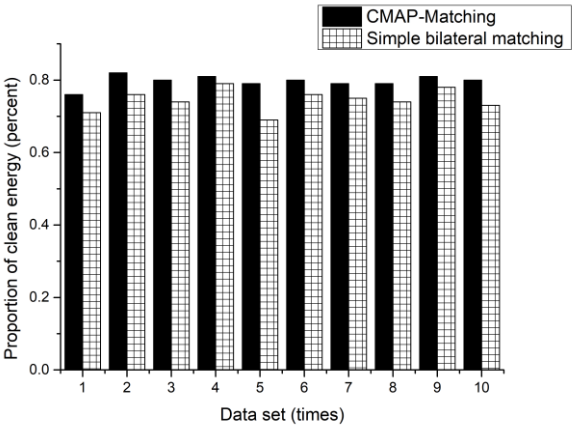


图 4.12. 清洁能源占比比较。

清洁能源占比如图 4.12 所示，CMAP-Matching 清洁能源占比略高于简单双边匹配。经计算，清洁能源平均占比分别为 79.70%和 73.90%，CMAP-Matching 高出 5.80%。这个结果可能有两个原因：一是 CMAP-Matching 使用了更完整的匹

配结果。其次，在购电者选择的 *Selling price*、*sTransmission loss*、*Environment-Protection Index* 三个匹配要求中，最后一个属性的 *Environment-Protection Index* 对结果的影响最小（因为三者的默认权重匹配要求为 0.5、0.3、0.2）。但还是可以看出，CMAP-Matching 对能量类型做了区分。

4.5 结论

本章提出了一种基于区块链的多属性偏好匹配能源交易系统，可应用于能源互联网微电网电力分布式交易市场。本系统提出了能源交易全流程在区块链上实现的交易方案，保证了能源交易的公平性和可靠性。该系统提供了一种同时包含交易双方对交易的多种匹配需求的交易撮合机制。描述了该系统在区块链上的实现，并描述了该方法在微电网能源交易中的可行性。实验结果表明，CMAP-Matching 在匹配成功电量、匹配满意度、传输损耗、清洁能源占比等方面均具有良好的表现。因此，匹配机制产生了良好的匹配结果，基于区块链的实现也适用于微电网能源交易场景。

第五章 适用于区域能源互联网区块链电力交易的共识机制研究

5.1 介绍

共识机制是区块链技术堆栈的一个核心部分，各区块链节点可通过共识机制来共同维护所记录信息的准确性与一致性。

在分布式电力交易中，共识机制是一个关键的技术难点，并且很大程度上影响着分布式电力交易相关应用的实践可行性。共识机制是区块链交易是否可信的关键，并影响着交易吞吐量、交易实体数量等实际应用中的核心性能。

随着越来越多的生产者和消费者加入能源互联网，尤其是具有大量交易节点的区域能源互联网微网结构正在成型，现有的能源区块链共识机制可能需要在共识效率、共识安全等方面具备更强的竞争力，以促进能源互联网区块链应用落地。现有的能源互联网区块链共识机制难以有效避免共识节点增加导致共识效率快速降低的问题。

针对现有电力交易区块链共识机制性能与快速成规模电力分布式链上交易需求的差距，本章提出耦合业务场景设计共识机制的研究思路，设计面向能源互联网分布式电力交易场景的分级异步共识架构，以 PBFT 结合声誉机制为例，对区域能源互联网分布式电力交易共识机制进行设计，当节点数量不断增加时，既保证去中心化场景下的共识效率，又保证共识结果的准确性。同时，共识机制的可扩展性也提供添加和退出微电网与节点的便利性，提高区域能源互联网场景下微电网的可扩展性。

本章的其余部分安排如下。第二节对能源互联网分布式电力交易的共识需求进行分析。第三节对分级异步共识架构的设计进行描述。第四节面向区域能源互联网微网分布式电力交易场景进行分级异步共识设计。实验和结果分析在第四节中进行讨论。第五节对本章在进行总结。

5.2 电力交易共识的需求分析

目前基于区块链的能源项目研究所采用的共识机制主要包括 PoW、PoS、

DPoS 和 PBFT 等几种，以及在它们基础上改进的共识机制[137]。针对能源交易的 PoW 共识算法及其改进算法，保证了各个节点记账的平等性，但是 PoW 共识过程需要耗费大量的算力，造成不必要的能耗。能源交易场景中的 PoS 和 DPoS 共识算法，在一定程度少减小了 PoW 共识的算力浪费，但由于“权益”的积累，易造成超级节点，使节点之间权利不对等，进而影响共识结果。针对能源互联网微网能源交易，部分研究选取定量的能源监管主体或数据中心节点，采用 PBFT 共识算法以及基于其改进的共识算法，然而，该类算法存在 1. 需要预先指定共识节点，不仅牺牲了系统去中心化的特性，还难以保证选举的共识节点长期可信，并且随着共识组节点数量的增多，共识效率会不断下降；2. 可扩展性差等缺陷。

随着越来越多的产消者加入电网，大量的电力交易共识需求产生，特别是面向有大量交易节点的 REI 微网，现有的能源区块链采用的共识机制除了上述挑战还普遍会有共识效率随节点增多下降过快等问题。

根据 REI 微网分布式电力交易场景特点，参与的用户容量较小，一般没有直接参与电网交易的能力，而是接入能源互联网后由微电网（综合能源站、虚拟电厂等）代理商整合辖内各个用户的能源需求和调节能力。各个微网代理再在高一层级的网络中交互进行能源供需匹配和调节。现有的技术方案无法直接映射这样的多层级分布式业务。若采用现有共识方案，那么不仅可能会造成性能的浪费（很多节点间短时间参与交易，长时间进行反复共识），也会增加达成共识的时长（很多节点为不认识、不接触的节点提供背书），降低共识效率。在耗费资源的同时对信任的生成难以起到支撑作用。这在有些传统公链中无法避免，但在节点有资产抵押，且流动性相较较低的能源联盟链中，可以通过本章提出的机制提升共识性能和效率。

面向能源互联网分布式交易的应用特点，共识机制的设计应考虑节点数目、去中心化程度、数据一致性和共识效率等因素，迫切需要一种在能源主体增多时，能相对保证共识效率的去中心化共识机制，同时需要够保证共识结果的一致性。

本章提出一种针对能源电力分布式交易场景的分级异步共识机制。其特点在于将微网与广域网、主干网的交易分离开，首先在频繁交易的微网内部进行共识，再由每个微网的代理进行全局共识，并且这个共识是以异步的形式达成的。这样不仅可以高效地满足各个微网内部的快速交易，同时在全局也可以较为快速地形

成区块记录，加快交易流程。

所提出方法也同时尝试解决全局共识与区域共识不同步的技术问题。这是用“异步”来实现的。在电力分布式交易平台解决方案的技术堆栈中使用所提出的共识机制改进现有广泛使用的共识机制，可减少共识形成时间，加速交易流程，实现快捷的能源交易。同时，本方法可以减少各节点达成共识所需处理能力，降低能量路由器硬件设备要求，促进制造区块链节点成本下降。

5.3 分级异步共识机制架构研究

基于将微网与广域网、主干网的交易分离开，但所有节点仍共同归属于同一个区块链记录与监管的设计方向，本节研究从分片网络划分，分片区域共识建立（共识节点选取、分片代理共识建立），全局分片间异步共识建立，三个部分对分布式电力场景的共识机制进行设计。

在区块链构建共识的过程中，首先对范围内所有节点进行分片，根据历史交易记录或监管节点建议将历史交易频繁的节点划入同一个分片中；随后，在各个分片内部按需建立区域共识；再通过各分片/区域的代理节点进行全局共识。区域一致性的建立与全局一致性的建立不同步，且全局一致性的建立与信息上链存证的过程不同步，故称为“异步”。

区域网络中的区块链节点会在区域网络节点中选出该区域的代理节点。此代理节点对外宣布所代表的区域网络/分片的共识结果，并与其他区域网络的代理节点进行交互，从而达成大网络的能源交易共识。

出于性能等多种因素考虑，区域共识的达成和全局共识的达成采用异步形式进行。即，代理节点首先对网络中所有节点发布其代理的节点达成的区域共识，并记录其他代理节点发布的其他区域共识记录，并在全局网络中对这些记录进行共识上链。之后，所有已上链的区域共识之间的准确性将被全局所有节点验证，并在下一次达成的全局共识中体现。上一区块中不准确的区域共识记录将被修正。提供不正确区域共识信息的节点及代理将被共识机制处罚。

本节提出的分级异步共识机制，可以降低分片间达成共识在时间尺度上的耦合度，适宜在不需要全局精确时间同步的前提下进行分布式电力交易场景的共识，

例如日前、中长期交易，可支撑可靠的新能源交易的融合应用区块链底层平台。具体实施方案如图 5.1 所示。

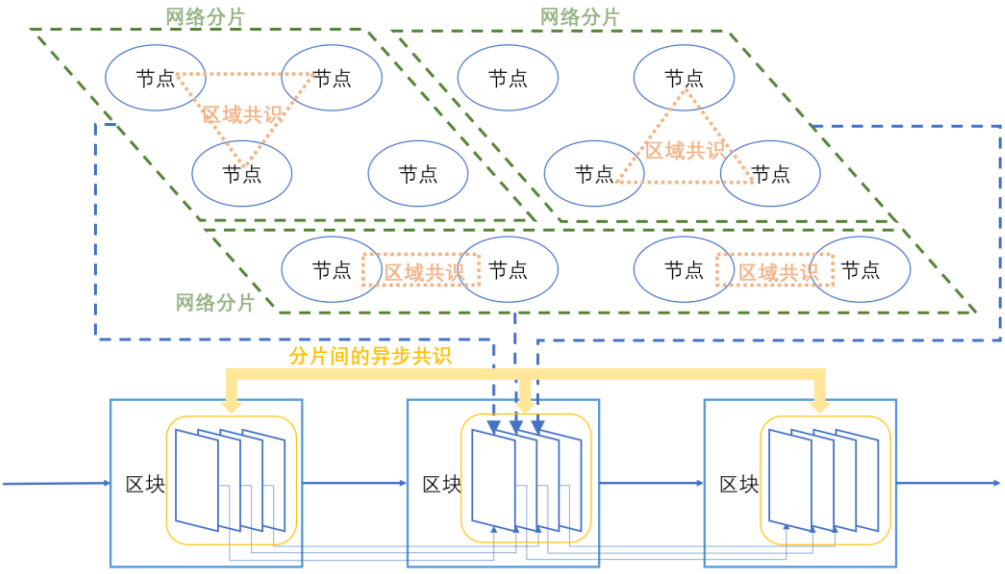


图 5.1. 分级异步共识算法设计思路。

5.3.1 网络分片划分方法

传统的中心化交易模式存在透明度低、成本高、效率低下、数据不可信等问题。而区块链技术作为一种非对称加密的分布式账本，具有去中心化、不可篡改、匿名等优点，具备满足点对点（Peer to Peer, P2P）交易模式、微网交易模式、群体用户交易模式等典型电力交易模式的潜力。点对点交易模式是直接交易模式的一种，在买方与卖方直接交易的自由市场下进行，不受第三方监管和约束；但由于 P2P 市场分散，缺乏统一的组织和章程，不易管理和监督，其交易效率有待验证。如图 5.2 所示，在微电网、虚拟电厂等场景中，终端参与的用户容量规模很小，没有直接参与电网交易的能力，而是入网后由微电网、综合能源站、虚拟电厂等总代理商整合辖内各个用户的能源需求和调节能力，代理用户与区域外的电网开展交易。在群体用户交易模式中，用户连接到区域内的虚拟电厂中心，提交分布式能源信息，并与其交易电能；该中心将区域内的用户统一组织起来，作为一个主体为电网提供调控服务，并以此获得相应的内部节能费用和参与电网调节的收益。

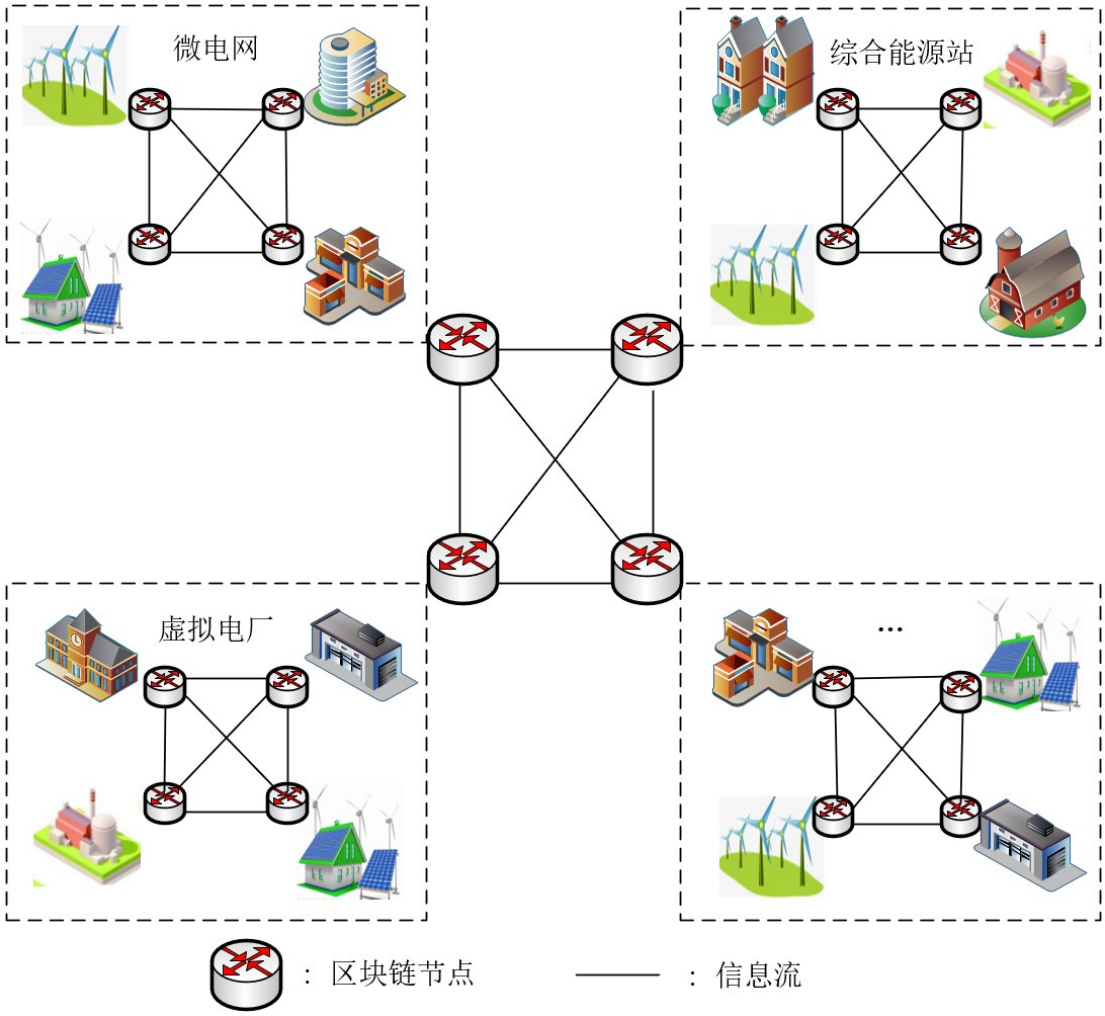


图 5.2 分布式电力交易场景。

基于本章前述需求描述及设计思路，推理可知尽量将交易频繁的节点划入同一个分片可以在很大程度上减少全局共识所需资源。解决分片问题或分片优化问题的关键在于如何随业务调整分片，将有更紧密交易关系的区块链节点放到同一个分片里，而不是对业务进行调整或对节点间交易进行调整或引导。本小节从这个角度针对 REI 分布式交易场景提出一套区块链网络建立分片、将节点划分到各个分片的方法，而后通过交易记录对分片进行优化，从而减少区块链网络整体的资源消耗，提升共识效率。原理上，本方法将区块链网络中所有节点抽象映射到笛卡尔坐标系，从而得到他们之间的欧拉距离，通过引入聚类算法，随交易持续进行分片优化。

分片方法包含以下步骤：

步骤 1. 初始化节点

当一个非监管节点（业务节点）$Node_i$，$i \in [1,N]$，N 为节点总数，加入区

块链网络中时，它必须通过一个监管节点$Node_Sup_j$申请加入区块链，监管节点间协调通过申请后，告知至少M个区域共识组节点$\mathrm{M} > (N_{consensus} - N_B)$。其中，$N_{consensus}$为全局共识节点总数，$N_B$为网络可以承受的最大的拜占庭节点数。

可选地，上述监管节点$Node_Sup_j$可以指派$Node_i$在下一个分片周期内进入某个分片S_j，$j \in [1, l]$，指派过程随所述步骤 2 开展，这种分配可以以微网的物理连接作为参考；或者可选地，通过该新加入节点形成$Node_i$的第一个交易所对应的另一个交易方$Node_k$确定该新加入节点所属分片。

步骤 2. 更新节点分片信息

当一个分片周期开始时，所有业务节点$Node_i$通过获取区块链上的分片信息获取本分片周期自己所在分片。 例如，业务节点$Node_i$被分在分片S_j中，它收到的“分片信息”是自己所属份分片的共识组的地址表$[Node_{S_m,1}, Node_{S_m,2}, \dots, Node_{S_m,k_i}]$，该共识组的$k_i$个节点在该分片周期内承担分片$S_j$内的区域共识生成工作，并与其他分片确认跨分片交易。若$Node_i$发现自己不在分片共识组地址表中，则将自己所需的交易服务提交给共识组中的节点，共识组节点将区分区块内外交易并与适当的共识节点开展共识；若业务节点$Node_i$被选为分片S_j的分片共识组，则他会收到其他所有分片的共识组信息$[Node_{S_1,1}, Node_{S_1,2}, \dots, Node_{S_1,k_1}]$，$[Node_{S_2,1}, Node_{S_2,2}, \dots, Node_{S_2,k_2}]$，……，$[Node_{S_l,1}, Node_{S_l,2}, \dots, Node_{S_l,k_l}]$，并承担相应责任，收集、整理、发送给自己所在区域的交易并与其他区域共识节点共识每个交易的真实性。

步骤 3. 统计节点相互之间的交易量

在一个分片周期内，每个分片的区域共识组节点$[Node_{S_m,1}, Node_{S_m,2}, \dots, Node_{S_m,k_i}]$统计分片内所有节点的点对点交易数量并进行记录，进行分片共识时，区域共识节点对该统计记录进行校验；区域共识节点在进行全局共识时对全局内所有节点的点对点交易数量进行统计与记录，进行全局共识时，全局共识节点对该统计进行校验。

在一个共识节点提出新区块时，还需通过步骤 4 方法提供下一个分片周期中所有节点的分片建议。分片建议在全局共识中被校验。如果统计结果及分片建议

通过全局共识，则该分片建议成为下一分片周期中的分片方法，被全局共识节点发布给所有业务节点。

步骤 4. 对下一个分片周期的分片方法提出建议

全局共识节点提出分片建议，首先将节点间的交易量映射到笛卡尔坐标系，再对不同分类数的聚类问题进行优化求解，自动化地选取哪些节点在下一个分片周期被划为一个分片，在保证分片共识安全有效进行的同时减少全局共识所消耗资源。具体方法如下：

i) 将当前收集到的所有点对点交易记录为一个矩阵$R_1 = \begin{bmatrix} 0 & \cdots & tx_{1,N} \\ \vdots & \ddots & \vdots \\ tx_{N,1} & \cdots & 0 \end{bmatrix}$。其中，$tx_{i,j}$表示在这个分片周期内，$Node_i$卖给 $Node_j$电的交易的数量。一般地，该矩阵是一个稀疏矩阵。

ii) 将矩阵 R 中第 i 行第 j 列与第 j 行第 i 列的值相加$tx_{(i,j)} = \begin{cases} \frac{1}{tx_{i,j}+tx_{j,i}}, tx_{i,j} + tx_{j,i} \neq 0 \\ 1 \quad , tx_{i,j} + tx_{j,i} = 0 \end{cases}$。将$tx_{(i,j)}$写入一个新的第 i 行第 j 列，可得$R_2 = \begin{bmatrix} 0 & \cdots & tx_{(1,N)} \\ \vdots & \ddots & \vdots \\ tx_{(1,N)} & \cdots & 0 \end{bmatrix}$。

iii) 在 N 维空间建立笛卡尔坐标系，将每一个业务节点映射到这个坐标系中的点，$Node_i$对应的点的坐标是R_2的第 i 行。

iv) 若新的聚类参数被监管节点声明，则：

a.) 取k $= [\frac{N}{\theta}]$，其中θ为分片常数。使用 K-mean 算法计算聚类数为$k \pm p\mu$时的聚类结果与聚类中心。其中，$p = (1,2,3,\cdots,\omega)$，$\mu$为步长，$\theta, \mu, \omega$由监管节点给出并广播至所有全局共识节点，并声明在哪个未来的分片周期中开始被使用。这种广播可以在任意时间进行，广播结果通过双方握手确认，更新后的参数将记录在新的区块中接受共识，并在所声称的周期中被使用。

b.) 计算每个点到所属聚类中心的距离$d_{p,S_m,Node_i}$。求和计算每个聚类结果的距离之和 $d_{p,\Sigma} = \sum_p d_{p,S_m,Node_i}$，取 $k \pm (p-1)\mu$ 使有

$\underset{p}{max}(\frac{d_{p-1,\sum}+d_{p+1,\sum}}{2}-d_{p,\sum})$的聚类结果作为下一分片周期建议的分片建议。

v) 若无新的聚类参数被监管节点声明，则：

a.) 使用 K-mean 算法计算聚类数为$l_{last}\pm p$（l_{last}为上一分片周期所采用的分片个数）时的聚类结果与聚类中心。其中，$p=(1,2,3,\cdots,\omega)$。

b.) 计算每个点到所属聚类中心的距离$d_{p,S_m,Node_i}$。求和计算每个聚类结果的距离之和$d_{p,\sum}=\sum_p d_{p,S_m,Node_i}$,取$k\pm(p-1)$使有$\underset{p}{max}(\frac{d_{p-1,\sum}+d_{p+1,\sum}}{2}-d_{p,\sum})$的聚类结果作为下一分片周期建议的分片建议。

在每一个分片周期中重复步骤 2-4，以基于交易持续优化分片。步骤 4 中的分片方法也可采用人工神经网络、支持向量机等算法获取分片方法，也可在分类后，由监管节点进行人工审查、确认。

5.3.2 分片区域共识建立

全局网络与区域网络建立后，网络中各交易方各自建立区块链节点并联网，所有节点通过网络协议握手并两两建立 P2P 通信网络。监管节点是一种特殊的全局节点，不属于电网业务节点，由监管方建立。

由监管方建立创世区块并分发给所有节点。创世区块包括但不限于下述内容：

1. 区块链网络规模，所有现有区块链网络节点地址；

2. 区块链架构、协议、各节点权限，架构、协议、权限的更新办法；

3. 智能合约引擎；

各节点根据创世区块完善自己的软件架构以适配能源电力区块链交易需求。

随后，各节点在创世区块协议规定的时刻开始构建第一个区块，并按协议规定的时间间隔开展交易。

区块链协议包括但不限于下属内容：

1. 区块记录规则及对应参数，包括但不限于：区块链加解密需求及支持的密码种类，区块链支持的全局共识与区域共识，及对应的增加、修改、删除的办法，交易开始时间，区域共识周期、全局共识周期及修改方法，区域共识组节点选出

的方法及修改方法，作恶的惩罚，等；

2. 协议升级办法、智能合约引擎升级办法；

3. 节点、区域网络及参数设立、修改、删除办法；

4. 区块链停止服务条件，停止办法。

除创世区块外，所有区块都包括但不限于下述部分：

1. 区块链网络部分：点对点通信相关的增删改查等；

2. 区块链架构部分：架构、协议、权限相关的增删改查等；

3. 智能合约部分：智能合约相关的增删改查等；

4. 处罚部分：列出作恶节点及相应的处罚；

5. 所有业务节点下一周期的分片方法；

6.交易部分：记录本周期内所有共识组节点提交的分片内交易及分片间交易；

7.异步共识部分：记录所有共识组节点对上一区块的分片间交易达成的共识；

在区块链构建共识的过程中。首先，各区域内部构建区域共识，根据各区域不同特性可采用 PoW，PoS，PBFT，Raft 等共识或基于其改进的共识机制。各区域（p）内构建区域共识的时间间隔 T_sub_p 可以不同。

全局共识会周期性地，在分片中的区块链节点中根据节点处理能力并带有随机性地选出该分片络的共识组节点，各分片的共识组对外广播所代表的分片的共识结果并参与全局共识。构建全局共识的时间间隔为 T_ttl。区域内部电力交易频繁，区域共识周期小于全局共识周期，即 $T\_sub_p<T\_ttl$。

5.3.3 全局分片间异步共识建立

在全局网络中，各个微网的共识组进行相互沟通，从而达成全局的交易共识。出于性能等多种因素考虑，区域共识的达成和全局网络共识的达成采用异步形式进行。即，大范围区块链节点网络中的各区域共识组节点，首先对网络中所有节点发布其共识组的节点在本 T_ttl 周期内达成的区域共识，并记录其他节点发布的其他微网共识记录。然后，在全局中使用全局共识机制对这些记录进行确认上链（分片）。之后，所有已上链的区域共识之间的准确性将被验证，并在下一次达成的共识中体现。上一区块中不准确的区域共识记录将被修正。

验证方法如下：

首先，所有节点会读取新区块中的所有交易，并将其中与自己世界状态相关的交易提取出来与自己的世界状态进行对比，如果没有问题则发送给自己的区域共识组节点无矛盾确认信息。如果有矛盾的地方，则将有矛盾的交易通知所有区域共识组节点，由共识组节点通知所出现问题的分片的共识组节点及监管节点。随后，由相关分片的所有共识组节点进行特别共识，确定修订的内容及相应处罚；或由监管节点通过智能合约发起核查，并将核查结果广播通知所有共识组节点。如果核查结果需要对之前区块进行修改，则修改结果会通过共识组节点间的全局共识写入新区块的异步共识部分。

如果需要进行修改，则可能会伴随着对某节点或共识组节点的处罚，处罚根据区块链协议中的相关规定裁量，处罚的结果会通过共识组节点进行全局共识后写入新区块中，并随着新区块传播到所有节点并有所有节点共同执行。

5.4 分级异步共识机制场景与具体设计

本小节选取能源互联网分布式电力交易场景，对该场景下的电力分布式交易所需分级异步共识方法进行针对性设计与仿真。为验证本节前述机制研究的可行性，针对能源互联网电力分布式交易场景进行分析，提出了一种融合 PBFT 算法与信任机制的分级异步共识方法，并进行仿真实验验证该方法的可行性。

针对前述问题，本小节面向能源互联网分布式电力交易场景提出了一种融合 PBFT 算法与信任机制的分级异步共识方法，在节点数量不断增多的情况下，既保证去中心化场景下的共识效率，又保证了共识结果的准确性，同时，共识机制的可扩展性也保证了节点与分片添加与退出的便利性。

在能源互联网建设的架构设计中，存在主干网-广域网-局域网的多层级架构，即能源互联网是以互联网理念构建的新型信息—能源融合“广域网”，它以 大电网为“主干网”，以微网、分布式能源、智能小区等为“局域网”，以开放对等的信息—能源一体化架构真正实现能源的双向按需传输和动态平衡使用。这种设计可以最大限度的适应新能源的接入。基于这个思路，本节提出的共识机制多层级架构，设计了分片内部交易共识方法和分片间交易共识方法两部分。

本节所提出的应用于区域能源互联网分片内部交易的区块链共识方法，包括如下步骤：

5.4.1 分片内部交易共识方法

当交易双方处于同一个分片当中时，使用微网外部交易共识。分片内部交易共识方法由以下步骤组成：

a. 初始化：所有区域能源互联网中的交易节点初始化各自的信誉值；

信誉值指的是依据节点参与共识的历史数据得出的诚信度，依据节点背书结果与共识结果是否相同来修改。所有节点的信誉值有相同的初始值(T_init)与上限(T_max)。正常完成一次，该节点能源交易共识背书信誉值增加固定值(T_up)；背书错误一次，信誉值降低一个固定值(T_down)。一般地，T_down >> T_up。信誉值达到上限之后不再增加。

b. 依据信誉值和随机值选取 n 个分片内部节点作为共识组节点；

分片内部会临时建立一个又多个节点组成的共识组，用于记录与分发共识。当选取共识组节点时，一个信誉值下限（T_min）被所有节点采用，即当信誉值高于该下限时，才可能被选取作为共识节点。在选举共识组节点时，为增加随机性而给信誉值达标的节点生成随机值（T_r）。随机值拥有一定的范围并在监管节点的监督下进行。将信任值与随机值相加，排名共靠前的多个未参与交易的节点（n 个），被认定为共识组。

c. 交易发起节点对交易记录进行私钥签名，并将其广播至共识组节点；

交易发起节点是电力购买节点。购买节点需提前与销售节点进行链上或链下沟通，双方同意交易后购买节点获取销售节点的签名并生成能源交易记录。购买节点作为交易发起节点将能源交易记录广播至共识组节点。具体信息至少包括：交易记录 ID，购电用户 ID，售电用户 ID，购电方私钥签名，售电方私钥签名，交易单价，交易量，交易金额。

d. 共识组节点针对收到的能源交易记录进行拜占庭共识验证；

共识验证主要包括预准备、准备、确认 3 个阶段，如图 5.3 所示。

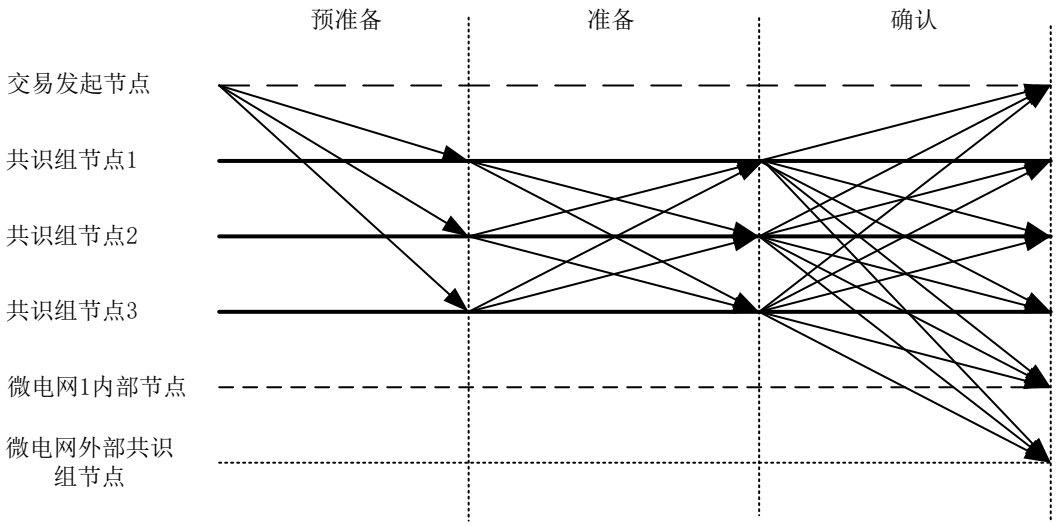


图 5.3. 分片内部交易共识验证方法。

在预准备阶段，交易发起节点将能源交易记录发送给共识组节点，共识组节点验证能源交易记录中的私钥签名以及交易金额，验证通过之后，对能源交易记录进行背书。

在准备阶段，共识组节点将背书之后的能源交易记录发送给除自身之外的共识组节点，共识组节点验证收集到的已背书的能源交易记录，若收到的已背书的记录数量大于：2m+1（$\exists m \in N, s.t. 3m+1 \geq n$）时，则生成对应能源交易记录的共识结果消息。

e. 共识节点将自己确认过的能源交易记录发送给网络中所有节点。

在确认阶段，共识组节点将共识结果消息广播至区域能源互联网中除自身之外的所有节点，所有节点依据收到的共识结果消息进行共识结果判定。每个节点收集到的共识组的结果消息的数量若大于 n/2，则判定为正确消息，并将能源交易记录存储到本地区块链中。所有节点修改本地信誉值列表中的共识组节点的信誉值。

所有节点根据预设及收到的消息结果正确与否，各自进行信誉值列表的更新。正常完成共识的共识组节点的信誉值增加 T_up。完成共识的共识组节点的信誉值降低 T_down。

5.4.2 分片间交易的共识方法

当交易双方不处于同一个微网当中时，使用微网外部交易共识。分片间交易共识方法由以下步骤组成：

a. 与分片内部交易共识组选取方法相同，有跨分片交易需求交易发起节点对交易记录进行私钥签名，并将其广播至分片内共识组节点；
b. 与分片内部交易共识组选取方法相同，共识组节点针对收到的能源交易记录进行拜占庭共识验证；
c. 与分片内部交易共识组选取方法相同，共识组节点将共识结果消息广播至区域能源互联网中除自身之外的所有节点；
d. 依据信誉值和随机值从参与交易的多个分片中选取 n 个节点，作为全局共识组节点。分片间交易的共识组节点，由参与交易的多个分片中选取信誉值与随机值之和排名前 n 名的所有节点组成，且参与交易的节点不能进入全局共识组。
e. 在一个全局共识周期内，全局共识组对上一个全局共识周期所对应的区块内所有的分片间交易进行共识，核对正确的进行记录，不正确的予以纠正，纠正结果在全局共识周期内在全局共识组间进行共识，并发送给所有节点，如图 5.4 所示。
f. 与分片内部交易共识组选取方法相同，所有节点修改本地信誉值列表中的共识组节点的信誉值。

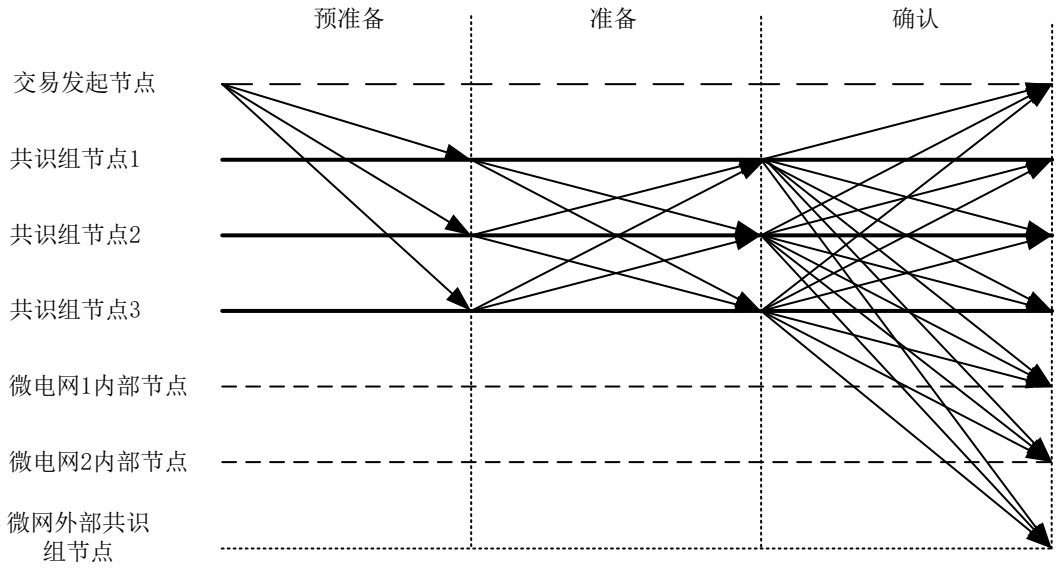


图 5.4. 分片间交易共识验证方法。

根据电力等能源的实际设计构架，一个分片内部节点与本微网内部节点交易更为频繁，与另一分片的节点交易相较之下不频繁。本节的设计在网络拓展的情

形下仍可以将共识规模控制在一定范围内，减小不必要的共识准备、通信与确认，提升共识效率。

5.5 仿真实验

共识机制实验设备为 16GB RAM、Intel(R) Core(TM) i5-1035G1 CPU 的联想小新 Air 14 2020 款笔记本一台，采用 Golang 语言多线程并发技术实现本共识机制，模拟多个客户端节点和服务器节点进行区块链交易的共识验证。客户端节点对应区块链网络中的客户终端，用于发起区块链交易；服务器节点对应共识过程中的共识节点，参与区块链交易的共识过程。需要说明的是，本研究为更好的进行性能测试，对服务器节点与客户端节点进行了分别设定。而本节提出的共识机制对服务器节点与客户端节点的重叠性并无要求。即，在实际应用中，服务器节点和客户端节点可以部署在同一个服务器中。各个实验的结果均为运行多次的平均值。

针对现阶段区域能源互联网场景共识机制，随着共识节点数量增多而导致共识效率显著下降的问题，我们对共识节点逐步增多的实验测试。本实验具体变量参数如表 5.1 所示。

表 5.1. 实验变量参数

实验序号	客户端节点个数	客户端拜占庭错误比例	服务器节点个数	服务器拜占庭错误比例	分片数量	共识组节点数量
1	20	0%	50-200 递增，每次增加 10 个	10%	10	4

本实验共设 10 个分片，每个分片对应 2 个客户端节点，服务端节点初始值为 50，即每个分片对应 5 个服务器节点，之后每次测试增加 10 个服务器节点，均匀增加在 10 个分片中，最大值为 200 个服务器节点。吞吐量计算公式如公式(5.1)所示，实验测试结果如图 5.5 所示。

$$\text{吞吐量} = \text{被正确共识的交易数}/\text{共识时间} \quad （5.1）$$

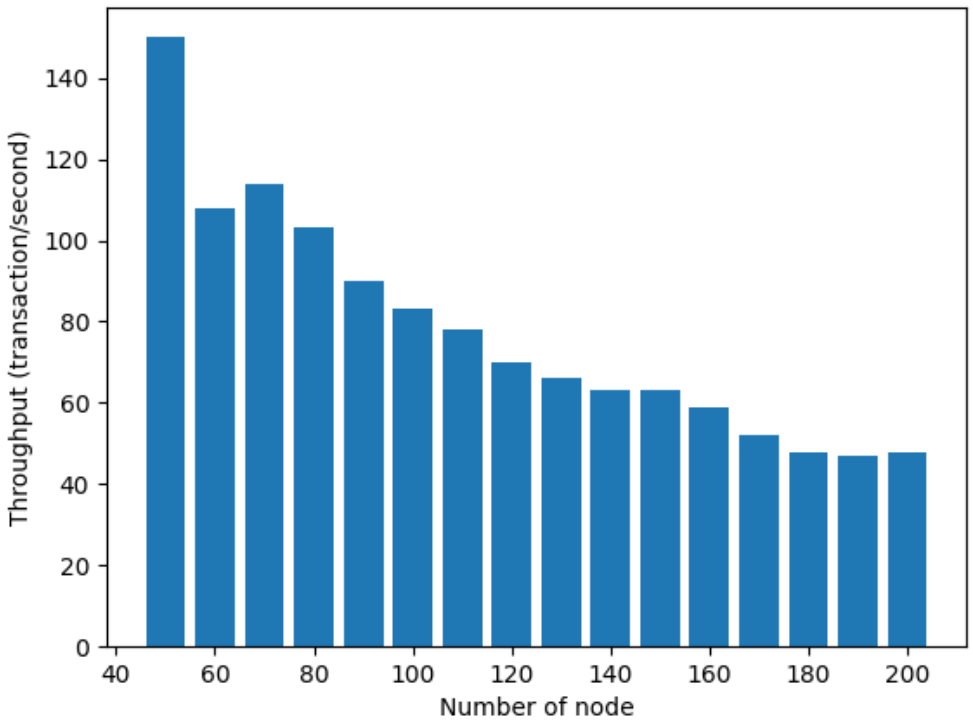


图 5.5. 区块链吞吐量与服务器节点数量之间的关系。

由图 5.5 可知，区块链共识的吞吐量一开始随着分片服务端节点的增加而降低。通过观测本共识机制在节点数量增多时的吞吐量变化，可以看出本共识机制在节点数量增多时的共识效率呈现出一种类似于线性化的降低趋势。且在网络规模增大到趋近于 180 个节点后停止了降低趋势。这种现象符合本共识机制的设计特点，即，将共识规模控制在一定的规模，以为能源互联网交易网络提供更灵活的扩展性。

为降低固定共识组节点被攻击的可能性，缓解固定共识组节点的共识压力，体现多组共识节点并发共识的共识效率，我们对多组共识节点并发共识的进行实验测试。本实验具体变量参数如表 5.2 所示。

表 5.2 实验变量参数

实验序号	客户端节点个数	客户端拜占庭错误比例	服务器节点个数	服务器拜占庭错误比例	分片数量	共识组节点数量
2	10-200 递增，每次增加 10 个	0%	100	10%	1	4

本实验设 1 个分片，客户端节点初始值为 10，所有客户端节点均属于同一个

分片，每个客户端交易选择不同的共识组节点进行共识，之后每次测试增加 10 个客户端节点，客户端节点最大值为 200，服务端节点数目保持 100 个不变。吞吐量计算公式如前述公式所示，实验测试结果如图 5.6 所示。

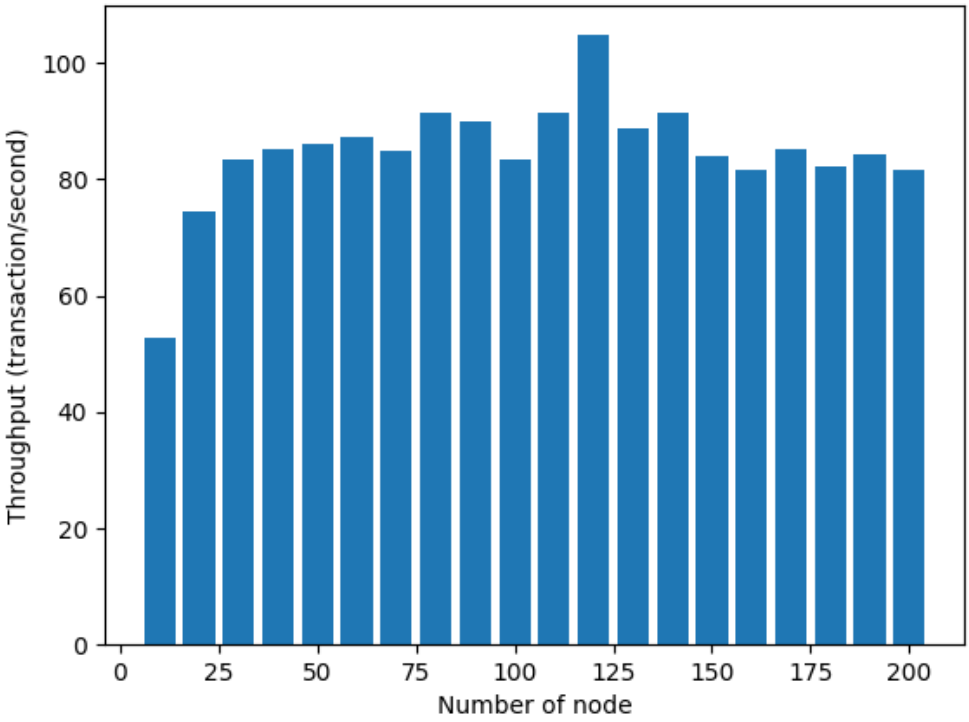


图 5.6. 区块链吞吐量与客户端节点数的关系。

由图 5.6 可知，除了在客户端节点数量较少时（客户端节点为 10,20 时）吞吐量可预料地逐渐提高，在达到 30 个客户端节点后，吞吐量位置在了一个较平均的水平上。个别实验的平均值的高低可能是由于实验次数有限导致，并不影响这个普遍稳定的现象体现出本节提出的共识机制在多组共识节点并发共识时的共识效率，相对稳定的结论。这样的共识机制对能源互联网中能源区块链交易的稳定执行具有重要意义。

针对多个分片内部交易自主共识的场景，我们对多分片扩展性进行实验测试，验证本共识机制对区域能源互联网场景下分片扩展性的提高。本实验具体变量参数如表 5.3 所示。

表 5.3 实验变量参数

实验序号	客户端节点个数	客户端拜占庭错误比例	服务器节点个数	服务器拜占庭错误比例	分片数量	共识组节点数量

3	20	0%	10 个/每个分片	10%	1-10 递增	4

本实验分片数量从 1 至 10 递增，每个分片包含 10 个服务器节点，服务器节点数量初始值为 10，每次测试增加 10 个服务器节点，属于同一个分片，表示扩展了一个新的分片，客户端节点数目保持 20 个不变。吞吐量计算公式如前述公式所示，实验测试结果如图 5.7 所示。

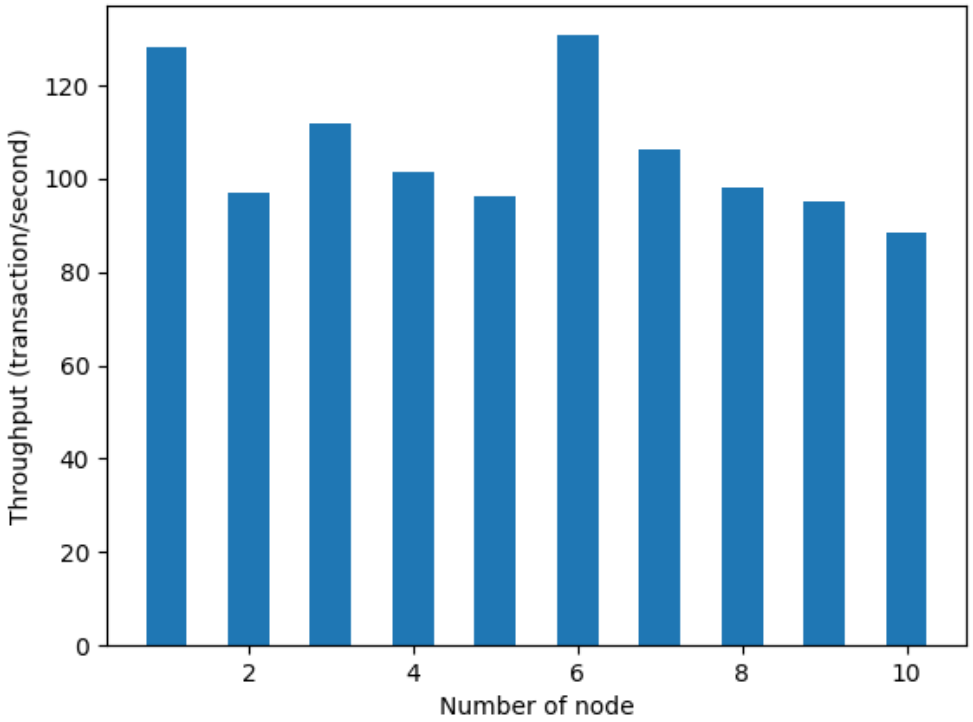


图 5.7. 区块链吞吐量与分片数量的关系。

本实验通过观测在分片扩展过程中的吞吐量变化，来验证分片扩展对本共识机制性能的影响。由图所示，虽然在多个分片内部交易自主共识的场景下，由于不同数量的微网的网络吞吐量出现波动，但基本上呈现出一种稳定状态。可以认为分片数目的增加对本节提出的多个分片内部交易自主共识的效率影响处于可控范围。

上述 3 个实验中的吞吐量实验中均出现了一定的不稳定性。该现象的来源可能源自于试验规模与实验次数的限制。在样本数量不足时很可能出现一定的不确定性。同时，上述实验的中吞吐量的波动也可能来源于一种或多种并未被展现出的原因，影响了实验结果。根据本工作建设的实验平台与开展的周期，探索这些原因将被考虑作为未来工作的一部分。

在能源区块链节点数量一定的情况下，为了得到更适合本共识机制的微电网数量划分，我们对不同划分下的客户端时延进行实验测试。客户端延迟测量标准设置为客户端向客户提交交易请求时终端收到交易请求确认所花费的时间。

在本实验中，分片的数量设置为 1~10 个，共识组节点数量保持不变，为 100 个，即不同的分片划分 100 个服务器节点。每个分片的节点数初始值为 10。每次测试增加 10 个客户端节点。服务器拜占庭错误率为 10%。共识组节点数设为 4，实验测试结果如图 5.8 所示。

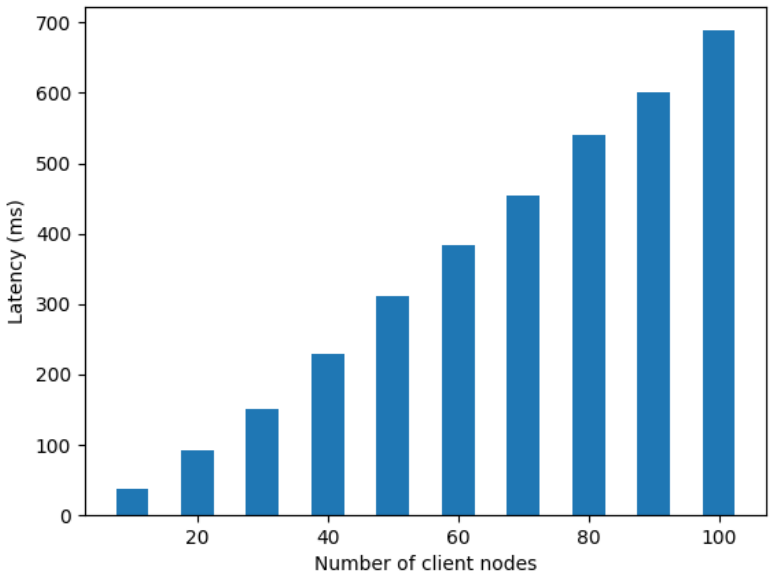


图 5.8. 客户端延迟与客户端数量的关系。

从图 5.8 可以看出，当服务器节点数不变时，共识的平均延迟随着微电网数量（客户端数量）的增加而增加。这符合所提出的共识机制的特点，延迟随着交易数量的增加而增长。此外，其增长不是类似 PBFT 共识机制的指数型增长，而是类似线性式的。这可能意味着，与采用延迟呈指数增长的共识机制的区块链相比，采用本节设计的共识机制的能源区块链可以具有更高的可扩展性。

5.6 结论

针对现有电力交易区块链共识机制性能与快速成规模电力分布式链上交易需求的差距，本章提出耦合业务场景设计共识机制的研究思路；提出了面向能源互联网分布式电力交易场景的分级异步共识架构，并以 PBFT 结合声誉机制为例，

对区域能源互联网分布式电力交易共识机制进行设计，提高区域能源互联网场景下微电网的可扩展性。实验结果证实了所提出机制的有效性。

第六章 总结与展望

6.1 总结

本研究报告主要在分析讨论能源互联网中区块链的应用现状的基础上，以分布式电力交易场景为例，进行了区块链在能源互联网分布式电力交易中的应用研究。研究从现有电力系统出发，逐步探索实现分布式电力交易所需的区块链技术并开展针对性研究。

第二章提出并构建基于区块链的能源互联网分布式电力交易系统的架构及链上异步结算存证方案；采用链下签约，链上自动化记录交易与结算的形式，适配现有中心化交易基础设施，实现在中心化交易所监管下的分布式交易。

在第三章中，分布式的交易撮合机制提出，综合计算和比较电价、交易量、传输距离、能源类型等影响电力匹配的因素，基于智能合约设计自动匹配、签名确认等功能为售、购双方提供自动化撮合与可控匹配；中心化交易所的角色消失，去中心/多中心的电力交易区块链基础设施与监管节点取而代之，适用更为分布式的能源互联网电力交易场景；系统架构设计较第二章更为独立并简化模块间的信息沟通，减弱区块链共识周期对于撮合与结算的影响；基于零知识证明和同态加密方法设计电力交易的隐私保护方法和算法实现。

第四章中提出了一种更为灵活的交易撮合机制，支持买卖需求的拆分匹配并支持灵活自选的多属性能源交易匹配偏好设置；提出并设计分布式电力交易的全流程链上交易方案，更好地满足未来能源互联网分布式电力交易需求。

针对第五章面向现有电力交易区块链对共识机制的需求，提出耦合业务场景设计共识机制的研究思路，提出面向未来能源互联网分布式电力交易场景的分级异步共识架构并针对设定场景进行具体共识机制的设计与验证。

6.2 展望

随着新一轮科技革命和产业变革的深入发展，能源产业转型加速，能源互联网加速成型。区块链作为一种重要的数字信息化工具将为能源互联网的发展提供信任支撑。

现阶段，区块链在能源互联网中应用的机遇与挑战并存。区块链作为一种由点对点网络、密码、共识、智能合约等多种计算机技术的新型技术组合，其多项

关键核心技术正处在完善突破阶段。包括共识算法、智能合约执行引擎、硬件加速等维度的区块链核心性能，以及安全、可扩展性、隐私保护、可监管性等方向的技术正在攻坚。

能源互联网中适用于区块链的应用场景正在普及和完善。分布式发电、储能技术的推广与智能电表、开关的广泛使用为分布式、自动化的电力交易提供了现实场景。

人工智能、大数据、云计算、物联网等数字信息化技术的发展普及为能源互联网区块链的应用提供了更多可能性。但目前看能源互联网区块链的业务设计及组织形态趋于一般化，更多针对性设计及研究有待发展。

当前能源互联网区块链应用案例仍处于起步探索阶段，应用案例以中小规模，试点示范，备份应用、轻应用为主，应用示范效应有待显现。且区块链应用初期投入成本较大，产业链、客户与公众对其仍需要一段适应期。但随着能源互联网的蓬勃发展，生产力的进步推动产业变革，相信在不久的将来区块链将成为能源互联网的重要技术基础，为其提供信任支撑。

参考文献

[1] 杰里米.里夫金．第三次工业革命[M]．新华社，2013．

[2] 关于推进“互联网+”智慧能源发展的指导意见[C].//中国农业机械工业协会风力机械分会,2016:7.

[3] 原凯，李敬如，宋毅，等.区域能源互联网综合评价技术综述与展望[J].电力系统自动化,2019,43(14):41-52+64.

[4] 周孝信, 曾嵘, 高峰, 等. 能源互联网的发展现状与展望[J].中国科学:信息科学,2017,47(02):149-170.

[5] 中华人民共和国国务院新闻办公室.《新时代的中国能源发展》白皮书（全文）[R/OL]. (2020-12-21)[2020-12-22]. http: //www.scio. gov.cn /zfbps/32832 /Document/1695117 /1695117.htm.

[6] 新华网. 部分地区电力供应紧张多部门紧急保供[R/OL]. (2020-12-21)[2020-12-22]. http://www.xinhuanet.com/energy/2020-12/21/c_1126885539.htm.

[7] AI Songpu, RONG Chunming, CAO Junwei. Energy Internet [M] .Cham: Springer, 2020: 297-320.

[8] 蔡文军, 朱艳. 应用于能源系统的区块链技术研究进展[J]. 智能电网, 2018, 008(003):P.205-212.

[9] 国网区块链科技公司. 第一届能源区块链生态大会在京召开——发布国家电网区块链十大应用场景构建区块链数字新生态[R/OL]. (2019-12-19) [2020-12-22]. http://www.sgec.sgcc.com.cn/html/sgec/col2019111312/2019-12/20/20191220151634 802982063_1.html.

[10] Andoni M, Robu V, Flynn D, et al. Blockchain technology in the energy sector: A systematic review of challenges and opportunities[J]. Renewable and Sustainable Energy Reviews, 2019, 100: 143-174.

[11] 张宁, 王毅, 康重庆, 等.能源互联网中的区块链技术:研究框架与典型应用初探[J].中国电机工程学报,2016,36(15):4011-4023.

[12] 杨德昌， 赵肖余， 徐梓潇, 等. 区块链在能源互联网中应用现状分析和前景展望[J]. 中国电机工程学报， 2017, 37(13):3664-3671.

[13] 周洪益， 钱苇航， 柏晶晶, 等. 能源区块链的典型应用场景分析及项目实践[J]. 电力建设， 2020, 41(02):11-20.

[14] 曹军威, 杨明博, 张德华, 等. 能源互联网——信息与能源的基础设施一体化[J]. 南方电网技术, 2014,8(04):1-10.

[15] 曹军威, 孟坤, 王继业, 等. 能源互联网与能源路由器[J]. 中国科学:信息科学, 2014.

[16] 曹军威, 袁仲达, 明阳阳, 等. 能源互联网大数据分析技术综述[J]. 南方电网技术, 2015,9(11):1-12.

[17] 马丽, 刘念, 张建华, 等. 基于主从博弈策略的社区能源互联网分布式能量管理[J]. 电网技术, 2016,40(12):3655-3662.

[18] 肖泽青, 华昊辰, 曹军威. 人工智能在能源互联网中的应用综述[J]. 电力建设, 2019,40(05):63-70.

[19] Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. Technical report (2008).

[20] 袁勇, 王飞跃. 区块链技术发展现状与展望[J]. 自动化学报, 2016,42(04):481-494.

[21] Nascimento S., Pólvora A., and Lourenço J. #Blockchain4EU: Blockchain for industrial transformations[R]. Ispra, Italy: Europe Commission, Joint Research Centre, 2018.

[22] E. Mengelkamp, J. Gärttnera, et al., Designing Microgrid Energy Markets: A Case Study: The Brooklyn Microgrid[J]. Applied Energy, , 2018, 210:870-880.

[23] 王蓓蓓, 李雅超, 赵盛楠, 等. 基于区块链的分布式能源交易关键技术[J]. 电力系统自动化, 2019, 043(014):53-64.

[24] Luo F, Dong Z Y, Liang G, et al. A Distributed Electricity Trading System in Active Distribution Networks Based on Multi-Agent Coalition and Blockchain[J]. IEEE Transactions on Power Systems, 2019, 34(5): 4097-4108.

[25] 龙洋洋, 陈玉玲, 辛阳, 等.基于联盟区块链的安全能源交易方案[J].计算机应用,2020,40(06):1668-1673.

[26] 郭鹤旋, 鲁斌. 基于交叉区块链的能源互联网信息物理安全防御框架[J]. 电脑知识与技术, 2018,14(23):7-9.

[27] 唐学用, 李庆生, 和远舰, 等. 基于区块链技术的电力交易系统安全建模及性能分析[J]. 南方电网技术, 2019,13(05):77-83.

[28] 平健, 陈思捷, 严正. 适用于电力系统凸优化场景的能源区块链底层技术[J]. 中国电机工程学报, 2020,40(01):108-116,378.

[29] 祁兵, 夏琰, 李彬, 等. 基于区块链激励机制的光伏交易机制设计[J]. 电力系统自动化, 2019,43(09):132-139,153.

[30] 佘维, 顾志豪, 杨晓宇, 等. 异构能源区块链的多能互补安全交易模型[J]. 电网技术, 2019,43(09):3193-3201.

[31] 佘维, 杨晓宇, 胡跃, 等. 基于联盟区块链的分布式能源交易认证模型[J]. 中国科学技术大学学报, 2018,48(04):307-313.

[32] 龚钢军, 王慧娟, 杨晟, 等. 区块链技术下的综合能源服务[J]. 中国电机工程学报, 2020,40(05):1397-1409.

[33] 朱兴雄, 陈绍真, 何清素. 基于区块链的微电网系统[J]. 电子技术与软件工程, 2018, 000(001):P.157-159.

[34] 欧阳旭, 朱向前, 叶伦, 等. 区块链技术在大用户直购电中的应用初探[J]. 中国电机工程学报, 2017,37(13):3737-3745.

[35] 吕凛杰, 李刚, 呼静雅, 等. 能源区块链中用户侧点对点交易支撑环境研究[J]. 电力建设, 2019,40(05):38-47.

[36] 李彬, 覃秋悦, 祁兵, 等. 基于区块链的分布式能源交易方案设计综述[J]. 电网技术, 2019,43(03):961-972.

[37] 崔金栋, 王胜文, 辛业春. 区块联盟链视角下智能电网数据管理技术框架研究[J]. 中国电机工程学报, 2020,40(03):836-848.

[38] 王莉鑫. 基于区块链共识机制的能源互联网协同优化研究[D].华北电力大学,2019.

[39] 黄虹, 文康珍, 刘璇, 等. 泛在电力物联网背景下基于联盟区块链的电力交易方法[J]. 电力系统保护与控制, 2020,48(03):22-28.

[40] 周国亮, 吕凛杰, 李刚. 基于区块链共识机制的能源互联网交易[C]. //数字中国 能源互联——2018 电力行业信息化年会论文集.中国电机工程学会电力信息化专业委员会:人民邮电出版社电信科学编辑部, 2018:236-239.

[41] 张维忠, 徐步尘, 高飞. 对用电信息保护的拜占庭容错联盟链共识算法[J]. 电气时代, 2020(01):75-78.

[42] Chen S, Liu C. From demand response to transactive energy: state of the art[J]. Modern power systems, 2017, 5(1): 10-19.

[43] 魏彬, 刘晓锋, 苟航. 基于公有链的分布式链上能源交易模式探究[J]. 长春师范大学学报, 2020,39(02):41-47.

[44] 马天男, 彭丽霖, 杜英, 等. 区块链技术下局域多微电网市场竞争博弈模型及求解算法[J]. 电力自动化设备, 2018,38(05):191-203.

[45] 郜雪, 孙宏斌, 郭庆来. 能源互联网中基于区块链的电力交易和阻塞管理方法[J]. 电网技术, 2016,40(12):3630-3638.

[46] 李刚, 孟欢, 周国亮, 等. 基于区块链技术的微网能量管理探析与方案设计[J]. 电力建设, 2018,39(02):43-49.

[47] Pee S J , Kang E S , Song J G , et al. Blockchain based smart energy trading platform using smart contract[C]// 2019 International Conference on Artificial Intelligence in Information and Communication (ICAIIC). 2019. 322-325.

[48] 韩冬, 张程, 正浩, 等. 基于智能合约的分布式能源交易体系架构研究[C]// 中国电机工程学会电力市场专业委员会 2018 年学术年会暨全国电力交易机构联盟论坛论文集. 2018:238-243.

[49] 平健, 陈思捷, 张宁, 等. 基于智能合约的配电网去中心化交易机制[J]. 中国电机工程学报, 2017,37(13):3682-3690.

[50] 韩冬, 张程, 正浩, 等. 基于区块链技术的智能配售电交易平台架构设计[J]. 电力系统自动化, 2019,43(07):89-96.

[51] 杨选忠, 张浙波, 赵申轶,等. 基于区块链的含安全约束分布式电力交易方法[J]. 中国电力, 2019,52(10):31-39.

[52] 周步祥, 杨明通, 史述青,等. 基于区块链的微电网市场势博弈模型[J]. 电力系统自动化, 2020,44(07):15-22.

[53] 王德文, 柳智权. 基于智能合约的区域能源交易模型与实验测试[J]. 电网技术, 2019,43(06):2010-2019.

[54] Wang J, Wang Q, Zhou N, et al. A Novel Electricity Transaction Mode of Microgrids Based on Blockchain and Continuous Double Auction[J]. Energies, 2017, 10(12):1971.

[55] 杨晓宇. 基于区块链的分布式能源调度与多元用户交易方法研究[D].郑州大学,2019.

[56] Saxena S, Farag H, Brookson A, et al. Design and Field Implementation of Blockchain Based Renewable Energy Trading in Residential Communities[J]. 2019.

[57] Zhao S, Wang B, Li Y, et al. Integrated Energy Transaction Mechanisms Based on Blockchain Technology[J]. Energies, 2018, 11(9): 2412.

[58] S. Ai，D. Hu, J. Guo, et al. Distributed multi-factorelectricity transaction match mechanism based on blockchain[C]. //2020 IEEE International Conference on Energy Internet (ICEI) , 2020: 121-127.

[59] S. Ai，D. Hu, J. Guo, et al. A Blockchain based Distributed Controllable Electricity Transaction Matching System[C]. //2020 IEEE International Conference on Energy Internet (ICEI), 2020: 56-62.

[60] S. Ai，D. Hu，T. Zhang，et al. Blockchain based power transaction asynchronous settlement system[C]. //2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring). Antwerp: Belgium. IEEE, 2020: 1-6.

[61] 陈爱林, 田伟, 耿建, 等. 跨国电力交易的区块链存证技术[J]. 全球能源互联网, 2020,3(01):79-85.

[62] E. Androulaki, A. Barger, V. Bortnikov, et al., Hyperledger Fabric: a distributed operating system for permissioned blockchains[C]. //Proceedings of the Thirteenth EuroSys Conference. Porto Portugal.NewYork, NY, USA: ACM, 2018.

[63] Li X, Jiang P, Chen T, et al. A Survey on the Security of Blockchain Systems[J]. Future Generation Computer Systems, 2020, 107: 841-853.

[64] 丁伟, 王国成, 许爱东, 等. 能源区块链的关键技术及信息安全问题研究[J]. 中国电机工程学报, 2018,38(04):1026-1034, 1279.

[65] 田秀霞, 陈希, 田福粮. 基于区块链的社区分布式电能安全交易平台方案[J]. 信息网络安全, 2019(01):51-58.

[66] Ullah I, Sultana T, Javaid N. Data Sharing System Integrating Access Control Mechanism using Blockchain-Based Smart Contracts for IoT Devices[J]. Applied Sciences, 2020, 10(2):488.

[67] 韩璇, 袁勇, 王飞跃. 区块链安全问题:研究现状与展望[J]. 自动化学报, 2019,45(01):206-225.

[68] 祝烈煌, 高峰, 沈蒙, 等. 区块链隐私保护研究综述[J]. 计算机研究与发展, 2017,54(10):2170-2186.

[69] Gai K, Wu Y, Zhu L, et al. Privacy-Preserving Energy Trading Using Consortium Blockchain in Smart Grid[J]. IEEE Transactions on Industrial Informatics, 2019:3548-3558.

[70] Ayoade G, Karande V, Khan L, et al. Decentralized IoT Data Management Using BlockChain and Trusted Execution Environment[C] //2018 IEEE International Conference on Information Reuseand Integration (IRI). Salt Lake City: USA. IEEE, 2018: 15-22 2018:15-22.

[71] Luo Y, Fan J, Deng C, et al. Accountable Data Sharing Scheme Based on Blockchain and SGX[C]// 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC). Guilin, China: IEEE, 2019: 9-16.

[72] Raman R K, Vaculin R, Hind M, et al. Trusted multi-party computation and verifiable simulations: A scalable blockchain approach [EB/OL]. 2018.

[73] 朱岩, 宋晓旭, 薛显斌, 等. 基于安全多方计算的区块链智能合约执行系统[J]. 密码学报, 2019,6(02):246-257.

[74] Zhou L, Wang L, Sun Y, et al. BeeKeeper: A Blockchain-Based IoT System With Secure Storage and Homomorphic Computation[J]. IEEE Access, 2018: 43472-43488.

[75] 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, 2016:840-852.

[76] Zhang Y, Wu S, Jin B, et al. A blockchain-based process provenance for cloud forensics[C]// 2017 3rd IEEE International Conference on Computer and Communications (ICCC). IEEE, 2017: 2470-2473.

[77] Noether S. Ring SIgnature Confidential Transactions for Monero[J]. IACR Cryptol. ePrint Arch., 2015, 2015: 1098.

[78] Yunsen W, Alexander K. Designing confidentiality-preserving Blockchain-based transaction processing systems[J]. International Journal of Accounting Information Systems, 2018, 30:1-18.

[79] 章建聪, 邱云翔, 金泓键. 超级账本 Fabric 平台 SDK 国密改造方案研究[J]. 网络安全技术与应用, 2020(03):37-39.

[80] 邓建球, 方轶, 丛林虎, 等. 基于改进国密算法与区块链的数据登记系统[J].兵器装备工程学报,2020,41(01):122-125, 129.

[81] 陈纯. 联盟区块链关键技术与区块链的监管挑战[J]. 电力设备管理, 2019(11):20-21, 28.

[82] 薄林, 颜中原, 李翼铭, 等. 数据挖掘和区块链技术的电力营销信息平台[J]. 信息技术, 2020,44(06):60-65.

[83] 方俊杰, 雷凯. 面向边缘人工智能计算的区块链技术综述[J]. 应用科学学报, 2020,38(01):1-21.

[84] Mylrea M. AI enabled blockchain smart contracts: Cyber resilient energy infrastructure and IoT[C]//2018 AAAI Spring Symposium Series. 2018.

[85] 郭慧, 汪飞, 张笠君, 等. 基于撮合交易的能源互联网最小网损路由算法[J]. 电力系统自动化, 2018,42(14):172-179.

[86] Rathore S, Pan Y, Park J H. BlockDeepNet: A Blockchain-Based Secure Deep Learning for IoT Network[J]. Sustainability, 2019, 11(14): 3974.

[87] 曹怀虎, 张艳梅, 王坚, 等. DAG 区块链中基于确定性退火技术的融合分割遗传任务调度算法[J]. 中国科学:信息科学, 2020,50(02):261-274.

[88] 孙凯俐, 李晖, 陈梅. 面向区块链节点负载预测的 ARIMA 组合预测方法[J]. 电子技术与软件工程, 2019(08):180-182.

[89] 邵炜晖, 许维胜, 徐志宇, 等. 基于区块链的虚拟电厂模型研究[J]. 计算机科学, 2018,45(02):25-31.

[90] 陈绍真, 王俊生, 伍燕. 基于古诺模型的能源互联网电能产品定价与交易模型研究[C]. 中国电机工程学会电力信息化专业委员会.数字中国 能源互联——2018 电力行业信息化年会论文集.中国电机工程学会电力信息化专业委员会:人民邮电出版社电信科学编辑部, 2018:206-213.

[91] 王毅, 陈启鑫, 张宁, 等. 5G 通信与泛在电力物联网的融合:应用分析与研究展望[J]. 电网技术, 2019,43(05):1575-1585.

[92] 夏旭, 朱雪田, 梅承力,等. 5G 切片在电力物联网中的研究和实践[J]. 移动通信, 2019,43(01):63-69.

[93] Zheng Q, Li Y, Chen P, et al. An innovative IPFS-based storage model for blockchain[C]//2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI). IEEE, 2018: 704-708.

[94] Kumar R, Tripathi R. Implementation of Distributed File Storage and Access Framework using IPFS and Blockchain[C]. // 2019 Fifth International Conference on Image Information Processing (ICIIP). IEEE, 2019: 246-251.

[95] A. Pouttu, J. Haapola, et al., P2P Model for Distributed Energy Trading, Grid Control and ICT for Local Smart Grids [C]. // 2017 IEEE European Conference on Networks and Communications (EuCNC), Oulu, 2017,1-5.

[96] H.R. Mubashir Husain, R. Martin, et al., Guest Editorial Special Section on Smart Grid and Renewable Energy Resources: Information and Communication Technologies with Industry Perspective[J]. IEEE Transactions on Industrial Informatics. 2017. 13(6): 3119-3123.

[97] A. Goranovic, M. Marcus, et al., Blockchain Applications in Microgrids: an Overview of Current Projects and Concepts [C]. // IECON 2017-43rd Annual Conference of the IEEE Industrial Electronics Society, Beijing, 2017, 6153-6158.

[98] Q. Chen, D. Liu, et al., Business Models and Market Mechanisms of Energy Internet (1) [J]. Power System Technology. 2015. 39(11): 3050-3056.

[99] K. Yu, M. Arifuzzaman, et al., A Key Management Scheme for Secure Communications of Information Centric Advanced Metering Infrastructure in Smart Grid[J]. IEEE Transactions on Instrumentation and Measurement, 2015, 64(8): 2072-2085.

[100] Z. Wu, Y. Liang, et al., Secure Data Storage and Sharing System Based on Consortium Blockchain in Smart Grid[J]. Journal of Computer Applications, 2017, 37(10): 2742-2747.

[101] Y. Yuan, and F. Wang. Blockchain: the State of the Art and Future Trends[J]. Acta Automatica Sinica, 2016, 42(4): 481-494.

[102] K.Ioannis, G.Raimondo, et al., Blockchain in Energy Communities A proof of concept[J]. Joint Research Centre (JRC), the European Commission's science and knowledge service, 2017.

[103] 王继业,高灵超,董爱强,郭少勇,陈晖,魏欣.基于区块链的数据安全共享网络体系研究[J].计算机研究与发展,2017,54(04):742-749.

[104] 蔡金棋,李淑贤,樊冰,等.能源互联网中基于区块链的能源交易[J].电力建设,2017,38(9):24-31.

[105] A. Hahn A, R. Singh, et al., Smart Contract-Based Campus Demonstration of Decentralized Transactive Energy Auctions[C]. //2017 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, 2017,1-5.

[106] Mihaylov, Mihail, et al., SCANERGY: A Scalable and Modular System for Energy Trading Between Prosumers[C]. //2015 International Conference on Autonomous Agents and Multiagent Systems, Istanbul, 2015,1917-1918.

[107] Hyperledger Fabric. (2020). Hyperledger Fabric [online]. Available: https://github.com/hyperledger/fabric

[108] A. Q. Huang, M. L. Crow, G. T. Heydt, et al., The Future Renewable Electric Energy Delivery and Management (FREEDM) System: The Energy Internet[C]. \\ Proceedings of the IEEE, 2011, 99(1):133-148.

[109] J. Cao, The essence and implementation path of energy internet[J]. High Technology and Industrialization, 2015, 000(012):48-51.

[110] M. A. Hannan et al., A Review of Internet of Energy Based Building Energy Management Systems: Issues and Recommendations[C]. \\ IEEE Access, 2018, 6:38997-39014.

[111] J. Wang, K. Meng, J. Cao, et al., A review of energy internet information technology research[J]. Computer Research and Development, 2015(05):117-134.

[112] X, Zhou, R. Zeng, F. Gao, et al., Current Status and Prospect of Energy Internet Development[J]. Scientia Sinica Informationis, 2017, 47(02): 149-170.

[113] J. Guo, J. Cao, Y. Yang, et al., Research Framework and Application Analysis of Regional Energy Internet Value Forms Facing User Demand[J]. Power System Technology, 2020,44(02):493-504.

[114] Chen and C. Liu, From demand response to transactive energy: state of the art[C]. \\ Journal of Modern Power Systems and Clean Energy. 2017, 5(1):10-19.

[115] T. W. Haring, J. L. Mathieu and G. Andersson, Comparing Centralized and Decentralized Contract Design Enabling Direct Load Control for Reserves[C]. \\ IEEE Transactions on Power Systems, 2016, 31(3):2044-2054.

[116] B. Kim, S. Ren, M. van der Schaar and J. Lee, Bidirectional Energy Trading and Residential Load Scheduling with Electric Vehicles in the Smart Grid[C]. \\ IEEE Journal on Selected Areas in Communications, 2013, 31(7):1219-1234.

[117] M. Vasirani, S. Ossowski, Smart consumer load balancing: state of the art and an empirical evaluation in the Spanish electricity market[J]. Artificial Intelligence Review, 2013, 39(1): 81-95.

[118] Z. Wu, Y. Liang, J. Kang, et al., Secure data storage and sharing system based on consortium blockchain in smart grid[J]. Journal of Computer Applications 2017, 37.10: 2742-2747.

[119] Y. Yuan, and F. Wang, Blockchain: the state of the art and future trends[J]. Acta Automatica Sinica 2016, 42.4: 481-494.

[120] P. Claudia, C. Tudor, A. Marcel, et al., Blockchain Based Decentralized Management of Demand Response Programs in Smart Energy Grids[J], Sensors, 2018, 18(2):162.

[121] X. Han, Y. Yuan, F. Wang, Security problems on blockchain: the state of the art and future trends[J]. Zidonghua Xuebao/acta Automatica Sinica. 2019, 45.1:206-225.

[122] E. Mengelkamp, B. Notheisen, C. Beer, et al., A blockchain-based smart grid: towards sustainable local energy markets[J]. Computer Science - Research and Development, 2018, 33(1): 207-214.

[123] T. Lv, and Ai. Qian, "Interactive energy management of networked microgrids-based active distribution system considering large-scale integration of renewable energy resources[J]. Applied Energy. 2016, 163: 408-422.

[124] N. Wang, W. Xu, Z. Xu, and W. Shao. Peer-to-Peer Energy Trading among Microgrids with Multidimensional Willingness[J]. Energies. 2018, 11: 3312.

[125] C. Zhang, J. Wu, Y. Zhou, M. Cheng, and C. Long. Peer-to-Peer energy trading in a Microgrid[J]. Applied Energy. 2018. 220: 1-12.

[126] J. Wang, Q. Wang and N. Zhou, A Decentralized Electricity Transaction Mode of Microgrid Based on Blockchain and Continuous Double Auction[C]. \\2018 IEEE Power & Energy Society General Meeting (PESGM), Portland, OR, 2018, 1-5.

[127] A. Paudel, K. Chaudhari, C. Long, and H.B. Gooi, Peer-to-Peer energy trading in a prosumer-based community microgrid: A game-theoretic model[J]. IEEE Transactions on Industrial Electronic 2019, 66(8): 6087–6097.

[128] T. Morstyn, A. Teytelboym, and M.D. McCulloch, "Bilateral contract networks for peer-to-peer energy trading[J]. IEEE Transactions on Smart Grid, 2019, 10(2): 2026–2035.

[129] C. Zhao, J. He, P. Cheng, and J. Chen, "Consensus-based energy management in smart grid with transmission losses and directed communication[J]. IEEE Transactions on Smart Grid. 2017,8(5): 2049–2061.

[130] M. Khorasany, Y. Mishra and G. Ledwich, "A Decentralized Bilateral Energy Trading System for Peer-to-Peer Electricity Markets[J]. IEEE Transactions on Industrial Electronics. 2020, 67(6): 4646-4657.

[131] China Aviation Planning and Design Institute. Industrial and Civil Distribution Design Manual (Fourth Edition) [M]. China Electric Power Press, 2017,01:22.

[132] B. Li, Y. Yang, J. Su, Z. Liang, and S. Wang, "Two-sided matching decision-making model with hesitant fuzzy preference information for configuring cloud

manufacturing tasks and resources[J]. Journal of Intelligent Manufacturing, 2020, 31(1).

[133] D. Yu, and Z. Xu, "Intuitionistic fuzzy two-sided matching model and its application to personnel-position matching problems[J]. Journal of the Operational Research Society, 2020, 71(2): 312-321.

[134] 关于调整本市一般工商业销售电价有关问题的通知[R/OL]. (2020-12-21) [2020-12-22]. http://www.beijing.gov.cn/zhengce/gfxwj/201905/t20190531_82985.html.

[135] 国家能源局发布 2019 年全国电力工业统计数据[R/OL] . (2020-12-21) [2020-12-22]. http://www.nea.gov.cn/2020-01/20/c_138720881.htm

[136] 全国行政区划信息查询平台[R/OL]. (2020-12-21) [2020-12-22]. http://xzqh.mca.gov.cn/map

[137] C. Fan, S. Ghaemi, H. Khazaei and P. Musilek, "Performance Evaluation of Blockchain Systems: A Systematic Survey[J]. IEEE Access. 2020, (8): 126927-126950.

附录 青岛国际院士港区块链+智慧能源园区/社区综合服务平台项目

附录 A 《区块链+智慧能源园区/社区综合服务展示平台研发成果报告》节选

A.1 研发约束说明.

搭建展示平台所需的物理系统，包括储能设备、智能开关、智能电表、通信模块、工控机、展台、展示屏等，包括设备的选型、采购、加工、安装调试等。

开发基于展台物理系统的软件系统，包括：区块链能源交易平台、区块链浏览器等。

A.1.1 硬件约束

平台相关物联网服务、Web 服务、Hyperledger Fabric 区块链服务、区块链浏览器服务，需要部署在 5 个树莓派及一个工控机上。其中树莓派型号为 3B+：单核 CPU、1GB RAM、64GB SD 卡存储；其中工控机为 6 核 CPU、8GB RAM、1TB SSD 硬盘。具体来说，物联网的数据采集、区块链的所有服务（peer、orderer）需要部署在树莓派上，其余部分部署在工控机上。

由于展览环境不确定，5 个树莓派与工控机之间需要独立无线路由器提供可靠的网络连接。工控机部署内网 DNS，各服务间使用开发域名进行访问。

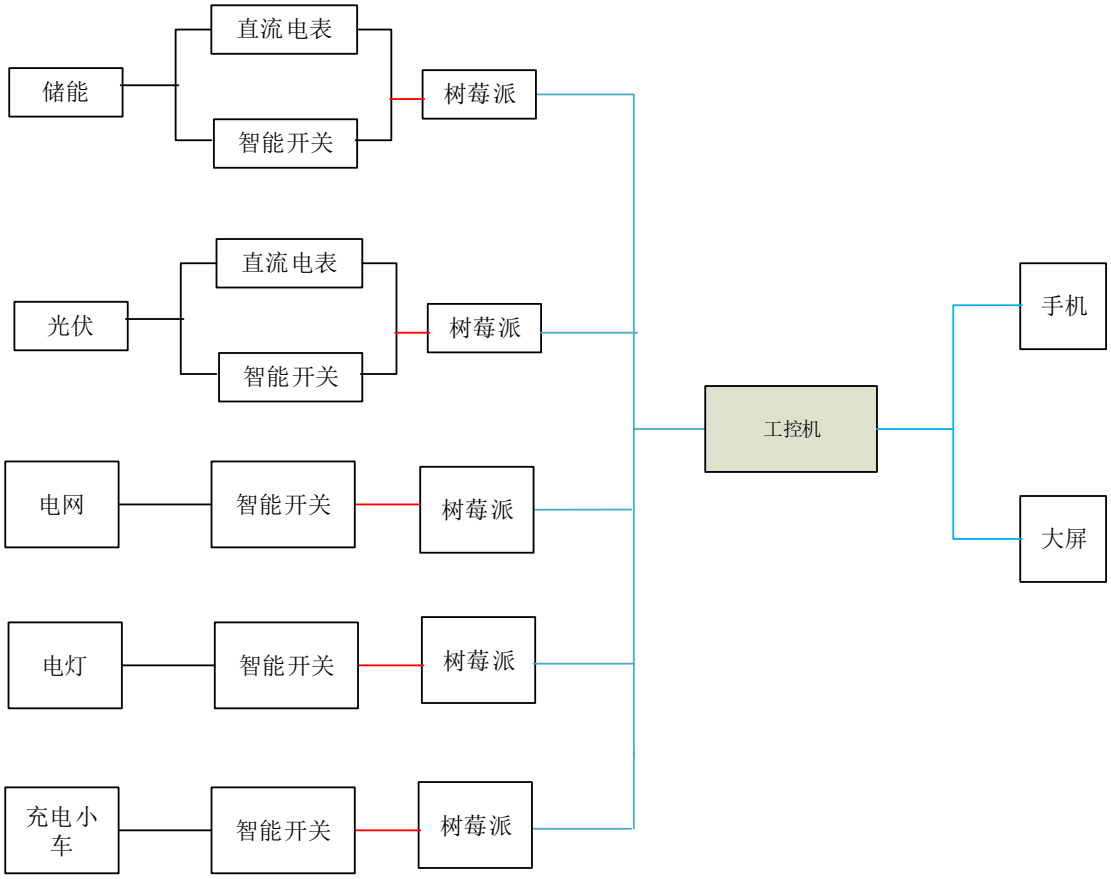
A.1.2 软件约束

物联网的数据收集使用 MQTT 协议；开发中使用到 Nodejs 为最新 LTS 版本，Golang 为 1.14 版本，PC 前端兼容当前正式版 Chrome 浏览器，手机前端兼容主流移动端浏览器；Web 后台及区块链浏览器需要使用 MongoDB、MySQL；

A.2 平台设计

A.2.1 硬件部分

硬件平台架构图:



连接方式说明：

1．黑线代表电路连接；

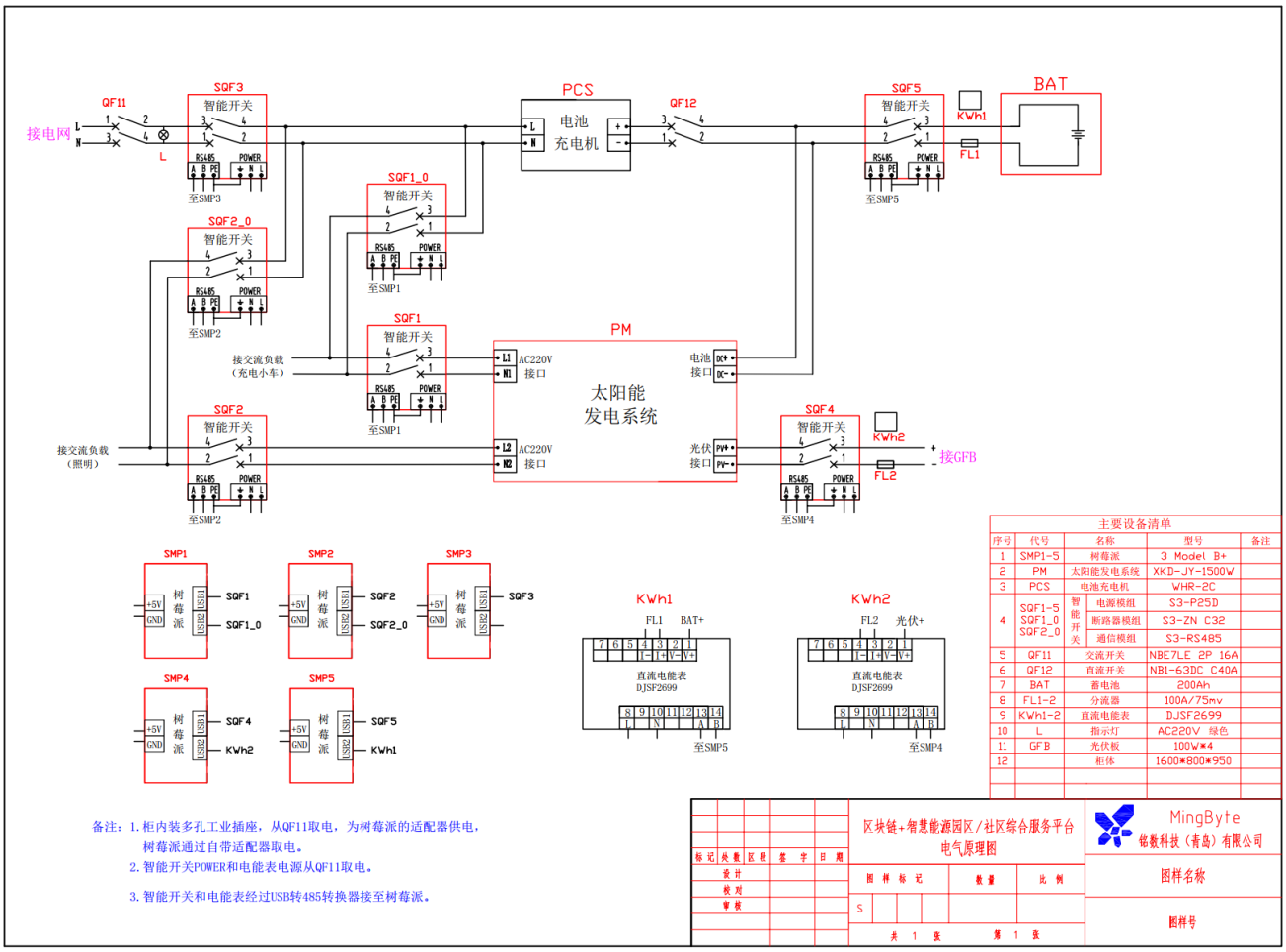
2．红线代表 RS485 通信线方式连接；

3．蓝线代表无线方式连接。

硬件平台搭建描述

名称	功能/模块	关键点
树莓派	直流电表与树莓派通信、智能开关与树莓派通信、储能设备的状态监控、充电小车的状态监控、数据与命令上传下传、区块链维护	数据与命令上传下传速度及反馈。
智能开关	获取交流电用电信息和控制电路闭合	与树莓派进行实时通信
直流电表	获取直流电的用电信息	与树莓派进行实时通信
储能设备	储能设备的状态监控、电器件间的兼容与电能交互	实时监控储能设备的状态。
充电小车	充电小车的状态监控、电器件间的兼容与电能交互	实时监控充电小车的充电开关状态
电灯	照明负载的状态监控，电器件间的兼容与电能交互	实时监控照明负载的开关状态
前端展示	微网状态展示和控制	充分展示、观感好、体现优势

电气设计：



主要设备清单

序号	代号	名称	型号	备注
1	SMP1-5	树莓派	3 Model B+	
2	PM	太阳能发电系统	XKD-JY-1500W	
3	PCS	电池充电机	WHR-2C	
4	SQF1-5 SQF1_0 SQF2_0	智能开关 电源模组	S3-P25D	
		断路器模组	S3-ZN C32	
		通信模组	S3-RS485	
5	QF11	交流开关	NBE7LE 2P 16A	
6	QF12	直流开关	NB1-63DC C40A	
7	BAT	蓄电池	200Ah	
8	FL1-2	分流器	100A/75mv	
9	KWh1-2	直流电能表	DJSF2699	
10	L	指示灯	AC220V 绿色	
11	GFB	光伏板	100W*4	
12		柜体	1600*800*950	

备注：1. 柜内装多孔工业插座，从QF11取电，为树莓派的适配器供电，
树莓派通过自带适配器取电。
2. 智能开关POWER和电能表电源从QF11取电。
3. 智能开关和电能表经过USB转485转换器接至树莓派。

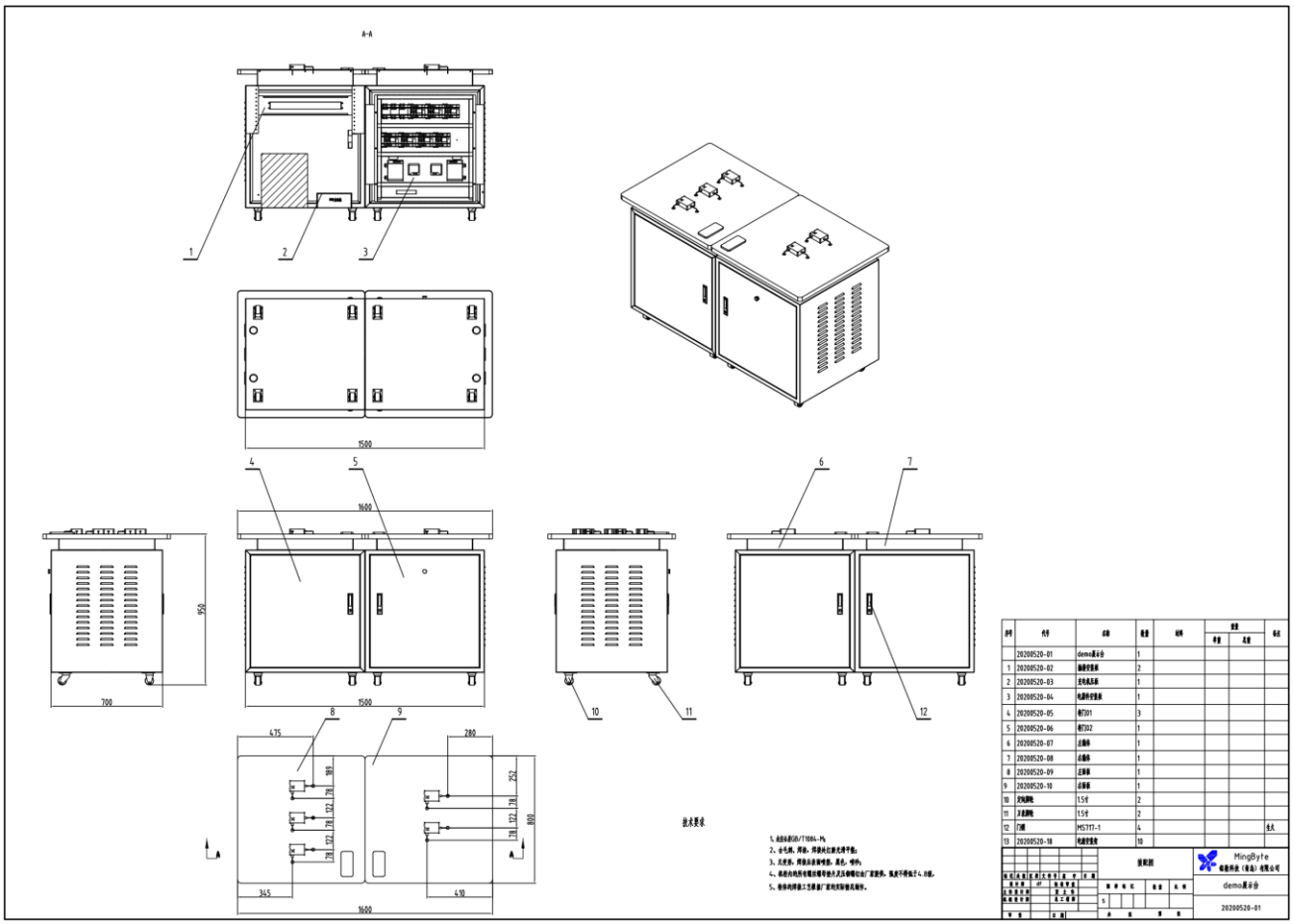
区块链+智慧能源园区/社区综合服务平台
电气原理图

MingByte
铭数科技（青岛）有限公司

图样名称

图样号

结构设计：



A.2.2 软件部分

总体设计说明

平台软件划分为：Web 前端、Web 服务端、分布式节点常驻服务、Hyperledger Fabric 链码及相关服务。详细描述如下：

Web 前端包括两部分，一部分用于触摸大屏，另一部分用于手机端。前者主要包含硬件状态展示、区块链浏览器、智慧社区服务，需要适配 1920*1080 分辨率，Chrome 当前稳定版；后者需要兼容主流移动端浏览器，主要包含硬件控制、部分硬件状态展示、智慧社区服务。

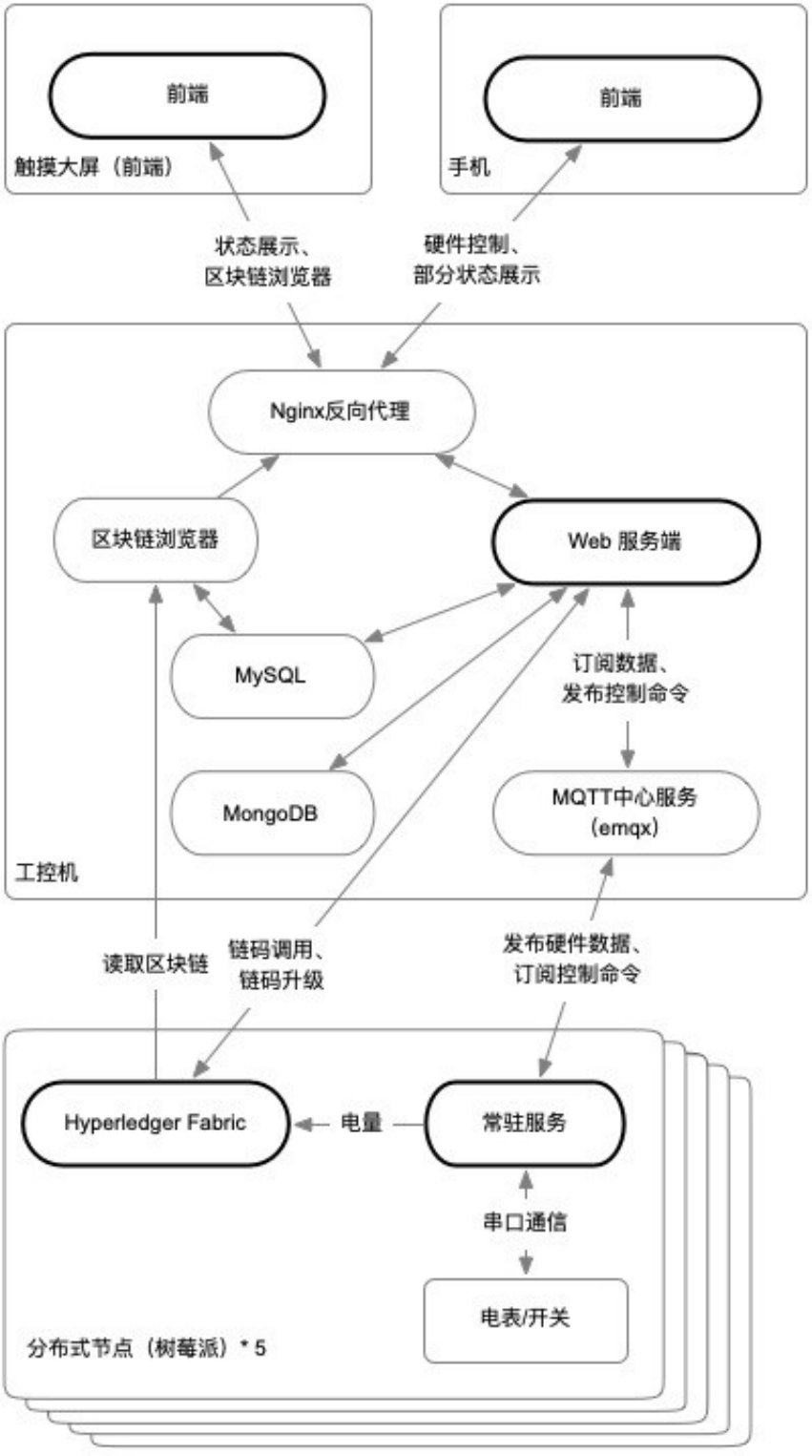
Web 服务端包含以下功能：物联网信息订阅、存储、推送，区块链链码升级、交易触发、历史数据查询，提供 Restful 接口供前端调用。

分布式节点常驻服务包含以下功能：读取硬件数据并上传，读取节点电量相

关数据并按固定周期上链，订阅硬件控制指令消息，并下发命令到硬件。

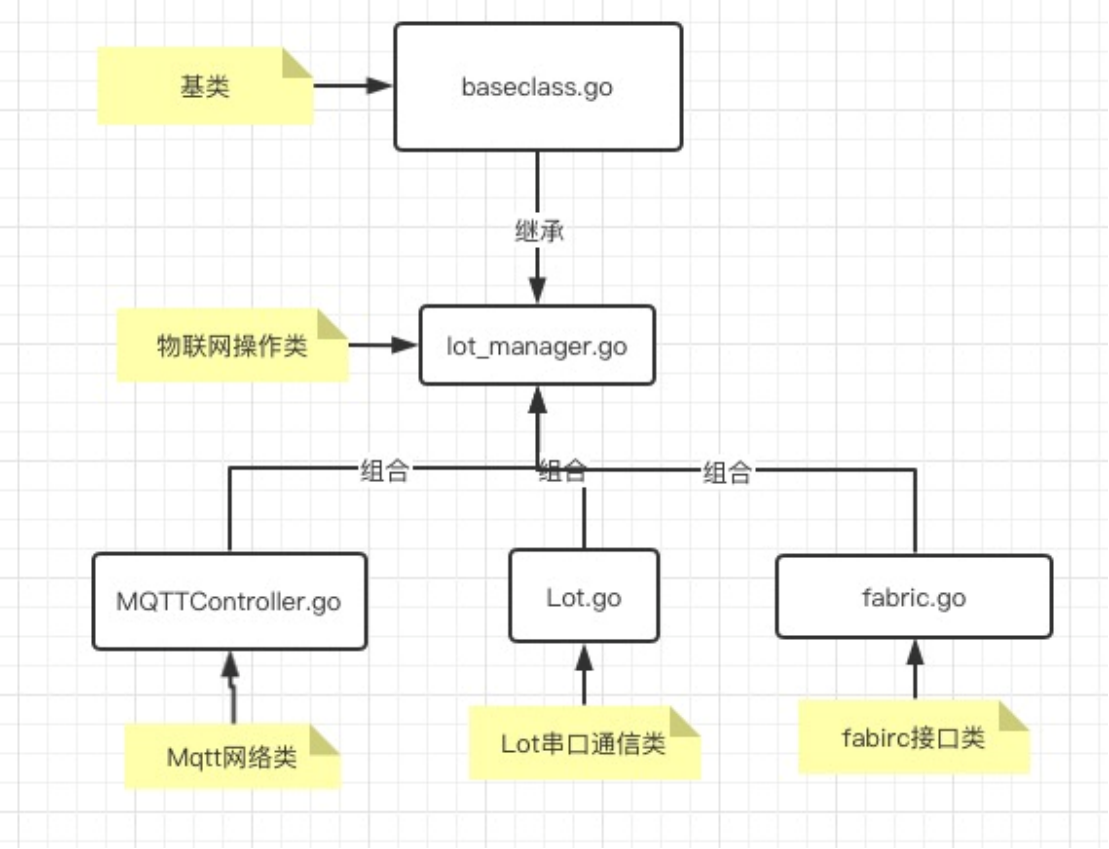
Hyperledger Fabric 链码及相关服务。链码部分：首先，按照《能源互联网交易结算系统研发需求说明书》（附录 B）中描述的结算机制，实现各节点上传电量数据的结算；其次提供相关交易数据的查询；最后实现用户管理、链码升级等基础功能相关的链码方法。其余 Fabric 相关服务需要重新构建，确保能够在树莓派硬件环境下稳定运行。

总体功能流程图如下：

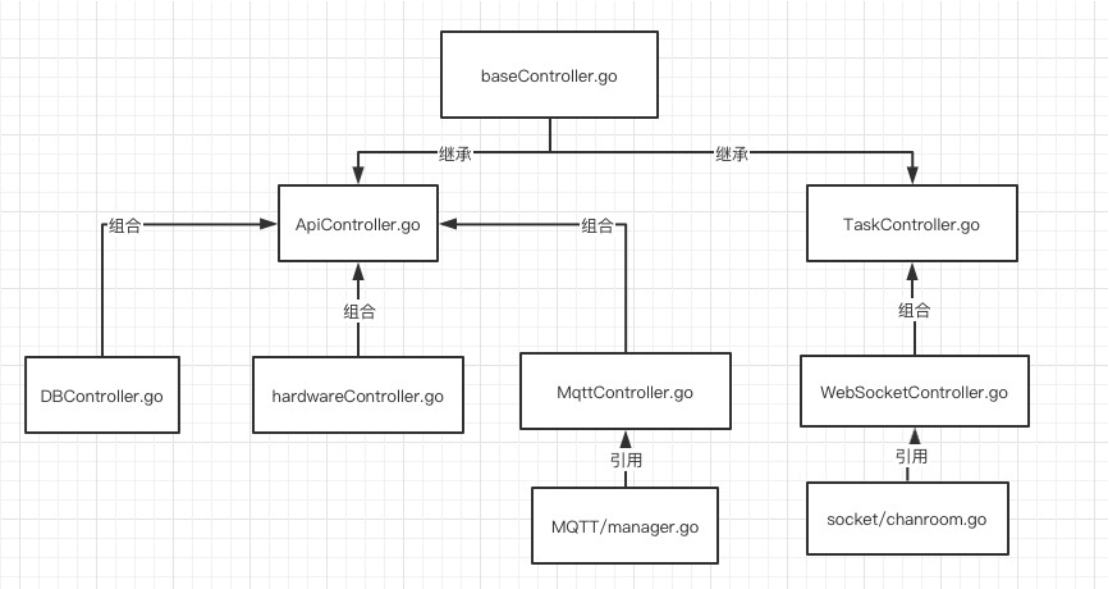

前端
触摸大屏（前端）
前端
手机
状态展示、
区块链浏览器
硬件控制、
部分状态展示
Nginx反向代理
区块链浏览器
Web 服务端
MySQL
MongoDB
订阅数据、
发布控制命令
MQTT中心服务
(emqx)
工控机
读取区块链
链码调用、
链码升级
发布硬件数据、
订阅控制命令
Hyperledger Fabric
电量
常驻服务
串口通信
电表/开关
分布式节点（树莓派）*5

结构和流程

- 前端
  - 触摸大屏前端：总览页展示平台硬件状态，各节点详细页面展示硬件状态以及近期数据（硬件状态数据、交易数据），其数据一部分来自服务端实时推送，一部分来自服务端 Restful 接口；区块链浏览器相关数据来自于单独部署的 Hyperledger Fabric 官方区块链浏览器服务；智慧社区相关页面由前端按需求模拟生成。
  - 手机浏览器前端：储能、负载两个页面提供对平台硬件通路的切换控制，并实时展示硬件状态，此外，分别展示储能、负载两个节点的交易数据、近期状态数据；智慧社区页面数据由前端按需求模拟生成；手机端任一页面打开时，触摸大屏需要同步弹出展示相同页面。
  - 后台服务与区块链服务统一由 Nginx 反向代理，面向前端提供同一域名下的接口，避免跨域，降低前端对接多数据源带来的维护难度。
- IOT 数据采集服务：用于采集 IOT 设备数据，将数据通过 Hyperledger Fabric Golang SDK 上传到区块链中,在 API 服务端中使用 MQTT 进行 IOT 设备的命令下发，结构图如下

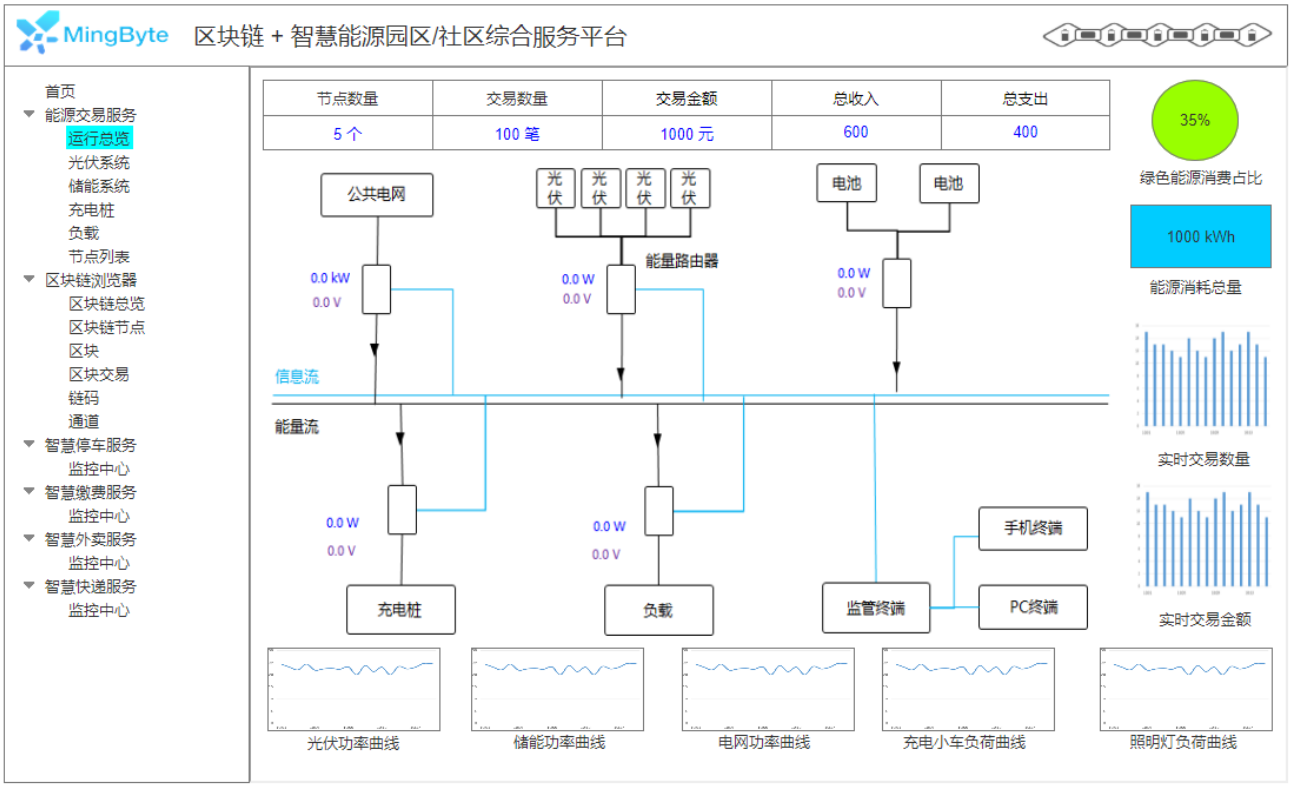


◆ API 后台服务，用于服务监控，指令下发，数据展示和移动端接口服务，其架构图如下



前端功能开发

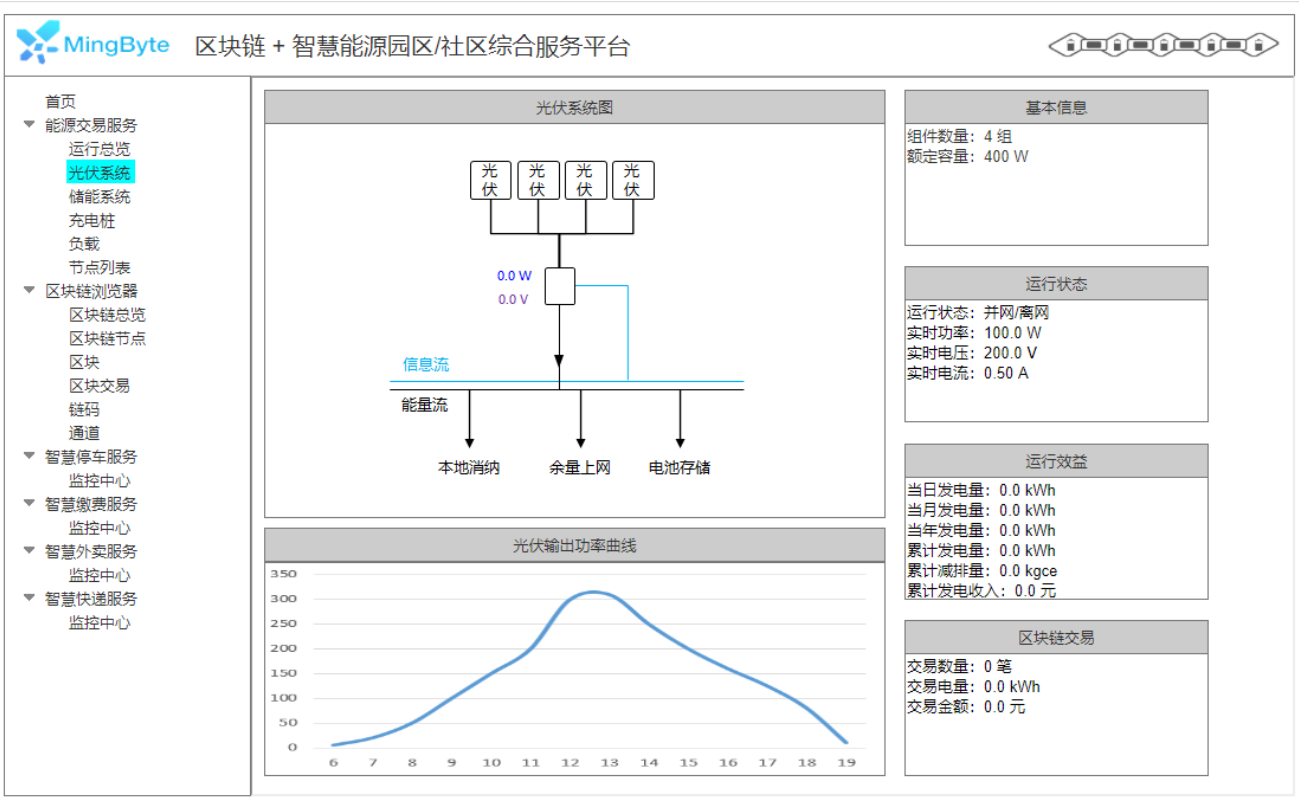
运行总览



功能点	功能描述及业务规则
节点数量	截止到目前系统中能源交易节点的个数，目前包括光伏、储能、电网、电动桩、负载共计 5 个。
交易数量	截止到目前发生的能源交易笔数（注意不能重复统计）
交易金额	截止到目前发生的能源交易金额（注意不能重复统计）
总收入	截止到目前所有节点卖出交易的总金额

总支出	截止到目前所有节点买入交易的总金额
绿色能源消费占比	截止到目前光伏发电量占（电网电量+光伏发电量）的比例
能源消耗总量	截止到目前（电网电量+光伏发电量）的合计；
实时交易数量	最近 15 分钟每分钟的交易笔数
实时交易金额	最近 15 分钟每分钟的交易金额
光伏功率曲线	最近 15 分钟的光伏功率曲线（横轴：时分，纵轴：功率）
储能功率曲线	最近 15 分钟的储能功率曲线（同上）
电网功率曲线	最近 15 分钟的电网功率曲线（同上）
充电小车负荷曲线	最近 15 分钟的充电小车负荷曲线（同上）
照明负载负荷曲线	最近 15 分钟的照明负载负荷曲线（同上）
系统图	实时显示电能流向（可根据功率的正负判断流向）； 实时显示每个能量支路的运行参数（功率 W、电压 V）

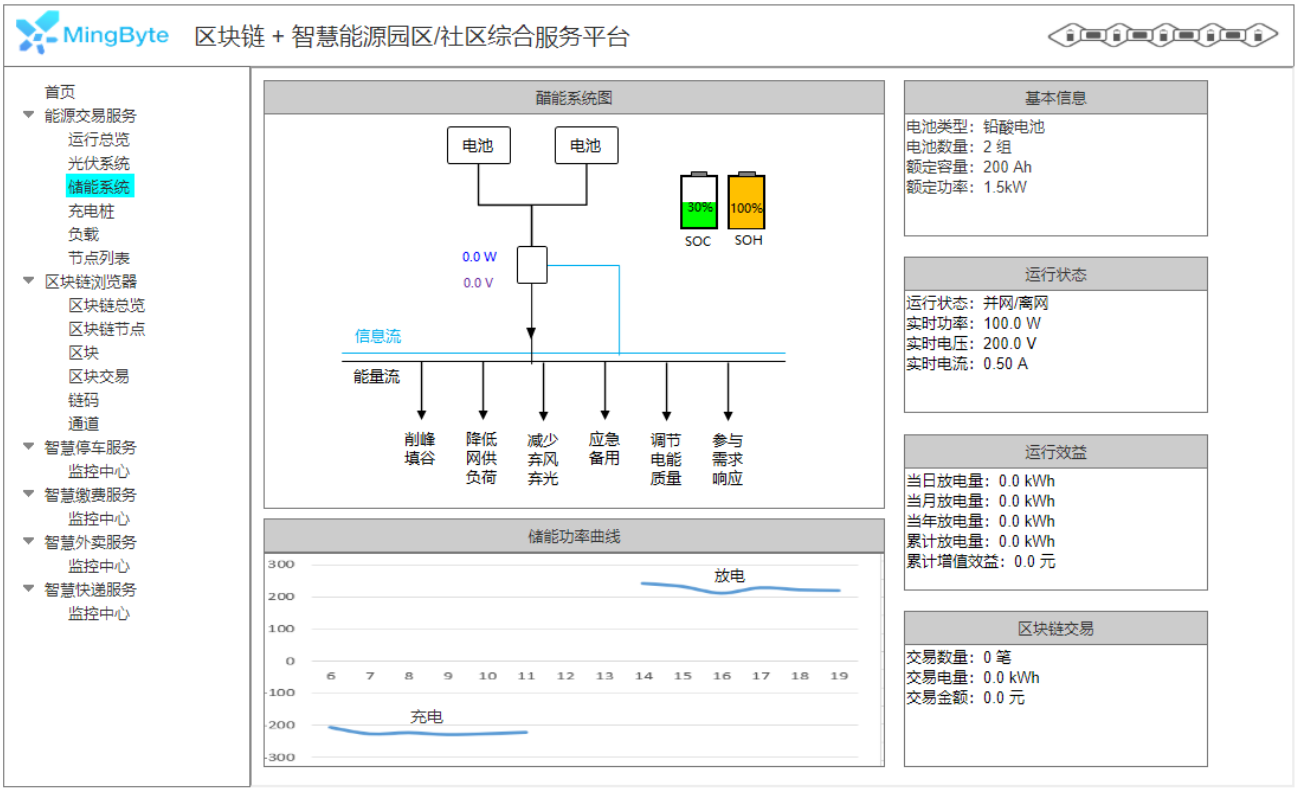
光伏系统



功能点	功能描述及业务规则
光伏系统图	实时显示电能流向（可根据功率的正负判断流向）； 中间路由器左侧实时显示功率和电压；
基本信息	静态信息
运行状态	运行状态：光伏开关断开时显示离网，闭合时显示并网； 实时功率：最新的光伏输出功率； 实时电压：最新的光伏输出电压； 实时电流：最新的光伏输出电流；
运行效益	当日发电量：当日的光伏发电量合计；

	当月发电量：当月的光伏发电量合计； 当年发电量：当年的光伏发电量合计； 累计发电量：历年光伏发电量合计； 累计发电收入：累计发电量 X 光伏发电价格
区块链交易	交易笔数：截止目前光伏节点发生的能源交易笔数合计； 交易电量：截止目前光伏节点发生的能源交易电量合计； 交易金额：截止目前光伏节点发生的能源交易金额合计；
光伏输出功率曲线	当日光伏发电的功率输出曲线（横轴：整点，纵轴：功率）

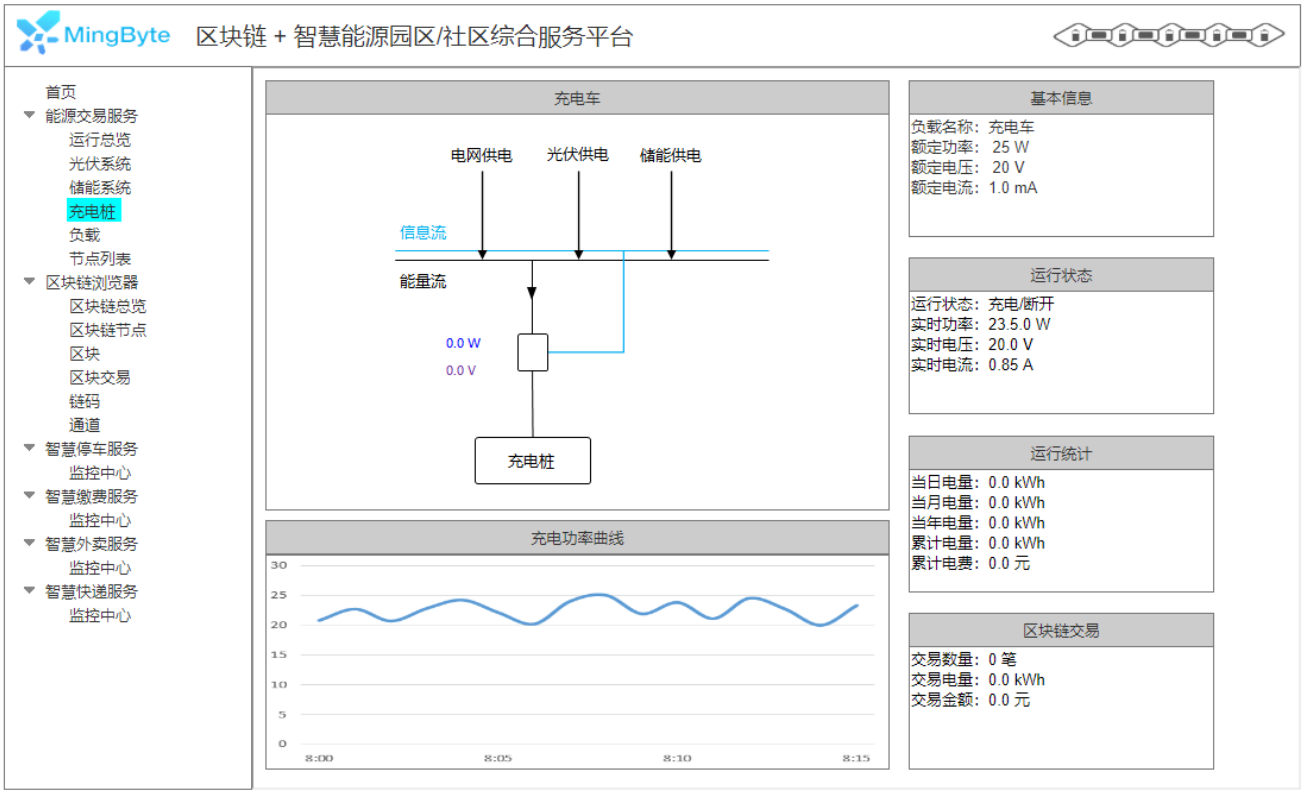
储能系统



功能点	功能描述及业务规则
储能系统图	实时显示电能流向（可根据功率的正负判断流向）； 中间路由器左侧实时显示功率和电压；
基本信息	静态信息
运行状态	运行状态：储能开关断开时显示离网，闭合时显示并网； 实时功率：最新的储能充/放电功率； 实时电压：最新的光伏充/放电电压； 实时电流：最新的光伏充/放电电流；
运行效益	当日放电量：当日的储能放发电量合计； 当月放电量：当月的能放发电量合计； 当年放电量：当年的能放发电量合计； 累计放电量：历年能放发电量合计； 累计增值收益：累计放电量 X 储能度电收益（价格表）

区块链交易	交易笔数：截止目前储能节点发生的能源交易笔数合计； 交易电量：截止目前储能节点发生的能源交易电量合计； 交易金额：截止目前储能节点发生的能源交易金额合计；
储能功率曲线	当日储能充放电功率曲线（横轴：整点，纵轴：功率）； 充电功率：负值，放电功率：正值；

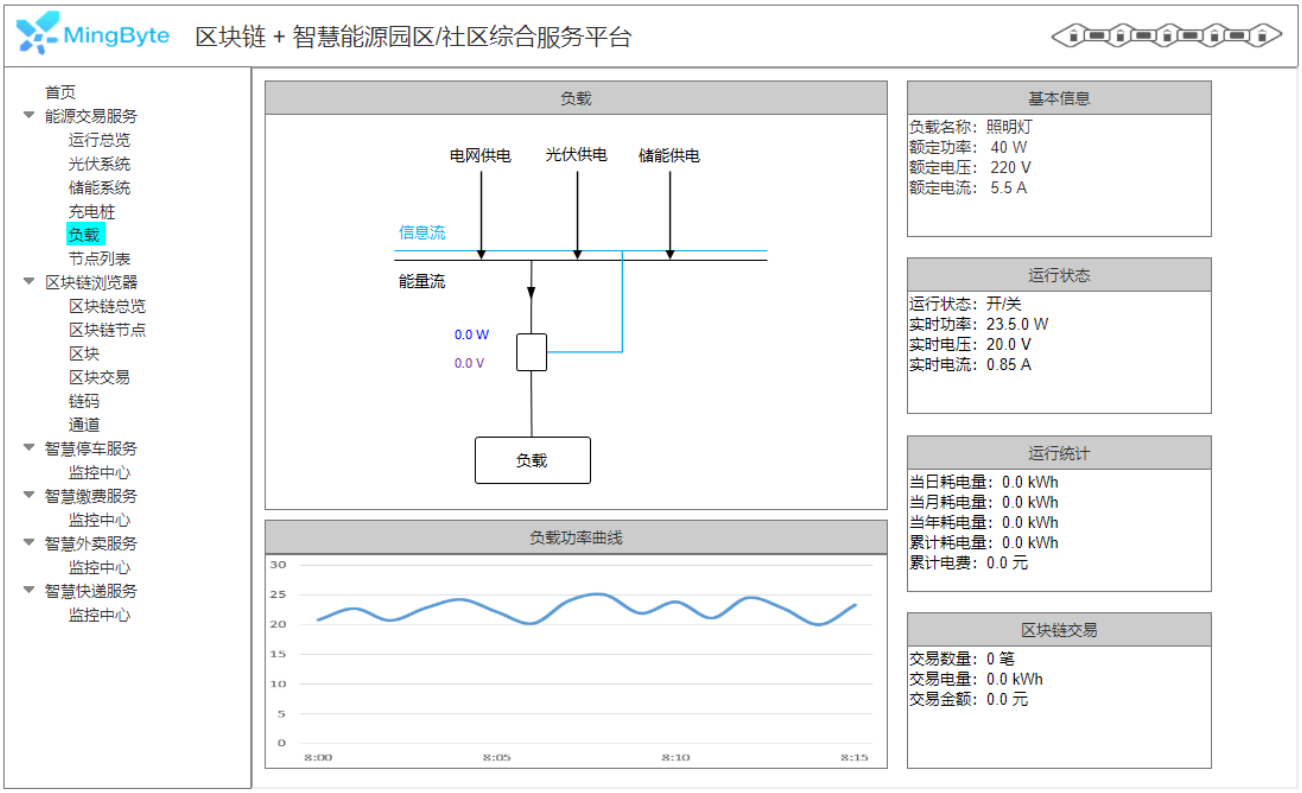
充电桩



功能点	功能描述及业务规则
系统图	实时显示电能流向（可根据功率的正负判断流向）； 中间路由器左侧实时充电功率和电压；
基本信息	静态信息
运行状态	运行状态：开关断开时显示断开，闭合时显示充电； 实时功率：最新的充电功率； 实时电压：最新的充电电压； 实时电流：最新的充电电流；
运行效益	当日电量：当日的充电电量合计； 当月电量：当月的充电电量合计； 当年电量：当年的充电电量合计； 累计电量：历年的充电电量合计； 累计电费：累计电量 X 用电价格（价格表）
区块链交易	交易笔数：截止目前充电车节点发生的能源交易笔数合计； 交易电量：截止目前充电车节点发生的能源交易电量合计； 交易金额：截止目前充电车节点发生的能源交易金额合计；

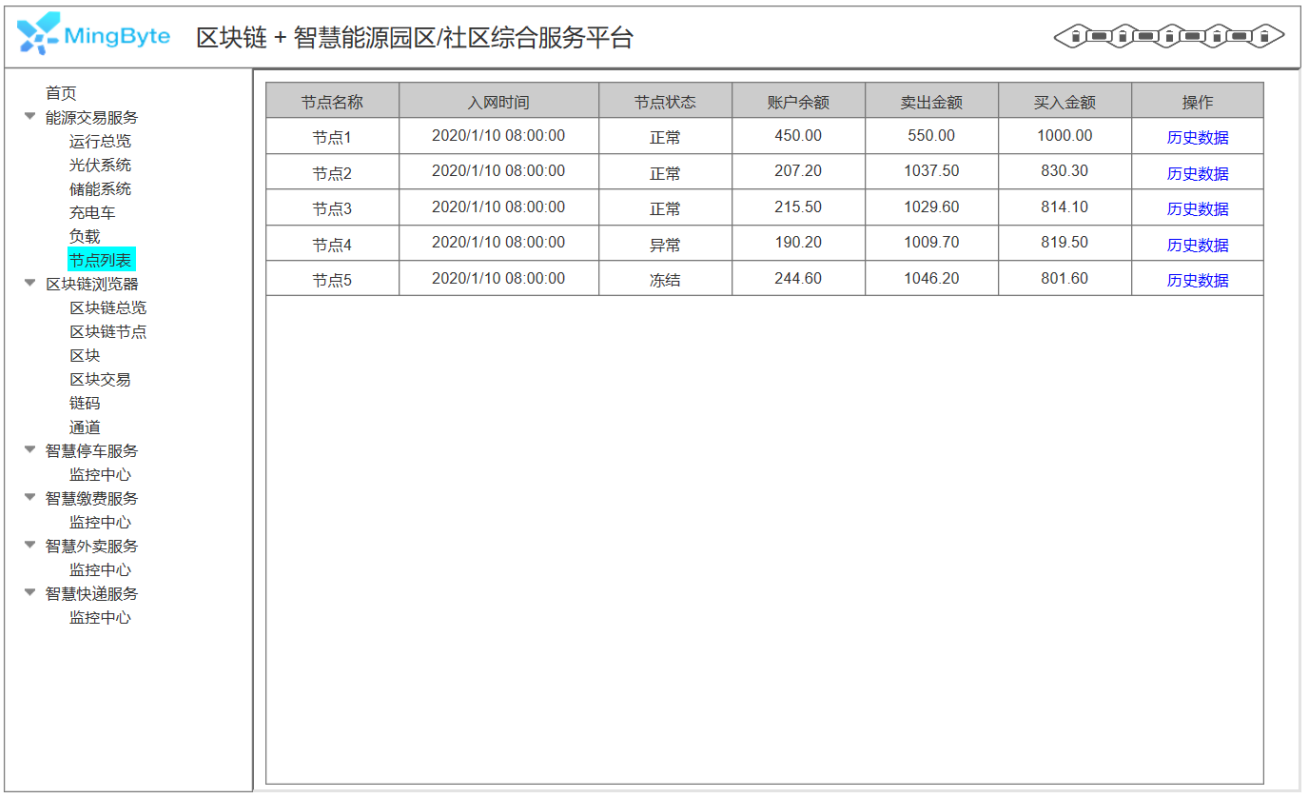
充电功率曲线	当日充电车充电功率曲线（横轴：整点，纵轴：功率）；

负载

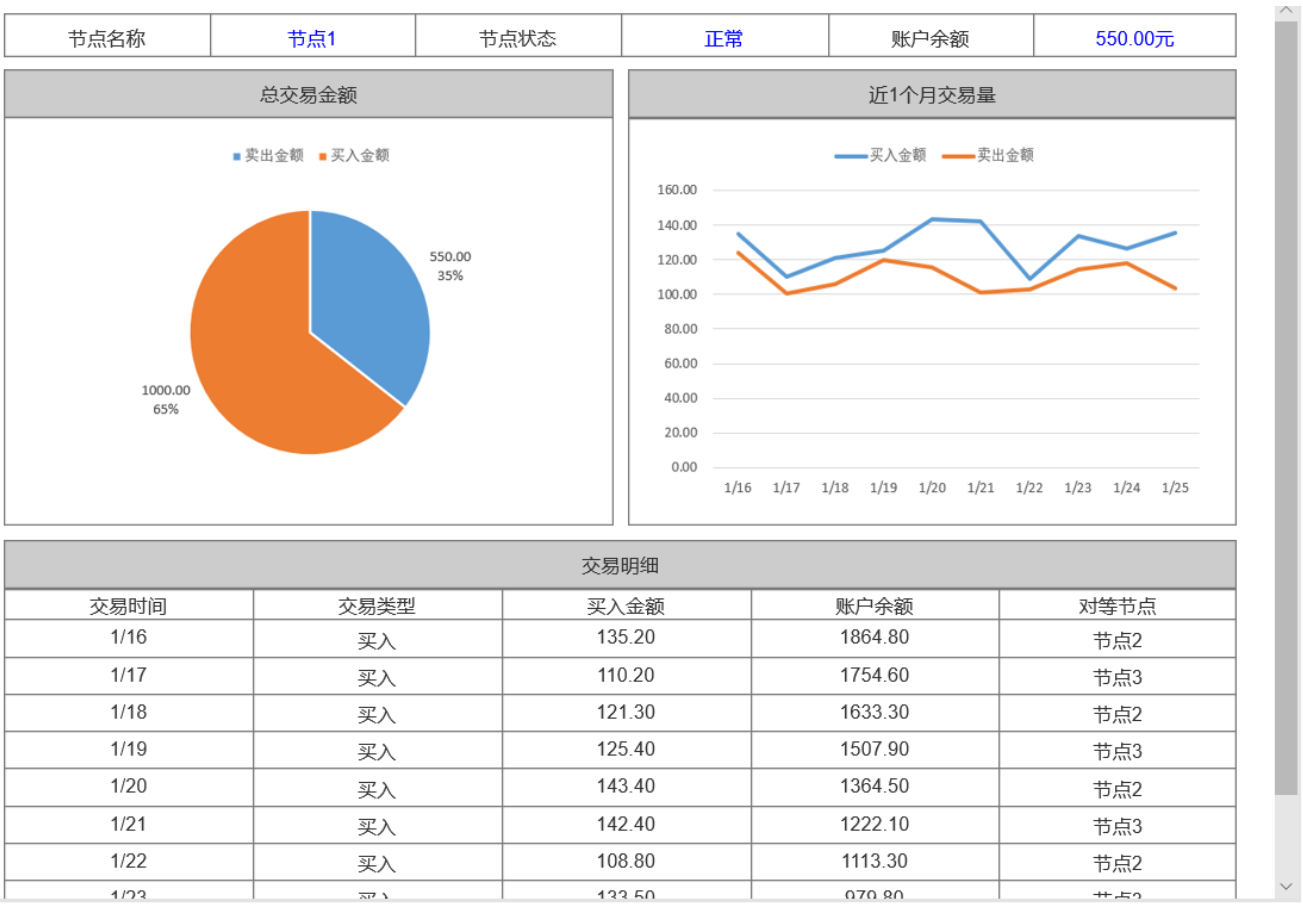


功能点	功能描述及业务规则
系统图	实时显示电能流向（可根据功率的正负判断流向）； 中间路由器左侧实时负载功率和电压；
基本信息	静态信息
运行状态	运行状态：开关断开时显示关，闭合时显示开； 实时功率：最新的负载功率； 实时电压：最新的负载电压； 实时电流：最新的负载电流；
运行效益	当日电量：当日的负载用电量合计； 当月电量：当月的负载用电量合计； 当年电量：当年的负载用电量合计； 累计电量：历年的负载用电量合计； 累计电费：累计电量 X 用电价格（价格表）
区块链交易	交易笔数：截止目前负载用节点发生的能源交易笔数合计； 交易电量：截止目前负载用节点发生的能源交易电量合计； 交易金额：截止目前负载用节点发生的能源交易金额合计；
充电功率曲线	当日负载用功率曲线（横轴：整点，纵轴：功率）；

节点列表



功能点	功能描述及业务规则
节点名称	显示节点的中文名称，在本项目中五个节点的名称分别是：电网、光伏、储能、充电车、负载
入网时间	显示本节点的入网时间，本项目是手动设置好的
节点状态	有正常、异常、冻结三种状态，显示本节点的实际状态，本项目一般都是正常状态
账户余额	显示本节点的实际余额，如果初始金额为零，那么账户金额等于卖出金额合计减去买入金额合计
卖出金额	显示本节点所有卖出交易的金额合计
买入金额	显示本节点所有买入交易的金额合计
历史数据	点击“历史数据”打开给节点对应的历史交易记录页面



功能点	功能描述及业务规则
上部的状态条	分别显示该节点的节点名称、节点状态、账户余额的实际值
总成交金额	饼图方式显示该节点卖出交易金额、买入交易金额及占比
近一个月交易量	曲线方式显示该节点一个月内每天的卖出交易金额、买入交易金额，横轴：日期、纵轴：金额
交易明细	列表方式显示该节点所有的买入和卖出交易记录明细

后端功能开发

区块链功能模块

功能	描述	备注
树莓派：硬件通信	树莓派常驻服务需要与各硬件进行通信，一方面去读硬件上传的数据，一方面将用户指令下发到硬件。	
树莓派：区块链交互	树莓派常驻服务需要与 Hyperledger Fabric 网络进行交互，调用、查询链码来实现链上数据的读写。	
树莓派：面向手机前端提供接口	为手机前端提供数据、接收手机端下发的指令。	其中部分数据需要实时推送。
工控机：面向前端提供数据接口	工控机常驻服务要为大屏前端提供数据接口，用于系统状态、历史数据的展示。	其中部分数据需要实时推送。
工控机：指令控制	树莓派收到手机指令，下发到硬件之前需要经过工控机进行安全校验；在无人操作的默认状态下，工	无人操作的默认状态可能需要后期明确具

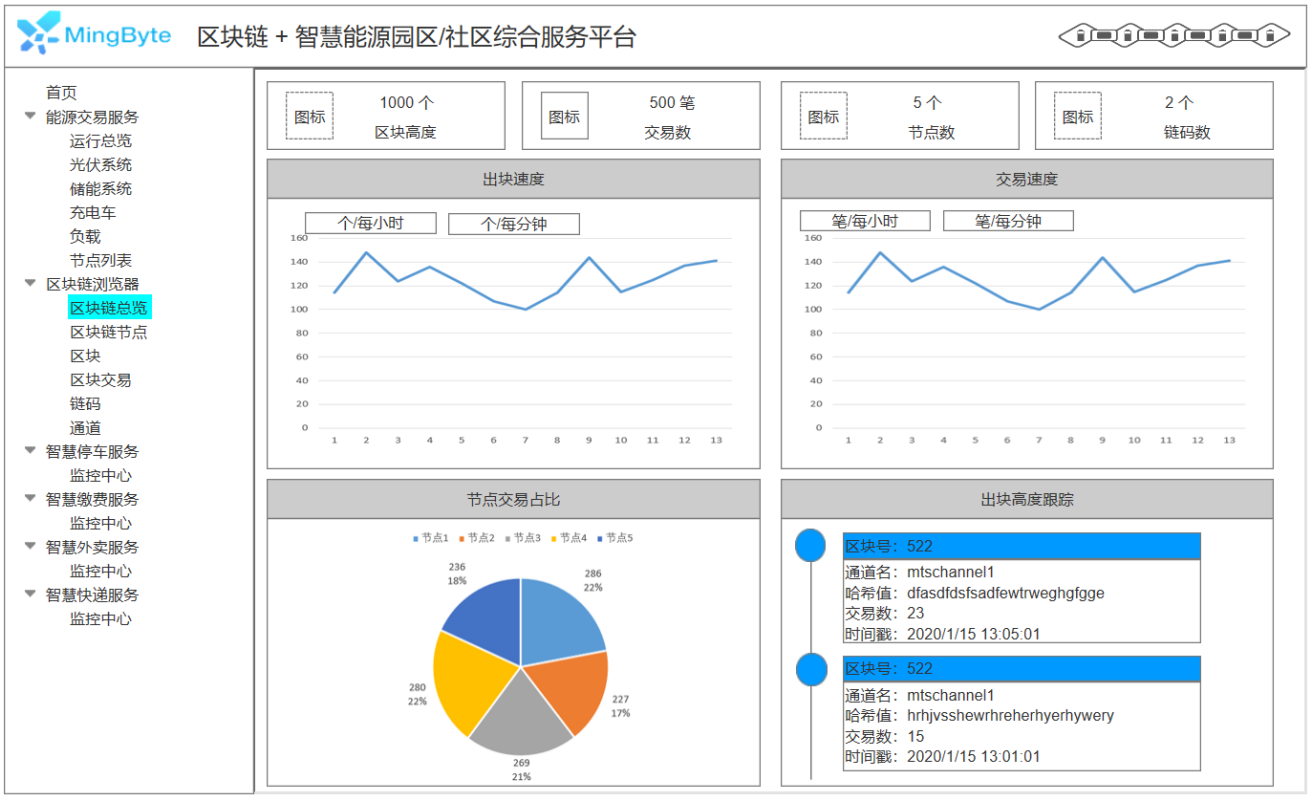
	控机负责下发硬件指令。	体表现。
工控机：区块链交互	工控机常驻服务需要与 Hyperledger Fabric 网络进行交互，调用、查询链码来实现链上数据的读写。	
工控机：区块链操作	工控机常驻服务需要为 Hyperledger Fabric 网络通道远程安装、升级链码	
区块链智能合约：数据管理	链码需要设计好上链数据的结构，提供链码方法，供其他模块对数据进行增删查改；需要考虑部分数据的私密性。	数据私密性可以通过私有数据或加密上链解决。
区块链智能合约：结算	链码需实现结算功能，基于各成员上传的真实数据进行能源交易。功能实现需考虑交易的触发机制、匹配规则、偏差处理	默认使用 2.0 的交易结算机制。

硬件通信功能模块

功能	描述	备注
智能直流电表与树莓派通信	智能直流电表应用在光伏和储能两个支路上，通过 RS485 方式与树莓派进行通信，智能直流电表把电表的实时用电量、电流值、电压值、充放电状态等传递给树莓派。	
智能开关与树莓派通信和控制	树莓派实时监视智能开关的状态，判断端口状态；智能开关把本路的实时用电量、电流值、电压值等传递给树莓派；树莓派获取前端下发的控制指令来控制开关。	
储能设备的状态监控	树莓派监控储能设备的充放电状态，充放电状态通过电流的正负值进行判断，储能设备的电量监控通过电压的变化来计算电量。	
充电小车的状态监控	树莓派监控充电小车的充电开关状态。	
数据与命令上传下传	以树莓派作为节点进行数据与命令的上传下传。	

区块链浏览器

区块链总览


MingByte
区块链 + 智慧能源园区/社区综合服务平台
首页
能源交易服务
运行总览
光伏系统
储能系统
充电车
负载
节点列表
区块链浏览器
区块链总览
区块链节点
区块
区块交易
链码
通道
智慧停车服务
监控中心
智慧缴费服务
监控中心
智慧外卖服务
监控中心
智慧快递服务
监控中心
图标
1000 个
区块高度
图标
500 笔
交易数
图标
5 个
节点数
图标
2 个
链码数
出块速度
个/每小时
个/每分钟
交易速度
笔/每小时
笔/每分钟
节点交易占比
节点1
节点2
节点3
节点4
节点5
236
18%
286
22%
280
22%
227
17%
269
21%
出块高度跟踪
区块号：522
通道名：mtschannel1
哈希值：dfasdfdsfsadfewtrweghgfgge
交易数：23
时间戳：2020/1/15 13:05:01
区块号：522
通道名：mtschannel1
哈希值：hrhjvsshewrhreherhyerhywery
交易数：15
时间戳：2020/1/15 13:01:01

区块链节点


MingByte
区块链 + 智慧能源园区/社区综合服务平台
首页
能源交易服务
运行总览
光伏系统
储能系统
充电车
负载
节点列表
区块链浏览器
区块链总览
区块链节点
区块
区块交易
链码
通道
智慧停车服务
监控中心
智慧缴费服务
监控中心
智慧外卖服务
监控中心
智慧快递服务
监控中心
节点名称 节点类型 服务地址 组织ID 区块高度
节点1 Peer p1.so,microgridmingbyte ServiceOrgMSP 522
节点2 Peer p2.so,microgrid.mingbyte ServiceOrgMSP 525
节点3 Oderer p2.so,microgrid.mingbyte ServiceOrgMSP 413
节点4 Oderer o3.so,microgrid.mingbyte ServiceOrdererMSP 321
节点5 Oderer o5.so,microgrid.mingbyte ServiceOrdererMSP 256

区块查询

区块交易查询

链码

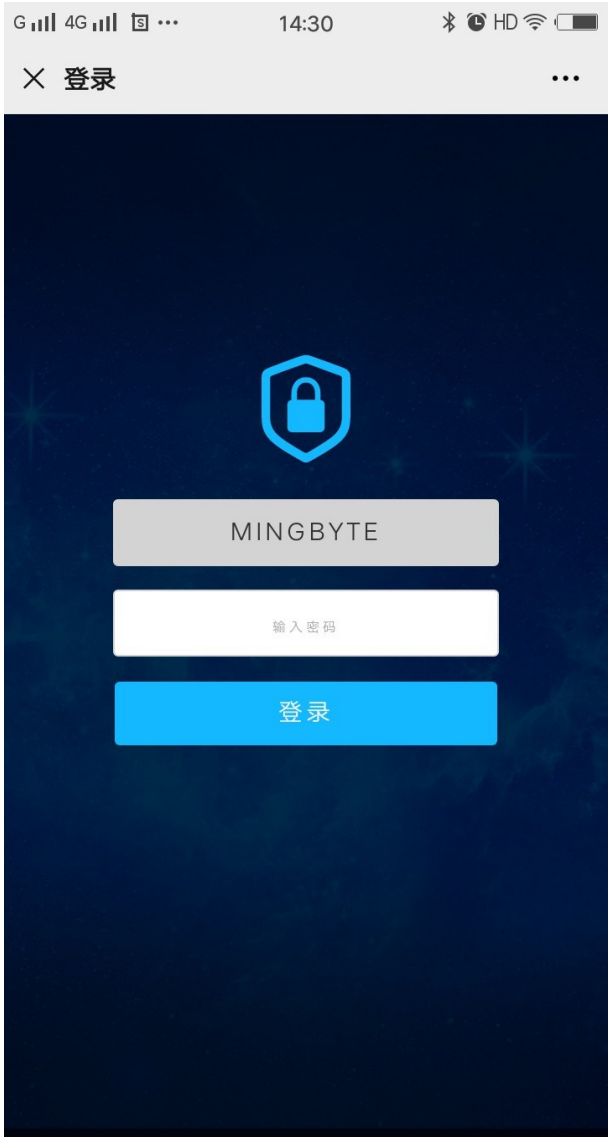

MingByte
区块链 + 智慧能源园区/社区综合服务平台
首页
能源交易服务
运行总览
光伏系统
储能系统
充电车
负载
节点列表
区块链浏览器
区块链总览
区块链节点
区块
区块交易
链码
通道
智慧停车服务
监控中心
智慧缴费服务
监控中心
智慧外卖服务
监控中心
智慧快递服务
监控中心
节点名称 节点类型 服务地址 组织ID 区块高度
节点1 Peer p1.so,microgridmingbyte ServiceOrgMSP 522
节点2 Peer p2.so,microgrid.mingbyte ServiceOrgMSP 525
节点3 Oderer p2.so,microgrid.mingbyte ServiceOrgMSP 413
节点4 Oderer o3.so,microgrid.mingbyte ServiceOrdererMSP 321
节点5 Oderer o5.so,microgrid.mingbyte ServiceOrdererMSP 256

通道


MingByte
区块链 + 智慧能源园区/社区综合服务平台
首页
能源交易服务
运行总览
光伏系统
储能系统
充电车
负载
节点列表
区块链浏览器
区块链总览
区块链节点
区块
区块交易
链码
通道
智慧停车服务
监控中心
智慧缴费服务
监控中心
智慧外卖服务
监控中心
智慧快递服务
监控中心
通道名称 区块数量 交易数量 时间戳

手机端

登录



首页

注：点击进入对应的功能页面。

负载

节点状态 正常 账户余额 1507.90元

当前时间 10:00:05

00:03:10
用电时长

0.5kW
用电功率

1.2kWh
交易电量

10次
交易次数

区块链交易记录

交易时间	交易类型	买入金额	账户余额	卖方节点
1/16 10:01	买入	135.20	1864.80	节点2
1/16 10:02	买入	110.20	1754.60	节点3
1/16 10:03	买入	121.30	1633.30	节点2
1/16 10:04	买入	125.40	1507.90	节点3

基本信息

负载名称	照明灯	额定功率	40W
额定电压	220V	额定电流	5.5A

运行状态

运行状态	开/关	实时功率	23.5.0W
实时电压	22.0V	实时电流	0.85A

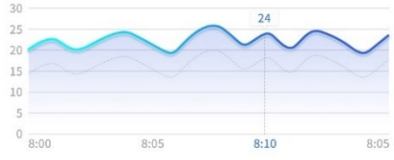
运行统计

当日耗电量	0.0kWh	当月耗电量	0.0kWh
当年耗电量	0.0kWh	累计耗电量	0.0kWh
累计电费	0.0元		

区块链交易

交易数量	0笔	交易电量	0.0kWh
交易金额	0.0元		

实时负荷曲线



功能点	功能描述及业务规则
系统图	动态显示能量的流向（根据电流的正负） 点击“电网”、“光伏”、“储能”任意一个节点时，提示“电网/光伏/储能供电”，激活点击的节点（开关打开，图标变亮），其他 2 个节点非激活状态（开关关闭，图标变灰或白）； 点击“负载”节点或“开/关”按钮时，“负载”节点在激活和非激活状态间切换，灯泡点亮或熄灭。
节点状态及账务余额部分	实时显示当前负载节点的状态和账户余额 当前时间：显示系统时间（时分秒） 用电时长：点击按钮“开”负载开始用电的累计时长（时分秒） 用电功率：负载节点的实时用电功率； 交易电量：负载节点本次用电时长内的用电交易电量； 交易次数：负载节点本次用电时长内的用电交易次数；
基本信息	和 PC 端对应的负载页面一致
运行状态	和 PC 端对应的负载页面一致
运行统计	和 PC 端对应的负载页面一致
区块链交易	和 PC 端对应的负载页面一致
实时负载曲线	和 PC 端对应的负载页面一致

储能

节点状态 正常 账户余额 1507.90元

充电/放电/待机
工作状态

10:00:05
系统时间

00:03:10
充电时长

0.5kW
充电功率

1.2kWh
充电电量

10次
交易次数

区块链交易记录

交易时间	交易类型	买入金额	账户余额	卖方节点
1/16 10:01	买入	135.20	1864.80	节点2
1/16 10:02	买入	110.20	1754.60	节点3
1/16 10:03	买入	121.30	1633.30	节点2
1/16 10:04	买入	125.40	1507.90	节点3

基本信息

- 电池类型 铅酸电池
- 电池数量 2组
- 额定定量 220Ah
- 额定功率 1.5kW

运行状态

- 运行状态 并网/离网
- 实时功率 100.0W
- 实时电压 200.0V
- 实时电流 0.50A

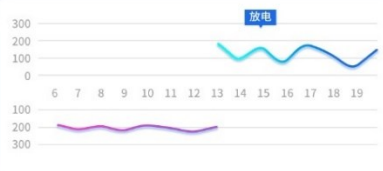
运行效益

- 当日放电量 0.0kWh
- 当月放电量 0.0kWh
- 当年放电量 0.0kWh
- 累计放电量 0.0kWh
- 累计增值效益 0.0元

区块链交易

- 交易数量 0笔
- 交易电量 0.0kWh
- 交易金额 0.0元

储能功率曲线



功能点	功能描述及业务规则
系统图	动态显示能量的流向（根据电流的正负） 点击按钮“充电“时，在光伏充电和电网充电两种模式间切换，一个激活状态（图标变亮，开关打开），一个非激活状态（图标变灰或白，开关打开）； 点击按钮“放电”时，负载节点在激活和非激活状态间切换，激活状态（图标变亮、开关打开），非激活状态（图标变灰，开关关闭）
节点状态及账务余额部分	实时显示当前储能节点的状态和账户余额 工作状态：当前处于充电/放电/待机的状态； 当前时间：显示系统时间（时分秒） 充/放电时长：点击按钮“充电”开始充电的累计时长（时分秒） 充/放电电功率：储能节点的实时充电功率； 充/放电电量：储能节点本次充/放电时长内的电能交易电量； 交易次数：储能节点本次充/放电时长内的电能交易次数；
基本信息	和 PC 端对应的储能系统页面一致
运行状态	和 PC 端对应的储能系统页面一致
运行统计	和 PC 端对应的储能系统页面一致
区块链交易	和 PC 端对应的储能系统页面一致
实时负载曲线	和 PC 端对应的储能系统页面一致

A.3 具体设计说明

Web 前端

采用 Vuejs 2.6.11 + Webpack 4.43 进行开发的单页应用，触摸大屏、手机端都在一个项目中，使用 Vuejs 单组件的 scoped 属性来隔离样式，样式预编译语言为 scss(sass)， JavaScript 为 ES5+，配合 babel 转译；代码格式检查使用 ESlint 及相应的 vuejs 插件、stylelint。部署时将打包文件上传至工控机/opt/fed/目录，由 Nginx 提供 http://console.energy.demo/ 的访问服务。

数据对接包含 WebSocket 和 Restful 接口的对接。其中 WebSocket 接口需要做好异常处理、自动重连。多图表页面需要考虑性能压力，使用 SVG 绘图、避免长时间阻塞渲染。

树莓派常驻服务

供需对接三方：与硬件开关/电表的串口通信、Hyperledger Fabric、MQTT 物联网中心服务。常驻服务是整个平台的数据来源、交易基础，因此要足够稳定。串口通信、电量上链、设备信息上传都需要按周期进行控制，树莓派性能允许的

前提下，尽可能缩小周期。

Hyperledger Fabric 链码

按照《能源互联网交易结算系统研发需求说明书》（附录 B）的实现，屏蔽其中禁用用户的功能，简化用户注册、激活的流程，添加链码升级相关代码。

Web 服务端

BaseController.go

基类用于全局功能,包含日志打印，错误处理，接口返回处理

APIController.go

提供 WebAPI 接口的具体功能，业务功能实现，web 端和移动端接口实现

TaskController.go

定时任务操作类,用于处理定时功能,定时推送数据给客户端,定时检查 MQTT 通信

DBController.go

数据库操作类，用于存储界面需要展示的历史数据

hardwareController.go

下发控制 Lot 设备的控制指令，其中包含指令的组合

MqttController.go

Mqtt 网络通信类用于发送和接收 MQTT 消息

MQTT/manager.go

MQTT 具体的实例化对象类

WebSocketController.go

提供 WebSocket 连接和发送功能，以及连接池的管理

Socket/chanroom.go

webSocker 具体的实例化对象类,用于配置和初始化

附录 B 《能源互联网交易结算系统研发成果报告》节选

目前，能源互联网是一种综合运用先进的电子技术、信息技术和智能管理技术，将大量由分布式能源采集装置、分布式能源存储装置和各种负载主体构成的各种类型的能源网络的能源节点互联起来，以实现能量双向流动的能量对等交换与共享网络。本软件使用 Fabric 框架结合 Golang 语言编写的智能合约，实现了一种基于区块链的能源互联网交易系统，系统实现了去中心化的点对点能源交易，同时利用异步结算的交易处理方法进行能源交易结算，不需要中心节点进行统一控制，提高了能源互联网上的业务执行效率。

本系统包含：

1、一条分布在各成员节点上的 Fabric 区块链；

2、一个中心化的管理服务，包含 Nodejs 服务和浏览器前端（B/S 模型）；

3、以及各个成员节点（能源路由器）上的 Fabric SDK 服务。

B.1 所需环境

成员节点：

操作系统：Linux（CentOS 7/Ubuntu 18.04）

CPU：双核 1.5GHz 及以上

内存：2GB RAM 及以上

存储：64GB 及以上

中心 Nodejs 服务：

操作系统：Linux（CentOS 7/Ubuntu 18.04）

CPU：双核 1.5GHz 及以上

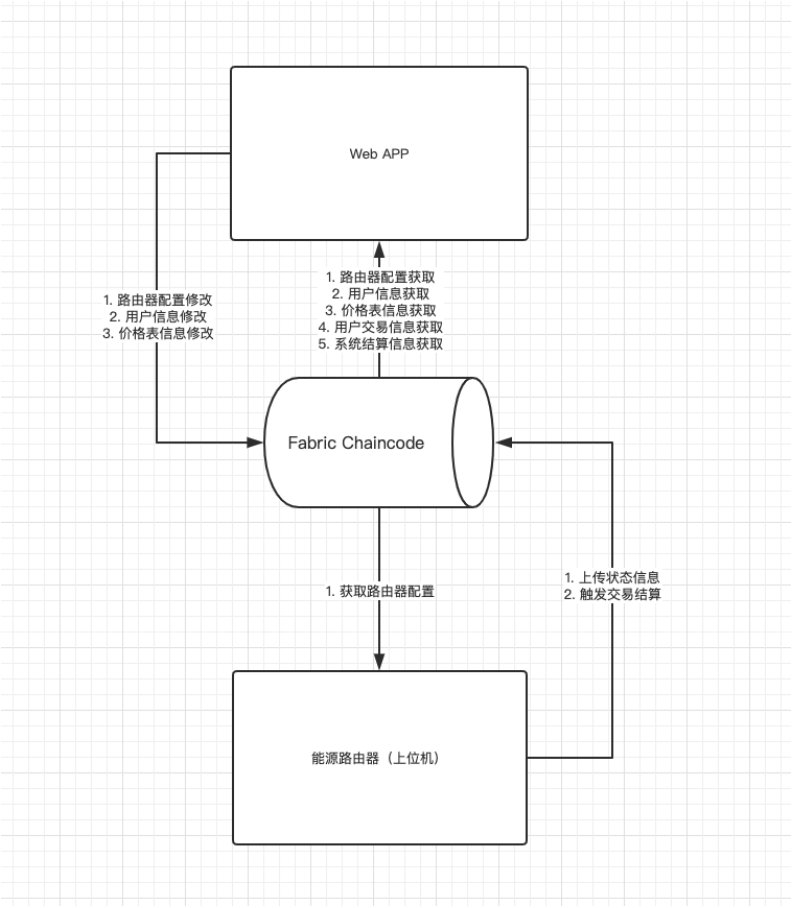
内存：4GB RAM 及以上

存储：100GB 及以上

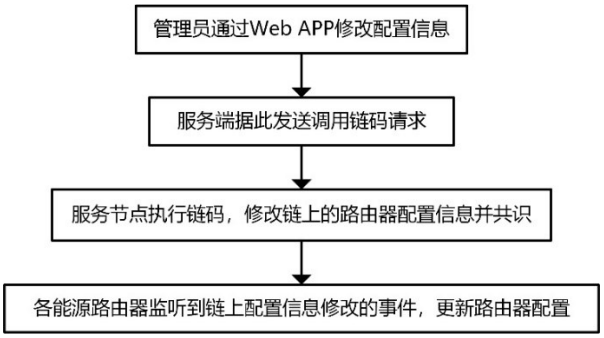
浏览器：PC 端 Firefox/Google Chrome/Safari/EDGE 等主流浏览器最近 3 个版本.

B.2 平台结构

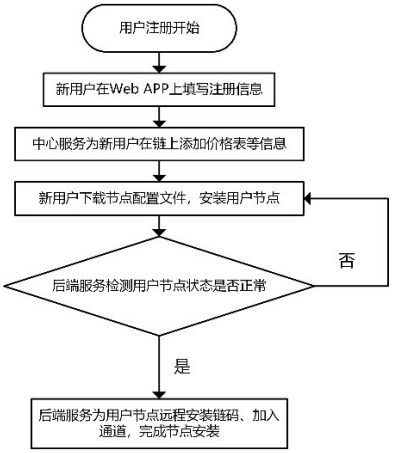
整体工作流程：



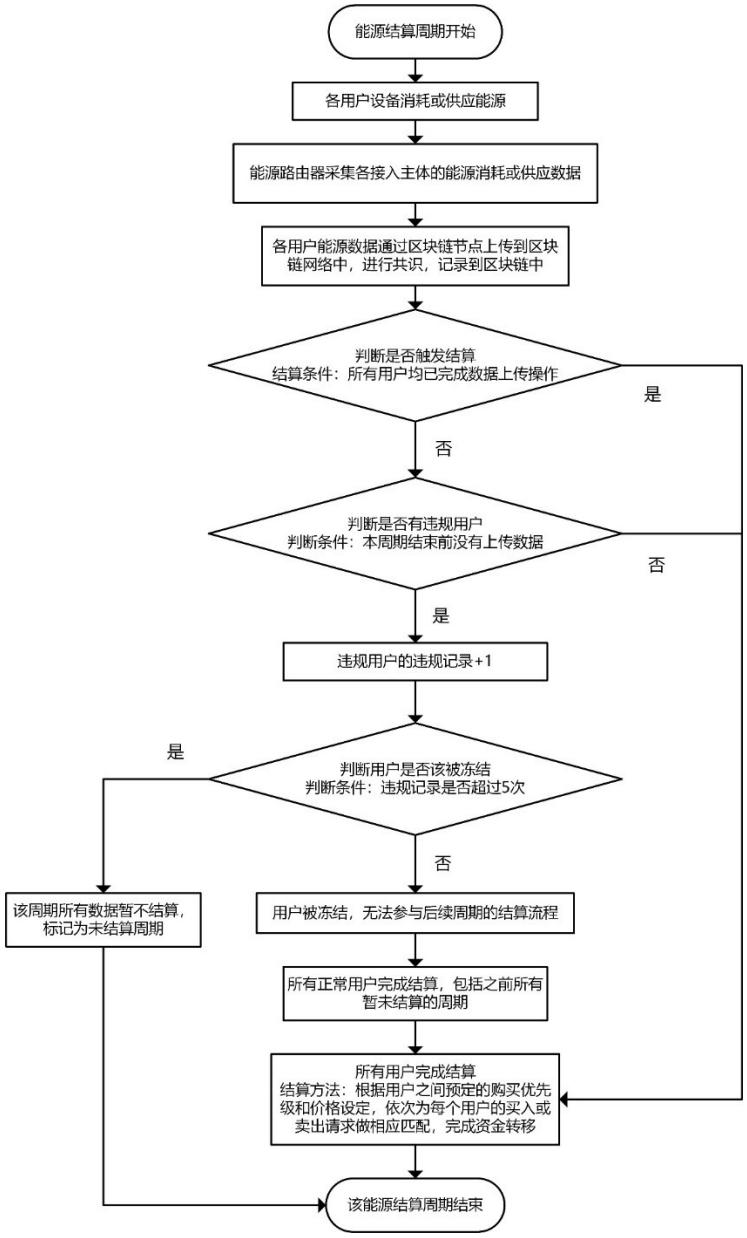
路由器配置修改-生效流程图：



用户注册流程图：


用户注册开始
新用户在Web APP上填写注册信息
中心服务为新用户在链上添加价格表等信息
新用户下载节点配置文件，安装用户节点
后端服务检测用户节点状态是否正常
否
是
后端服务为用户节点远程安装链码、加入通道，完成节点安装

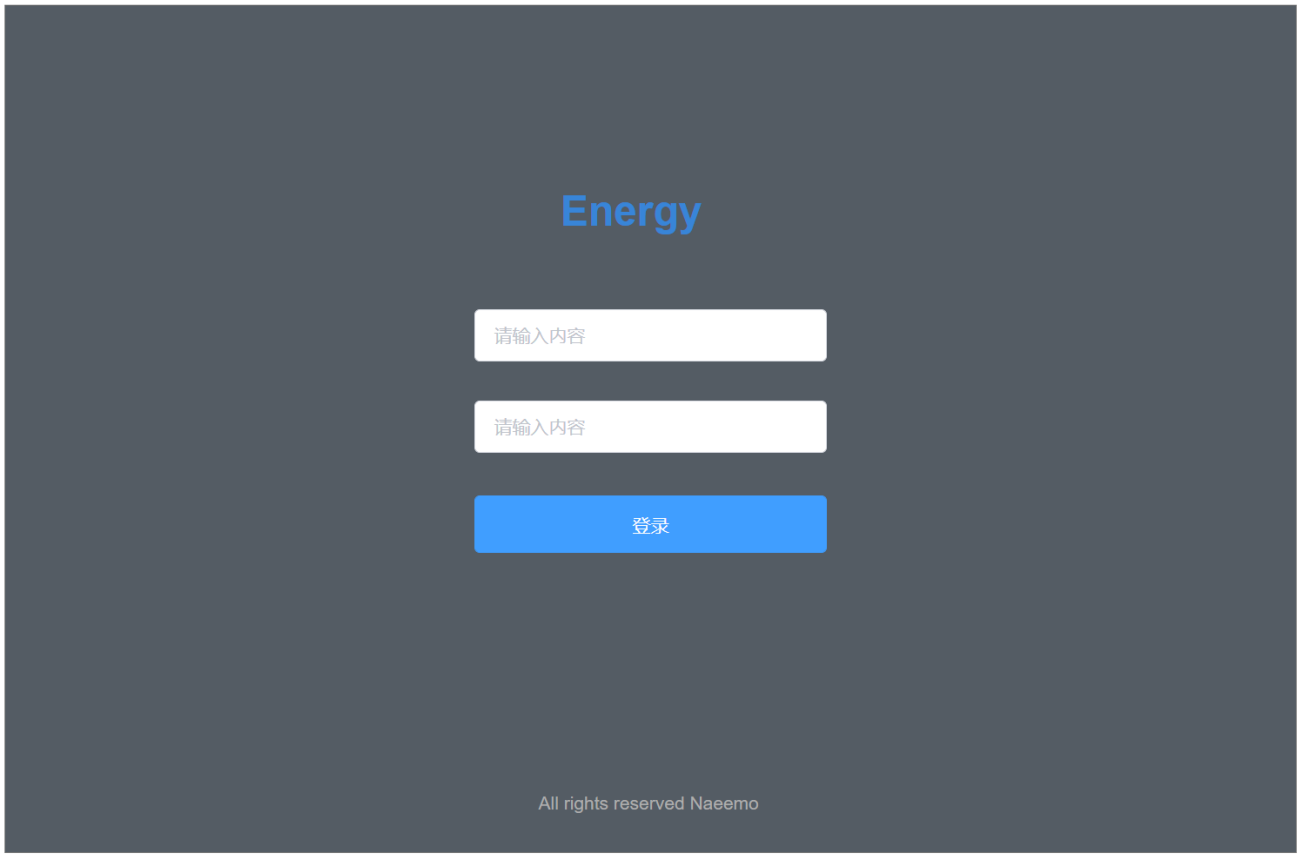
交易结算流程图：


能源结算周期开始
各用户设备消耗或供应能源
能源路由器采集各接入主体的能源消耗或供应数据
各用户能源数据通过区块链节点上传到区块链网络中，进行共识，记录到区块链中
判断是否触发结算
结算条件：所有用户均已完成数据上传操作
是
否
判断是否有违规用户
判断条件：本周期结束前没有上传数据
否
是
违规用户的违规记录+1
判断用户是否该被冻结
判断条件：违规记录是否超过5次
是
否
该周期所有数据暂不结算，标记为未结算周期
用户被冻结，无法参与后续周期的结算流程
所有正常用户完成结算，包括之前所有暂未结算的周期
所有用户完成结算
结算方法：根据用户之间预定的购买优先级和价格设定，依次为每个用户的买入或卖出请求做相应匹配，完成资金转移
该能源结算周期结束

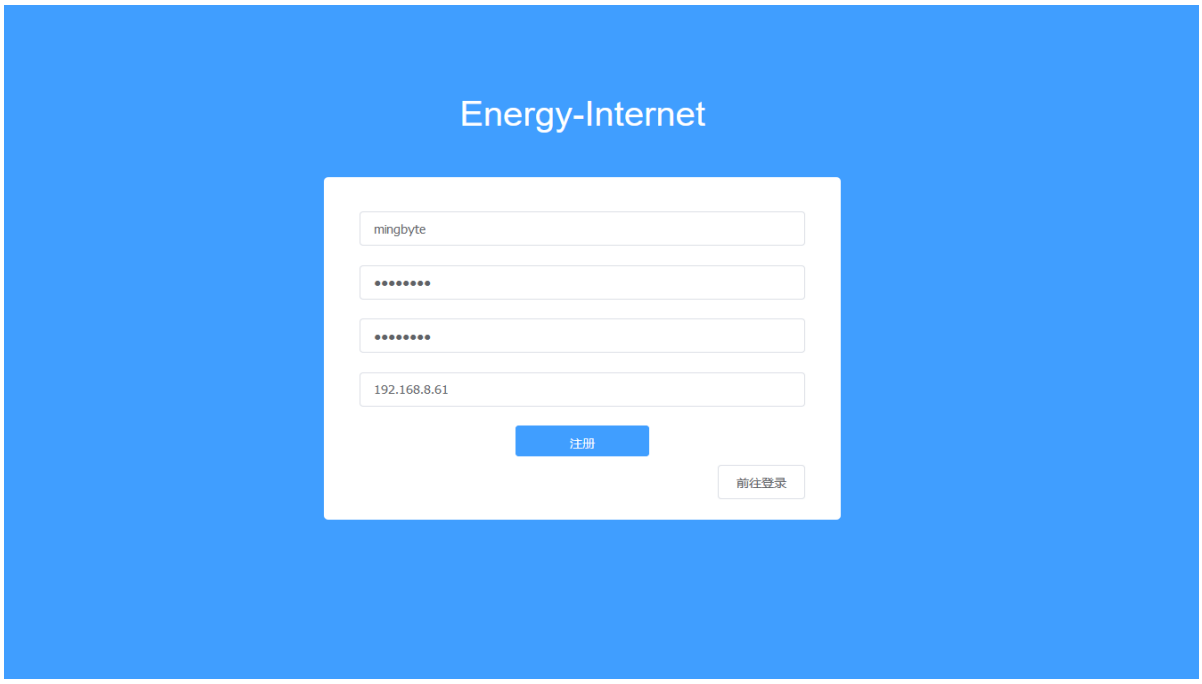
B.3 软件研发内容详述

B.3.1 界面设计

登陆页：

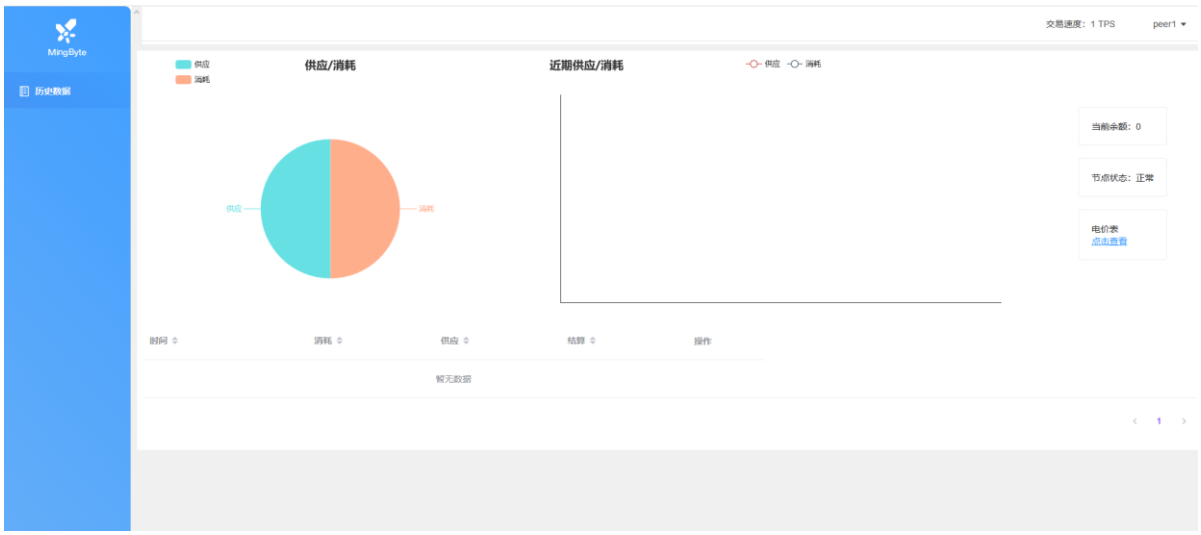


注册页：


Energy-Internet
mingbyte
192.168.8.61
注册
前往登录


注册成功，下载文件配置网络
节点名称：peer1
点击检测
下载
请先下载配置文件进行配置，再进行节点检测，此过程会耗费一定时间，请耐心等待。

用户数据页：

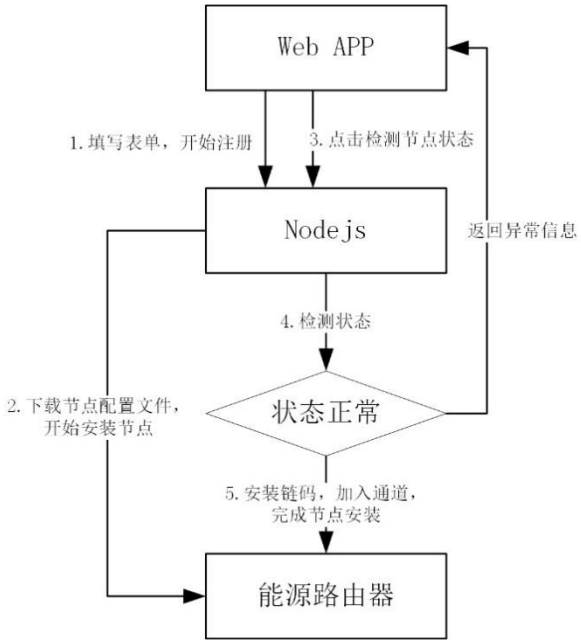


B.3.2 功能模块列表

模块	包含功能
用户操作管理模块	用户注册、登录、列表查看、详情查看、修改、下载部署配置，管理用户资金
能量路由器模块	远程配置、检测在线状态、上传计量数据，
区块链节点模块	用户交易记录、系统交易记录、交易结算等特定数据传输通信，并且依据共识机制完成数据上链。
智能合约模块	提供各种功能的智能合约，处理智能合约调用请求，

模块	包含功能
智能合约管理模块	远程升级、部署智能合约

用户操作管理模块用于依据普通用户注册信息完成区块链节点身份认证注册和管理用户资以及提供各种用户操作功能，新用户注册流程如下图所示；

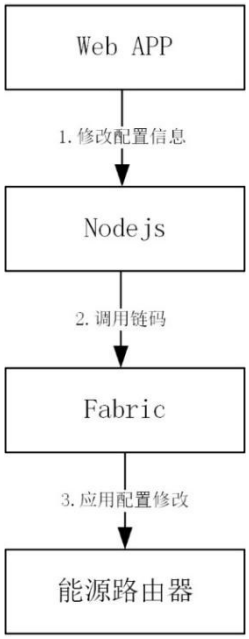


智能合约模块用于为各个模块提供相应功能的智能合约，处理各个模块的智能合约调用请求，智能合约功能简介如下表所示；

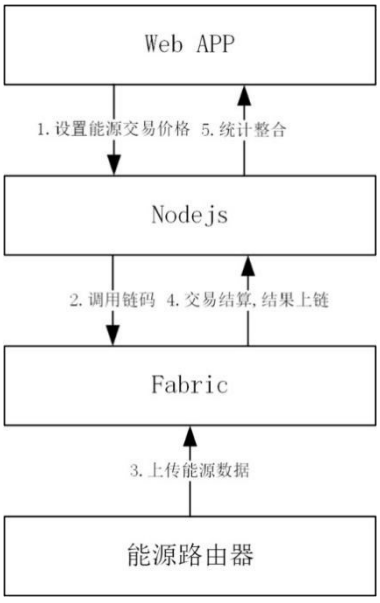
合约名称	合约功能	合约调用对象
用户注册合约	完成新用户的注册以及区块链节点的分配	用户操作管理模块
数据上链合约	完成区块链交易信息中能源数据的共识上链存储	区块链节点模块
交易结算合约	完成能源数据的周期性结算	区块链节点模块

资金管理合约	完成用户供耗电结算之后的资金转账	区块链节点模块
违规处罚合约	完成对违法用户的惩罚	区块链节点模块

能量路由器模块用于远程配置能量路由器，依靠能量路由器采集能源接入主体的供耗电数据，并整理成区块链交易传输到区块链网络节点，能量路由器配置修改-生效流程下图所示：



交易结算流程如下图所示：



链码管理模块用于为用户对应的区块链节点与区块链网络进行特定数据传

输通信，并且依据共识机制完成数据上链。

B.3.3 任务拆分：

链码：

接口	方法名	所属模块	指标、关键点
创建新用户	createUser	用户	
获取用户	getUser	用户	
批量获取用户	getUsers	用户	
用户充值	rechargeUser	用户	
激活用户	activateUser	用户	
获取用户最近 10 条状态	getUserRecentStates	用户、交易	
新增一个供应节点（注册用户之后）	addSupplier	用户、交易	
获取某用户的供应信息	getUserSuppliers	用户、交易	
设置用户供应信息	updateUserSuppliers	用户、交易	
获取所有用户的供应列表	getAllSuppliers	用户、交易	
分页读取用户交易记录	getUserTransactions	交易	Fabric 状态数据库 CouchDB 对分页查询支持有限，复杂查询可能不支持。
触发交易结算	settleTransaction	交易	

统计系统状态（总供应/消耗）	sumUsers	交易	总供应/消耗不在链上直接存储，由该时刻所有用户各自的供应/消耗累加求得。
上传设备状态，准备交易数据	uploadRouterState	交易、能源路由器	
读取路由器的配置参数	getRouterConfig	能源路由器	
设置路由器的配置参数	setRouterConfig	能源路由器	路由器可配置参数可能很多。

中心服务 Nodejs 接口：

接口	方法名	所属模块	指标、关键点
登录	controller.user.login	用户	
判断用户名是否已经注册	controller.user.isUserExist	用户	用户名唯一
注册	controller.user.register	用户	
打包下载用户节点部署所需文件	controller.user.downloadCredentials	用户	
用户列表	controller.user.getUsers	用户	
用户详情	controller.user.getUser	用户	
修改用户	controller.user.editUser	用户、交易	充值
用户最近状态	controller.user.getRecentStates	用户、交易	时间倒序
获取用户电价表	controller.user.getUserPrice	用户、交易	

修改用户电价表	controller.user.setUserPrice	用户、交易	
获取总电价表	controller.user.getPriceAll	用户、交易	
用户交易记录	controller.user.getTransactions	交易	
系统最近信息记录	controller.system.recent	交易	时间倒序
系统信息记录	controller.system.getStates	交易	分页、时间倒序
系统当前状态	controller.system.status	交易	展示系统状态信息（交易速度等）
获取能源路由器的配置	controller.router.getConfigs	能源路由器	Fabric 节点能否响应测试请求
修改能源路由器的配置	controller.router.setConfigs	能源路由器	
检测路由节点是否正常在线	controller.router.isPeerReady	能源路由器	
链码列表	controller.contract.getContracts	链码管理	
新增链码	controller.contract.createContract	链码管理	
删除链码	controller.contract.deleteContract	链码管理	
启用链码	controller.contract.installContract	链码管理	

中心服务前端：

页面	功能	所属模块	指标、关键点
登录	用户登录	用户	
注册	用户注册，引导下载	用户	注册交互细节：注册后引导用户下载配置进行

	配置文件		安装；下载配置后安装节点后，使用检测接口进行状态检测；检测成功后进入用户首页。
用户列表	用户列表分页展示	用户	
用户首页	用户总供应/消耗饼图、最近供应/消耗折线图，余额，用户节点状态，价格表查看，用户交易记录分页展示	用户、交易、能源路由器	
首页	系统供应/消耗折线图，供应/消耗历史记录	交易	区块链上不记录一些统计结果，只记录原始数据，减少数据冗余，也能避免因计算错误等导致的数据冲突。Single source of truth.
电价及优先级配置页	修改各个交易节点之间结算的优先级和电价	交易	以买入方为主体，设置一个供应列表。列表中各供应方按优先级排序并设定供应价格。
链码管理页	管理区块链网络中运行的智能合约	交易	1. 同一时刻只能运行一个版本的链码； 2. 链码启用后，该链码进入“正在安装”状态，此时不可以启用其他链码； 3. 不在运行，且不在安装状态的链码可以删除； 4. 版本号遵守语义化版本规范，且版本名不能重复； 5. 链码包文件最大支持 20MB，后缀名为 .pak
路由器配置页	路由器远程设置：路由器上传及结算周期	交易、能源路由器	实际上，由于结算结果必须要等待 Fabric 出块才能确认，所以最小周期就是 Fabric 出块的时间。

设备端 SDK：

功能		所属模块	指标、关键点
读取计量数据	与能源路由器通信，获取计量数据	能源路由器	配合硬件设备的需求
响应远程配置变更	监听区块链上对设备配置项的变动，并按照最新配置调节自身行为	能源路由器	配置变更不能影响正常的数据收集和上传
上传计量数据	某周期内计量数据上传完毕，发起结算	能源路由器、交易	定时串行上传数据
触发周期结算	某周期内计量数据上传完毕，发起结算	能源路由器、交易	触发结算与上传数据异步执行

B.3.4 功能模块详述

模块		详述
用户操作管理模块	注册	通过公网域名部署的前端访问注册页面，注册成功之后下载节点安装配置文件压缩包，并复制到能量路由器中，进行解压安装；
		安装成功之后，进入系统登录页面进行登入，登入成功进入检测页面，点击“点击检测”进行智能合约远程安装、状态检测环节。
		智能合约远程安装、检测成功之后，自动返回到用户首页。
	登录	管理员账户登录之后，跳转系统首页；
		普通用户登录后，如其节点状态正常则跳转用户首页，否则跳转检测页面；
	用户列表	分页表格展示系统内所有普通用户，每页默认 20 条数据，按入网时间倒序排列；
		数据列包括：用户名、节点状态、余额、供应价（每千瓦时）、入网时间、总消耗、总供应；
		针对每行数据（即每个用户）提供查看历史数据的操作，点击历史数据跳转到该用户的用户首页；

	用户首页（用户历史数据页）	饼图展示当前用户总消耗/供应，折线图展示当前用户最近的消耗供应变化；
		展示用户的余额、用户节点状态、供应电价；
		当前用户即为登录用户时，供应价提供修改操作，点击修改弹出确认输入框进行修改；
		分页表格展示用户的交易记录，默认每页 20 条数据，按时间倒序排列；每条交易数据提供“消耗明细”的操作，点击“消耗明细”弹出该次交易的供需细节；
能量路由器模块		管理员进入路由器配置页，可以修改“路由器更新间隔”，点击保存按钮确认操作；
		能量路由器上监听到配置发生变化时，需根据最新的配置调整自己的行为；期间不能影响正常的计量数据收集及上传；
区块链节点模块		能量路由器上的 Fabric SDK 服务按照设定的“路由器更新间隔”定时上传计量数据，计量数据来自于硬件通信；
		上传的数据中包含：用户 ID、时间、上次上传至今的供应电量、消耗列表（记录上次上传至今，消耗了哪些用户的电能，各消耗多少）；
		链码接收到计量数据后，按照计量数据中供需细节进行结算并进入共识-出块流程；成功出块且交易标记有效后，完成一次结算。
智能合约模块		为各个模块提供相应功能的智能合约，处理各个节点的智能合约调用请求，智能合约包括用户注册合约、数据上链合约、异步结算合约、资金管理合约、违规处罚合约；
		用户注册合约供用户管理模块调用完成新用户的注册以及区块链节点的分配； 数据上链合约供区块链节点模块调用完成区块链交易信息中能源数据的共识上链存储； 异步结算合约供区块链节点模块调用完成能源数据的周期性结算；资金管理合约供区块链节点模块调用完成用户供耗电结算之后的资金转账； 违规处罚合约供区块链节点模块调用完成对违法用户的惩罚；
智能合约管理模块		用于对新版本智能合约进行远程升级、部署，新版本智能合约指的是根据用户需求在现用智能合约的基础上开发的功能更强大的智能合约；
		智能合约远程升级部署指的是在用户同意的情况下，系统管理员节点对普通用户节点的智能合约进行远程升级部署；