

能源系统中的区块链：概念、应用与展望

颜拥^{1,2,3}, 赵俊华⁴, 文福拴^{5,6}, 陈星莺^{1,2}

(1. 河海大学能源与电气学院, 南京市 211100;

2. 江苏省配用电与能效工程技术研究中心, 南京市 211100;

3. 国网浙江省电力公司电力科学研究院, 杭州市 310009;

4. 香港中文大学(深圳)理工学院, 广东省深圳市 518100;

5. 浙江大学电气工程学院, 杭州市 310027;

6. 文莱科技大学电机与电子工程系, 文莱斯里巴加湾 BE1410)

摘要:互联网作为第三次工业革命的代表性技术改变了现代社会的生活方式和经济发展模式,而以去中心化和信任机制为主要特征的区块链技术作为新一代互联网技术的重要组成部分,很有可能推动现有计算模式的变革,在金融、能源等诸多领域将产生广泛而深远的影响。首先对区块链进行了概述,给出了区块链的定义和技术框架,阐述了区块链的特点和意义;之后,介绍了区块链在一些领域的应用情况;最后,概述了区块链在能源系统领域的研究现状,并对能源区块链的研究做了展望。

关键词:区块链;去中心化;信任机制;能源系统;能源区块链

Blockchain in Energy Systems: Concept, Application and Prospect

YAN Yong^{1,2,3}, ZHAO Junhua⁴, WEN Fushuan^{5,6}, CHEN Xingying^{1,2}

(1. College of Energy and Electrical Engineering, Hohai University, Nanjing 211100, China;

2. Jiangsu Engineering Research Center for Distribution, Utilization and Energy Efficiency, Nanjing 211100, China;

3. Electric Power Research Institute of State Grid Zhejiang Electric Power Company, Hangzhou 310009, China;

4. School of Science and Engineering, Chinese University of Hong Kong (Shenzhen),
Shenzhen 518100, Guangdong Province, China;

5. School of Electrical Engineering, Zhejiang University, Hangzhou 310027, China;

6. Department of Electrical & Electronic Engineering, Universiti Teknologi Brunei, Bandar Seri Begawan BE1410, Brunei)

ABSTRACT: As a representative technology of the Third Industrial Revolution, the Internet has changed the way of life and economic development in modern society. The blockchain technology, which is characterized by decentralization and trust mechanism, is an important part of the new generation of Internet technology. The blockchain may promote the transformation of the existing computing paradigm, and have far-reaching impacts in finance, energy and many other areas. This paper first gives an overview of the blockchain, discusses its definition and technical framework, and expounds its characteristics and significance. After that, the applications of the blockchain in some fields are introduced. At last, the research status of blockchain in energy systems is summarized, and potential research problems in energy blockchain are prospected.

KEYWORDS: blockchain; decentralization; trust mechanism; energy system; energy blockchain

中图分类号:TM 71;TP 399

文献标志码: A

文章编号: 1000-7229(2017)02-0012-09

DOI: 10.3969/j.issn.1000-7229.2017.02.002

基金项目:国家重点基础研究发展计划项目(973计划)(2013CB228202);国家自然科学基金项目(51477151)

Project supported by National Basic Research Program of China (973 Program) (2013CB228202); National Natural Science Foundation of China (51477151)

0 引言

美国著名学者杰里米·里夫金在其著作《第三次工业革命》^[1]一书中首先提出了“能源互联网”(Energy Internet)的概念和愿景,在国内外引起了广泛关注。文献[2]给出了能源互联网的初步定义:能源互联网是以电力系统为核心,以互联网及其他前沿信息技术为基础,以分布式可再生能源为主要一次能源,与天然气网络、交通网络等其他系统紧密耦合而形成的闭环运行的复杂多网流系统。能源互联网将改变传统的电、热、冷、气等能源“平行流动”的状况,实现在生产、输送、存储、消费等各个环节的耦合,使得不同形式能源在诸多环节可相互转化,实现多流网络的协同运行。能源互联网不仅可在工业系统中应用,也可在居民区甚至家庭内实施^[3-4]。到目前为止,对能源互联网的研究总体上尚处于理论研究和架构设计层面,真正运行的能源互联网尚很鲜见。

能源互联网可实现能量与信息的高效传递,但能源行业的价值链并没有打通,源、网、荷、储等多个环节还未能深度融合,各个环节之间的交易存在广泛的摩擦。随着能源互联网中的分布式电源、储能、电动汽车、电转气等设备的快速发展,能源消费者可能同时成为生产者,参与者的身份逐渐多元化。能源互联网因参与主体多,系统复杂性强,以及身份的模糊性、资源的多样性及分布性等特性,导致能量流、信息流、资金流的流向复杂,在能量流动和价值流动过程中交易管理等成本大大增加。以电力市场环境下的电力调度为例,调度中心一直被人诟病采用的调度方式不公平、不透明;事实上,即使调度是公平的,外界也不会相信,这种信任问题是中心化调度方式所导致的。如何适当监督调度机构并要求其披露相关信息给市场参与者,以便让参与者信任调度中心,是一个相当困难的问题。能源互联网可以实现能量与信息的高效传递,但参与主体之间存在的信任问题会给交易带来很高的附加成本。

2015年10月31日《经济学人》刊发了一篇题为“*The promise of the blockchain: the trust machine*”的封面文章^[5],认为区块链(blockchain)技术具有改变人与人合作模式和商业合作模式的巨大潜力,是“创造信任”的技术。这篇文章的发表使得区块链技术开始受到广泛关注(如图1所示)。区块链基于密码学原理解决交易过程的所有权确认问题,保证交易系统对价值交换活动的记录、传输、存储结果都是可信的。区块链记录的信息一旦生成将永久记录,且无法篡改。区块链被认为是继大型计算机、个人电脑、互联

网、移动/社交网络之后计算范式的第5次颠覆式创新,是人类信用进化史上继血亲信用、贵金属信用、央行货币信用之后的第4个里程碑。

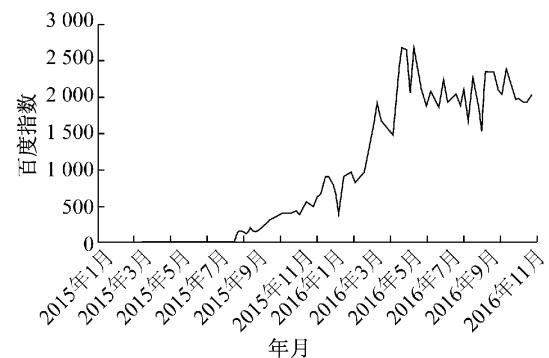


图1 “区块链”百度指数图
Fig. 1 Baidu index on the topic “blockchain”

区块链技术属于分布式存储技术,数据保存在网络中的每个节点,由所有节点共同维护,难以篡改,这样就能够有效解决交易双方间的信任问题。针对能源互联网的特征,对区块链技术进行重构与二次开发,是解决能源互联网中参与者间信任问题的有效途径。

区块链是一个很新的概念,尚不存在公认的定义,其所包括的研究和技术内容与范围还没有清楚的界定,理论和应用研究都在快速发展之中。在此背景下,本文首先介绍区块链的定义、意义及其发展历程;之后,概述区块链技术的应用现状,着重介绍其在能源行业的应用潜力;最后,对区块链技术在能源互联网中的应用前景进行展望。

1 区块链概述

区块链技术源于比特币,系比特币的底层技术;比特币也是区块链技术最早的应用对象。在2008年全球金融危机爆发后,一位自称中本聪(Satoshi Nakamoto)(其真实身份至今不明)的人发表了一篇题为“*Bitcoin: a peer-to-peer electronic cash system*”^[6]的论文。

2009年1月4日,比特币正式诞生。不过,因其投机风险过大,且易被用于贩毒、走私、洗钱等非法活动,中国人民银行联合工信部、银监会、证监会和保监会于2013年12月5日印发了《关于防范比特币风险的通知》,要求金融机构和支付机构不得开展比特币相关业务,比特币在国内遭到封杀。国际上对比特币虽然有较大争议,但隐藏在比特币背后的区块链技术却逐步获得广泛认可。IBM和Intel等几十家国际科技巨头参与了超级账本项目(Hyperledger Project),

其中的核心就是区块链技术;万达集团已加入该项目并成为第一个来自中国的董事会核心成员。区块链联盟R3则致力于采用区块链技术解决跨境银行支付、交易和结算成本高的问题,已有近50家正式成员,其中包括花旗、摩根大通、高盛等银行业巨头,中国平安和香港友邦也已加入(近期高盛等部分成员退出该联盟,独自开展区块链技术研究)^[7]。国内网络科技巨头如百度、阿里巴巴、腾讯(BAT)等都已经对区块链技术进行了战略布局。百度投资区块链支付应用公司Circle;阿里巴巴旗下的蚂蚁金服宣布开发基于区块链技术的支付宝爱心捐赠平台;腾讯旗下的微众银行加入金融区块链合作联盟。至此,国内外多个著名的互联网科技与银行巨头已实际参与或密切关注区块链技术研究。

2016年1月20日中国人民银行数字货币研讨会在北京召开,行长周小川要求进一步明确央行发行数字货币的战略目标,做好关键技术攻关,研究数字货币的多场景应用,争取早日推出央行发行的数字货币^[8]。央行数字货币研究所已于2016年12月正式成立,并已取得阶段性成果,原型方案已初步确定,法定数字货币的原型系统有望在2017年春节后推出^[9]。2016年12月,国务院印发的《“十三五”国家信息化规划》中包括了区块链技术^[10]。在数字货币的即将推出和十三五规划政策助力的背景下,区块链技术有望得到快速发展和应用。

2016年12月28日,在公安部、工信部、中国科学院等相关部门的大力支持下,“首届中国区块链技术创新应用大赛”由中关村区块链产业联盟主办,国网浙江省电力公司电力科学研究院、微软(中国)有限公司、IBM(中国)有限公司等单位协办,共同为国内外广大区块链研发人员提供了交流与展示平台,旨在推动区块链技术的创新与应用,引起巨大反响^[11]。

2 区块链的定义和技术框架

2.1 区块链定义

虽然区块链技术在2016年受到了非常广泛的关注,但到目前为止尚没有公认的定义。美国学者Melanie Swan在其《区块链:新经济蓝图及导读》一书^[12]中给出了区块链的定义:区块链技术是一种公开透明的、去中心化的数据库。这个定义强调了区块链的2个特点,但过于笼统。在工信部发布的《中国区块链技术和应用发展白皮书(2016)》^[13]中,区块链被定位为分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式。工信部的这个定义

点出了所涉及到的关键技术,但未说明这些关键技术之间的关系。文献[14]认为区块链技术是利用加密链式区块结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用自动化脚本代码(智能合约)来编程和操作数据的一种全新的去中心化基础架构与分布式计算范式。该定义明确了区块链技术是由加密算法、共识机制等关键技术有机组合而成的一种去中心化的技术框架,相对比较全面。

区块链本质上是一个数据库,主要通过安全散列算法(secure hash algorithm, SHA)、非对称加密等密码学原理、共识机制等一系列技术巧妙配合所形成的技术集合。笔者尝试在文献[14]的基础上给出如下定义:区块链技术是基于时间戳的“区块+链式”数据结构、利用分布式节点共识算法来添加和更新数据、利用密码学方法保证数据传输和访问的安全、利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新分布式基础架构与计算范式。

2.2 区块链技术框架

区块链的核心技术框架主要包括数据层、网络层、共识层、激励层、合约层和应用层(见图2),对于不同的项目和平台,细节方面也有所不同。文献[14]给出了比较详细的技术细节。



图2 区块链技术框架图
Fig. 2 Technical framework of the blockchain technology

(1)数据层。“区块链”这个词本身包含了“数据区块+链”的含义,即由数据区块和链式结构组成。通过对数据区块打上时间戳后,可以对数据进行标记,形成数据区块链条,从而记录区块链数据的完整历史,能够提供区块链数据的溯源和定位功能,任意数据都可以通过此链式结构追本溯源。采用哈希函数(Hash function)将原始数据编码为特定长度的由数字和字母组成的字符串,具有单向性(从哈希函数的输出几乎不能反推输入值)、定时性(不同长度输入的哈希过程所消耗的时间基本相同)、随机性(即使输入仅相差一个字节也会产生截然不同的输出值)

等优点,可用于数据存储、验证等。非对称加密通常在加密和解密过程中使用2个非对称的密钥(分别为公钥和私钥),用其中一个密钥(公钥或私钥)加密信息后,只有另一个对应的密钥才能解开,这主要用于对信息加密、数字签名和登录认证等。Merkle树是区块链的重要数据结构,用于快速归纳和校验区块数据的存在性和完整性。从数据存储角度看,区块链没有本地数据库,有点类似于云存储,但云存储通常由某一中心化机构提供,而区块链则采用去中心化的分布式存储。

(2) 网络层。网络层主要包含P2P网络技术(又称为点对点传输技术或对等互联网络技术)、传播机制和验证机制。现有的区块链项目几乎都采用了著名的P2P技术,电驴、迅雷、BT下载等软件也均采用了P2P技术。当数据在服务器上集中式存储时,下载的人越多,服务器承载的压力就越大,下载速度就越慢。采用P2P技术时,在下载一个文件的同时,也不断将数据传输给别人,每个节点既是下载者也是服务器,使得资源的分享不再依赖于中央服务器。下载的节点越多,下载数据越快。

(3) 共识层。共识层主要包含共识机制,即能够在决策权高度分散的去中心化系统中使得各节点高效地针对区块数据的有效性达成共识,这是区块链核心技术之一。共识问题是分布式计算领域的重要研究问题,著名的“拜占庭将军问题”(Byzantine failures)抽象地反映了分布式计算所遇到的问题。早期的比特币区块链采用高度依赖节点算力的工作量证明(proof of work, PoW)机制来保证比特币网络分布式记账的一致性。随着区块链技术的发展,权益证明机制(proof of stake, PoS)和授权股份证明机制(delegated proof of stake, DPoS)等共识机制相继出现。

(4) 激励层。区块链需要大量参与者提供算力来支撑运算,因此就需要设计激励机制来吸引参与者贡献算力。比特币中的区块链采用了“挖矿”机制,激励参与者不断提供算力来获得奖励。虽然这些算力目前尚未用于解决实际问题,预期在不久的将来就会得到实际应用。

(5) 智能合约。区块链技术可提供灵活的脚本代码系统,支持用户创建高级的智能合约、货币或其他去中心化应用。智能合约的代码是透明的,对去中心化系统而言具有重要意义,因为对用户来讲,只要能够接入到区块链中,用户就可以看到编译后的智能合约,从而对代码进行检查和审计。在中心化系统中,智能合约对用户而言就是一段不可见的代码,类

似于黑匣子。智能合约的运作机制如图3所示,可见其和中心化系统中常见的自动控制原理极其类似,均是在满足给定触发条件时进行响应。当某个复杂事件需要多方参与才能执行时,自动控制就是一种智能合约。从某种意义上讲,智能合约就是一种广义的自动控制;中心化系统中的自动控制也可视作一种特殊的智能合约。因此,去中心化是采用区块链的前提。对于中心化系统而言,并不需要采用区块链。



图3 智能合约的运作机制
Fig. 3 Operation mechanism of a smart contract

3 区块链的特点和意义

3.1 区块链的特点

区块链采用密码学、区块链式结构、共识算法等一系列技术组合,具有去中心化、可追溯、集体维护、可编程和安全可信等特点。

(1) 去中心化。区块链数据的验证、记账、存储、维护和传输等过程均是基于分布式系统结构,采用纯数学方法而非中心机构来建立分布式节点间的信任关系,从而形成去中心化的可信任的分布式系统。需要指出,分布式和去中心化是不同的概念。实际上,分布式也可以是中心化的,比如同一家公司的多个异地机房;集中式也可以是去中心化的,例如要求所有选民到同一地方进行全民公投。图4给出了中心化和去中心化示意图。

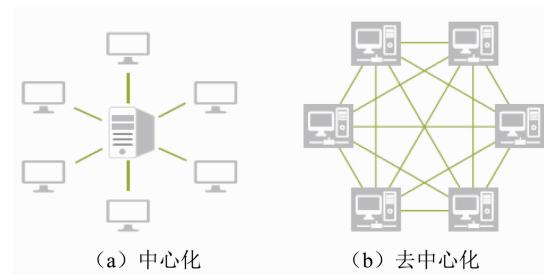


图4 中心化和去中心化示意图
Fig. 4 Illustrations of centralization and decentralization

(2) 开放透明。区块链系统的开放和数据透明是其赢得信任的基础。除了账户隐私信息被加密外,其他数据都是对所有人或者参与者公开的,可以通过公开接口查询数据记录,信息高度透明。大量的区块

链程序是开源的,数据和规则在全网所有节点均可查询。

(3)安全可信。区块链的安全性包含数据安全性和系统安全性2个方面。区块链技术采用非对称密码学原理对数据进行加密,利用共识算法形成的强大算力来抵御外部攻击、保证区块链数据不可篡改和不可伪造,因而具有较高的数据安全性。区块链采用了链式结构和时间戳,所有数据都有先后顺序和时间标记,区块链采用共识机制来实现竞争性数据的读写权,系统管理员并不掌握数据的读写权、无法像对普通数据库那样随意插入或删除,因此通常认为区块链的数据是不可篡改的。如果需要对数据进行修订,只能通过增加数据备注的方式进行操作,但所有操作都被记录在区块链数据库中,只是最终展现的是更新后的数据。以比特币区块链为例,只有控制了51%的计算能力才有可能实施数据篡改,但比特币区块链的算力非常惊人,要进行数据篡改的成本远大于可能获得的收益,这样参与者试图篡改数据的概率极低,因此区块链中的数据是安全的。如果某个节点遇到网络问题、硬件故障、软件错误或者被黑客控制,不会影响其他节点和整个系统。问题节点在排除故障并完成数据同步之后,便可随时再加入到系统中继续工作。所以,每个节点可以选择地下线,进行例行维护,同时还能保证整个系统的不间断工作。微软、谷歌、阿里巴巴等全球著名的互联网公司也曾多次出现宕机事件,但比特币系统运行8年还未出现过宕机。目前,比特币的市值已超过150亿\$,单价在1 000\$左右,系统曾被无数世界顶尖黑客攻击却固若金汤,因此可以说区块链技术创造了人类历史上最稳定、最安全的计算机系统。

3.2 区块链的意义

区块链技术是密码学、计算机科学、经济学等多个学科发展到一定阶段后的产物,有效融合了多个学科的杰出成果。区块链技术的出现为解决人类社会的信任问题提供了有力工具,进而将人类社会带入群智时代。

(1)创造信任。区块链系统本身能产生信用,这种具有信用的产品不是来自第三方,而是来自程序(算法),因为区块链记录信息的产生需要全网络节点确认,而一旦生成将永久记录,无法篡改。互联网的底层协议是TCP/IP协议,实现了信息的低成本高效率传播;区块链可认为是一种新的底层技术,建立了新的信用体系。区块链取代了目前互联网对中心服务器的依赖,使所有数据信息都被记录在一个云系统之上,理论上实现了数据传输中的数据自我证明,

从深远意义上讲,这超越了传统和常规意义上需要依赖第三方的信息验证模式,降低了建立全球信用体系的成本。总之,区块链解决了信任问题。

(2)群智时代。在区块链出现之前,大规模多边协作通常由共同的信任中心对整个组织进行协调;信任中心要么是多个主体共同的“上级”机构,要么是共同组建的一个第三方机构,而该机构往往能够成为各参与方的实际权力中心,因此传统的大型规模协作方式都是以中心化机构为基础。中心化机构一定会伴随着较高的人为决策风险,受制于人的教育背景、经历、个性特征等因素,因而经常出现中心化机构无法驾驭大规模协作的情形。区块链提供了激励机制,参与者在作出贡献的同时能够获得回报,这样就调动了参与者的积极性。

区块链以对等方式把参与方连接起来,由参与方共同维护一个系统,通过共识机制和智能合约来表达协作规则,实现更有弹性的协作方式。因为参与方职责明确,不用向第三方机构让出权力,无须维护第三方信任机构的成本,有利于各方更好地开展协作。因为解决了信任问题,采用区块链有望实现低成本、高效率的全新协作模式,形成更大范围、更低成本的新协同机制。

区块链采用群体智慧、互联网思维实现。群体智慧采用简单规则将个体联系起来,每个个体看似微不足道,但汇聚起来的智慧和力量却无比强大,往往强大到能够超越种群自身智力或体系结构上的限制,整个系统运行看似混乱却保持着惊人的和谐。在虚拟数字世界中,“机器的智慧”体现在计算能力上。在区块链中,针对每个节点采用了独特的集体竞争式计算,即不断生成随机字符串直到获得正确答案,最终单个节点的计算能力得以汇聚成系统的超强计算能力。在2016年,比特币的区块链已经达到每s进行 8×10^{18} 次运算的能力。区块链的计算能力约为世界上最快的单台计算机的计算能力的28 000倍。区块链的集体式计算从技术上实现了群体智慧,由个体汇聚而成的“超级计算系统”的计算能力超越了个体的限制^[15]。

4 区块链的应用现状

区块链最早应用在数字货币中,比特币就是最初的形态,这就是所谓的区块链1.0。后来出现了智能合约,其中定义一些触发条款,条款满足时自动执行合约,扩大了区块链的应用空间,为区块链的快速发展奠定了基础,这就是区块链2.0。当区块链除了在货币、金融、市场中应用外,逐步拓展到政府、健康、科

学、文化和艺术方面后,从各方面改变了我们的社会和生活,这就成为区块链3.0。下面概述区块链在共享经济、支付、物联网等几个方面的典型应用^[15]。

4.1 真正的共享经济

共享经济是运用信息技术为个人、企业、非营利组织和政府提供服务,通过对闲置资产和服务的再分配、共享和重复利用实现资源优化。共享经济已经通过大举释放此前封闭的私人领域产能而对某些行业带来了颠覆性影响,如Uber公司的租车业务和Airbnb公司的租住业务。然而,现实中的共享经济未必是真正的共享经济。例如,Uber实际上是线上“出租车”公司,充当调度中心,享有统一的定价权。因此,Uber等公司采用中心化方式实现的共享经济,本质上是“中介公司”,而中介公司经常出现个人隐私泄漏、抬高中介费等问题。

采用基于区块链的安全且防篡改的系统,可以提高主客双方的使用便捷度和安全性。区块链有望通过建立身份及“信誉管理”系统而助推共享经济的快速发展,用户可以通过验证身份和过往行为而实现身份自证。Fermat.org平台基于区块链技术开发了去中心化的“Airbnb”,使得用户可以跨过中介直接同对方联系;Arcade City和La’Zooz公司均基于区块链技术开发了去中心化的“Uber”。

4.2 跨境支付

传统的跨境结算方式需要经过开户行、央行、境外银行、代理行、清算行等机构。每个机构都有自己的账务系统,彼此之间需要建立代理关系,需要有授信额度,每笔交易还需在各机构之间分别记录,进行清算和对账等,这导致交易速度慢、效率低、成本高。区块链技术能够提供信任保证,减少支付双方摩擦,加快结算和清算速度,减少资金闲置时间,提高资金利用效率。通过采用区块链技术,跨境支付的2个开户行之间可以直接进行支付、结算和清算,不需要经过中间机构,能够实现全天候支付、实时到账、提现简便以及没有隐形成本,避免中转过程中产生的手续费。根据麦肯锡公司的测算,在全球范围内,区块链技术在跨境支付和结算中的应用可以使交易成本从每笔约26\$下降到15\$^[16]。Visa计划采用基于区块链技术的银行间结算平台,并投资了区块链公司Chain。Ripple公司为银行类金融机构提供跨境支付服务,希望取代SWIFT的跨境转账平台,打造全球统一的网络金融传输协议。加拿大ATB Financial银行在2016年7月14日宣布其成功利用区块链技术,用20s的时间将1000加元发送到德国,而传统的支付方式一般需要2个以上的工作日来完成。

4.3 供应链

供应链由物流、信息流、资金流共同组成,不同主体之间存在大量的交互和协作,而在整个供应链运行过程中所产生的各类信息被离散地保存在各个环节各自的系统内,信息流缺乏透明度。信息不透明、不流畅影响供应链的效率,且当出现纠纷时举证和追责困难;物流环节区域跨度大、时间跨度长,使得假冒伪劣产品问题难以彻底消除。区块链技术可使得数据对交易各方公开透明,在整个供应链条上形成完整的信息流,确保参与各方及时发现供应链系统运行过程中存在的问题,进而提升供应链管理的整体效率。区块链所具有的数据不可篡改和时间戳的特质能很好地运用于解决供应链体系内各参与主体之间的纠纷,实现轻松举证与追责,彻底解决供应链的假冒伪劣问题,同时可降低成本、提高效率和透明度,降低欺诈风险和人工工作失误风险。据麦肯锡估计,如在全球范围内将区块链应用于供应链,1年可为金融机构和买卖双方带来170~200亿\$的价值^[16]。

京东、IBM和斯坦福大学研发了区块链在供应链领域的创新应用;以色列OGYDocs公司利用分布式账本对商品在国际贸易运输过程中的所有权进行管理;英国Everledger公司利用钻石的4C信息(颜色、切工、纯净度、克拉)等特征数据,为每个钻石生成一个独有的标识用于身份识别。

4.4 物联网

传统的物联网由中心化的数据中心来负责收集所连接的各个设备信息,但这种方式在成本和信息安全等方面有严重缺陷。信息安全问题尚未很好解决;例如,有些智能家居被入侵导致个人隐私泄漏,政府安全部门可以未经授权方式就对存储在中央服务器中的数据内容进行审查,而运营商也可能出于商业利益将用户隐私数据出售给广告公司。区块链为解决这些问题提供了很好的途径。在去中心化的物联网中,区块链能够促进交易处理和交互设备之间的协作。可以建立能够不断扩展的通用、保证隐私、安全和无需信任交易的物联网。

4.5 存证

假证横行使得证明身份是一件非常困难的事情,而类似于需证明“你妈是你妈”的场景很多。要完成这样的证明,必须依赖强有力的、任何人都无法伪造和销毁的证据链,或者让伪造成本极其高昂,区块链技术的不可篡改恰好可用于解决这类问题。美国Factom公司在底层锚定比特币的基础上,构建了基于区块链技术的存证系统。MIT采用区块链技术开发了学历认证系统。IBM的商业价值研究院调查了

全球200家大型医疗公司,发现约有16%的公司已经开展了相关区块链实验,并期望在2017年商业化。

4.6 云存储

目前的云存储主要是中心化的,存在着安全风险和成本高等问题。美国棱镜门事件的揭秘者斯诺登在接受卫报采访时称Dropbox是棱镜计划的伙伴,泄露用户隐私;中心化云存储包括人工成本、法律成本、租金等无法避免的固定成本,导致中心化云服务的价格高。去中心化的系统能够使云储存更安全、更快捷、成本更低,解决了传统云储存的安全与隐私问题,保证用户上传的资源由自己掌握,储存文件的主机不能翻阅其所存储的文件,而且即使在系统大面积瘫痪的情况下文件也能够不受损坏。另外,基于区块链的去中心化云存储具有成本优势,其只有中心化存储成本的1/100~1/10。现有的去中心化云存储的服务商包括Storj、SIA和MaidSafe等。

4.7 公益

近年来公益慈善行业爆发出一些“黑天鹅”事件,极大地打击了公众对公益行业的信任度。社会舆论对公益机构、公益行业信息不透明不公开具有强烈质疑。每个人都想知道自己捐助的钱在何时给了何人。区块链创造了信任机制,天然适合于公益事业,可以解决善款公示的“最后一公里”问题。2016年7月,支付宝与公益基金会合作,在其爱心捐赠平台上设立了第一个基于区块链的公益项目,从技术上可以保障公益数据的真实性,节省信息披露成本。

4.8 知识产权

在现代互联网环境下,知识产权侵权现象严重,网络著作权官司纠纷频发,举证困难,维权成本高等。例如,在传统模式下,音乐人很难获得合理的版税。利用区块链技术,可使音乐的整个生产和传播过程中的收费和用途透明、真实,有效确保音乐人直接从其作品的销售中获益。另外,音乐人可跨过出版商和发行商,在区块链平台自行发布和推广作品,不需要担心侵权问题,还能更好管理自己的作品。优酷首次试用BlockCDNs的区块链内容分发网络,较传统方法可以使成本降低90%。

5 区块链在能源领域的研究现状

区块链目前主要应用于金融业,不过国内外已开始研究“区块链+能源”并取得了初步成果,尚处于概念证明阶段或前期研究,没有商业化应用报道。

Grid Singularity公司开发了能源支付捐赠平台,捐助者可将钱直接发送到比特币驱动的预付费电表,无须通过中介组织,保证捐赠款不会被挪用。能源公

司LO3和区块链公司ConsenSys一起开展了TransActive Grid项目,验证了基于区块链技术的分布式P2P能源交易可成功将居民家中太阳能板产生的过剩电能卖给邻居。目前,西门子公司的next47部门也加入了TransActive Grid项目。德国RWE与区块链公司Slock.it合作研发出基于区块链技术的电动汽车支付系统Block Charge,用户直接与机器,而非与人或公司签订合同。

美国的Filament公司计划在澳洲利用区块链技术和物联网技术,通过在电线杆上装设的传感设备,将其数据通过区块链传输出去,以及时报告停电隐患。在物联网中,Filament采用无线传感器组件,使各个智能设备进行独立沟通和交互。同时,这些智能设备还能进行价值交换,包括比特币、数据和网络接口在内的多种内容都能进行交换。另外,设备间的交易是由智能合约直接管理的,因此是自动执行的。美国的IDEO CoLab采用区块链技术和物联网设计了基于区块链技术的太阳能电池板设备,利用Filament的接口直接与纳斯达克平台联系,在追踪记录发电量的同时自动形成可再生能源证书/补贴(RECs)。这可以激励可再生能源市场的发展,并保证RECs市场的透明性。

国网浙江省电力公司电力科学研究院承担了国家电网公司第一个区块链科技项目,是国内最早将区块链应用于能源互联网的科研机构。万向区块链实验室将投资2000亿元在杭州建设新聚能城,在云端使用区块链技术,来重构“数字化城市”,建设集物联网、互联网、车联网于一体,以研发、孵化、转化、生产、运营为生命全周期,以智能生活、智能交通、智能服务为内容的万物互联互通的智能城市。

能源区块链实验室将建成能源区块链主链,发行以核证碳减排量(Chinese certified emission reduction,CCER)为基础资产的数字资产即碳票,并以碳票为应用结算单位。文献[17]介绍了碳排放权认证、信息物理系统安全、虚拟发电资源交易以及多能源系统协同等应用场景。

6 能源区块链的研究展望

区块链技术在金融等行业已有较多应用,且有些已经商业化。本节对区块链技术在能源领域的应用进行展望。

6.1 P2P电力交易

TransActive Grid项目考虑邻近电力公司之间的电力交易,把电力当作普通商品来处理,未考虑网络安全约束。文献[18]试图在P2P电力交易中考虑安

全约束,并进行阻塞管理;不过,该文认为在缺乏中心化机构管理的情形下,电力市场交易主体之间存在信任问题。事实上,区块链的主要特征就是提供了信任机制,如果讲在区块链上进行交易存在信任问题,那只能说明区块链设计得不够合理。另外,该文提出的弱中心化机构和传统的中心化机构的主要区别在于能够更好地保护用户隐私,不过该文所述的弱中心化交易机构需要设置进入门槛,从而就需要一个身份认证中心,这样的身份认证中心仍然面对隐私泄露风险。因此,从隐私和安全校核的角度来看,采用区块链技术开发电力交易平台未必合适。

P2P电力交易的思路摈弃了交易中心模式,笔者认为在P2P交易框架下如要考虑安全校核,交易就必须程序化且软件代码公开,这样才符合区块链的思想。P2P电力交易的理想应用场景为含有分布式电源和/或储能等有公用双方且可以形成自治的微网环境。考虑到电力系统的安全性要求,主网的电力交易不适用于采用P2P交易模式。

6.2 电动汽车充电桩

电动汽车充电桩的运营商数量众多,通常每个运营商都建立了自己的支付平台;各充电设施建设机构出于运营考虑,发行不同的充电卡,并可能采用不同的收费标准,这给电动汽车用户带来很大不便。由于区块链是去中心的、可信任的,采用区块链技术建立统一的充电桩底层支付平台更容易为公众所接受。

在电动汽车与电力系统的交互领域,尚存在私人充电桩难以实现共享、电动汽车V2G尚缺乏激励机制、动力电池梯级利用无法保证电芯质量等众多问题。采用区块链技术有望解决这些问题。例如,可采用基于智能合约和分布式总账的充电桩按时租赁、基于虚拟货币激励机制的电动汽车V2G自动响应、基于区块链的电池电芯生命周期数据的储存和认证等。

6.3 物理信息安全

电力信息系统一般是孤立系统,通常认为其受网络攻击的可能性不大。在2010年,人们发现了有史以来第一个专门针对工业控制系统的计算机病毒Stuxnet,其通常首先通过受感染的USB等设备渗透计算机网络,这样与外部网络相互隔离的企业内部网络也可能受到Stuxnet的攻击。2015年底,由于电力信息系统遭黑客攻击,导致乌克兰发生了大规模停电。可见,能源系统防御恶意网络攻击的能力有待加强。

如果无法保证足够的信息安全,就需要限制未来的信息网络从专用网向互联网的跨越,“互联网+能源网”的融合模式也就难以形成。电网公司目前采

用的最主要的信息安全防护方式是内外网隔离,但在有些情况下必须进行内外网数据交互,虽然有防火墙进行隔离,但防火墙难免存在漏洞,不能保证万无一失。

智能电表等信息采集设备的数量非常庞大,传统的通过构建专网进行数据采集的方式成本过高,而利用互联网等公用信息网络则存在网络攻击、数据篡改等安全威胁。主要原因在于目前采用的数据库是中心化的,一旦中心数据库遭到入侵,则数据可被读取和篡改,信息安全就无法得到保障。区块链的高冗余存储、去中心化、高安全性和隐私保护等特点使其特别适合存储和保护重要隐私数据,以避免因中心化机构遭受攻击或权限管理不当而造成的大规模数据丢失或泄露。因此,基于区块链的数据安全技术可提升能源互联网的信息安全。

6.4 能源互联网的商业模式

区块链技术的发展能够给能源互联网引入新的商业模式,可通过大力推动光伏电站众筹、资产证券化等模式实施。目前,用户配电设施主要由用户自己投资建设,资金一次性投入较大。采用众筹方式进行投资建设,可以降低客户负担,而投资者也可获得收益。该模式需要解决的主要问题在于怎样确定众筹标的物和现实情况是对应的,如果无法确认标的物的真实性,就存在很大的投资风险,从而影响投资积极性。另外,配电资产的投资收益和用电量有关,只有提供精确可信的计量数据,才能保障投资者利益。区块链技术能解决这两个难题,基于区块链的众筹配售电有望成为一种新型商业模式。

区块链技术正在高速发展之中,在能源领域具有很大的应用前景。在能源区块链领域,目前尚未形成规范的技术标准。在相关国际标准形成之前,工业界和学术界需要投入大量人力物力开展相关研发工作,以抢占这一领域的理论和技术研究高地。区块链技术与其他技术领域如大数据技术^[19-20]的融合也是值得关注的重要课题。

7 结语

能源系统中各个市场主体间如果缺乏信任就容易导致交易摩擦,而在参与者众多的情形下这一般难以避免。区块链技术具有去中心化、公开透明、安全可信的特点,为解决能源系统中的交易摩擦提供了重要途径。虽然区块链技术在能源等行业有不同程度的应用研究,但总体上处于初期阶段,仍存在着效率较低、资源浪费等技术难题,导致区块链技术尚未得到广泛应用。本文概述了区块链技术的定义、技术、

特点、意义与应用等,以促进区块链技术在能源系统中应用的研究与开发。

8 参考文献

- [1] RIFKIN J. The third industrial revolution: How lateral power is transforming energy, the economy, and the world [M]. New York: Palgrave MacMillan, 2011.
- [2] 董朝阳,赵俊华,文福拴,等.从智能电网到能源互联网:基本概念与研究框架 [J]. 电力系统自动化, 2014, 38(15):1-11.
DONG Zhaoyang, ZHAO Junhua, WEN Fushuan, et al. From smart grid to energy internet: Basic concept and research framework [J]. Automation of Electric Power Systems, 2014, 38(15):1-11.
- [3] 张华一,文福拴,张璨,等.考虑能源需求不确定性的居民小区能源中心运行策略 [J]. 电力建设, 2016, 37(9):14-21.
ZHANG Huayi, WEN Fushuan, ZHANG Can, et al. Operation strategy in residential quarter energy hubs considering uncertainties of energy demands [J]. Electric Power Construction, 2016, 37(9):14-21.
- [4] 张华一,文福拴,张璨,等.计及舒适度的家庭能源中心运行优化模型 [J]. 电力系统自动化, 2016, 40(20):32-39.
ZHANG Huayi, WEN Fushuan, ZHANG Can, et al. Operation optimization in home energy hubs considering thermal comfort [J]. Automation of Electric Power Systems, 2016, 40(20):32-39.
- [5] The Economist. The promise of the blockchain: the trust machine [EB/OL]. [2017-01-18]. <http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine>
- [6] SATOSHI Nakamoto. Bitcoin: a peer-to-peer electronic cash system, 2009 [EB/OL]. [2017-01-18]. <https://bitcoin.org/bitcoin.pdf>
- [7] 颜拥. 电网人区块链观察系列一:初识区块链 [EB/OL]. (2016-05-17) [2017-01-18]. <http://www.sgcctop.com/pcnewsview/getNewsInfo.do?id=-1413055205>
- [8] 中国人民银行. 中国人民银行数字货币研讨会在京召开 [EB/OL]. (2016-01-20) [2017-01-18]. <http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/3008070/index.html>
- [9] 闫斌. 关于《央行法定数字货币研究取得阶段性成果》 [EB/OL]. (2016-05-05) [2017-01-18]. <http://www.eeo.com.cn/2017/0105/295992.shtml>
- [10] 中华人民共和国国务院. 国务院关于印发“十三五”国家信息化规划的通知国发[2016]73号《“十三五”国家信息化规划》 [EB/OL]. (2016-12-15) [2017-01-18]. http://www.gov.cn/zhengce/content/2016-12/27/content_5153411.htm
- [11] 中关村区块产业联盟. 中国区块链技术创新应用大赛决赛 [EB/OL]. (2016-12-31) [2017-01-18]. <http://mp.weixin.qq.com/s/XgEDKUhZ9IbC8EO-XFzU5g>
- [12] SWAN M. Blockchain: blueprint for a new economy [M]. USA: O'Reilly, 2015.
- [13] 中国区块链技术和应用发展白皮书, 2016 [EB/OL]. (2016-10-21) [2017-01-18]. <http://mt.sohu.com/20161021/n470943606.shtml>
- [14] 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(4):481-494.
YUAN Yong, WANG Feiyue. Blockchain: the state of the art and future trends [J]. Acta Automatica Sinica, 2016, 42(4):481-494.
- [15] 颜拥. 区块链: 不信任才是最大的信任 [EB/OL]. (2016-07-19) [2017-01-18]. <http://finance.qq.com/a/20160719/034323.htm>
- [16] 区块链—银行业游戏规则的颠覆者 [EB/OL]. (2016-05-27) [2017-01-18]. <http://chainb.baijia.baidu.com/article/472991>
- [17] 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):4011-4022.
ZHANG Ning, WANG Yi, KANG Chongqing, et al. Blockchain technique in the energy internet: preliminary research framework and typical applications [J]. Proceedings of the CSEE, 2016, 36(15):4011-4022.
- [18] 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.
TAI Xue, SUN Hongbin, GUO Qinglai. Electricity transactions and congestion management based on blockchain in energy internet [J]. Power System Technology, 2016, 40(12):3630-3638.
- [19] 王钦,蒋怀光,文福拴,等. 智能电网中大数据的概念、技术与挑战 [J]. 电力建设, 2016, 37(12):1-10.
WANG Qin, JIANG Huai Guang, WEN Fushuan, et al. Concept, technology and challenges of big data in smart grids [J]. Electric Power Construction, 2016, 37(12):1-10.
- [20] 赵俊华,董朝阳,文福拴,等. 面向能源系统的数据科学:理论、技术与展望 [J]. 电力系统自动化, 2017, 41(4):1-12.
ZHAO Junhua, DONG Zhaoyang, WEN Fushuan, et al. Data science for energy systems: Theory, techniques and prospect [J]. Automation of Electric Power Systems, 2017, 41(4):1-12.

收稿日期:2016-11-03

作者简介:

颜拥(1986),男,博士研究生,主要研究方向为区块链技术及其应用、电力市场、互联网+电力营销;

赵俊华(1980),男,“青年千人计划”入选者,副教授,主要研究方向为电力系统分析与计算、智能电网、数据挖掘与计算智能、电力市场;

文福拴(1965),男,教授,博士生导师,本文通信作者,主要研究方向为电力系统故障诊断与系统恢复、电力经济与电力市场、智能电网与电动汽车;

陈星莺(1965),女,教授,博士生导师,主要研究方向为智能配电网运行分析与控制、配用电自动化及其高级应用、电力市场与电力经济。

(编辑 张媛媛)