基于区块链的电力物联网接入认证技术研究*

陈孝莲[1],虎 啸[1],沈 超[1],李 洋[2],高 雪[2],于 佳[2]
(1.国网无锡供电公司,江苏 无锡 214002;2.南瑞集团有限公司(国网电力科学研究院),江苏 南京 211106)

摘 要:随着信息通信技术的发展和“云、大、物、移”战略的实施,电力物联网已为电网发输变配用电等环节提供重要支撑,然而目前集中式的接入认证方式给认证中心带来了巨大的计算和通信压力,特别是大规模并发接入和移动接入为系统认证效率带来严重影响。利用区块链技术去中心化、不可否认的特性,结合电力系统特点,提出了适用于电力物联网的分布式认证方案,方案结合 Shamir 门限秘密共享机制实现了一种 PBFT 共识机制,已经合法接入的终端组成认证组,发起对新入终端的分布式认证,并通过区块链分布式账本进行记录。实验表明,该方案可有效提高电力物联网终端并发接入效率。

关键词:区块链;电力物联网;智能合约;共识机制;分布式认证
中图分类号:TN915 **文献标识码**:A **DOI**:10.16157/j.issn.0258-7998.190791

中文引用格式:陈孝莲,虎啸,沈超,等. 基于区块链的电力物联网接入认证技术研究[J].电子技术应用,2019,45(11):77-81.
英文引用格式:Chen Xiaolian,Hu Xiao,Shen Chao,et al. Research on access authentication technology of power IoT based on Blockchain[J]. Application of Electronic Technique,2019,45(11):77-81.

Research on access authentication technology of power IoT based on Blockchain

Chen Xiaolian[1],Hu Xiao[1],Shen Chao[1],Li Yang[2],Gao Xue[2],Yu Jia[2]
(1.Wuxi Power Supply Company,Wuxi 214002,China;
2.NARI Group Corporation(State Grid Electric Power Research Institute),Nanjing 211106,China)

Abstract:With the development of information and communication technology and the implementation of the strategy of "Cloud, Big, Things, Move", the power Internet of Things has provided important support for the transmission, transformation, distribution and power consumption of power grid. However, the centralized access authentication method has brought tremendous pressure on the authentication center, especially the large-scale concurrent access and mobile access, which have a serious impact on the system authentication efficiency. Based on the decentralized and undeniable characteristics of Blockchain technology and the characteristics of power system, a distributed authentication scheme for power Internet of Things is proposed. The scheme realizes a PBFT consensus mechanism by combining Shamir threshold secret sharing mechanism. The legally accessed terminals form an authentication group, initiating distributed authentication for new terminals, and recording through Blockchain distributed account book. Experiments show that the scheme can effectively improve the concurrent access efficiency of power Internet of Things terminals.
Key words:Blockchain;power Internet of Things;intelligent contract;consensus mechanism;distributed authentication

0 引言

随着信息通信技术的发展,电网智能化业务以及能源互联网泛在业务接入需求的不断增加,对信息通信技术支撑电网业务的能力提出了更高的要求,电力通信网支撑业务安全、可信、灵活接入的需求非常迫切[1-3]。

当前电力通信网是典型的汇聚型网络,终端与终端之间几乎没有数据交互。随着能源互联网的建设,大量终端之间直接通信的需求日益凸显,传统中心化汇聚型网络在认证性能和效率上难以满足泛在业务需求[4]。

电力物联网的广泛应用也带来了愈加严峻的安全挑战。一方面,电力物联网终端节点数量多部署范围广,节点物理环境不可控,容易受到物理劫持、节点复制、信号截获窃取重放、中间人攻击等威胁;另一方面,电力物联网终端由于体积和电量限制,其计算、存储和通信能力有限,无法部署完整的密码算法。

电力物联网存在海量的设备,应采用去中心化的安全体系,构建轻量级的密钥管理系统。区块链是一种在对等网络环境下,通过透明和可信规则,构建可追溯的块链式数据结构,实现和管理事务处理的模式,具有分布式对等、防伪造和防篡改、透明可信和高可靠性等方

*基金项目:国网江苏省电力有限公司科技项目(J2018-91719-XTKJ)

面的特征,可以有效解决物联网发展中面临的大数据管理、信任、安全和隐私等问题,从而推进物联网发展到分布式、智能化的高级形态。

区块链是一种允许创建交易分布式数字账本的技术,其账本共享给网络中的所有节点,具有主体对等、公开透明、安全通信、难以篡改和多方共识等特性,已应用到越来越多的领域中[5-7]。

本文针对电力物联网接入认证需求,利用区块链技术去中心化、不可否认的特性,结合 Shamir 门限秘密共享机制实现了一种 PBFT 共识机制,提出了适用于电力物联网的分布式认证方案,并仿真分析了方案的实际效能。

1 相关研究

1.1 物联网接入认证

接入认证是物联网终端设备接入电力物联网系统实现其功能的第一步,实现对物联网设备的可信认证以及对于操作者身份的可信确认,从而确定该用户对电力物联网资源是否具有相应的访问和使用权限,进而使物联网系统的访问控制策略能够可靠、有效地执行。

认证就是在物联网工作过程中确认资源申请者身份的过程,是控制资源非法外泄的有效手段,也是实现分级管理的有效方法,当前的认证技术主要有口令认证、X.590 的认证、域认证等。

静态口令和动态口令认证都属于口令认证,早期一般都使用静态口令认证,包括 PC 登录口令、系统认证口令、金融系统认证口令等。静态口令认证比较简单,在计算机上容易操作,但是安全性不高。鉴于这种缺点才提出了动态口令认证,动态认证使用了智能认证和特征认证相结合的认证方法,加强了口令的抗攻击性和破解难度。

X.509 的认证是基于 X.509 证书的一种认证技术,该认证技术主要依靠权威机构实现,并且采用加密算法加密使得实现更加安全简单,持有 X.509 证书的主体可以获得 CA 的认证。

在 X.509 里,组织机构通过发起证书签名请求(CSR)来得到一份签名的证书。首先需要生成一对钥匙对,然后用其中的私钥对 CSR 进行签名,并安全地保存私钥。CSR 进而包含有请求发起者的身份信息、用来对此请求进行验证的公钥以及所请求证书专有名称。CSR 里还可能带有 CA 要求的其他有关身份证明的信息。然后 CA 对这个专有名称发布一份证书,并绑定一个公钥,组织机构可以把受信的根证书分发给所有的成员。

目前电力物联网接入认证主要是基于公钥证书的中心化认证方式[8-10]。PKI(公钥基础设施)技术采用证书管理公钥,通过第三方的可信任机构 CA(认证中心),把用户的公钥和用户的其他标识信息(如名称、E-mail、身份证号等)进行绑定,用于验证用户的身份。这种认证方式需要可信的第三方认证服务器来对用户进行身份管理,通过用户的数字证书或身份令牌来确认用户身份。电力物联网具有覆盖范围广、传输地区多、提前信息量庞大的特点,采用集中认证的方式会降低认证效率和安全性,分布式的、点对点的认证方式更适合于电力大型电力物联网。

1.2 基于区块链的接入认证

基于数字证书的认证是一项重要的身份认证技术,由于 CA 是数字证书的关键部分,目前实现数字证书管理的集中式 PKI 在分布式环境中面临的最大问题是 CA 的可信性问题。

基于区块链的接入认证方法领域已有研究主要利用区块链的去中心化特征建立分布式 PKI,例如,麻省理工大学的 Conner 等人利用公共总账来记录用户证书,用公开的方式把用户 ID 与公钥证书关联,实现了首个区块链分布式 PKI 系统[11]。该系统虽然支持用户查询证书签发过程,但是带来了隐私泄露隐患,无法应用于电力物联网等对用户隐私保护有要求的场景。为此,AXON L 等提出了一个隐私感知的区块链认证模型 PB-PKI,该模型用线上和线下密钥进行用户身份保护,减少了隐私泄露的风险[12]。MASTSUMOTO S 针对提高认证 CA 的安全性问题,提出了机遇以太坊激励策略的 PKI 框架 IKP[13]。

2 基于区块链的分布式认证

2.1 认证模型

身份认证技术是通过密码学手段在计算机系统中确认实体对某种资源或服务是否有访问权限的方法和机制。电力物联网中终端节点数量多、单点计算存储能力弱,其身份认证需要采用效率高的方案。常见的电力物联网接入场景如图 1 所示。物联网终端通过接入网关接入电力通信网,访问相关业务。其中所有合法接入的物联网终端共同维护一个区块链分布式账本,用于记录合法的接入事件。

合法接入的电力物联网终端根据其配置不同分为主节点和从节点两类。其中,电力物联网业务系统的每次合法接入形成一个区块,新物联网节点申请加入时,主节点从区块链上随机选择符合阈值数量的合法接入节点形成认证组,认证组通过共识算法进行分布式认证,认证通过后生成新加入物联网节点的数字证书,并将接入过程记录在一个新的区块中。成功接入的物联网节点通过链上部署的智能合约实现业务功能。

所有合法的电力物联网终端节点的接入过程存储在可方便查询、无法篡改的区块链分布式账本中。区块保存节点接入业务系统的时间、业务类型、权限和状态信息。区块包含区块头和区块体两部分。其中区块头包含前一区块的 hash 值、时间戳、随机数、目标区块 hash 值和 Merkle 根等内容,通过前后的 hash 值形成可追溯的链状结构;区块体存储接入认证所需要的信息,包括物联网终端节点 ID、公钥和证书、运行状态、接入时间、业务类型和权限等级。

电力物联网终端节点需要接入认证时,首先向主节点发送认证请求,主节点进行首次验证并将认证请求进

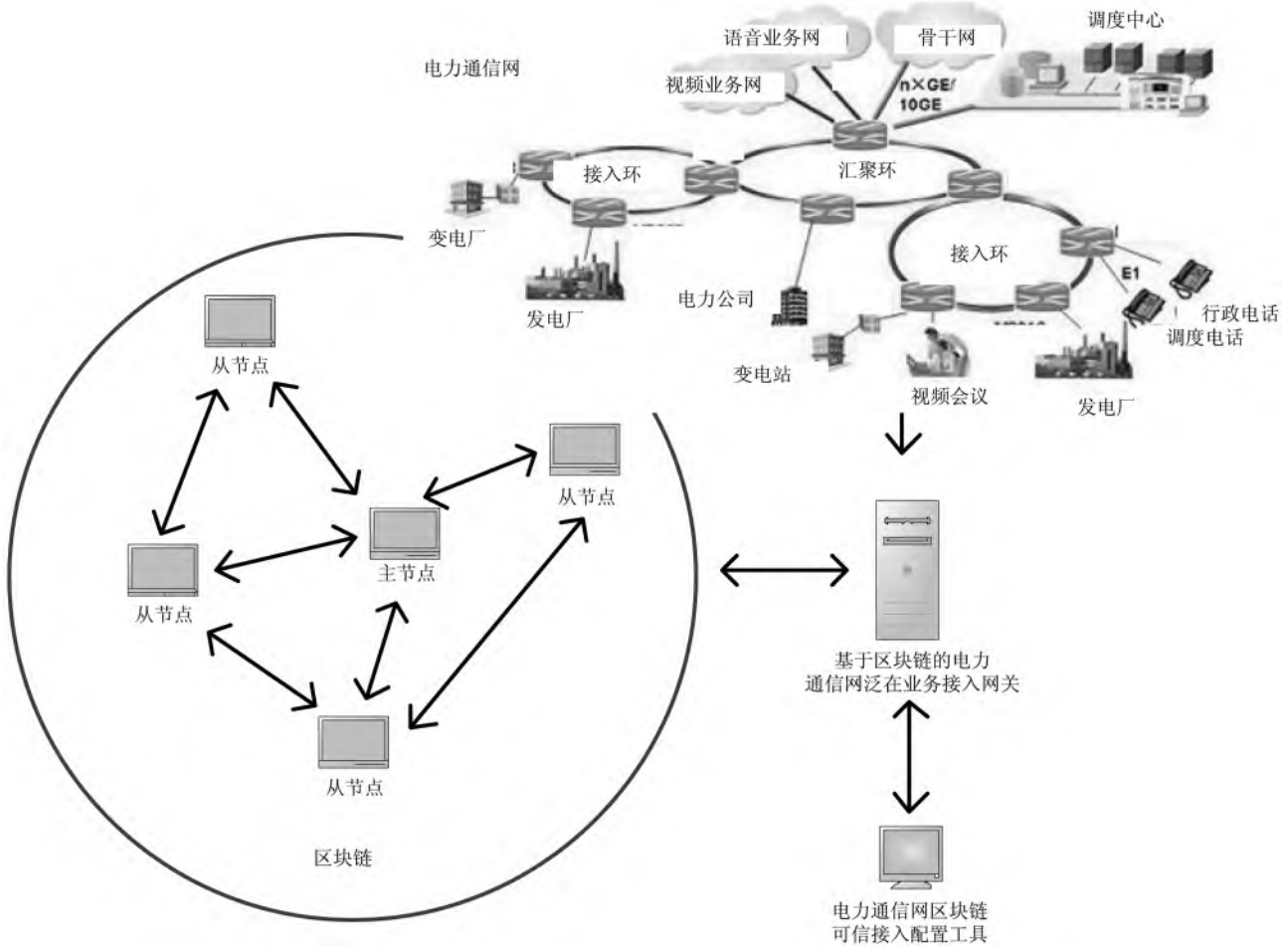

图 1 电力物联网接入示意图

行封包,同时检索接入认证区块链中合适的节点,形成分布式认证组。合适节点首先应满足合法性,即节点已经成功接入业务系统;其次应满足认证性,例如与待接入节点属于同类业务或同小区的业务;第三应满足功能要求,即有足够的电量和处理能力运行认证算法。随后主节点通过组播方式将请求发送给认证组,发起分布式认证。认证中结合投票式共识算法和待接入节点的公钥证书,形成新的区块。接入认证过程如图 2 所示。

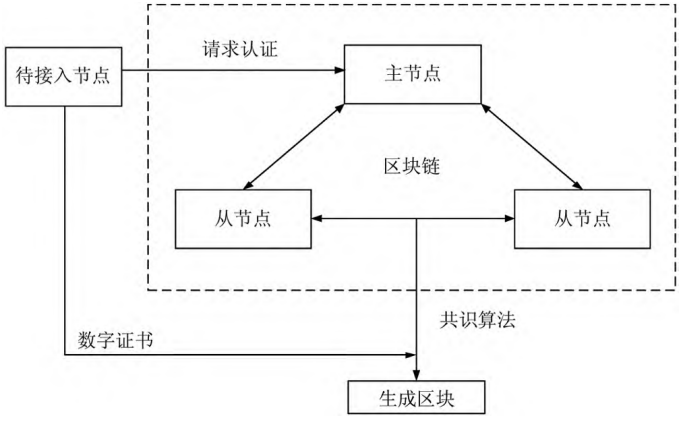

图 2 接入认证过程示意图

2.2 认证过程

具体认证过程分为请求和确认两个阶段:

(1)请求阶段

电力物联网终端向主节点发起认证申请,申请信息包括终端标识的注册信息,其中,ID 为包含终端类型字段的唯一标识字符串,表示终端对 ID 的签名;Pub 为终端公钥;R 为授权机构颁发的数字证书。主节点使用终端公钥对终端签名进行确认,提取请求信息形成分布式认证协议请求报文。

(2)确认阶段

确认阶段是基于区块链的分布式认证过程。主节点响应认证申请,从终端 ID 中截取节点类型字段作为关键词检索认证区块链,从区块链节点中的节点类型、接入时间、运行状态和业务类型进行综合匹配,择优选取满足阈值设定数量的节点,组成认证组 $G=\{P1,P2,\cdots,Pt\}$,并在 G 中广播发送认证协议请求报文。G 中节点运行 PBFT 共识算法完成分布式认证,并生成新的区块,主节点返回确认信息给终端。

在共识算法执行过程中,采用(t,t)门限秘密共享算法实现接入认证秘密信息的分发与合成。在(t,t)门限秘密共享体制中,秘密 K 被分成 t 个部分(称作子秘密或

影子密钥),分别给 t 个参与者持有,使得:①同时获得 t 个参与者所持有的部分信息可重构 K;②少于 t 个参与者所持有的部分信息则无法重构 K。

G 节点数量为 t,共享的秘密信息 $K=R$。

认证组节点运行的 PBFT 共识算法包含预准备、准备、提交等过程,如图 3 所示。

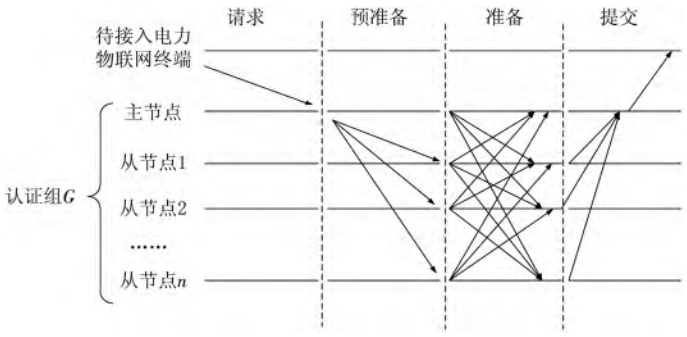

图 3 基于 PBFT 共识的接入认证交互过程

①预准备

主节点随机选择 $t-1$ 个元素,令 $a_1,\cdots,a_{t-1}\in Z_p^*$,$f(x)=R+a_1x+a_2x^2+\cdots+a_{t-1}x^{t-1}$,计算 $y_i=f(x_i)$,$1\leqslant i\leqslant n$,将 y_i 分配给从节点 i 作为其子秘密。

②准备

G 中所有节点收到认证请求和认证份额后,运行秘密共享算法中的恢复算法。具体如下:G 中节点之间互相交换所持有的秘密份额,从而得到 t 个点对:$(x_1,y_1),\cdots,(x_t,y_t)$。根据拉格朗日插值算法,可得待认证终端的证书信息:

$$R=\sum_{j=i}^{t} y_j \prod_{1<l<t,l\neq j} \frac{x_l}{x_l-x_j} \tag{1}$$

从而恢复出共享秘密 R,G 中每个节点可根据第三方公信机构的公钥信息对 R 进行验证。

③提交

G 中对待接入终端认证通过的节点提交认证结果给主节点,主节点综合认证组结果,完成对电力物联网终端的认证,生成接入会话密钥给电力物联网终端。同时在系统中形成一个新的区块,区块以分布式总账的方式记录了新节点的接入情况。

终端返回加密后的确认信息给网关,认证结束。

系统通过共识算法形成区块后,合法接入的电力物联网终端节点根据链上智能合约进行电力网业务访问,主要实现业务接入、费用计算和权限控制等功能。

3 仿真实验

电力物联网系统属于行业应用,因此采用基于 Hyperledger Fabric 联盟链进行实验环境的搭建。联盟链是指其共识过程受到预选节点控制的区块链,是介于私有链和公有链之间的一种区块链,除具有一般区块链的优点外,还具有可控性强、数据默认不公开、交易速度快、可定制访问控制策略等优点。

HyperLedger Fabric 是由 Digital Asset 和 IBM 公司贡献的、由 Linux 基金会主办的一个超级账本项目,是目前非常流行的模块化区块链网络框架实现方案。HyperLedger Fabric 支持认证、共识和智能合约模块的即插即用和定制开发,并适应整个经济生态系统的复杂性和高精度性。HyperLedger Fabric 利用 docker 容器技术运行称为链码(Chaincode)的智能合约,该合约包含了系统的应用程序逻辑。

本文的验证环境采用 Hyperledger Fabric 1.0 版本运行于 CentOS 中的 docker 18.06 容器中。接入网关采用 Intel i7-7700HQ CPU,主频 2.80 GHz,16 GB DDR2400 内存。物联网终端采用树莓派 3b 模拟,配置为博通 BCM2837B0 SoC,集成 4 核 ARM Cortex-A53 64 位 CPU,主频为 1.4 GHz,具有 1 GB LPDDR2 SDRAM。

图 4 显示了基于区块链的电力物联网接入认证方案中认证时间随物联网规模变化的情况。可以看出,在传统的集中式接入认证方案下,当认证节点数量增多时,认证中心计算和网络开销增大,认证效率降低,认证时间增长迅速。在基于区块链的分布式认证方案下,当物联网终端节点数量较少时,认证效率较集中式认证低,这是因为区块链方案中运行分布式认证协议开销在网络规模较小时占比较大,当物联网规模增大时,认证效率提高较明显。

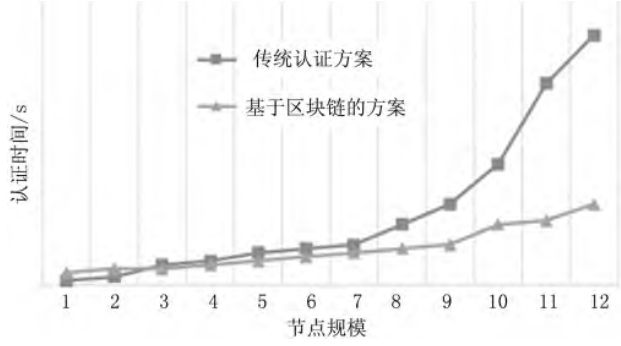

图 4 认证效率曲线

图 5 为相同物联网节点规模下,认证组节点阈值分别在 3、5、7 下的认证时间对比。根据拜占庭容错原理可

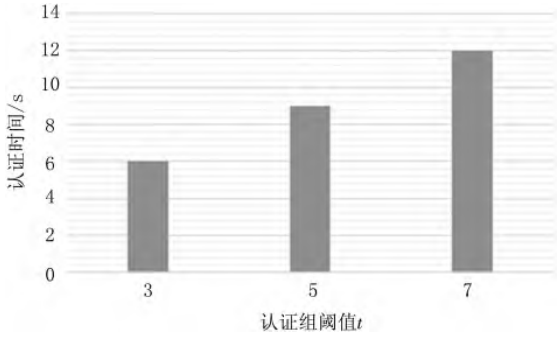

图 5 认证组规模对认证效率的影响

知，认证组节点数量增加会带来安全性的增加，但信息交互次数增加使认证时间相应增大，降低了认证效率。

图 6 为新区块生成时间与已有区块链规模的关系，数据显示，随着区块链长度的增加，新区块生成时间相应增加，但总体性能下降不明显，因此可适用于大规模并发接入的情景，符合智能化电力物联网系统应用需求。

4 结论

随着物联技术在智能电网领域的深入发展，电力物联网终端对分布式智能化高效率接入提出了更高的要求。本文基于区块链中去中心化的分布式总账技术、全网验证的共识机制，提出了一种适用于电力物联网安全高效接入认证方案。相比于传统方案，本方案基于区块链的可验证性，避免了验证时运行解密算法所带来的系统开销。通过基于 Hyperledger 平台的仿真实验显示，所提方案比传统集中式认证方案在认证效率上有显著提升。下一步研究将侧重于在实际电力业务应用场景中，通过试点应用，测试系统在海量接入情况下的接入认证性能。

参考文献

[1] 陈昕，姜怡喆，王雪，等.互联网视角下的能源互联网发展研究[J].中国电力，2018，51(8)：43-48.

[2] 高峰，曾嵘，屈鲁，等.能源互联网概念与特征辨识研究[J].中国电力，2018，51(8)：10-16.

[3] 于佳，马平，刘锐，等.电力无线专网业务支撑能力研究[J].广东电力，2018，30(12)：49-56.

[4] 李黎，华奎，姜昀芃，等.输电线路多源异构数据处理关键技术研究综述[J].广东电力，2018，31(8)：124-133.

[5] 王安平，范金刚，郭艳来.区块链在能源互联网中的应用[J].电力信息与通信技术，2016，14(9)：1-6.

[6] SAMANIEGO M，DETERS R.Blockchain as a service for IoT[C].2016 IEEE International Conference on Internet of Things(iThings) and IEEE Green Computing and Communications(GreenCom) and IEEE Cyber，Physical and Social Computing(CPSCom) and IEEE Smart Data(SmartData)，Chengdu，2016：433-436.

[7] KAN L，WEI Y.，MUHAMMAD A H，et al.A multiple Blockchains architecture on Inter-Blockchain communication[C].2018 IEEE International Conference on Software Quality，Reliability and Security Companion(QRS-C)，Lisbon，Portugal，2018：139-145.

[8] Li Huige，Tian Haibo，Zhang Fangguo，et al.Blockchain-based searchable symmetric encryption scheme[J].Computers and Electrical Engineering，2019，73：32-45.

[9] 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.

[10] LOU J，ZHANG Q，QI Z，et al，A Blockchain-based key management scheme for named data networking[C].2018 1st IEEE International Conference on Hot Information-Centric Networking(HotICN)，Shenzhen，China，2018：141-146.

[11] FROMKNECHT C，VELICANU D.CertCoin：a NameCoin based decentralized authentication system[R].Technical Report，6.857 Class Project，Massachusetts Institute of Technology，2014.

[12] AXON L.Privacy-awareness in blockchain-based PKI[R].CDT Technical Report.University of OxFORD，2015.

[13] MATSUMOTO S，REISCHUI R M.IKP：Turning a PKI around with decentralized automated incentives[C].2017 IEEE Symposium on Security and Privacy，2017.

(收稿日期：2019-07-11)

作者简介：

陈孝莲(1977-)，女，硕士，高级工程师，主要研究方向：电力系统信息通信技术与智能电网。

虎啸(1988-)，男，硕士，工程师，主要研究方向：电力系统信息通信技术与智能电网。

于佳(1985-)，通信作者，女，硕士，高级工程师，主要研究方向：电力无线通信技术、智能电网通信技术，E-mail：yujia@sgepri.sgcc.com.cn。

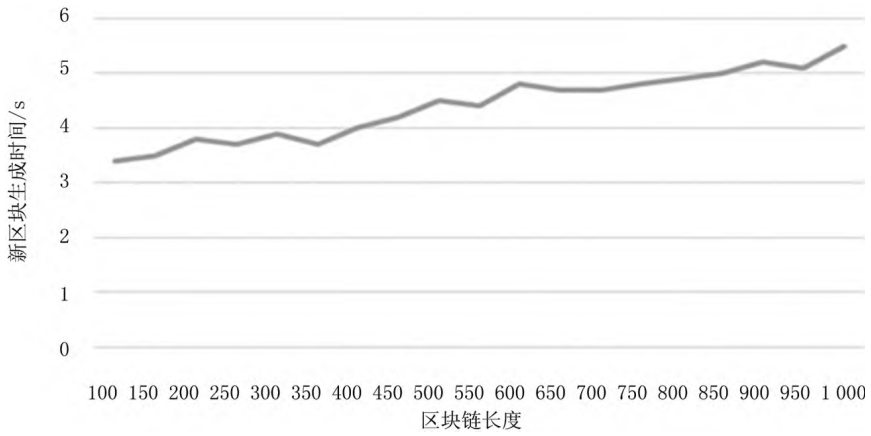

图 6 区块生成曲线