DOI：10.13334/j.0258-8013.pcsee.170353 文章编号：0258-8013 (2018) 04-1026-09 中图分类号：TM 73

能源区块链的关键技术及信息安全问题研究

丁伟[1]，王国成[2]，许爱东[1]，陈华军[1]，洪超[1]

(1. 南方电网科学研究院有限责任公司，广东省 广州市 510663;
2. 新能源电力系统国家重点实验室(华北电力大学)，北京市 昌平区 102206)

Research on Key Technologies and Information Security Issues of Energy Blockchain

DING Wei[1], WANG Guocheng[2], XU Aidong[1], CHEN Huajun[1], HONG Chao[1]

(1. Electric Power Research Institute, CSG, Guangzhou 510663, Guangdong Province, China;
2. State Key Laboratory of Alternate Electrical Power System with Renewable Energy Sources, North China Electric Power University, Changping District, Beijing 102206, China)

ABSTRACT: As an emerging decentralized architecture and distributed computing paradigm, blockchain has great significance for breaking through the bottleneck of trust lack among the participants as well as promoting the smooth implementation of energy internet. Firstly, this paper analyzed the technical requirements and applicability of blockchain to energy internet, meanwhile put forward the concept of energy blockchain. Then, the key technologies during the development of energy blockchain were then analyzed from three aspects-consensus mechanisms, encryption algorithms and smart contracts. In addition, this paper has emphatically analyzed the security challenges and corresponding strategies of energy blockchain from three aspects(private key lost, privacy disclosure and protocol attack), as well as discussed how to construct a security protection system for energy blockchain. Finally, some related suggestions of energy blockchain were proposed.

KEY WORDS: energy blockchain; consensus mechanism; information security; secret sharing; security protection

摘要：区块链作为一种全新的去中心化的基础架构和分布式计算范式，对突破能源互联网各参与主体间缺乏信任的根本瓶颈，实现能源互联网的平稳落地具有重要意义。首先分析了能源互联网对区块链的技术需求和引入区块链的适用性，并提出能源区块链的概念；在此基础上从共识机制、加密算法和智能合约 3 个方面对能源区块链发展的关键技术进行分析；接着从私钥丢失、隐私泄露和协议攻击 3 个角度重点分析了区块链应用于能源互联网所面临的安全挑战和应对策略，并探讨了能源区块链安全防护体系的构建；最后，给出了能源区块链发展的相关建议。

关键词：能源区块链；共识机制；信息安全；秘密共享；安全防护

0 引言

2008 年，比特币的创始者中本聪发表了一篇名为《比特币:一种点对点电子现金系统》[1]的论文，从此区块链技术开始进入国内外学者的视野。作为比特币的底层技术和基础架构，从狭义上来讲，区块链是一种将数据区块以时间顺序依次相连形成的一种链式数据结构，并利用密码学技术实现数据安全传输与访问的分布式账本[2]。

区块链技术最大的特点是去中心化。其在节点无需相互信任的前提下，通过采用分布式共识机制、加密算法、点对点传输和智能合约等技术，即可实现可信任的点对点交易，从而为解决目前依靠中心或者第三方机构普遍存在的高成本、低效率和信息安全等问题提供了切实有效的技术方案[3]。区块链被认为是推动新一轮技术产业革命到来的突破性技术。随着区块链技术的快速发展，国内外众多研究机构和学者开始密切关注并参与到区块链技术的探索中来。

区块链技术的去中心化、开放、智能和共享与能源互联网的理念相吻合[4-5]，业界普遍认为其在能源互联网中的应用将有效支撑多类型能源系统的开放互联和多用户的广泛深度参与，通过共同维护可信任的分布式账本，能够实现未来能源交易中能量流、信息流和价值链的有效衔接。针对区块链在能源互联网中的应用，国内外学者也逐步开展了一些研究。文献[6]从多维度多角度对区块链技术在能源互联网中的应用进行了归纳和分析，并选取典型应用场景深入分析了区块链技术在能源互联网中

的具体应用方式。文献[7]了区块链技术在辅助服务市场中应用的关键性技术和发展思路。文献[8]提出了一种基于区块链的弱中心化电力交易系统，并探讨了相关的安全校核、阻塞管理及区块链的具体应用细节问题。文献[9]重点分析了区块链在能源领域各个环节的应用场景和业务模式，并给出未来能源区块链发展的相关建议。文献[10]针对去中心化的分布式能源交易系统的交易安全问题，提出一种使用区块链技术、多重签名、匿名加密消息流的方法使交易双方匿名协商交易价格，从而保证交易安全。然而上述研究大多针对区块链在能源互联网中的各个应用场景的应用模式、关键技术和发展思路等进行探索，都没有系统地对区块链应用于能源互联网的信息安全问题进行研究。

本文首先分析了能源互联网引入区块链的技术需求和适用性，并提出能源区块链的概念；在此基础上从共识机制、加密算法和智能合约 3 个方面对能源区块链发展的关键技术进行归纳与分析；然后在分析区块链自身安全特性的基础上，阐述了能源区块链在私钥丢失、隐私泄露和协议攻击 3 方面所面临的安全挑战和应对策略，并提出以“结构＋本体＋管理”为基础，全面覆盖分区分域、边界防护、数据安全、应用安全、密钥安全、安全审计与预警、应急机制 7 个维度的全方位立体安全防护体系；最后给出近阶段我国能源区块链发展的相关建议。

1　能源区块链

1.1　能源互联网引入区块链的技术需求

近年来，能源互联网带动众多的新兴能源市场和能源产业的发展，但同时也逐渐暴露出交易效率、信息安全、主体权益保障等诸多风险。具体来讲，一是未来能源市场的交易主体类型、主体属性、交易模式、市场组合以及交易商品都将呈现多元化的态势，交易主体和交易数量都将大幅增加，由此产生的海量数据，将使现有的集中决策式能源交易系统面临决策效率低下甚至指令执行和信息处理出现错误的风险；二是能源系统将由传统的集中决策模式逐渐演变成分布决策模式，由此将引发交易主体间信任缺失的问题；三是各个能源子系统的价值单位不同，将导致能源系统在能量流动和价值流动过程中的成本激增。

1.2　区块链于能源互联网的适用性分析

在能源互联网中引入区块链是否合适，一是要分析引入的可行性，二是要分析引入的必要性。

首先，从能源互联网和区块链的理念进行分析，得出二者具有去中心化、开放、智能和共享四个共同理念。此外，在能源互联网中，能量路由器通过信息流获取能量流的状态信息，从而实现调度和控制等功能[11]。未来通过在能源路由器上搭载分布式计算和数据存储模块并加载特定的智能合约程序，即可实现区块链节点的功能。综上，无论是从理念上还是从技术上，在能源互联网中引入区块链都是可行的。

其次，针对能源互联网所面临的潜在风险，区块链的技术优势体现在以下几个方面：区块链以分布式决策模式通过智能合约技术对交易信息自动进行处理、传输和存储，从而可以大幅提高能源交易系统的交易效率，并通过各系统节点间运行的共识机制实现决策结果最优化；区块链使用加密算法和共识机制，无需设置第三方信任主体，即可有效防止能源交易中的抵赖、篡改和欺诈等行为，利于提高交易主体的自律性和构建能源系统信用体系；区块链能够将不同能源子系统的价值进行串联，促进能源互联网向价值互联网的转变，有利于构建新型能源生态圈。综上所述，区块链的引入能够从多方面克服能源互联网所面临的技术风险并促进能源互联网的发展，具有较强的必要性。

1.3　能源区块链

区块链与能源互联网相辅相成，前者能为后者提供技术支撑，促进新型能源供需体系的建设；后者能为前者提供市场和应用背景，实现技术价值。与传统的网络体系相比，区块链的优势主要体现在安全、透明和高效 3 个方面。而能源互联网具有供需分散、系统扁平、交易开放等特征[12-13]，由此区块链与能源互联网便找到了契合点即能源区块链。如图 1 所示，所谓能源区块链就是指电力、石油、天然气以及交通运输网络等各能源节点利用链式的加密区块验证存储能源交易数据，利用共识机制进行分布式决策，利用智能合约自动完成交易处理的全新的去中心化能源互联结构，从而最终实现能源交易过程中能量流、信息流和价值流的有效衔接。

2　能源区块链关键技术分析

能源区块链能够作为底层技术框架，在能源生产、能源配送、能源消费、能源储存、能源交易等五个能源互联网价值链环节进行应用，能够突破能源应用的技术限制，并促进新型能源供需体系的构

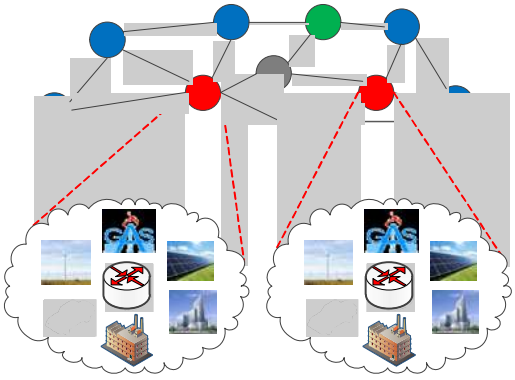

图 1 能源区块链

Fig. 1 Energy blockchain

建。结合能源互联网的需求和发展趋势，对区块链的共识机制、安全算法和智能合约等关键技术进行分析。

2.1 共识机制

共识机制是指能源区块链系统中各能源企业、能源服务商、用户、金融机构、政府等各个分布式节点之间验证行为、建立信任和获取权益的数学算法，通过该机制各参与节点共同记账，保证交易信息的可溯源。其设计参考因素主要包括节点结构、身份验证、隐私性、交易完整性、容错性和交易性能等[14]。常用的共识机制包括工作量证明机制(proof of work，PoW)、权益证明机制(proof of stake，PoS)、股份授权证明机制(delegated proof of stake，DPoS)和实用拜占庭容错机制(Practical Byzantine Fault Tolerance，PBFT)等。

虽然区块链最大的特点是去中心化，然而在能源互联网中涉及到多角色能源交易，完全地实现无政府或行业主管部门监管是不现实的。为此，从合规监管、性能效率、资源消耗、容错性和是否需要代币五个维度对现有的典型共识机制的技术水平进行评价如表 1 所示。具体来讲，PoW 机制能够完全实现去中心化，节点自由加入和退出，但存在资源消耗高、性能效率低下等缺点，并不适合于能源互联网的商业应用。PoS 机制根据每个节点所占代币的比例和时间，等比例地降低挖矿难度，从而加快找随机数的速度，虽然在一定程度上缩短了共识达成的时间，但仍然不适合商业应用。DPoS 机制采用类似于董事会投票的模式，大幅缩小参与验证和记账节点的数量，缩减对于确认的需求将使得交易速度直线上升，可以达到秒级的共识验证。然而整个共识机制还是依赖于代币，但能源互联网应用背景是不需要代币存在的。PBFT 机制也是一种采用许可投票、少数服从多数来选举领导者进行记账的共识机制，其特点是允许强监管节点参与，具备权限分级能力，性能效率更高，资源消耗低，且不需要代币。可见，PBFT 更加适合多能源角色参与的能源区块链应用模式。

表 1 典型共识机制技术水平对比

Tab. 1 Technical level comparison of typical consensus mechanisms

评价维度	PoW	PoS	DPoS	PBFT
合规监管	弱	弱	较弱	强
性能效率	低	较低	较高	高
资源消耗	高	较高	较高	低
容错性	50%	50%	50%	33%
是否需要代币	是	是	是	否

未来针对能源互联网中不同环节和场景下的应用，可根据具体应用场景和性能需求的不同灵活选取，也可以研发更加高效更加符合能源互联网监管机制的共识机制。

2.2 加密算法

能源区块链基于多种密码学原理进行数据加密及隐私保护，主要包括哈希算法和非对称加密算法两种。不同的加密算法性能不同，单一算法很难满足能源互联网中各个应用的需求，一般需要组合使用。对于能源区块链来说，加密算法在保证安全可靠的同时，还要保证满足特定应用场景所需的性能效率。下面对两类算法的性能进行比较。

哈希算法作为一种单向密码体制，其主要特征就是能够将任意长度的信息变换成固定长度的消息摘要，且其输出是唯一的。典型的哈希算法有 MD5、SHA1、SHA256 和 SM3[15]。从表 2 的对比结果来看，SHA256 和 SM3 二者运算速度与安全性大致相同，目前比特币的加密算法以 SHA256 为主。

表 2 典型哈希算法性能比较

Tab. 2 Performance comparison of typical hash algorithms

加密算法	安全性	运算速度	输出大小/位
MD5	低	快	128
SHA1	中	中	160
SHA256	高	比 SHA1 略低	256
SM3	高	比 SHA1 略低	256

非对称加密算法使用一对密钥分别完成加密和解密。非对称加密算法密钥分配管理简单，但加解密速度较慢，常用的非对称加密算法有 RSA、ECC 和 SM2。目前，比特币和以太坊均采用比 RSA 安全性更高、运算速度更快的 ECC 算法。而与 ECC 算法相比，国密算法 SM2 有以下 3 点优势：

1）运算效率方面：SM2 算法无需对待加密数据进行编码任何处理，运算效率更高；

2）数据原文正确性的判断方面：SM2 算法加密后的密文中有原文的杂凑值，解密的同时对原文做哈希运算，可验证数据原文的正确性。

3）密钥长度限制方面：ECC 算法将密钥长度限制在有限域的素数之内，而 SM2 算法容纳的密钥长度可以达到$(2^{32}-1)v$比特的长度(v表示 SM3 杂凑比特值，一般为 256)。

能源区块链未来作为国家关键信息基础设施，防止外部对能源企业的安全威胁、强化对控制类指令的身份认证、保护用户隐私和数据资产安全以及实现信息安全防护的“可控、能控、在控”将成为能源行业安全防护的重点。国产密码作为网络安全要素技术，在能源安全生产中进一步广泛应用已成必然趋势。从算法的安全性、运算效率以及自主可控性等方面综合考虑，建议我国能源区块链采用国产密码算法 SM3 和 SM2。

2.3　智能合约

智能合约是能源区块链的重要组成部分，其本质上是一段由事件驱动、具有状态且运行在可复制共享区块链上的程序，具有自动处理数据以及控制管理区块链上的资产等功能。智能合约运行机制主要包括预定义的状态机、触发事件、响应规则等[16-17]。能源区块链需要实时监控智能合约的状态，并通过核查外部数据源，确认满足特定的预置触发条件后激活并按照预置的响应规则执行合约。智能合约依靠各能源参与主体的实际信息来实现，不仅可以降低管理的成本，还可以避免不必要的争议，因为所有的行为在智能合约下能够精确地执行，可以有效应对未来能源互联网中交易主体类型、主体属性、交易模式、市场组合以及交易商品、交易主体和交易数量大幅增加的趋势，从而提高交易效率。

智能合约最重要的是要保证其程序代码的合法合规性和安全性。能源互联网中智能合约的制定不仅需要各交易主体的参与，同时需要政府及能源监管机构进行监督审查，应预防死循环导致的 DoS 攻击，可采用容错机制和运行环境隔离等机制，从而有效促进不同能源子系统间的自协作，降低不同系统间的交易成本，有利于能源交易的公平公正。

3　能源区块链的信息安全

能源互联网的典型特征是信息与物理系统融合，主要基本功能包括：信息与物理系统的实时监控与综合仿真；信息集成、共享和协同；大规模实体控制和系统全局优化。区块链在能源互联网中的应用使得能源信息系统从专网专用、采用专有协议向网络日益开放、采用标准协议进行转变。能源信息系统中标准协议和智能电子设备的广泛应用一方面为实现能源系统智能化提供了技术保障，但另一方面也带来了网络安全问题。未来能源区块链面临的安全问题包括除了物理系统和信息系统自身的安全问题外，信息系统与物理系统间的交互影响、内在联系以及跨空间的连锁故障也有待进一步充分研究。为此，分析能源区块链面临的安全挑战，加强能源区块链网络安全、提高其对风险威胁和恶意攻击的防御水平具有重要意义。

3.1　区块链自身安全特性分析

区块链系统不依赖第三方中介或信任机构，系统中所有参与节点都是平等的，所有节点共同进行决策，验证交易的合法性。即使系统中部分节点遭到攻击和破坏，也不会对整个区块链系统造成破坏[18]。与此同时，区块链通过加密机制、数字签名等技术保证信息的可追溯性和不可窜改性。

即便如此，区块链仍然面临着诸多安全威胁。以比特币采用的 PoW 机制为例，采用文献[1]中的攻击模型来分析区块链潜在的被攻击风险，诚实链和攻击链之间的演进可以用二叉树随机漫步过程来描述，而攻击者成功消除既定 z 个区块差距的概率问题则类似于赌徒破产问题。因此攻击者成功追赶上诚实链的概率计算方法如下：

$$q_z=\begin{cases}1, p\le q\\ \left(\dfrac{q}{p}\right)^2, p>q\end{cases} \tag{1}$$

式中 p 和 q 分别为诚实节点和攻击节点获取下一区块记账权的概率，且 $p+q=1$。

攻击者的区块延伸长度符合泊松分布，其期望值为

$$\lambda=z\frac{q}{p} \tag{2}$$

将攻击者区块延伸长度分布的概率密度与该情况下攻击者依然成功追赶上诚实链的概率相乘，可得攻击者的篡改成功概率 q_s 为

$$q_s=\sum_{k=0}^{\infty}\frac{\lambda^k e^{-\lambda}}{k!}\begin{cases}(q/p)^{(z-k)}, k\le z\\ 1, k>z\end{cases} \tag{3}$$

为了说明攻击者的篡改成功率与区块差距 z 、

攻击节点获取下一区块记账权的概率 q 之间的关系，本文采用 Matlab 进行仿真，实验结果如图 2 所示。可见攻击者的篡改成功率随着区块差距 z 的增大呈指数趋势下降趋势，同时可以发现在区块差距相同时，区块伪造成功率随着攻击者伪造能力(计算能力)的提高急剧上升。而当攻击者掌握全网 50%以上的算力时，就可以通过重新计算已确认的区块或控制新区块的产生，实现双重支付、阻止交易的确认和阻止其他节点产生新区块。

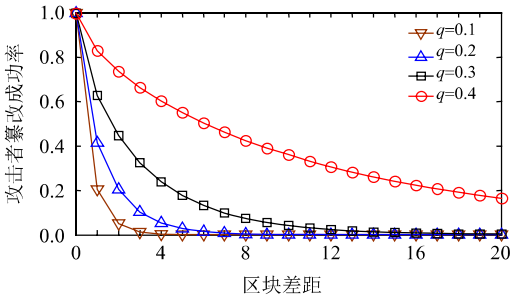

图 2 篡改成功率

Fig. 2 Tamper success rate

3.2 区块链面临的安全挑战和应对策略

1）私钥丢失。区块链上的信息具有不可篡改性，但这是以私钥安全为前提的。目前普遍采用的私钥存储方案是由区块链系统中每个用户自行将私钥加密后保管在用户设备上，但是这种方法无法抵抗攻击者在获取用户设备后对其使用离线字典攻击，因此区块链面临私钥被窃取的风险。总的来说，目前尚缺少私钥认证所需的可信环境，区块链的分布式存储结构也不利于私钥的补发管理。

为了防止私钥丢失，可以采用秘密共享机制对节点私钥进行保护。在图 3 所示的(t，n)秘密共享

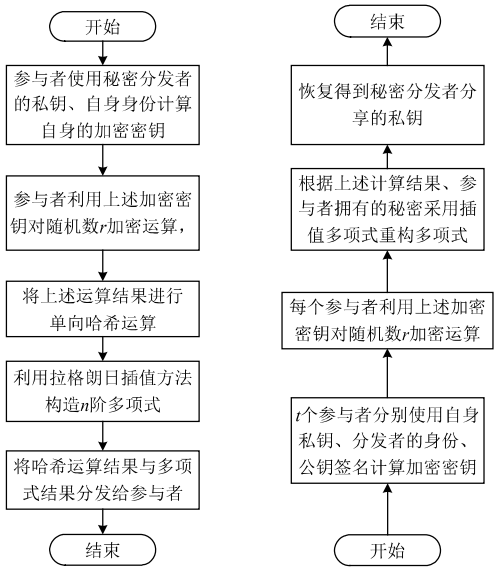

图 3 私钥分享与重构

Fig. 3 Private key sharing and refactoring

私钥保护方案中，将节点私钥分成 n 份，由 n 个参与者共同保存，只有当 t 个及 t 个以上参与者共同合作才能重构私钥[19-20]。在秘密共享过程中，各参与者使用其身份标识自身的私钥份额，并使用自身的私钥作为秘密份额，可以在秘密分发的同时进行秘密份额的分发，事先无须进行任何处理。私钥重构过程中，为防止各个参与者之间的相互欺骗，任意参与者均可验证某参与者提交的份额是否有效，重构中也无需真正的秘密份额，因此既保证较高的处理效率，又无需维护安全通道。

为了说明上述机制的计算开销，基于 C++环境利用 Miracle 库提供的类函数进行仿真。表 3 给出了不同(t，n)组合下数字签名的请求时间。当秘密分发者数量 n 确定的情况下，私钥请求时间随着门限值 t 的增大显著升高；而当门限值 t 给定的情况下，分发者数量 n 对私钥请求时间的影响不大。为此，可根据能源互联网不同的应用需求，结合应用需要的安全性和运行效率，选择合适的门限值。

表 3 签名请求时间对比

Tab. 3 Comparison of signature request time ms

请求时间	t=3	t=(n−1)/2
n=5	366.6	379.8
n=7	365.2	420.7
n=9	367.4	457.6
n=11	369.2	570.5
n=13	368.3	685.4

2）隐私泄漏。目前区块链上传输和存储的交易数据都是公开透明的，比特币仅通过分隔开交易地址和地址持有人真实身份的关联这种“伪匿名”的方式对交易双方身份信息进行一定的隐私保护。然而通过地址 ID、IP 地址等信息仍然可以发现帐户和交易的关联性[21]。对于涉及众多能源子系统交易用户隐私的能源互联网来说，数据的公开显然不符合监管要求，尤其是敏感数据需要平衡隐私保护和合规监管。一方面应保护能源互联网各参与主体在区块链上的交易隐私，另一方面又要防止非法参与者利用其进行非法交易。

为加强各参与主体的隐私保护，可采取如下应对策略：一是由认证机构代理参与主体进行交易，从而避免参与主体的隐私和重要信息的泄露。二是限制交易数据的广播范围，将交易数据的传输限制在部分关键节点之间。三是设置相应的访问权限控制机制，对数据信息的读写进行控制。四是采用环签名、同态加密、零知识证明等技术，避免隐私

暴露。

3）协议攻击。区块链无论使用何种共识机制，都面临着一定程度的协议攻击问题。能源行业具有较强的垄断性，某些利益集团完全有可能拥有超过某种共识机制容错性的能力，从而使能源区块链面临着严峻的安全威胁。此外，当区块链的协议需要更新时，会出现某些节点无法获取新版本或无法及时获取新版本的问题，导致不同节点运行的协议版本不一致，进而带来硬分叉和软分叉的问题。硬分叉是指运行新版协议的节点判定为有效的区块，会被运行旧版协议的节点判定为无效，从而造成永久分裂；软分叉是指令现有的核验规则更加严格，使未更新协议版本的老节点产生一些无效的区块或交易，而运行新版协议的节点校验通过的区块也可被老节点接受，进而使老节点去主动更新协议，在该情形下最多会产生一些临时的小型分叉而已。图 4 为以 PoW 机制为例具有 60%算力占比的节点更新了协议版本后，硬分叉和软分叉对新版协议的支持情况对比。

为此，一方面应采用共识机制和现实监管相结合的方式，如通过资产抵押、法律监管等手段进行联合管控，对能源互联网各参与主体的准入进行严格把关。另一方面，在更新区块链的共识机制时，应避免产生硬分叉，尽可能使用软分叉。

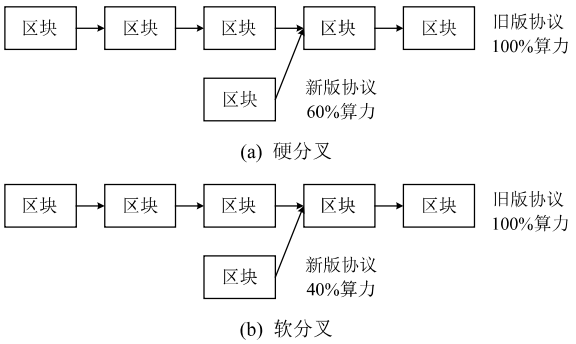

图 4　硬分叉和软分叉示意图

Fig. 4　Schematic diagrams of hard fork and soft fork

3.3　能源区块链的安全防护体系构建

能源区块链的安全性受加密算法、共识机制、使用场景、实现和系统等多方面因素的影响[22]。为应对能源区块链面临的各种安全挑战，如图 5 所示，提出以“结构＋本体＋管理”为基础，全面覆盖分区分域、边界防护、数据安全、应用安全、密钥安全、安全审计与预警、应急机制七个维度的全方位立体防护体系，同时安全防护必须贯穿能源区块链信息系统的全生命周期，从而有效适应未来能源区块链的发展需要。

图 5　能源区块链安全防护体系

Fig. 5　Security protection system of energy blockchain

3.3.1　结构安全

分区分域。未来能源互联网引入区块链技术后，可参考电力行业网络安全防护经验，综合考虑能源区块链承载业务的重要性、对能源子系统的跨度、涉及信息系统开放程度以及能源子系统自身安全性等因素对能源区块链信息系统进行恰当的分区，在安全分区内根据子系统的功能特点、业务范围进行适当的分域，实现能源企业内部网络、外网

与内网的逻辑隔离。

边界防护。结合能源区块链的分区情况，在各通信边界部署防火墙或其他访问控制设备，还可采用虚拟专用网等措施对能源区块链系统中的主机、网络设备等进行保护，加强能源区块链的边界防护。

3.3.2 本体安全

数据安全。能源区块链中交易节点首先应评估数据的重要程度、安全级别，再决定是否向全网广播该交易数据。应基于数据脱敏技术，针对性地构建脱敏算法库，对节点间交易数据进行脱敏，并建立用户隐私数据泄露风险的衡量模型，定性定量地衡量数据发生泄露的风险。结合能源区块链的用户认证体系、权限管理体系以及隐私数据不同保护级别的权限管理体系，实现对隐私数据基于审批制的数据访问机制。

应用安全。能源区块链本身的安全性并不能保证其上层应用的安全性。应用系统通常存在源代码预置漏洞或恶意代码、认证强度不足、数据明文传输等问题，且目前针对应用系统的攻击手段也比较繁杂。为此，应在应用系统上线前开展恶意代码检测，充分利用数据挖掘与机器学习技术，基于 PE 文件头、机器码字节序列等多维特征构建恶意代码特征提取方法，并结合有效的特征选择方法和分类器，提高恶意代码的检测精度与泛化能力，更早地发现未知恶意代码。基于 Fuzzing、二进制比对、静态分析与动态分析等多种漏洞挖掘技术，开展能源区块链上线前的预置漏洞挖掘，从而主动发掘并修补存在的漏洞，避免面临安全威胁。

密钥安全。能源区块链中密钥的存储、传输等安全风险依然存在，黑客可直接通过窃取用户私钥获得用户数据或者资产的控制权。以去中心化为主要特征的区块链也缺少私钥补发与管理机制，可以采用基于秘密共享的私钥保护技术，或基于物理安全的私钥硬件存储方案来对用户的私钥进行保护，从而确保能源区块链的安全。

3.3.3 管理安全

安全审计与预警。应对能源区块链系统重要用户行为、数据的读写、系统资源的异常使用进行审计，且审计范围应覆盖到区块链上的所有设备和系统。在此基础上，利用数据融合、数据挖掘和智能分析等技术，开展基于多源日志的网络安全态势感知要素获取，进行多源日志的关联分析、融合分析和态势要素分析，对能源区块链的网络安全状态进行分析评价，及时感知系统中的异常事件与整体安全态势，以便做出预警和风控措施。

应急机制。为了有效预防、及时控制和最大限度地消除网络攻击、恶意代码感染等各类突发网络安全事件的危害和影响，应针对能源区块链应用场景编制相应的应急预案，明确能源区块链各参与角色的职责与应急处理措施，定期开展应急演练，并在事后查找网络安全问题的来源和系统漏洞，加固安全措施，避免再次遭受攻击。

4 能源区块链发展相关建议

目前来看，能源区块链在全球范围内仍处于实践探索阶段，能源行业及各有关企业不可操之过急，应借助能源互联网等新兴市场带来的机遇，逐步探索其应用。能源区块链不仅面临技术层面的风险，还面临着监管治理层面的风险。二者兼顾才能有效保障各参与主体的利益。

1）出台能源区块链的相关扶持政策及治理措施。国家和能源监管部门应尽快建立健全能源区块链的相关扶持政策、技术路线以及治理措施，支持能源区块链的发展。制定能源区块链的技术层面和监管法规层面的治理规则，确保能源区块链健康发展。

2）加快关键核心技术攻关，组织开展能源区块链应用示范。加快共识机制、智能合约、分布式存储、数字签名等核心关键技术的攻关，研究安全策略更新、系统更新、数据结构更新等问题，研究数据加密和认证机制，为区块链技术在能源互联网中的应用提供安全保障[23-25]。针对区块链技术在能源互联网中的应用场景，开展可行性研究，研究应用区块链技术进行能源互联网价值传递、决算审计、电力结算等问题，探索形成能源区块链的应用推广模式。

3）制定能源区块链的相关标准。由国家和能源监管部门统一制定能源区块链的规范和标准体系。结合电力、石油、天然气以及交通运输网络等各行业标准体系，在通用区块链的标准基础上，完善融合后纳入到能源区块链的标准体系当中。建议从基础标准、支撑技术、可信和互操作、业务和应用、信息安全等五个方面考虑，建立能源区块链的标准体系框架，如图 6 所示。

4）建立能源区块链的投资效益评估机制。建议构建能源区块链的投资效益评估机制，从而对区块链在能源互联网中的投资、建设、运营和效益进

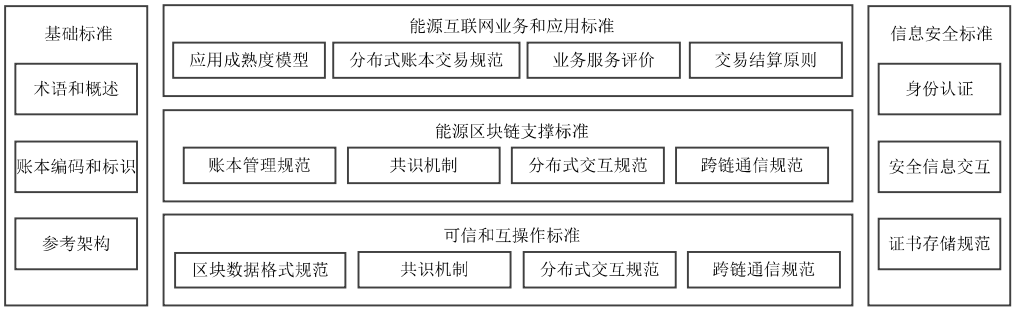

图 6　能源区块链标准体系架构

Fig. 6　Standard system framework of energy blockchain

行科学准确的评估，以此作为引导，优化后续区块链在能源互联网中的建设应用。同时建议在开展投资效益评估时，综合考虑各参与主体的价值，从而充分调动各方对能源区块链投资的积极性，促进能源区块链的发展。

5　总结

区块链技术的去中心化、开放、智能和共享与能源互联网的理念相吻合，业界普遍认为其在能源互联网中的应用将有效支撑多类型能源系统的开发互联和多用户的广泛深度参与。本文结合能源互联网的实际应用需求，对能源区块链的共识机制、加密算法和智能合约等关键技术进行对比分析。在此基础上，针对私钥丢失、隐私泄露和协议攻击等信息安全问题，提出相应的应对策略，并从结构安全、本地安全、管理安全三个方面构建能源区块链的安全防护体系。最后，给出了当前能源区块链的发展建议。希望本文的研究成果对解决区块链在能源系统中应用的信息安全问题提供一定的参考。需要指出，本文重点关注的是能源区块链的信息安全问题，未来有关能源区块链的交易性能、软硬件局限性、治理规则等问题还有待进一步深入地研究。

参考文献

[1] Nakamoto S．Bitcoin：a peer-to-peer electronic cash system[J]．Consulted，2009．

[2] Azaria A，Ekblaw A，Vieira T，et al．MedRec：using blockchain for medical data access and permission management[C]//Proceedings of the 2nd International Conference on Open and Big Data．Vienna，Austria：IEEE，2016．

[3] 阿尔文德·纳拉亚南，约什·贝努，爱德华·费尔顿，等．区块链：技术驱动金融[M]．林华，王勇，帅初，等译．北京：中信出版社，2016．

[4] 孙宏斌，郭庆来，潘昭光，等．能源互联网：驱动力、评述与展望[J]．电网技术，2015，39(11)：3005-3013．
Sun Hongbin，Guo Qinglai，Pan Zhaoguang，et al．Energy internet：driving force，review and outlook[J]．Power System Technology，2015，39(11)：3005-3013(in Chinese)．

[5] 曾鸣，杨雍琦，李源非，等．能源互联网背景下新能源电力系统运营模式及关键技术初探[J]．中国电机工程学报，2016，36(3)：681-691．
Zeng Ming，Yang Yongqi，Li Yuanfei，et al．The preliminary research for key operation mode and technologies of electrical power system with renewable energy sources under energy internet[J]．Proceedings of the CSEE，2016，36(3)：681-691(in Chinese)．

[6] 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(in Chinese)．

[7] 李彬，曹望璋，祁兵，等．区块链技术在电力辅助服务领域的应用综述[J]．电网技术，2017，41(3)：736-744．
Li Bin，Cao Wangzhang，Qi Bing，et al．Overview of application of block chain technology in ancillary service market[J]．Power System Technology，2017，41(3)：736-744(in Chinese)．

[8] 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(in Chinese)．

[9] 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．
Wang Anping，Fan Jin'gang，Guo Yanlai．Application of blockchain in energy interconnection[J]．Electric Power Information and Communication Technology，2016，14(9)：1-6(in Chinese)．

[10] Aitzhan N Z，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(99), doi: 10.1109/TDSC.2016.2616861(in Press).

[11] 慈松. 能量信息化和互联网化管控技术及其在分布式电池储能系统中的应用[J]. 中国电机工程学报, 2015, 35(14): 3643-3648.
Ci Song. Energy informatization and internet-based management and its applications in distributed energy storage system[J]. Proceedings of the CSEE, 2015, 35(14): 3643-3648(in Chinese).

[12] 马钊, 周孝信, 尚宇炜, 等. 能源互联网概念、关键技术及发展模式探索[J]. 电网技术, 2015, 39(11): 3014-3022.
Ma Zhao, Zhou Xiaoxin, Shang Yuwei, et al. Exploring the concept, key technologies and development model of energy internet[J]. Power System Technology, 2015, 39(11): 3014-3022(in Chinese).

[13] 田世明, 栾文鹏, 张东霞, 等. 能源互联网技术形态与关键技术[J]. 中国电机工程学报, 2015, 35(14): 3482-3494.
Tian Shiming, Luan Wenpeng, Zhang Dongxia, et al. Technical forms and key technologies on energy internet[J]. Proceedings of the CSEE, 2015, 35(14): 3482-3494(in Chinese).

[14] Kraft D. Difficulty control for blockchain-based consensus systems[J]. Peer-to-Peer Networking and Applications, 2016, 9(2): 397-413.

[15] Sasaki Y, Wang Lei, Aoki K. Preimage attacks on 41-step SHA-256 and 46-step SHA-512[R]. IACR Cryptology ePrint Archive, 2009, 479-494.

[16] 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(in Chinese).

[17] 朱建明, 付永贵. 基于区块链的供应链动态多中心协同认证模型[J]. 网络与信息安全学报, 2016, 2(1): 27-33.
Zhu Jianming, Fu Yonggui. Supply chain dynamic multi-center coordination authentication model based on block chain[J]. Chinese Journal of Network and Information Security, 2016, 2(1): 27-33(in Chinese).

[18] Bradbury D. The problem with Bitcoin[J]. Computer Fraud & Security, 2013, 2013(11): 5-8.

[19] 张子振, 毕殿杰. 一种基于秘密分享的认证中心私钥保护方案[J]. 计算机系统应用, 2011, 20(1): 62-65.
Zhang Zizhen, Bi Dianjie. Protection for CA private key based on secret sharing scheme[J]. Computer Systems & Applications, 2011, 20(1): 62-65(in Chinese).

[20] 庞辽军, 李慧贤, 王育民. 基于 LUC 密码体制防欺诈的秘密共享方案[J]. 电子科技大学学报, 2007, 36(1): 108-111.
Pang Liaojun, Li Huixian, Wang Yumin. A secret sharing scheme with ability to identify cheaters based on LUC cryptosystem[J]. Journal of University of Electronic Science and Technology of China, 2007, 36(1): 108-111(in Chinese).

[21] Zyskind G, Nathan O, Pentland A S. Decentralizing privacy: using blockchain to protect personal data[C]// Proceedings of 2015 IEEE Security and Privacy Workshops(SPW). San Jose, USA: IEEE, 2015.

[22] Alam M T, Li H, Patidar A. Notice of violation of ieee publication principles bitcoin for smart trading in smart grid[C]//Proceedings of the 21st IEEE International Workshop on Local and Metropolitan Area Networks. Beijing: IEEE, 2015: 1-2.

[23] 颜拥, 赵俊华, 文福拴, 等. 能源系统中的区块链: 概念、应用与展望[J]. 电力建设, 2017, 38(2): 12-20.
Yan Yong, Zhao Junhua, Wen Fushuan, et al. Blockchain in energy systems: concept, application and prospect [J]. Electric Power Construction, 2017, 38(2): 12-20(in Chinese).

[24] Ron D, Shamir A. Quantitative analysis of the full bitcoin transaction graph[M]//Sadeghi A R. Financial Cryptography and Data Security. Berlin, Heidelberg: Springer, 2013: 57-59.

[25] 李彬, 张洁, 祁兵, 等. 区块链: 需求侧资源参与电网互动的支撑技术[J]. 电力建设, 2017, 38(3): 1-8.
Li Bin, Zhang Jie, Qi Bing, et al. Block chain: supporting technology of demand side resources participating in grid interaction[J]. Electric Power Construction, 2017, 38(3): 1-8(in Chinese).

丁伟

收稿日期: 2017-02-27。

作者简介:

丁伟(1991), 男, 工学硕士, 助理研究员, 主要从事电力信息与通信、信息安全方面的研究工作, dingwei@csg.cn;

王国成(1993), 男, 硕士研究生, 主要从事电力信息与通信方面的研究工作, 445830120@qq.com;

许爱东(1977), 男, 教授级高级工程师, 主要从事电力系统自动化方面的研究工作, xuad@csg.cn。

(责任编辑 乔宝榆)

 DOI：10.13334/j.0258-8013.pcsee.170353

Research on Key Technologies and Information Security Issues of Energy Blockchain

DING Wei[1], WANG Guocheng[2], XU Aidong[1], CHEN Huajun[1], HONG Chao[1]

(1. Electric Power Research Institute, CSG; 2. North China Electric Power University)

KEY WORDS: energy blockchain; consensus mechanism; information security; secret sharing; security protection

The characteristics of blockchain, i.e. decentralization, openness, intelligence and sharing, are consistent with the spirit of energy internet. Its application in energy internet will effectively support the interconnection of multiple types of energy systems, and the extensive participation of a wide range of users. This paper mainly discusses the key technologies and information security issues of energy blockchain.

This paper analyzes the technical requirements of energy internet firstly. Energy internet currently exposes many risks, including transaction efficiency, information security, and the protection of the principal's rights and interests. The adaptability of blockchain in energy internet is analyzed from two aspects, feasibility and necessity. On this basis, this paper puts forward the concept of energy blockchain. According to the demand and development trend of energy internet, the key technologies of blockchain such as consensus mechanism, security algorithm and intelligent contract are analyzed.

In order to ensure the security of energy blockchain, the security characteristics of blockchain itself are analyzed. Taking the PoW mechanism used in bitcoin as an example, this paper illustrates the relationship between tamper success rate and block gap by modeling the potential attack risk, which can be seen in Fig. 1. When more than 50 percent of the network power is obtained, the attacker can realize double payment, and prevent the transaction confirmation and the production of new blocks by recalculating the confirmed blocks or controlling the generation of new blocks.

This paper emphatically analyzes the security challenges and corresponding strategies of energy blockchain from three aspects including private key lost, privacy disclosure and protocol attack. A secret sharing mechanism is proposed to protect the private key. The simulation study shows that, the request time of private key is related to the threshold value rather than the number of private key distributors. In order to strengthen the privacy protection of each participant, some solutions are put forward to prevent privacy leak, such as limiting the broadcast range of transaction data, setting access rights control mechanism and so on. Furthermore, this paper makes a comparison on hard fork and soft fork to avoid protocol attack.

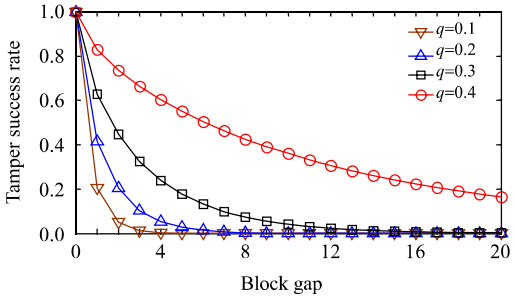

Fig. 1 Tamper success rate

The security of energy blockchain can be affected by many factors, such as encryption algorithms, consensus mechanisms, usage scenarios, implementation and system, etc. To address the various security challenges facing by the energy blockchain, a comprehensive and three-dimensional security protection system which is based on structure security, ontology security and management security is built. The security protection system fully covers seven dimensions of network partition, border protection, data security, application security, key security, security audit and warning, and emergency mechanism. Finally, some suggestions on the development of energy blockchain are given.

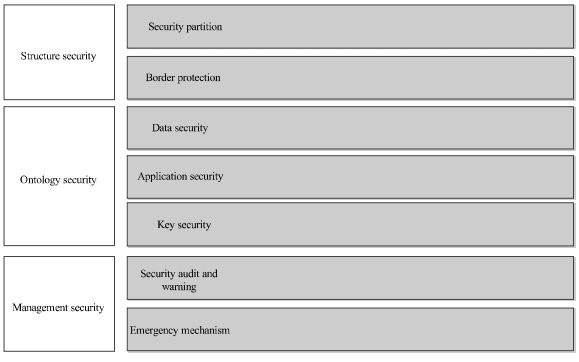

Fig. 2 Security protection system of energy blockchain