文章编号：1000-3673（2020）03-0953-09 中图分类号：TM 721 文献标志码：A 学科代码：470·40

一种面向分布式新能源网络的终端安全接入技术

梅文明[1,2]，李美成[1]，孙炜[2]，余文豪[3]

（1. 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；
2. 国家电网有限公司，北京市 西城区 100031
3. 中国电力科学研究院有限公司，北京市 海淀区 100192）

Terminal Security Access Technology for Distributed New Energy Networks

MEI Wenming[1,2], LI Meicheng[1], SUN Wei[2], YU Wenhao[3]

(1. State Key Laboratory of Alternate Electrical Power System With Renewable Energy Sources (North China Electric Power University), Changping District, Beijing 102206, China;
2. State Grid Corporation of China, Xicheng District, Beijing 100031, China;
3. China Electric Power Research Institute, Haidian District, Beijing 100192, China)

ABSTRACT: In the context of the application of distributed new energy into the grid, there appears a risk of centralization of security protection solutions. Aiming at this problem, this paper proposes a terminal secure access technology for distributed new energy networks. First, the security model is analyzed in depth, and the feasibility and the implementation method of constructing identity authentication and access control services based on the blockchain are proposed. And then the identity authentication model and access control model are designed based on the actual application scenario, and the evaluation of terminal trust is suggested. Then on this basis, a blockchain-based terminal secure access scheme is proposed, and the application mode and the scheme flow are described in detail. The experimental results show that the scheme can effectively combat the single point risk of the new energy grid security scheme and has a better performance.

KEY WORDS: distributed new energy; terminal security access; blockchain; identity authentication; access control

摘要：在分布式新能源并网的应用背景下，安全防护方案存在中心化的风险。针对这一问题，该文提出一种面向分布式新能源网络的终端安全接入技术。首先对安全模型进行深入分析，提出基于区块链构建身份认证和访问控制服务的可行性和实施方法，进而结合实际应用场景设计了身份认证模型和访问控制模型，并提出了终端信任度的评估方法。然后在此基础之上提出基于区块链的终端安全接入方案，详细描述了应用模式和方案流程。实验结果表明，该方案能够有效对抗新能源电网安全方案的单点化风险，并具有良好的性能。

关键词：分布式新能源；终端安全接入；区块链；身份认证；访问控制

DOI：10.13335/j.1000-3673.pst.2019.2366

0 引言

新能源是区别于传统能源的新型能源形式，如风能、太阳能、生物质能等，是未来电网发展的重要趋势，对国计民生具有重大的战略意义。随着新能源产业的不断壮大，新能源场站规模呈快速增长的态势，在国家电网的发展中处于越来越重要的地位[1-3]。

随着越来越多新能源场站的建设和入网，新能源场站的网络安全风险日益突出。新能源场站面临的主要安全威胁包括终端接入风险、远程运维风险、场站监控中心网络外连、物理安全风险、系统本体安全风险和人员管理风险等。其中，在分布式新能源并网的新型网络架构下，由于场站分布广，终端数量庞大，恶意终端的接入会造成网络攻击能够更快更广地蔓延，从而导致更加严重的电网事故。例如，在新能源场站内部，攻击者能够通过物理突破风机进行终端接入，进而展开大规模的网络渗透[4]。在场站外部，攻击者可以从互联网端发起对场站信息管理区、发电集团集控中心和第三方运维中心的攻击，实现对监控数据的篡改或破坏。因此，针对分布式新能源网络的终端安全接入技术具有很高的研究价值和研究意义。如何实现海量终端设备的安全接入是构建泛在电力物联网安全防护体系的一个重要环节。

目前，面向电网的终端安全接入技术分为 3 个防护维度：一是终端层的安全，需要采取安全措施对终端的软硬件进行加固，例如采用基于安全芯片的可信计算技术；二是通道安全，需要解决终端接

入过程的信道安全，采用的技术主要有身份认证技术、访问控制技术、加密隧道技术，这些技术均需要密码作为支撑；三是站控层的安全，需要在该层面部署各种安全系统为电网的终端连接提供各种安全服务，如身份认证系统，数据交换系统，集中监管系统等。在上述的安全方案中，身份认证、安全通道和访问控制是最接近于实用化的安全技术，但传统的安全方案存在严重的中心化风险。身份认证和安全通道的建立依赖于传统的公钥基础设施(public key infrastructure，PKI)。而目前集中式的 PKI 系统存在 3 大安全问题[5]：单点失效问题，证书颁发机构(certificate authority，CA)易受攻击问题，中心渎职问题。在访问控制方面，传统的访问控制机制存在策略决策中心化和访问控制单点化的问题，这些问题会导致中心化的安全方案成为分布式新能源网络结构的安全突破口，一旦安全中心被突破，终端接入的安全基石将不复存在。因此，急需研究一种面向分布式新能源并网的终端安全接入技术，解决终端安全接入的集中式风险。目前，相关研究者已经提出基于区块链技术[6-8]实现更加健壮安全的身份认证[9-15]和访问控制[16-20]研究。

本文分析分布式新能源并网的安全需求，并以此为牵引，提出一种面向分布式新能源网络的终端安全接入技术，建立终端安全接入的信任契约，实现跨域分布式的身份认证和访问控制，解决中心化带来的安全风险。本文针对分布式能源网络的特点，结合现有的研究成果，设计基于区块链的终端接入认证和访问控制模型，进而提出终端的信任度评估算方法，设计基于区块链的终端接入流程，以 Hyperledger Fabric 为基础，搭建实验环境，模拟多终端跨域接入网络的行为，验证上述方案的可行性。

1 模型设计

1.1 安全模型设计

本文探索在大规模分布式新能源场站并网的情况下，如何构建分布式的 PKI 体系，实现更加健壮的身份认证和访问控制服务。该服务不仅能够解决跨域认证的问题，也能够为场站内部的终端接入提供服务。安全服务模型如图 1 所示，新能源场站的认证访问控制服务跨域互联，形成具有高安全分布式属性的电力系统终端接入的管控网络。本文提出的安全服务模型分为 2 个维度：一是跨域终端接入安全，重点解决不同能源场站与调度中心、发电集团集控中心、第三方运维中心之间的终端安全接入问题；二是站内终端安全接入安全，解决场站内部的终端安全接入问题。

目前，新能源的网络平面存在 2 种连接方式。一是调度中心和各场站的生产控制区，基于 SGDnet 和纵向加密装置的连接，各场站之间并不连接，本文称之为生产控制网络平面。二是发电集团集控中心、第三方运维中心基于 Internet 与场站的信息管理区进行互联，各场站之间通用不需要互联，本文称之为信息管理网络平面。按照目前的场站互联网络架构，PKI 基础设施的核心机构 CA 只能采取集中式的部署方法。在生产控制平面，由场站自身构建，实现场站内部的身份认证和访问控制；由调度中心统一构建、实现统一的身份和访问策略管理，进而实现场站内部的身份认证和访问控制。在信息管理网络平面，由场站自身构建，实现场站内部的身份认证和访问控制；由集控中心或运维中心提供，实现统一身份和访问管理。因此，无论在哪个网络平面，均无法规避单点化的安全基础设施带来的安全风险。

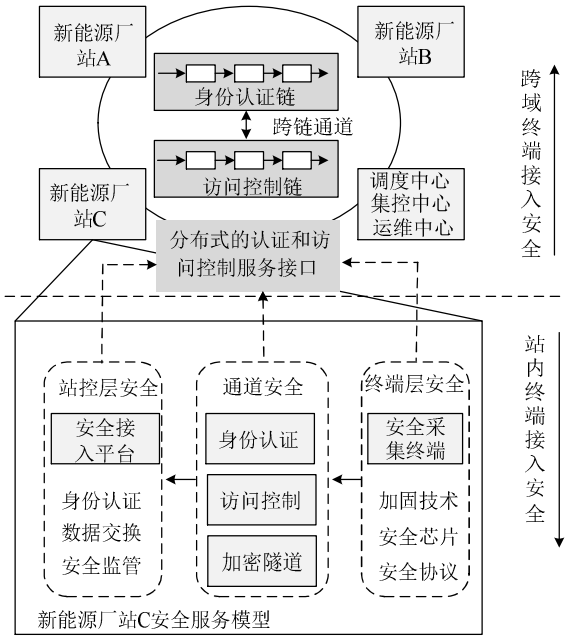

图 1 安全服务模型

Fig. 1 Security service model

区别于传统集中式的安全防护措施，本文的安全服务模型基于 2 个能够跨链互连的区块链系统，身份认证链和访问控制链。其中，身份认证链提供基础的分布式的 PKI 服务，由各新能源场站和安全管控机构提供节点组成。访问控制链在身份认证链的基础上，提供终端接入时的访问控制服务，终端对任何资源的访问都由访问控制链决策实施，任何节点都无法单方面篡改访问控制策略。区块链系统提供分布式的认证和访问控制服务接口，网络的所

有参与者均可以调用该接口获取安全服务。

基于区块链实现分布式的访问控制与身份认证的账本，具有多种优势：提高安全中心的抗打击能力；增强终端接入相关审计数据的抗毁能力；能够让各场站之间感知到其他场站或者运维中心存在安全风险，例如，多个场站同时感受到某个场站存在非法终端接入的安全问题，就能够对该场站实施脱网处置，防止场站内部的安全风险向运维中心和其他场站扩散。

实现基于区块链的分布式安全服务的方法有多种，但必须保证 2 个方面：一是区块链节点由不同的信任主体维护，二是每个场站能够快速接入区块链服务。因此基于各个场站去构建区块链服务是一个可行且方便的思路。这里强调的是安全服务的互通互联，而不是新能源场站之间的互通互联。因为区块链的引入客观上可能增加通信安全问题，比如当前的新能源场站并未实现互联，而在区块链的架构下，场站之间存在互联的信道，安全风险可以从场站直接向另一个场站渗透。我们可以对区块链节点之间的通信进行严格的管控，例如封闭所有和区块链服务无关的端口，增强流量异常检查，采用多种安全防护手段保证场站之间只有区块链的节点可以互相通信等。

本文提出的基于区块链的安全服务模式是一种广义上的概念，在实际部署时，需要根据安全服务所需要支持的网络平面进行灵活的设计和部署。

在生产控制网络平面，由调度中心提供多个区块链节点，由新能源场站提供节点，并且新能源场站的区块链数据同步需要经过调度中心信息数据转发，最终构建分布式的安全服务。这种设计弱化了区块链在通信层面的去中心化的概念，但是有意义的，一方面各场站的安全服务节点能够形成对中心服务的监督，可以发现中心安全服务作恶的行为，及时告警；另一方面，可以通过设计合理的密码学协议保证中心只能转发数据，而不能解密或篡改数据，安全中心在网络通信层面的作恶同样会被发现。在信息管理网络平面，由于该平面基于 Internet 互相连接，因此可以实现场站之间的互联互通，保证该层面的区块链安全服务直接是真正的 P2P 的通信。在这种网络假设下，终端在该平面的接入安全将由更加健壮的分布式安全服务保证，防止由于安全服务不可信带来的非法接入情况。另外，可以进一步设计一种分布式抗毁的监控数据存储系统，将场站监控数据保存在区块链接点中，可防止因发电集团集控中心和第三方运维中心(数据中心)被黑客攻击破坏，对监控数据的可靠性和完整性带来的威胁。但数据服务不是本文研究点，不作进一步延伸。

1.2　基于区块链的认证模型

基于区块链的认证模型如图 2 所示，模型描述分为 2 个层次：一是基础服务层，二是协议流程层。

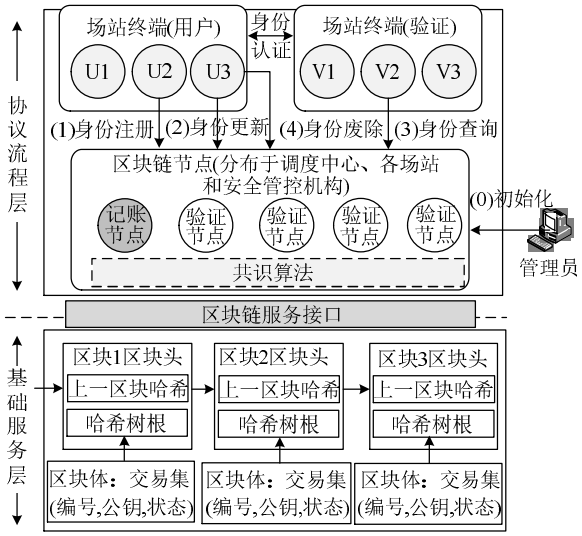

图 2　基于区块链的认证模型

Fig. 2　Blockchain-based authentication model

基础服务层维护基础的区块链数据结构，各数据区块以哈希链的方式前后相连。数据区块分为区块头和区块体，其中区块头存储上一区块的哈希值，并记录该区块的哈希树根，这样就形成了不可篡改的数据记录。区块体是交易集合，在应用于身份认证场景是，通常包括身份编号(identity，ID)，公钥(public key，PK)和状态(用于说明该公钥是否有效)。在本文的认证模型中，利用区块链技术实现分布式的公共账本，将用户身份和证书公钥关联，构建去中心化的 PKI 系统。由于任何用户都可以查看证书的签发过程，解决了传统 PKI 体系面临的 CA 单点化问题和证书不透明的问题。

协议流程层定义了基于区块链的认证模型在面向分布式新能源并网环境下的运行流程。与目前基于区块链构建 PKI 的解决方案不同，本文引入了管理员对区块链系统进行初始化操作，对参与组成 PKI 系统的节点进行身份定义。该设计原因在于，身份认证是网络系统信任关系建立的出发点，必须由管理员作为可信方参与进来，才能给分布式的 PKI 节点建立业务逻辑上的关联。结合实际应用场景描述如下：

1）初始化。各新能源场站和安全管控机构提供计算节点，用于组成分布式的 PKI 认证系统。管理员将各 PKI 节点的公钥组成 PKI 服务成员列表，

用外置硬件导入的方式，下发到每一个参与构成PKI服务的计算节点。完成分布式PKI的初始化。具体而言，参与组成PKI认证系统的节点包括调度中心、各场站和安全管控机构，确保分布式认证服务由分布式新能源场景的各参与方共同组成并维护。

2）身份注册。电力网络中的终端生成用户信息，并向PKI系统广播注册。其中，位于生产控制网络平面和在信息管理网络平面的终端分别向各自网络平面的区块链认证系统发起注册请求。信息包括节点类型(如站控系统，采集终端，安全设备等)和节点身份(ID，PK)。各区块链节点对该提议进行验证，并由本阶段的区块链记账节点将注册信息打包到新区块中，进而被全网验证通过，完成注册。

3）身份更新。电力网络中的终端生成新的公钥信息，并附上新公钥对旧公钥的所有权证据。该请求经过共识后写入区块链系统，原公钥的状态变更为失效。

4）身份查询。验证者通过遍历区块链账本获取所要查询节点的身份是否合法。在实际应用时，通常会维护一个状态数据库对区块链账本进行实时解析，从而提高查询的效率。

5）身份废除。触发身份废除有2种类型。一种是节点主动发送消息，申请对本节点身份的废除。另一种是访问控制链判断某节点存在严重的异常行为，经过跨链通道发送消息到PKI系统，申请对某节点身份的废除。

总之，基于区块链实现新能源并网环境下的PKI从结构上更符合分布式网络的特点，能够为海量的电网设备和控制节点提供安全可靠的身份认证服务。在本文其余部分的描述中，我们将本节提出的模型抽象成一个独立的认证服务，不再强调分布式的特点。

1.3 基于区块链的访问控制模型

本文对基于属性的访问控制模型进行了扩展，用区块链交易的形式对访问控制策略进行管理，基于区块链的访问控制模型如图3所示。其中交易类型包括2种：一种是策略创建交易(policy creation transaction，PCT)，另一种是权限转移交易(right transfer transaction，RTT)。PCT用于实现策略的创建、更新和撤销，而RTT用于实现用户之间的权限转移。基于区块链进行权限和策略的交易能够形成分布式不可篡改的日志审计功能，有效对抗各参与者的欺诈行为。

例如，某厂站站控系统A拥有对采集终端P的

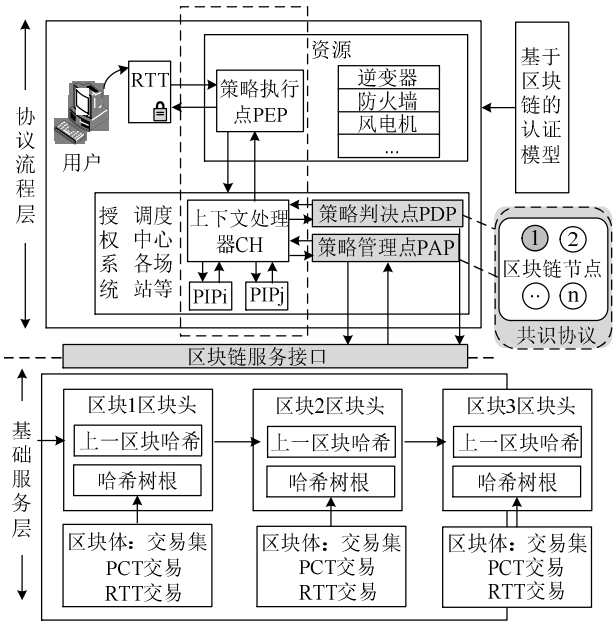

图3 基于区块链的访问控制模型

Fig. 3 Blockchain-based access control model

控制权，并将采集终端访问控制策略设置为所有具有该场站F部门成员都可以访问采集终端P，并进行相关设置。假设3种场景：1）站控系统将终端P的访问管理策略修改为只有E部门管理员可以访问终端P，此时需要创建的交易类型是PCT；2）如果站控系统A将自己拥有的管理权限转移给站控系统B，此时需要创建的交易类型是RTT，一旦RTT交易被确认，B将拥有同样的权限；3）M部门的成员尝试连接到采集终端P，但由于区块链上的策略定义是只允许F部门成员，因此该接入申请将被拒绝。

上文的例子直观给出了该访问控制模型的功能效果，进而对基于区块链的访问控制模型的一般性工作流程进行定义。需要说明的是，虽然分布式新能源环境中的终端类型很多，访问请求的类型多样，但是其过程和数据格式相似，都可以抽象为用户对某种资源的访问，这在访问控制决策方面是相同的。具体的流程为：

1）用户发送资源访问请求，由策略执行点(policy execution point, PEP)将该请求转发给上下文处理器CH。需要说明的是，上下文处理器一般要求和策源处于同样的计算环境，但是对于低功耗的嵌入式设备，由于计算资源有限，这2个部件可以分离。被访问的资源为新能源场站中的设备，如逆变器，防火墙，风电机等，只有具备访问管理使用权限的用户才能够安全接入这些设备。

2）CH向策略管理点(policy admin point，PAP)发送策略查询请求，由PAP基于请求中的资源权

限，并从区块链中检索并得到该资源拥有者签发的所访问控制策略。其中，CH、PAP 和策略信息点(policy information point，PIP)由调度中心、各场站和安全管控机构提供节点组成分布式访问控制服务。

3）PAP 将检索策略进行整合，以标准策略的格式返回给 CH。PAP 是由多个区块链节点组成，只有足够多的 PAP 节点签发的策略，CH 才判定是有效的。

4）CH 向策略信息点 PIP 检索属性，并将该请求转发到策略判决点(policy determine point，PDP)。

5）PDP 对访问控制进行判决，并将判决结果返回到 CH。PDP 同样由多个区块链节点组成，只有大多数 PDP 节点进行了同样的决策，才是有效的。

6）CH 收集到足够的判决结论后，将判决结果转发回 PEP，由 PEP 实施访问控制。

1.4　终端信任度评估方法

本节以 1.1 节安全模型设计，1.2 节基于区块链的认证模型和 1.3 节基于区块链的访问控制模型为基础，提出终端接入时的信任度评估方案，以此为依据对终端的接入行为进行判决。对核心组成部分与核心函数方法进行半形式化定义。

给出各核心组成部分的定义：

定义 1：基于区块链的认证模型。

AuthChain：($AU_1 \rightarrow AU_2 \rightarrow \cdots \rightarrow AU_n \rightarrow \cdots$)

式中 AU_i 为包含身份认证信息的区块。

定义 2：基于区块链的访问控制模型。

AccessChain:($AC_1 \rightarrow AC_2 \rightarrow \cdots \rightarrow AC_n \rightarrow \cdots$)

式中 AC_i 为包含访问控制信息的区块。

定义 3：节点 i 的历史行为记录。

H_i={ID，PK，HAB{}，AB{}，Owner}

式中：ID 为节点编号；PK 为节点公钥；HAB 为 historical abnormal behavior，默认值为 NULL，记录节点 i 的异常行为；AB 为 access behavior，默认值为 NULL，记录节点的访问行为；Owner 为节点拥有者。

定义 4：节点 i 的访问请求。

R_i={ID，PK，RA{}，Owner}

式中 RA 为 requested access，记录节点 i 本次的访问请求。

定义 5：网络中可信任节点的集合。

T={T_1{}，T_2{}，T_3{}，…，T_n{}}

式中：T_i{}={ID，PK，Owner，E-time，F-time}；E-time 为 effective time,记录该节点在信任列表中的生效时间；F-time 为 Failure time，记录该节点在列表中的失效时间。

给出各核心函数方法的定义：

定义 6：Verify_Identity(ID，PK，AuthChain)为身份合法性验证函数，向 AuthChain 查询节点提供的身份是否合法。

定义 7：Verify_Access(ID，PK，R_i，AccessChain)为访问合法性验证函数，向 AccessChain 查询节点的访问请求是否合法。具体方法是检查节点是否在信任节点集合 T 中，并且授权是否过期。若节点在集合 T 中，且授权未过期，则进一步验证该节点是否有对申请资源的访问权限，并进行细粒度的权限申请判决。

定义 8：Apply_Join(ID，PK，Re)，新节点 i 申请对某资源 Re 的访问权限。核心是对集合 Hi 进行检查。首先验证 ID 和 PK 是否有效；然后检查 HAB{}集合中有无异常行为，若有，则需要进一步确认异常行为是否得以解决；然后检查 AB{}，对节点 i 的历史访问行为进行关联分析，判断该节点常访问的节点是否存在异常，并根据实际安全策略进行更深入的分析检查；最后得出是否同意该节点加入网络的决策，更新 AccessChain。

2　基于区块链的终端安全接入方案

2.1　总体框架

面向分布式新能源并网的网络环境是复杂的，其中包括专网、公网、卫星、无线等多种通信手段。本文首先假设该网络已进行了合理的网络分区，并设置了有效的身份属性和访问控制规则。例如，信息管理大区和生产控制大区之间存在安全隔离装置，防火墙能够有效隔离不同的生产区域。本文的终端安全接入方案的目标是对终端的跨域和站内互联接入行为进行高效可靠的管控。

本文在第 1 节中对核心模型进行了设计，本节将在此基础上，提出基于区块链的终端安全接入方案。总体框架如图 4 所示。

1）网络。

生产控制网络平面，由调度中心和新能源场站提供组成，通过电力通信链路 SGDNet 互联。信息管理网络平面，由发电集团集控中心、第三方运维中心和场站组成，通过 Internet 组成。在这个链路之上，承载基于 P2P 通信的身份认证链和访问控制链。这 2 个区块链系统由各能源场站和安全管控机构提供计算节点组成。每个计算平面分别运行一套身份认证和访问控制服务。

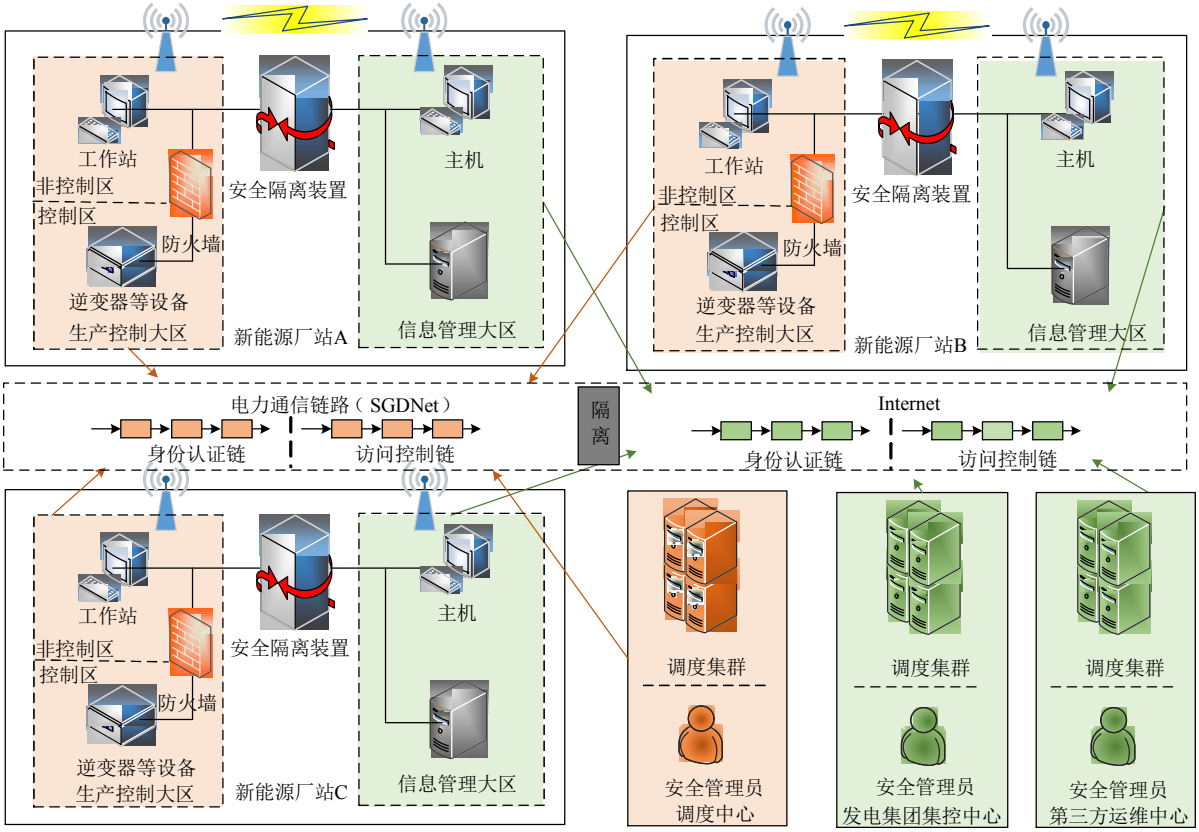

图 4　总体框架

Fig. 4　Overall framework

2）实体。

该框架下有 2 种参与实体。

一是新能源场站，根据业务和安全需求划分为信息管理大区和生产控制大区。2 个业务区域通过安全隔离装置进行隔离。在生产大区内部，又分为非控制区和控制区 2 类安全区域，分别运行工作站和逆变器等生产设备。生产控制大区属于生产控制网络平面，信息管理大区属于息管理网络平面。

二是安全管控机构，根据安全功能分为调度中心、发电集团集控中心和第三方运维中心。需要说明的是，调度中心属于生产控制网络平面，另外 2 个属于信息管理网络平面。运维中心提供的基于更强计算能力的安全监管和审计服务，并不是安全中心，在基于区块链的分布式认证和访问控制服务中，安全管控机构的地位和新能源厂站是相同的。

3）安全服务。

该框架下的安全服务特指基于区块链的身份认证和访问控制，二者以智能合约服务接口的形式为整个网络系统提供认证和访问控制基础支撑。其中，身份认证是访问控制的基础，安全服务的所有行为和决策都将记录到区块链当中，形成不可篡改的历史存证，能够极大提高分布式网络的安全性。

2.2　终端安全接入执行流程

在 2.1 节提出的总体框架之下，终端安全接入流程如图 5 所示，描述如下：

1）初始化阶段。各终端注册身份，初始化身份认证链和访问控制链。在生产控制网络平面，由调度中心提供多个区块链节点，由新能源场站提供节点。

2）终端接入申请。终端 A 发起对终端 B 的接入申请。需要说明的是，这里的终端是一个泛化的概念，不具体确认设备类型。这里可以是管理员对防火墙等安全装备的管理配置，也可以是场站工作人员对逆变器等电力生产设备的日常运维，也可以是安全中心收集设备运行状况数据。

3）终端 B 调用 Verify_Identity(ID，PK，AuthChain)，向区块链认证服务查询终端 A 的身份是否合法。

4）认证服务返回查询结果。若身份不合法，则拒绝 A 的接入申请。若合法，则进行步骤(5)。身份认证能够初步判断本次接入的安全性，例如，普通员工伪装成管理员，企图接入风电机，修改运行配置。身份认证可以成功阻断，并且该认证是可信可靠的。

5）终端 B 调用 Verify_Access(ID，PK，R_i，AccessChain)向区块链访问控制服务查询终端 A 的资源访问申请是否符合访问控制策略。

6）访问控制服务返回判决结果。

7）终端 B 根据判决结果决定是否接受 A 的接入申请。若判决通过，则进入步骤(8)；若判决不同过，则进入步骤(9)。访问控制判决能够对本次的权限请求进行细粒度的判决。例如，管理员需要对某核心防火墙进行安全规则配置，访问控制能够决策其是否有相应的权限。

8）双方建立安全连接。

9）用户 C 调用 Apply_Join(ID，PK，Re)申请对终端 B 的连接权限。例如，用户 C 只负责 1 号和 2 号风电机的管控，需要临时对风电机 3 号进行管控。此时，用户 C 需要申请对 3 号风电机的管控权限。这里的终端 B 就是 3 号风电机。

10）访问控制服务对用户 C 的历史行为进行审计，并对当前的访问权限申请进行判决，如果通过，则赋予用户 C 访问终端 B 的权限。根据访问类型、主体客体的区别，可以设置更加灵活的访问控制规则，以满足实际的业务需求。

3　实验验证

3.1　实验设计

对本文提出的面向分布式新能源网络的终端安全接入技术进行实验，以验证该方法的可行性。在该方案中，区块链是一种技术手段，因此不限制具体使用哪种区块链平台。

本文基于 Hyperledger Fabric1.4[21]搭建实验环境。Hyperledger Fabric 是 Linux 基金会所主导的 Hyperledger(超级账本)的项目之一，旨在作为开发模块化体系结构的区块链应用程序的基础，以便诸如共识和会员服务等组件可以即插即用。它使用容器技术来托管构成系统应用逻辑的智能合约(也称为链代码)。简而言之，Hyperledger Fabric 是为企业构建的领先的开源、通用区块链结构。

在 Ubuntu 16.04 系统下，利用 Docker 容器作为 Hyperledger Fabric1.4 的节点运行环境，然后安装 Docker 相关配置文件和 Go 语言的运行环境，进而模拟各用户和区块链服务。区块链容错能力设置为 2/3，也就是最多容忍 1/3 节点是恶意的。实验分为 4 个部分，首先对第一节设计的基于区块链的认证模型和访问控制模型进行验证，重点测试其吞吐量和服务延迟。然后基于上述 2 个原型系统，对终端安全接入的完整方案进行实验测试。最后模拟 3 个典型的攻击场景，进行安全性的分析。具体到本文的方案中，每一个新能源厂站可以看做一个 Org(Hyperledger 中信任组织的概念)。Client 是调用区块链服务的客户端，通过 invoke 方法调用智能合约接口，通过 event 消息监测特定的的区块链事件。

1）基于区块链的认证模型实验。

模拟 4 个 Org，并分别提供 2 个 Peer 组成区块链网络。每一个节点运行在 4 核 CPU，8GB 内存的 Ubuntu 虚拟机上。在身份认证的智能合约中分别定义身份注册、身份更新、身份查询和身份废除的函数接口，实现认证模型中的所有功能。分别测试 10 次取平均值。

①身份注册。

吞吐量为 516TPS，延迟为 912ms。

②身份更新。

吞吐量为 521TPS，延迟为 893ms。

③身份查询。

吞吐量为 1679TPS，延迟为 98ms。

④身份废除。

吞吐量为 532TPS，延迟为 889ms。

从实验结果分析可知，身份查询的性能明显优于其他 3 个，原因在于身份查询不需要经过区块链共识的过程，只需要查询解析区块链数据库即可。

2）基于区块链的访问控制模型实验。

模拟 4 个 Org，并分别提供 2 个 Peer 组成区块链网络。每一个节点运行在 4 核 CPU，8GB 内存的 Ubuntu 虚拟机上。在访问控制的智能合约中分别定义访问控制判决和新节点申请的函数接口，实现访问控制中的所有功能。分别测试 10 次取平均值。

①访问控制判决。

吞吐量为 1682TPS，延迟为 281ms。

②新节点申请。

吞吐量为 418TPS，延迟为 1293 ms。

从实验结果分析可知，访问控制判决过程只需要查询区块链系统，因此吞吐量较高。但是访问控制需要经过多点判决，因此带来额外的延迟开销。而新节点申请入网时需要经过历史记录检索与分析，并且需要经过区块链的共识过程，因此吞吐量较低，延迟较大。

3）终端安全接入完整方案实验。

模拟 4 个 Org，并分别提供 2 个 Peer 组成区块链网络。每一个节点运行在 4 核 CPU，8GB 内存的 Ubuntu 虚拟机上。另外，为了还原真实的网络环境，我们将网络延迟设置为 40 ms。模拟终端接入成功和接入失败后进行权限申请的过程。

①终端接入成功。

吞吐量为 1458TPS，延迟为 452ms。

②终端接入失败。

吞吐量为 328TPS，延迟为 1920ms。

我们可以看到，吞吐量和访问控制模型中的数据相近，因为访问控制是终端安全接入的核心且主要的流程。而增加网络延迟后，终端接入的延迟有了明显的上升。

另外，我们对 Fabric 的基础平台性能进行测了测试，作为对照组。在同样的节点配置情况下，运行简单交易范例：查询过程的吞吐量为 2130 TPS，延迟为 82 ms；共识过程的吞吐量为 612 TPS，延迟为 765 ms。因此，本文方案的系统开销主要取决于区块链基础性能。

4）攻击性实验。

和传统集中式的安全方案相比，本文引入区块链技术构建分布式身份认证和访问控制服务的核心优势在于对抗单点化带来的安全风险。因此，进行了 3 个典型的攻击性实验以证明本文方案的安全优势。假设在本文实验环境的 8 个验证节点中有 2 节点是恶意的。

场景 1：恶意用户串通恶意区块链节点，伪造用户身份，企图将恶意用户注册为某类型设备的管理员。

实验结果：在该用户申请访问设备时，2 个恶意区块链节点返回身份认证通过的结论，其余 6 个区块链节点返回身份认证失败的结论。由于没有收集到超过 2/3 的判决结论，最终，恶意用户身份认证失败。区块链具有多点共识的安全特性，少部分节点无法伪造数据。

场景 2：恶意用户串通恶意区块链节点，篡改某类型设备的访问控制策略，企图扩大用户的访问权限或者伪造访问权限。

实验结果：在该用户申请访问设备时，2 个恶意节点返回访问请求通过，其余 6 个区块链节点返回访问请求失败的结论。由于没有收集到超过 2/3 的判决结论，最终，恶意用户访问请求失败。区块链具有防篡改的安全特性，少部分节点无法修改链上存储的访问控制策略，从而能够保证访问控制策略的安全可靠。

场景 3：恶意用户 D 在分布式电网中实施内网渗透性测试，和恶意区块链节点串谋，尝试对多个设备发起连接，申请新的访问权限，并嗅探网络的脆弱性。

实验结果：与场景 1 和场景 2 相同，D 用户由于不具备相关的权限，连接申请被拒绝。由于 D 用户的异常连接行为已记录到区块链中，并且该记录无法被删除。当 D 申请获得访问权限时，会因异常的历史行为被区块链系统拒绝。

综上所述，基于区块链构建的分布式身份认证和访问控制服务具有更强的安全性，能够抵抗传统集中式的安全给分布式新能源电网带来的安全威胁。并且该方案具有普适性，能够经过改造应用于其他的信息系统。

3.2 实验分析

本文设计了对照实验，验证了基于区块链的身份认证模型和访问控制模型的可行性，然后对终端安全接入的实际场景进行了模拟，证明了本文所提方案的可行性。

但是对性能分析可知，该原型方案的性能无论是吞吐量和延迟均无法满足实际的需求。经过对照分析可知，其性能瓶颈主要来自于 Fabric 平台本身，本文所提模型的开销并不大。Fabric 的官方论文分析表明，该平台在 16-vCPU，8 GB 内存的实验条件下，只能够实现 3000 TPS，延迟更是接近秒级。区块链系统的性能核心取决于共识协议，如果采用最新的共识算法 HotStuff[22]，该算法的吞吐量能够达到 10 KTPS，延迟低于 20ms，完全能够满足分布式新能源并网的实际需求。

4 结论

针对分布式新能源并网面临的中心化网络安全方案的风险，本文以区块链为基础，提出一种面向分布式新能源网络的终端安全接入技术，建立终端安全接入的信任契约，实现跨域分布式的身份认证和访问控制，解决中心化带来的安全风险。给出基于区块链的终端接入认证和访问控制模型，提出终端的信任度评估算法，设计基于智能合约的终端接入流程，以 Hyperledger Fabric 为基础，搭建实验环境，模拟多终端跨域接入网络的行为，验证了上述方案的可行性，同时对存在的性能问题分析并提出了可行的解决方案。

参考文献

[1] 李兴鹏. 新能源并网的关键技术研究[D]. 杭州：浙江大学，2013.

[2] 李明节，于钊，许涛，等. 新能源并网系统引发的复杂振荡问题及其对策研究[J]. 电网技术，2017，41(4)：8-15.
Li Mingjie，Yu Zhao，Xu Tao，et al. Study of complex oscillation caused by renewable energy integration and its solution[J]. Power System Technology，2017，41(4)：8-15(in Chinese).

[3] 杨荣峰，于雁南，俞万能，等. 新能源船舶并网逆变器电网支撑协调控制[J]. 电工技术学报，2019，34(10)：161-174.

Yang Rongfeng，Yu Yannan，Yu Wanneng，et al．New energy ship grid-connected inverter grid support and cooperative control [J]．Transactions of China Electrotechnical Society，2019，34(10)：161-174(in Chinese)．

[4] 连线．黑客入侵风力发电厂全过程[EB/OL]．[2017-07-03]．https：//www.aqniu.com/hack-geek/26368.html．

[5] Fromknecht C，Velicanu D．Certcoin：a namecoin based decentralized authentication system[J]．Massachusetts Institute of Technology，2014，21(2)：857-867．

[6] 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)．

[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)：60-68．
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)：60-68(in Chinese)．

[8] 邵奇峰，金澈清，张召，等．区块链技术：架构及进展[J]．计算机学报，2018，41(5)：969-988．
Shao Qifeng，Jin Cheqing，Zhang Zhao，et al．Blockchain：architecture and research progress[J]．Chinese Journal of Computers，2018，41(5)：969-988(in Chinese)．

[9] Al-bassam M．SCPKI：A smart contract-based PKI and identity system[C]//Proceedings of the ACM Workshop on Blockchain，Cryptocurrencies and Contracts．NewYork：ACM，2017：35-40．

[10] Hari A，Lakshman T V．The internet blockchain：a distributed，tamper-resistant transaction framework for the internet[C]//The 15th ACM Workshop．Atlanta：ACM，2016．

[11] Matsumoto S，Reischuk R M．IKP：turning a PKI around with decentralized automated incentives[C]//Security and Privacy(SP)，2017 IEEE Symposium on．San Jose，CA，USA：IEEE，2017：410-426．

[12] Chen J，Yao S X，Yuan Q，et al．Certchain：public and efficient certificate audit based on blockchain for TLS connections[C]//IEEE INFOCOM 2018．Honolulu，HI，USA：IEEE，2018．

[13] Wang Z，Lin J，Cai Q，et al．Blockchain-based certificate transparency and revocation transparency[C]//Financial Cryptography and Data Security 2018．Curacao：IFCA，2019．

[14] Axon L，Goldsmith M．PB-PKI：a privacy-aware blockchain-based PKI[C]//14th International Conference on Security and Cryptography．Madrid，Spain：IACR，2017．

[15] Paul D，Petitcolas F A P．A first look at identity management schemes on the blockchain[J]．IEEE Security & Privacy，2018，16(4)：20-29．

[16] 王秀利，江晓舟，李洋．应用区块链的数据访问控制与共享模型[J]．软件学报，2019，30(6)：1661-1669．
Wang Xiuli，Jiang Xiaozhou，Li Yang．Model for data access control and sharing based on blockchain[J]．Journal of Software，2019，30(6)：1661-1669(in Chinese)．

[17] Cruz J P，Kaji Y，Yanai N．RBAC-SC：role-based access control using smart contract[J]．IEEE Access，2018，32(6)：12240-12251．

[18] Zyskind G，Nathan O，Pentland A S．Decentralizing privacy：using blockchain to protect personal data[C]//2015 IEEE Security and Privacy Workshops．San Jose，CA，USA：IEEE，2015．．

[19] 刘明达，拾以娟，陈左宁．基于区块链的分布式可信网络连接架构[J]．软件学报，2019，30(8)：2314-2336．
Liu Mingda，Shi Yijuan，Chen Zuoning．Distributed trusted network connection architecture based on blockchain[J]．Journal of Software，2019，30(8)：2314-2336(in Chinese)．

[20] 刘明达，拾以娟．基于区块链的远程证明模型[J]．计算机科学，2018，45(2)：48-52．
Liu Mingda，Shi Yijuan．Remote attestation model based on blockchain[J]．Computer Science，2018，45(2)：48-52(in Chinese)．

[21] Elli A，Artem B，Vita B，et al．Hyperledger fabric：a distributed operating system for permissioned blockchains[C]//EuroSys 2018．Porto，Portugal：EuroSys，2018．

[22] Maofan Yin，Dahlia Malkhi，Michael K Reiter，et al．HotStuff：BFT Consensus with Linearity and Responsiveness[C]//2019 ACM Symposium．Chaminade，Santa Cruz，California：ACM，2019．

梅文明

收稿日期：2019-11-18。

作者简介：

梅文明(1983)，男，高级工程师，通信作者，博士研究生，研究方向为能源互联网、可再生能源与清洁能源，E-mail：wenmingmei@sina.com；

李美成(1973)，男，教授，博士生导师，从事可再生能源与清洁能源研究、电力系统分析等，E-mail：mcli@ncepu.edu.cn；

孙炜(1977)，男，高级工程师，从事电网信息化与网路安全相关工作，E-mail：sunwei@sgcc.com.cn；

余文豪(1992)，男，硕士，研究方向为电力工控安全、威胁情报分析，E-mail：xintong-yuwenhao@epri.sgcc.com.cn。

（实习编辑　宋钰龙）