基于区块链的电网稳控参数实时在线管理体系设计与实践

柯贤波[1]，任 冲[1]，王吉利[1]，谢海鹏[2]，封 科[3]

（1. 国家电网公司西北分部，陕西 西安 710048；2. 电力设备电气绝缘国家重点实验室（西安交通大学电气工程学院），陕西 西安 710049；3. 南瑞集团有限公司（国网电力科学研究院有限公司），江苏 南京 210003）

摘要：传统的稳控管控体系难以适应当前日益庞大的稳控系统，为提升稳控系统管控水平，首先分析了当前稳控管理系统存在的不足，阐述了区块链的块链式数据结构、非对称加密等技术特点，基于区块链技术提出稳控参数管理系统整套解决方案，设计了稳控管理系统的技术架构、硬件结构与软件功能，实现了稳控系统的可靠身份认证、参数管理、事故追溯与风险评估等全流程管控功能，最后基于实际稳控制系统搭建了实验环境，实验结果证明所提的系统架构可实现快速身份认证与数据处理，有效提高稳控系统的安全性与可靠性。

关键词：安全稳定控制系统；区块链；参数管理；智能合约；体系架构；软件开发

Design and practice of power grid stability control parameter management system based on blockchain

KE Xianbo[1], REN Chong[1], WANG Jili[1], XIE Haipeng[2], FENG Ke[3]

(1. Northwest Branch of State Grid Corporation of China, Xi'an 710048, China; 2. State Key laboratory of Electrical Insulation and Power Equipment (School of Electrical Engineering, Xi'an Jiaotong University), Xi'an 710049, China;3. NARI Group Corporation /State Grid Electric Power Research Institute, Nanjing 210003, China)

Abstract: The traditional stability control and management control system are difficult to meet the requirements. In order to improve the control level of Safety and stability control system, in this paper, firstly the shortcomings of the current stability control management system are analyzed, and the blockchain data structure, asymmetric encryption and other technical characteristics of blockchain are expounded. Then a complete set of solutions for constructing the stability control parameter management system using blockchain technology are proposed. The technical architecture, hardware structure and software function of the stability control management system based on blockchain are designed, and the whole process control functions such as reliable identity authentication, parameter management, accident traceability and risk assessment of the stability control system are realized. Finally, a test environment is built based on the actual Safety and stability control system. The experimental results show that the proposed system architecture can realize fast identity authentication and data processing, and effectively improve the safety and reliability of Safety and stability control system.

Keywords: safety and stability control system; blockchain; parameter management; smart contract; architecture; software development

国家电网公司科技项目（SGNW0000DKMM2100146）；国家重点研发计划资助项目（2016YFB0901900）

0 引言

安全稳定控制系统可以在出现事故时通过各种紧急控制策略，保证系统的供电持续性与实时电量平衡，已成为当前保障电网安全稳定运行与提高输电能力的重要手段[1-2]。

随着电力系统的发展与建设，安全稳定控制系统的规模逐渐向大型化、广域化与多元化方向发展，运行逻辑愈发复杂[3-4]。安全稳定控制系统的正确运行依赖于海量参数数据的正确管理与配合，关键参数主要包括装置定值、压板、策略表、软件版本和动作报文五类信息。这些参数根据电网的运行方式与安全稳定控制系统的升级改造等诸多因素发生频繁与复杂的删除、修改或更新。这一过程涉及单位多，管理难度大，任一节点对关键参数的错误修改都会对整个系统的运行造成较大的影响，增加了电网安全稳定运行的潜在威胁。

当前稳控装置的关键参数管理主要依托于部署在调度中心的安全稳定控制管理系统（Stability Control Management System，SCMS），系统具有定值管理、告警及事件记录、远方控制等功能，在一定程度上减轻了管理压力[5]。然而在实际管理过程中存在很多新需求：由于关键参数的修改缺少有效公证，导致管理者和修改者的真实操作无法追溯，为避免责任的纠缠，亟需建立关键参数修改信任机制；稳控系统动作后，稳控装置动作指令的收发、执行缺乏有效第三方记录存证，稳控装置实际动作、响应情况查证困难，需要建立动作指令存证机制；当前SCMS通过调度数据网与稳控装置进行通信，通过纵向加密等方式保证通信安全，但攻击者可以接入调度数据网，使用回放攻击等手段破坏稳控关键参数管理系统的正常运行，因此亟需更有效的通信安全手段[6-7]。针对稳控系统管理面临的关键参数维护、动作指令追溯、节点身份认证和数据安全等管控难题，亟需建设全程留痕、易防难攻和安全高效的稳控关键参数管控系统，全面提升稳控系统管控水平。

区块链作为一类新兴的分布式数据存储技术，由于其去中心化、分布式存储等特点[8]，引起了电力行业的高度重视，并正成为驱动电力系统技术创新与产业变革的重要力量。近年来，区块链技术在电力行业中的应用主要集中于市场交易与信用背书两个方面。在市场交易方面，文献[9]介绍了区块链背景下的分布式交易系统在交易形式上的现状与发展趋势。文献[10]分析了电力批发市场、电力零售市场与分布式发电市场中区块链的应用前景。文献[11]总结了能源互联网与区块链技术的相似点，为能源区块链的开发奠定基础。文献[12]采用分布式迭代算法与双链交互形式，实现了电力市场中的实时阻塞管理。文献[13]提出了改进的拜占庭容错算法，以实现多能源主题的交互，提高多能源系统的能源利用率。文献[14]将新能源发电与绿证交易有机结合，开发了绿色证书的多链运行平台。在信用背书方面，文献[15]通过工作量证明机制实现了系统分布式能源交易市场中的信用风险的管理与控制。文献[16]基于区块链的共识机制提出了分布式的最优潮流算法，避免了恶意行为对最终结果的影响。文献[17]改进了微电网电能的交易流程，并通过基于信用证明的共识机制实现用户的信用自激励。文献[18]开发了区块链网络下的用户行为聚类算法，对用户的异常行为进行实时分析与预警。文献[19]采用基于信用的共识机制为微电网双端交易提供了天然的信用背书。

以上研究多着眼于区块链在电力市场与能源互联网等场景下的应用。近年来落地的电力交易系统中有超过一半涉及了区块链技术[20]，并逐渐延伸拓展至电动汽车[21]、虚拟电厂[22]、需求侧响应[23]与电力附属品市场[24]等领域。然而，区块链技术在电力系统中的应用局限于能源交易与能源市场中。事实上，区块链技术多主体特性与安全稳定系统的多节点网络属性具有相似的结构，且基于区块链的分布式存储与记账技术有望为稳控系统关键参数的管理提供有力的支撑，在本领域尚未有研究。

本文分析了稳控系统运行特性与现有信息

安全隐患，针对现存问题基于区块链技术提出稳控参数管理系统整套解决方案，设计了稳控管理系统的技术架构、硬件结构与软件功能，同时设计了电网稳控参数管理体系，实现了将设备的入网、关键参数的修改与校核、事故的追溯等流程转移至链上，大幅提升了稳控系统管控水平。

1 稳控系统运行特性与存在的信息安全隐患分析

随着电网运行复杂化与互联化，稳控系统也呈现出大型化与复杂化的趋势。稳控系统的安全可靠运行风险持续累积。

1.1 稳控系统运行特性

图1为稳控系统的运行示意图。稳控系统呈现联合调度、分区运行和分级管理的特点。各个分区通常存在一个区域控制主站，在与其他区域的控制主站交互更新调度命令的同时，通过专用的高速调度数据网络与各类具体安稳系统子站（如捷列控制子站、精准切负荷子站等）相连[25]。部分较为复杂的控制系统还会下连多个子站与执行站。

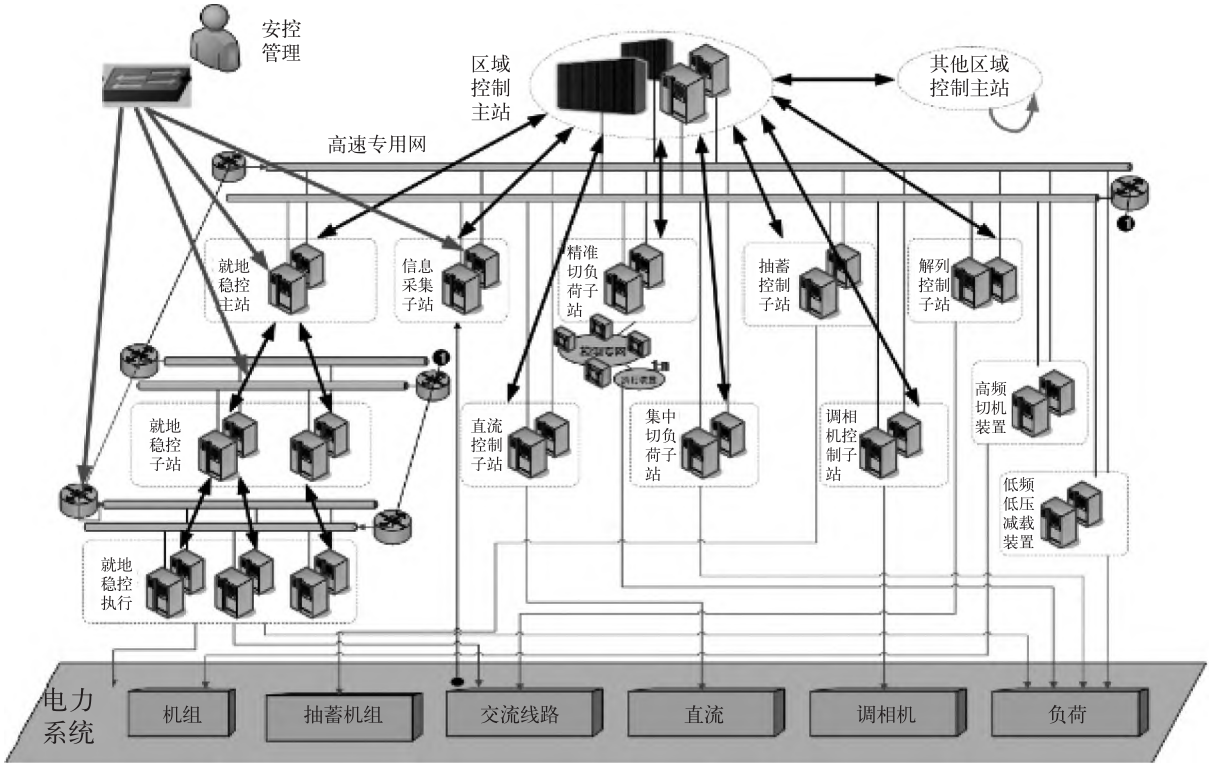

图 1 安全稳定控制系统示意图

Fig. 1 Diagram of safety and stability control system

调度者也可以通过集中管理系统（SCMS）与调度数据网络对各主站或其下子站进行直接调整与控制，以适应系统需求。各下级站点直接与电力系统中的一次设备（如机组、线路与负荷）相连，保障系统的安全稳定运行。

调度数据网中传递大量与系统状态、运行特征和调度命令相关的数据，对稳控系统的正确动作起着决定性的关键作用。

1.2 稳控系统中存在的信息安全隐患

基于上述运行特点与系统架构，现今的稳控系统存在部分安全隐患[26-28]，威胁系统的稳定运行。

（1）终端身份管理缺乏

现有的稳控系统多在封闭式的系统中运行，且装置的安装由专人负责，因此大多直接认可所有在线设备与新增装备的合法性。然而实际运

行过程中，恶意攻击者可以通过外接设备侵入系统内装置，并伪造成该装置与其他合法设备进行数据交互，通过修改稳控装置的关键参数，对电网二三道防线造成破坏。且现有管理系统难以察觉、阻止此类的恶意篡改，导致稳控系统出现误动作或拒动作的可能，对电网造成严重的后果。现今部分稳控系统也开始尝试基于公钥基础设施（Public Key Infrastructure，PKI）的数字证书认证机制[27]，但是随着系统愈发庞大，数字证书的计算资源需求日益增多，SCMS的数据处理与存储压力越来越大，无法满足系统的快速要求。

（2）数据维护难度大

系统的关键运行参数包括软件版本、稳控定值、稳控策略、压板状态和稳控管理规定等，这些参数根据系统运行状态的变化需要频繁更新、修正。同时由于上述参数涉及单位多、管理链条长，包括调度稳控系统研发人员、厂家现场支撑人员和广泛分布的现场运维人员等，上述用户均有可能修改稳控系统关键参数，若对所有修改的时间、人员与原因增加记录，将造成巨大的数据冗余与浪费。此外，任一节点对关键参数的错误修改都有可能对稳控系统造成较大的影响，增加了电网安全运行的潜在威胁。

（3）调度数据网安全防护不足

各个站点需要通过调度数据网进行通信互联，虽然通信过程可以通过加密的方式保证安全互通，但是恶意攻击者也可以利用网络监听等方式直接接入调度数据网，并在不对信息解密的条件下直接在网络中再次广播该信息，其他节点就会再次执行广播的信息，这将导致系统中某些元件中的数据回到该重复广播时的状态，以起到破坏系统连接或撤销参数修改的效果，破坏系统的正常运行。

（4）动作响应查证与责任追溯困难

稳控系统动作时，参数的修改、装置动作指令的收发和执行都缺少有效的第三方记录。当稳控系统不正确动作导致电网事故发生时，多方站点各执一词，甚至出现数据伪造与数据抹除的情况，难以准确判断事故责任人，且对事故原因的准确溯源起到消极的影响。

2 基于区块链的稳控系统解决方案

2.1 区块链技术特点

区块链是一种按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构，并以密码学方式保证不可篡改和不可伪造的分布式账本[28]，主要有以下核心技术。

（1）去中心化的分布式架构

去中心化是区块链技术的最大特点。在区块链网络中，所有节点都拥有区块链账本的完整或部分复制，其中记录着该条区块链诞生以来的所有数据。任意节点对账本记录的修改或添加都需要得到网络中多数节点的认同，从而避免了任意节点单独完成对账本信息的修改。此外，由于没有特定的主节点，因此任意节点退出不会对该网络的正常运行造成任何影响。

（2）块链式的数据存储结构区块链

区块链由许多区块构成，而区块中又包括区块体与区块头两部分。区块体中存储账本数据，区块头由该区块的生成时间、区块体数据与上一个区块的区块头等数据经过单向加密得到。因此每个区块都会引用上个区块的数据，从而构成了链状的结构[29]。基于这种“区块+链”式的存储结构，不仅避免了数据的修改，还可以通过区块头快速查找账本中的任一记录。

（3）非对称的加密方式

不同于一般加密方法，一个用户只有一个密码，区块链采用的加密方式中用户具有两个密码，分别称为公钥与私钥。任意信息通过一个密码加密后仅能通过另一个密码解密。私钥由用户保管，而公钥广播至系统中由所有节点保管。用户可以通过私钥向其他用户传递消息，其他节点可以通过公钥验证用户合法性；其他节点也可以通过公钥向该用户传递信息，此时仅拥有该私钥的用户可以对信息解密。

（4）可独立运行的智能合约

智能合约是记录在区块链中自动验证与执行

的计算机协议[30]。智能合约可赋予区块链在运行状态满足某些先决条件时自动执行合约规定的相关内容，在提高系统运行智能性的同时，不仅拓展了区块链作为账本的作用，还避免了部分动作的人为干预，提高了区块链系统的封闭性与安全性。

2.2 区块链与稳控系统的契合点

区块链技术与稳控系统具有天然的契合点。通过调度数据网相连的大量稳控装置，可以作为区块链网络中的参与节点。利用去中心化的架构可以构建一套分布式、智能加密的身份认证及信息管理平台，不仅保护业务信息管理，也使得系统更易维护。任意节点的入网需要得到系统中大多数节点的认证，确保了身份认证的安全性；块链式的存储结构存放着系统中所有节点稳控关键参数的修改记录，参数的修改需得到系统大部分节点的认可，因此没有任何机构或个人可以轻易修改关键数据，让稳控系统运行管理变得更加安全、便捷和可靠；非对称式的加密机制确保了系统中传递的任意信息可以直接与系统中的一个节点唯一对应，不仅保证了通信的安全性，还为事故发生后的追溯提供了有利条件；独立运行的智能合约赋予了系统自动运行的能力，不仅能自动更新账本，下载已达成共识的参数数据，还可以对系统的实时运行风险进行自检，进一步提高系统的安全性。

3 基于区块链的稳控参数管理体系架构

基于稳控系统现有的特点及与区块链技术的契合点，本文开发了基于区块链系统的稳控参数管理体系架构。

3.1 系统硬件架构

由于稳控系统属于内部系统，具有一定的封闭性，且稳控装置停运改造安全等级高、流程繁琐，对于存量稳控装置进行区块链改造需要充分考虑实施的灵活性。因此，本文提出的系统硬件架构如图2所示。基于区块链的稳控参数管理系统由调度端、厂站端及调数网组成。调度端在SCMS平台基础上进行区块链功能扩展，作为区块链系统的管理节点；厂站端增加区块链终端装置，实现稳控装置稳控关键参数上链功能；其他硬件架构与原系统保持不变，避免了大规模改造带来的经济性与安全性问题。

硬件配置方面，调度侧加装应用服务器与计算服务器，为区块链运行提供网络与算力支撑，同时作为管理节点，对所有参与节点信息进行管控，并提供丰富的高级应用功能。

厂站端稳控装置通过加装区块链终端参与区块链运行，该区块链终端作为稳控装置的区块链专用处理组件，仅需T接入稳控装置网口与2M网络，施工方便，在不改变稳控装置原有的硬件架构的基础上，实现对系统指令的监听与自动记录。

区块链终端作为稳控装置的区块链专用处理组件，不影响稳控装置原有的稳控正常功能，终端具备如下功能：

1）对信息进行区块链结构加工处理。

2）实现关键参数信息账本的发起、校核及分布式存储。

3）利用非对称加密技术，确保通信、信息安全。

4）实现身份入网可靠性验证。

5）采用标准化模块设计，支持容器化部署。

关键参数数据都被存储在K-V型数据库中，其中关键值都是二进制的。具体而言，有三个数据库，分别是BlockDB、StateDB和EvidenceDB。BlockDB保存了块的主体内容，包括块头；StateDB 保存了账户的状态数据库；EvidenceDB记录了每次共识的信息，包括参与验证者和投票信息。

3.2 系统技术架构

区块链系统通常具有六个技术层面，即数据层、网络层、共识层、激励层、合约层与应用层。由于稳控管理系统中没有市场交易的经济行为，无须激励节点参与网络，因此无须激励层[31]。本系统五层技术架构如图3所示。

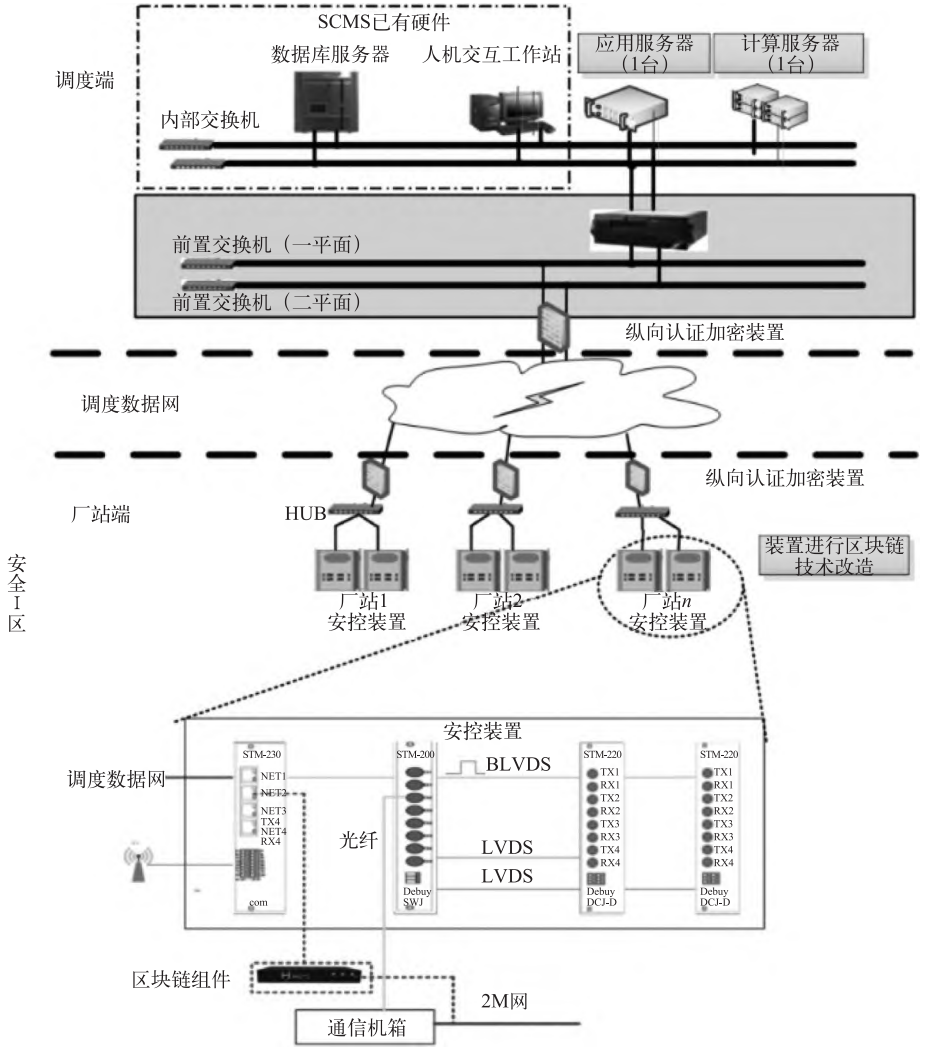

图 2　系统硬件组成

Fig. 2 Hardware topology of the system

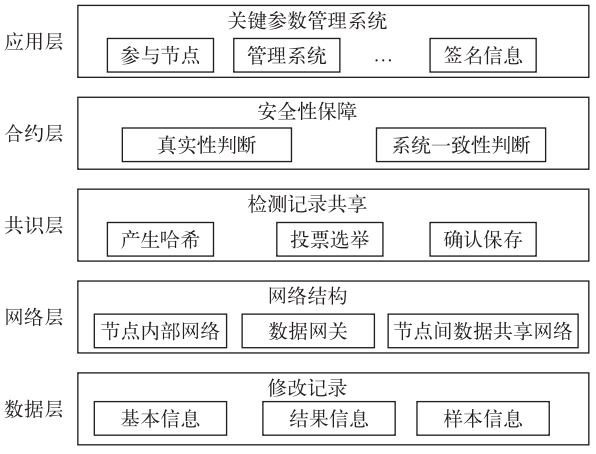

图 3　系统技术架构

Fig. 3 Technical architecture of the system

数据层主要存储系统的关键信息，主要包括节点状态、参数定制、压板状态、策略表信息、动作报文和系统版本等。在系统发生修改时，数据层将信息按照特定顺序连接加密，根据修改时间与区块高度自动生成新区块并上传。

网络层为系统提供数据传播与验证机制。主要由调度数据网将各个站点相连，且各站点间通信通过纵向加密与非对称加密保证安全性。

共识层为各节点提供达成信息统一的方法与形式。考虑到稳控系统中SCMS的特殊作用及系统对部分节点被攻击后的安全性，系统共识机制选择实用拜占庭容错（Practical Byzantine Fault Tolerance, PBFT）算法，为系统在弱中心化的条件下提供对节点攻击的鲁棒性[32]。当需要进行节点入网或参数修改等共识行为时，由发起人提出请求，并发送至全网进行公证，各节点收到信息后对该行为进行投票，若投票数达到预设值，则认为达成共识。在采用PBFT算法时，掉线或被恶意控制的节点数少于1/3即可确保系统的稳定可靠运行。

合约层利用自动合约为系统提供安全性保障。当系统出现新节点接入、参数修改或装置动作时，系统可以自动启动智能合约，对用户行为进行风险评估或对参数修改值进行巡检与校核，进一步为系统提供安全保障。

应用层提供了系统的应用场景与应用功能，为系统正常运行提供应用支撑。主要包括节点接入时的身份认证、关键参数的管理与事故发生时的责任追溯。

3.3 系统的软件功能

根据上述技术架构，可以设计该系统的软件功能，以适应实际需求。系统主要的软件功能如图4所示。

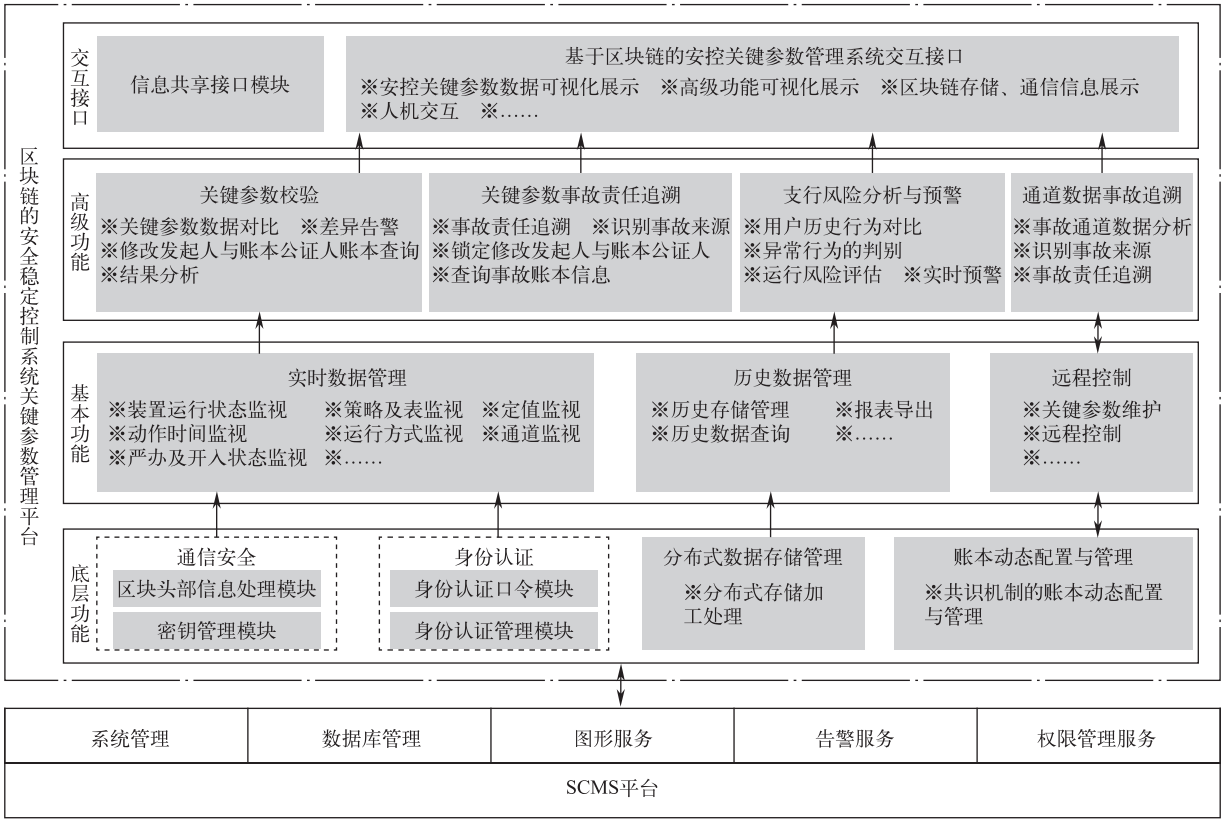

图 4 系统软件功能

Fig. 4 Software function of the system

系统的软件功能主要包括底层功能、基本功能与高级功能。其中底层功能为区块链运行必备的数据结构与共识机制的设计，主要包括密钥管理、身份认证、数据存储与共识网络四个部分，为系统提供通信、数据与网络安全。基本功能依托于底层功能，主要实现数据的管理与远程控制，为系统提供运行支撑。高级功能主要依靠智能合约，实现对关键参数的校验、事故后的责任追溯与系统实时运行风险，为系统提供进一步的安全保证。上述功能依托于现有SCMS的管理与服务，并可将操作结果显示至交互接口中，实现信息可视化与人机交互。

本文所提系统相对于原SCMS增加的功能包括身份认证、参数管理、事故追溯与风险评估四大部分。

（1）身份认证

各个站点新入网或断线重连后，需要经过身份认证证明自己的合法身份，避免非法装置接入系统。各节点的私钥设置为区块链终端的硬件模块，并经过一次单向加密储存在SCMS终端。在各个节点申请入网时，需同时上送本地私钥单向加密后的结果，SCMS首先查验该结果与本地结果是否相同，若相同再由所有节点对该节点的入网申请进行投票，若通过后则认为该节点为正常节点，向网络广播自己的公钥，并同步参数账本，完成身份认证流程。

将私钥设置为本体硬件模块，即使攻击者可以获得装置的电子身份，也无法获得该节点的私钥，无法生成正确的加密信息。SCMS存储的信息为私钥单向加密后的结果，无法破译为私钥，保证了即使SCMS节点遭受数据攻击，也不会泄露系统各节点的重要信息。

（2） 参数管理

由于系统的关键参数经常发生修改与变化，当系统的稳控定值或稳控策略发生变化时，由各个节点向SCMS发送更改记录请求，SCMS首先对修改信息进行预检测，若数据没有明显错误，则将该请求广播至全网进行共识流程，当同意修改节点达到PBFT共识满足条件的全网2/3节点时，认为达成共识，请求通过。SCMS向所有节点下发记账请求，各节点记录参数变化，完成参数修改流程。

除参数修改外，参数管理还支持对异常信号、压板投退、动作事件、策略表、定值单和通信报文等数据的历史结果的检索、浏览、导出与统计等功能，并在紧急情况下支持SCMS对各站点的直接调度与控制。

（3）事故追溯

数据修改由系统中相应节点发起，若由于某些关键参数的修改导致事故出现，则对应节点须对事故承担相应责任。

当事故发生时，首先对所有节点账本数据进行锁定，并调取所有节点的区块头数据进行比对，若出现区块头数据不一致的情况，则证明此处全网数据不一致，是事故的由来；若数据都一致，则证明事故是由于最后一次数据修改造成的；系统再次调取对应区块的具体数据，结合事故的动作报文进行比对，快速确定事故的数据来源与事故责任人，为事故的定责提供有效凭证。

由于全网区块头数据在得到共识的情况下应当相同，但事故发生的速度可能快于全网的数据统一，因此必须以各节点本地数据进行事故溯源，并通过区块头数据的比对快速锁定事故来源。

（4）风险评估

风险评估包括用户行为风险与数据风险。其中，用户行为风险指的是用户对参数的修改明显错误或者用户频繁做出异常的投票行为。系统可以在用户发起修改或做出公证时自动运行相应智能合约，抓取用户一段时间内的行为记录进行对比，并筛选出用户的异常行为，向SCMS实时告警，并根据系统存在异常行为的节点数与节点重要性对系统运行风险进行实时预警。

数据风险指的是系统关键参数已发生恶意修改后对系统造成的隐患。系统可以定时比较各节点的关键参数数据与SCMS的关键参数数据是否一致，如果有差异或者发现不符合规程的非法数据，则向SCMS实时告警，为系统运行提供进一步的安全保障。

4 系统测试与验证

4.1 测试系统环境

测试平台参照图2所示的硬件架构进行搭建。系统由1个SCMS平台与6台稳控装置构成一个小型安全稳定控制系统，稳控装置包括1个主站、2个子站与3个执行站。其中，SCMS已部署区块链信息管理功能；6台稳控装置与区块链终端通过交换机相连，由终端模块实现区块链的计算、加密与分布式存储等功能。

系统区块链关键信息包括：参数的出厂定值、内部定值与用户定值；压板的状态；稳控策略表信息；软件版本信息；装置动作指令与动作后的事件顺序记录信息。可实现参数的管控、装置入网的身份认证、数据的自动恢复与更新及节点状态的实时监视等功能。系统界面如图5所示。

图 5 系统人机交互界面

Fig. 5 Human-machine interaction interface of system

4.2 测试结果

针对上述系统对装置入网、数据修改、数据更新与实时监视功能进行了测试。对于装置入网，对同一数据进行多次入网与身份认证测试，测试结果见表1。

表 1 装置身份认证测试耗时

Tab. 1 Time consuming of device authentication

（单位：ms）

测试环节	最长耗时	最短耗时 / ms	平均耗时 / ms
装置入网	311	296	304
身份认证（成功）	161	104	125
身份认证（失败）	101	85	91

当节点发起数据修改时，经测试，在线节点超过4个（即全网节点的2/3），数据修改可以顺利进行，且数据修改速度快，吞吐率保持在1 000 TPS（超过1 000次交易/s的交易性能），能够满足稳控装置对参数修改的快速性要求。

系统可以对节点的在链状态与区块链终端通信进行实时监视。当断开稳控装置的网络连接时，SCMS人机交互界面上将显示对应节点掉链；当断开区块链终端与装置的连接时，SCMS人机交互界面上将显示对应节点区块链终端通信异常。此外，系统还可以在后台自动监视各个节点的在链状态、通信状态、存储状态和时标等信息，并在异常时实时告警。

当节点发生不可避免的硬件故障、断电或信息通道故障时，节点会退出系统；当节点从故障中恢复后，将自动重新连接入区块链系统，并发起对区块链账本的信息同步。采用并行处理，同步区块链状态的恢复时间在10 s左右，同步1～25个区块所需时间差距基本可以忽略，同步区块数量与所需同步时间的关系如图6所示，在装置故障时可以很快实现数据恢复，满足稳控装置恢复时间需求。

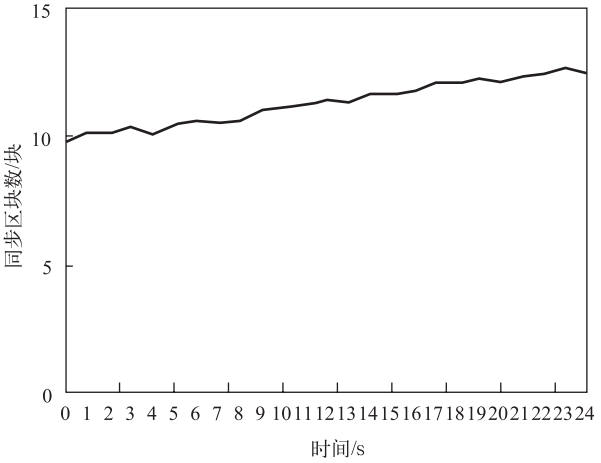

图 6 同步区块数量与所需同步时间

Fig. 6 Number of synchronization blocks and time required for synchronization

此外，开展区块链改造前后稳控参数系统功能实验，从安全性、数据格式等多方面进行比对，结果见表2。

表 2 改造前后测试结果比对

Tab. 2 Comparison of test results before and after renovation

序号	项目	改造前	改造后
1	安全性	装置可修改记录	一旦记录不可修改
2	数据格式	只有修改信息	块链式结构，带有身份、时间等信息，可追溯
3	存储模式	单方存储，只有SCMS拥有全部数据	链上装置都拥有全部数据，分布式存储，多备份
4	记录方式	定时召唤	一旦修改主动记录
5		高级功能	身份认证、责任追溯、宕机恢复、风险评估等

本文所开发的基于区块链的电网稳控参数实时在线管理体系，无论在数据安全性还是存储方式方面都优于现有系统，同时区块链的特性使得系统增加了身份认证、责任追溯和风险评估等高级功能。

5 结束语

本文介绍了稳控系统的运行方式与运行特点，并分析了现今稳控管理工作的新需求。为解决相应问题，开发基于区块链的稳控关键参数管理体系，设计系统的硬件结构与技术架构，将关键参数的修改行为记录在区块链网络中，为系统身份认证、参数管理、事故追溯和风险评估等问题提供了解决方案。本文所提架构在具有稳控集中管理的系统以及6台稳控装置构成的小型系统中进行了性能和功能测试。测试证明：

1）新装置入网身份认证耗时≤350 ms；数据修改吞吐率≥1 000 TPS；宕机恢复时间在10 s左右。

2）系统新增身份认证、责任追溯和风险评估高级功能。

本文所提架构安装便捷、功能完善，目前已在西北电网开展示范应用，具有广泛的工程推广前景。

参考文献

[1] 祁忠，施志良，李枫，等．安全稳定控制管理系统的研制及应用[J]．电力系统保护与控制，2016，44(1)：122-127．

[2] 颜云松，孙宁，张楠，等．基于预防检修周期优化的电网稳定控制系统失效风险评估[J]．电力系统保护与控制，2021，49(17)：139-146．

[3] 汤涌．电力系统安全稳定综合防御体系框架[J]．电网技术，2012，36(8)：1-5．

[4] 彭云豪，董希建，周海强，等．电网安全稳定控制系统可靠性评估[J]．电力系统保护与控制，2020，48(13)：123-131．

[5] 祁忠，施志良，李枫，等．安全稳定控制管理系统的研制及应用[J]．电力系统保护与控制，2016，44(1)：122-127．

[6] 汤奕，王琦，倪明，等．电力信息物理融合系统中的网络攻击分析[J]．电力系统自动化，2016，40(6)：148-151．

[7] 罗剑波，董希建，崔晓丹，等．关于大型安全稳定控制系统可靠性研究的探讨[J]．电力系统保护与控制，2018，46(8)：65-72．

[8] 陈思捷，王浩然，严正，等．区块链价值思辨：应用方向与边界[J]．中国电机工程学报，2020，40(7)：2123-2132，2392．

[9] 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(3)：961-972．

[10] 谢开，张显，张圣楠，等．区块链技术在电力交易中的应用与展望[J]．电力系统自动化，2020，44(19)：19-28．

[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] 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．

[13] 王德文，王莉鑫．基于实用拜占庭容错算法的多能源交互主体共识机制[J]．电力系统自动化，2019，43(9)：41-49．

[14] 骆钊，秦景辉，梁俊宇，等．含绿色证书跨链交易的综合能源系统运行优化[J]．电网技术，2021，45(4)：1311-1320．

[15] 平健，严正，陈思捷，等．基于区块链的分布式能源交易市场信用风险管理方法[J]．中国电机工程学报，2019，39(24)：7137-7145，7487．

[16] 张玲，陈思捷，严正，等．基于区块链共识机制的多区域最优潮流分布式算法[J]．中国电机工程学报，2020，40(20)：6433-6442．

[17] 秦金磊，孙文强，李整，等．适用于微电网区块链的信用共识机制[J]．电力系统自动化，2020，44(15)：10-18．

[18] HUANG B，LIU Z，CHEN J，et al．Behavior pattern clustering in blockchain networks[J]．Multimedia Tools & Applications，2017．

[19] ALASHERY M K，YI Z，SHI D，et al．A blockchain-enabled multi-settlement quasi-ideal peer-to-peer trading framework[J]．IEEE Transactions on Smart Grid，2020，99：1．

[20] 裴凤雀，崔锦瑞，董晨景，等．区块链在分布式电力交易中的研究领域及现状分析[J]．中国电机工程学报，2021，41(5)：1752-1771．

[21] KANG J，YU R，HUANG X，et al．Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains[J]．IEEE Transactions on Industrial Informatics，2017，13(6)：3154-3164．

[22] 何奇琳，艾芊．区块链技术在虚拟电厂中的应用前景[J]．电器与能效管理技术，2017(3)：14-18．

[23] 李彬，卢超，曹望璋，等．基于区块链技术的自动需求响应系统应用初探[J]．中国电机工程学报，2017，37(13)：3691-3702．

[24] 蔡元纪，顾宇轩，罗钢，等．基于区块链的绿色证书交易平台：概念与实践[J]．电力系统自动化，2020，44(15)：1-9．

[25] 陈汹，朱钰，封科，等．基于区块链的电力系统安全稳定控制终端身份认证[J]．广西师范大学学报(自然科学版)，2020，38(2)：8-18．

[26] 张盛杰，顾昊旻，李祉岐，等．电力工业控制系统信息安全风险分析与应对方案[J]．电力信息与通信技术，2017，15(4)：96-102．

[27] 刘刚，梁野，李毅松，等．数字证书技术在电力二次系统中的实现及应用[J]．电网技术，2006(增刊2)：71-75．

[28] 工业和信息化部．中国区块链技术和应用发展白皮书(2016)[EB/OL]．[2021-05-20]．http://www.cbdio.com/Big Data/201610/21/content_5351215．

[29] 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．

[30] NAKAMOTO S．Bitcoin：A peer-to-peer electronic cash system [EB/OL]．https://bitcoin.org/bitcoin.pdf

[31] 贺海武，延安，陈泽华．基于区块链的智能合约技术与应用综述[J]．计算机研究与发展，2018，55(11)：2452-2466．

[32] 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．

[33] 袁勇，倪晓春，曾帅，等．区块链共识算法的发展现状与展望[J]．自动化学报，2018，44(11)：2011-2022．

作者简介

柯贤波（1979—），男，硕士，高级工程师，研究方向为电力系统稳定运行与控制 。

任冲（1984—），男，通信作者，硕士，高级工程师，研究方向为电力系统稳定运行与控制。

王吉利（1981—），男，博士，高级工程师，研究方向为电力系统稳定运行与控制 。

（收稿日期：2022-02-23）