基于区块链的电网安稳控制通信报文记录与审计系统研究

颜云松[1,2] 陈 汹[3,1] 于同伟[4] 封 科[1] 李俊娥[5] 王 永[5] 余发江[5] 赵思宇[5]

[1](国网电力科学研究院有限公司 江苏 南京 211000)

[2](东南大学电气工程学院 江苏 南京 210096)

[3](东北电力大学 吉林 吉林 132012)

[4](国网辽宁省电力有限公司电力科学研究院 辽宁 沈阳 110000)

[5](空天信息安全与可信计算教育部重点实验室武汉大学国家网络安全学院 湖北 武汉 430072)

摘 要 随着电网安全稳定控制系统向广域化、复杂化方向发展,安稳控制通信报文数量多,通信链条长,易被篡改。当通信报文异变或损坏导致安控系统发生误动或拒动时,难以准确判断事故原因。针对该问题,提出一个基于区块链的电网安稳控制通信报文记录与审计系统。基于安控系统架构与管理需求设计半中心化系统模型,并针对安控系统架构与业务特点设计交叉多链结构。实验结果表明,该方案能够提高安稳控制通信报文记录与审计的真实性、完整性和安全性,同时具有较好的性能。

关键词 安全稳定控制系统 区块链 通信报文记录与审计 半中心化系统模型 交叉多链结构

中图分类号 TP3 **文献标志码** A DOI:10.3969/j.issn.1000-386x.2024.04.018

BLOCKCHAIN-BASED COMMUNICATION MESSAGES RECORDING AND AUDITING SYSTEM OF SECURITY AND STABILITY CONTROL FOR ELECTRIFIED WIRE NETTING

Yan Yunsong[1,2] Chen Xiong[3,1] Yu Tongwei[4] Feng Ke[1] Li Jun'e[5] Wang Yong[5] Yu Fajiang[5] Zhao Siyu[5]

[1](*State Grid Electric Power Research Institute*, *Nanjing 210000*, *Jiangsu*, *China*)

[2](*School of Electrical Engineering*, *Southeast University*, *Nanjing 210096*, *Jiangsu*, *China*)

[3](*Northeast Electric Power University*, *Jilin 132012*, *Jilin*, *China*)

[4](*Research Institute of State Grid Liaoning Electric Power Company*, *Shenyang 110000*, *Liaoning*, *China*)

[5](*Key Laboratory of Aerospace Information Security and Trusted Computing*, *Ministry of Education*, *School of Cyber Science and Engineering*, *Wuhan University*, *Wuhan 430072*, *Hubei*, *China*)

Abstract With the development of security and stability control system in the direction of wide-area and complexity, the number of security and stability control communication messages is large, the communication chain is long, and it is easy to be tampered with. When the communication messages are abnormal or damaged, leading to miss operations or miss trips of the security and stability control system, it is difficult to accurately trace the cause of the accident. To address this problem, we propose a blockchain-based communication messages recording and auditing system of security and stability control. A semi-centralized system model was designed based on the architecture and management requirements of security and stability control system, and a crossed multi-chain structure was designed for the architecture and business characteristics of security and stability control system. The experimental results show that this scheme not only can improve the authenticity, integrity and security of communication messages, but also has good performance.

Keywords Security and stability control system Blockchain Communication messages recording and auditing Semi-centralized system model Crossed multi-chain structure

---

收稿日期:2021-01-21。国家电网公司总部科技项目(SGLNDK00DWJS1900035)。**颜云松**,高工,主研领域:电力系统安全稳定控制技术。**陈汹**,高工。**于同伟**,高工。**封科**,工程师。**李俊娥**,教授。**王永**,博士生。**余发江**,副教授。**赵思宇**,硕士生。

0 引　言

安全稳定控制系统是保证电网安全生产的重要防线,它是当电力系统出现紧急状态后,通过执行切机、切负荷、快速减出力、直流功率紧急提升或回降等紧急控制措施,使电力系统恢复到正常运行状态下的控制系统[1]。随着安控系统向广域化、复杂化方向发展,安稳控制通信报文数量多,通信链条长,易被篡改。安控系统的正常工作需要众多由不同厂家运维的稳控站点和装置的高度协同配合[2],当通信报文异变或损坏导致安控系统发生误动或拒动时,难以准确判断事故原因,经常出现各执一词或无据可查的问题[3]。因此,有必要在安控系统中部署通信报文记录与审计系统。当前安稳控制通信报文记录和审计已有方案通过安控集中管理系统(SCMS)来实现,SCMS 采用的集中式数据管理方式不仅带来了较大的资源开销,而且面临着所记录的通信报文被恶意非法篡改的安全风险[4],从而导致监管部门得不到真实有效的审计数据。

区块链是利用块链式数据结构来验证与存储数据、利用密码学保证数据传输和访问安全、利用分布式共识算法来生成和更新数据、利用智能合约来编程和操作数据的一种全新的分布式基础架构与计算方式[5-8]。区块链具有开放共享、防篡改、抗抵赖、可追溯等技术特性[9-10],与安稳控制通信报文记录与审计有高度的契合度:1) 利用区块链分布式账本技术,将安稳控制通信报文写在区块链上,可以确保安稳控制通信报文的防篡改性和不可抵赖性;2) 区块链分布式记录和存储下的数据冗余备份能够保证安稳控制通信报文的可恢复性,便于事故后的追溯;3) 利用区块链的智能合约能够减少安稳控制通信报文管理、传输环节的人工干预和执行成本,对于后期安控在线定值管理、多站定值实时匹配具有重要意义;4) 基于区块链的数据共享能够打破安控厂家、调度管理部门、运行维护单位、技术支撑单位等多方之间的数据壁垒,实现信息互联互通,做到安稳控制通信报文记录和审计全过程的透明可信,让监管工作有理有据。

国内外众多学者针对区块链与审计相结合工作进行了研究。文献[11]分析了区块链应用于审计工作的可行性,探讨了如何用区块链改进审计工作的路径。文献[12]提出了一种将区块链作为多方审计通信通道的方案。通过将标有接收方身份的消息放到基于区块链的通信信道上,任何访问区块链的人都可以验证该消息。文献[13]提出了基于区块链的公开审计证书管理系统。通过设计新的数据结构 CertOper 来记录证书操作,保证证书操作的可追溯性和高效的查询响应。文献[14]以区块链网络为底层通信架构,提出一种符合 ISO/IEC 15408-2 的安全审计系统。文献[15]提出了一种基于区块链的网络存储可仲裁数据审计方案。通过设计一种具有可信仲裁的数据审计协议,以防止恶意验证者在无法察觉的情况下作弊。文献[16]提出了基于区块链的灵活存储系统 Audita,该系统可以保证数据保护,并解决隐私和可扩展性等挑战。文献[17]提出了 BlockAudit,通过将审计日志转换为与区块链兼容的数据结构,从审计日志内的数据中创建了带有时间戳的交易,并将它们汇总到一个区块中。文献[18]提出了一种基于 Hyperledger Fabric 的物联网数据完整性安全审计方案,解决了信任第三方审计的中心化问题。然而,现有基于区块链的审计系统采用的区块链主要是为交易类应用而设计的,它们的架构、算法和通信协议并不适用于实时性高且计算和存储资源有限的安控系统。目前未见有将区块链应用于安稳控制通信报文记录和审计的方案。

因此,本文提出一种适用于电网安控系统的通信报文记录与审计方案。首先,本文结合区块链和 SCMS 提出适用于安控系统架构和管理需求的半中心化系统架构。其次,本文基于安控系统架构和业务特点设计交叉多链结构。最后进行安全性分析和实验测试,验证本文所提方案能够提高安稳控制通信报文记录与审计的真实性、完整性和安全性,同时具有较好的性能。

1 安控系统和 SCMS

1.1 安控系统架构

在安控系统的通信网络中,各站点通常按照“主站-子站-执行站”模型进行通信[19],如图 1 所示。其中:主站负责制定稳控策略,通过子站实时监控各站点状态信息并发布控制命令;子站负责接收主站发出控制命令并收集本站状态信息并发送给主站;执行站负责监测本站状态信息并发送给子站,同时接收并执行子站发送的控制命令。

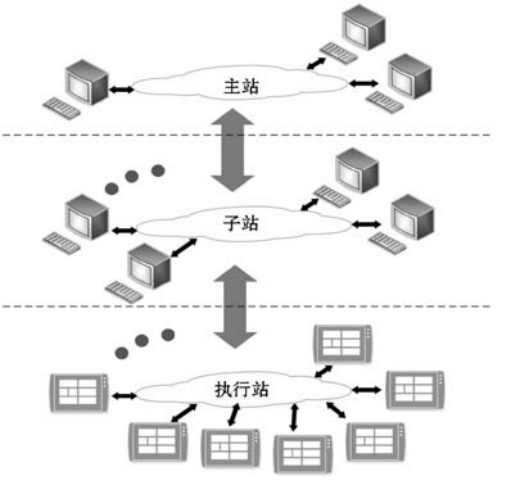

图 1　安全稳定控制系统架构

1.2 安控系统通信规约

安控系统通信规约格式如表 1 所示。电网安稳控制装置实际发送的数据帧分为正常数据和命令数据，正常数据是各电网安稳控制装置相互发送的状态信息，可以作为控制策略的依据。命令信息是上级站点对下级站点发送的动作命令，也是电网安稳控制通信报文记录与审计的重点。

表 1 安控系统通信规约

编号	正常数据定义	命令数据定义
0	报文头(0x55 + 地址) (地址 0 – 255)	报文头(0x99 + 地址) (地址 0 – 255)
1	识别码	识别码
2	Info1	Info1
3	Info2	Info2
⋮	⋮	⋮
10	Info9	Info9
11	校验和(以上 11 个字的累加和取反)	

1.3 SCMS 架构

SCMS 由位于厂站端的稳控装置、通信网络和位于调度中心的服务器、工作站等组成[20]，如图 2 所示。各站稳控装置通常采用双重化配置，经由站内交换机接入电力调度数据网与调度中心进行通信。

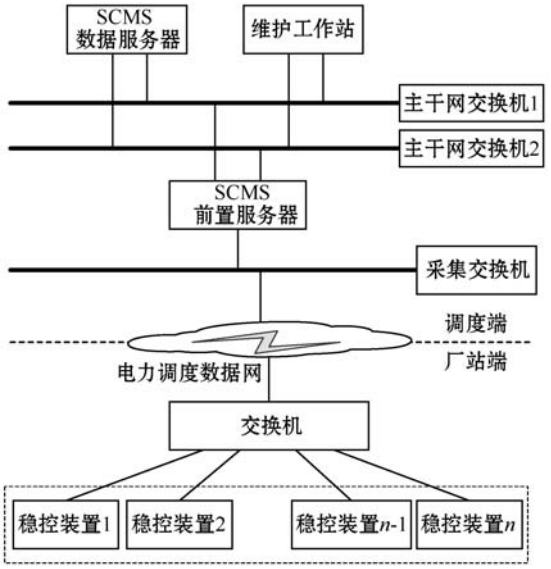

图 2 安控集中管理系统架构

2 安稳控制通信报文记录与审计方案

2.1 系统模型

本文设计的电网安稳控制通信报文记录与审计系统模型如图 3 所示。该模型包括 5 种不同的实体，分别是管理员(Admin)、审计员(Auditor)、安控集中管理系统(SCMS)、安控节点(SCN)和仲裁节点(AN)。

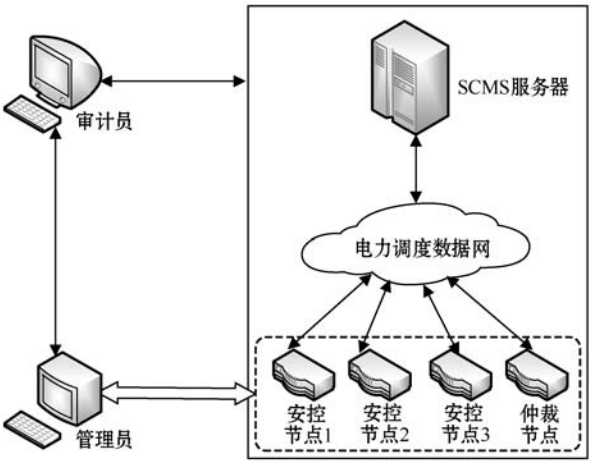

图 3 安稳控制通信报文记录与审计系统模型

管理员(Admin)负责在系统中维护节点列表、审核数据、发送审计请求并接收审计报告。管理员通过厂站内部通信组网向该站位于稳控装置管理模块的通信报文记录与审计系统发送相应的本地操作请求。

审计员(Auditor)负责为用户提供审计服务。审计员具有从包括 SCMS 在内的一系列节点获取信息的权限。当管理员需要对通信报文进行审计查询时，会向审计员发出审计数据查询请求，审计员将根据该请求读取数据的相关索引信息。根据索引信息，审计员将通过电力调度数据网访问 SCMS 的管理模块，执行远程验证并调用通信报文记录与审计系统内的审计查询接口读取对应的数据分片，通过校验数据的 Hash 值验证数据的完整性，最后向管理员反馈审计结果。

安控集中管理系统(SCMS)是安控系统通信网络的关键节点，安控系统各节点通信数据均会上传至该节点。在审计流程中，审计员也可以向 SCMS 节点进行审计查询，获取对应查询结果用以向相关管理员返回审计结果。

安控节点(SCN)即安控系统中各主站、子站、执行站对应的装置节点。安控节点负责记录安控系统通信报文等数据。

仲裁节点(AN)随机从其他链上的安控节点中选取。设置仲裁节点的目的是为了防止区块链节点成员集体造假，增强审计数据的安全性。

2.2 区块链架构

现有区块链的单链结构不能满足由多个“主站-子站-执行站”三层架构模型组成的安稳控制通信报文记录与审计系统需求。因此，为了尽量减少一条区块链上的节点数目，以使每个节点存储的数据量尽可能少，根据安控系统的通信特点，本文设计了多链结构，每一

条链对应一条由“主站-子站-执行站”组成的通信通道,链与链之间事务隔离、账本隔离。但是,一条通信通道的“主站-子站-执行站”通信模型中只有三个节点,由于节点数过少,很难保证通信报文的安全性。为此,需要在每条区块链上增加两个仲裁节点,仲裁节点随机从其他区块链节点上选取。由于所有稳控装置都会通过电力调度数据网和 SCMS 系统通信,因此有必要将 SCMS 作为一个节点加入每一条区块链。本文设计的交叉多链示例如图 4 所示。

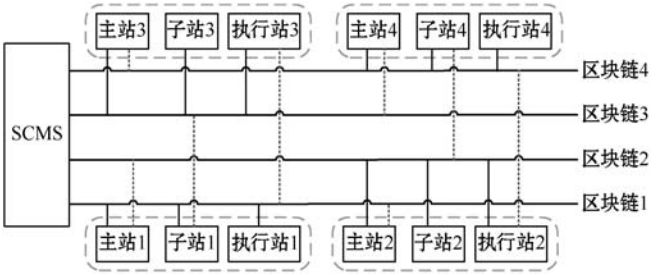

图 4　适用于安控系统的交叉多链示例

在图 4 中,共有四条区块链,每条区块链上共有 6 个节点,分别是主站节点、子站节点、执行站节点、SCMS 节点和两个仲裁节点(图 4 中虚线条所连接的节点是随机选取的仲裁节点)。交叉多链的优点是每条链上的节点数量少,节点之间的通信量低,使得区块链的性能相对较好,对安控系统的影响也较低。

2.3　系统初始化

基于区块链的安稳控制通信报文记录与审计系统的初始化主要包括链结构初始化和链上成员配置两个过程。

1)链结构初始化过程对各链进行初始参数配置,包含标识不同区块链的通道号 ChannelID、区块链初始化时间 Initime 和该链主要所属机构 Org 等关键初始信息,各链在初始参数配置完成的基础上分别完成创世区块的生成和初始节点入链等操作。

2)为了更好地通过多链结构来提高审计仲裁的公平性,需要对链上成员进行合理配置。各链上包含的节点将由审计系统的负责人员进行预先设置,各节点所属的链及其在该链上的身份(通信节点或仲裁节点)等将被预置入配置文件,在系统启动时指示节点加入相关区块链完成对应任务。

2.4　通信报文上链

在节点加入区块链系统之后,系统会首先完成账本状态检查,进而实现通道内的账本同步,以便与其他节点进行一致的后续通信报文上链和记录过程。

当一个记录着稳控装置通信报文的区块经过共识投票确定后,区块链会向链上的其他节点广播,全面同步到每个节点区块。通信报文上链的流程如图 5 所示。节点广播通信报文(Info)到系统内后,相应节点首先经过远程节点的验证以校验该通信报文的签名合法性并依据签名者的身份,判断通信报文内容的合法性。在所有合法性校验通过生成对应数据项后,可以按照交易预案,调用智能合约,通过拜占庭容错算法(PBFT)形成共识。相同通道的交易将在通道主节点(orderer)处被打包成数据块广播给通道中所有的成员。在经过链上所有节点的共识后,通信报文将被储存于各节点的相应区块链账本上,该过程保证了链上数据的真实性和防篡改性。

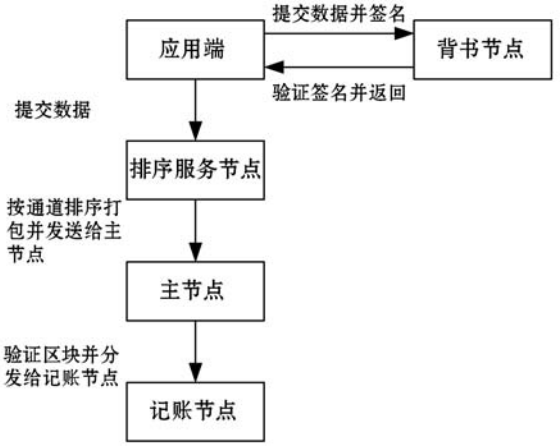

图 5　通信报文上链

电网安稳控制通信报文的上链核心算法如算法 1 所示。

算法 1　Upload

输入:待上传消息 Info,身份凭据 C。

输出:处理结果 Flag。

```
1. function Upload(Info, C)
2. 基于 Info 构建待发送的认证消息 inf
3.     Tx ← RemoteAuth(inf, C)
4.     if !Verify(Tx) then
5.         return false
6.     end if
7.     开始针对 Tx 的 PBFT 共识过程
8.     if !GetState(Tx) then
9.         return false
10.    end if
11.    return true
12. end function
```

2.5　通信报文审计查询

安稳控制通信报文的审计查询包括请求授权和查询信息两个部分,查询模式为通过电网安稳控制设备 IP 查询、通过通信报文发出的时间查询。通信报文的审计查询的流程如图 6 所示。当审计员接收到区块数据查询的请求后,会根据该请求读取数据的相关索引

信息,并根据索引信息去读取对应的数据分片,通过校验数据的 Hash 值验证数据的完整性,最后向用户反馈审计结果。

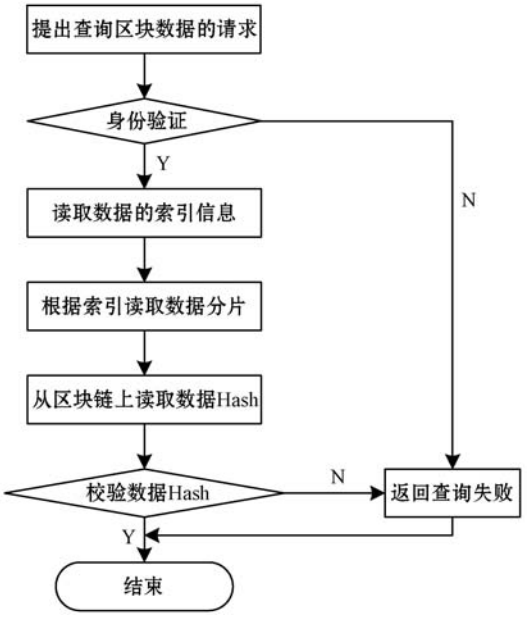

图 6 审计查询流程

电网安稳控制通信报文的审计查询核心算法如算法 2 所示。

算法 2 Query

输入:查询请求 Req,身份凭据 C。

输出:查询结果 Result。

```
1. function ExcuteQuery(Req, C)
2.     if !CapabilityCheck(C, Req.type) then
3.         return null
4.     end if
5.     iter ← leveldb.newIterator()
6.     hasNext ← iter.seek(Req.Key)
7.     while hasNext do
8.         使用 iter.value()从账本中遍历提取消息 Info
9.         Append(result, info)
10.    end while
11.    return Result
12. end function
```

3 安全性分析

区块链具有去中心化、公开透明、防篡改及可追溯等技术特征,区块链数据实时广播、节点间保持同步,以此为基础提出的电网安稳控制通信报文记录与审计系统具有较强的健壮性和安全性。

3.1 通信报文的不可抵赖性

审计系统的每条通信报文经过共识投票确定后,就会全面同步到每个节点区块,不可再撤销。通道内各 Peer 节点独立存储全部数据,即使某个节点账本储存出现问题,该 Org 对应通道中包括仲裁节点在内的其他节点仍旧正常运行,记录了全部数据信息副本,最大程度防止了该 Org 的审计数据丢失或成员串通抵赖。因此,区块链网络能够作为记录通道来实现安稳控制通信报文的不可抵赖性。

3.2 通信报文的防篡改性

在基于区块链的审计系统中,安稳控制通信报文一旦在通道内得到各通信节点和仲裁节点(Peers)的认证,就会添加在相应通信通道对应的链上形成新的区块,每个区块的头结构都包含一个信息的录入时间戳(Timestamp)字段,使得区块链形成一条按时间序列排列的链条。如果要修改某一区块内的某一 Info 结构内容,就需要修改该 Channel 包含这一区块在内的之前所有区块的区块头,并且还要与每个 Peer 节点达成共识,这在目前的区块链网络中无法实现。因此,在所提的审计系统中,单个 Org 无法篡改任何通信报文,从而满足防篡改性。

3.3 抵御 DoS 攻击

本文提出的审计系统采用分布式架构,区块链分布式记录和存储下的数据冗余备份能够保证安稳控制通信报文的可恢复性,即使某个节点遭受 DoS 攻击,也能被其他节点平等替代,整个系统依靠剩余的节点依然可以正常运转。

4 实验仿真与结果分析

4.1 实验环境和系统功能实现

实验硬件环境:Intel(R) Core(TM) i5-6300HQ CPU @2.50 GHz,8 GB RAM。

实验软件环境:1) Windows 10 操作系统和 Ubuntu 16.04 虚拟机,均进行了节点部署和测试;2) 实验平台采用开源区块链项目 Hyperledger Fabric v1.4.0;3) 编程工具主要采用 Goland。

Hyperledger Fabric 区块链平台在实验过程中主要被用来完成包括配置节点、创建通道、智能合约部署和智能合约操作在内的区块链基础环境配置任务。以 Fabric 内的节点(nodes)来表示安稳控制通信报文记录与审计系统的各装置节点。实验中存在一个位于所有区块链通道内的特殊节点,对应架构中的 SCMS,其他 Fabric 节点则对应各架构中的各装置节点,按照 2.1 节中的部署进行通道成员设计,进一步完成实验。

本文基于 Go 语言实现系统所需的智能合约,用于处理被区块链上各节点所认可的业务逻辑。智能合约

函数设计如表 2 所示。

表 2　智能合约函数

函数名	函数功能
Init	智能合约初始化函数
Invoke	接受并处理请求
isAllowAdd	检测是否可以添加通信报文
addInfo	添加通信报文
isAllowQuery	检测是否可以查询通信报文
queryInfoByIP	根据电网安稳控制设备 IP 查询通信报文

在系统数据存储的过程中,数据处理时由智能合约执行。在调用智能合约时,首先调用 Init 方法将智能合约初始化,然后智能合约会调用 Invoke 方法,以发送写入数据消息和获取数据消息的方式向 peer 节点发送预提交状态和获取账本状态信息。智能合约将结果发送给 peer 节点,peer 节点对结果进行签名背书。如果是通信报文上链操作,则收集所有 peer 节点签名背书后的通信报文,将通信数据发送到 orderer 节点进行排序,由 orderer 节点打包生成区块,然后广播到各个 peer 节点,完成通信报文的上链。如果是通信报文查询操作,则不需要提交通信报文。

4.2　系统性能分析与对比

1）系统内操作时间分析。电网安全稳定控制系统业务运行具有高实时性要求,其通信报文审计也需要较高的实时性和持续性。本文通过实验仿真得出了节点数目对入链时间的影响以及节点数和数据容量对节点审计查询时间的影响。实验设置初始通道内节点数为 4,且各节点每隔 0.5 s 上传一组审计数据。测试时每次向链上添加一个节点,分别统计上链操作时延。具体实验结果如图 7 所示。

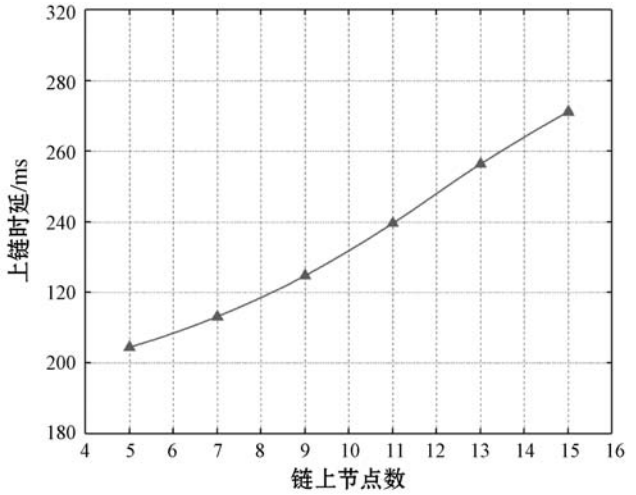

图 7　现有节点数对新节点上链时延的影响

在每次添加节点后,系统进行审计查询操作并统计平均审计查询时延。具体实验结果如图 8 所示。

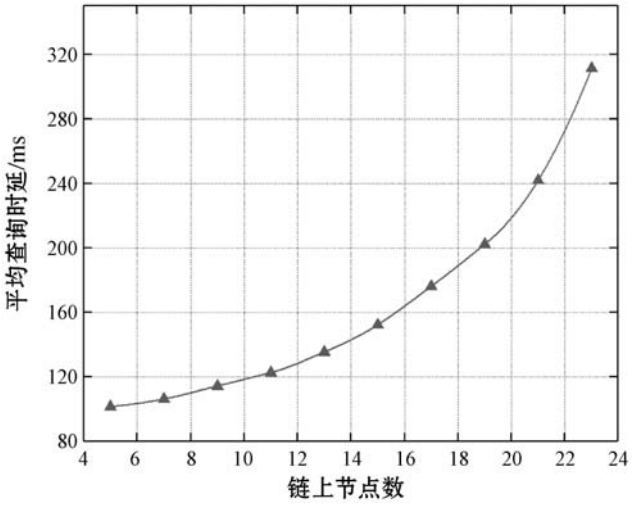

图 8　链上节点数对审计查询延时的影响

可以看出,当链上节点数保持在 19 个以内,审计查询时延较低并缓慢增长。当链上节点数超过 19 个时,审计查询时延会快速增长,并带来较大的审计查询时延。本文设计的多链结构将区块链系统的节点分散在多个区块链上,使得每条区块链上的节点数量不超过 19 个,在各节点满足审计要求的情况下,数据上链操作的频率和时间开销相应降低。本文方案的审计查询时延比文献[18]低得多。这也突出了本文 2.1 节设计的多链结构的优势。

我们将审计系统链上节点数设置为 7,调整系统参数使区块容量从 320 字节开始逐渐增加到 960 字节,在此基础上测试区块容量对审计查询时延的影响。具体实验结果如图 9 所示。

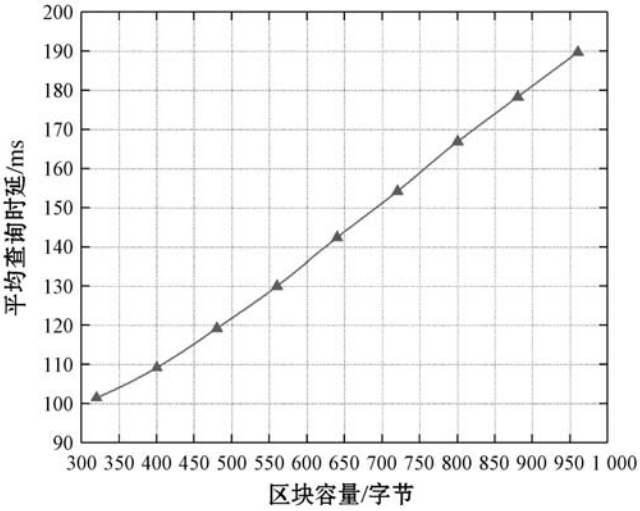

图 9　区块容量对审计查询延时的影响

可以看出,随着区块数据容量的增大,审计时间越来越长,几乎呈线性增长。本文设计的多链结构使得除了 SCMS 以外的节点存储的账本数据容量大大降

低,本文基于电网安控系统通信特点设计的审计系统只记录通信报文的功能码,并不记录完整的通信报文,因此,本文方案相比其他方案允许使用更小的区块容量,从而减少系统的审计查询时延。本文方案的审计查询时延比文献[16]低得多。这进一步突出了本文2.1 节设计的交叉多链结构的优势。

2)存储开销分析。在审计数据存储空间开销方面,系统测试中定义的单项数据约占 35 字节。随着数据吞吐量的增加,单位时间内节点账本增长量会随之增加,但实际稳控业务中,关键动作命令发送频率较低,实验中将一个区块链通道内数据吞吐量设置为平均每 5 分钟各节点发送一条审计数据,超出实际业务需求,此时区块大小平均值约为 2 KB。在实验中超出实际需求的数据吞吐量条件下,一个含 6 个节点的通道内产生的审计数据量将在较长周期内(5 年以上)低于 100 MB,因此本文系统可以满足实际电网安全稳定控制终端的资源消耗需求。

5 结 语

针对当前电网安稳控制通信报文记录与审计面临的问题,本文结合区块链技术提出一个基于区块链的电网安稳控制通信报文记录与审计系统。本文根据安控系统架构、业务特点和管理需求创新设计半中心化系统架构和交叉多链结构。安全性分析和实验结果表明,本文方案能够提高安稳控制通信报文记录与审计的真实性、完整性和安全性,具有防篡改、抗抵赖、可追溯、透明可信等优势。本文工作有利于促进区块链技术在安控系统应用的加速落地。

参 考 文 献

[1] 张倩. 智能变电站环境下安全稳定控制装置通信系统研究[D]. 南京:东南大学,2015.

[2] 熊先云. 区域电网稳定控制系统的研究及应用[D]. 北京:华北电力大学,2015.

[3] Wang Y, Li J, Chen X, et al. Remote attestation for intelligent electronic devices in smart grid based on trusted level measurement[J]. Chinese Journal of Electronics, 2020, 29(3):437 - 446.

[4] 刘志鹏,李献,余加喜,等. 海南电网安全稳定控制集中管理系统的研究[J]. 云南电力技术,2018,46(4):23 - 26,31.

[5] 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.

[6] 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.

[7] 江沛佩,王骞,陈艳姣,等. 区块链网络安全保障:攻击与防御[J]. 通信学报,2021,42(1):1 - 12.

[8] 刘明达,陈左宁,拾以娟,等. 区块链在数据安全领域的研究进展[J]. 计算机学报,2021,44(1):1 - 27.

[9] 徐恪,凌思通,李琦,等. 基于区块链的网络安全体系结构与关键技术研究进展[J]. 计算机学报,2021,44(1):55 - 83.

[10] 郭含月,周霁婷,王嘉麒,等. 基于区块链技术的跨境商品授权与存证系统[J]. 计算机应用与软件,2021,38(1):21 - 26,57.

[11] 袁曙. 区块链技术在企业联网审计中的应用[J]. 财会通讯,2018(7):99 - 101.

[12] Suzuki S, Murai J. Blockchain as an audit-able communication channel[C]//41st Annual Computer Software and Applications Conference, 2017:516 - 522.

[13] Chen J, Yao S X, Yuan Q, et al. CertChain: Public and efficient certificate audit based on blockchain for TLS connections[C]//IEEE Conference on Computer Communications, 2018:2060 - 2068.

[14] Cha S C, Yeh K H. An ISO/IEC 15408-2 compliant security auditing system with blockchain technology[C]//IEEE Conference on Communications and Network Security, 2018: 1 - 2.

[15] Xu Y, Ren J, Zhang Y, et al. Blockchain empowered arbitrable data auditing scheme for network storage as a service [J]. IEEE Transactions on Services Computing, 2020, 13(2):289 - 300.

[16] Francati D, Ateniese G, Faye A, et al. Audita: A blockchain-based auditing framework for off-chain storage[C]// 9th International Workshop on Security in Blockchain and Cloud Computing, 2021:5 - 10.

[17] Ahmad A, Saad M, Bassiouni M, et al. Towards blockchain-driven, secure and transparent audit logs[C]//15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, 2018: 443 - 448.

[18] Dong G F, Wang X. A secure IoT data integrity auditing scheme based on consortium blockchain[C]//5th IEEE International Conference on Big Data Analytics, 2020: 246 - 250.

[19] 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.

[20] 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.