基于区块链的试验控制信息审计与监控模型

陈 峰
(92493 部队,辽宁 葫芦岛 125000)

摘 要：随着联合试验、体系试验需求的日益凸显,装备试验分布式、网络化特征日趋明显,给装备试验控制安全性带来了新的挑战,装备试验系统一旦被恶意控制或控制数据被恶意篡改,会带来难以估量的政治影响和军事经济损失。基于区块链去中心化、不可篡改等特性技术,首先提出了一种基于区块链的控制信息审计与监控系统模型,并利用智能合约实现闭环反馈控制的全流程监督,能够保证分布式联合试验的可信监管;然后,给出了模型实现的方案步骤;最后,通过仿真试验验证了模型的有效性。

关键词：装备试验系统;区块链;智能合约;信息审计
中图分类号：TP393 **文献标识码**：A DOI:10.16157/j.issn.0258-7998.212328

中文引用格式：陈峰. 基于区块链的试验控制信息审计与监控模型[J].电子技术应用,2022,48(9):123-126.
英文引用格式：Chen Feng. Blockchain-based control information auditing and monitoring technology[J]. Application of Electronic Technique,2022,48(9):123-126.

Blockchain-based control information auditing and monitoring technology

Chen Feng
(Army of 92493, Huludao 125000, China)

Abstract: With the increasing demand for joint experiments and system testing, the distributed and networked characteristics of equipment testing have become increasingly obvious, which brings new challenges to the security of equipment test control. Once the equipment test system is maliciously controlled or the control data is maliciously tampered with, it will bring incalculable political influence and military economic losses. Based on the characteristics of blockchain decentralization and non-tampering technology, firstly, this article proposes a blockchain-based control information auditing and monitoring system model, and smart contracts are used to achieve full-process supervision of closed-loop feedback control, which can ensure distributed joint trustworthy supervision of the test. Then, the steps of the model realization scheme are given in this article. Finally, the validity of the model is verified by the simulation test.

Key words: equipment test system; blockchain; smart contract; information auditing

0 引言

随着现代化网络技术和信息化的不断发展,如今的装备控制形态早已从过去传统的人力控制型转变为信息自动化控制型。我国也在努力研制国产化自主研发装备,结合相关领域的快速发展,我国军事装备领域取得了稳健的发展态势。装备控制主要涉及自动控制技术、机械技术、计算机信息技术、机电一体化技术等。军事装备一体化技术在我国多方领域应用广泛,为军事现代化的推进提供支持和指导。

现代化军事装备控制系统牵一发而动全身,对其各项组成部分,各项单元和指标有极为严格的要求。首先是要求军事装备系统尽量自动化,要求军事装备系统能够提升其先进性,利用机电一体化技术,使装备系统在每一步执行中自动触发,减少操作人员对系统的操纵和干预;其次是可靠性,由于军事装备的特殊性,对装备系统的可靠性要求非常严格,可靠性的高低决定了其军事装备在实战当中的可用性,增强装备系统在干扰环境下的持续可用性;第三是对装备系统的准确性要求,在军事领域当中,每一个装备运行的方向角度、轨道位置、温度范围等都非常严格,要求装备系统能够利用辅助系统(如自动跟踪系统、温度反馈系统和自动瞄准系统等)提高自身的准确性,保障装备系统整体的精准程度。

新时代中国特色社会主义思想的核心内容的“八个明确”中指出了新时代的强军目标。军事装备系统的先进性对实现强军目标具有重要意义。一旦某个军事装备被不法分子或敌军控制,将对我方装备系统、财产安全,甚至人员生命安全造成不可估量的伤害。例如 2001 年的“9.11 事件”,被恐怖分子劫持的两家民航客机撞毁美国世界贸易中心的两幢楼,后续又撞毁位于华盛顿的美国国防部五角大楼。“9.11 事件”造成的损失十分严重,

遇难者人数达到 2 996 人，经济损失约 2 000 亿美元。因此，在军事装备控制系统中安排预设的自毁指令是十分必要的，一旦某武器装备被敌军所控制，自毁指令可使我方的各方面伤害和损失最小化。

现有的装备控制系统的检测和审计机制主要是依赖于中心化的服务器，一旦中心化服务器遭到攻击或破坏，对整个装备控制系统将会是毁灭性的打击。本文针对传统中心化装备控制系统的致命性风险，研究分布式装备试验控制信息审计与监控技术，为装备控制系统的安全性提供可靠保障。

本文首先提出了基于区块链的分布式装备试验控制信息审计与监控技术五层系统模型，并利用智能合约实现闭环反馈控制的全流程监督，实现了分布式联合试验的可信监管；然后，以飞行器试验控制器为最小系统为例，给出了模型实现的方案步骤；最后，通过仿真试验验证了模型的有效性。

1 相关工作

1.1 装备控制安全

装备控制系统的安全性极为重要，许多学者接连提出解决方案和机制保护其安全性。文献[1]通过分析大量的数据资源建设现状，分析数据泄露的原因，建立了装备数据安全分析方法，构建了装备数据全生命周期的安全防护体系；文献[2]对安全射界装置进行了安全需求分析，构建了软件框架和硬件电路，对舰载设备发射的可靠性和安全性进行验证；文献[3]对航空装备保障工作中的安全因素进行了分析，理论上探讨了提高航空装备安全性的对策；文献[4]提出在军事智能化迅速发展的今天，虽然人工智能等新兴技术提高了军事装备的战斗效率，但其安全问题也日益凸显，倡导消除军事智能化带来的安全隐患；文献[5]指出现代化军事装备系统逐渐智能化、复杂化，在执行过程中难免会产生大量的不确定性风险，调查了现有军事装备事故处理方法的局限性，提出建立军事装备保险机制，并理论分析了其可行性及优势。

1.2 区块链

因区块链去中心化、不可篡改、永久记录、可追溯、公开可验证等特性，在数据安全和可靠性方面，适用于众多行业[6-11]。在工控系统的智能电网供电方面，文献[12]提出了通过区块链的分布式账本记录相关电力数据，并提供给矿工再汇总权限，但是执行效率不高；文献[13]提出了基于结合区块链的用电数据存储方案，结合区块链的节点共识机制，实现了用户对敏感用电数据的存储和信息共享；文献[14]在烟草行业的工控系统利用区块链的不可篡改、可靠数据库等特点设计了安全防护系统，实现从信息管理层到现场设备层的信息安全保护和可靠身份认证；文献[15]提出 ICS-BlockOpS 的这一新型架构，将完整性检查机制与区块链结合，保证数据的不可篡改性和冗余性，以提高工控系统中的数据安全性，并将该原型架构实施在正在运行的水处理厂中。

2 系统模型

基于区块链技术，提出了装备试验控制的五层系统模型，包括数据采集层、通信层、分布式存储层、共识层和应用层，如图 1 所示。

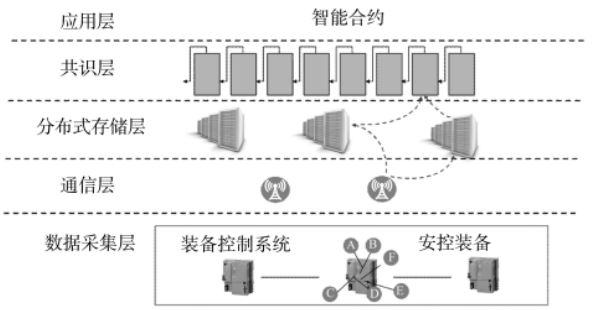

图 1 系统模型

2.1 数据采集层

数据采集层建立在装备试验控制系统上，系统中存在大量安控装备，应由不同的制造商生产或具有不同的设计框架。由于安控装备部署在整个装备试验控制系统中，它们会收集飞行器的飞行状态、方向信息和位置信息等，这些数据将通过通信层传输并存储在分布式存储层中。

2.2 通信层

通信层由基站和网络路由器构成。数据采集层中的安控装备通过无线连接作为点对点网络相互联结。通过这一层，收集到的数据将在整个网络中传播。

2.3 分布式存储层

分布式存储层由安全存储设备组成，能够安全地存储安控装备采集到的数据。此外，系统将为安控装备在一段时间内收集的每个数据段生成消息摘要。

2.4 共识层

共识层是区块链系统的核心算法。在一个区块链系统中，所有组成该系统的安控装备都具有相同的共识。根据所选择的共识，系统中的安控装备首先检查收集的数据的正确性，并将正确收集数据的消息摘要记录在区块链中。共识层能够确保区块链采用的数据得到大多数安控装备的信任或同意。

2.5 应用层

应用层由共识层实现。装备试验控制系统各个阶段产生的正确数据都会被记录在区块中，因此，可以开发许多基于区块链的智能合约来灵活地处理数据。并且，区块链可以将数据处理结果与决策数据进行对比，一旦出现较大差异，表明本系统判断错误时，智能合约会发出警报，防止系统受到进一步损害。

3 具体方案

装备试验安全保密要求高、时敏性强，涉及光、雷、

遥等多类、多型测量控制设备及网络通信设备，在广泛的试验区域内，存在被恶意控制、仿冒的风险，必须设计可靠有效的监管审计方案，保证试验系统的稳定安全运行。

本节以飞行器试验控制器为最小系统实例，详细描述系统具体实施方案。在飞行器飞行过程中，安控装备能够收集飞行器的飞行状态、方向信息和位置信息，并上传至智能合约。通过对飞行器的方向和位置判断，若飞行器不断靠近重点目标对象，一旦超过最短距离阈值，则智能合约触发要求飞行器自毁的指令，防止飞行器由于控制系统错乱或被敌方控制而对重点目标造成伤害。

如图 2 所示，在这个最小系统中部署了多个安控装备。其中，部分安控装备用于检测飞行器的方向信息，部分安控装备用于检测飞行器的位置信息。

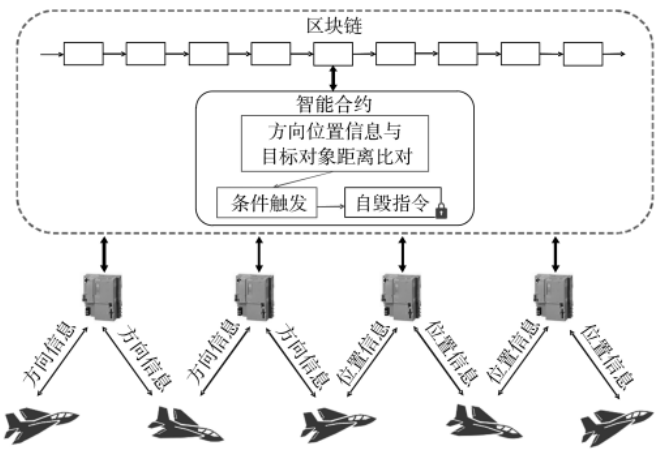

图 2　具体装备控制方案

在本系统中，安控装备可同时作为区块链的矿工，系统采用现有的委托权益证明(DPoS)共识机制。如果安控装备的计算能力有限，也可以将高性能计算机作为矿工进行挖矿，与安控装备相同，这些高性能计算机也由不同的制造商生产或具有不同的框架。系统流程如下：

(1)初始化。首先，系统执行该算法，以对系统模型的每一层进行初始化设置。在输入安全参数时，系统选择具有相对安全级别的密码算法，同时传感器之间建立点对点网络和区块链创世纪块。此外，初始化区块链参数，包括 DPoS 共识机制中的受托人个数 N。

(2)数据收集。部分安控装备收集并检测飞行器方向信息，部分安控装备收集并检测飞行器的位置信息。然后，安控装备相互传输数据摘要并将数据存储在分布式存储设备中。

(3)数据验证。受托人收集数据后，将验证数据的正确性。首先，受托人会比较不同安控装备收集的数据，如果收集到的某些数据与其他安控装备的大部分数据相差甚远，则将其丢弃。该步骤确保收集到的数据经过可信验证。

(4)区块生成。当验证数据正确，即超过一半的安控装备数据几乎相同时，受托人将摘要记录在区块中，然后将新生成的区块发布到整个系统。该步骤保证了分布式存储设备中记录的数据安全且不可篡改，同时为数据提供审计服务。

(5)智能判断。基于与装备试验控制系统相同的反馈控制方法，可以使用许多智能合约。并且，基于卡尔曼滤波器等数据处理算法，受托人会计算平均反馈输入数据，然后计算理论反馈输出数据。接着，受托人会检查飞行器与目标对象的距离是否过近(超过阈值)。一旦两者距离过近，智能合约将触发自毁指令，迫使该飞行器进行立即自毁。该步骤确保系统功能性，是整个框架的核心。

(6)区块验证。当指定的受托人发布区块时，其他安控装备会验证区块中的数据是否正确以及受托人是否诚实地进行智能判断。一旦发现块不正确，每个安控装备都可以警告操作员，并且对受托安控装备进行修理或更换；如果块被验证是正确的，各安控装备会将区块添加到现有区块链的末尾。

4 系统分析

在本系统中，安控装备或高性能计算机均可以作为矿工，挖矿产生新区块。假设安控装备或不同厂商不同架构的计算机担任矿工时，有 51%以上的矿工为诚实的，攻击者无法同时对 51%以上的安控装备或计算机攻击成功，即系统不会受到 51%算力攻击。在攻击者无法对全网进行干预的情况下，智能合约能够根据预先定义的转换规则，在实际执行和理论反馈数据相差较大时，自动执行相应的业务逻辑，向操作员发出警示，降低人在装备控制系统监管过程中的参与度，提高信息处理和审计效率。此外，系统采用的区块链技术，使得已上传至链上的工控信息不可篡改且永久记录，保障了信息审计的安全性。

本系统中，指令传达的延迟可能会对整个系统的可用性造成极大的影响。在装备控制系统中，延迟最主要来源于智能合约执行的速度和区块链自身的吞吐量。因此，对本文提出的装备控制系统中智能合约执行的延迟进行测试。测试系统为 Cent OS 7 四核处理器，具有 4 GB RAM、20 GB 硬盘，使用的联盟链为 Hyperleger Fabric v2.3，用 Go 语言编程智能合约。

如表 1 所示，本测试系统的测试用例成功传达指令 7 627 次，无失败的指令传达，发送率为 100%，即 257.7 TPS。测试系统的吞吐量在257.6 TPS 左右，平均延迟为 0.01 s，最大延迟为 0.05 s。考虑实际系统的应用场景，智能合约的延迟较低，是可接受的。

表 1　装备控制系统智能合约延迟

名称	成功次数	失败次数	发送率/TPS	最大延迟/s	最小延迟/s	平均延迟/s	吞吐量/TPS
readAsset	7 627	0	257.7	0.05	0.00	0.01	257.6

5 结论

本文针对装备试验控制系统中存在的装备试验控制信息安全问题，提出了一种基于区块链的装备试验控制信息审计与监控系统，利用区块链的去中心化、不可篡改、永久记录、可追溯、公开可验证等特性，实现非可信环境下装备试验信息的可靠记录和存储，为装备试验控制审计和统计提供支持。在此基础上，利用区块链的共识机制和算法的透明性，智能合约能够实现闭环反馈控制的全流程监督。该系统能够实现分布式装备试验控制的可信监管，具有良好的效率和较高的安全性，极大地保障了装备试验控制系统的信息安全，在实际应用中具有很高的部署价值。

参考文献

[1] 姜波，凌军，万文乾.装备大数据安全保护研究[J].国防科技，2021，42(2)：138-142.
[2] 王赟，符丽君.舰载武器装备安全射界测量与设计[J].计算机测量与控制，2015，23(5)：1595-1598.
[3] 李彤.浅谈质量在航空装备安全保障工作中的意义及影响因素[J].中国新技术新产品，2013(11)：249.
[4] 陈东恒，李新安.重视军事智能化发展安全问题[N].解放军报，2020-10-13(007).
[5] 梁新，刘宝平，李柱.建立军事装备保险机制的必要性分析[J].装备学院学报，2016，27(2)：51-54.
[6] DORRI A，KANHERE S S，JURDAK R.Towards an optimized BlockChain for IoT[C]//The Second IEEE/ACM Conference on Internet of Things Design and Implementation，IoTDI 2017. ACM，2017.
[7] ALMADHOUN R，KADADHA M，ALHEMEIRI M，et al.A user authentication scheme of IoT devices using Blockchain-enabled fog nodes[C]//2018 IEEE/ACS 15th International Conference on Computer Systems and Applications(AICCSA). IEEE，2018.
[8] SAMANIEGO M，DETERS R.Blockchain as a service for IoT[C]//IEEE International Conference on Internet of Things. IEEE，2017.
[9] YU B，JAROD W，SURYA N，et al.IoTChain：establishing trust in the Internet of Things ecosystem using Blockchain[J]. IEEE Cloud Computing，2018，5(4)：12-23.
[10] LI D，WEI P，DENG W，et al.A Blockchain-based authentication and security mechanism for IoT[C]//2018 27th International Conference on Computer Communication and Networks(ICCCN)，2018.
[11] ALPHAND O，AMORETTI M，CLAEYS T，et al.IoTChain：a Blockchain security architecture for the Internet of Things[C]//2018 IEEE Wireless Communications and Networking Conference(WCNC).IEEE，2018.
[12] AZARIA A，EKBLAW A，VIEIRA T，et al.Med REC：using blockchain for medical data access and permission management[C]//2016 2nd International Conference on Open and Big Data(OBD)，2016.
[13] 张利华，万源华，付东辉.基于区块链的用电数据存储方案[J].计算机应用与软件，2021，38(9)：21-27，52.
[14] 徐元清，卓蔚.区块链技术在烟草系统工控安全中的应用[J].微型电脑应用，2019，35(3)：113-116.
[15] MAW A，ADEPU S，MATHUR A.ICS-BlockOpS：Blockchain for operational data security in industrial control system[J]. Pervasive and Mobile Computing，2019，59：101048.

(收稿日期：2021-11-14)

作者简介：
陈峰(1974-)，男，硕士，高级工程师，主要研究方向：区块链、试验数据工程。

扫码下载电子文档

(上接第 122 页)

[11] 安轲，马宏，李英乐，等.面向电信网数据的 ETL 系统的设计与实现[J].信息工程大学学报，2020，21(4)：442-447.
[12] 刘洋.企业内部的数据孤岛现象的内在成因和解决建议[J].信息系统工程，2018(4)：93-95.
[13] 程云鹏.涉密信息系统中的应用服务安全防护解决方案[J].信息安全与通信保密，2011，9(8)：26-28.
[14] 黄承速，莫红英.信息管控平台实现与应用[J].电脑编程技巧与维护，2016(9)：67-69.
[15] 祝守宇，蔡春久.数据治理：工业企业数字化转型之道[M].北京：电子工业出版社，2020.

(收稿日期：2021-07-30)

作者简介：
南静(1987-)，女，硕士，工程师，主要研究方向：网络安全和信息化。
张天维(1994-)，男，本科，助理工程师，主要研究方向：网络安全与信息化。
陈雪飞(1997-)，男，本科，助理工程师，主要研究方向：云计算与大数据、网络安全与信息化。

扫码下载电子文档

版权声明