基于区块链的数字化指挥控制系统信息传输与追溯模式研究

杜行舟[1] 张 凯[1] 江 坤[1] 马昊伯[2]
(中国船舶工业系统工程研究院 北京 100094)[1] (北京好扑信息科技有限公司 北京 100022)[2]

摘 要 文中阐述了数字化指挥控制业务场景下的信息传输与追溯模式,典型的数字化指挥控制系统通常以对等网络拓扑运行,且能够详尽记录交互指令事务。提出了基于区块链的具备高效数据传输及关键事务追溯能力的系统设计方案,借助其加密、去中心化、防篡改的技术属性完善数据一致性、业务时效及信息安全,在持续追加数据区块的共识协议约束下实现指挥控制交互指令在系统控制端、受控端、观察端之间的完整传输及有序追溯。

关键词 区块链,指挥控制,信息安全,交互指令
中图法分类号 TP305 **文献标识码** A

Research on Blockchain-based Information Transmission and Tracing Pattern in Digitized Command-and-Control System

DU Xing-zhou[1] ZHANG Kai[1] JIANG Kun[1] MA Hao-bo[2]
(System Engineering Research Institute, CSSC, Beijing 100094, China)[1]
(Beijing Hoopox Information and Technology Co., Ltd., Beijing 100022, China)[2]

Abstract This paper stated an instruction transmission and tracing pattern in digitized command-and-control business. A typical digitized command-and-control system generally runs in a peer-to-peer network, in which each transaction of interactive instructions should be well recorded. This paper proposed a blockchain-based solution to implement efficient transmission and tracing of significant transactions which could be precisely defined by system designers. With nature attributes of encryption, decentralization and tamper resistance, blockchain-based solution focuses more on data consistency, transaction timeliness and information security. Prime events of command-and-control interactive instructions between master nodes, slave nodes and witness nodes of instruction would be completely transmitted and sequentially appended to traceable records data blocks in restraint of consensus mechanism.

Keywords Blockchain, Command-and-control, Information security, Interactive instruction

1 引言

数字化指挥控制系统是基于数字交互指令电子数据形式存储而搭建的,高效运行的指挥控制业务流需要指令控制端、受控端以及具备事后追溯功能的观察端协作实现,指令协作包括数据传输、指令校验、指令执行、业务分析、状态反馈及过程追溯等流程。随着计算机网络技术的进步,上述指令交互流程已广泛应用于军事指挥、工业生产及设备维护领域。然而,数据冗杂、架构混乱、传输失效、数据格式繁杂等严重问题成为制约指挥控制遗产系统功能实现及性能提升的潜在威胁。

区块链(Blockchain)[1]作为数字加密货币系统的新兴技术架构,已被证明可作为价值网络系统(Value Network System)[2]的可行方案。在技术方面,区块链以分布式交易或事务记录的加密数据集形式存在,同时创新性地以去中心化、安全、防篡改的方式使有价值的数据能够被对等网络中的全部节点共享。近年来,区块链的应用场景已拓展至跨境支付、信用登记、供应链管理及共享经济等领域,引领可信互联网(Trusted Internet)[3]的发展浪潮。

本文旨在提出一种基于区块链的数字化指挥控制系统设计方案,以区块链网络拓扑和业务流程为立足点,详细探讨该系统内在的信息传输与追溯模式,亦即指令交互模式。

2 数字化指挥控制系统中的区块链

2.1 面向交互指令的对等网络

一个完备的指挥控制系统通常以网络形式存在,兼具复杂性与灵活性特性的对等网络(P2P Network)通常用于模拟指挥控制系统模型[4]。系统参与者依据其在具体指挥控制业务指令交互模式中的职责分为控制端、受控端及观察端的节点,节点的对等连接组成整个指挥控制系统的价值网络。

如图 1 所示,系统节点通过其网络设备互相连接,组成内联的对等网络。在特定交互指令运行生命周期中,控制端节点以指令生成与发起者身份运作,受控端节点以指令接收与执行者身份运作,观察者节点以指令筛选过滤及数据搜集者身份运作。

杜行舟(1990-),男,硕士生,工程师,主要研究方向为电子武器与装备系统,E-mail:duxingzhou@hotmail.com;**张 凯**(1983-),男,硕士生,高级工程师,主要研究方向为电子武器与装备系统;**江 坤**(1981-),女,高级工程师,主要研究方向为电子武器与装备系统;**马昊伯**(1989-),男,主要研究方向为区块链平台与系统。

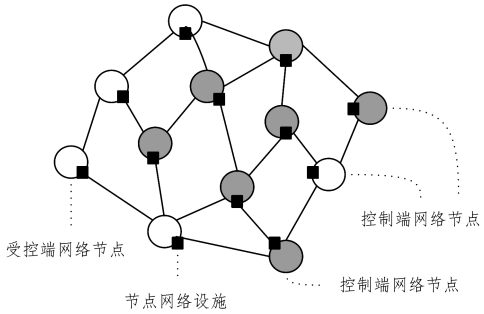

图 1　指挥控制系统对等网络示意图

现有的指挥控制系统网络设计方案通常通过在数字指令数据传输中限制节点 IP 地址、定义通信协议字段及控制字等方式使系统对网络外部节点保密，以确保指令信息的真实可信。然而，搭线窃听、数据污染和匿名攻击（如 DDoS）长期显著地威胁着网络安全，严重时可导致系统瘫痪、指令执行数据丢失等问题。此外，人为因素的系统协议外泄失密及节点协作成本的提升也是现有指挥控制系统网络设计中需要注意的关键问题。

2.2　区块链与价值网络系统设计

区块链包含一种去中心化的对等网络技术，仅依赖内部开放节点对电子数据进行加密、传输、校验及存储。在指挥控制系统视角下，区块链具备分布式数字指令交互节点的天然拓扑。不同形式的系统数据能够在控制端、受控端及观察端的节点间被传输与追溯。区块链的开源属性使得除数字签名加密的指令数据集之外的系统服务拓展更加透明并对外部请求保持开放。系统网络中的诸节点能够通过系统接口高效检索追溯归档的包含交互指令及反馈的电子数据。借助数字签名（Digital Signature）技术[5]，电子数据中存储的指挥控制信息高度可信。

2.2.1　区块链网络价值场景模型定义

基于区块链的指挥控制系统设计方案的核心概念在于定义多种潜在业务场景下的价值模型。据此，为搭建一个安全高效的信息交互渠道，通过对现有遗产系统复杂指挥控制网络拓扑进行分析归纳，抽象出指挥控制价值单元子系统[6]的必要典型场景模型。

指挥控制系统价值网络通常由多种价值单元子系统场景模型组合构成。如图 2 所示，我们定义了价值单元子系统的 4 种典型场景模型。不同的系统角色及其行为模式决定了指挥控制网络在处理交互指令过程中的运行状态。

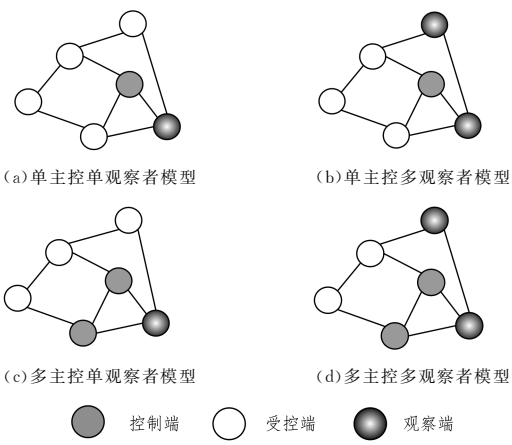

图 2　指挥控制价值单元子系统典型场景模型示意图

2.2.2　场景模型内部运行模式剖析

单主控与多主控模式主要影响交互指令元数据的发起及签名策略，该数据包含了交互指令细节及控制端数字签名信息。一个单主控节点可独立编制交互指令数据信息并在发送前执行数字签名操作将其封装为元数据。在多主控模式下，其他主控节点在特定主控节点发起交互指令后协助进行联合签名，以确保对相关交互指令元数据的认可，覆盖所有主控节点的发起意图。

单观察者与多观察者模式主要描述对于归档的交互指令及其执行反馈数据的请求方式是集中式追溯或分布式追溯。单观察者模式授权特定观察端完整的数据访问权限，包括数据获取解析及数据访问接口的管理维护权限。相对而言，在多观察模式下，数据访问权限分别部署在不同的观察端节点中，以确保能够通过分别授权实现交互指令信息追溯的节点协作。多观察者模式能够更加灵活地配置节点功能及评审流程，因此与指挥控制系统的实际应用能够进行更好的契合。

指挥控制场景模型的技术实现模式及应用实例分析如表 1 所列。

表 1　指挥控制场景分析

场景模型名称	技术实现模式	应用实例
单主控单观察者场景模型	网络报文单播，数据读-写模式	通知、公告类系统
单主控多观察者场景模型	网络报文广/组播、发布-订阅模式	物流配送、仓储管理类系统
多主控单观察者场景模型	RPC 通信，异步回调模式	设备管理，基础设施维护系统
多主控多观察者场景模型	信号槽机制、生产者-消费者模式	军事作战指挥、交通调度系统

值得注意的是，在上述场景模型分类中，受控端节点始终处于多数。一方面，对于指挥控制系统而言，其能力要求是完成交互指令的妥善执行，受控端无论以发布订阅形式响应指令还是以生产者-消费者形式响应指令，均是以集群服务节点的角色参与指令执行；另一方面，受控端节点正确解析指令并执行，期间产生的日志、状态及结果反馈数据均需由其自身完成封装并整合到历史数据集中，受控端需以并发形式完成数据归档，否则易发生单点故障，导致数据存储失效，下一节将对受控端节点处理归档数据进行详细描述。

3　基于区块链的信息传输与追溯方法

3.1　基于区块链的数据流模型

交互指令数据流是一个包含传输与追溯的动态过程，在此将通过一个分层视角呈现基于区块链的指挥控制信息传输与追溯数据流。

区块链网络依托密码学的公私钥理论搭建了图灵完备的去中心化信任机制[7]，该机制能够直接对节点相关的交互指令数据的有效性及合法性进行鉴别。如图 3 所示，基于区块链的指挥控制系统网络节点间通过其网络设备进行通信，其物理标识和设备参数以节点 ID 和 IP 地址形式表现。交互指令数据信息在数据流中随其处理过程而相继发生状态改变，存在的状态包括指令元数据（Instruction Metadata，IMD）、已签名的指令元数据（Signed Instruction Metadata，SIMD）、指令执行反馈数据（Instruction Feedback Data，IFD）、可追溯的指令执行反馈数据（Traceable Instruction Feedback Data，TIFD）。

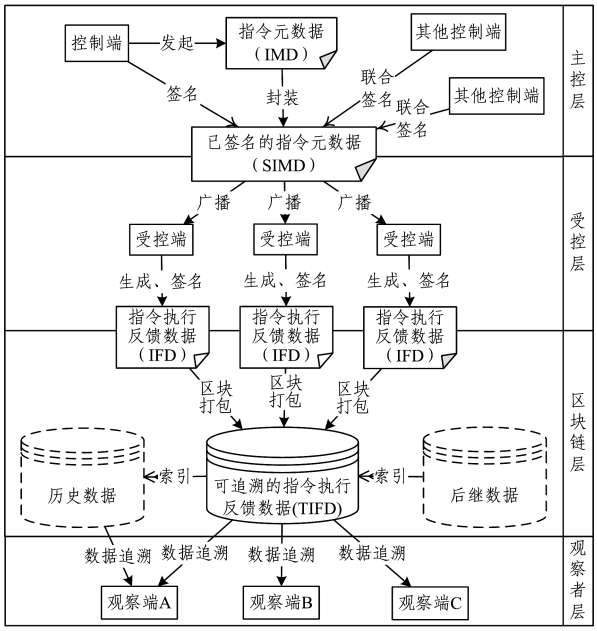

图 3 基于区块链的指挥控制系统数据流图

3.2 指挥控制信息传输与追溯流程分析

图 3 中,以交互指令生命周期诸阶段的时序为依据,将整个基于区块链的指挥控制系统网络划分为主控层、受控层、区块链层以及观察者层。

3.2.1 指挥控制信息数字签名及广播

数字签名的技术目标在于创建一个易于验证而难于伪造的算法模型,使得第三方在不持有签名方核心权限的前提下能够验证签名方是否对签名对象表达了确认。一如现实中的签名行为,我们能够确认签名人对文件、合同是否进行了审阅,但完美伪造签名人的签名具有很高的成本,数字签名技术使这个成本更加高昂。数字签名技术通过以下算法步骤实现技术目标:

$$\langle K_{public}, K_{private} \rangle = generate(seed, size) \tag{1}$$

$$\langle S_{data} \rangle = sign(K_{private}, data) \tag{2}$$

$$\langle V_{data} \rangle = validate(K_{public}, data, S_{data}) \tag{3}$$

Generate 算法以随机数种子 seed 和密钥空间大小 size 为输入生成一组密钥,包含公钥 K_{public} 和私钥 $K_{private}$。Sign 算法允许签名方使用私钥 $K_{private}$ 对给定的数据 $data$ 执行签名,得到已签名数据 S_{data}。Validate 算法允许第三方通过公钥 K_{public}、数据 $data$ 和已签名数据 S_{data} 得出签名方是否执行过签名的结论 V_{data}。据此,任一第三方在不掌握私钥的情况下即可验证签名方的签名行为,因此数字签名技术解决了匿名场景下的授权校验问题。

主控层描述了交互指令处理的初始阶段。控制端将交互指令编码为电子数据形式,生成指令元数据(IMD)。在单主控模式下,控制端对其发起的 IMD 完成数字签名即可向全网广播;在多主控模式下,其他控制端需共同完成对 IMD 的联合数字签名才能向全网传输。数字签名由控制端使用其私钥通过 RSA 或 DSA 加密算法完成[8],签名对象为 IMD 及当前系统时戳,完成数字签名后封装为已签名的指令元数据(SIMD),再向指挥控制系统网络广播。

受控层主要描述受控端对交互指令数据的接收、解析、执行及反馈过程的数据流。当受控端接受到 SIMD 后,可通过控制端公钥及系统时戳对交互指令数据进行校验鉴权,验证无误后开始执行指令。受控端对交互指令的执行日志及执行结果反馈数据可追加至 SIMD,使用受控端私钥针对追加后的数据及系统时戳进行数字签名,封装生成指令执行反馈数据(TFD)。

区块链层主要描述指挥控制系统交互指令信息及其执行反馈数据的逻辑归档过程。受控端节点签名、封装生成的 IFD 通过区块链共识协议被依次打包进区块。

3.2.2 指挥控制系统区块链共识机制

现有的区块链系统共识机制主要有工作量证明(Proof of Work,PoW)、权益证明(Proof of Stake,PoS)、委任权益证明(Delegated Proof of Stake,DPoS)、实用拜占庭容错算法(Practical Byzantine Fault Tolerance,PBFT)等[9],其设计理念及典型产品如表 2 所列。

表 2 区块链系统主流共识机制概览

共识机制名称	设计理念	典型产品
工作量证明(PoW)	通过哈希运算实现算力证明,优势算力节点对系统数据共识有较大影响	比特币、莱特币等
权益证明(PoS)	通过代币数额及持有周期实现权益定量,高权益的节点对系统数据共识有较大影响	点点币、以太坊、未来币等
委任权益证明(DPoS)	通过委托代理机制指定特定的区块生成节点,被指定的节点对系统数据共识有较大影响	比特股、AElf 等
实用拜占庭容错算法(PBFT)	基于对消息传递诸过程的同步反馈实现多节点消息一致性,当系统总节点数 $N>3f+1$ 时共识生效(f 为故障节点数)	超级帐本 Fabric 等

数字化指挥控制系统区块链为私有链(Private Chain)运行模式[10],因搭载具体业务应用服务而不能使用资源消耗较高的 PoW 机制;网络拓扑在具体的业务应用场景下较为固化,不必采用对节点数量要求较高的 PBFT 机制;控制端节点和观察端节点与用户直接交互而不参与区块打包过程,因此以受控端节点为权益代表的 DPoS 机制可作为指挥控制系统区块链的共识协议。

在区块链系统中,共识协议决定着记账节点的“挖矿”行为,如比特币系统中记账节点需找到特定算力难度目标的随机数以确保区块有效。在基于区块链的指挥控制系统中,受控端节点形成的 DPoS 核心集群承担类似比特币“挖矿”的任务,以分布式协同存储的形式动态维护整个系统的指挥控制信息数据。

区块链系统共识机制的核心原理在于用整个 P2P 网络节点资源的均衡性规避个别异常节点的不可信操作,构建整个网络的信任。比特币系统充分利用了节点的计算资源,并以全网计算资源的均衡性确保全局账本的可信,相对地,也存在 51%攻击的系统风险。基于区块链的指挥控制系统作为网络规模相对稳定的私有链系统,其可靠性设计应依托诸子系统的核心集群而构建。因此,以子系统集群能力为权益基础,基于 DPoS 共识算法搭建指挥控制信息传输与追溯模式的信任是一种适宜的设计决策。

3.2.3　指挥控制系统信息归档与追溯机制

通过共识协议，IFD 数据被打包放入区块[9]中，封装形成可追溯的指令执行反馈数据（TIFD）。每一项 TIFD 在追加进区块链时会索引当前链首的 TIFD 区块，进而形成持续增长的 TIFD 区块链，随着后续区块的跟进索引，已归档的 TIFD 区块篡改复杂度也持续提升[11]，增强了系统数据的安全性。同时，受控端作为 DPoS 核心节点，实现了去中心化的 TIFD 区块归档，规避了系统运行中的单点故障类问题，增强了系统网络的健壮性。

观察者层则呈现了观察端对指挥控制信息数据的追溯模式。持续增长的 TIFD 区块中整合封装了交互指令数据、控制端身份及时戳、指令执行日志、指令执行状态及结果、受控端身份及时戳。具备权限的观察端节点可针对获取的 TIFD 进行校验与解析，从而追溯交互指令各业务阶段及相关指挥控制网络节点的信息。在多观察者模式下，观察端节点可分布式部署[12]，并依靠特定业务权限及审核流程执行信息追溯。TIFD 索引式的数据组织能够提升观察端的数据追溯效率，同时规避了数据版本混杂等一致性问题。

观察端节点对于指挥控制信息的追溯技术实现亦因区块链技术的引入得以拓展。现有遗产系统通常通过 WebService 等形式实现数据追溯接口，而在区块链领域，侧链索引、闪电网络、智能合约技术[8]能够使信息追溯业务流程更加灵活。通过侧链索引技术，可以直接构建并发演进系统间的索引关联，共享指挥控制资源信息；通过闪电网络技术，能够实现高效的跨系统实时通信；通过智能合约技术，可以将信息追溯业务逻辑直接提交，符合规则的节点行为可自动触发关联的指挥控制信息追溯业务。

综上，指挥控制交互指令数据，分别经历了主控层控制端发起、签名，受控层受控端解析、执行、封装、签名，区块链层索引、归档，观察者层访问、追溯的生命周期，并通过生命周期动态构建了指挥控制业务数据流，促进整个系统网络节点的协同，完成交互指令的传输与追溯以实现指挥控制业务目标。在系统安全方面，区块链技术的引入也实现了交互指令整个生命周期记录的可验证以及交互指令执行完成后归档数据的防篡改，极大提升了指挥控制业务系统的可靠性。

4　结论

本文所提出的基于区块链的数字化指挥控制系统信息传输与追溯模式可在现有系统部署模式维持不变的基础上，通过对消息层与数据层业务服务进行重构来实现。具体描述如下：

1）消息层重构，将点播数据报重构为全局组播/广播数据报，并统一数据报内部业务单元信息格式（即规范全网元数据）；

2）数据层重构，将中心化数据存储重构为分布式数据冗余存储，对业务单元信息数据的接收发送增加数字签名鉴权机制，只有通过鉴权的数据方可被分布式节点存储；

3）分布式协同重构，通过 DPoS 共识机制实现数据分片（Sharding）间的同步，基于分布式系统一致性、分区容忍性设计原则实现诸子系统集群间的数据协同。

本文通过对数字化指挥控制系统信息传输与追溯模式的剖析，结合区块链系统去中心化、防篡改的技术优势，提出了基于区块链的数字化指挥控制信息系统设计方案。同时，通过对以区块链网络为骨干的指挥控制系统的分层架构及数据流的阐述，阐明该方案对指挥控制典型业务场景需求的实现策略，并针对指挥控制私有链共识机制的选择给出了设计决策，在文末对相关技术验证实验进行了初步规划。

结束语　本文基于对数字化指挥控制系统业务复杂场景进行的抽象与归纳，以区块链系统网络为基础对数字化指挥控制系统信息传输与追溯模式进行了重构。后续的研究工作将主要围绕私有链时统服务、交互指令数据广播洪泛及系统实时性优化等问题展开。

参 考 文 献

[1] NAKAMOTO S. Bitcoin：A Peer-to-Peer Electronic Cash System[Z]. 2008.

[2] ALLEE V. Value network analysis and value conversion of tangible and intangible assets[J]. Journal of Intellectual Capital，2008，9(1)：5-24.

[3] GOL MOHAMMADI N，et al. Trustworthiness Attributes and Metrics for Engineering Trusted Internet-Based Software Systems. International Conference on Cloud Computing and Services Science[J]. Communications in Computer and Information Science，2013，453：19-35.

[4] GUPTA R A，CHOW M Y. Networked Control System：Overview and Research Trends[J]. IEEE Transactions on Industrial Electronics. 2010，57(7)：2527-2535.

[5] 邵奇峰，金澈清，张召，等. 区块链技术：架构及进展[J/OL]. 计算机学报，2017：1-20. http://kns. cnki. net/kcms/detail/11.1826. TP. 20171115. 2302. 006. html.

[6] DIMARIO M J. System of systems interoperability types and characteristics in joint command and control[C]// IEEE/SMC International Conference on System of Systems Engineering. 2006.

[7] PILKINGTON M. Blockchain Technology：Principles and Applications[J]. Social Science Electronic Publishing，2015.

[8] NARAYANAN A，BONNEAU J，FELTEN E，et al. Bitcoin and Cryptocurrency Technologies：a Comprehensive Introduction[M]. Princeton University Press，2016.

[9] 韩璇，刘亚敏. 区块链技术中的共识机制研究[J]. 信息网络安全，2017(9)：147-152.

[10] 沈鑫，裴庆祺，刘雪峰. 区块链技术综述[J]. 网络与信息安全学报，2016，2(11)：11-20.

[11] XU X W，et al. The Blockchain as a Software Connector[C]// 13th Working IEEE/IFIP Conference on Software Architecture (WICSA). 2016.

[12] KISHIGAMI J，et al. The Blockchain-Based Digital Content Distribution System[C]// IEEE Fifth International Conference on Big Data and Cloud Computing. 2015.