文章编号:1001-506X(2022)09-2817-09
网址:www.sys-ele.com

基于区块链的动态指控方法研究

潘永淇[1,2],魏 巍[1,*],刘 毅[2],朱 承[2]
(1. 国防科技大学信息通信学院,湖北 武汉 430000;
2. 国防科技大学信息系统工程重点实验室,湖南 长沙 410000)

摘 要:面向动态指控过程中指挥权限跨域重构与资源点对点动态调配需求,基于区块链技术设计了动态指控组织架构模型,在此基础上分别研究了基于认证联盟与共识阈值的权限流转模型、基于任务表单和装备表单的任务执行模型,并依托智能合约建立了应急响应机制,为动态指控中指挥权限可信流转与装备点对点访问提供了解决方案。通过 Hyperledger Fabric 搭建原型系统,实验结果证明了方案具备可信性与较好的运行效率。

关键词:区块链;动态指控;权限流转;智能合约
中图分类号:TP 399 **文献标志码**:A **DOI**:10.12305/j.issn.1001-506X.2022.09.15

Blockchain based method of dynamic command and control

PAN Yongqi[1,2], WEI Wei[1,*], LIU Yi[2], ZHU Cheng[2]
(*1. College of Information and Communication, National University of Defense Technology, Wuhan 430000, China;*
2. Science and Technology on Information Systems Engineering Laboratory, National University of Defense Technology, Changsha 410000, China)

Abstract: Facing the requirements of cross-domain reconfiguration of command authority and point-to-point dynamic reallocation of resources in the process of dynamic command and control, corresponding organization structure model based on blockchain technology is designed, and on this basis, the authority transfer method based on the authentication alliance and the consensus threshold, as well as the task execution model based on task list and equipment list are studied. An emergency response system with blockchain smart contract mechanism is established and it provides a solution for trusted flow of command authority and point-to-point access to equipment in dynamic allegations. A prototype system is built with Hyperledger Fabric, and test results show feasibility and good efficiency of our solutions.

Keywords: blockchain; dynamic command and control; authority transfer; smart contract

0 引 言

动态指挥控制是一种指控构成要素能实时适应任务特征,并通过动态匹配调节,最大限度满足作战资源发挥效能的指挥控制体系[1]。随着现代战争步入信息与智能化时代,战场环境瞬息万变,任务内容复杂多样,作战样式呈现出有人无人协同、多域融合与跨域攻防等作战特点[2],能够打破军种、领域之间的界限,实现陆、海、空、天、网等力量在各作战域、各层级、各地域间整合协同的动态指控方法愈发成为军事理论研究的热点方向。

然而,传统的军事指挥控制系统中,由于采用了常见的 C/S 架构设计[3],多形成了层级式、预设式体制,主要存在以下弊端:① 组织结构固化、审批流程复杂。信息指令传递需要层层反馈逐级下达,这导致双向信息在传递过程中速度缓慢,且易造成变形或流失,影响了指挥控制效率。② 跨域权限交互过程中缺乏有效信任机制。现行体制下指挥关系以及任务权限在行动前按照层次化原则进行预设,如需调整则需要多方协商并取得上级指挥所的确认授权,导致各作战领域跨域合作难,不易调配资源。③ 应急响应能力不足。面对突发情况,部队或资源难以实现按需动态组合。

收稿日期:2021-06-21;**修回日期**:2021-09-01;**网络优先出版日期**:2022-03-03。
网络优先出版地址:https://kns.cnki.net/kcms/detail/11.2422.TN.20220303.1816.026.html
基金项目:国家自然科学基金面上项目(71571186)资助课题
*通讯作者.
引用格式:潘永淇,魏巍,刘毅,等. 基于区块链的动态指控方法研究[J]. 系统工程与电子技术,2022,44(9):2817-2825.
Reference format: PAN Y Q, WEI W, LIU Y, et al. Blockchain based method of dynamic command and control[J]. Systems Engineering and Electronics, 2022, 44(9): 2817-2825.

针对传统指挥控制模式存在的不足，利用区块链技术去中心化、灵活可信特点支撑军事指挥控制活动，并应用于跨域协同与权限控制的方法开始逐步受到学者们的关注。Zhu 等人[4]指出了区块链对提高军队作战效能的重要作用，并分析了其应用于军事管理、安全以及指挥的技术优势。Raja 等人[5]则进一步阐述了将多个区块链应用于战场的用例场景，包括资源管控以及行动监管等方面。文献[6－8]从资源管控的角度分析研究了基于区块链的军事供应链，提高了资源管控的性能和安全性，但未给出跨域协作的方法。文献[9－12]则从通信的角度提出了区块链如何保护和管理数据以及防范恶意攻击，为权限管控与跨域协同提供了保障；赵国宏[13]讨论了区块链技术对现行作战以及管理模式的影响，提出了分散式指挥决策和指挥控制等核心应用及指控授权的技术路线。王飞跃等人[14]则将平行智能与区块链技术结合并引入军事信息系统，从而优化指挥决策。刘毅等人[15]进一步面向敏捷指控的需求，提出了区块链赋能下的跨域协同方法，引入商业交易系统中“通证化”模式赋能权限转移，以确保权限转移的灵活高效与安全性。但文献[14－15]并未提供支撑动态指控授权的区块链组织架构，也没有给出动态权限流转的完整模型。刘瑞等人[16]结合陆军的指挥架构设计了基于区块链分级分域的“兵器链”，通过适应性选择智能合约与共识库支撑跨域认证与权限管理。杜行舟等人[17]则从区块链架构及指令交互流程两方面重构了指令信息传输与追溯模式，提升了指控业务的可靠性，但文献[16－17]仅关注了节点的管理方式，未针对性给出资源访问权限或指挥权限的管控方法。巫岱玥等人[18]则将“多链”结构应用于信息系统为分层节点划分权限，从而保障数据的访问可控与安全性。舒展翔等人[19]从区块链架构和权限策略集角度，通过设计“多链”区块链架构和制定相关用户权限策略构建了贝尔-拉帕杜拉模型(Bell-lapadula model，BLP)，实现了灵活的指挥信息系统用户权限管控设计，但文献[18－19]主要是针对域内权限以及信息资源的高效访问与控制，而对于跨域权限动态流转并未形成有效的解决方案。Wrona 等人[20]利用区块链技术为各类传感器数据存储与交互设计了体系结构，实现了跨域传感器的可信点对点交互。文献[21]则基于区块链构建了无人机协作系统，实现了无人机数据等资源的共享，但文献[20－21]主要针对无人设备的数据共享与交互，对于有人场景下的权限跨域流转未给出方案。综上可知，目前区块链技术应用于指挥控制领域，主要从网络架构、节点管理、数据访问以及权限控制 4 个方面进行改进，但对于数据及权限的管理尚集中于节点相对固定和仅可在域内交互的阶段，针对节点灵活管理和权限的跨域动态流转，未有较好的解决方案。

针对上述问题，本文提出了一种基于区块链的动态指控方案，使得任务单元可以根据任务需求改变指挥协作关系，实现灵活的权限交互和资源调配。本文的主要研究内容及贡献如下：① 提出了组织架构设计，使层级式组织架构向扁平化、分布式转变。② 设计了权限管控机制，实现了从固定式权限管控方法向基于认证和规则的方法转变。③ 针对任务执行模式进行设计，实现了从预设式任务执行模式向灵活可定义、互监督、分布式执行的智能合约模式转变。④ 设计了相应的数据管理方法，实现了中心化的数据管理向互鉴证分布式的转变。本文在 Hyperledger Fabric 框架下开发了测试样例，结果证明了该方案具备可行性与较好的运行效率。

1 组织架构模型

指控组织是由战场任务驱动的指控实体相互关系及其规范化行动的集合。美国国防部部长助理办公室研究室主任 Alberts 认为指控组织中主要包括决策实体、感知实体、执行实体，整个作战活动围绕这 3 种实体进行[22]。本文在此基础上以指挥控制协同能力为目标给出动态指控过程的 3 类参与节点，定义如下：

(1) 指控节点(node_cmd)：发布任务，下达指令，管理指挥权限，对其他节点实施控制的单元，是指控组织的决策核心；

(2) 信息节点(node_info)：针对作战任务，负责指令及信息的传递与交互的单元，是指控组织的交互核心；

(3) 装备节点(node_equip)：执行作战任务的装备资源(战机、战车等)，是指控组织任务实施的载体。

这 3 类节点即可构成一个基本的指控组织单元。在每个组织单元内部，3 类节点采用如图 1 所示的模式进行交互。

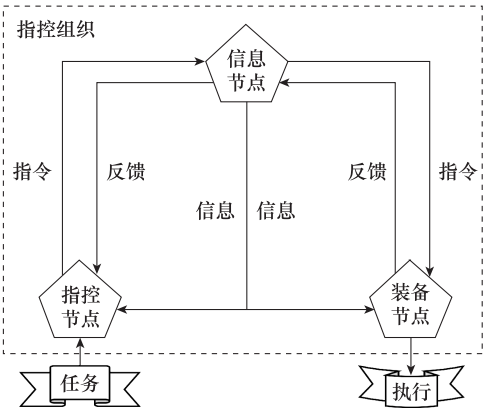

图 1 指控组织单元内实体交互模式

Fig. 1 Interaction pattern of entities within the command and control organizational unit

其典型交互模式为：指挥员通过指控节点实施指挥控制活动，将指挥指令提交信息节点并接收反馈；信息节点负责指令等信息的传递与转达，以及区块链系统的共识功能；装备节点负责管控装备资源，通过链接到信息节点上完成相应的业务活动。其中信息节点作为各单元间相互连接的对等节点，使跨组织的资源共享以及权限管理可以避免树形结构的多层审批，直接进行交付。

结合作战环境下各级指控组织的拓扑结构与高效可信的动态权限流转需求，组织单元间可进一步建立区块链网络连接关系，构建指挥控制网络拓扑模型[23]。图 2 展现了

不同领域、不同层级组织间的连接与交互关系。其中，Org1 是领域 A 的组织，Org1_1 是 Org1 的下级组织，Org2 是领域 B 的组织，Org2_1 是 Org2 的下级组织，各组织信息节点是建立组织间连接关系的锚点，并为跨域的指令下达与权限流转提供通信机制；Ordering service 是由各个指控组织专属的信息验证节点构成的认证联盟[24]，为系统提供认证服务，其中 Order1 至 Order4 分别是来自 4 个组织的具有验证功能的信息节点，共同负责为区块链网络模型中各组织的节点、用户等提供数字证书生成、身份认证服务以及参与区块链数据的维护与管理，通过认证联盟使得各个指控单元可在有监管下进行点对点交互，为资源共享以及权限流转提供了支撑。

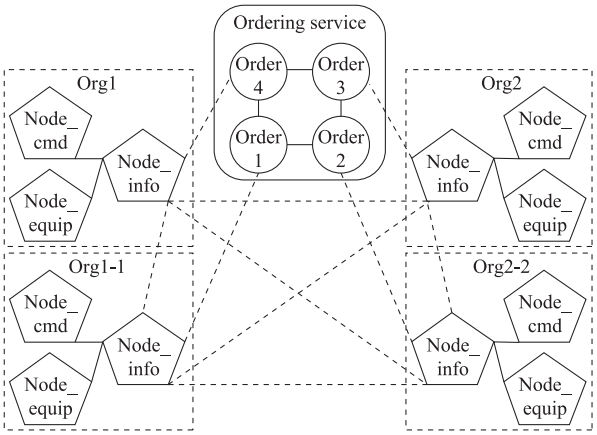

图 2　区块链网络模型

Fig. 2　Blockchain network model

为了确保任务的机密性和实现不同任务间的数据隔离，本文引入了任务通道机制[25]，为每个任务过程创建一个通道，通道内仅包含对应任务所涉及的组织。本文第 3 节将对任务通道进行详细说明。

通过上述组织架构设计，我们将层级式的组织结构变得更加扁平化，提高了组织的去中心化水平与抗毁能力，为实现动态指控授权建立了组织基础。

2　权限管控模型

权限管控机制是跨域协同的运行规则支撑。本节从节点管理和权限流转两个方面设计了动态指控中的权限管控模型。

2.1　节点管理规则

本文在考虑指挥层级关系的基础上，基于认证联盟设计组织与节点的准入与退出规则。

2.1.1　组织加入规则

除了构建认证联盟时的初始组织，其余的组织加入区块链网络需要得到一定数量的已加入组织的认可，以此保证组织跨域协作的可信度。设 $O=\{O_1,O_2,\cdots,O_n\}$ 是已加入网络的组织集合，O_i 为 O 中已存在的组织，$\mathrm{VPT}_{\mathrm{org}}$ 是组织准入的共识阈值，阈值确定常用规则有简单多数原则、2/3原则、80％原则[26]等，根据不同任务场景严格或者松散程度要求，选取不同的阈值设定原则，$\alpha=\{\alpha_1,\alpha_2,\cdots,\alpha_n\}$ 为已加入网络组织的公信力[27]集合，可以依据指挥体系的特点灵活设置或调整各组织的公信力大小，公信力设置原则可依据组织的层级、具备的资源以及参与协同任务的信誉评价等[28]。Permitted() 为判别组织 O_i 是否认可组织 O_j 的函数，通过收集投票信息来赋值：

$$\mathrm{Permitted}(O_i,O_j)=\begin{cases}1, & \text{认可}\\ 0, & \text{不认可}\end{cases} \tag{1}$$

则组织 O_j 想要加入区块链网络，须满足：

$$\sum_{i=1}^{n}\alpha_i\cdot\mathrm{Permitted}(O_i,O_j)\geqslant\mathrm{VPT}_{\mathrm{org}} \tag{2}$$

即在联盟各组织公信力加权投票数满足预设阈值条件下，批准新组织的加入请求。

2.1.2　节点加入规则

指控节点或装备节点的加入需要其所隶属组织的认可，同时也需要网络中一定数量的组织的同意，以确保节点的高可信度。若 Node 为申请加入的节点，$\mathrm{VPT}_{\mathrm{node}}$ 为节点准入的共识阈值，O_{belong} 是要加入网络的节点所隶属的组织，则指控或装备节点加入网络，需满足：

$$\begin{cases}\sum_{i=1}^{n}\alpha_i\cdot\mathrm{Permitted}(O_i,\mathrm{Node})\geqslant\mathrm{VPT}_{\mathrm{node}}\\ \mathrm{Permitted}(O_{\mathrm{belong}},\mathrm{Node})\neq 0\end{cases} \tag{3}$$

即在本级组织同意基础上，联盟各组织公信力加权投票数满足预设阈值条件，才能批准新节点的加入请求。

2.1.3　退出网络规则

指控节点或装备节点退出网络仅需其所隶属组织的认可。若 Node 为申请退出网络的节点，O_{belong} 是要退出网络的节点所隶属的组织，则指控或装备节点退出网络，需满足：

$$\mathrm{Permitted}(O_{\mathrm{belong}},\mathrm{Node})\neq 0 \tag{4}$$

即在本级组织同意情况下，批准节点的退网请求。

2.2　权限流转规则

动态指挥控制的过程主要涉及到指挥权限转让和装备资源的点对点按需调度。本文重点针对指控和装备访问权限的授予与取消过程，设计权限流转的规则。

2.2.1　基于阈值的权限授予规则

权限授予包含指挥权限和资源访问权限的授予。组织 O_i 在组织 O_j 加入区块链网络后，可以依据任务需要向 O_j 授予部分权限，除 O_i 需要对权限授予行为进行签名，也需要一定数量组织的签名。$\beta=\{\beta_1,\beta_2,\cdots,\beta_n\}$ 为网络中各组织签名的效用值集合，各组织签名的效用值依据其授予权限组织的层级关系及领域相关度决定，$\mathrm{VPT}_{\mathrm{right}}$ 是权限流转的共识阈值。Sign() 是判别组织 O_i 是否签名的函数：

$$\mathrm{Sign}(O_i)=\begin{cases}1, & \text{是}\\ 0, & \text{否}\end{cases} \tag{5}$$

则组织 O_i 进行权限授予需满足：

$$\begin{cases}\sum_{k=1}^{n}\beta_k \cdot \mathrm{Sign}(O_k) \geqslant \mathrm{VPT}_{\mathrm{right}} \\ \mathrm{Sign}(O_i) \neq 0\end{cases} \tag{6}$$

即在本级组织签名基础上，联盟各组织签名的加权效用值满足预设阈值条件，才能批准权限的授予行为。

2.2.2 基于阈值的权限取消规则

权限取消包含指挥权限和资源访问权限的收回，分为主动归还与被动收回两种模式。如需取消组织 O_i 对组织 O_j 授予的权限，主动归还模式下由组织 O_j 发起取消申请并签名，被动收回模式则由组织 O_i 发起并签名，两种模式均需要一定数量组织的签名批准：

$$\begin{cases}\sum_{k=1}^{n}\beta_k \cdot \mathrm{Sign}(O_k) \geqslant \mathrm{VPT}_{\mathrm{right}} \\ \mathrm{Sign}(O_i) + \mathrm{Sign}(O_j) \neq 0\end{cases} \tag{7}$$

即权限授予组织或被授予组织签名的前提下，联盟各组织签名的加权效用值若满足预设阈值，则批准权限的取消行为。

3 任务执行模型

动态指控任务执行包含任务指挥权限转移、资源访问权限转移以及应急响应权限转移 3 个主要场景，权限的授予与流转过程在前述管控规则下通过智能合约执行实现。

为保证任务间保密性和通信效率，本文为每项任务构建专用任务通道，任务通道是特定任务成员相互通信的专用“子网”，任务相关事务都在任务通道中执行。任务相关方加入通道，并在身份验证和授权后才能在该通道上完成业务，装备的借调同样在任务通道中进行，通道账本记录了装备调配的过程以及一项任务的完整过程。完成任务时将任务通道的账本数据经过 Hash 运算形成任务链 Hash 存储在系统的总账本中。

3.1 任务指挥权限转移

本文在区块链任务通道中基于任务表单[29]设计了任务指挥权限转移方案。

任务表单是包含了当前任务预设信息的规范化数据，以智能合约的形式在任务通道中流通，根据任务阶段和条件不同具备不同的状态标签。其典型数据结构如表 1 所示。

表 1 任务表单数据结构

Table 1 Data structure of the task table

字段	解释
MissionID	任务编号
State	任务表单状态
Applicants	受领任务组织
Content	任务基本内容
Authority	指挥权限
ReleaseTime	任务发布时间
ChangeTime	任务调整时间
FinishTime	任务完成时间
Result	任务完成情况
Evaluation	任务效果评估

任务指挥权限转移包含了任务发布与申领、任务动态调整和任务完成与反馈 3 个主要环节。如图 3 所示，3 个环节的主要交互流程相近，但内涵的具体业务逻辑不同。

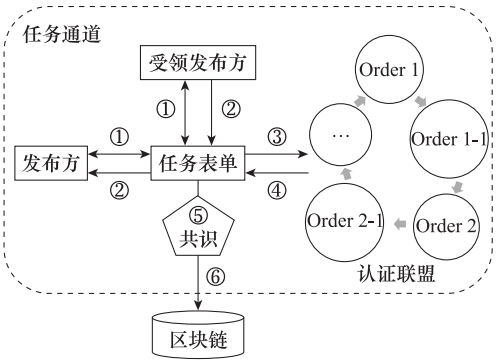

图 3 任务指挥权限转移流程

Fig. 3 Process of command authority transfer

3.1.1 任务发布与申领

任务发布与申领主要划分为两种模式：任务申领模式及任务指派模式。其中任务申领模式引入众包的思想，生成任务的组织负责任务发布，而相关组织根据自身情况进行申领。任务发布方、受领方与认证联盟加入任务通道，任务申领的流程如下。

(1) 任务发布阶段

① 任务发布方读取链上合约模板，构建初始任务表单；

② 发布方更新表单 Content 项，并将表单 State 字段设置为“发布”，对表单签名；

③ 表单在任务通道中广播；

④ 认证联盟进行验证与签名，并生成任务发布事务；

⑤ 事务提交任务通道中进行共识同步；

⑥ 事务共识成功后提交通道事务区块。

(2) 任务申领阶段

① 通道之中其他组织的指控节点读取 State 字段值为“发布”的任务表单；

② 受领方对任务表单发出受领申请，填写 Applicants 字段信息，并修改 State 字段为“待批”，并对表单签名；

③ 表单在任务通道中广播；

④ 认证联盟进行验证与签名，并生成任务申请事务；

⑤ 事务提交任务通道中进行共识同步；

⑥ 事务共识成功后提交通道事务区块。

(3) 任务确认阶段

① 发布方读取 State 字段值为“待批”的表单；

② 发布方对受领方进行审核决定是否交由其执行，若同意则完善任务表单，将任务需要的权限填入表单的 Authority字段，对表单签名；

③ 表单在任务通道中广播；

④ 认证联盟依据权限授予规则进行验证签名，若达到

阈值要求即将表单 State 字段设为“执行”，并生成任务确认事务；

⑤ 事务提交任务通道中进行共识同步；

⑥ 事务共识成功后提交通道事务区块。

受领方通过签名及时间戳对任务数据和指挥权限进行校验，验证无误后受领方即可具有对应的指挥权限并开始执行任务。

除了申领模式，有些任务则需要指派特定的组织进行完成，这即是任务执行的另一种情形，任务指派模式。发布方将表单信息按照确认阶段的标准填写，任务执行方接受确认后即可进入任务执行阶段，相关事务在链上同步记录。相较于任务申领模式，指派模式具有较高的效率，适用于目的明确、指向性强的任务场景。

3.1.2　任务动态调整

在任务执行的过程中考虑到战场环境变化等因素，需要对任务指挥权限、任务内容等要素进行灵活调整以实现动态指控要求。任务调整流程的步骤如下：

(1) 任务发布方读取 State 字段值为“执行”的任务表单；

(2) 发布方更新任务细节或权限填入 Content 项或 Authority 项并签名；

(3) 表单在任务通道中广播；

(4) 认证联盟对其进行验证与签名，若满足权限授予规则与权限取消规则，任务表单即可更新成功，并生成相应事务；

(5) 事务提交任务通道中进行共识同步；

(6) 事务共识成功后提交通道事务区块。

任务执行方依据更新后的任务内容与任务指挥权限执行任务。

3.1.3　任务完成与反馈

任务执行的结果需要反馈给发布任务的组织进行审核，以此评估任务执行的效果，并决定是否结束任务，分为反馈与审核两个阶段，步骤如下：

(1) 反馈阶段

① 任务受领方在任务完成时从链中读取 State 字段值为“执行”的任务表单；

② 受领方将任务完成情况写入任务表单 Result 字段，同时修改 State 字段为“待审核”，并对修改后的表单签名；

③ 表单在任务通道中广播；

④ 认证联盟进行验证与签名，生成任务反馈事务；

⑤ 事务提交任务通道中进行共识同步；

⑥ 事务共识成功后提交通道事务区块。

(2) 审核阶段

① 任务发布方读取链上 State 值为“待审核”的任务表单；

② 发布方对执行情况进行审核和评估决定任务是否已完成，若认可任务执行情况则填写 Evaluation 字段信息并将 State 字段更新为“完成”，并对表单进行签名；

③ 表单在任务通道中广播；

④ 认证联盟依据权限取消规则进行验证与签名，生成任务审核事务；

⑤ 事务提交任务通道中进行共识同步；

⑥ 事务共识成功后提交通道事务区块。

此时，任务表单已无法继续修改，任务执行方的指挥权限也已被收回。

3.2　资源访问权限转移

除了任务执行时指挥权限的流转，还需要对资源权限进行管理，装备的权限流转同样在任务通道中进行。与任务表单类似，本文基于装备表单实现装备点对点按需调配和权限流转。其典型数据结构如表 2 所示。

表 2　装备信息数据结构

Table 2　Data structure of equipment information

字段	解释
EquipID	装备编号
State	装备状态
Owner	装备所属组织
Kind	装备类型
Description	装备基本描述
Content	装备借调信息
Secondment	装备借调组织

3.2.1　装备借调

通道中的组织可以借用其他组织处于闲置状态的装备，流程如图 4 所示，分为申领阶段与批复阶段。

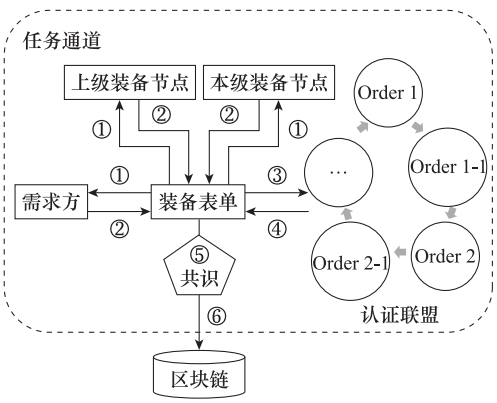

图 4　装备申领流程

Fig. 4　Equipment application process

(1) 申领阶段

① 需求方读取 State 字段为“闲置”的装备表单；

② 需求方对装备表单的 Content 字段更新装备请求，修改 State 字段为“待批复”并签名；

③ 表单被发布到通道中广播；

④ 认证联盟对事务进行验证并签名，生成装备资源申

领事务；

⑤ 事务在通道中进行共识；

⑥ 若共识成功即将事务提交通道事务区块。

(2) 批复阶段

① 本级组织的装备节点与上级组织的装备节点均可读取 State 字段为“待批复”的装备表单，查看表单的 Content 项并进行审核批复；

② 若本级组织的装备节点同意且上级组织装备节点未提出拒绝，或是上级组织的装备节点同意(无论本级组织同意与否)，则将装备表单的 State 字段更新为“借调”并签名；

③ 表单在通道中进行广播；

④ 认证联盟依据权限授予规则对申请进行验证与签名，若符合阈值标准便形成批复事务；

⑤ 事务交由通道成员进行共识；

⑥ 若共识成功即将事务提交通道事务区块。

参照文献[30]，装备的逻辑与物理访问权限的具体管控方法可以借助基于 Hash 计数器的权能令牌实现。

3.2.2 装备归还

当需求方结束装备使用或者是装备所属方的本级装备节点因任务需求等原因需收回装备，则需要执行装备归还操作，分为主动归还与被动收回两种模式，如图 5 所示，其中虚线为被动收回模式，实线为主动归还模式。步骤如下：

(1) 需求方或装备所属方的本级装备节点读取 State 项为“借调”的装备表单；

(2) 填写表单的 Description 字段，并更新表单的 State 项为“归还”；

(3) 表单在通道中进行广播；

(4) 认证联盟依据权限取消规则对事务验证，若符合阈值要求则进行签名，并生成归还事务；

(5) 事务交由通道成员进行共识；

(6) 若共识成功即将事务提交通道事务区块。

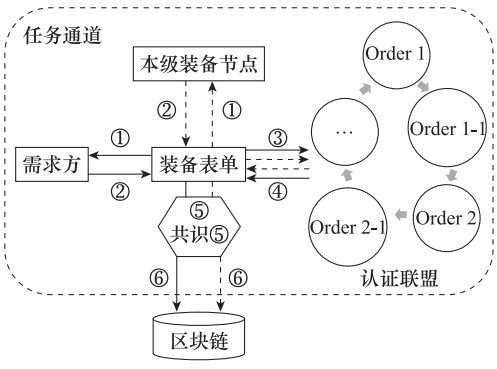

图 5 装备归还流程

Fig. 5 Equipment return process

此时装备中计数器进行迭代。当装备闲置时，本级组织的装备节点可以将装备状态从归还更新为闲置，供下一步装备借调。

3.3 应急响应权限转移

为减轻指挥员及参谋的记忆压力，强化应急响应能力提高响应效率，本文通过将触发应急响应的条件与相应的应急响应方案编写成应急响应智能合约库形成自动化、智能化的高效响应机制，满足应急响应条件即可实现相应的指挥权限及资源权限的获取，应急响应过程如图 6 所示。

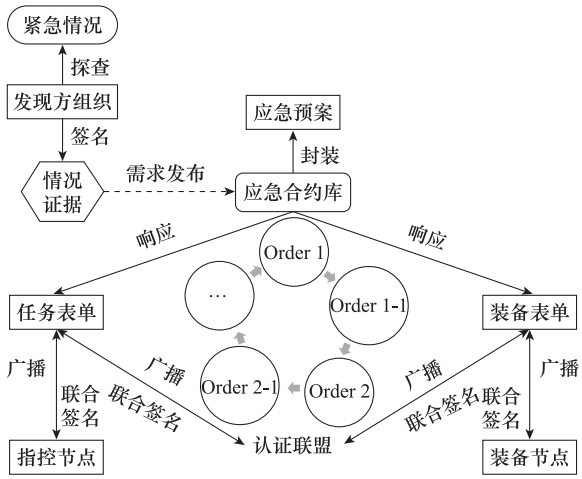

图 6 应急响应流程

Fig. 6 Emergency response process

发现情况的节点将紧急情况的证据以及私钥签名作为事务输入，由智能合约判定是否符合条件，若符合则将其广播到区块链网络进行共识，若共识成功则触发相应的规则集，规则集则预设了需要执行的任务类型以及需要提供的资源，并给出了任务表单以及装备表单模板，指挥员仅需要根据情况填写执行方等信息从而进行任务表单创建及权能令牌的建立，而应急响应需求则可作为任务基本内容或装备借调理由供相应组织进行快速审核与共识。

4 指控事务记录模型

本文基于 Hash 链设计了指控事务记录模型，用于存储任务通道中任务执行相关的数据记录，形成指控事务区块链。

指控事务区块链按照时间顺序对网络中发生的事件进行记录，包括任务执行事件和装备权限操作事件。任务执行事件主要记录包括时间戳信息、任务通道标签、发布任务节点、受领任务节点、任务表单 Hash 值等信息，装备权限操作事件则记录包括时间戳信息、执行操作的节点、装备表单 Hash 值、装备操作类型等信息。每条记录均含有由时间戳标记的前序事件的 Hash 值，由此形成了链接关系，任务执行事件和装备权限操作事件均记录在任务通道账本，如图 7 所示。通过使用任务表单 Hash 与装备表单 Hash 进行 Hash 寻址，建立指控事务区块链与任务表单及装备表单的关联关系。

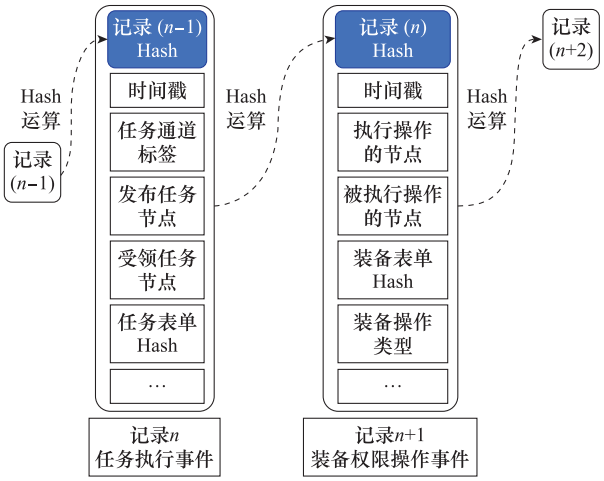

图 7　指控事务区块链结构

Fig. 7　Structure of command and control affairs blockchain

5　实验验证与分析

实验采用 Hyperledger Fabric[31] 作为区块链架构实现了文中主要业务过程，并采用 Hyperledger Caliper[32] 工具对性能指标进行测试，总体环境配置如表 3 所示。

表 3　测试环境配置信息

Table 3　Configuration information of the test environment

名称	指标/版本
CPU	Intel(R) Core(TM) i7-7700HQ 2.80 GHz
内存(RAM)	8 GB
Ubuntu	20.04
go	1.15.6
fabric	2.3
docker	20.10.1
docker-compose	1.25.0
caliper	0.4.2
node	10.19.0

参照文献[33]，本文将核心业务划分为数据读取、验证签名、完整交易、共识、数据上链几个阶段，并以此给出核心业务所需时间的计算方式，其中不同阶段所需时间的符号表示如表 4 所示。

表 4　符号表示

Table 4　Symbolic representation

名称	解释
t_1	读取链上数据的时间
t_2	验证与签名所需时间
t_3	调用智能合约完成事务所需时间
t_4	广播及数据同步等共识过程所需时间
t_5	数据上链的时间

则核心业务所需时间 t_{all} 为

$$t_{all}=\mathrm{sum}(t_1,t_2,t_3,t_4,t_5) \tag{8}$$

通过以任务指挥权限转移过程为代表测试时间 t_{all}。则事务处理效率

$$E=\frac{1}{t_{all}} \tag{9}$$

在此过程中，节点间因为共识与通信等因素产生事务延迟，主要包括节点间共识延迟与通信延迟[33]，而延迟由于网络抖动分为最大延迟、平均延迟以及最小延迟。

在典型的跨域协同指控场景中，一般包含跨域协同需求组织、跨域协同组织以及它们的联合指挥机构 3 部分，以空地协同为例，参与方包括空中编队、火炮阵地与联合指挥所，当空中编队侦察到敌情时，需要火炮阵地协助打击，空中编队需获取火炮阵地的火力打击控制权，并将相关数据访问权赋予火炮阵地，权限授予均无需通过联合指挥所，指挥所仅进行验证与监管。为验证本文方法的有效性，将场景中两个参与组织抽象为指控节点，将联合指挥机构抽象为信息节点，以指挥权限转移为例，测试方法的性能。据此，实验中本文构建了两个初始组织，其中每个组织各包含一个指控节点。

在传统跨域协同过程中权限授予需要逐级上报，经联合指挥部审批后下达，任意一级失效都会导致权限无法成功授予。因此，传统跨域协同方法延迟与鲁棒性不佳。将其与本文方法进行定性的对比分析，结果如表 5 所示。

表 5　性能对比分析

Table 5　Comparative analysis of performance

参数	传统协同方法	基于区块链的动态指控方法
指令转发次数	多	少
审批单元数量	多	少
抗毁性	弱	强
数据存储量	小	大
带宽需求	小	大

对于方法跨域协同的性能，本文在保持其他参数不变的情况下通过递增共识结点的数量，测试事务处理效率和事务延迟的变化，规律如图 8 和图 9 所示。

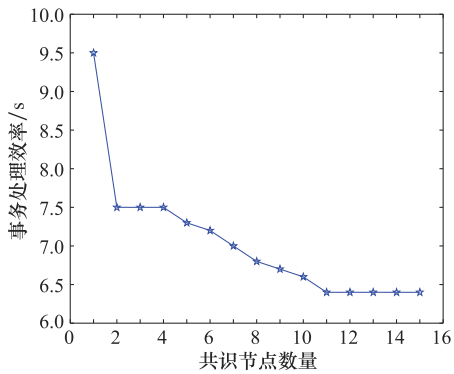

图 8　共识节点数量对任务执行效率影响

Fig. 8　Impact of the number of consensus nodes on task execution efficiency

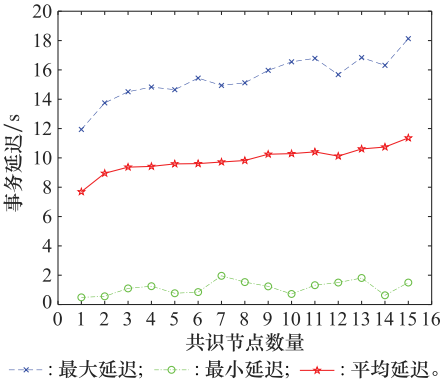

图 9 共识节点数量对事务延迟影响

Fig. 9 Impact of the number of consensus nodes on transaction latency

由测试结果可知，事务处理效率在共识节点增多过程中呈现下降趋势，在共识结点增多至 11 个后进入缓慢下降的状态；事务平均延迟和最大延迟随着共识节点数量增加呈增长趋势，而最小延迟对共识节点数不敏感。

6 结 论

本文以区块链技术视角对动态指控问题展开研究，进行了组织架构与权限流转规则的设计，给出了基于指挥权限授权的任务分发、指派，以及资源权限流转的装备点对点按需调配方法，并在此基础上通过设计应急响应规则构建了应急响应机制，实现了弱中心或无中心指挥节点场景下的动态指控，为指挥权限重组、资源按需调配提供了解决思路。

实验验证证明了本文方法的可行性，在此基础上针对军事背景下的高效公式方法设计与改进，是今后研究的重点方向。

参考文献

[1] ALBERTS D S, HAYES R E. Power to the edge: command control in the information age[M]. Washington, DC: CCRP Publication Series, 2003.

[2] ALBERTS D S, BERNIER F, CHAN K, et al. C2 in underdeveloped, degraded and denied operational environments[C]// Proc. of the International Command & Control Research Symposium, 2013.

[3] TRAN H T, DOMERANT J C, MAVRIS D N. A system-of-systems approach for assessing the resilience of reconfigurable command and control networks[C]// Proc. of the AIAA SciTech Forum, 2015.

[4] ZHU Y, ZHANG X, JU Z Y, et al. A study of blockchain technology development and military application prospects[J]. Journal of Physics: Conference Series, 2020, 1507(5): 052018.

[5] RAJA W A, HAYA H, IBRAR Y, et al. Blockchain for aerospace and defense: opportunities and open research challenges[J]. Computers & Industrial Engineering, 2021, 151: 106982.

[6] RAHAYU S B, JUSOH N, HALIP M H M, et al. A conceptual model of military blockchain for repair parts supply chain management[C]// Proc. of the International Conference on Computer & Information Sciences, 2021: 146 - 150.

[7] SIMERLY M T, KEENAGHAN D J. Blockchain for military logistics[J]. Army Sustainment, 2019, 51(4): 48 - 49.

[8] BILYANA L, SALE L. Weaponising blockchain: military applications of blockchain technology in the US, China and Russia[J]. Royal United Services Institution, 2021, 166(3): 46 - 56.

[9] GOLAM M, LEE J M, KIM D S. A UAV-assisted blockchain based secure device-to-device communication in internet of military things[C]// Proc. of the International Conference on Information and Communication Technology Convergence, 2020: 1896 - 1898.

[10] WU Y, DAI H N, WANG H, et al. Blockchain-based privacy preservation for 5G-enabled drone communications[C]// Proc. of the IEEE Network, 2021: 50 - 56.

[11] AKTER R, BHARDWAJ S, LEE J M, et al. Highly secured C3I communication network based on blockchain technology for military system[C]// Proc. of the International Conference on Information and Communication Technology Convergence, 2019: 780 - 783.

[12] GHIMIRE B, RAWAT D B, LIU C, et al. Sharding-enabled blockchain for software-defined internet of unmanned vehicles in the battlefield[C]// Proc. of the IEEE Network, 2021: 101 - 107.

[13] 赵国宏. 军事区块链研究[J]. 指挥与控制学报, 2019, 5(4): 259 - 268.
ZHAO G H. Military blockchain research[J]. Journal of Command and Control, 2019, 5(4): 259 - 268.

[14] 王飞跃, 袁勇, 王帅, 等. 军事区块链：从不对称的战争到对称的和平[J]. 指挥与控制学报, 2018, 4(3): 175 - 182.
WANG F Y, YUAN Y, WANG S, et al. Military blockchain: from asymmetric war to symmetrical peace[J]. Journal of Command and Control, 2018, 4(3): 175 - 182.

[15] 刘毅, 朱承, 成清. 面向敏捷指控的区块链赋能跨域服务架构[J]. 指挥与控制学报, 2020, 8(2): 169 - 178.
LIU Y, ZHU C, CHENG Q. Blockchain empowered cross-domain service architecture for agile command and control[J]. Journal of Command and Control, 2020, 8(2): 169 - 178.

[16] 刘瑞, 马玉皓, 祁志民. 面向未来陆战场作战的区块链技术军事应用构想[J]. 火力与指挥控制, 2020, 45(11): 16 - 21.
LIU R, MA Y H, QI Z M. Conception of military application of block chain technology for future land battlefield operations[J]. Fire and Command and Control, 2020, 45(11): 16 - 21.

[17] 杜行舟, 张凯, 江坤, 等. 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[J]. 计算机科学, 2018, 45(S2): 576 - 579.
DU X Z, ZHANG K, JIANG K, et al. Research on information transmission and traceability mode of digital command and control system based on blockchain[J]. Computer Science, 2018, 45(S2): 576 - 579.

[18] 巫岱玥, 余祥, 王超, 等. 基于区块链的信息系统数据保护技术研究[J]. 指挥与控制学报, 2018, 4(3): 183 - 188.
WU D Y, YU X, WANG C, et al. Research on data protection technology of information system based on blockchain[J].

Journal of Command and Control, 2018, 4(3): 183 - 188.

[19] 舒展翔, 李腾飞, 余祥. 基于区块链的指挥信息系统用户权限管理问题研究[J]. 指挥与控制学报, 2019, 5(2): 107 - 114.
SHU Z X, LI T F, YU X. Research on user permission management of command information system based on blockchain[J]. Journal of Command and Control, 2019, 5(2): 107 - 114.

[20] WRONA K, JAROSZ M. Use of blockchains for secure binding of metadata in military applications of IoT[C]// Proc. of the IEEE 5th World Forum on Internet of Things, 2019: 213 - 218.

[21] TEJASVI A A, VINAY C A, NISHAD S A, et al. Applications of blockchain in unmanned aerial vehicles: a review[J]. Vehicular Communications, 2020, 23: 100249.

[22] ALBERTS D S, GARSTKA S. Network centric warfare: developing and leveraging information superiority[M]. Washington DC: CCRP Publication Series, 1999.

[23] LEVCHUK G M, LEVCHUK Y N, LUO J. Normative design of organizations-part Ⅱ: organizational structure[J]. IEEE Trans. on Systems, Man, and Cybernetics-Part A: Systems and Humans, 2002, 32(3): 360 - 375.

[24] BALLARD J J. The proper application of nominative fair use in trademark law: why international information systems security certification consortium, Inc.v. Security University, LLC sets the preeminent standard[J]. Loyola of Los Angeles Law Review, 2018, 51: 523.

[25] 尹荣荣, 张文元, 杨绸绸, 等. 基于简化云与 K/N 投票的选择性转发攻击检测方法[J]. 电子与信息学报, 2020, 42(12): 2841 - 2848.
YIN R R, ZHANG W Y, YANG C C, et al. A selective forwarding attack detection method based on simplified cloud and K/N voting model[J]. Journal of Electronics & Information Technology, 2020, 42(12): 2841 - 2848.

[26] HORS A J L, KUHRT T. Smart contracts and chaincode[EB/OL]. [2021 - 06 - 11]. https://hyperledger-fabric.readthedocs.io/en/release-2.2/smartcontract/smartcontract.html#channels.

[27] AGRAWAL P, TARCA A, WOODLIFF D. External auditors' evaluation of a management's expert's credibility: evidence from Australia[J]. International Journal of Auditing, 2020, 24(1): 90 - 109.

[28] PITT R, WYBORN C, PAGE G, et al. Wrestling with the complexity of evaluation for organizations at the boundary of science, policy, and practice[J]. Conservation Biology, 2018, 32(5): 998 - 1006.

[29] ZAKIROVA Y, LATYPOVA M, GAFUROVA S. The concept of creating a form-based code of Zelenodolsk[C]// Proc. of the E3S Web of Conferences EDP Sciences, 2021, 274: 01021.

[30] PAN Y, LIU Y, ZHU C. Secure personal unmanned aerial vehicle lease scheme based on blockchain[C]// Proc. of the IEEE 14th International Conference on Anti-counterfeiting, Security, and Identification, 2020: 197 - 203.

[31] ANDROULAKI E, BARGER A, BORTNIKOV V. Hyperledger fabric: a distributed operating system for permissioned blockchains[C]// Proc. of the 13th EuroSys Conference, 2018.

[32] International Business Machines Corporation. Hyperledger caliper[EB/OL]. [2021 - 06 - 11]. https://hyperledger.github.io/caliper/.

[33] DREYER J, FISCHER M, TONJES R. Performance analysis of hyperledger fabric 2.0 blockchain platform[C]// Proc. of the Workshop on Cloud Continuum Services for Smart IoT Systems, 2020: 32 - 38.

作者简介

潘永淇(1999—),男,博士研究生,主要研究方向为区块链、动态指控。

魏　巍(1991—),男,讲师,硕士,主要研究方向为区块链、指挥信息系统。

刘　毅(1989—),男,讲师,博士,主要研究方向为敏捷指控、指挥信息系统。

朱　承(1976—),男,教授,博士,主要研究方向为敏捷指控、指挥信息系统。