**1.1区块链基本概念和原理**

关于区块链的定义,从狭义讲区块链是一个分布式的数字账本, 单点发起,全网广播,交叉审核,共同记账。从广义上讲,工信部《中国区块链技术和应用发展白皮书》将其表述为分布式数据存储、点对点传输、共识机制、加密算法等计算机技术在互联网时代的新型应用模式。

简单讲,区块链是由区块加链组成的,区块记录经过完全验证的信息, 链则记录着区块之间的先后顺序,代表了数据完整的历史。为通俗理解区块链的概念和原理, 可将其概为一种模式、二个特征、三种架构、四大技术、五个优势和六个层次。

一种模式即区块链是一种全网记录数据的模式,对同一数据采取全网共同审核和记录的方式；二个特征即去中心化和去信任化。区块链基于端到端对等网络,不存在中心设备和集中管理机构,每个节点权限对等。区块链的机制,能够保证节点之间无需互相信任,就可以自动安全地验证和交换信息；三种架构即区块链按照全部授权、部分授权和指定授权区分为公共链、联盟链和私有链；四大技术即基于P2P对等网络的分布式存储技术、以哈希(Hash)算法和非对称加密(Asymmetric Encryption) 为代表的加密技术、以工作量证明(Proof of Work, POW)和拜占庭容错(Practical Byzantine Fault Tolerance, PBFT)等方法为代表的共识机制(Consensus Mechanism)由自动化脚本代码组成的可编成智能合约(Smart Contract)技术。进一步讲,区块链是利用分布式对等节点存储数据、利用密码学的方式保证数据传输和访问的安全、利用共识算法来验证和生成数据、利用智能合约来编程和操作数据。五个优势是从效果角度而不是方法上讲, 区块链具有安全、抗毁、容错、优化、自动等优势。区块链采取基于加密的块链结构,确保信息不被篡改;采取全网记录的分布式存储方式, 抗毁灾备能力强;运用共识算法,建立了容错机制;建立了竞争机制,确保决策最优;依托智能合约,保证自主运行。六个层次即应用层、合约层、激励层、共识层、网络层、数据层。其中,应用层包括了区块链的各种应用场景; 合约层是自动化运行脚本、算法等合约的集合; 激励层封装的是与应用背景相关的激励因素;共识层主要封装各类识别和验证算法;网络层主要包括了对等组网机制、数据传播与验证机制;数据层封装了基于加密算法、时间戳、校验等信息的链式区块数据结构和相关数据信息。

**1.2 对区块链的认识**

单纯从技术视角看,区块链似乎算不上一种新的颠覆性技术,它是将点对点传输、分布式存储、密码学、共识机制等成熟技术进行了融合集成,然而其创造性的价值恰恰体现在结构创新和模式创新上集中体现在以下3个方面：

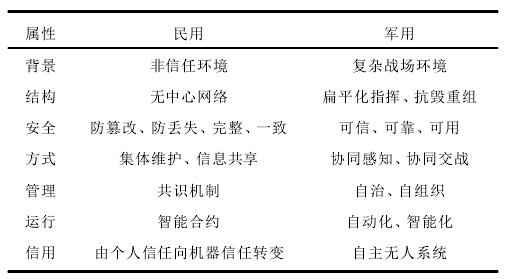
1. 区块链创造了一种新的组织形式,即在无中心的条件下,各个节点能够在没有集中统一操控的情况下,通过共识机制实现了系统的自治, 达成信息共享、认知统一、行动一致,实现了所谓的自治, 而通过智能合约则可实现体系的自动运行。
2. 区块链创造了一种新的决策机制, 即分散式决策。通过网络中多个节点之间的动态博弈和合理的激励机制,实现了有限资源的合理配置、成员利益的一致化和集体效益的最大化, 达成了所谓的帕累托最优(Pareto Optimality)和激励相容 (Incentive Compatibility)。
3. 区块链创造了一种新的计算范式, 通过经济学的机制设计(Mechanism Design) 理论和最新信息技术的有机融合, 保证了在非信任环境下和信息不对称情况下复杂系统中信息的可信可靠和体系的协调高效运作。这种技术架构具有很强的普适性, 可以为金融、经济、军事甚至社会等领域带来革命性的变革。
   1. **区块链与军事结合**

区块链展现出来的特质和优势，契合了战场指挥领域发展和运用的特殊需求。一是从应用背景看，区块链基于一种非信任的环境，因此非常适合于处理复杂战场信息；二是从结构上看，现有的数据链采用分布式组网，即网络中各个节点地位相同，从而具有更强的抗干扰能力，而区块链采用无中心组网，去中心组织的方式，能够很好的应

用于数据链，与数据链相结合，降低对指挥中心的依赖性，满足扁平化指挥，提高抗毁性等需求；三是从安全上性要求来看，区块链防篡改、防丢失、信息完整、可追溯等特征，非常契合战场系统对信息可信、可靠、可用的高标准要求；四是从方式上看，区块链集体维护、信息共享的模式，保证各作战平台在信息上的一致性，契合了联合作战、集群作战协同感知、协同决策、协同交战的需求；五是从管理上看，区块链基于共识算法的竞争和验证机制，契合了自组织和自治化管理等需求；六是从运行上看，基于区块链的智能合约能够根据系统状态被自动执行，且执行结果的可信性有所保证，将智能合约应用于数据链中的信息流转与决策，能够有效的实现数据链中信息的流转与作战决策的智能化与自动化。特别是打击时间敏感目标自动交战的要求；七是从信用上看，区块链实现了由个人信任向机器信任的转变，减少了军事管理过程中人为因素带来的不确定性、多样性和复杂性。

因此, 区块链在军事领域既具有迫切的必要性,又具有广阔的应用前景。如下表1-1所示：

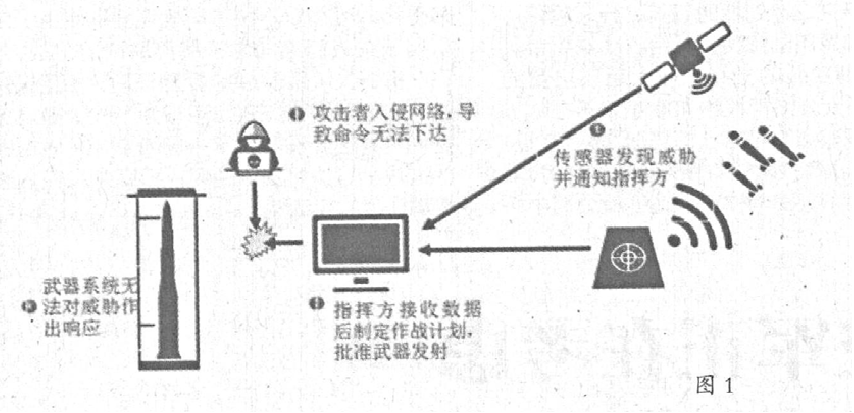
表1-1 区块链技术与军事应用的契合性



* 1. 军事区块链实现装备控制系统的去中心化

图1-1展示了当前常见的集中式系统指挥控制功能的高阶抽象模型。系统接收到传感器数据后通知指挥方发现威胁，指挥方引导武器系统对威胁发起攻击。这种集中式的系统模式意味着外部攻击者可以对单个漏洞进行攻击，使指挥方和自动化控制器/人类控制员收到错误或欺骗信息，导致武器系统被恶意操纵或无法响应发现的威胁。

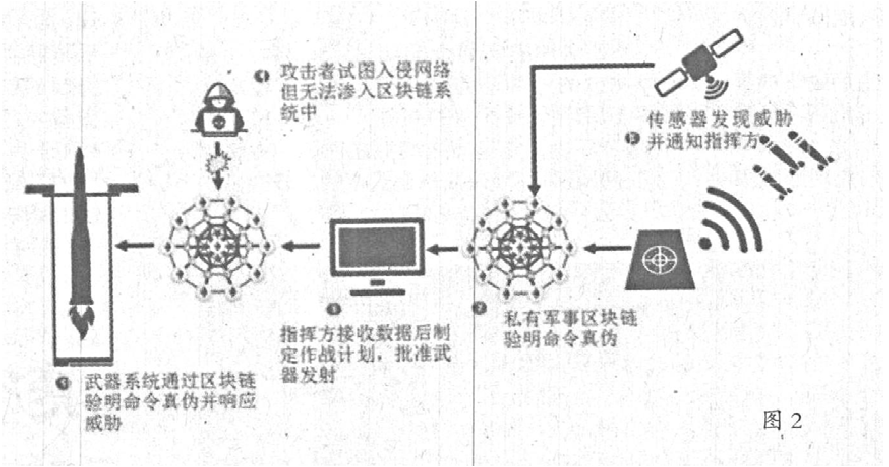
图1-1 集中式系统指挥高阶抽象模型



现代战争对抗愈加激烈，指挥机构、通信枢纽及其存储的关键信息，已经成为作战双方重点摧毁的首选目标，建立可靠的网络架构，成为未来战争制胜的关键因素之一。区块链去中心化的特性恰好能够契合抗毁生存的军事需求。区块链采取分布式核算和存储，不依赖第三方管理机构，具有良好的抗毁性、容错性和扩展性，每一节点都存储着完整的数据备份，一个节点出现问题，其他节点会继续数据的更新和存储，即使部分节点被破坏后，仍可保存数据存储能力和网络计算能力，并通过共识算法维持网络的正常运行，可有效避免在敌精确打击下被敌“一锅端”。指挥机关网络只需直接将数据传输给指挥对象网络中的任一节点，即可由此节点将相应信息更新于区块链数据账簿之中，进而确保上下级之间的指挥畅通。即使上一指挥层级失效，各下属层级可通过区块链网络直接与更上一级指挥部取得联络，及时执行新的作战任务。

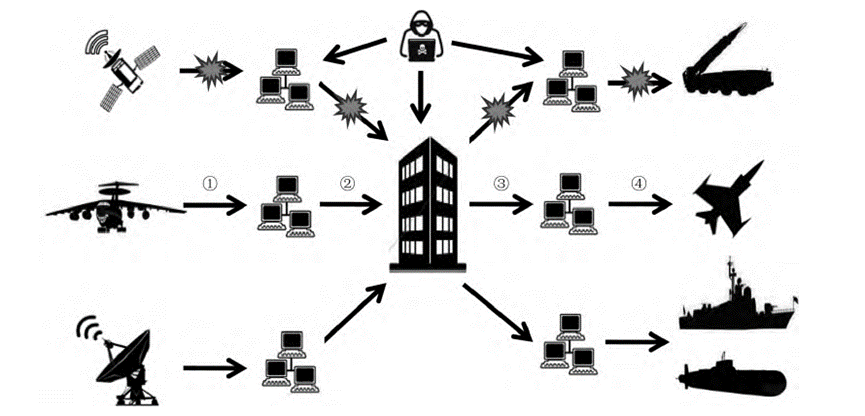
图1-2展示了基于区块链去中心化技术的武器系统控制模式。数据传输必须通过在分布式系统中大部分节点的验证，才能确认数据来自合法发起者。所有节点都是独立且受到加密技术保护的，因此攻击者必须拥有极其强大的计算能力对所有节点发起同步攻击才有可能成功。可以看出，当节点数量足够多时，系统将变得“无法破解”。

图1-2 去中心化技术的武器系统控制模型



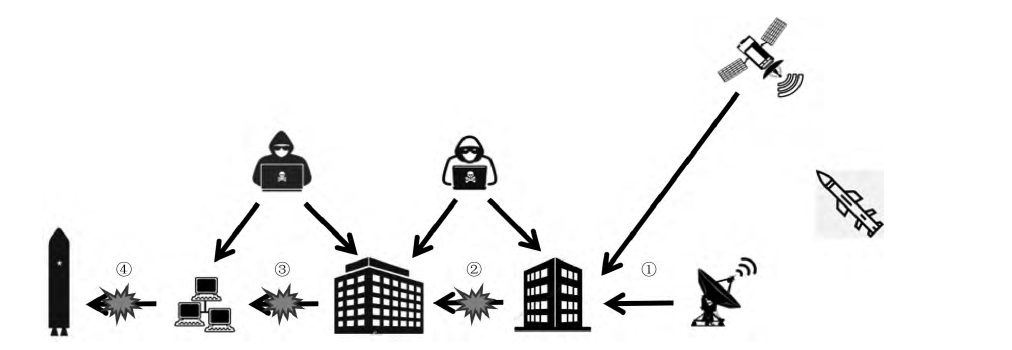
战场情报获取、融合、共享是联合作战的前提和基础。有中心层级指挥模式下,各军兵种侦察手段获取的情报信息首先传送到军兵种情报中心进行融合;其次,在联合指挥所融合三军情报信息,形成统一的战场态势图 (Common Operational Picture, COP);而后,再将这些信息传送到各军兵种指挥机构;最后传送到各军兵种武器平台，如图1-3所示。

图1-3 有中心层级化指挥模式联合情报共享概念图



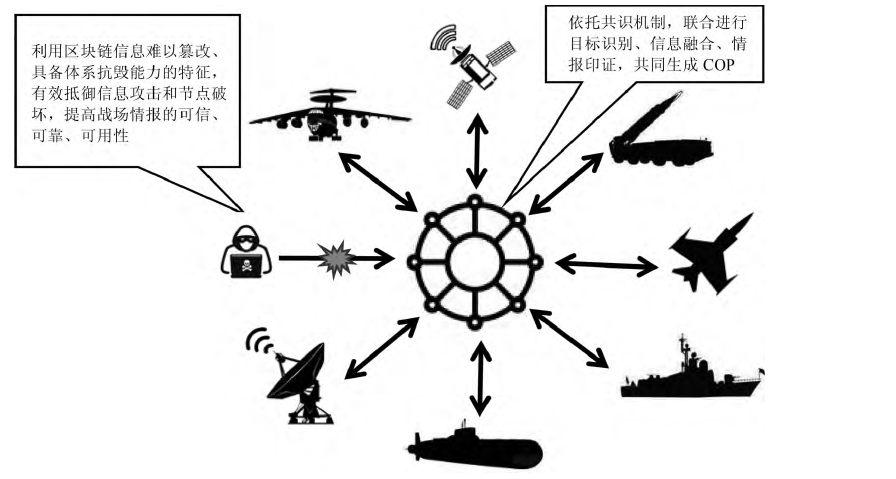
这种中心层级化指挥模式导致了整个作战通信体系存在链路长、效率低等问题, 特别是难以满足武器平台打击时间敏感目标对时效性的要求。以战略核武器反击作战指挥控制为例，在集中式指挥控制模式下,战略预警中心接收到预警卫星和雷达的敌方来袭数据后,首先生成预警威胁情报,然后通知作战指挥中心进行反击决策,在授权的情况下指挥中心向导弹发射控制站发布作战命令,引导导弹武器系统对目标发起攻击。这种集中式的系统指挥链路长,环节多,每个节点都有可能受到信息攻击,使得情报系统、指挥系统和武器系统无法收到信息或接收到错误的信息, 导致整个系统失效。如图1-4所示。

图 1-4 集中式武器控制模式概念图



基于区块链的联合情报共享机制,各种侦察手段、信息处理中心、武器平台均是网络中的对等节点。区块链技术通过快速网络运算、智能合约及网络共识机制，可减少指挥过程中人为因素带来的不确定性、多样性和复杂性，实现组织信息传输和处理的网络化，缩短决策——指挥——行动的周期，提升快速反应能力。实现联合进行目标识别、信息融合、情报印证,共同生成 COP,并可将相关情报信息端到端快速直达武器平台进行目标指示,实现对时间敏感目标的快速打击。

图1-5 基于区块链的联合情报共享机制概念图

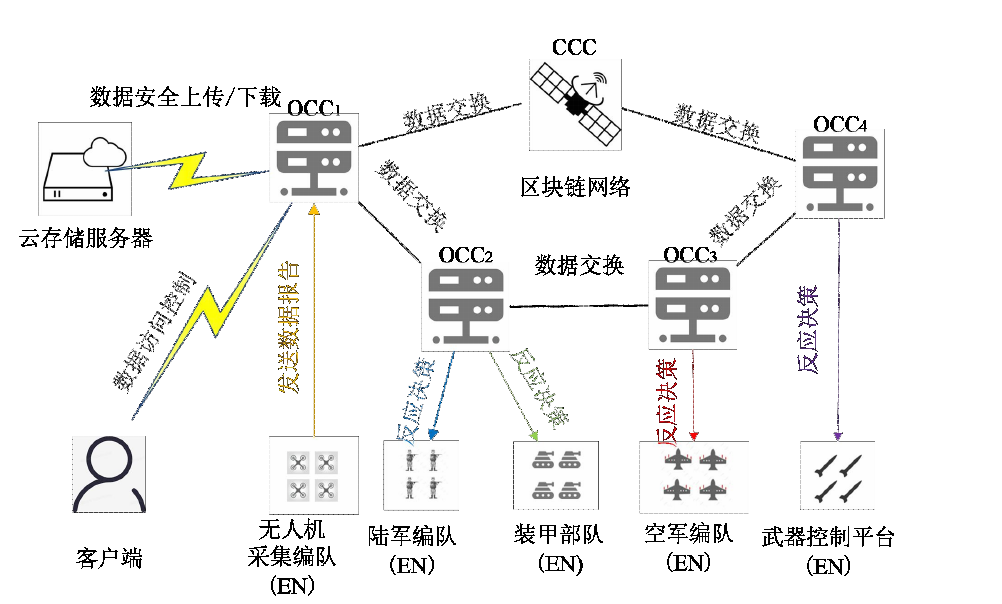


* 1. 军事区块链实现层级指挥特点

军事网络与民用网络不同，军队指挥系统各级有各级的职责和权限, 遵循上级指挥下级,下级服从上级的原则因此我们必须有针对性的选择区块链的类型。区块链一般可分为三种类型，公有链、私有链和联盟链。其中，公有链采用去中心化架构，区块链中的所有信息对公众开放，任何节点都可以成为矿工来参与到区块的生成与区块链的维护工作中来，这也即是我们所说的比特币区块链；私有链为中心式架构，即区块的生成与维护完全由一个中心实体来完成；联盟链介于二者之间，采用了部分去中心化架构，即区块链的维护工作由整个网络中的部分节点来完成，而其它节点仅仅具有对链上数据的访问权限。

针对以上三种区块链的特点，联盟链是最适合于军事系统的一种区块链体系，我们可以根据军事体系，将整个区块链网络划分为：一个总指挥中心（Chief Command Center , CCC），多个不同区域的作战指挥中心（Operational Command Center, OCC）和各种类型的执行节点(Execution Node, EN)，如步兵、装甲部队、武器平台、空中分队等组成，如图1-6所示。

图1-6 联盟链实现的军事区块链



其中，CCC 和 OCC 共同维护区块链网络。区块链存储所有系统中信息流转的记录，并存储运行用于数据传输控制和数据传输历史的智能合约代码；EN 负责采集数据、上传数据以及执行 OCC 的命令。在整个区块链网络中采用严格的权限管理，系统用户(Client)只能通过管理员分配的权限进入系统。

总指挥中心节点用户拥有系统的管理员权限，在系统初始化的时候就将 CCC 用户写入系统，可以对系统内的其他用户进行添加、删除、更新等操作管理，并且能够对整个系统的信息数据进行管理，以及对系统所有功能的使用。指挥中心节点用户登录后可以对自

身相关的网络节点进行管理，并且使用系统的大部分功能。执行节点用户登录后，一部分是 OCC 节点下的观测节点，负责采集战场数据并发送给 OCC 节点。另一部分是是战场执行节点EN，负责发送战场情况数据给智慧节点并且响应执行指挥节点发布的战场命令。客户端用户Client是系统访客用户，可以查看系统中目前的信息情况。所有除 CCC用户的其他用户，都需要获得 CCC 用户的允许才能够注册访问系统。

采用联盟链实现的军事区块链不仅能改进原有军事网络集中式系统指挥控制的弊端，而且还能够适应军队网络区别于民用网络的多层级体系特点。

* 1. 军事区块链实现指挥的去信任

军事行动中的信息传输过程，经常遭到敌方干扰、破坏和伪造，如何验证网络信息的真实性、保证信息能够安全准确地传输，是一大难题。武器系统和作战系统的效能发挥必须依赖于可信的数据,而现代战争中网络战是非常重要的战斗手段,黑客利用中心化的数据库和单点故障进行网络攻击使得整个敌方系统瘫痪,或者通过盗取并伪造身份信息篡改数据使得敌方踏进安全陷阱,这些潜在风险的存在,意味着作战人员可能会面临着数据真实性不明的情形, 极为可能基于恶意数据做出错误决策。比如我们如何确定无人机作战平台上当前运行的程序是我方最初安装部署的原始程序, 而不是敌方经过攻击之后篡改过的；在此前提下, 我们又如何确保无人机侦察平台传回指控中心的数据是最初拍摄或摄录的原始数据,而不是敌方恶意欺骗的。

因此，要实现军事系统信息安全的关键问题就是建立实体间的信任问题，例如身份认证、访问控制、数据保护等。身份认证技术实

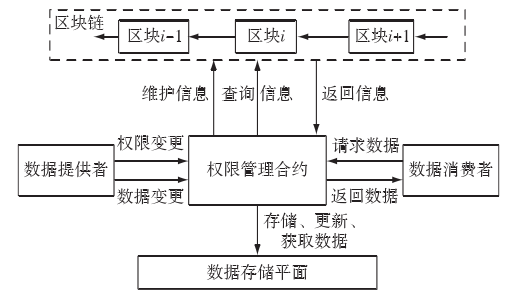
现系统用户身份合法性的鉴别，访问控制技术使得合法用户只能按照其所拥有的权限访问系统内相应的资源，数据保护能够确保数据的可用性、机密性和完整性。军事信息系统作战指挥和综合保障效能的发挥必须依赖于用户身份合法、权限分明、数据可信。

传统信息安全技术常采用可信第三方背书的信任机制，如利用第三方认证服务器对用户身份进行认证，基于中心架构实现用户权限管理，基于中心系统存储系统关键数据等。然而，这种基于中心的信任机制难以满足分布式条件下的身份认证、安全透明可信的访问控制和复杂环境下可信数据保护等更高需求，面临单点故障、访问越权、数据滥用等安全风险。

针对以上问题，区块链的开放共识、可追溯、不可篡改的特性能够帮助提供可信的指挥信息。因为区块链在构建之初就假定网络中各节点不是完全可信的，它从底层上被设计用于在竞争性、不可靠的网络环境中运行维护数据。

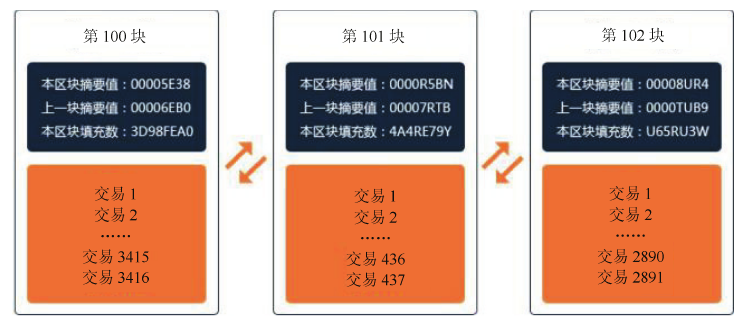
在区块链中通过采用共识机制来代替可信的第三方，达到一种“去信任”的效果。共识机制是指以去中心化的方式就网络的状态达成统一协议的过程，也被称为共识算法，区块链系统采用共识机制来确保所有区块链节点都对同一消息达成共识一致，并且最新区块已正确添加到链中；同时这种链式结构也使得任何对区块链内容的修改能够被快速检验，原因是区块链通过时间戳保证每个区块依次顺序相连，时间戳使区块上每一次交易数据都注入了时间标记，证明了交易中什么时候发生了什么事情，并且任何人都不能篡改，时间戳在区块链技术中扮演着公证人的角色，远比传统的公证机制更为可靠，这保障了对于数据改写过程全程可追溯。同时分布式存储以及共识机制的存在还使得单一实体对内容的修改无法影响到整个区块链系统中存储的数据，区块链系统中任意节点间的信息交换都必须得到全部或大部分节点的同意才能被系统承认。被承认的交易将被记录在一份共享的数字账本副本中，与所有交易记录保持关联。恶意攻击者除非同时修改超过51%的节点，才可能篡改破坏信息，因而使得整个系统中的数据具有很强的不可篡改的特性；针对于访问越权问题，可以将访问控制策略分布式存储，各节点保存一份数据副本，对数据的访问请求需经过全网节点的共识，避免越权访问的情况发生。确保用户能够自己掌控数据的管理权，了解自己数据被访问的情况，增加访问控制的透明性。对数据的共享访问被记录到区块链上，审计人员只需要对区块链进行向上追溯即可完成对数据的审计。流程如图1-7所示。

图1-7 基于区块链的军事信息系统访问控制



在区块链网络中,区别于传统的数据库存储技术,数据不再是存储在一个中心化的数据库系统中,而是利用先进的密码学技术分布式记录在所有的区块链节点中,每一个节点都能复制获得一份完整的数据副本,同时因为这些节点之间又采用了复杂的共识算法来确保数据的一致性,所以即使网络中部分节点遭受到黑客攻击或者因为故障而停机,也不会影响整个网络系统的正常运行，区块链区块结构如图 1-8所示。

图 1-8 区块链区块结构示意



区块链系统中用以存储数据的区块,每一个区块与前一个区块, 乃至再前一个区块之间通过哈希算法相连, 也就是说,如果不知道前一个区块的内容,就无法生成当前这个区块,因此,每个区块必定按照时间顺序跟随在前一个区块之后,这就使得从第一个区块 (创始块) 开始一直到当前区块,连接在一起形成了一条长链, 这也是区块链概念的来源。

这样的存储结构特性,使得如果有黑客想要篡改一个区块里面的数据内容,那么需要篡改的就不单是这一个区块,还包含这之后的所有区块,即从这个区块开始向后的所有的数据历史,而这些历史不仅是存在于一台服务器上,而是同一瞬间遍布各地的所有区块链节点上,并且这些数据历史还在使用密码学相关技术进行保护。这样对于数据存储和管理的新方式,使得区块链系统相比较传统的信息系统，拥有更为安全的特性。

考虑到军事信息密级较高，并要求在一定范围内可控。我们还可以使用区块链非对称加密技术获得较强的信息安全性，解决信息密级与承载网络密级间不对等的问题。

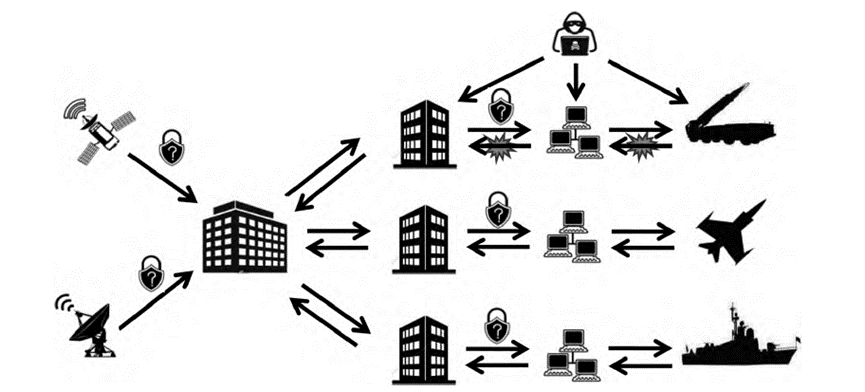
应用区块链技术，既可提升作战数据收集、传输、处理的能力水平，也为作战数据信息的传播提供了更加安全、可靠、便捷的技术通道，避免敌采取各种信息插入手段发布假命令，扰乱指挥体系。使得网络攻击产生的破坏力得以降低,作战人员手中数据的真实性也能因此得到保障,这种对于风险的规避,能极大提升战场上的不对称优势, 可能会改变战争领域的游戏规则。

* 1. 军事区块链实现军事作战的可扩展

当前军事通信体系在联合作战指挥中难以做到科学快速决策。未来作战,联合作战已经成为主要方式,任务式指挥可能成为常态模式。一是在联合作战中,不同军兵种作战力量必须打破烟囱式层级化指挥模式, 能够在扁平化越级指挥条件下实现协同作战。二是在任务式指挥模式下,要求任务部队能够根据上级赋予的作战任务自主筹划、自主作战。

从联合指挥所到集群指挥所,再到任务部队指挥所从上到下层层明确并分解作战任务,从下向上层层综合,进行任务完成度分析和冲突检查,这一过程可能要多次迭代才能形成可行的作战方案计划。在这整个过程中往往需要进行跨军兵种指挥机构、跨作战地域通信、跨战役战术和武器平台层级、跨陆海空天电打击领域以及跨指挥网和业务网络，如图1-9所示。

图1-9联合作战指挥概念图



但是由于在研制各种战术数据链的初期,缺乏全面统一的总体框架与标准体系, 特别是存在跨网络数字签名和证书难统一，导致不同的数据链系统兼容性差，无法保证各个作战平台决策的协调一致，传统的数据流转方法是在各方间加入中间存储设备来实现各方的数据交换，这就使得数据链网络难以扩展，形成数据孤岛，难以真正实现数据共享。且各个作战指挥中心孤立分散，在作战行动中不能有效的联合利用各方优势，难以实现各兵种的联合作战。除此之外还存在敌方仿冒或盗用我方身份，进行干扰和破坏的可能性。

基于区块链的联合决策机制, 将参与决策的各军兵种、各层级、各要素作为网络的对等节点。采用统一的哈希算法和非对称加密等方法解决跨网络数字签名和证书一致性的难题,基于区块链的智能合约能够自动收集来自于各节点的战场信息，检测系统状态并自动触发执行共识协议，并根据生成的转发规则自动转发信息，整个过程不需要中心调控。保证各作战平台在作战信息上的一致性，实现多层次数据链态势信息分布式融合和处理，减少对指挥方的依赖，降低系统响应时间，提髙任务协同的效率，真正实现各作战平台的协同作战。因此，将区块链与数据链有机的结合，能够有效地弥补数据链的不足，当前和未来区块链系统结合主动兼容和被动兼容模式打通多个不同层级的数据链之间的孤岛，实现多链的跨链互联。这对于实现各平台自适应协同作战以及作战的智能化与自动化具有重要的意义。

* 1. 区块链实现军事通信的可信流转

在区块链中，除各参与者私有信息加密外，数据对所有人透明公开，并基于协商一致的规范和协议，自动安全地验证和交换数据。基于上述特点，区块链应用到军事领域，每一作战单元或平台在可能遭受敌软硬复合攻击的非完全信任网络中，无需依赖第三方认证，即可根据权限随时安全地获取和发布信息，实现通信过程中数据的可信流转。这种数据的可信性体现在四个方面：

第一,决策可信:比特币和区块链诞生于2008年末,其初衷就是要解决中心化机构、银行和政府与用户之间的信任问题。区块链把中心化决策、监管和控制变成了去中心化、自底向上的共识和共治,因而特别适合需要高度确定性和精准可信决策的军事管理场景。

第二,网络可信:区块链技术促使军事管控网络转变为去中心化、点对点的网络,在这个网络中,每个节点都是平等的,没有任何中心控制和层级机构,无论是在战时还是在平时,对于军事管理信息的团体误判以及不当行为的团体勾连很难实现。

第三,数据可信:从技术角度看,区块链用共识算法来更新数据, 数据上链前需要所有或者大部分节点验证,而日常维护也须每一个节点参与, 因此数据的可信性大大增强。这一点对于现代军事管理十分重要, 因为数据、信息、情报是现代战争决胜的关键因素,只有保证数据的绝对可信,基于此做出的军事决策才能高效可靠。

第四,账本可信:区块链账本基于哈希值存储链式结构，共识机制的存在保证了账本难以篡改且不可伪造。任何跟军事管理决策有关的信息和行为一旦被记入区块链就难以被篡改和伪造,保证了历史信息的完整性和可追溯性。

同时，针对于当前各种数据链在多层级数据链之间数据流转的通信消息可验证性差、异构无人系统之间通信安全和跨域信任的需求，利用区块链跨链技术可以实现多层级数据链消息的可验证性与安全性。通过设计有效的原子互换协议，以保障跨链事务的原子性；选择合适的“中间人”，实现跨链数据的准确传递，进而基于公证人机制完成跨链事务确认，真正实现跨链价值的自由可信流通。

* 1. 区块链技术促进战术终端设备轻量化

随着现代科技的高速发展,各类战术终端设备越来越小型化,平台空间的限制也不允许多个标准的数据链设备同时存在。一种方案是对当前所有数据链的决策标准进行统一，另一种方案是构建适用于数据链的区块链，将分布式自组织网络、高效的共识算法及指挥信息数据存储等基于区块链无人作战系统核心部分进行封装，实现与其他有人系统、武器装备的无缝衔接，当系统中接收到观测节点观测的信息后，根据战场形势，自动调用智能合约得到各个作战平台的响应策略，并通过共识算法在各个作战指挥中心以及总指挥中心之间达成一致，从而保证了各个作战平台之间协调一致，且区块链的不可篡改特性，为响应策略的可信性提供了保证。通过将区块链技术与数据链相结合，可以越过不同标准的数据链设备，从而实现战术终端设备的轻量化设计。

但是，由于区块链每一个节点都必须实时同步全部账本数据，有多少个区块就要存储多少次重复数据，而且随着数据量的增长和新节点的追加，系统冗余度将进一步提高，需要消耗大量的存储资源，这对作战单元或平台终端的存储、计算和通信能力提出很高要求，与装备的轻量化、小型化发展趋势又相悖。随着区块链节点数量的扩大，每个节点同步数据而消耗的算力、带宽和能源也会越来越大，节点越多则对后续新增节点的存储要求越高、接入难度越大、同步时间越长、整体运行效率越低。

为此，我们可以选择构造适用于数据链的联盟区块链。首先，联盟链采用的共识算法，如PBFT，在节点数量不超过100个的情况下，在确认时间和吞吐量方面具有很好的表现，因而可以满足数据链低延迟等要求；其次，联盟链通常不需要挖矿，因而降低了计算资源开销，提高了效率；此外，同一时间内只有一个节点负责区块生成，而主节点能够在各节点间进行轮换，因而在保证去中心化的同时，避免了区块链分叉问题，能够更快地达成与确认信息的一致性。因此，联盟链能够有效地应用于数据链中，并实现髙效、低延迟的数据链控制机制。

同时还可以通过将部分链上动作移出到链外来提高军事区块链的效率，例如通过状态通道、闪电网络等链下扩容技术来提高军事区块链的计算与存储可扩展性。

* 1. 实现国产自主可控

区块链可以在军事行动和国防工业中发挥重要作用，早在区块链诞生不久后，立即引起了美国等世界军事强国的广泛关注。他们纷纷探索区块链技术在军事领域的应用，以期在新一轮军事变革中占据有利地位。美国 2018 年颁布的《国防授权法案》就要求国防部对区块链进行全面研究，探讨如何将其应用于军事领域。美国国防高级研究计划局授予美国两家计算机安全公司价值 180 万美元的合同，研究区块链应用于保护军用卫星、核武器等高度机密数据免遭黑客攻击的潜力，提高关键系统的安全性。美国国防部（DOD）下属机构国防高级研究计划局（DARPA）与美国技术公司 ITAMCO、圣母大学计算机研究中心合作，开发基于区块链的军用级加密通信和交易平台，确保各部队与总部之间、情报官员与DOD 之间通信安全传输，DOD 后勤采购等交易安全。北约也十分关注区块链的军事化应用并举办了区块链创新竞赛，寻求发现提高军事后勤、采购和财务效率的军事级区块链项目。爱沙尼亚和北约正尝试使用区块链技术开发下一代系统，以实现北约网络靶场防御平台的现代化。俄罗斯国防部 2018 年宣布将启动一个研究实验室，分析如何使用区块链技术来缓解赛博安全攻击和支持军事行动。据《消息报》报道，该实验室的首要任务是开发一种智能系统，以检测和防御对重要数据库和武器系统的赛博攻击。俄罗斯国防部表示希望建立安全的区块链平台，使赛博攻击的痕迹难以隐藏，并跟踪想要进入系统的赛博入侵者。

目前区块链技术在军事领域中的运用尚处于萌芽阶段，各大项目还未落地，但任何科学技术的发展都要经历一个渐变累积的过程。未来，区块链技术一旦成功应用于军队网络安全管理和武器全寿命管理等领域，必将超越传统军事管理体系，引发军队建设和作战方式的革命性变化。本项目意在利用区块链技术实现全军共用信息系统装备，补全并推动我军当前在此领域的发展，达到国产自主可控的目标。助力我军在新一轮军事变革中占据有利位置，在未来信息化战争中掌握军事竞争主动权，抢占世界军事制高点。