

引言

当前，区块链技术已成为与人工智能、量子信息、物联网同等重要，并可能产生颠覆性影响的新一代信息技术。同其他新兴技术产生后必然运用于军事领域一样，区块链技术在军事领域同样有着广阔的应用发展前景，其在军事领域取得应用突破，势必产生深刻影响。

区块链军事应用的潜在价值

区块链技术的去中心化、不可篡改、全程留痕、可以追溯、集体维护、公开透明等特点，使其除了在数字货币、资产认证、供应链等民用领域得到普及应用外，在军事领域同样有重要的潜在应用价值。

分布式结构、去中心化的特性能够提供可靠的网络架构。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。区块链技术采用分布式的对等网络，具有良好的抗毁性、容错性和扩展性，其“去中心化”特性，符合现代战场网络部署特点。应用区块链技术必将加速推动部队指挥结构从“树状结构”向“网状结构”转化，在该结构下，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”。

可以追溯、不可篡改的特性能够提供可信的指挥信息。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。区块链在构建时就假定网络中各节点不是完全可信的，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，使数据改写过程全程可追溯，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。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。

透明开放、集体参与的特性能够提供安全的共享信息。区块链的任何参与者都是一个权限平等的节点，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。第二代区块链还引入人工智能判决方式，对网络节点行为进行分析，智能识别网络中潜在的窃密者和攻击者。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，从而从机制上强制打破各军兵种各部门之间的信息壁垒，尽可能地优化资源配置，实现不同作战平台的系统融合，在更大程度上巩固己方的军事优势。

智能合约、网络共识的特性能够提供高效的反应机制。传统指挥体制下，军事行动信息通过树状网络结构，在汇总、上报、下发、执行各环节均会产生延迟，甚至贻误战机。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。尤其是随着智能化战争的来临，部队将广泛使用具有自主性的智能装备，区块链通过“智能合约”，模拟群聚生物的协作行为与信息交互方式，以自主化和智能化的整体协同方式完成作战任务，大大提高部队作战效能。

区块链军事应用的外军探索

近年来，基于区块链技术在军事领域的应用潜力，外军纷纷探索区块链技术的军事应用，以期在新一轮军事革命大潮中占据先机。

探索国防基础网络安全防御新手段。利用区块链技术的去中心化、强加密等特点，提升国防基础网络的安全性抗毁性，增强防御体系的弹性韧劲。如，美国国防部提出“区块链网络安全之盾”四年计划设想，并在2020年预算中提供96亿美元资金投入，以确保海量国防数据安全。俄罗斯国防部组建区块链研究实验室，探索开发以区块链技术为基础的智能系统，检测并抵抗对重要数据库的网络恶意攻击。波兰研制“无钥签名基础设施”，快速检测国防系统面临的高级持续性威胁，及时跟踪系统被查看或被篡改的情况。

探索国防供应链物流体系管理新模式。利用区块链技术的全程留痕特点及机器信任机制，促进国防供应链、采购、物流系统实现高效的全寿期管理。如，美国海军采用区块链技术提高增材制造系统的安全性，全程跟踪管理组件设计参数、试验数据、战技状态、维修记录等信息，并在组件损坏或生命周期结束时发出警报；美国穆格公司开发的基于区块链的VeriPart分布式交易系统，可对增材制造的部/组件进行溯源和质量控制，提高售后服务效率和安全性，为国防部建立安全可追踪的智能数字供应链。

探索复杂战场环境军事通信新方法。利用区块链技术的分布式特性，力求构建覆盖范围广、容灾性强、安全性高的通信系统，探索在任意时刻、任意地点的安全通信。如，美国《2018财年国防授权法案》明确要求国防部对区块链技术展开全面研究，美国国防部高级研究计划局（DARPA）开展了利用区块链技术解决复杂战场安全通信问题。俄罗斯将量子密码的防窃听防截获特性应用于区块链网络，可大幅提升区块链网络的防御功能，将对现有信号截获、破译、侦收产生颠覆性影响。

积极推进区块链的军事应用

恩格斯曾指出：“一旦技术上的进步可以用于军事目的并且已经用于军事目的，它们便立刻几乎强制地，而且往往是违反指挥官的意志而引起作战方式上的改变甚至变革。”为此，我们要强化科技是核心战斗力的思想，加快推进区块链军事应用，不断拓展其应用的广度和深度。

加强顶层设计和整体规划。区块链部署是集群部署而非单点部署，通常需要跨军种、跨部门、跨领域。鉴于此，为避免各军种在同一建设领域内重复研发，造成有限资源不必要的浪费，应加强统筹规划，注重顶层设计整体规划。一方面，要深入开展区块链军事应用的研究论证，细致分析区块链军事应用的优先领域及其必要性、可行性、预期军事效益和可能风险，形成区块链军事应用路线图，并纳入军队建设相关发展规划。另一方面，要立足联合作战需要，结合智能化战争军事需求，明确应用项目的牵头部门、参与单位、任务分工、工作机制以及技术体系架构、技术方向和技术标准等，从整体上规划建设，确保各级在区块链技术军事应用上协调一致、有序推进。

规范研发标准和运用模式。区块链技术在民用领域除比特币外，目前尚没有非常成熟的应用案例，其军事应用也处于起步阶段，还存在高冗余度高能耗弊端，现有共识机制和加密算法等也存在技术瓶颈，距离军事需求还有较大差距。因此，一方面，要针对军事领域对区块链应用的特殊要求，加快区块链和人工智能、大数据、物联网等前沿信息技术的深度融合，弥补区块链性能不足或弱点，提高区块链系统的运行效率。同时加大共识机制、智能合约、分布式通信与存储等底层技术开发力度，兼顾满足“去中心化”“安全”“性能与效率”三项要求，使区块链系统性能达到军用级标准。另一方面，要尽快把握区块链运行机理、技术特点和发展水平，进一步挖掘、细化和拓展区块链的军事应用领域，可选风险小、见效快的应用领域进行先期试验、试点，探索区块链军事应用的软硬件环境要求、运行规则、配套机制等，形成成熟的模式后加速向多领域推开应用。

注重搞好军地协作开发。现代战争对制信息权、制智能权的争夺，成为决定战争最终胜负的关键因素。在信息与知识获取方面，区块链技术高度契合这一军事需求，它的发展将促使不对称信息军事博弈转变为对称信息博弈。因此，鉴于区块链技术作为一种底层的技术框架，本身并不存在明显的军民界线，无论是应用于民用领域还是军事领域，其基本的算法与设计思路是相同的，可以采取军地合作方式共研共用，从整体上带动我军信息化、智能化发展。另一方面，要注重深度整合民用技术，通过“拿技术、拿产品、拿人才”等方式把民用市场上先进技术、成熟产品和优秀人才吸纳进来，形成军事区块链应用的“人机结合、知行合一、虚实一体”新时代洪流，全面推进我军智能化发展，不断提高基于信息网络体系的联合作战能力。
(何俊林)