**项目目标**

建立一个基于区块链的军用装备全生命周期数据管理平台。

**核心功能**

1. 数据加密存储，涉及到加密算法、密钥管理、数据上链、数据存证、检索、索引。
2. 数据分享，涉及到人员权限管理、数据授权方案，可以考虑隐私保护的场景（设计一个零知识证明的场景）。
3. 身份认证，跟数据分享相关，用于确定人员身份，构建 CA-PKI 体系等，可以扩展到设备身份管理。
4. 溯源。每套设备的全部数据可追溯，每条数据的全部访问操作历史可追溯。

**关键技术**

需要确定几项关键技术，作为我们在区块链领域的方向，通过一两个项目在这几个关键技术上积累经验，形成成熟方案后，有利于后续项目根据不同应用场景快速给出解决方案。

1. 共识算法
   共识算法是区块链领域的核心技术之一，应当研究经典的共识算法，并跟踪区块链共识的前沿研究和应用，掌握发展方向。

2. 数据加密存储、授权
   密码学是区块链的基础，必须掌握常用的加密算法的原理与应用场景，以便为不同项目的不同应用场景设计安全方案。
   应当跟进密码学前沿研究，包括零知识证明、安全多方计算、同态加密等。
   数据也是很多应用的基础，数据安全是比较常见的研究方向。
   密码学本身过于侧重理论知识，研究加密算法需要很强的数学知识背景，我们应当侧重在应用密码学上。

3. 身份管理
   包含人、设备、组织等的数字身份管理方案。
   分布式身份目前在区块链领域是很热门的方向，也是比较有机会落地实际应用的方向之一，这一领域也使得很多前沿技术有了实际应用场景，比如零知识证明、隐私证书等。

**主要工作**

1. 共识协议研究
   a) 学习传统分布式系统的共识协议，例如 RAFT、PBFT、PAXOS 等，以及区块链中常见的 PoW、PoS、DPoS 等。比较这些算法的性能、优缺点和适用场景等。
   b) 确定符合本项目的共识算法，可以是朴素地实现并应用，或针对项目本身在经典算法的基础上做优化。

c) 在 fabric 框架下，如果需要，对共识模块进行替换。

2. 系统加密方案设计
   a) 调研并了解军用装备生产的主要数据类型（格式）、涉及的机构和人员、生产流程等。
   b) 针对性地设计全流程加密加密方案，可能会用到对称、非对称加密、数字证书、PKI 系统、哈希函数等密码学工具，实现数据的加密存储、共享以及机构和人员的权限管理，同时，需要引入监管机构。
   c) 调研国密算法的各类语言实现（主要是 Golang），并在 fabric 的框架下，完成加密模块的国密替换。
3. 应用开发
   a) 学习掌握 docker 和 K8S 等技术，完成 fabric 区块链网络的云端快速部署或内网物理机集群部署。
   b) 开发智能合约，处理核心数据管理的逻辑。
   c) 应用层的前后端技术选型与开发。Fabric 本身使用 Go 语言开发，智能合约也主要使用 Go 语言（也支持多语言，例如 Java, node.js 等），因此，应用使用 Go 语言生态中的技术框架是比较好的选择。