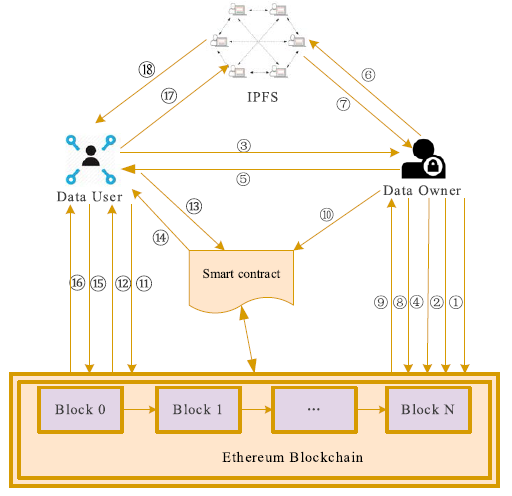
**基于区块链的安全数据共享系统**

云平台作为数据外包服务的常见实现手段，可以有效降低企业管理和分析数据的成本，但安全与隐私问题已成为制约其发展的重要因素。用户的敏感数据被存储在云端服务器后会超出云服务使用者的掌控范围，安全性完全依赖云服务提供商，数据安全问题是云服务使用者密切关注的问题。同时，传统的云存储模型以集中存储的方式运行，因此单点故障可能导致崩溃的系统。对于数据安全问题，基于属性的加密(ABE)被认为是一种解决数据隐私和细粒度访问控制问题的重要技术。区块链技术作为一种分散式存储模式，可以解决单点故障问题，具有价格低、吞吐量高等优点。

本课题要求实现一个分布式数据存储与共享方案，将IPFS（星际文件系统）、区块链和ABE技术结合起来。数据所有者能够向数据使用者分发密钥，通过指定访问策略对共享数据进行加密，实现细粒度访问控制。基于智能合约的关键字搜索实现对分散存储在IPFS中的密文建立索引，数据使用者能够对加密后的数据进行检索。本课题的创新点在于智能合约的设计。

系统主要包括如下四个功能：用户注册、文件保存、文件上传和文件下载。数据所有者和数据使用者想使用系统功能都需要注册账户。文件拥有者分享文件分为文件上传和文件保存两步。文件上传过程记录文件的基本信息，文件保存包括对文件的加密、将密文上传至区块链等功能。数据使用者申请使用文件需要进行文件下载。



参考文献：

1. Shangping W, Yinglong Z, Yaling Z . A Blockchain-Based Framework for Data Sharing with Fine-grained Access Control in Decentralized Storage Systems[J]. IEEE Access, 2018:1-1.
2. 包括各种ABE相关方案的charm库：<https://github.com/JHUISI/charm>，建议使用其中最简单的方案
3. 区块链也可以使用超级账本