doi:10.1631/FITEE.1800119

题目：基于一致性哈希算法的低能耗共识协议

概要：当前区块链共识协议在去中心化、安全性和能耗方面存在“三难”优化困境。针对这个问题，基于一致性哈希算法，设计了两个新的区块链共识协议，分别为CHB-consensus和CHBD-consensus。在新的共识协议下，诚实的“矿工”可以公平地获得创建新区块的机会。在创建新块时，诚实矿工不再需要付出海量竞争性算力，且该新区块可获取整个区块链网络公平验证及确认共识协议。恶意矿工则必须付出海量算力资源才能攻击新区块，以创建特权或实现“双花”。由CHB-consensus和CHBD-consensus共识形成的区块链网络基于与比特币系统相同的安全性假设，在节省海量电力的同时，不会牺牲去中心化和安全性。分析了可能的攻击行为，并给出严格但可调整的验证策略。CHB-consensus和CHBD-consensus共识引入数字身份证书管理机构（CA），CA对区块链网络或区块链数据结构没有特殊管理权或控制权，但依据CA系统信誉和可靠性，存在一定隐私泄露风险。最后，分析了CHB-consensus和CHBD-consensus共识的鲁棒性和能耗，并通过理论推导证明它们的优势。

关键词：区块链；共识协议；一致性哈希；低能耗；去中心化