平成30年度 情報工学コース卒業研究報告要旨

楫 研究室	氏　　名	百瀬孝紀
卒業研究題目	Hybrid-DAG Consensus: 非中央集権的で高速処理可能な許可無しモデルにおけるコンセンサスプロトコル	

2008年にSatoshi Nakamotoの提案したBitcoinは, 暗号通貨のみならず許可無しモデルにおけるビザンチン故障耐性のあるコンセンサスプロトコルを実現した. しかし, Bitcoinにはスループットに制限がある, トランザクションの定着時間が遅いなど, 深刻なスケーラビリティの問題が存在する. また, システムの運営コストが一部の参加ノードに集中するため, 中央集権化しているという問題もある. これらの問題を解決すべく, 多くのコンセンサスプロトコルが提案されている. 例えば, PHANTOMやSPECTREは, Bitcoinやその他の多くの暗号通貨に用いられているデータ構造であるブロックチェーンを拡張したblockDAGを用いることでスループットの制限, 中央集権化問題の解決を目指している. Hybrid Consensusでは, Bitcoinのコンセンサスを利用して特別なノードの集合であるCommitteeを決定し, Committeeによってトランザクションの処理を行うことで, 許可無しモデルから許可有りモデルに帰着し, スループットの制限やトランザクションの定着時間の問題を解決することを目指している. しかし, これらのプロトコルにもいくつかの問題点が存在する. 本研究では, Hybrid Consensusに改良を加え, 高速なトランザクション処理性能を確保したまま, Committeeに集中しがちなシステムの運用コストを参加ノード全体に分散可能な, 非中央集権的なコンセンサスプロトコルHybrid-DAG Consensusを提案する. Hybrid-DAG ConsensusではHybrid Consensusと異なり, トランザクション処理をCommittee以外のノードが並行して行うことによって, ネットワーク全体でトランザクションの大規模な分散並列処理を可能にしている. これにより, システム全体のトランザクションのスループットを大幅に上げることが可能になる上, Hybrid Consensusで懸念されるトランザクションの大量生成によるCommitteeへのDoS攻撃も防ぐことができる. また, Hybrid-DAG Consensusでは高速なトランザクション処理と同時にCommitteeの選択も行うため, Committeeの選択も高速に行うことができる. このため, Committeeに含まれるノードが長い時間に渡って処理を続ける必要がなく, 非中央集権的なプロトコルになる. Hybrid-DAG Consensusでは, トランザクション処理とCommitteeの選択という2つの作業を行うことで, Hybrid-DAGというデータ構造を生成する. Hybrid-DAGは, PHANTOMやSPECTREでトランザクション処理に利用されているblockDAGを拡張したデータ構造であるが, blockDAGとは異なり, 部分的線型構造を有する. このため, ブロック間の全順序を決定するのが難しいというblockDAGの問題点も解決している. さらに, 動的なパラメータの調整にも有利であり, スケーラビリティの点においても有利であるという特徴を持つ.