ブロックチェーンの Proof-of-Work の計算資源を利用して最適化問題の解探索を行うプロトコル(ポスター発表)

柴田直樹†

奈良先端科学技術大学院大学

1 はじめに

ビットコイン[1]の登場以来，ブロックチェーンを利用した暗号通貨が多数開発されてきた．Proof-of-work(PoW)と呼ばれる仕組みにより正しい取引の結果を決めており，コインの二重使用等を防いでいる．PoW では，ネットワークに参加するノードがある計算を行うことで，ノードの持つ計算量に応じた投票権を行使できるような多数決がとられる．なりすましの容易な計算機ネットワークにおいて，PoW は非常にロバストに動作する一方，PoW のために浪費される計算資源および電力が社会問題となっている．本稿では PoW を代替するブロックチェーンの仕組みを提案する[2]．提案手法では，ブロックチェーンにおいて多数決をとるために必要な計算量を任意の最適化問題のインスタンスの近似解を探索するために利用できる．提案手法によりブロックチェーンを最適化問題を解くためのバッチ処理システムとして利用することができ，ジョブの登録，実行，見つかった最適解のクライアントへの提供などの仕組みなどが提供される．任意のユーザが最適化問題のインスタンスをジョブとして登録することができる．

2 ビットコインと PoW

ネットワークにおいては多数の IP アドレスを確保するのが容易であり，IP アドレスに対して投票権を与える多数決は機能しない．PoW は計算量に投票権を与える多数決である．複数の項目からなる情報をブロックとし，多数のブロックをリンクトリストとしたものがブロックチェーンである．各ブロックには一つ前のブロックのハッシュ値が含まれる．新しいブロックがチェーンに追加される毎に，新しいブロックのハッシュ値が計算され，ネットワーク上にブロードキャストされる．各ブロックには，ナンスと呼ばれる整数値を格納するエントリが用意されており，ブロック全体のハッシュ値が決められた数のゼロビットで始まるナンスを持つブロックのみが，有効なブロックとして受理される．新しいブロックを追加することに成功したノードにインセンティブとして新しいコインが授与される．ブロックを追加しようとするノードのことをマイナーと呼ぶ．善意のマイナーは最も長く，かつ正しい内容のチェーンにブロックを追加しようとする．大半の CPU 資源が善意のマイナーにより供給される限り正しい取引を記録したチェーンが最も速く伸びる．

3 提案手法

本稿では PoW のために浪費される計算資源を最適化問題の近似解の探索に利用するための完全分散型多数決プロトコルを提案する．任意のノードが任意の最適化問題の解探索ジョブを登録することができる．整数値の代わりに解候補とその評価値を連結したものをナンスとして用いる．有効なナンスを生成するためにはマイナーは何らかの解候補を評価する必要がある．多数決を取る過程において多数のナンスが生成され従って多数の解候補が評価される．解探索を効率化するために，遺伝アルゴリズムのような解探索アルゴリズムの実装をジョブに含める．これは内部的に何度も解候補を評価し，そのたびに対応するナンスを含むブロック全体のハッシュ値を計算し，それが指定された個数のゼロビットで始まるか調べ，そうである場合は新たなブロックをネットワークにブロードキャストする．ノード間の共謀を防止するため，提案手法では二つの異なった方法でマイニングノードにインセンティブを提供する．新しいブロックを追加することに成功したマイナーに対しては PoW と同様に新たなコインを授与する．各ジョブに対し最も良い近似解を見つけたノードに対しては解探索ジョブを登録したノードが料金を支払う．クライアントはマイニングをすることなくジョブを登録することができ，マイナーはジョブを登録する必要はない．ジョブがなければ，提案手法は PoW と同等の働きをする．

参考文献

[1] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” Dec 2008.

[2] N.Shibata, “Proof-of-Search: Combining Blockchain Consensus Formation With Solving Optimization Problems,” in IEEE Access, DOI: 10.1109/ACCESS.2019.2956698

† Naoki Shibata, Nara Institute of Science and Technology