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

柴田直樹（奈良先端大）

背景と目的

- ビットコインは，善良な計算機が十分多く参加する限り正しく動作する
  - ネットワーク上のデータに金銭的価値を与えるために必要な性質
- ブロックチェーンと言うネットワーク上にデータを保持する方法を利用
- Proof-of-Work(PoW, 仕事量の証明) と呼ばれる仕組みにより正しい取引を保証
  - PoWは参加ノード間で多数決を取る方法
- PoWには，**電力と計算資源を浪費**する欠点
  - ブロックチェーンのために浪費された電力はアイルランド全体の電力に匹敵

- **提案手法では，浪費されていた計算量を任意の最適化問題の解探索に利用できる**

ビットコインの仕組み

- 多数の計算機ノード間で多数決を取ることで正しい取引を保証
  - 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 → IPアドレスに投票権を与えるやり方はうまくいかない
  - IPアドレスではなく計算量に投票権を与える
- ブロックチェーン
  - 全取引情報を記録，全ノードが参照可能
  - 複数の取引の情報をブロックに格納
  - 新しいブロックが次々と追加される
  - 過去のブロックを書き換えることはできない
- Proof-of-Work
  - ブロックにナンスと呼ばれる整数値を格納できるエントリを設ける
  - ブロック全体のハッシュ値が指定された数のゼロビットで始まるようなナンスを探す
  - そのようなブロックのみが有効なブロック
- 多数決を取る
  - ノード群が上記のようなナンスをこぞって探す
  - 最も長く，正しい内容のチェーンに対して新しいブロックを追加しようとする
  - これにより，多数決として働く
  - ブロックを追加したノードにはコインが与えられる

提案手法でできること

- PoWを代替するプロコトル
- 最適化問題を解くためのバッチ処理システムとしてブロックチェーンを利用可能
  - ブロックチェーンを構成するネットワーク上の計算機群が，解探索をしつつ多数決を取る
  - 任意のユーザが事前登録なしに利用可能
  - 任意の最適化問題の近似解の探索が可能
  - ユーザの支払った金額に応じて解探索に利用されるCPU資源が可変

- **利用手順**
  1. ユーザが解探索プログラムを実装
  2. プログラムと探索料金をブロックチェーンに登録
  3. 探索料金は仮想通貨の口座から自動引落
  4. ブロックチェーンを構成する計算機群が解探索を実行
  5. 解探索に使用されるCPU資源の期待値は支払った料金に比例
  6. やがてブロックチェーンに見つかった解が登録される

提案手法のアイデア

- 多数決をとりつつ解探索を行う
  - 遺伝アルゴリズムなどでは，多数の解候補を評価することにより解探索が進行
  - ハッシュ関数を計算する代わりに解候補の評価値を計算
- 最適化問題の解候補とその評価値の連結をナンスとする
  - PoWと同様に、ブロックのハッシュ値が決められた数のゼロビットで始まるようなナンスを見つけることでブロックを追加する
  - ナンスを生成するために新たな解候補を評価

- 不正を防止するために
  - ジョブ登録前にあらかじめ計算しておき，解探索のインセンティブを不正に取得
  - **解決法**：良い解を見つけるインセンティブを探索を依頼するノードが支払う
  - ブロックを追加する報奨金と良い解を見つける報奨金を独立させる

発表論文等

- Naoki Shibata : “Proof-of-Search: Combining Blockchain Consensus Formation with Solving Optimization Problems, ” IEEE Access, doi: 10.1109/ACCESS.2019.29566
- 柴田直樹 : “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” 高度交通システムとスマートコミュニティ研究会研究報告　2019-ITS-79(25) pp. 1-6