プレスリリース

2019 年 12 月 2 日

報道関係者各位

国立大学法人　奈良先端科学技術大学院大学

ブロックチェーンで浪費されている電力を有効利用
資産運用、工学研究などの最適化問題の解を探索する安価な手法を開発

【概要】

奈良先端科学技術大学院大学（学長：横矢直和）先端科学技術研究科 情報科学領域 モバイルコンピューティング研究室の柴田直樹准教授は、ビットコインなど仮想通貨の仕組みであるブロックチェーンという分散管理、相互監視のシステムを維持する際に浪費されている電力や計算資源を利用して計算することにより、最適な解（近似解）を低コストに探索する仕組みを開発しました。工学、生物学の解析研究や資産運用、ニューラルネットワークの構築などの際に、一般ユーザが登録して使えます。

工学研究や、その成果を社会での応用に結びつける際に、与えられた制約のもとで最も良い選択を行うことが必要になる場面があります。例えば、タンパク質の構造解析、投資ポートフォリオの最適化、神経網を模した「ニューラルネットワーク」の数理モデルの構築などです。このような選択の場合、様々な要因の組合せに対して、それがどの程度良いか評価を行い、最も良いものを探索する必要があります。このような課題は、最適化問題と呼ばれ、取り入れる要因の数が増えるに伴い、組合せの数が爆発的に増加するため、解くテーマによっては、極めて大きな計算量が必要となります。
一方、ビットコインなどの暗号通貨に利用されているブロックチェーンでは、取引の正しさを保証するために極めて大きな計算量が必要になり、計算機を動かすために膨大な電力が必要となっている現状があります。

今回開発した手法により、この浪費されている電力と計算資源（CPU やメモリの稼働時間など）が最適化問題の解探索のために併用できるようになります。解探索を行うためには、ブロックチェーンを構成している多数の計算機からなるネットワークに対し、一般ユーザが任意の最適化問題の解探索ジョブを登録します。ブロックチェーンを構成する計算機群は、登録されたジョブの解探索を行う一方で暗号通貨の取引の正しさを保証します。従来手法では、取引の正しさを保証するためだけに計算を行っていたところを、開発した手法では同時に一般ユーザが求める解探索を行うことで正しさを保証できるようにして余剰の電力を活用したことが、新しい点です。また、提案手法は、一般ユーザが任意の解探索ジョブを登録したり、探索の結果得られた解を受け取ったりすることのできる仕組みを提供し、利便性を確保します。

最適化問題の種類は非常に多く、実社会のあらゆる分野において存在します。本手法の特徴として、任意の最適化問題の解探索が安価に行える利点があります。タンパク質の構造解析、投資ポートフォリオの最適化、ニューラルネットワークの最適化に加え、LSI（大規模集積回路）の設計、生産計画や輸送計画の策定、自動車や建築物の構造最適化など、計算量の多い組合せ最適化問題が安価に解けるようになると期待されます。

この成果は、2019 年 11 月 28 日付けで IEEE Access にオンライン公開されました。(URL：https://ieeexplore.ieee.org/document/8917609)

つきましては、関係資料を配付いたしますので、取材方よろしくお願いいたします。

【ご連絡事項】

(1)本件につきましては、奈良先端科学技術大学院大学から奈良県文化教育記者クラブをメインとし、学研都市記者クラブ、大阪科学・大学記者クラブへ同時にご連絡しております。
(2)取材希望がございましたら、恐れ入りますが下記までご連絡願います。
(3)プレスリリースに関する問い合わせ先

奈良先端科学技術大学院大学　先端科学技術研究科
情報科学領域モバイルコンピューティング研究室　柴田直樹
TEL： 0743-72-5251　　E-mail： n-sibata@is.naist.jp

【開発の背景】

ビットコインは、外部の計算機や組織に依存せず、善良な計算機が十分多く参加し、相互監視し続ける限り正しく動作するという性質を持ちます。これにより、ネットワーク上の単なるデータに金銭的価値を与えるという、ビットコインの登場前には考えられなかったことを可能にしました。ビットコインでは、ブロックチェーンと呼ばれる、ネットワーク上にデータを保持する方法を利用して、プルーフオブワーク(PoW、仕事量の証明）と呼ばれる仕組みにより多数決を取り、正しい取引を保証しています。ただ、PoW は非常に頑健に動作する一方で、電力と計算資源を浪費する欠点を持っており、2018 年にビットコインを含むブロックチェーンのために浪費された電力(少なくとも 2.55GW)は、アイルランド全体で消費された電力(3.1GW)に匹敵するという調査結果もあります。

【課題】

これまでにも PoW を代替する仕組みが提案されてきました。しかしながら、PoW と同等に頑健な手法の実現は困難であり、そのため依然として PoW がよく使われています。PoW の持つ良い性質として、以下が挙げられます。

- 外部の計算機や組織に依存しないこと
- 単一故障点が存在せず、任意の計算機が任意のタイミングで予期せぬ動作をしても、他に正しく動作する計算機が十分に多く参加し、カバーしている限り全体として正しく動作すること
- なりすまし行為に対する耐性があること
- 事前登録なしにいつでも参加できること

提案手法では、上記の性質をすべて保ったまま、ブロックチェーン上での最適化問題の解探索を実現します。

【開発した技術】

本研究では、PoW を代替するブロックチェーンの仕組みを開発しました。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近似解を探索するためにも使うことができます。この手法により、一般ユーザが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できるようになります。また、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を提供します。

さらに、任意のユーザが任意の最適化問題の解探索ジョブをブロックチェーンに登録することができ、その際に支払った対価に応じた計算量で解探索が実行されます。例えば、あるクライアントが、最適化すべき問題を持っているとします。このクライアントは、この問題の解探索に支払う料金を決め、問題の解を探索するプログラムを実装します。次いで、これらを組み合わせてジョブを作成し、ブロックチェーンに登録します。この料金は自動的に仮想通貨の口座から引き落とされ、その際にこのジョブのために使用される CPU（中央演算処理装置）の計算資源としての期待値が、料金に比例するように調整されます。このようにして、ブロックチェーンを構成する計算機群がこの問題の解を

探索し、見つかった解はいずれブロックチェーンに登録され、クライアントは支払った料金と引き替えに見つかった解を受け取ることができます。

【今後】

複雑なデータを処理するためには、通常高性能な計算機が必要になります。一台の高価で高性能な計算機の代わりに、多数の安価なコンピュータを利用する、分散コンピューティングという方式があります。この方式により、世界中の PC の余った計算能力を集めて、スーパーコンピュータに匹敵する計算速度を実現するプロジェクトが世界中で実行されています。例えば、Berkeley Open Infrastructure for Network Computing(BOINC)では、分散コンピューティングのためのクライアント・サーバ型ソフトウェアを提供しており、このソフトウェアを利用した分散コンピューティングが世界中で稼働しています。これらのうちの少なくとも一部は最適化であり、比較的容易に提案手法の枠組みでも実行できるようになると考えています。例えば、Folding@Home は、タンパク質の折りたたみ構造を解析し、これに関係する様々な疾病の治療に役立てるプロジェクトで、多数のタンパク質の折りたたみパターンの中から正しい折りたたみ構造を選ぶことは最適化問題の解に相当します。

今後、提案手法を実装し、上記のようなプロジェクト等に貢献できるようにするため、実証実験を進めていく予定です。そのときに最も困難が予想されるのは、クライアントが実装した解の探索プログラムを動作させるための性能の良い実行環境の設計・実装です。提案手法を正しく動作させるためには、いくつかの性質を満たすジョブの実行環境が必要となります。インタプリタと呼ばれる、プログラムを逐次解釈しながら実行する環境であれば容易に実現できますが、性能が出ません。今後、性能の良い実行環境の設計・実装や、その他の部分についての実装も行っていきます。

【用語説明】

ブロックチェーン
仮想通貨等で用いられるデータをネットワーク上で保持する仕組み。複数のデータの項目を格納したブロックのリストであり、一度、ブロックチェーンに追加されると、そのブロックを変更することが困難であるように設計されている。

プルーフオブワーク(PoW)
ネットワーク上ではなりすましが容易にできてしまうので、IP アドレスに対して投票権を与えるような多数決の仕組みは、IP アドレスをたくさん確保できるユーザにより乗っ取られることがある。その事態を防ぐため、PoW は、計算量に対して投票権を与えるような多数決の仕組みであり、ビットコインはこのような仕組みを取り入れることで、ほとんどの計算量が善良なノードによって供給される場合に正しく動作する。

バッチ処理システム
あらかじめ登録した処理手順を一括して行うシステム。計算処理を対話的に行うシステムと異なり、計算処理のリクエストであるジョブを貯めておき、ある時点で一括して実行する。

インタプリタ

人が理解できるプログラミング言語で書かれたソースコードを逐次解釈しながら、機械語で実行するプログラム。ソースコードをまず機械語に変換するコンパイラによる実行と比べると、実行速度が遅い。

【参考資料】

日本語の概要およびプレゼンテーションスライドが下記 URL から参照できます。

https://researchmap.jp/?action=cv_download_main&upload_id=291890
https://www.slideshare.net/NaokiShibata/proofofwork-196973124

【本プレスリリースに関するお問い合わせ先】

奈良先端科学技術大学院大学　先端科学技術研究科
情報科学領域モバイルコンピューティング研究室　柴田直樹
TEL：　0743-72-5251　　E-mail：　n-sibata@is.naist.jp