称号及び氏名	博士（工学）　Kudzin Alexander Nicholas
学位授与の日付	2024 年 3 月 31 日
論　文　名	「Blockchain technology for the energy grid's information system」
論文審査委員	主査　石亀 篤司
	副査　山田　誠
	副査　林　海

論文要旨

分散型再生可能エネルギーなどの発電形態の変化によるユーザーの行動変化の結果、世界のエネルギーグリッドはトポロジカルな変貌を遂げている。2050 年カーボンニュートラルを達成するためにエネルギーグリッドを脱炭素化する中で、電力システムでは、太陽光や風力発電などの分散型電源の大量導入や、さまざまな電力市場の開設、需要形態の変化、VPP 事業を展開するアグリゲータ等、グリッドトポロジにおいて大変革が起きている。

このユーザー行動と発電形態の変化がエネルギー管理システム（EMS）に及ぼす影響は、ピアツーピア（P2P）販売や小規模分散型エネルギーグリッドなど、情報システムにおけるユーザー対話量の増加によるものである。EMS に対する従来の集中型アプローチでは、通信量とシステムの複雑さの急激な増大に対処するには非効率であり、AI ベースのエネルギー制御手法とスマートメータなどの計測機器が次々に開発され、需要家ノードへ展開されることにより、EMS はハイブリッド分散階層システムへと発展してきた。

しかし、従来型発電に比べて分散型再生可能エネルギーの比率が高まるにつれ、管理の複雑さや通信量が増大し、制御手法の研究も AI の協調化に向けて進んだ結果、通信量はさらに増加している。需要家ノードに対するパフォーマンス要件も高度化し、EMS トポロジはハイブリッド分散階層型から分散型システムへと再び進化してきており、ブロックチェーンが将来の分散型エネルギーグリッドの基礎となるインフラを形成する可能性について多くの関心が集まっている。

本論文ではまず、分散型エネルギーグリッドの要件が提案されている分散型エネルギーグリッドを調査し、分散型エネルギーグリッドへの適合性についてさまざまなブロックチェーンを評価した。次に電力システムへの適用要件を満たすために、レジリエンス、セキュリティ、プライバシー、柔軟性、さらにスループットとスケーラビリティを考慮して Ethereum 2.0 を選定し、そのアルゴリズムの高速化と信頼性向上のための研究を行った。

初期段階での検討では、Ethereum 2.0 で利用されるクロスシャード通信方式であるロールアップのスループットは、エネルギーグリッドの要件を満たすために大幅に向上出来る可能性があ

ることに着目した。この課題が解決されれば、EMS の分散型エネルギーグリッドの基盤システムとして展開できるようになる。そこで本研究では、通信量やその手順を大幅に改善するための 3 つのアプローチを提案した。

アプローチ 1　効率的なデータ構造によるメッセージサイズの削減

Ethereum 2.0 での仕様データ構造を分析し、特にツリーとメッセージの構造とレイアウトに関して複数の効率改善の可能性があることを明らかにした。これらをより効率的なデータ構造に改良することで、ブロックに収容できるクロスシャードトランザクション(TX)数の増加が可能となる。これらの効率的なデータ構造により、使用する実装アプローチによるが、TX サイズを 65% から最大 97.6% 削減でき、通信パフォーマンスを 2 倍以上向上させることを実現した。

アプローチ 2　ロールアップの集約証明認証の計算コストの削減

Ethereum 2.0 で提案されている最先端のペアリングチェックには、2 つのペアリング、3 つのべき乗（Exp)、3 つの乗算（Mul)、および 1 つの加算（Add）が含まれており、n 個の集約された Kate-Zaverucha-Goldberg 多項式約定(KZG)のためにセキュリティ因子を S 回実行する必要がある。この手順において提案法では、検証者と証明者の両方に対して、計算時間を大幅に改善した。計算回数の削減を以下に示す。

1）検証者の場合：ペアリングチェック 2 回、Exp なし、Mul 1 回、Add 1 回

2）証明者の場合：ペアリングチェック 1 回、Exp なし、Mul 4 回、Add 1 回。

アプローチ 3　Ethereum 2.0 と比較したロールアップの証明集計の計算コスト削減

現行の集計方法では 指数オーダーの計算が発生しコスト高となるため、IoT スマートメータ(SM) などの IoT デバイスへの共有ブロックチェーンの展開が難しくなる。この問題を解決するために、並列計算化を実装し O(ℓ)の計算時間となる代替集計法を提案した。しかし、初期配列を作成するために必要な加算計算コストや、配列計算に必要な冗長な加算数など、複数の問題が発生した。その解決法として、必要なすべての加算を並列化して O(n) 時間で計算する手法と、計算ステップを減らすための手法を新たに提案し、63.99% のパフォーマンス向上を得ている。

提案法では、n 個の加算を処理するために利用できる n/2 個のノードがある場合、計算コストを $O(\log 2n + (\log 2\ n) * c)$ に改善することが可能となった。

最後に、すべての提案を一括して電力システムを対象としたブロックチェーンに適用し数値シミュレーションを行った。その結果、 i）データサイズの削減、ii）検証コストの削減、および iii）集計コストの削減が達成され、非常に有用な結果が得られた。

提案法の適用において、KZG を使用する KZG ロールアップへの切り替えには、データサイズが TX あたり 34 バイトから 37 バイトに大幅に増加するという望ましくない影響が生じる。ただし、このデータサイズの増加は、検証と集計の低コスト化によって軽減され、KZG ロールアップのバイトあたりのガスコストを 68 ガス/バイトの削減できるため、悲観的に見たロールアップと KZG ロールアップの間でブロックあたりのロールアップのパフォーマンスを同等に維持できる。このガスコストの安さは、KZG の使用を制限する最後の大きなボトルネックである SM などの IoT デバイスの KZG ロールアップにおける ii）および iii）の改善の直接の結果である。

審査結果の要旨

本論文は，2050 年カーボンニュートラルを目指してトポロジカルな大変革が続いている電力システムに対して、ブロックチェーン技術を取り入れた P2P（Peer to Peer）販売などの新たな需要形態に対する，システム構成の効率化と電力取引の高速化に関する課題解決について研究したものであり，以下の成果を得ている。

（1）効率的なデータ構造によるメッセージ サイズの削減

Ethereum 2.0 での仕様データ構造を分析し、特にツリーとメッセージの構造とレイアウトに関して複数の効率改善の可能性があることを明らかにした。これらをより効率的なデータ構造に改良することで、ブロックに収容できるクロスシャードトランザクション(TX)数の増加が可能となる。これらの効率的なデータ構造により、使用する実装アプローチによるが、TX サイズを 65% から最大 97.6% 削減でき、最終的に、通信パフォーマンスを 2 倍以上向上させることを実現した。

（2）ロールアップの認証計算コストの削減

Ethereum 2.0 で提案されているペアリングチェックには、2 つのペアリング、3 つのべき乗、3 つの乗算、および 1 つの加算が含まれており、n 個の集約された Kate-Zaverucha-Goldberg 多項式約定のためにセキュリティ因子を S 回実行する必要がある。ロールアップの集約証明認定の計算コストを削減する本提案法では、検証者と証明者の両方に対して、計算時間を大幅に改善することを確認した。

（3）ロールアップの証明集計コストの削減

現行の集計方法では指数オーダーの計算が発生しコスト高であるため、IoT スマートメータなどへの共有ブロックチェーンの展開が難しくなる。この問題を解決するために、並列化計算を実装し O(ℓ)の計算時間となる代替集計法を提案した。しかし、初期配列作成に必要な加算計算コストや、配列計算に必要な冗長な加算数などの問題が発生したため、必要な全ての加算を並列化して計算し、計算ステップを減らすための手法を新たに提案し、パフォーマンスが 63.99% 向上していることを確認した。

以上の諸成果は，ブロックチェーン技術に基づく P2P システムを実現していくうえで有用な検討結果であり，これからの新エネルギーとの共存，新形態グリッドの登場という新たなフェーズに対して，電力システムのトポロジィ形成に貢献するところ大である。また，申請者が自立して研究活動を行うのに必要な能力と学識を有することを証したものである。学位論文審査委員会は、本論文の審査および最終試験の結果から、博士（工学）の学位を授与することを適当と認める。