様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　４ 年　 ６ 月 ２３ 日現在

機関番号：２３２０１
研究種目：研究活動スタート支援
研究期間：2019～2021
課題番号：１９Ｋ２４３５０

研究課題名（和文）1000倍規模のブロックチェーン取引生成に耐えるGPU内ブロックチェーンシステム

研究課題名（英文）In-GPU Cache for Acceleration of Transaction Generation in Blockchain System

研究代表者
森島　信（Morishima, Shin）

富山県立大学・工学部・講師

研究者番号：９０８４３７４８

交付決定額（研究期間全体）：（直接経費）　　2,200,000円

研究成果の概要（和文）：ブロックチェーンシステムにおいて、フルノードの処理性能が取引生成向上を妨げる一因となっている。本研究では、取引検索、取引の異常検知といった読み込み処理と書き込み処理のボトルネックとなる取引の検証処理を対象とした。並列処理性能に優れたGPU(Graphics Processing Unit)上に取引データをキャッシュし、GPU内で処理を行うことで対象の処理を高速化することで、フルノードの処理のボトルネックを解消し、フルノードの処理性能の向上を実現した。

研究成果の学術的意義や社会的意義
ブロックチェーンは、P2Pネットワークで構築された分散型台帳システムであり、国際送金や個人間取引を直接取引により短時間かつ低コスト化する手段として用いられているが、取引生成性能の低さが大きな問題となっている。問題解決の手法の一つとして、ブロックチェーンの取引生成のプロトコルを変えることで多くの取引を生成させる方法が提案されている。しかし、そのような変更が行われれば、現状のシステムでは取引を処理するノードの処理性能が不足してしまう。本研究では、フルノードの処理性能を高めることで、既存の取引性能向上法を適用可能にし、ブロックチェーンの取引生成性能の向上に貢献した。

研究成果の概要（英文）：In blockchain systems, the processing performance of full nodes is one of the bottleneck of transaction generation.
In this study, we targeted the read process, such as transaction search and transaction anomaly detection, and the transaction verification process, which is the bottleneck of the write process. By caching transaction data on a Graphics Processing Units (GPUs), which has high parallel processing performance, and accelerating the target processing using GPUs, the bottleneck of the full node was eliminated and the performance of the full node was improved.

研究分野：計算機システム

キーワード：ブロックチェーン　GPGPU　並列処理

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

本研究の対象であるブロックチェーンは、P2P ネットワークで構成された分散型の台帳システムであり、最大の特徴は、銀行などの信頼できる第三者を要さずに送受信者が直接取引できる点であり、国際送金や個人間取引を直接取引により短時間かつ低コスト化する手段として用いられている。ブロックチェーンの問題点は、取引生成性能の低さである。現在、代表的なシステムであるビットコインの平均スループットは約 3tps　（transactions per second）であり、取引システムとしては極めて小さい。既存の取引システムの例では、VISA 社のクレジットカードの決済システムの平成 29 年の平均スループットは、年次報告によると約 3,500tps である。ブロックチェーンのネットワークは全ての取引を検証するフルノードで構築されており、各ノードでの取引検証等の処理の時間を確保するために取引量に制約が課されており、取引性能を低くしている。取引性能向上のため、この制約の緩和や、複数のネットワークでブロックチェーンを作成し、これを跨ぐクロスチェーン等のプロトコルが提案されている。しかし、これらの手法は共にフルノードが処理しなければならない取引量が増加するため、これらを実現するためにはフルノードの処理性能向上が不可欠である。

２．研究の目的

背景で示したフルノードの取引生成性能の向上を目的として、本研究では、並列処理性能に優れた GPU（Graphic Processing Unit)内にフルノードの取引情報を格納し、フルノードの性能向上にあたってボトルネックとなる処理を全て GPU で処理する GPU 内ブロックチェーンシステムによるフルノードの高性能化を行う

３．研究の方法

フルノードの処理の高性能化を行うにあたって、取引の読み込み処理、書き込み処理に分けてそれぞれの高性能化を行った。読み込み処理においては、取引情報を用いるにあたって必須となる取引の検索処理と不正取引等の不正防止に有効な取引の異常検知を対象とした。書き込み処理では、ブロックチェーンの取引生成の際には全てのノードで取引の検証を行う必要があり、この検証処理がボトルネックとなることから、取引検証処理を対象とした。

４．研究成果

前述した取引検索、取引の異常検知からなる読み込み処理と取引の検証処理のそれぞれの処理に対し、GPU 内で処理を行い、その情報を保持するのに適したデータ構造及びそのデータ構造を用いた GPU 処理アルゴリズムを提案し、性能評価を行った。その結果、読み込み、書き込み処理共に高速化に成功した。以下にそれぞれの処理の提案手法とその評価結果の概要を示す。

(1) 取引の検索処理

ブロックチェーンの取引データの特徴として、一度承認された取引は修正や削除がされず、書き込み処理は追加のみであるという点がある。この特徴を活かし、データの追加のみを考慮し、削除や修正を考慮せず、GPU 処理に適した木構造の配列表現をデータ構造に用いて GPU 内にキャッシュすることで高速化を行った。評価では、現状ブロックチェーン取引のデータ格納に用いられているキーバリューストアにおける検索と性能を比較した。その結果、CPU を用いた既存手法に対して 5.6 倍、GPU を用いた既存手法の 3.4 倍のスループットを達成した。

(2) 取引の異常検知

ブロックチェーンでは、秘密鍵の盗難等の不正な取引であっても、プロトコル的に誤った取引でなければ承認されてしまい、承認された取引は後に修正や取り消しを行うことが出来ず、不正取引の被害が拡大しやすいという問題がある。この問題に対処するためには、不正な取引がネットワーク上に流れ、承認が行われるまでの間に検知し、修正する必要がある。不正取引を検出する方法として異常検知が挙げられる。異常検知によって過去の取引データから実際の不正取引を検出することには既存手法でも成功していたが、処理性能の問題から取引の承認までに異常検知を実行するのは困難であった。

そこで、本研究ではブロックチェーンのユーザをグラフ表現で表したユーザグラフから、対象となる取引に関連した取引群のみからなるサブグラフを抽出し、サブグラフを用いて特徴量抽出と異常検知を行う手法を提案した。これにより、ブロックチェーンの取引量全体が増えても、計算量を一定に保ち実行時間を削減することに成功した。また、ユーザグラフを GPU 内にキャッシュし、サブグラフの作成、特徴量抽出、異常検知を全て GPU 内で実行することでそれぞれの処理自体も高速化することに成功した。この結果、異常検知の実行時間を取引承認までの時間であるブロック生成間隔よりも短い時間で異常検知を行うことに成功した。

(3) 取引の検証処理

ブロックチェーンの取引の検証処理は、様々な処理の組み合わせで実行されており、本研究では、取引の検証処理を構成する処理を分析し、ボトルネックとなる処理を特定した上でその処理を CPU と GPU の双方を用いて高速化した。取引検証処理でボトルネックとなる処理は、過去の取引の検索、ハッシュ計算、署名検証の三つの処理であり、これらの内 GPU による並列化の恩恵が小さい検索処理は CPU で行い、その処理と重複させて残りの 2 つの処理を GPU で処理することで、高速化を行った。その結果、提案手法は、バッチサイズを現時点の主要なシステムであるビットコインのブロックサイズとした場合に CPU 処理の 14.0 倍、GPU の並列処理性能に適したビットコインの 4 倍相当のブロックサイズとした場合に CPU 処理の 46.0 倍のスループットを達成した。

５．主な発表論文等

〔雑誌論文〕　計4件（うち査読付論文　4件／うち国際共著　0件／うちオープンアクセス　1件）

１．著者名 Morishima Shin	４．巻 92
２．論文標題 Scalable anomaly detection in blockchain using graphics processing unit	５．発行年 2021年
３．雑誌名 Computers & Electrical Engineering	６．最初と最後の頁 107087～107087
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.compeleceng.2021.107087	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 森島 信、松谷 宏紀	４．巻 J102-D
２．論文標題 GPUを用いたブロックチェーンのフルノードにおける取引検索の高速化	５．発行年 2019年
３．雑誌名 電子情報通信学会論文誌D 情報・システム	６．最初と最後の頁 378～389
掲載論文のDOI（デジタルオブジェクト識別子） 10.14923/transinfj.2018JDP7043	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 MORISHIMA Shin、MATSUTANI Hiroki	４．巻 E103.D
２．論文標題 In-GPU Cache for Acceleration of Anomaly Detection in Blockchain	５．発行年 2020年
３．雑誌名 IEICE Transactions on Information and Systems	６．最初と最後の頁 1814～1824
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transinf.2019EDP7159	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 森島　信	４．巻 -
２．論文標題 GPUを用いたブロックチェーンにおける取引検証の性能評価	５．発行年 2022年
３．雑誌名 電子情報通信学会論文誌D 情報・システム	６．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計1件（うち招待講演　0件／うち国際学会　1件）

1．発表者名 Shin Morishima
2．発表標題 Scalable Anomaly Detection Method for Blockchain Transactions using GPU
3．学会等名 20th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT 2019)（国際学会）
4．発表年 2019年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

6．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

7．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

8．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関