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　　元 年　　６ 月 ２４ 日現在

機関番号：６２６１５
研究種目：挑戦的萌芽研究
研究期間：2016～2018
課題番号：１６Ｋ１２４２５

研究課題名（和文）分散アルゴリズムへのブロックチェイン技術の応用に関する調査

研究課題名（英文）Study on Applications of Block-chain as Distributed Algorithms

研究代表者
佐藤　一郎（Satoh, Ichiro）

国立情報学研究所・情報社会相関研究系・教授

研究者番号：８０２８２８９６

交付決定額（研究期間全体）：（直接経費）　　2,600,000円

研究成果の概要（和文）：ビットコインなどの仮想通貨システムの基盤技術となるブロックチェインは、本来対象の仮想通貨以外にも分散システムの汎用技術としての可能性があるという仮定にも続く研究となる。本研究では、分散アルゴリズムにおける機能要件がビットコイン実装技術の機能で解決できるかを体系的に整理するとともに、代表的な分散アルゴリズムをビットコイン技術で実現する方法を明らかにした。なお、ビットコインの実現技術を分散アルゴリズムの実現技術として利用する場合、仮想通貨と分散アルゴリズムでは技術要件が違うために、ビットコインの実現技術のうち改変できる余地があるが、それも合わせて提案した。

研究成果の学術的意義や社会的意義
本研究により、ブロックチェインにより実現できる分散同意により、分散相互排除やリーダ選出など、複数コンピュータの同一情報を保持することが求められる分散アルゴリズムを実現できることがわかった。しかし、ブロックチェインが必要となるPoWは従来の分散アルゴリズムには負担を分散システムに求めること、ブロックチェインで実現できる分散アルゴリズムは多数ある一方、ブロックチェイン以外では実現できない、または実現が困難となる分散アルゴリズムは見いだせないことも明らかになった。

研究成果の概要（英文）：Blockchain is the core technology of existing electric currency systems, e.g., Bitcoin, was studied on the assumption that there were possibilities as general-purpose technologies of distributed systems in addition to their intial target, virtual currency. In this research, we systematically organized whether the functional requirements in the distributed algorithm can be solved by the function of the bitcoin implementation technology, and clarified the method to realize the representative distributed algorithm with the bitcoin technology. When using Bitcoin implementation technology as a distributed algorithm implementation technology, there is directions for modification among bitcoin implementation technologies because the virtual currency and the distribution algorithm have different technical requirements.

研究分野：分散システム

キーワード：分散アルゴリズム　ブロックチェイン　分散同意問題

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９、ＣＫ－１９（共通）

１．研究開始当初の背景

ビットコイン(Bitcoin)に代表される仮想通貨は、その実現技術としてブロックチェイン(Block Chain)と呼ばれる機構を利用している。ここでブロックチェインとは、非集中制御型の台帳情報の共有で連携する技術及びその実現システムの総称となる。ブロックチェインはビットコインのコア技術として開発されたものであり、台帳に相当する、ブロックと呼ばれ、鎖（チェーン）のように連結していくことによりデータを保管するデータベースを構成する。このデータベースは順序付けられたレコードの連続的に増加するリストを持ち、各ブロックには、タイムスタンプと前のブロックへのリンクが含まれている。

ここで連続するブロックの正当性は、起源となるブロックがもつハッシュ値を拠りところとする。すなわち、各々のブロックは、その一つ前のブロックのハッシュ値を持っており、そのハッシュ値を遡ってたどることで、ブロックが、どのようにつながっているかを辿ることができる。仮にフォークと呼ばれる、あるブロックを一つ前のブロックとして指し示すブロックが複数作成され、ブロックチェーンが分岐する現象が起きたとしても、そのうち長いほうが主鎖として合意され、その他のものは孤児ブロックとして、主鎖から外される。

ブロックチェーンに参加する者は、プルーフ・オブ・ワーク（Proof of Work, PoW）と呼ばれる、計算に時間のかかる値を最初に計算すると、次のブロックを生成することができるようになる。あるブロックの内容はそのブロックのハッシュ値が直後のブロックに記載されることで証明されることから、いったんチェーンに追加されたブロックを改竄するには、それ以降のブロックを全て破棄し、これまでに時間をかけて行われてきた各ブロックのプルーフ・オブ・ワークの演算を全てやり直さなくてはならないため､現実的には改竄はできないとされている。

本研究の目的は、前述のように既存の分散アルゴリズムの実現技術として、ブロックチェインが利用できるのか、利用できるとしてどのような実現方法が求められるのか、またその際の機能的及び性能的なメリットとデメリットがあるのかを知ることとなる。ここで分散アルゴリズムとは、相互接続されたコンピュータにより構成されるハードウェア上で実行するためのアルゴリズムである。分散アルゴリズムは分散コンピューティングの多くの応用分野において使われている。分散アルゴリズムによって解決された標準的な問題として、リーダー選出、分散合意、分散検索、全域木生成、相互排除、リソース割り当て、原子ブロードキャストなどがある。

２．研究の目的

本研究ではブロックチェインにより、分散アルゴリズムを構築することの可能性や問題点を明らかにすることである。さてブロックチェインであるが、分散アルゴリズム的な視点からみると、コンピュータの誤動作がありえるビザンチン故障を想定した状況における複数のコンピュータ間で同じ情報を保有するための機構といえる。このため、既存の分散アルゴリズムの実現技術として、ブロックチェインが利用できるのか否かを明らかにすることは、分散アルゴリズムに関する研究及びブロックチェインの応用に関する研究に対して有用な知見となる可能性があるという仮説を設定して、その知見などを調査することが研究の目的となる。なお、分散合意などの特定の分散アルゴリズムについてはブロックチェインとの類似性が指摘されているが、既存の研究は概念的な議論にとどまっているが、本研究では体系化を行うこととする。

３．研究の方法

本研究では、(1)ブロックチェーンと分散アルゴリズムのシステム要件や、課題解決における前提と結果に違いに関する体系的な比較と､(2)前述のように分散アルゴリズムにより解決されうる、分散システムにおける標準的な問題をブロックチェーンによる実現可能性の調査という二つの方向が研究を実施した。ブロックチェーンと分散アルゴリズムの相違として、加えてビザンチン将軍問題を例にして両者の違いを調査していくこととした。ブロックチェーンによる分散アルゴリズムの実装は、分散アルゴリズムとして、リーダー選出、分散合意、相互排除に着目して実装可能性を調べる。

(1)ブロックチェーンと分散アルゴリズムの相違：分散アルゴリズムの難しさは、コンピュータ間通信における通信遅延により、全域的な情報(Global view)が見ることができないことによる。つまり、あるコンピュータから通信を受け取っても、その瞬間にはそのコンピュータは停止している可能性は排除できない。また、複数コンピュータ間であるひとつの状態を共有する、つまり分散合意を実現する場合、通信で保持すべき状態をコンピュータ間で共有するが、通信遅延のために同時性を維持できず、そもそも同時性についても因果関係などの何らかの順序関係に応じて与えられることになる。一方、ブロックチェーンは、ブロック間の有向グラフに基づくことになるために、分散アルゴリズムとのミスマッチが予想される。

(2)ビザンチン将軍問題とブロックチェーン:ビザンチン将軍問題を新しい解決手段としてブロックチェーンを位置づけられることが多い。ここでビザンチン将軍問題とは、相互に通信するコンピュータ群からなる分散システムにおいて、通信および個々のコンピュータが故障または故意によって偽の情報を伝達する可能性がある場合に、全体として正しい合意を形成できるかを問う問題である。さてビザンチン将軍問題では、将軍の人数を n、反逆者の人数を t としたとき、解決策が存在するのは n が (3 × t + 1) 以上の場合のみであるとされる。これは分散システムのコンピュータ数を n としたとき、n > 3t を満たさない場合の解が存在しない。言い換えれば、全プロセスの 3 分の 1 未満が障害という状況でないと、正しい動作を保証できないことを意味する。前述のようにブロックチェーンにより、n > 3t よりも効率的にビザンチン将軍問題が解けるという主張の妥当性を示した。

(3)ブロックチェーンによる分散アルゴリズムの実現可能性：リーダー選出、分散合意、相互排除に着目して実装可能性を調べる。なお、各アルゴリズムにおける動作の再現性に加えて、それぞれのアルゴリズムの要件、例えば相互排除アルゴリズムであれば、高々一つのコンピュータしか、クリティカルセクションを実行ができないことをアルゴリズムレベルで確認していく方法を用いる。なお、当初は、リーダー選出、分散合意、分散検索、全域木生成、相互排除、リソース割り当てなどの課題に関する代表的な分散アルゴリズムそれぞれをブロックチェインにより実現できるかを調査することを想定していた。手順としてはまず分散合意に関して、ブロックチェインによる実現可能性を調べることとした。

これは代表的な分散アルゴリズムは分散合意が解決すると容易に実装ができるからである。例えばリーダー選出と相互排除は、前者は分散システムを構成する複数コンピュータで保持する現在のリーダーに関する情報が同じになることが実現の鍵となる。また、後者は現在クリティカルセクションを 実行中扱いとなっているコンピュータは高々一個で、他のコンピュータは自らがクリティカルセクションを実行していないことを維持することである。その意味では分散合意により、前者は現在リーダーとなるコンピュータの情報を維持できればよく、一方、後者はクリティカルセクションを実行中または非実行中のコンピュータに関する管理できればよい。また、原子ブロードキャストは分散合意による合成形成を複数回を逐次的に実行しているのに他ならない。

４．研究成果

上記の３つの研究方法ごとに研究成果をまとめる。

(1)ブロックチェーンと分散アルゴリズムの相違：ところで分散アルゴリズムの難しさは、コンピュータ間通信における通信遅延により、全域的な情報(Global view)が見ることができないことによる。つまり、あるコンピュータから通信を受け取っても、その瞬間にはそのコンピュータは停止している可能性は排除できないという本質的かつ不可避は制約が分散システムに横たわっている。その制約そのものはブロックチェインも同じであるが、ブロックチェインはブロックという単位で扱っていることであるある。

しかし、ブロックチェインにおけるブロックの連鎖は 5 分間や 10 分間などの比較的長い所定時間ごとに行われることから、仮に 5 分間ごとにブロックを生成するブロックチェーンの場合、5 分間は待たないといけない。さらにブロックチェインは分散台帳と呼ばれるブロックが適切な状態となるのはタイミングは不確定である。仮に全体を大きく 2 分割するフォークが起きた場合、多数決により解決することとしているだけであり、仮に間違ったブロックでも過半数以上が支持してしまえば、主鎖として採用されることになる。また、ブロック連鎖においてフォークが生まれている可能性は直ちに判定できない。このため、ビットコインなどのブロックチェーンを用いた仮想通貨の取引において、一般に連鎖する複数ブロックの生成と確認をしたうえで処理の妥当性の判断しているのが実状である。一方、分散アルゴリズムの多くはコンピュータ間で一連のメッセージ交換を経ることで処理が終わることを想定している。従って、ブロックチェーンと分散アルゴリズムは課題設定が相違することとなる。

また、分散アルゴリズムにおいて合意に要する時間はメッセージ交換における通信遅延時間に依存するが、海底ケーブルを経由するような地球規模の分散システムであっても、分散アルゴリズムの一連の処理において 1 分間以上かかることは希である。以上より、ブロックチェーンにおける合意と、一般の分散アルゴリズムの合意は、合意の意味が違いあり、両者は同列に比較できるものではない。この他、ブロックチェーンでは PoW に代表されるブロックの発見に関わるコストが大きいが、分散アルゴリズムでは同様のコストがかかることはないといえる。

2)ビザンチン将軍問題とブロックチェーン：ビザンチン将軍問題では、メッセージに嘘があったとしても、反逆的な将軍が全将軍の人数の 3 分の 1 未満であれば「ビザンチン・フォールト

トレラント性」は達成される。前述のようにビザンチン将軍問題は、将軍の人数を n、反逆者の人数を t としたとき、解決策が存在するのは n が (3 × t + 1) 以上の場合のみであることが証明されている（n > 3t を満たさない場合の解が存在しない)。これは一人の司令官と二人の副官を想定したとき、司令官が反逆者ならば「司令官と副官」問題を解決できないことを証明することで､3分の1以上の反逆者がいる場合の解決策がないことを証明したのである｡A、B、C の三人がいて、A が反逆者だったとする。A が B には攻撃すると言い、C には撤退すると言い､B と C が相互にやりとりして A からどう指示されたかを教えあった場合､B も C も誰が反逆者であるかを判断できないことになる。

一方、ブロックチェーンでは、ビザンチン将軍問題における反逆者、つまりコンピュータまたはネットワークが間違った結果を返す状況では、その分散システムにおいて半数よりも多いコンピュータがブロックを認めればよいこととなっており、その意味ではブロックチェーンの耐故障性は、反逆者を 1/3 未満とするビザンチン・フォールトトレラント性よりも高いようにみえるが、前述のように両者は想定している設定が両者では相違することから、解いている課題が違うといえ、世の中でみかけるブロックチェーンはビザンチン将軍問題を解決し、されに効率もよいというのは合理的な見解とはいえないことがわかった。

(3)ブロックチェーンによる分散アルゴリズムの実現可能性:研究方法で述べたように分散合意を先行して実現の可能性を示したうえで、他の分散アルゴリズムの個別の実現する手順を実現可能性を調べていったが、研究成果 2)において説明したように、ビザンチン将軍問題とブロックチェーンの関係性、つまり、ビザンチン将軍問題は、コンピュータ及びネットワークに故障による間違いが存在する状況における分散合意の要件を示しているのに他ならない。従って、ブロックチェーンはビザンチン将軍問題の本質的な解決にならないということがわかったことから、他の分散アルゴリズムに関しても部分的な解決にならないことを意味している。

ここで前述のビザンチン将軍問題とはそもそもコンピュータ及びネットワークに故障による間違いが存在する分散システムを一般化した問題と位置づけることができる。個々の分散アルゴリズムの要件に限定すれば、ブロックチェーンにより解決ができる可能性はありえることから、分散合意アルゴリズムの実行が不可能とわかったが、引き続き個々の分散アルゴリズムについて調べることとした。

ただし、前述のように、分散アルゴリズムは個々の課題における分散合意を解決するためのアルゴリズムであることが多いことから、個々の分散アルゴリズムにおける分散合意に関わる側面とそれ以外に分けて調査を行った。例えばリーダー選出アルゴリズムは、リーダーの故障判定及びリーダーを選ぶプロセスは分散合意に含まれない。従って、分散合意をブロックチェーンで実現できれば、リーダー選出アルゴリズムの実現は故障判定及びリーダー選択プロセスを作れるかとなる。なお、その方法であるが、ブロックチェーンの外側、つまり一般の分散システムとして実現する場合、そのリーダー選択アルゴリズムは書くコンピュータが保持する現在のリーダーにする情報を維持するだけにブロックチェーンを利用することになるが、リーダーにする情報の維持は分散合意と同じである。

このため､仮にブロックチェーンによりリーダー選択アルゴリズムを実行する場合､分散合意以外のプロセスにおけるブロックチェーンの有用性と実装可能性を調べた。その結果、リーダー選出プロセスに関しては、①リーダーが故障していることを判断するサブプロセスと、その結果としてリーダーの故障が確認されたとき、②そのリーダー以外のどのコンピュータから次のリーダを選ぶサブプロセス、そして、仮に故障した思われた当初のリーダーを含めて、③本来リーダーではないコンピュータがリーダーとして振る舞った場合にそれを排除するサブプロセスがある。

まず①をブロックチェーンで実装した場合、故障したリーダーにより不適切な処理によってフォークが発生した場合、ブロックチェーンにより判定できる可能性がある。しかし、単純に故障発見であれば、同一の処理を複数コンピュータに処理を行わせる、つまり多重化を行い、その結果を多数決で選別すると質的な相違があるわけではない。その処理による計算コストにも依存するが、ブロックチェーンの PoW の方がその処理よりも大きくなることが想定され、その場合、ビザンチン・フォールトトレラント性に対応するにしても、処理の多重化でよく、ブロックチェーンを用いる合理的な理由があるとは言い難いという結論に至った。

そして、②については既存のリーダー選出アルゴリズムでは、コンピュータに予め与えられた識別子により決めることが多く、ブロックチェインを用いたからといって、特別な方法が想定されるわけではないといえる。

また、③については①の場合と同様に、本来リーダーではコンピュータがリーダーとして名乗ることは、そのコンピュータをリーダーとするブロックは、多数決の判断、つまり他のコンピュータの半分以上から賛同が得られなければ不適切なフォークと処理できる。ただし、多数決を実装するだけならばブロックチェーン以外の方法あり、ブロックチェーンを用いる積極的

理由は少ないといえる。さて本研究では、他の分散アルゴリズムについても、同様にブロックチェーンにより実装することの可能性とそれのメリットやデメリットを調査した。結論としては、分散アルゴリズムにおける分散合意に相当する部分に関して、仮にブロックチェーンにより代用可能だったとしても、各分散アルゴリズム特有の処理を実現することは、ブロックチェーンは利用可能性があるものの、他の方法の効率よく実現できるといえる。

この他、当初計画になかったが、分散トランザクションをブロックチェーンで実装できるかについても検討した。結論だけ述べると、分散トランザクションは、他のトランザクションと同様に、トランザクションの開始からコミットまでの機能的な一連の動作で完結する。しかし、ブロックチェーンの場合、例えば 10 分間単位というブロックの生成処理においてひとつのブロックにおける一連処理をクローズすることから、機能的な完結を前提にした分散トランザクションをブロックチェーンで実装した場合は、その齟齬を埋められることが前提になる。しかし、前述のようにそれを埋めるには分散トランザクションのセマンティクスの変更が必要となり、やはりブロックチェーンは分散トランザクションの実装技術的としては必ずしも適切とはいえないと結論づけるしかない。

また、本研究ではブロックチェーンの PoW を含む実行コストの定量的評価は、提案時の計画に含めなかったようにその研究実施においても評価していない。その理由は分散アルゴリズムを実現するためだけに、高いコストをかけて PoW を実行するよりも、他の方法でその課題は解決できるので、PoW にインセンティブがあるのは仮想通貨などの経済的なメリットが明確な場合に限られるという判断からである。なお、例えば何らかのデータの信頼性管理のためにその対象データの利用者が PoW の負担を負うなどの受益者負担のスキームも想定されるところであるが、当初計画通りに本研究では対象外とした。

５．主な発表論文等

〔雑誌論文〕（計 0 件）

〔学会発表〕（計 4 件）

発表者名：Ichiro Satoh:
発表標題：Mobile Agent: Lost Agent Technology. Why could Mobile Agents be in Practice?
学会等名：International Conference on Practical Applications of Cyber-Physical Multi-Agent Systems 2017(招待講演)(国際学会)
発表年：2017 年

発表者名：Ichiro Satoh
発表標題：An Approach for Recovering Distributed Systems from Disasters
学会等名：8th International Conference on Bio-inspired Optimization Methods and Their Applications(国際学会)
発表年：2018 年

発表者名：Ichiro Satoh
発表標題：Developing and Testing Networked Software for Moving Robots
学会等名：14th International Conference on Evaluation of Novel Approaches to Software Engineering, ENASE 2019(国際学会)（ベストポスターアワード受賞）
発表年：2019 年

発表者名：Ichiro Satoh
発表標題：Adaptive Software Deployment
学会等名：11th International Conference on Adaptive and Self-Adaptive Systems and Applications (ADAPTIVE 2019) (国際学会)（ベスト論文アワード受賞）
発表年：2019 年

〔図書〕（計 0 件）

〔産業財産権〕
○出願状況（計 0 件）

○取得状況（計 0 件）

６．研究組織

(1) 研究分担者
該当なし

(2)研究協力者
該当なし