ブロックチェーンを利用した セキュアな分散処理を実現するフレームワークの提案

城島 翔太[†1]　金子 晃介[†2]
西田 裕輝[†1]　堤 優亮[†3]　櫻井 幸一[†4]

概要：コンピュータで計算を行う際に，扱う問題の規模が大きい場合，単一のコンピュータでは多大な計算時間を要することがある．このような場合，複数のコンピュータの計算容量を用いて計算を分散させ，並列的に処理を行うことで計算時間の短縮を望むことができる．そこで本研究では，ネットワークに接続された不特定多数のコンピュータ同士が Peer-to-peer（以下，P2P）ネットワークで接続された環境において，分散計算が可能なフレームワークの開発を目指す．本研究の課題として，不特定多数のコンピュータ同士による P2P ネットワークで分散処理を行う際に，不具合のあるノードを介して誤った結果を出すことや悪意あるノードによる攻撃に晒されて信頼性のある結果が得られないということが挙げられる．そこでノード間で正しい値がやりとりされているかチェックを行いたいが，不特定多数のノードが参加するネットワークで値の正誤判別は難しい．よって本発表では，この問題を解決するために，ブロックチェーン技術を用いた分散処理を実現するフレームワークの提案を行う．

キーワード：ブロックチェーン，分散処理，P2P

The Proposition of Framework to Achieve Secure Distributed Computing by Using Block chain Technology

SHOTA JOHJIMA[†1]　KOSUKE KANEKO[†2]
YUKI NISHIDA[†1]　YUSUKE TSUTSUMI[†3]　KOUICHI SAKURAI[†4]

Abstract: When computing with computers, if the scale of the problem to be handled is large, a single computer may require a lot of calculation time. In such a case, it is possible to shorten the calculation time by distributing the calculation using the computational capacity of multiple computers and processing them in parallel. Therefore, in this research, we aim to develop a framework capable of parallel distributed computation in an environment where many unspecified computers connected to the network are connected by a peer-to-peer (P2P) network. The problem of this research is that reliable results cannot be obtained by a malicious node when distributed processing is performed on P2P network. Therefore, we want to check whether the correct value is exchanged between the nodes, but it is difficult to determine the correctness of the value in the network. In this presentation, in order to solve this problem, we propose a framework that realizes distributed processing using block chain technology.

Keywords: Block chain, Distributed Computing, P2P

1. 背景

近年のICT（情報通信技術）の進展により，IoTデバイスの取得情報の増加やウェブサーバ等で取得できるログデータが増大し，多種多量のデータ（ビッグデータ）が取得可能になった[1]．ビッグデータは信号機制御による渋滞緩和やウェブ通販サービス利用者の好みに合わせた商品のおすすめなど，様々な分野に活用されている[2]．ビッグデータを活用する為には，マイニングや機械学習などビッグデータの解析を行う必要がある．ビッグデータはその容量が多く，数テラバイト以上のデータを指すのが一般的である．その為ビッグデータの解析には多大な計算量と計算時間を要することが多い[3].

ビッグデータを用いた大規模な計算を行う際，自身の持つコンピュータでは十分な計算が行えない場合，外部の計算容量が十分なサーバを利用して計算を行う方法がある.この方法をクラウドコンピューティングという．クラウドコンピューティングとはネットワークを通じて外部のサーバコンピュータにアクセスし，サービスや計算領域，記憶容量を利用するシステムの事である．サーバの利用者に制限を設けるシステムをプライベートクラウド，インターネットを介して誰でも利用できるシステムをパブリック

†1 九州大学　大学院システム情報科学府
Graduate School of Information Science and Electrical Engineering, Kyushu University
†2 九州大学　サイバーセキュリティセンター
Cybersecurity Center, Kyushu University
†3 九州大学　理学部
School of Science, Kyushu University
†4 九州大学　大学院システム情報科学研究院
Faculty of Information Science and Electrical Engineering, Kyushu University
Security Laboratories, YY Corporation.

クラウドと呼ぶ．クラウドコンピューティングのメリットとして，利用者は外部のサーバの一部の計算領域使用するため，必要に応じて使用する計算領域の拡張，縮小が行う事ができることがあげられる．一方で計算や保管をクラウドサーバで一手に担う為，クライアント・サーバ型ネットワークの問題でもあるクラウドサーバがダウンした際に計算不可能となることや，クラウドサーバへの攻撃の際に利用者が対応できる手段がないなどのデメリットが存在する．他の計算方法として，ネットワークを介し複数のコンピュータに計算を分散させ委託する分散処理を行う事で計算を短時間で実行する方法がある．外部の複数コンピュータを用いて計算を行う具体例として，ボランティアコンピューティングがあげられる．ボランティアコンピューティングとは，インターネットを通じて有志者を募り，有志者がコンピュータを使用していない，もしくは使用している中で余った計算容量を用いて大規模な計算を分散させ並列に処理する計算方法である．計算に貢献した者は，その割合によって特典や報酬を得ることができる．メリットとして，クラウドコンピューティングより安価に計算容量を使用することができる事があり，デメリットとしては有志者のコンピュータを利用する為，信頼性に欠けることがあげられる．このように，大規模な計算問題を外部のコンピュータを用いて計算する方法の需要が高まっている．

一方で，外部のコンピュータの計算容量を利用することが理由で問題が生じている．外部のコンピュータを利用する際，クラウドコンピューティングのようにネットワークを介してつながれるコンピュータがサービスの利用者側・提供者側にわかれるシステムをクライアント・サーバ方式といい，ネットワークを構成するコンピュータが情報提供側であるサーバと情報利用者側のクライアントと2種類の役割に分かれる特徴を持つ．このタイプの通信方式では，サーバが停止するとクライアントとの通信が成り立たずシステムが停止するという問題が存在する．一方で，ボランティアコンピューティングのようなサーバやクライアントと役割を分けない同等の役割を持つコンピュータで構成するネットワークをPeer-to-Peer（以下，P2P）ネットワークという．P2Pネットワークとは，ネットワークを構成するコンピュータを情報提供側であるサーバと情報利用者側のクライアントと別の役割に分けるクライアント・サーバ型側とは異なり，サーバやクライアントと役割を分けずに同等の役割を持つコンピュータで構成するネットワークである．クライアント・サーバの通信方式の場合，サーバのみが情報提供側となるため，サーバの停止や攻撃を受けるとシステムが停止する時間，ダウンタイムが存在する．しかし，P2Pネットワークの場合では少数のクライアントが停止した場合でもシステムは維持され，ダウンタイムが存在しないというメリットが存在する．一方で，ネットワークで接続されるコンピュータは同等の役割を持つために上下関係が存在しない[4]．そのため，P2Pネットワーク内のコンピュータに間違った計算をするコンピュータが紛れ込んだ場合，その発見や対処が容易ではない問題がある．しかし，間違った計算を行うコンピュータが紛れ込んでは出力される結果の信頼性が失われてしまう．そこで，結果の信頼性をあげるため間違った解を排除しようと従来では冗長化と多数決が行われてきた．冗長化と多数決とは，あるコンピュータに依頼する計算と同等の計算を他の複数のコンピュータにも依頼し，それらのコンピュータの結果で最も多い答えを正しい答えとして採用する方式である．このような信頼できない外部コンピュータへ計算を委託する際，その答えが正しいものか検証を行うものをVerifiable Computingという．多量の外部計算資源を利用することが出来ても，計算結果に信頼性がなければその結果は使用できない為，Verifiable Computingの需要は高まっている[5].

しかし，上記の冗長化と多数決方式は同等の計算依頼の多くを悪意のあるコンピュータに依頼してしまった場合に信頼性の無い結果が採用される事や，同等の計算を多く行う事により信頼性は高まるが，計算の効率は落ちるなどいまだ課題が多い．

よって本稿では，ボランティアコンピューティングなどのP2Pネットワークで不特定多数のコンピュータ同士による分散処理を行う際に課題となる，悪意のあるノードにより信頼性のある結果が出ない問題の解決案として，ブロックチェーン技術を用いた新たなフレームワークの提案を行う．

2. ブロックチェーン

2.1 ブロックチェーン概要

ブロックチェーンとは分散台帳の技術であり[6]，Bitcoin等仮想通貨に活用されている．ブロックチェーンは，ユーザの取引情報をブロックに残し，そのブロック同士を連結しブロックチェーン参加者で共有する技術である．連結されたブロックは誰でも取得できるため，過去の取引情報を参照，確認することができる．そのため，新しく生成されるブロックに含まれる取引情報が正しいかどうかを第三者の公平な立場から確認することができる．ブロックチェーン参加者であればブロックの生成ができるが，参加者間で一意的に情報を共有する必要があるためブロックは単連結となる．そのためブロックを生成・連結する際に複数の連結候補ブロックがある場合，どのブロックを連結して共有するか決定する必要がある．どのブロックを共有するか選択肢が一つに限定されずに複数のブロックが連結された場合，ブロックが枝分かれしてユーザ間で同じ情報の共有ができずに台帳としての機能を果たせない．このように複数

の判断候補がある状況においてユーザ間で決定を共有できない問題をビザンチン将軍問題という．P2P ネットワークシステムが正常に稼働する為の必要条件として，ビザンチン将軍問題を解決できる必要があるといわれる[7]．この問題の解決のため，ブロックチェーンは複数の連結候補ブロックから一つを選ぶためにコンセンサスアルゴリズムを採用している．コンセンサスアルゴリズムとは，ある条件を満たしたユーザの生成したブロックを採用するアルゴリズムである．例えば，ビットコインが採用しているプルーフオブワーク（Proof of Work, PoW)では，計算力の大きいノードほどブロックを生成しやすい仕組みとなっている．他のコンセンサスアルゴリズムとして，Ethereum が着目している PoS（Proof of Stake, PoS）やノード間で多数決をとる Practical Byzantine Fault Tolerance（PBFT）[8]などが存在する．上記のアルゴリズムで生成される連結ブロック中のあるブロックは，そのブロックに連結されている直前ブロックの情報のハッシュを含んでいる．そのため，悪意ある参加者があるブロック情報の書き換えを行った場合，その次のブロックに含まれる前ブロックのハッシュ情報が一致しなくなるので容易に書き換えが行えない特徴を持つ．上記の理由により，ブロックチェーンでは情報の改ざんに対して耐性を持ち，一意的にネットワーク全体で情報の共有を行うことができる．

2.2 51%attack

ブロックチェーン技術を利用したプラットフォーム Ethereum は現在コンセンサスアルゴリズムとして PoW 使用しているが、将来的に PoS コンセンサスアルゴリズムの採用を試みている[9]．PoS は PoW を改善するために考案されたアルゴリズムである．PoW のブロック生成権は計算量に依存するのに対し，PoS のブロック生成は仮想通貨の所有数が影響する．PoW に有効な攻撃として 51%attack が存在する．51%attack とは，コンセンサスアルゴリズムでブロック生成権を得るための条件の全体の 51%以上を特定のグループが有すことで生成権を得てそのシステムから公平性を欠く攻撃である．例えば PoW を採用している広く知られた例として Bitcoin では，Bitcoin のブロックチェーンネットワークに参加するノードの計算力の 51%以上を特定のグループが有する場合に成立する．この攻撃への対策として，51%以上を意図的に確保することが難しいものにする方法や，51%以上保有された場合に攻撃者に得が生じないようにすることで攻撃の動機をなくすシステムを構築するなどが存在する[10]．つまり，PoS は所持する仮想通貨量がブロック生成権に関係する為，悪意ある参加者がブロック生成権を得ようとするなら，Ethereum の仮想通貨の全体の 51%以上を保有し攻撃を成立させようとする．しかし，悪意ある参加者が攻撃を成功させると，システムの信頼性が下がり，悪意ある参加者の保有する仮想通貨 51%以上の価値を下げることになる．よって，51%attack を行うことで攻撃者にとってデメリットが生じる．この仕組みが 51%attack への対策となっている．

2.3 エクリプス攻撃

エクリプス攻撃とは，P2Pネットワークにおいて攻撃対象ノードが合意形成を行う事を意図的に阻害し，ネットワークから攻撃対象ノードを切り離す攻撃である．攻撃者はP2Pネットワークで情報を伝達する際，下図1の様に攻撃対象ノードに送る情報を意図的に改竄，もしくは情報の伝達を行わないことにより，攻撃対象ノードが属していたP2Pネットワークで共有する情報とは別の情報を保有させる．攻撃対象ノードは攻撃者の恣意的な情報を受け取る為，攻撃者にとって都合の良い動作をすることになる．具体的には，攻撃対象ノードのマイニングを利用してコンセンサスアルゴリズムに対する攻撃を行う事や，支払情報の偽装を行い，仮想通貨を盗み出すことが可能となる．2015年にBitcoinがエクリプス攻撃に脆弱性を持つことがEthan Heilmanらによって指摘され[11]，2018年にはEthereumがエクリプス攻撃に対して脆弱であることがYuval marcusらによって指摘されている[12].

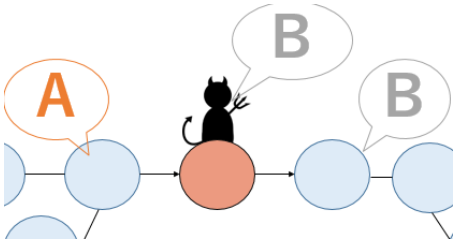

図1 エクリプス攻撃

3. 関連研究

本研究が着目するボランティアコンピューティングに関する研究は以下のようなものが存在する．

SETI@home:地球外生命体発見の為，宇宙から電波を受信し解析する研究である．カリフォルニア大学バークレー校が運営を務めて参加者 520 万人以上となり，実行性能は 769TFLOPS を達成した[13].

FightAIDS@home:AIDS 治療に見込みのある組み合わせの計算，検証を行う研究である．このプロジェクトにより，HIV プロテアーゼ阻害剤から生じた薬剤耐性株に対して有望であることを示された[14].

Folding@home:タンパク質を解析し，タンパク質に由来する疾病の治療薬を作る研究である．家庭用ゲーム機 Play Station3 でも計算に参加出来る仕組みを持つ．2007 年当時のスーパーコンピュータ，BlueGene の性能が 478TFLOPS であるのに対し，Folding@home は 1000TFLOPS を達成し，最高性能の分散コンピュータとしてギネス登録された[15].

Quake-Catcher:参加者のノート PC に内蔵されている 3 次元加速度センサーの情報をサーバに集約し，分散する参加者

の位置情報とセンサー情報から地震の震源地を特定する研究である[16].

4. 提案手法

4.1 提案手法の目的

前に述べたように, P2P ネットワークにおける分散コンピューティングでは参加者の中に悪意あるノードが紛れた場合に，悪意あるノードの答えを排除しなければならない課題が存在する．関連研究で述べた研究の多くは，この問題を冗長化と多数決によって対策としている．冗長化と多数決とは，同じ計算問題を複数ノードに配布し，各ノードが答えを返す，そのノード内で最も多い答えを解とする方法である．しかし，この方法は計算問題配られたノードの中で悪意あるノードが多数派を占めると 51%attack が成立してしまう．この点を解決するために Luis F. G. Sarmenta らは信頼度に基づいて解を一つに定める手法を提案した[16]. この手法は，同じ計算問題を複数ノードに配布し，各ノードが答えを返し，ノードの中で最も信頼度の比率が大きい答えを解とするものである．この手法により，信頼度を得ていない複数の新規ノードが誤った答えを出しても，その解を無視する事ができるようになる．

しかし, この手法では悪意あるノードが計算に参加して正しい解を出し続け，十分な信頼度を得てから誤った解を出すとその誤りを受け入れてしまう可能性がある．提案手法ではこの問題を解決する．

4.2 提案手法

新規に提案する方法では，参加者が計算に参加する場合にブロックチェーンを導入し P2P ネットワークをつくる．これにより計算に貢献したノードは計算提供者から仮想通貨が提供される仕組みを作る．仮想通貨が提供されるノード，つまり計算に貢献するノードを計算ノードと呼ぶ．

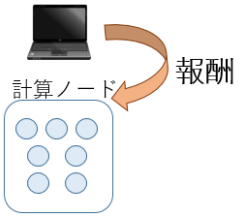

図 2　計算提供者と計算ノードの関係

参加者は計算ノードとなることで利益を得られるが，ネットワークに参加したばかりのノード，野良ノードは計算ノードにはなれない．野良ノードは計算の需要がうまれると，計算ノードが正しい計算を行っているかチェックを行う監査ノードとなる．

監査ノードは，既存の方法である冗長化と多数決と似た役割を持つ．また，監査ノードは既存研究である信頼度の仕組みを持つ．監査ノードの役割は以下の流れとなる．

1. ある計算ノードの同様の問題を複数の監査ノードに配布する．
2. 監査ノード各々で問題を解く．
3. 監査ノードらは信頼度によるコンセンサスアルゴリズムを用いて解を一意に決定する．
4. 一意に決定された解と同じ答えを出した監査ノードは信頼度が加算される．
5. 計算ノードの答えが監査ノードらの答えと異なる場合，その計算ノードは誤った答えを出したと判断する．

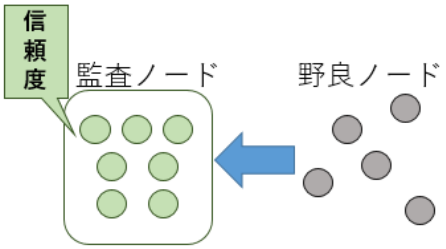

図 3　野良ノードと監査ノードの関係

上記の仕組みで計算ノードの監査を行い，信頼度を高めていくのが監査ノードの役割であり，計算提供者から報酬が与えられることはない．上記の 5 で計算ノードが誤った答えを出したと判断された場合，そのノードは即座に計算ノードから外され，野良ノードとなる．そのノードの穴埋めや，他の計算の需要ができた場合，監査ノードの中の信頼度の高いノードが計算ノードを務める．

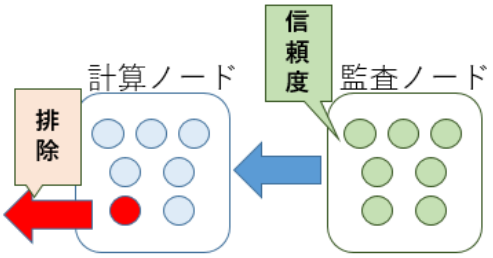

図 4　計算ノードと監査ノードの関係

この仕組みを構築することにより，悪意あるノードが計算結果を狂わせるためには，まず監査ノードから始めて監査に貢献し信頼度を稼ぐ必要がある．その後貢献を続け計算ノードになることで計算結果を狂わせることが出来ても，監査ノード群により誤りが発覚した場合は報酬も十分に貰えず計算ノードから放逐される事になる．従来の手法では，悪意あるノードは信頼度が上昇せず答えが採用されにくくなるだけでペナルティが無く，悪意あるノードが残留し溜まる可能性があったが，このシステムはその点を改善している．ペナルティを設けることで，悪意あるノード

が計算ノードになっても答えを狂わせることによるデメリットが生まれる．この攻撃により攻撃者にデメリットが生じるシステムによる耐性は，Ethereum が採用予定である PoS も試みるものである．

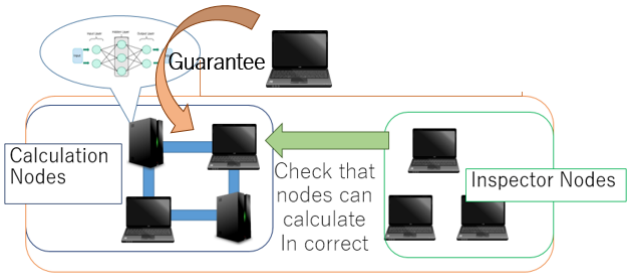

図 5　システムの全体図

5. まとめ

ボランティアコンピューティングは大規模な計算を安価に解決できる方法である．しかし，P2P ネットワークでの計算は悪意ある参加者のエクリプス攻撃などの攻撃により信頼性が得られない課題が存在する．本稿では P2P ネットワークの分散処理で得られる解の信頼性を高めるため考案された既存手法の問題点である，悪意あるノードが信頼度を高めてから計算を狂わせる攻撃への対抗として，ブロックチェーンで仮想通貨を使用した新たなフレームワークの提案を行った．

謝辞　本研究は，国立研究開発法人科学技術振興機構(JST)戦略的国際共同研究プログラム(SICORP)の支援，並びに JSPS 科研費 JP15H02711 の助成を受けたものです，ここに感謝します．

参考文献

[1] ”ビッグデータとは何か － 総務省” http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h24/html/nc121410.html(参照 2018-08-20)
[2] “ビッグデータの活用範囲 |HITACHI”http://www.hitachi.co.jp/products/it/bigdata/column/column02.html(参照 2018-08-20)
[3] ”CREST”http://research.nii.ac.jp/~uno/CREST/index.html(参照 2018-08-20)
[4]FOX, Geoffrey. Peer-to-peer networks. *Computing in Science & Engineering*, 2001, 3.3: 75-77.
[5] GHODSI, Zahra; GU, Tianyu; GARG, Siddharth. Safetynets: Verifiable execution of deep neural networks on an untrusted cloud. In: *Advances in Neural Information Processing Systems*. 2017. p. 4672-4681.
[6] Nakamoto, S., “Bitcoin: A Peer-to-Peer Electronic Cash System”, http://bitcoin.org/bitcoin.pdf, 2008.
[7] Lamport, L., Shostak, R. and Pease, M., “The Byzantine Generals Problem”, ACM Trans. Program. Lang. Syst., Vol. 4, No.3, pp.382-401, 1982.
[8] L M. Castro and B. Liskov, Practical Byzantine Fault Tolerance and Proactive Recovery, ACM Transactions on Computer Systems, v. 20 n. 4, pp. 398-461, 2002.
[9] JPBITCOIN.COM:Ethereum ＜https://jpbitcoin.com/bitcoin2/ethereum>(参照 2018-08-20)
[10] Bastiaan, Martijn. "Preventing the 51%-attack: a stochastic analysis of two phase proof of work in bitcoin." Availab le at http://referaat. cs. utwente. nl/conference/22/paper/7473/preventingthe-51-attack-astochastic-analysis-of-two-phase-proof-of-work-in-bitcoin. pdf. 2015.
[11] HEILMAN, Ethan, et al. Eclipse Attacks on Bitcoin's Peer-to-Peer Network. In: *USENIX Security Symposium*. 2015. p. 129-144.
[12]MARCUS, Yuval; HEILMAN, Ethan; GOLDBERG, Sharon. Low-Resource Eclipse Attacks on Ethereum's Peer-to-Peer Network. *IACR Cryptology ePrint Archive*, 2018, 2018: 236.
[13]ANDERSON, David P., et al. SETI@ home: an experiment in public-resource computing. *Communications of the ACM*, 2002, 45.11: 56-61.
[14] “FightAIDS@Home”http://fightaidsathome.scripps.edu/
[15] PANDE, Vijay. Folding@ home. *URL: http://www. stanford. edu/group/pandegroup/Cosm*, 2000.
[16]COCHRAN, Elizabeth S., et al. The quake-catcher network: Citizen science expanding seismic horizons. *Seismological Research Letters*, 2009, 80.1: 26-30.
[17]SARMENTA, Luis FG. Sabotage-tolerance mechanisms for volunteer computing systems. In: *Cluster Computing and the Grid, 2001. Proceedings. First IEEE/ACM International Symposium on*. IEEE, 2001. p. 337-346.