グラフクリーク探索問題に対するビットコイン・マイニングの評価

松島, 智洋
九州大学

穴田, 啓晃
長崎県立大学 : 准教授

川本, 淳平
九州大学大学院システム情報科学研究院

Bag, Samiran
Fuclty of Information Science and Electrical Engineering, Kyushu University

他

出版情報：火の国情報シンポジウム. 2016, pp.4B-2-, 2016-03-02. 電子情報通信学会九州支部
バージョン：
権利関係：

グラフクリーク探索問題に対するビットコイン・マイニングの評価

松島 智洋[1,a)]　穴田 啓晃[2,b)]　川本 淳平[1,c)]　バグ・サミラン[1,d)]　櫻井 幸一[1,e)]

概要：仮想通貨において，マイニングとは取引に関する計算困難問題の解を探索することである．仮想通貨の安全性において，マイニングを複数回行った時に要する時間の分散は小さいほうが望ましい．ところが，ビットコインはマイニングを複数回行った時に要する時間の分散が大きいという問題がある．グラフクリーク探索に基づくマイニングはオリジナルのビットコイン・マイニングに代わる新しいマイニング方法である．このマイニング手法は，要する時間の分散が小さいという特徴を持つと予想されてきたが理論的な解析が難しい．本研究では，単一の計算機がマイニングを行う場合において実際にビットコインに比べ分散が小さくなることを確認した．

Evaluation of Bitcoin-Mining for Search Problem of Graph Cliques

Tomohiro Matsushima[1,a)]　Hiroaki Anada[2,b)]　Junpei Kawamoto[1,c)]　Samiran Bag[1,d)]
Kouichi Sakurai[1,e)]

Abstract:
In cryptocurrency, mining is searching a solution of hard computation problem about transaction. In safety of cryptocurrency, it is disirable that the variance of the time to need mining several times is small. However, there is a problem in bitcoin that the variance of the time to need mining several times is large. Mining based on searching a graph clique is a new mining method instead of original bitcoin mining. It has been expected that the variance of the time to need this mining method has a characteristic to be small, but theoretical analysis is difficult. In this study, when a single computer perform mining, we confirmed that the variance is actually smaller than bitcoin.

1. はじめに

通貨を用いた取引において，取引が正当であることに対する合意の形成方法は多様化している．ビットコインの誕生以前は，全ての取引は VISA や銀行などの第三者機関を通して行わなければならなかった．一方，2009 年に考案されたビットコイン [5] はブロックチェーンとプルーフオブワークシステムを利用することによって，第三者機関無しで取引の正当性を保証する．ここでブロックチェーンとは，全取引履歴をネットワーク全体が監視するための公開台帳である．プルーフオブワークシステムとは，取引履歴がブロックチェーンに取り込まれる際に，ネットワーク上の計算機（マイナー）が計算困難問題の解を探索する（マイニングする）システムである．この解は探索という困難な作業を成し遂げた証拠となる（プルーフオブワーク）．なおかつこの解が取引履歴に関連付けられるため，取引履歴のチェーンを分岐する（仮想通貨を二重使用する）ことが困難となる．この仕組みから，プルーフオブワークシステムで取引履歴が正当であると合意することが可能となっている．なお，この解が確かに解であることの確認は，一つの計算機でも短時間で出来なければならない．

[1] 九州大学
Kyushu University
[2] 長崎県立大学
University of Nagasaki
[a)] 1SC12053G@s.kyushu-u.ac.jp
[b)] anada@sun.ac.jp
[c)] kawamoto@inf.kyushu-u.ac.jp
[d)] samiran.bag@gmail.com
[e)] sakurai@inf.kyushu-u.ac.jp

ビットコインはブロックチェーンとプルーフオブワークシステムを備えており，複数のマイナーが，報酬としてビットコインをもらえるというインセンティブの下に，一定時間毎にマイニング競争を繰り返している．本稿では，このプルーフオブワークシステムにおけるマイニング競争について考察する．

ビットコインでは，マイニングに要する時間の平均値は事前に決められている．しかし幸運な計算機が，平均値に比べて非常に短時間でマイニング出来たり，必要以上にマイニングに時間がかかると，仮想通貨ネットワークにとって，次の三つの問題が発生する [6].

(1) お金が供給される時間にばらつきが出ることによって個人的な資金計画をするのが困難である．
(2) 規則的な時間間隔で支払いが行われないため，すべてのネットワークシステムが正常に機能しているかを技術的に確かめるのが困難である．
(3) マイニングの勝者はインセンティブをもらうことができ，仮想通貨ネットワークにとって法定貨幣における造幣局のような役割を果たしているが，ネットワーク内の収入資源の分散が高いと，ネットワーク全体にストレスがかかる．

よって，仮想通貨ネットワークの安全性にとって，マイニングを複数回行ったときに要する時間のばらつきが小さいほうが望ましい．ところがオリジナルのビットコインでは，マイニングにかかる時間の分散が大きいという問題がある．

Bag らのマイニング手法 [7] では取引の情報に基づいたグラフを作成し，そのグラフにおけるクリーク探索問題を計算困難な問題として用いている．クリーク探索問題では，探索時間が長くなるにつれて単位時間あたりに探索できるグラフの範囲が広くなるという特徴を持つ．よって，クリーク探索問題を利用した Bag らのマイニング手法はオリジナルのビットコインより分散が小さいことが期待されるが，理論評価は困難であり，評価式が得られていない．

本研究では，単一の計算機によってマイニングを行うことをソロマイニングと定義し，グラフクリーク探索に基づくマイニングについて，ソロマイニングの実装評価を行う．

まず既存のビットコインのマイニングについて，ソロマイニングの理論評価を行い，実装評価によってその理論評価が正しいことを確認した．次にグラフクリーク探索に基づくマイニングの評価方法と探索アルゴリズムを提案した．最後にその探索アルゴリズムを利用して，グラフクリーク探索に基づくソロマイニングをシミュレーションし，その分散についてビットコインと比較した．

第 2 節では，本論文で用いるパラメータと記法の説明やマイニングにかかる時間の分散，その分散の測定方法について記す．第 3 節では，ビットコインのマイニングについて，アルゴリズムと理論評価，実装評価について記す．第 4 節では，グラフクリーク探索に基づくマイニングのアルゴリズムについて記す．第 5 節では，グラフクリーク探索に基づくマイニングの実装実験について，実験結果の評価方法と探索アルゴリズムの提案，実験結果について説明する．第 6 節では，本論文のまとめと今後の課題について記す．

2. 関連研究

2.1 プライムチェーンを利用した仮想通貨のマイニング

2013 年に考案されたプライムコイン [4] はプライムチェーンの探索が計算困難問題である事に着目し，それを新しいマイニング方式として利用した仮想通貨である．プライムコインのマイニングはビットコインよりも難易度調整に可塑性があり，また新しい巨大な素数の発見という数学的な利点がある．以下ではプライムコインのマイニングのアルゴリズムについて説明する．

2.1.1 プライムチェーン

p を自然数とする．オリジンを $p+1$ としたとき，$p, p+2$ がどちらも素数の時，この $p, p+2$ の組み合わせを第 1 カンニガム鎖という．また $2p+1, 2p+3$ がどちらも素数の時，この $2p+1, 2p+3$ の組み合わせを第 2 カンニガム鎖という．さらに $p, p+2, 2p+1, 2p+3$ がすべて素数の時，bi-twin chain という．オリジンを $2p+2$ として，第 2 カンニガム鎖 $4p+3, 4p+5$ であるかどうかを確かめる．このような $p, p+2, 2p+1, 2p+3, 4p+3, 4p+5, ...$ という素数からなるチェーンをプライムチェーンという．例えば 29,31,59,61 はオリジンが 30，長さ 4 のプライムチェーンである．

$p, p+2$ が素数となる組み合わせが無限に存在かどうか，またチェーンの分布はわかっていない．[2] またチェーンの長さが長くなるにつれて，そのチェーンを探す時間は指数的になる．

2.1.2 アルゴリズム

図 1 プライムコインのマイニングアルゴリズム
Fig. 1 Algorithm for primecoin mining

- 長さ $d = k + (P_k - r)/P_k$ のプライムチェーンを探す．ただし，直前に探索したプライムチェーンを $P_0, P_..., P_{k-1}$, P_k の剰余を r とする．
- チェーンの 1 番最初のオリジンがブロックヘッダーハッシュで割り切れる．
- 1 番最初のオリジンとブロックヘッダーハッシュの商が nonce となる．

プライムコインのマイニングアルゴリズムを図 1 に示す．素数であることの確認は classical Fermat test と Euler-Lagrange-Lifchitz test を使用する．一回のマイニング毎に生成されたプライムチェーンから次のマイニングの難易度（プライムチェーンの長さ）を決めるため，マイニング毎ではなく一定時間ごとに難易度調整を行うビットコインに比

べて難易度調整に可塑性があり安全性につながる．

3. 準備

本節では，本論文で用いるパラメータと記法と，マイニングにかかる時間の分散の測定方法について説明する．

3.1 パラメータと記法

本論文では，演算子 $\|$ にて文字列の連結を表す．文字列 s のハッシュ値を $H(s)$ とする．マイニングを行う人をマイナーと呼ぶ．マイニングを単一の計算機で行う場合をソロマイニング，複数の計算機で行う場合をプールドマイニングと呼ぶことにする．特に，ビットコインによって定められた方法でマイニングを行う場合をそれぞれ，ビットコインのソロマイニング，ビットコインのプールドマイニングと呼ぶ．また，グラフクリーク探索を用いて，一人あるいは複数人でマイニングを行うことをそれぞれグラフクリーク探索に基づくソロマイニング，グラフクリーク探索に基づくプルードマイニングと呼ぶ．μ_{bs} はビットコインのソロマイニングにかかる時間の期待値を表す．μ_{cs} はグラフクリークに基づくソロマイニングにかかる時間の期待値を表す．σ_{bs} はビットコインのソロマイニングにかかる時間の標準偏差を表す．σ_{cs} はグラフクリーク探索に基づくソロマイニングにかかる時間の標準偏差を表す．を表す．また，グラフクリーク探索に基づくマイニングにおいて，2 頂点同士で辺を持つ確率をエッジハッシュレートと表す．v はグラフの頂点数，r はエッジハッシュレート，c はクリークの大きさを表す．

3.2 仮想通貨におけるマイニング

本論文において，マイニングとは文献 [5] 内の取引に関する計算困難問題の解の探索のことである．以下にマイニングの概要を記す．

仮想通貨のネットワークは，タイムスタンプサーバーを持つ．タイムスタンプサーバーは，タイムスタンプされる取引情報を含んだデータをハッシュして，そのハッシュ値をネットワーク全体に放送する．そして，そのネットワークの参加者はそのデータを用いて，マイニングと呼ばれる計算競争（計算困難問題の解の探索）を行う．この時の解を nonce と呼ぶ．計算競争に勝利した参加者は，ネットワークの参加者全員に nonce を放送する．

よってマイニングとは，タイムスタンプサーバーからデータを受け取るごとにそのデータに関する計算を行い，一番最初に解（nonce）を発見した人が現れた瞬間にその計算を終了する，という試行である．厳密的には，nonce をネットワークの計算機全体に伝搬することに時間を要するが，マイニングにかかる時間に比べて非常に短いため無視できるものとする．

3.3 マイニングにかかる時間の分散の測定方法

本論文において，定性的な評価を行わず定量的な評価を行う．なぜならばグラフクリーク探索に基づくマイニングはマイニングにかかる時間の確率分布を立式できないからである．プールドマイニングの評価方法において，ソロマイニングの評価の結果に基づいてプールドマイニングの評価を決める．ソロマイニングの結果を用いるのは，実装評価もしくは理論評価によって，ソロマイニングにかかる時間の確率分布を立式することが出来れば，プールドマイニングにかかる時間の確率分布を導くことが出来るからである．本研究で測定する値は，マイニングを始めてから nonce が最初に見つかるまでの時間である．測定値を，一定時間の間に見つかる解の個数ではなく，マイニングを始めてから nonce が最初に見つかるまでの時間とした理由は以下の 2 点である．

(1) マイニングにかかる時間の分散について厳密に評価できる．
(2) グラフクリーク探索に基づくマイニングはクリーク探索をする際に，クリークの部分グラフがクリークであることを利用して枝刈りを行いながらハッシュ計算を行う．よって，探索時間の予測が立てれず，平均時間を求めることができないため，一定時間の間に見つかる解の個数を想定できない

また，本研究ではソロマイニングについての評価を行った．

4. ビットコインのマイニング

本節ではビットコインのマイニングについて，そのアルゴリズムを示す．またビットコインのソロマイニング要する時間の理論評価を行い，ソロマイニングに対して，実際に要する時間を実装評価する．

オリジナルのビットコインのマイニングのアルゴリズムを示す．マイナーはマイニングする際に，今までの全ての取引が含まれているブロックチェーンのデータと，直前のタイムスタンプから次のタイムスタンプまでの取引情報のデータを受け取る．タイムスタンプは，その取引がタイムスタンプされた時点で存在していたことを証明するためのものである．マイナーはこの 2 つの値に，nonce を連結させてハッシュ計算を行い，ハッシュ値が予め決められた値以下になる nonce を探索する．

つまりビットコインのマイニングは，今までの全ての取引が含まれたデータを B，直前のタイムスタンプからタイムスタンプされるまでの取引情報のデータを T，予め決められた値を d とすると，以下の条件式を満たす nonce を探索することである．

$$d < H(B \| T \| nonce) \tag{1}$$

一様ランダムに選択した nonce が式 (1) の条件を満足す

る確率 p は，$p = d/2^{256}$ である．3.1 の試行は条件を満たすか満たさないかであるので，この試行はベルヌーイ試行である．よって初めてこの確率 p の事象が起きるまでの試行回数の確率分布は幾何分布 [3] である．以上より，初めて nonce が見つかるまでの試行回数を確立変数 X とするとき，k 回目で初めて nonce が見つかる確率分布は $P(X = k) = p(1-p)^{k-1}$ であり，試行回数の期待値は $1/p$ 標準偏差は $\sqrt{(1-p)/p^2}$ である．単位時間あたりに 1CPU が計算するハッシュ計算回数を n とすると，初めて nonce が見つかるまでの時間を確立変数 Y とするとき，t 秒後に初めて nonce が見つかる確率分布は

$$P(Y = t) = p(1-p)^{nt-1} \tag{2}$$

である．さらに平均時間，標準偏差はそれぞれ

$$\mu_{bs} = 1/np,\ \sigma_{bs} = \sqrt{(1-pn)/p^2n^2} = \sqrt{\mu_{bs}^2 - \mu_{bs}} \tag{3}$$

である．

4.1 ビットコインのソロマイニングの実装評価

本研究では $d = 2^{228}$（$p = 1/16^7$），ソロマイニングの試行回数 800 回，B，T は乱数としてシミュレーションを行った．実装環境は表 1 の通りである．

表 1 実装環境
Table 1 experiment environment

メモリ	62.9GB
プロセッサ	Intel Core i7-3960X CPU@3.30GHz × 12
OS 種別	64 ビット
プログラム言語	Python3

結果 $\mu_{bs} \approx 538.6$，$\sigma_{bs} \approx 535.3$ となった．

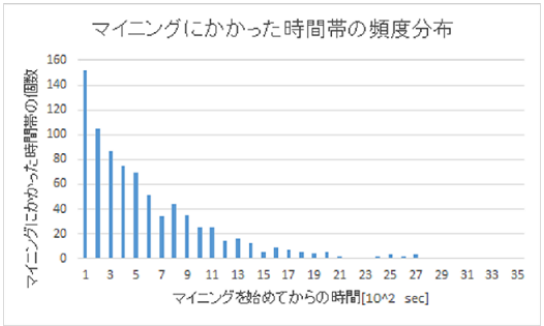

図 2 マイニングにかかった時間の頻度分布

図 2 はマイニングにかかった時間の頻度分布を表す．横軸はマイニングを始めてからの時間，縦軸はマイニングにかかった時間帯の個数を示す．実験結果は，理論評価で求めた式 (2)，式 (3) に添うことが分かる．

5. グラフクリーク探索に基づくマイニング

第 1 節より，仮想通貨のマイニング手法として利用できる問題は，計算困難問題であること，また解を発見した場合，それが解であることの確認は 1 つの計算機の計算能力でも短時間で出来るような問題でなければならない．グラフクリーク探索問題は NP 完全問題であるため，これらの条件を満たす．

5.1 グラフクリーク探索問題

グラフ理論において，無向グラフ $G = (V, E)$ のクリークとは，頂点の部分集合 $C \subseteq V$ のうち，C に属するあらゆる 2 つの頂点を繋ぐ辺が存在する場合をいう．クリークに属する頂点数をそのクリークの大きさという．与えられたグラフに指定された大きさのクリークがあるかどうかを求める問題をクリーク問題といい，NP 完全 [1] である．

5.2 アルゴリズム

文献 [7] から，頂点数 2^{30}，エッジハッシュレート r，クリークの大きさ c の場合のグラフクリーク探索に基づくマイニングのアルゴリズムを図 3 に示す．

図 3 グラフクリーク探索に基づくマイニングのアルゴリズム
Fig. 3 Algorithm for mining based on search problem of graph cliques

- マイニングするノードは，取引データ，r，c を受け取る．この取引データの個数を $T_i, 0 \leq i \leq 2^u$ とする．
- 受け取った取引のデータ，マイニングを行う人の公開鍵を用いて頂点数 2^{30} のグラフ作成する．
- 頂点が持つ値 V は，マイナーの公開鍵を P_k とすると $V = T_i \parallel P_k \parallel j, 0 \leq j \leq 2^{30-u}$ である．
- 辺を持つ条件は 2 頂点 m，n の持つ値を連結してハッシュを取った値 $H(V_m \parallel V_n)$ の先頭 s ビットが 0 であることである．$r = 2^{256-s}/2^{256}$ である．
- 大きさ $c = \frac{2 \log n}{r}$ のクリークを探索する．

6. グラフクリーク探索に基づくマイニングの実装実験

本章ではグラフクリーク探索に基づくマイニングのシミュレーション評価を行う．まず，評価の方法を決める．その後，探索アルゴリズムを 2 種類提案し，より計算時間が短いほうを比較対象として選択する．最後に実験結果を用いて，ビットコインのマイニングにかかる時間の分散と比較する．

6.1 評価方法

まず，ビットコインのソロマイニングとグラフクリーク

探索に基づくソロマイニングの分散の比較方法を述べる．式 (3) より，$\sigma_{bs} = \sqrt{\mu_{bs}^2 - \mu_{bs}}$ であるので，ビットコインのソロマイニングにかかる時間の標準偏差はビットコインのソロマイニングにかかる時間の平均時間のみによって決定する．よって，グラフクリーク探索に基づくソロマイニングにかかる時間の平均時間と標準偏差がシミュレーションによって求まると，その平均時間がビットコインのソロマイニングにかかる時間の平均時間と仮定した場合のビットコインのソロマイニングにかかる時間の標準偏差 σ_{bs} を得ることができる．つまり，測定値 μ_{cs} に対して $\mu_{bs} = \mu_{cs}$ と仮定すると，$\sigma_{bs} = \sqrt{\mu_{bs}^2 - \mu_{bs}} = \sqrt{\mu_{cs}^2 - \mu_{cs}}$ である．よってこの σ_{bs} と測定値 σ_{cs} を比較することで，グラフクリーク探索に基づくマイニングの評価が出来る．分散の小ささを表す尺度として $a = \sigma_{cs}/\sigma_{bs}$ となる a を用いる．

以上よりビットコインのソロマイニングとグラフクリーク探索に基づくソロマイニングの比較を行う際は $\mu_{bs} = \mu_{cs}$ として σ_{bs} と σ_{cs} を比較する．

6.2 実験環境

実験環境は表 1 の通りである．

本研究は以下のスケールで実験を行った．

スケール 1: $v = 2^{14}, r = 1/2^8, c = 4$

スケール 2: $v = 2^{14}, r = 3/2^7, c = 5$

6.3 探索アルゴリズムの提案手法について

実際に 5.2 節のアルゴリズムを実装する際，マイニングを行う人はインセンティブ [5] の為に，可能な限り早く解を見つけることができるようなアルゴリズムを使用することが予想される．

よって想定される 2 つの探索方法について実装比較し，平均時間が短い方法をビットコインのマイニングとの比較対象とする．

6.3.1 探索アルゴリズム A

図 4 探索アルゴリズム A の疑似コード
Fig. 4 Pseudocode of the search algorithm A

（1）頂点の値を算出する．
（2）辺の有無を確認するためにハッシュ計算 $H(V_m \parallel V_n)$ を全て行い，グラフを完成させる．
（3）大きさ c のクリークを探索する．

探索アルゴリズム A の疑似コードを図 4 に示す。実装結果は図 5 のようになった．実装環境は表 2 に従う．

6.3.2 探索アルゴリズム B

探索アルゴリズム B の疑似コードを図 6 に示す。結果は図 7 のようになった．実装環境は表 3 に従う．

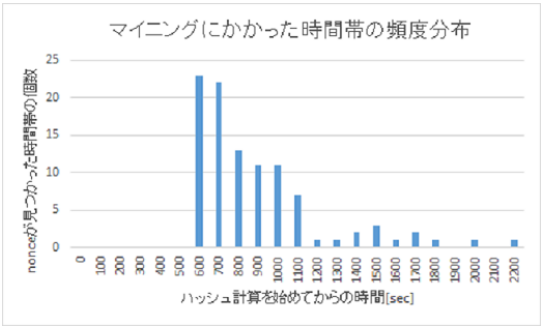

図 5 マイニングにかかった時間の頻度分布（探索アルゴリズム A）
Fig. 5 Frequency distribution of the mining time (A)

表 2 実装環境
Table 2 experiment environment

メモリ	8.00GB
プロセッサ	Intel Core i5 CPU M560 @2.67GHz 2.67GHz
OS 種別	64 ビット
プログラム言語	Python3

図 6 探索アルゴリズム B の疑似コード
Fig. 6 Pseudocode of the search algorithm B

（1）頂点の値を算出する．
（2）隣接行列と同じ大きさ v^2 の行列を確保し，要素に-1 を代入する．
（3）大きさ c のクリークを探索する．ただし辺の有無を確認する際に-1 が入っている時はハッシュ計算 $H(V_m \parallel V_n)$ を行い，0 か 1 を代入する．

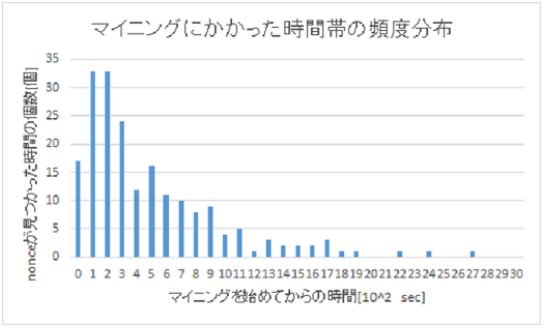

図 7 マイニングにかかった時間の頻度分布（探索アルゴリズム B）
Fig. 7 Frequency distribution of the mining time (B)

6.3.3 探索アルゴリズムの決定

$v = 2^{14}, r = 1/2^8, c = 4$，試行回数 200 回で探索アルゴリズム A と探索アルゴリズム B を比較した結果，探索アルゴリズム B の平均時間が探索アルゴリズム A の平均時

表 3 グラフクリーク探索に基づくマイニングの実装結果
Table 3 Implementation result of mining based on search for graph cliques

	スケール 1	スケール 2
V(頂点数)	2^{14}	2^{14}
r(エッジハッシュレート)	$1/2^8$	$3/2^7$
c(クリークの大きさ)	4	5
μ_{cs}	327.56[sec]	255.94[sec]
$\sqrt{\mu_{cs}^2 - \mu_{cs}}$	327.06[sec]	255.44[sec]
σ_{cs}	313.24[sec]	187.49[sec]
a	0.95722	0.73399

間 0.65 倍であったので，探索アルゴリズム B を採用する．

6.4 実験結果

実験結果を表 3 に示す．実装環境は表 5.1 に従う V(頂点数)，r(エッジハッシュレート)，c(クリークの大きさ) は実験条件，実験による測定値は μ_{cs}，σ_{cs}，a はビットコインのソロマイニングにかかる時間の分散に対するグラフクリーク探索に基づくソロマイニングにかかる時間の分散の割合を表す．

6.5 考察

実験結果より, 本研究でシミュレーションした条件（v,r,c）全てにおいて，グラフクリーク探索に基づくソロマイニングの方が標準偏差が小さくなることが分かった．また，パラメータによって a の値に幅があることが分かった．

7. まとめ

グラフクリーク探索に基づくマイニングにかかる時間の平均値は理論式を立てられず予測できないが，実験によって得られたグラフクリーク探索に基づくソロマイニングの平均時間と標準偏差からビットコインのソロマイニングと比較することができる．その結果，グラフクリーク探索に基づくソロマイニングの方が，かかる時間の標準偏差が小さくなることが分かった．プールドマイニングにかかる時間の標準偏差の評価ができていない．また標準偏差の比較 (a) にばらつきがあるが，それはどのパラメータによって決められるのか不明確である．

謝辞 本研究は JSPS-DST 日印二国間共同研究の一環である．第二著者及び第五著者に関し本研究は部分的に JSPS 科研費 15H02711 の助成を受けている．

参考文献

[1] M. R. Garey and D. S. Johnson. *Computers and intractability*, volume 29. wh freeman New York, 2002.
[2] D. Goldston. Are there infinitely many twin primes, 2009.
[3] C. M. Grinstead and J. L. Snell. *Introduction to probability*. American Mathematical Soc., 2012.
[4] S. King. Primecoin: Cryptocurrency with prime number proof-of-work, 2013.
[5] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system.
[6] M. Rosenfeld. Analysis of bitcoin pooled mining reward systems. *CoRR*, abs/1112.4980, 2011.
[7] K. S. Samiran Bag, Sushmita Ruj. On the application of clique problem for proof-of-work in cryptocurrencies.