ビットコインと待ち行列モデル

笠原　正治

ビットコインは 2008 年に Satoshi Nakamoto を名乗る人物によって考案され，2009 年に本格運用が開始された仮想通貨である．ビットコインの送金トランザクション数は年々増加し，日本でもビットコインを利用できる店舗・サービスが増加しつつある．ビットコインは送金コストがほとんどかからないといった利点がある一方，トランザクション承認に時間がかかるという欠点がある．本稿ではビットコインの仕組みを技術的観点から概観し，ユーザや協力者を巻き込んだビットコイン・エコシステム確立のもととなっているインセンティブ・メカニズムについて紹介する．次にトランザクション承認処理に焦点を当て，待ち行列理論と極値理論を用いた確率モデルによるトランザクション承認時間解析を紹介する．また，数理モデルの数値結果と実データを比較することにより，参加ノードであるマイナーの挙動について考察する．

キーワード：ビットコイン，ブロック・チェーン，トランザクション処理，集団サービス待ち行列

1. はじめに

ビットコインは Satoshi Nakamoto なる人物によって 2008 年にホワイトペーパーがインターネット上に公開され [1]，2009 年から運用が開始された仮想通貨である．クレジットカードやデビットカードのような既存のオンライン決済システムと異なり，ビットコインには管理責任[1]をもつ中央機構が存在しない．ビットコインはインターネット上で中央集中型のサーバをもたずに貨幣を実現している．

ビットコイン自体はオープンソースのソフトウェアで実現されており，ビットコインの取引（トランザクション）はすべてブロック・チェーンと呼ばれる取引台帳に記録される．ブロック・チェーンはピア・ツウ・ピア (P2P) ネットワークを通じてグローバルな公開情報として維持管理されている．

ビットコインはインターネット上の仮想通貨のために，インターネットがつながっている場所であれば世界中のどこでも瞬時に送金することができる．また，既存の決済システムと比べて送金コストがほとんどかからないという利便性を有している．そのため当初は発展途上国の出稼ぎ労働者の送金手段として需要が高まり，金融機関では取り扱いが難しい少額送金（マイクロペイメント）手段としての需要も高まってくることが予想されていた．しかしながら，近年ビットコインは投機対象として注目され，短期間での値動きが激しいために通貨としての機能を失いつつある．2018 年 3 月時点のビットコインの統計情報を表 1 に示す（表中の BTC は通貨単位としてのビットコインを表す）．

表 1　2018 年 3 月時点でのビットコイン統計情報 [2–4]

発行済ビットコイン	約 1686 万 BTC （≈ 1388 億米ドル）
参加ノード数	約 11,000
累積トランザクション数	約 2 億 9880 万
Wallet 数	約 2298 万
ブロック・チェーン・サイズ	156.0 GB
生成ブロック数	約 50 万個
取引トランザクション数/日	約 17 万 6 千
ハッシュレート	20.4 EH/s
消費電力量	48.37 TWh

H/s は単位時間当たりのハッシュ計算数を表す. EH/s は 10^{18} H/s.

ビットコインは経済学や社会科学，さらには情報科学といったさまざまな研究分野において活発に研究が展開されている．文献 [5] では，ビットコインの基本技術や歴史，危険性と規制動向に関して包括的な報告を行っている．既存の決済システムとビットコインの比較，および仮想通貨の経済的影響については [6] に詳しい．

本稿ではビットコインの仕組みを技術的観点から概観し，ユーザや協力者を巻き込んだビットコイン・エコシステムのもととなっているインセンティブ・メカニズムについて紹介する．次にビットコインのスケーラビリティに関する問題に焦点を当て，トランザクション承認時間を分析するための待ち行列理論的アプローチについて紹介する．

[1] コイン自体の発行主体はプロトコルに従うソフトウェア群であり，これらソフトウェア群全体を一つのシステムとして捉えると，システムの処理結果（アウトプット）の一つにコイン発行がある．一方で日本銀行券のような法定通貨や電子マネーと異なり，信用力を担保する法律もなければ組織も存在しない．

かさはら　しょうじ
奈良先端科学技術大学院大学
〒 630–0192　奈良県生駒市高山町 8916–5

2節ではビットコイン取引の概要，ボランティアノードが貢献しようとするインセンティブ・メカニズム，スケーラビリティ問題について紹介する． 3節ではトランザクション承認遅延の分析のための待ち行列理論的アプローチを紹介し，最後に 4 節でまとめを述べる．

2. ビットコインの概要

本節ではビットコイン取引の流れを技術的観点から要約する．なお，本節の内容は [5, 7, 8] に拠っている．

2.1 トランザクションとブロック

ビットコインシステムでは，インターネット上でトランザクションとブロックの 2 種類のデータをやりとりすることによって仮想通貨を実現している．トランザクションは送金元ユーザが送金先ユーザに送金するときの取引データで，送金元・送金先のビットコインアドレス，取引金額の情報を含んでいる．一方，ブロックは複数のトランザクションをまとめて格納したコンテナ型データであり，P2P ネットワーク上の全ノードで過去の取引記録を同期させるために用いられる．

トランザクションには送金元のアドレスが入力として，送金先のアドレスが出力として記載されている．アドレスには，楕円曲線 DSA 署名に用いる秘密鍵（アドレス保有者のみが所持）と公開鍵（一般公開）の対が紐付けされている．送金元ユーザは送金時にトランザクションに対して秘密鍵を用いて署名し，署名情報（と公開鍵そのもの）をトランザクションに埋め込むことで，なりすましや否認を防止している．

ブロックは P2P ネットワークの参加ノード群による承認手続きを経てブロック・チェーンと呼ばれる取引台帳に追加される．ブロックの承認は次節で紹介するマイニングと呼ばれる手続きを経て行われ，平均 10 分間の時間がかかる仕組みになっている．ブロック・チェーンにはビットコインサービス開始以降のすべての取引が記録されており，ビットコインの流通の一貫性を保証している．

2.2 ブロック・チェーンとマイニング

ユーザが発行したトランザクションは P2P ネットワークを通じて全参加ノードに伝搬され，マイナー（Miner：採掘者）と呼ばれるボランティア・ノードのメモリ上に一時的に蓄積される．新規ブロックの構成には，そのブロックに含められるトランザクション情報，直前ブロックのもつハッシュ値，およびナンス (nounce) と呼ばれる文字列，の 3 点の情報を必要とする．この三つの情報をハッシュ関数に入力したときの出力文字列が，整数とみなしたときにある値以下になるようなナンスを見つけるというのがマイニングである[2]．直前ブロックのハッシュ値を次ブロックに含めることで，ブロックの改ざんを試みる者は，後続ブロックのハッシュ値をすべて再計算しなければならない．改ざんを防ぐこの仕組みを proof-of-work と呼ぶ．

マイニングに勝利したマイナーが新規ブロックをブロック・チェーンに登録し，ビットコインシステムから報酬を獲得する．ブロックにはユーザから発行されたトランザクションとは別に coinbase と呼ばれる勝利マイナーへの報酬支払い用トランザクションが用意されている．2018 年 3 月時点での 1 ブロック当たりの報酬は 12.5 ビットコイン（日本円で約 1 千万円）である．報酬額は 21 万ブロックごとに半減するよう設定されており，1 ブロックのマイニングには平均 10 分間かかることから，報酬額は約 4 年ごとに半減する計算になる．パズル的問題の難易度は，承認時間間隔が平均 10 分間となるようにシステムが自動的に調整する．

マイニングに勝利するマイナーは必ずしも一人とは限らない．仮に二人のマイナーがほぼ同時にナンスを発見することができた場合，二つのブロックは分岐（フォーク）する形でブロック・チェーンに登録される．これ以降は個々の分岐チェーンで独自にブロックが登録されることになるが，分岐したチェーンの一つがある数以上のブロックを登録したとき，長いチェーンが正当と判断され，以降は長いほうのチェーンのみにブロックが登録されるようになる[3]．ビットコインでは，計算パワーをより多くかけることにより，悪意をもつユーザからの不正行為を防ぐ構造となっており，長いチェーンのほうが短いチェーンよりも多くの計算パワーをかけているという観点から，長い分岐チェーンを選択する仕組みとなっている．

2.3 不正な取引に対する頑健性

電子マネーの代表的な不正取引は，取引情報の改ざんと二重使用である．ビットコインでは，ブロックチェーン自体がこれらの不正取引を防ぐ役割を担っている [9]．

攻撃者がビットコインで取引情報を改ざんしようとする場合，過去に登録されたブロック中のトランザクションを書き換えなければならない．この場合，フォー

[2] 2018 年 3 月現在，16 進数のハッシュ関数出力文字列の先頭 18 個がすべて 0 になるレベルの難易度になっている．16 進数で 1 文字が 0 になる確率は 1/16，18 個の 0 が並ぶ確率は $(1/16)^{18} \approx 2.118 \times 10^{-22}$，約 212 垓（がい）分の 1 程度である．

[3] 約 5〜6 個のブロックが接続された分岐のほうが正当とみなされる．そのため，トランザクションの承認確定は約 1 時間後である．

クによって枝分かれが発生し，攻撃者は改ざんしたブロック側の枝を伸ばすべく，マイニングに勝ち続ける必要がある．しかしながら，もし別のマイナーが勝利すると正しいブロックがつながっている枝のほうを伸ばしてしまうことになる．つまり，攻撃者が勝ち続けることは計算コスト的にハードルが極めて高く，それだけの計算パワーを改ざんに向けるよりもマイニングに参加して成功報酬を得るほうが得策になる[4]．

一方で，コインの二重使用に対しては，ブロックチェーン自体が過去の全取引を記録した取引台帳となっており，P2P ネットワークに参加している全ノードが新規トランザクションが正当な取引かどうかを確認するようになっている．このため，二重使用のトランザクションは入金・出金の履歴から直ちに検出される構造となっている．

2.4 インセンティブ・メカニズム

ビットコインでは，マイナーによるくじ引き競争（マイニング）が取引の一意性を保証するためには欠かせない．マイナーがくじ引き競争に参加する最大の動機は coinbase と呼ばれる成功報酬の獲得である．2009 年のサービス開始時点の成功報酬は 50 BTC であったが，前述したとおり約 4 年ごとに成功報酬は半減する仕組みになっており，執筆時点（2018 年 3 月）での成功報酬は 12.5 BTC（約 1 千万円）である．成功報酬がある値[5]を下回ると新規発行が行われなくなる仕様になっており，このため，ビットコインの発行上限数は約 2100 万 BTC であり，22 世紀中頃に新規コインの採掘が終了する見込みである．このことは，将来的にはマイナーの貢献意欲を低下させ，ブロックチェーンのセキュリティが脆弱になることを意味している．

くじ引き競争に勝利したマイナーに与える別の報酬として，トランザクションに付随する手数料 (transaction fee) がある．手数料の設定はオプションであるが，現在出回っているソフトウェアでは 0.0001 BTC の手数料がデフォルトとして設定されている[6]．文献 [10] による参照実装では，手数料が高いトランザクションほど優先的に新規ブロックに取り込まれるようになっている．文献 [11] では 5 千万件以上のトランザクションから支払われた手数料の傾向を分析し，手数料が払われていないトランザクションは手数料を払っているトランザクションよりも承認時間が長い傾向にあること，および支払われた手数料の多さがトランザクション承認時間に与える影響は特に見られないこと，などを明らかにした．

将来的に成功報酬が減額していくと，手数料がマイニングのインセンティブになることが予想される．利用者側の観点からすると，高額送金には手数料を高く払うという動機が働く一方，小額なやりとりには手数料をあまり払いたくない，と考えるのが自然である．将来的にマイクロペイメントの需要が増大すると，承認処理中のブロックに含まれない未処理トランザクション数が増大し，特に低額送金のトランザクションの承認処理遅延が増大することが予想される．一方，成功報酬が減額されていくとマイナーの貢献意欲が下がり，ビットコイン自体のセキュリティが脆弱化する恐れもある．そのため，マイナーに対する貢献意欲をどのように高めるかがビットコインの存続に欠かせない問題となっている．

2.5 スケーラビリティの問題

ビットコインでは，ブロックサイズの上限は 1 Mbyte と定められている [12]．トランザクションの平均サイズは約 500〜600 byte であることから，1 ブロック当たりおよそ 1,600〜2,000 個のトランザクションしか格納することができない．これに加えてマイニング処理で新規ブロックが生成されるまでに平均 10 分間かかることから，1 秒当たり約 3 個のトランザクションしか処理できない．ビットコインは世界中で使われる通貨としては処理能力が極めて低いということがわかる．

ビットコインの開発コミュニティでは，ブロックサイズを大きくしたり，署名部分を簡素化してトランザクションのデータサイズを小さくする，といった方策が議論されているが [13, 14]，コミュニティ全体で合意に達していないこともあり，抜本的な改良には至っていない．

3. 待ち行列理論によるトランザクション承認時間の分析

前節で見てきたように，ビットコインのトランザクションは手数料による優先的取り扱いや，1 Mbyte というブロックサイズの上限に起因する低い処理能力の影響を受けるために，承認までにかかる時間を定量的に評価することが重要となる．ここでは文献 [15] のビットコインのトランザクション処理を表す基本的な集団サービス待ち行列モデル，および新規ブロックが生成

[4] 悪意のマイナーが 50%を超えて存在するようになると，このメカニズムが破綻する（51%アタックと呼ばれている）．
[5] 0.00000001 BTC，1 satoshi と呼ばれる最小単位を下回るとコイン発行が停止する．
[6] 2014 年の一年間で取引されたトランザクションのうち，97%のトランザクションは 0.0001 BTC の手数料を払っていた [5].

される時間間隔を分析する確率モデルを紹介する．

3.1 トランザクション処理の待ち行列モデル

ユーザからのトランザクションは率 λ のポアソン過程に従って発生すると仮定する．複数のトランザクションは一つのブロックを構成し，ブロックはマイニングが終了した時点でブロック・チェーンに登録される．トランザクションを待ち行列に到着する客と捉えると，ブロックの生成間隔はその客のサービス時間に相当する．j 番目のブロックの生成間隔を S_j で表し，S_j は独立同一な一般分布 $G(x)$ に従うものと仮定する．また，$G(x)$ の密度関数を $g(x)$ とする．

ブロックには 1 個以上 b 個以下のトランザクションを含めることができる．系に到着したトランザクションは現在マイニング中のブロックに空きがある場合，そのブロックに格納され，空きがない場合には待合室であるマイニングプールで待機する．待合室の容量は無限大と仮定する．

上記の仮定より，トランザクション処理過程は集団サービスをもつ $\mathrm{M/G}^b/1$ 待ち行列モデルとなる．今，時刻 t における系内トランザクション数を $N(t)$，経過サービス時間を $X(t)$ とする．また，$P_n(x,t)$ $(x,t\geq 0,$ $n=1,2,\ldots)$ と $P_0(t)$ を次式で定義する．

$$P_n(x,t)\mathrm{d}x=\Pr\{N(t)=n, x<X(t)\leq x+\mathrm{d}x\},$$
$$P_0(t)=\Pr\{N(t)=0\}.$$

$P_n(x,t)\mathrm{d}x$ は時刻 t で系内トランザクション数が n，経過サービス時間が x である結合確率を表している．これに対して以下の極限確率を定義する．

$$P_n(x)=\lim_{t\to\infty}P_n(x,t),\quad P_0=\lim_{t\to\infty}P_0(t).$$

また，サービス時間 S に対するハザード率を $\xi(x)$ とすると，$\xi(x)$ は次式で与えられる．

$$\xi(x)=\frac{g(x)}{1-G(x)}.$$

$E[S]$ を S の期待値とし，$\lambda E[S]<b$ の成立を仮定すると，系は安定で極限

$$P_n(x)=\lim_{t\to\infty}P_n(x,t),\quad P_0=\lim_{t\to\infty}P_0(t),$$

が存在し，次の微分差分方程式を得る．

$$\lambda P_0=\sum_{k=1}^{b}\int_0^\infty P_k(x)\xi(x)\mathrm{d}x,$$

$$\frac{\mathrm{d}}{\mathrm{d}x}P_n(x)=-\{\lambda+\xi(x)\}P_n(x)+\lambda P_{n-1}(x),\quad (1)$$
$$n=2,3,\ldots,$$

$$\frac{\mathrm{d}}{\mathrm{d}x}P_1(x)=-\{\lambda+\xi(x)\}P_1(x).\quad (2)$$

また，境界条件として次式を得る．

$$P_n(0)=\int_0^\infty P_{n+b}(x)\xi(x)\mathrm{d}x,\quad n=2,3,\ldots,\quad (3)$$

$$P_1(0)=\int_0^\infty P_{1+b}(x)\xi(x)\mathrm{d}x+\lambda P_0.\quad (4)$$

さらに正規化条件は次式で与えられる．

$$P_0+\sum_{n=1}^{\infty}\int_0^\infty P_n(x)\mathrm{d}x=1.$$

ここで確率母関数

$$P(z;x)=\sum_{n=1}^{\infty}P_n(x)z^n,$$
$$P(z)=P_0+\int_0^\infty P(z;x)\mathrm{d}x,$$

を定義すると，(1) 式と (2) 式より

$$\frac{\mathrm{d}}{\mathrm{d}x}P(z;x)=-\{\lambda+\xi(x)-\lambda z\}P(z;x),$$

が得られ，$P(z;x)$ について次式を得る．

$$P(z;x)=P(z;0)\{1-G(x)\}\exp\{-\lambda(1-z)x\}.\quad (5)$$

(3) 式と (4) 式の境界条件より，$P(z;0)$ は次式で与えられる．

$$P(z;0)=\frac{\sum_{k=1}^{b}\alpha_k(z^{b+1}-z^k)}{z^b-G^*(\lambda-\lambda z)}.\quad (6)$$

ここで $G^*(s)$ は $G(x)$ のラプラス・スティルチェス変換

$$G^*(s)=\int_0^\infty e^{-sx}\mathrm{d}G(x),$$

であり，

$$\alpha_k=\int_0^\infty P_k(x)\xi(x)\mathrm{d}x,$$

とおいた．(5) 式と (6) 式より，最終的に

$$P(z)=\frac{1}{\lambda}\sum_{k=1}^{b}\alpha_k+\frac{\sum_{k=1}^{b}(z^{b+1}-z^k)\alpha_k}{z^b-G^*(\lambda-\lambda z)}$$
$$\times\frac{1-G^*(\lambda-\lambda z)}{\lambda-\lambda z},\quad (7)$$

を得る．トランザクションの系内滞在時間を T とすると，$E[T]$ は (7) 式とリトルの公式より求めることができる．

3.2 ブロック生成間隔の分布

サービス時間であるブロック生成間隔の分布 $G(x)$ について，文献 [16] では，莫大な数のナンスから条件

に合うナンスを見つける行為を成功確率が極めて小さいベルヌイ試行と考え，ブロック生成間隔を独立同一な指数分布と推測していた．

実際のマイニングにおいては，ブロックヘッダに含まれるナンスのフィールド（4 バイト），および coinbase トランザクションのエキストラ・ナンス・フィールド（8 バイト）の合計 12 バイトからなるビット列の値を変更してハッシュ計算を行うことが繰り返されている [7]．ナンスの探索は 2^{96} の莫大な探索空間で行われているが，現在は複数のマイナーノードが協力して探索空間を分割して探索するマイニング手法が主流である．この状況は，有限個のくじから当たりくじを引く行為とみなすことができる．

今，均一な性能をもつ n 台のマイナー・ノードがマイニングを行っている状況を考える．各マイナーは m 枚中 1 枚の当たりが入っているくじ引きを行う．i 回目に当たりを引く確率は離散一様分布 $1/m$ で与えられることに注意する．以下では，マイナー k $(k = 1, \ldots, n)$ が当たりくじを引くまでの時間 Y_k が独立同一で連続的な一様分布 $U(0, m)$ に従うものと仮定する．

$$\Pr\{Y_k \le x\} = \begin{cases} x/m, & 0 \le x \le m, \\ 0, & \text{その他.} \end{cases}$$

ブロックの生成は，n 台のマイナーのうち，一番最初に当たりくじ（ナンス）を見つけた時点で生成される．ブロックの生成間隔を Z_n とすると，$Z_n = \min\{Y_1, \ldots, Y_n\}$ であり，分布は次式で与えられる．

$$\begin{aligned} \Pr\{Z_n \le x\} &= \Pr\{\min(Y_1, \ldots, Y_n) \le x\} \\ &= 1 - \Pr\{\min(Y_1, \ldots, Y_n) > x\} \\ &= 1 - \left(1 - \frac{x}{m}\right)^n. \end{aligned}$$

ここで Z_n が従う極値分布を考える（極値理論の解説と情報システム分析への応用については [17] を参照）．Z_n を正規化した $\Pr\{(Z_n - \beta_n)/\alpha_n \le z\}$ に対し，$\alpha_n = 1/n, \beta_n = 0$ とすれば，$0 \le z \le n$ に対して

$$\begin{aligned} \Pr\left\{\frac{Z_n - \beta_n}{\alpha_n} \le z\right\} &= 1 - \left\{1 - \frac{(z/m)}{n}\right\}^n \\ &\to 1 - e^{-z/m}, \quad n \to \infty. \end{aligned}$$

すなわちワイブル分布の特殊型である指数分布が得られる．これより，n が非常に大きいところでは

$$\Pr\{Y_n \le x\} \approx 1 - \exp\{-(n/m)x\},$$

すなわちパラメータ n/m をもつ指数分布で近似できることが予想される．

われわれは過去の研究 [15] において，2013 年から 2015 年の 2 年間におけるブロック・チェーンのブロック情報とトランザクション情報を解析し，ブロック生成間隔が指数分布に従うことを確認した．

3.3 過去の研究成果

3.3.1 優先権付き M/G^b/1

われわれは [15] において，手数料がトランザクション承認時間に与える影響について分析を行った．具体的には，3.1 節で紹介した M/G^b/1 モデルをもとに，トランザクションに対する優先権制御を考慮したモデルを考え，各優先権クラスに属するトランザクションの平均承認時間を導出し，2013 年から 2015 年の 2 年間におけるトランザクション承認時間の平均と比較を行った．その結果，優先権を考慮しない場合の平均トランザクション承認時間について，実データに基づく平均承認時間は約 19 分，解析モデルでは約 9 分と，2 倍近く差のある結果が得られた．解析モデルでは，新規トランザクションが到着した時点でサービス中のブロックに空きがある場合，そのトランザクションはブロックに取り込まれる，ということを仮定していた．実際のマイニングでは，新規トランザクションはサービス中のブロックに空きがあっても取り込まれることなく，次以降のブロック構築に後回しされる，ということが推測される．

また，優先権付きモデルに対しては，手数料が 0.0001 BTC 以上のトランザクションを高優先クラス，0.0001 BTC 未満の手数料をもつトランザクションを低優先クラスとして，理論値と実データを比較した．その結果，実データより算出した低優先トランザクションの平均承認時間が 1 時間以上，理論値（約 11 分）よりも著しく大きいということが判明した．これより実際のマイニングでは，マイナー・ノードは手数料の少ないトランザクションを意図的にブロックに取り込まないことを行っていることが推測される．

3.3.2 優先権付き M/G^b/1 の修正モデル

[15] で推測されたマイニングの挙動を取り込むため，[18, 19] では，新規トランザクションは現在サービス中のブロックに含められず，その次以降のブロックに含められるという，遊休期間をもつゲート式サービスの待ち行列モデルを検討した．数値例より，改良モデルの平均トランザクション承認時間は約 19 分，実データとの差は約 12 秒と，かなり良好な値を得ることができた．その一方で，ブロックに含められるトランザクション数を変化させて理論モデルの妥当性を検討したところ，ブロック・サイズが小さいところでは理論

値とトレース駆動型シミュレーションとで大きな乖離が見られた．これは，実際のトランザクションの到着間隔の変動がポアソン過程よりも大きいことに起因することが考えられる．

3.3.3 到着過程を一般化した待ち行列モデル

前節までの待ち行列モデルでは，トランザクションの到着をポアソン過程と仮定していたが，実データの分析より，到着間隔の変動が指数分布よりも大きいことが判明した．この結果を受けて，われわれは [20] で到着過程の一般化を試みた．具体的には，トランザクションの到着間隔を独立同一な一般分布に従う集団サービス待ち行列 $GI/M^b/1$ を考え，行列解析法によりトランザクションの平均承認時間を導出した．数値例では，トランザクション到着間隔を超指数分布と仮定し，EM アルゴリズムによるパラメータ推定を行ったところ．推定された分布の平均値は実データのものと一致し，2 次モーメントについても良好な精度で一致していることを確認した．この推定分布をもとに平均トランザクション承認時間を計算し，トレース駆動型シミュレーションと比較してみたが，理論値と実データとで乖離が観察された．このことは，トランザクション到着間隔が独立同一な超指数分布では適切にモデル化できないことを示唆している．

4. まとめ

本稿ではビットコインの仕組みを技術的な観点から概観し，マイクロペイメントの需要増大や成功報酬の減額がビットコインの持続的発展において大きな課題となっていることを紹介した．次にトランザクション承認時間を分析するための待ち行列理論的アプローチについて，過去に得られた研究成果を中心に紹介した．理論値と実データとの比較検証により，新規トランザクションはマイニング中のブロックには含められないこと，マイナー・ノードは低い手数料のトランザクションを故意にブロックに含めていないことなど，待ち行列モデルをもとに実際のビットコイン・マイニングの一面を明らかにできたことは大きな収穫であったと考えている．現在ビットコインに代わる新しい仮想通貨やスマートコントラクトの枠組み [21] が活発に研究開発され，マイニング時間短縮に向けた合意形成アルゴリズムや成功報酬の与え方の工夫など，興味深いトピックが生まれてきており，性能予測や挙動理解に対する数理的分析研究がますます重要となってきている．

謝辞 関西学院大学教授・三道弘明氏には通貨発行の原則について貴重なコメントをいただいた．記して感謝の意を表する．本研究の一部は JSPS 科研費 15H04008 の支援を受けて実施している．

参考文献

[1] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” https://bitcoin.org/bitcoin.pdf（2018 年 6 月 8 日閲覧）
[2] https://blockchain.info/（2018 年 6 月 8 日閲覧）
[3] https://charts.bitcoin.com/（2018 年 6 月 8 日閲覧）
[4] https://bitnodes.earn.com/（2018 年 6 月 8 日閲覧）
[5] R. Böhme, N. Christin, B. Edelman and T. Moore, “Bitcoin: Economics, technology, and governance,” *Journal of Economic Perspectives*, **29**, pp. 213–238, 2015.
[6] 野口悠紀雄，『仮想通貨革命』，ダイヤモンド社，2014.
[7] A. M. Antonopoulos, *Mastering Bitcoin*, O’Reilly, 2014.
[8] F. Tschorsch and B. Scheuermann, “Bitcoin and beyond: A technical survey on decentralized digital currencies,” *IEEE Communications Surveys & Tutorials*, **18**, pp. 2084–2123, 2016.
[9] 山崎重一郎，“仮想通貨の技術的イノベーションと課題，” 電子情報通信学会ソサイエティ大会講演論文集，AK-2-1, 2014.
[10] https://en.bitcoin.it/wiki/Transaction_fees（2018 年 6 月 8 日閲覧）
[11] M. Möser and R. Böhome, “Trends, tips, tolls: A longitudinal study of Bitcoin transaction fees,” Lecture Notes, The 2nd Workshop on BITCOIN Research, 2015.
[12] https://en.bitcoin.it/wiki/Scalability（2018 年 6 月 8 日閲覧）
[13] http://www.coindesk.com/segregated-witness-bitcoin-block-size-debate/（2018 年 6 月 8 日閲覧）
[14] https://www.coindesk.com/segwits-slow-rollout-bitcoins-capacity-hasnt-seen-sudden-boost/endthebibliography（2018 年 6 月 8 日閲覧）
[15] S. Kasahara and J. Kawahara, “Effect of Bitcoin fee on transaction-confirmation process,” *Journal of Industrial and Management Optimization*, arXiv: 1604.00103
[16] J. Göbel, H. P. Keeler, A. E. Krzesinski and P. G. Taylor, “Bitcoin blockchain dynamics: The selfish-mine strategy in the presence of propagation delay,” *Performance Evaluation*, **104**, pp. 23–41, 2016.
[17] 笠原正治，“極値理論と情報システム評価への応用，” 電子情報通信学会誌，**100**, pp. 266–272, 2017.
[18] Y. Kawase and S. Kasahara, “Transaction-confirmation time for Bitcoin: A queueing analytical approach to blockchain mechanism,” In *Proceedings of the 12th International Conference on Queueing Theory and Network Applications (QTNA2017)*, pp. 75–88, 2017.
[19] Y. Kawase and S. Kasahara, “Priority queueing analysis of transaction-confirmation time for Bitcoin blockchain,” *Journal of Industrial and Management Optimization*, to appear.
[20] 河瀬良亮，笠原正治，“$GI/M^b/1$ モデルによるビットコイン・トランザクション承認時間解析，” 待ち行列シンポジウム「確率モデルとその応用」，pp. 109–118, 2018.
[21] Etherem Project, https://www.ethereum.org/（2018 年 6 月 8 日閲覧）