利己的マイニングと分岐（フォーク）について

相　模　裕　一

序

2008年，Satoshi Nakamoto の論文［12］により登場したビットコイン（BTC）は，2009年１月９日に Nakamoto 自身によってネット上でリリースされ（Bitcoin v0.1 released），当初１BTC は0.07円の価値であったが，その後市場価値はブームと急落を繰り返しながら拡大している。現在2024年11月17日の時点では１BTC＝14,034,880円と1400万円を超え，その市場規模も1800億ドル（27兆円）と成長している。しかしこのビットコインの発行条件枚数は2100万枚と決められており，既に2000万枚近く発行済みなので発行上限に達する日は遠くない。こうした実体の無い暗号資産のビットコインが持続的に高騰するとは考え難く，いつ暴落してもおかしくない。ビットコインはもはや通貨ではなく投機対象の資産と言えよう。

Nakamoto の論文［12］の真の貢献はビットコインの生成よりもビットコイン取引の実行を支えているブロックチェーンの構築を示したことにある。このブロックチェーンは，たとえビットコインが消滅しても今後も発展・拡充が期待される革新的技術である。

本論文ではこのブロックチェーンの持続・拡大の要である連結作業について分析をおこなう。連結作業は参加者の承認過程（コンセンサス・アルゴリズム）であり，Proof of Work，Proof of Stake，Delegated Proof of Stake，Proof of Importance などが有名であるが，ここではビットコインで採用されている Proof

of Work について，特に２種類のマイニングについてモデル分析を行う。すなわち Nakamoto のプロトコルに従う正直なマイナーとプロトコルを無視する利己的なマイナーによるマイニングについてである。

本論文の構成は以下の通りである。まず１節では，ブロックチェーンの構造と Proof of Work について，特にそのマイニングの仕組みとブロック生成・連結過程について詳述する。２節では Nakamoto プロトコルに従うマイナーの行動についてモデル分析を行い，最適化行動として期待利潤の最大化をもたらすハッシュパワーを求める。３節では利己的マイニングによるブロックチェーンの分岐（フォーク）について論じ，４節では利己的マイナーの最適化行動を分析し，私的分岐の最適ブロック数を求める。また分岐を制限する条件についても検討を行う。そして最後の５節ではまとめと今後の課題について触れる。

1　ブロックチェーンの構造と Proof of Work

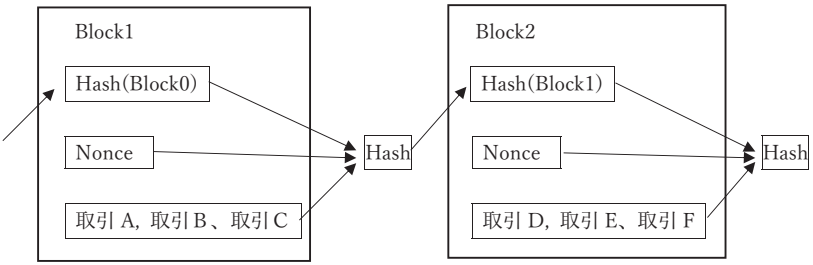
ブロックチェーンは第三者機関（銀行・政府等）の介在なしに直接ユーザー（ノード）間で取引が実行される P2P 型分散型台帳のネットワークシステムである。第三者機関の認証・制御無しに自律的に作動し，匿名性が高く改竄が極めて困難であることを特徴としている。

Nakamoto の論文で示されたブロックチェーンは，Satoshi Nakamoto が独自に考案したのではなく，これまで発表された様々なアイデアを巧みに統合して，現実に実行可能なプラットフォームとしたものである。まず，ブロックチェーンの原型は既に1991年の Haber and Stornetta の論文［５］で提示されていた。彼らは文書データのハッシュ値を求め，タイムスタンプを付して保存する方法を考案していた。ブロックチェーン上では，各ブロック間の連結が重要であり，ビットコインの場合はこの連結作業をマイナーの Proof of Work によって行っている。Proof of Work とは数値計算による演算証明（課題の解法）であり，膨大な計算量が要求される作業である。各ブロックには前のブロックのハッシュ値がヘッダーに組み込まれているため，ある時点 t の文書 Dt の改竄を試みるならば，それ以降のすべてのブロックが連結不整合となり改竄が発覚する。

そのため改竄者は自ら Proof of Work を行い新たなナンス（Nonce）を見出し，時点 t 以降の全てのブロックについて膨大な計算をしなければならない。

この Proof of Work というコンセンサスアルゴリズムのアイデアは，1992年の Cynthia Dwork and Moni Naor のジャンクメール排除の論文［３］で示されており，その後1999年 Jakobsson and Juels［７］，2002年 A. Back［１］で展開されたものである。ビットコインの基本構造は，デジタルタイムスタンプによる分散型台帳に Proof of Work と暗号技術（公開鍵と秘密鍵）を組み合わせたものである。それぞれ別の目的のために考案されたアイデアがブロックチェーンとなり，広く認知されるようになったのである。

では，Proof of Work で行われる演算証明マイニングとはどのようなものであろうか。次の図を用いて説明しよう。



上の図の Block1 には１個前の Block0 のハッシュ値と，取引情報 ｛取引 A，取引 B，取引 C｝，そしてナンス（Nonce）が入っている。この３つの情報をハッシュ関数に入力したときの出力値がある値以下になるようにナンスを見つけるというのがマイニングである。具体的には新たなハッシュ値が256桁（16進数ならば64桁）で最初の16桁（18桁の場合もある）が０となるように32ビットのナンスを求めるという課題である。求めるナンスを X とし，Hash（・）をハッシュ関数として表すと Hash（Hash（Block0），取引情報，X）＜0000……***** となる。記号を用いて記述するならば以下のようになる。

$$B_i = [H[B_{i-1}], N_i, H[T_i]] \quad \cdots\cdots\cdots (1)$$

ここで B_i を i 期のブロック，H[]をハッシュ関数，T_i は i 期の取引である。

$$H[B_i] = H[H[B_{i-1}], N_i, H[T_i]] < 2^{256}/D \quad \cdots\cdots\cdots(2)$$

D を難度として，D≒$10^{22.9}$ を想定している。Proof of Work の演算証明とは，(2)の式が成立する N（ナンス）を見つけることである。

ハッシュ関数は一方向の関数である。入力変数を１数，１文字の変化させると，出力される値は不連続に全く別の値になる。１万桁の数も１桁の数も出力値は同じ256桁である。またハッシュ関数には逆関数は存在しない。それゆえ出力値から入力値を求めるには，総当たりで片っ端から数値代入を行うこととなる。ハッシュ値が16進数の場合，16個の０の並ぶ確率は（1/16）[16]となり，ほとんど確率０である。マイナーには膨大な計算が課されるのである。直前の Block のハッシュ値が次の Block に組み込まれているので，取引情報の改竄を試みる者は，後続の Block のハッシュ値を全て計算するというペナルティーが課され不正防止となっている。

演算課題の難易度は，Proof of Work による承認時間が平均10分になるように調整されている。もし10分以内で作業が終わる場合は，０の桁が18個に増やされ難易度が上がるようになっている。各マイナーは同程度の機能を持つ計算マシーンで作業をしているので，二人のマイナーがほぼ同時にナンスを発見する場合がある。このとき，ブロックは分岐（フォーク）する形でブロックチェーンが形成される。これ以降は，個々の分岐したチェーンが独自にブロックを連結されていくことになる。５～６個のブロックが接続され長くなった分岐の方が正当とされる。それは，長いチェーンの方が短いチェーンよりも不正行為を防ぐ効果があるからだ。悪意の不正者は短いチェーンよりも長いチェーンの方がより多くの困難な計算を強いられ難易度が上がるようになっている。悪意の不正者は１つのノード（PC など）での修正ではなく，全ノードの半数を超える修正をおこなうことになる。10分間という限られた時間での作業であることから，不正は絶望的な行為となる。次節では，マイニングを行うマイナーの最適化行動について分析をおこなう。

２　マイニング・モデル

この節ではマイナーの最適化行動を定式化し，最適ハッシュパワーを求めよう。ここで分析するマイナーは Nakamoto プロトコルに従ってマイニングを行うマイナーである。プロトコルを無視するマイナーについては３節で分析する。今，マイナーの数を $m(\in N)$ として，マイナー $i \in \{1,2,3,\cdots m\}$ のハッシュパワーを $H_i \in R_+$ とする。マイナー i が最初に演算課題に適合的なハッシュ値をもたらすナンスを見出す確率を以下のように記す。$i \gg j$，$i \neq j$，$i,j \in \{1,2,3,\cdots m\}$ は i が一番先にナンスを見つける状況を表す。

$$Pr(i \gg j) = \frac{H_i}{\sum_{i=1}^{m} H_i}$$

また，マイナー $j(\neq i)$ が最初にナンスを見つける場合の確率は以下のようになる。

$$Pr(j \gg i) = \frac{\sum_{j \neq i} H_j}{\sum_{i=1}^{m} H_i}$$

ここでマイナー i が受け取るリターン（報酬）を R，暗号資産の価格を p とすると，

$$R = \alpha p$$

ビットコインの場合，α は４年ごとに半減し，2024年では $\alpha = 3.125$ である。マイナー i の費用関数を以下のように表す。

$$C_i(H_i) = c_i H_i + C_F$$

ここで c_i を限界費用，C_F を固定費用とする。マイナーの期待利潤 $E\pi$ は以下のようになる。

$$\begin{aligned} E\pi_i &= Pr(i \gg j)\big(R - C_i(H_i)\big) - Pr(j \gg i) C_i(H_i) \\ &= \frac{H_i}{\sum_{i=1}^{m} H_i} R - C_i(H_i) \qquad i \in \{1,2,3,\ldots m\} \end{aligned}$$

期待利潤の最大化により，

$$\frac{\sum_{j\neq i} H_j}{\left(\sum_{i=1}^{m} H_i\right)^2}\alpha p = c_i \quad \cdots\cdots\cdots(3)$$

ここで，各マイナーのハッシュパワーを同じと仮定しよう。$H_i = H_j = H$
(3)より，

$$\frac{(m-1)H}{(mH)^2}\,\alpha p = c_i \quad \cdots\cdots\cdots(4)$$

これより，マイナー i の最適ハッシュパワー H^*は以下の式で表される。

$$H^* = \frac{m-1}{m^2}\cdot\frac{\alpha p}{c_i} \quad \cdots\cdots\cdots(5)$$

(5)より，最適ハッシュパワーはマイナーの増加と限界費用の上昇により低下し，暗号資産価格の上昇により，増加することが分かる。（ビットコインの場合，α は４年ごとに半減するので，４年ごとに暗号資産価格が２倍に増加しない限り，最適ハッシュパワーは低下していく。）

３　利己的マイニングと分岐

前節では，演算課題を一番最初に解いたマイナーが即座にブロックを公開し，報酬を得るという Nakamoto プロトコルに従うマイナーについて最適化行動を分析した。Nakamoto［10］では，この想定のみでマイニングのインセンティブは十分と考えているが，Eyal and Sirer［2014］はこの想定のみではインセンティブは十分ではなく，分岐が生じる可能性があることを示した。Nakamoto［10］では，マイニングを10分間以内の演算計算ゲームとして，言わばワンショットのゲームとして捉え，マイナーは正直に即座に結果を公表することになっている。それは１回限りの早い者勝ちゲームだからである。しかしそれに従わないマイナーがいた場合，またゲームをワンショットゲームではなく，多

段階・異時点間のゲームと捉えるマイナーがいた場合，インセンティブに瑕疵が出てくる。いわゆる利己的マイニング（Selfish Mining）の存在である。

利己的マイニングとは，新たに接続するブロックの公開を意図的に遅らせることで利益を増やす行為である。以下，具体的にその手順を示そう。ここで，マイナーを利己的なマイナーと正直なマイナーに２分割しよう。

利己的マイナーとはマイニングに成功してもブロックを公開せず，私的分岐（private branch）を行い，マイニングしたブロックに続くブロックのマイニングを継続するマイナーのことである。これに対して正直なマイナーとは新しく発見したブロックを即座に公開し，私的分岐を行わないマイナーのことである。利己的マイナーは２個，３個と可能な限りマイニングを行い，利己的マイナーは正直なマイナーがマイニングに成功するまで，２個，３個とマイニングを続け，正直なマイナーがマイニングに成功し，新しいブロックの公開と同時に保持していたブロックを公開し，フォーク（分岐）を維持する。ブロックチェーンは，１節で前述したように分岐した場合は，より長い方のチェーンが正当とされるので，利己的マイナーは生成したブロックの数だけ報酬を受け取ることができる。

以下では Eyal and Sirer［４］にならって利己的マイニングのマルコフ過程モデルを展開しよう。

図１

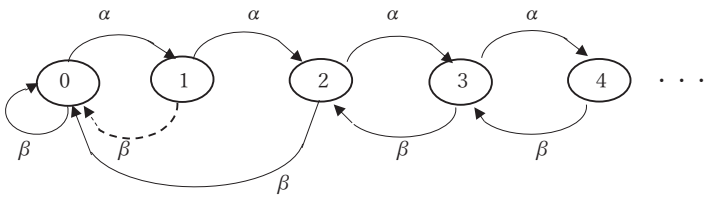
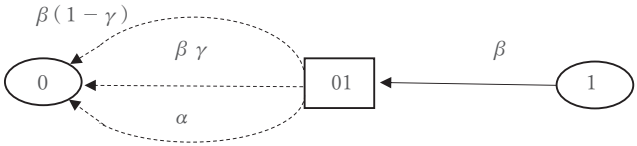


図１には，状態間を遷移するマルコフ過程が示されている。各○印の数字は利己的マイナーの私的分岐によって保有するブロックの数である。０の状態とは，正直なマイナーがマイニングに成功し，ブロックが即座に公開され，利己

的マイナーがマイニングに失敗した状態である。ここで利己的マイナーがマイニングに成功する確率をαとし，正直なマイナーがマイニングに成功する確率をβとしよう。毎回どちらかが必ずマイニングに成功するので，$\alpha + \beta = 1$となる。

状態１は利己的マイナーがマイニングに成功し，私的分岐においてブロックを隠し持っている状態である。ここで正直なマイナーが利己的マイナーよりも先にマイニングに成功した場合，状態１は状態０に遷移するが，この遷移は複雑である。その状況を図示すると以下のようになる。



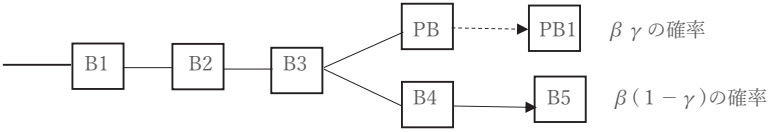
状態１において，正直なマイナーがマイニングに成功すると，利己的マイナーは隠していたブロックを公開し，ブロックの私的保有はゼロとなる。しかし，この時は状態０と異なり，フォークが存在したままである。状態０と区別するため，状態01としよう。次にこの状態01から状態０に遷移する過程は，以下のようにまず２通りに分かれる。

１．利己的マイナーがαの確率でマイニングに成功し，状態０に遷移する場合
２．正直なマイナーがβの確率でマイニングに成功し，状態０に遷移する場合

しかし，この場合，正直なマイナーは分岐したブロックが私的なものか，公開された正当なものかを区別できない。そこで正直なマイナーのうちγの確率で私的なブロックチェーン上でマイニングに成功する場合と，$1 - \gamma$の確率で正当なブロックチェーンでマイニングに成功する場合の２つに分かれる。

以上より，状態01から状態０への遷移は，α，$\beta\gamma$，$\beta(1 - \gamma)$の確率で行われ，３通りの可能性が生じることになる。以下に状態01での正直なマイナーのマイニングを示そう。

図２



これより，上記図１の遷移モデルより，定常状態における各状態の確率を求めよう。ここで各状態の確率を p_0，p_{01}　p_1，p_2，p_3，p_4…としよう。すると，状態０と状態１，状態２の関係は以下のようになる。

$$\alpha p_0 = \beta\, p_1 + \beta p_2 = (1-\alpha)p_1 + (1-\alpha)p_2 \quad \cdots\cdots\cdots(6)$$

状態01と状態１との関係は以下に示される。

$$p_{01} = (1-\alpha)p_1 \quad \cdots\cdots\cdots(7)$$

状態１以上については次式で示され，

$$\alpha p_i = (1-\alpha)p_{i+1} \quad i \geq 1 \cdots\cdots\cdots(8)$$

全事象の確率は１より

$$\sum_{i=0}^{\infty} p_1 + p_{01} = 1 \quad \cdots\cdots\cdots(9)$$

(8)より $i \geq 2$ において

$$p_i = \left(\frac{\alpha}{1-\alpha}\right)^i \cdot p_1 \quad \cdots\cdots\cdots(10)$$

(6)と(10)より

$$\alpha p_0 = (1-\alpha)p_1 + (1-\alpha)\frac{\alpha}{1-\alpha}p_1 = p_1 \cdots\cdots\cdots(11)$$

(9)に(7)，(10)，(11)を代入すると，次式を得る。

$$p_0 + \sum_{i=1}^{\infty} p_i + p_{01} = \frac{1}{\alpha}p_1 + \sum_{i=1}^{\infty}\left(\frac{\alpha}{1-\alpha}\right)^{i-1} \cdot p_1 + (1-\alpha)p_1 = 1 \cdots\cdots\cdots(12)$$

(12)より

$$\frac{1-4\alpha^2+2\alpha^3}{\alpha(1-2\alpha)}\cdot p_1 = 1 \cdots\cdots\cdots(13)$$

これより，各状態の確率が求められる。

$$p_0 = \frac{1}{\alpha}p_1 = \frac{1-2\alpha}{1-4\alpha^2+2\alpha^3} \cdots\cdots\cdots(14)$$

$$p_{01} = \frac{\alpha(1-\alpha)(1-2\alpha)}{1-4\alpha^2+2\alpha^3} \cdots\cdots\cdots(15)$$

$$p_1 = \frac{\alpha(1-2\alpha)}{1-4\alpha^2+2\alpha^3} \cdots\cdots\cdots(16)$$

$$p_i = \left(\frac{\alpha}{1-\alpha}\right)^{i-1}\cdot\frac{\alpha(1-2\alpha)}{1-4\alpha^2+2\alpha^3} \quad i \geq 2 \cdots\cdots\cdots(17)$$

4　利己的マイナーの最適化行動

ここで利己的マイナーの期待利潤を求めよう。利己的マイニングの従来の分析では，マイニングの費用に関してほとんど論じられていない。マイニングコストを固定費と見なしているようだ。しかしながら，マイニングのコストは新ブロックの作成（ナンスの発見）の度に増加しており，固定費ではない。ここでは１ブロック作成ごとに一定の費用がかかることを想定しよう。

利己的マイニングによる私的分岐のブロックチェーンはどこまで延ばすべきか。分析では無限まで伸ばして定常状態を求めているが，ここでは有限の離散分析を行う。状態の成立確率は毎回減少していき，一方毎回費用が増えていくことを考えれば，ある段階で期待利潤が負になることは明白である。

利己的マイナーの期待利潤（$E\pi$）を次のように定義しよう。毎回の期待報酬をＲとし，私的分岐での１つのブロック生成の費用をＣ，固定費を C_F とすると，

$$E\pi(n) = \sum_{i=1}^{n} p_i\, nR - nC - C_F \cdots\cdots\cdots(18)$$

上記の(14)～(17)より，

$$E\pi(n) = \left(\sum_{i=1}^{n}\left(\frac{\alpha}{1-\alpha}\right)^{i-1}\cdot p_1\right)nR - nC - C_F$$

$$= \left(\frac{\alpha^2(1-\alpha)(1-2\alpha)\left\{1-\left(\frac{\alpha}{1-\alpha}\right)^n\right\}}{1-4\alpha^2+2\alpha^3}\right)\cdot n(R-C) - C_F \quad \cdots\cdots\cdots(19)$$

まず(19)の期待利潤式が n の増加と共に減少することを確認しよう。ここで記号の整理を行う。

$$\theta(\alpha) = \frac{\alpha^2(1-\alpha)(1-2\alpha)}{1-4\alpha^2+2\alpha^3} \cdots\cdots\cdots(20)$$

(19)と(20)より，

$$E\pi(n) = \theta(\alpha)\left\{1-\left(\frac{\alpha}{1-\alpha}\right)^n\right\}\cdot n(R-C) - C_F$$

$$= -\theta(\alpha)\left(\frac{\alpha}{1-\alpha}\right)^n\cdot n(R-C) + \theta(\alpha) - C_F \cdots\cdots\cdots(21)$$

ここで $E\pi(n)$ と $E\pi(n+1)$ の差を計算すると，

$$E\pi(n+1) - E\pi(n) = -\theta(\alpha)(R-C)\left(\frac{\alpha}{1-\alpha}\right)^n\left\{\frac{\alpha}{1-\alpha}(n+1) - n\right\}$$

$$= -\theta(\alpha)\left(\frac{R-C}{1-\alpha}\right)\left(\frac{\alpha}{1-\alpha}\right)^n\{(2\alpha-1)n+\alpha\} \cdots\cdots\cdots(22)$$

(22)より，$(2\alpha-1)n+\alpha > 0$ すなわち，

$$n > \frac{\alpha}{1-2\alpha}$$

であるかぎり，(22)は負となるが，$0 < \alpha < 0.5$ であることより，（$\theta(1/2) = 0$ となる。）

$$0 < \frac{\alpha}{1-2\alpha} < 1 \quad n \in N \quad \text{(自然数)}$$

これより，$R > C$ である限り，$E\pi(n+1) - E\pi(n) < 0$

となり，ブロックを追加的増加すると期待利得は低下する。よって期待利潤がゼロになるブロック数 n が私的マイナーにとって総期待利潤を最大化すると

ころである。

ここで期待利潤が０になる n と α，R，C の関係について検討しよう

$$\theta(\alpha)\left\{1-\left(\frac{\alpha}{1-\alpha}\right)^{n}\right\}\cdot n(R-C)=C_F \cdots\cdots\cdots(23)$$

(23)から n と α，R，C の関係を陽表的に示すのは困難なので，α に値を代入して議論を進めよう。ここで R＝mC と仮定し，m＞1 としよう。

α ＝0.25のとき，θ (1/4)＝0.03より

$$0.03\left\{1-\left(\frac{1}{3}\right)^{n}\right\}\cdot n(m-1)C=C_F \cdots\cdots\cdots(24)$$

となる。これより，２ブロックを多く得るためには，どれだけの報酬が必要になるかを計算できる。

n＝2 とすると，(21)より

$$m=1+18.75\cdot\frac{C_F}{C} \cdots\cdots\cdots(25)$$

$$R=mC=C+18.75\cdot C_F \cdots\cdots\cdots(26)$$

すなわち，C_F（固定費）大きい場合，２つのブロック分岐でプラスの利益をだすにはかなり大きな報酬が必要である。ビットコインの場合，報酬 R は，次式より

$$R=3.125\times P_{BTC}$$

P_{BTC}（ビットコイン価格）の3.125倍であるから，2024年11月17日現在1400万円より4,375万円（１ブロック10分間）上の例では２ブロックであるので8,750万円とマイニングのための費用との比較となる。以上より，ビットコイン価格の上昇は，利己的マイニングに私的分岐へのインセンティブを与えるが，ビットコイン価格低下においては，従来の Nakamoto プロトコルに従うと思われる。

５　まとめと今後の課題

本論文ではこのブロックチェーンの連結作業であるマイニングについて分析をおこなった。この連結作業は参加者のコンセンサス・アルゴリズムでもあり，同時にブロックチェーンの安全性を担保するものでもある。本論文ではビットコインで採用されている Proof of Work について，特に２種類のマイニングについてモデル分析を行った。すなわち Nakamoto のプロトコルに従う正直なマイナーとプロトコルを無視する利己的なマイナーによるマイニングについてである。

まず１節では，ブロックチェーンの構造と Proof of Work について，特にそのマイニングの仕組みとブロック生成・連結過程について展開した。ブロックチェーンは Nakamoto のオリジナルではなく，その原型は既に1991年の Haber and Stornetta の論文［５］で提示されている。すなわち文書データのハッシュ値を求め，タイムスタンプを付して保存する方法である。また情報をツリー状態で圧縮する Merkle tree（ハッシュ・ツリー）は1979年に Ralph C. Merkle［10］が考案したものである。さらに Proof of Work というコンセンサスアルゴリズムのアイデアは，1992年の Cynthia Dwork and Moni Naor のジャンクメール排除の論文［３］と1999年 Jakobsson and Juels［７］，2002年 A. Back［１］で展開されたものである。こうした多くの研究成果を組み合わせ，巧みに実装可能なプロトコルに仕上げたのが Nakamoto［12］である。

２節では Nakamoto プロトコルに従うマイナーの行動についてモデル分析を行い，最適化行動として期待利潤の最大化をもたらすハッシュパワーを求めた。最適ハッシュパワーはマイナーの増加と限界費用の上昇により低下し，暗号資産価格の上昇により，増加することを明らかにした。

３節では利己的マイニングによるブロックチェーンの分岐（フォーク）について論じ，私的分岐のブロック数に対応する状態をマルコフ過程モデルで表した。そして定常状態における各状態確率を求めた。続く４節では利己的マイナーの期待利潤を定義し，利己的マイニングの最適ブロック数について検討をおこなった。ここではこれまで論じられてこなかったマイニングの費用，特に

固定費用の大きさが重要であることを明らかにした。さらにビットコインの場合はその価格の大小により私的分岐が生成されることをモデルの上で示した。

今後の課題としては，こうした私的分岐を阻止し，インセンティブを維持するプロトコルの設計があげられる。分岐はブロックチェーン上の安全性の脅威であるだけでなく，正直なマイナーのマイニングを無駄にし，膨大な資源（電力など）を浪費してしまうからである。

参考文献

[1] Back, A (2002)
Hashcash-a denial of service counter-measure　http://www.hashcash.org/hashcash.pdf
[2] Dimitri, N. (2017)
Bitcoin Mining as a Contst. Ledger 2, 31−37
[3] Dwork, C., and Naor, M (1992)
Pricing via Processing or Combatting Junk Mail. Annual International Cryptology Conference, 1992 − Springer
[4] Eyal, Ittay, and Emin Gün Sirer, (2014)
“Majority Is Not Enough: Bitcoin Mining Is Vulnerable,” Proceedings of International Conference on Financial Cryptography and Data Security 2014, Lecture Notes in Computer Science, 8437, Springer, 2014, pp. 436−454.
[5] Haber, S., and Stornetta, W. S (1991)
How to Time-stamp a Digital Document. Journal of Cryptology, Vol. 3, No. 2, pp. 99−111.
[6] Houy, N (2016)
The Bitcoin Mining Game, Ledger 1, 53−68
[7] Jakobsson, M., and Juels, A (1999)
Proofs of Work and Bread Pudding Protocols Secure Information Networks, Leuven, Belgium pp. 258−272
[8] Lewenberg, Y., Bachrach, Y., Sompolinsky, Y., Zohar, A. and Rosenschein, J. S (2015)
Bitcoin mining pools: A cooperative game theoretic analysis. Proceedings of the 2015 International Conference on Autonomous Agents and Multiagents Systems 919−927
[9] Ma, J., Gans. J. S, and Tourky, R (2018)
Market Structure in Bitcoin Mining NBER Working Paper No. 24242 Issued in January 2018
[10] Merkle, Ralph C., (1982)
“Method of Providing Digital Signatures,” Google Patents, 1982 (available at https://www.google.com/patents/US4309569, 2024年11月1日).
[11] Narayanan, A., Bonneau, J., Felten, E., Miller, A and Goldfeder, S (2016)
BITCOIN AND CRYPTOCURERENCY TECHNOLOGIES Princeton University Press.
[12] Satoshi Nakamoto (2008)
Bitcoin: A peer-to-peer electronic cash system, https://bitcoin.org/bitcoin.pdf