最適マイニングとハッシュレート

相　模　裕　一

序

2009年１月にビットコインが作られてから11年が経過した。当初，P2P ネットワークに公開された分散台帳，デジタル署名，Proof of Work など経済とは無縁と思われた諸概念は今やビジネスにおいては必須の知識となっている。この間，リップルやイーサリアムなど沢山の暗号通貨も発行されてきた。しかし，それらは未だ通貨としての活用よりも投機対象としての保有がメインであるようだ。こうした暗号通貨の行方は不明だが，これらの通貨を支える基盤としてのブロックチェーンの進展は確実だ。

本論文ではブロックチェーンの有用性を実際に示したビットコインについて，とくにその承認システムである Proof of Work について検討を行うことにする。Proof of Work はビザンチン将軍問題（互いに信認のないところでの合意形成）の解決策であり，ネットワークを管理者無しに自律的に運用可能とするプロトコルである。しかし，そのために必要となるマイニング（演算証明）は膨大な消費電力を費やし，その社会的費用は大きい。

本論文の構成は以下の通りである。まず１節では，Satoshi Nakamoto 登場前のブロックチェーン形成期に触れる。続く２節では 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。３節ではマイナー（マイニングを行う人）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ている。最後の４節では現実のビットコイン価格とハッシュパワー（ハッシュレート），そしてビットコイン・ネットワークの費用である消費電力の関係について検討し，以下の３つの結果を得ている。１）BTC 価格／消費電力はほぼ一定であること。２）消費電力と

Hash Rate は正の相関をもち，Hash/BTC 価格は上昇トレンドにあること。３）消費電力と Hash/BTC 価格も正の相関を有し，ハッシュレートの上昇傾向が続く限り，膨大な電力が消費されることが示されている。

１．ビットコインの構造とその起源

2008年 Satoshi Nakamoto の論文［10］で提唱されたビットコインは，2009年１月３日にそのネットワークが運用開始し，９日の17時５分に Nakamoto 自身によってネット上でリリースされた。（Bitcoin v0.1 released）当初１BTC は0.07円の価値であったが，2012年に1000円以上になり，2017年にブームを迎える。１月１日に11万円であったが12月１日にピークとなり，瞬間的に237万円となったことで衆人の注目を集めたが，１年後の2018年12月９日に最安値35万円をつけ，ビットコインのバブルは崩壊し，多くの投資家は離れた。しかし半年後の2019年６月23日には瞬間的に149万円まで高騰し，2020年１月６日には81万円となっている。１日の取引での変動幅は大きく10万～100万円であり，30分間で10万円前後の変動も稀ではない。ビットコインはもはや通貨ではなく投機対象の資産といえよう。

このビットコインの取引は P2P（Peer to Peer）型のネットワークシステムでなされており，第三者の仲介（銀行等）の介在なしに直接ユーザー間で実行されている。そして取引の記録は全て分散型台帳によって全てのユーザーに公開されている。（公開情報は全て16進数で暗号化されているので，匿名性は担保されている。）この公開型台帳システムのことをブロックチェーンという。Satoshi Nakamoto がブロックチェーンを考案したのではなく，ブロックチェーンを用いて実行可能なデジタル通貨を考案したといった方が適切であろう。実に Nakamoto 論文［10］は様々なアイデアを統合させているのである。

まず，ブロックチェーンの原型は1991年の Haber and Stornetta の論文［4］で提示された。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 D_t 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。文書の１字を変える者に対して絶望的な作業が課せられるのである。この演算課題とナンス，そして計算量については後述する。

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［6］，2002年 A. Back［1］で展開されたものである。

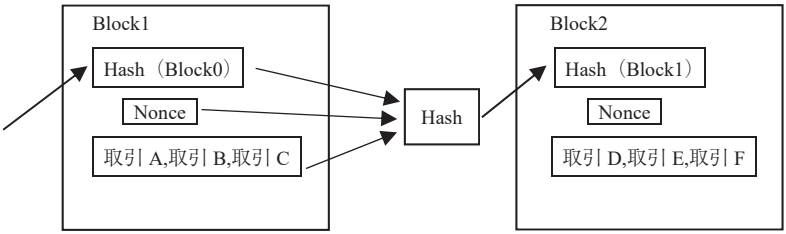
ビットコインの基本構造は，デジタルタイムスタンプによる分散型台帳（ブロックチェーン）に Proof of Work と暗号技術（公開鍵と秘密鍵）を組み合わせたものである。それぞれ別の目的のために考案されたアイデアがビットコインという暗号通貨の流通によって衆人に知られるようになり，さらにブロックチェーン独自の発展可能性についても広く認知されるようになったのである。

２．Proof of Work について

本論文では，ビットコインの Proof of Work に注目し，その演算証明を行うマイナーの活動を取り上げる。マイナー（採掘者）は演算証明（マイニング）を行い，他のマイナーよりも一番早く課題を解決した場合のみ，ビットコイン12.5BTC（2020年５月ごろ，6.25BTC に半減する。）と送金手数料を得ることができる。（手数料は取引が次のブロックに入る場合（10分以内），３ブロック以内（30分以内），６ブロック以内（１時間以内）で異なり，時間がかかるほど安くなる。）

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。

以下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）＜000…０****** となる。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。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，労を厭わず総当たりで片っ端から数値代入を行うこととなる。ハッシュ値は16進数なので，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。悪意の不正者にとって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ることになる。

ビットコインの場合，こうしたマイナーによるマイニングがブロックチェーンの形成に重要である。他の暗号通貨の場合，例えばリップルでは Proof of Consensus がなされリップルネットワークに P2P で繋がっている Validator（主に金融機関）の80％の承認でブロックを形成している。時節では，マイナーの最適化行動についてモデル分析を試みる。

３．マイニングモデル

この節では，マイナーの最適化行動を導出しよう。マイナーの数を $m \in \mathrm{N}$ として，マイナー$i \in \{1, \cdots, m\}$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[1]を以下のように記す。

$$prob\left(i\text{が}1\text{番}\right) = \frac{H_i}{\sum_{i=1}^{m} H_i}$$

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

$$prob\left(j \neq i\text{が}1\text{番}\right) = \frac{\sum_{j \neq i} H_j}{\sum_{i=1}^{m} H_i}$$

ここで，マイナーiが受け取るリターン（ビットコイン）を B，ビットコインの価格を p とし，費用関数を以下のように記す。

$c_i(H_i) = c_i H_i + C_F$　ここで c_i は限界費用，C_Fは固定費用である。

ここでマイナーi の利潤π_iは以下のようになる。

$$\pi_i = \begin{cases} pB - c_i(H_i) & \dfrac{H_i}{\sum_{i=1}^{m} H_i} \text{ のとき} \\ -c_i(H_i) & \dfrac{\sum_{j \neq i} H_j}{\sum_{i=1}^{m} H_i} \text{ のとき} \end{cases}$$

これよりマイナーi の期待利潤$E\pi_i$は以下のように記される。

$$E\pi_i = \frac{H_i}{\sum_{i=1}^{m} H_i} pB - c_i(H_i) \qquad i \in \{1, \cdots, m\}$$

期待利潤の最大化より，

$$\frac{\sum_{j \neq i} H_j}{\left(\sum_{i=1}^{m} H_i\right)^2} pB = c_i$$

ここで各マイナーの限界費用の総和を求めよう。すると，

$$\sum_{i=1}^{m} c_i = \frac{\sum_{i=1}^{m} \sum_{j \neq i} H_j}{\left(\sum_{i=1}^{m} H_i\right)^2} pB = \frac{m-1}{\sum_{i=1}^{m} H_i} pB$$

これより

$$pB = \frac{\sum_{i=1}^{m} H_i \sum_{i=1}^{m} c_i}{m-1}$$

ここで，$H_i = H_j = H$，$c_i = c_j = c$ としてシンメトリーなナッシュ解を求めよう。最適戦略としてのハッシュパワーをH^*とすると，

$$H^* = \frac{m-1}{m^2} \cdot \frac{pB}{c}$$ となり，

$E\pi_i = \frac{pB}{m^2} - C_F$　これより非負の期待利潤が得られる最大マイナー数 $m^* = \sqrt{\frac{pB}{C_F}}$ となる。

以上より，ハッシュパワーはビットコインの価格と限界費用（主に電気料金）の比率に依存し，p /c の上昇がハッシュパワーの増加をもたらすことがわかる。またマイナー数（参入数）がリターンと固定費用の比率に依存することも常識と合致する。

上記の分析ではマイニングに勝つ確率にハッシュパワーの相対比率を用いた。これは多くの分析で用いられている手法であるが，大事な点が分析できない。それはマイナーが10分未満の早期に演算課題を解いたとき，課題の難易度が上げられる点である。そこで，以下では，マイナーiが1番となる確率に課題の困難度を導入して考えよう。

以下の分析は，J.Ma-J.S.Gans-R.Tourky［8］による。

まず，マイナーiはハッシュパワーH_iの下で演算課題を解くのに最低 Z 回（Z∈N）の計算が必要と仮定しよう。

H_iはポワソン過程に従い，単位期間内で計算を完了する時間t_iを示す。そのt_iはガンマ分布に従い，$t_i \sim G(Z, H_i)$となり，　Z　は形状パラメータ，H_iはスケールパラメータである。

以上より，確率密度関数は以下の形となる。

$$f(t_i|Z, H_i) = \frac{1}{\Gamma(Z)} {H_i}^z {t_i}^{z-1} e^{-t_i H_i}$$

ここで各マイナーの演算課題の証明時間の集合を T，マイナーi が 1 番となる集合をT_i とする。

$$T = \{t_i \in R_+^m : i \in \{1, \cdots, m\}\} \quad T_i = \{t \epsilon R_+^m : t_i < t_j \ i \neq j\}$$

これより，マイナーi が 1 番となる確率は以下の式で表される。

$$prob\left(i\text{が}1\text{番}\right) = prob(t \in T_i) = \prod_{i \neq j} \left[1 - \int_0^{t_i} f(t_i|Z, H_j) dt_i\right]$$

よってマイナーi の期待利潤$E\pi_i$は以下のように記される。

$$E\pi_i = prob(t \in T_i) pB - c_i(H_i) = \prod_{i \neq j} \left[1 - \int_0^{t_i} f(t_i|Z, H_j) dt_i\right] pB - c_i(H_i)$$

以後$\prod_{i \neq j} \left[1 - \int_0^{t_i} f(t_i|Z, H_j) dt_i\right] = \varphi(T_i|Z, H_i, H_{-i})$ とする。$H_{-i} = \left(H_j : j \neq i\right)$

ここでハッシュパワーの増加が確率に与える影響について調べよう。

$$\frac{\partial}{\partial H_i} prob(t \in T_i) = \frac{\partial}{\partial H_i} \varphi(T_i|Z, H_i, H_{-i}) = \frac{\partial}{\partial E(t_i)} \varphi(T_i|Z, H_i, H_{-i}) \frac{\partial E(t_i)}{\partial H_i}$$

$$= \frac{\partial}{\partial E(t_i)} \varphi(T_i|Z, H_i, H_{-i}) \left(\frac{-Z}{{H_i}^2}\right) > 0$$

また，２階の偏微分より，

$$\frac{\partial^2}{\partial {H_i}^2} prob(t \in T_i) = \frac{\partial^2}{\partial {H_i}^2} \varphi(T_i|Z, H_i, H_{-i}) = \frac{\partial^2 \varphi}{\partial E(t_i)^2} \left(\frac{\partial E(t_i)}{\partial H_i}\right)^2 + \frac{\partial \varphi}{\partial E(t_i)} \frac{\partial^2 E(t_i)}{\partial {H_i}^2}$$

$$= \frac{\partial^2 \varphi}{\partial E(t_i)^2} \left(\frac{-Z}{{H_i}^2}\right)^2 + \frac{\partial \varphi}{\partial E(t_i)} \left(\frac{2Z}{{H_i}^3}\right) < 0$$

となる。１階と２階の符号判定の詳細は付論で展開する。これより，

$E\pi_i = \varphi(T_i|Z, H_i, H_{-i})pB - c_i(H_i)$　よって

$$\frac{\partial E\pi_i}{\partial H_i} = \frac{\partial \varphi}{\partial H_i}pB - c_i = 0$$

$$\frac{\partial^2 E\pi_i}{\partial {H_i}^2} = \frac{\partial^2 \varphi}{\partial {H_i}^2}pB < 0$$

期待利潤は極大値をもち，一意的なナッシュ解H^*の存在する。すなわち，

$H^* = (H_1^*, H_2^*, \cdots, H_m^*)$　ここで，$H_i^* = \theta(pB|Z, T)$　となる。

では，演算証明の困難度 Z が引き上げられた場合に最適ハッシュパワーがどのように変化するかを調べよう。

先に展開した単純なモデルと同様にシンメトリーなナッシュ解の下で考えよう。すなわち，

$H_i = H_j = H$より，

$\varphi(T_i|Z, H) = \left[1 - \int_0^{t_i} f(t_i|Z, H)dt_i\right]^{m-1} = \frac{1}{m}$　となるのは理解されよう。すなわち，これはすべてのマイナーは共通の確率密度関数を持つことを意味している。この条件下でＺ＋ε が全マイナーに生じても確率は不変であることより，次式が成立する。

$f(t|Z, H^*) = f(t|Z + \varepsilon, H^*)$

$$\frac{1}{\Gamma(Z)}H^{*Z}t^{Z-1}e^{-tH^*} = \frac{1}{\Gamma(Z+\varepsilon)}H^{*Z+\varepsilon}t^{Z+\varepsilon-1}e^{-tH^*}$$

$$\frac{1}{\Gamma(Z)} = \frac{1}{\Gamma(Z+\varepsilon)}H^{*\varepsilon}t^{\varepsilon}$$

$$H^* = \sqrt[\varepsilon]{\frac{\Gamma(Z+\varepsilon)}{\Gamma(Z)t^{\varepsilon}}}$$

$\Gamma(Z)$は凸関数で，$\frac{\Gamma(Z+\varepsilon)}{\Gamma(Z)}$は$Z$の増加関数であること，さらに$\varepsilon \to 1$ならば，

$$H^* \to \frac{Z+1}{t}$$

よってH^*がZの増加により，増大することがわかる。すなわち，困難度の上昇はH^*の増加となる。以上のモデル分析より，ハッシュパワーに関して次の２点が明らかになった。

１）ハッシュパワーはビットコインの価格pと限界費用cの比率に依存し，p/cの上昇はハッシュパワーの増加をもたらす

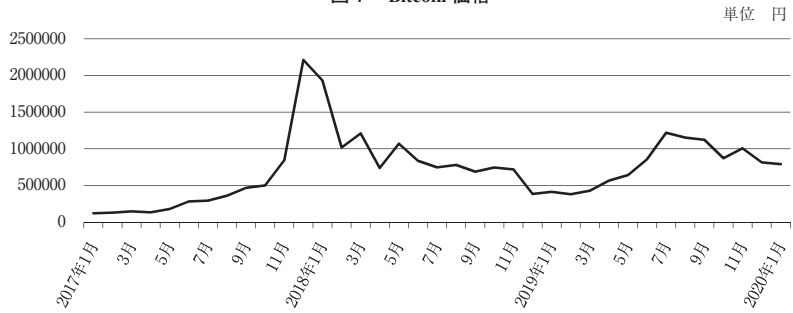
２）ハッシュパワーは演算証明の困難度の上昇により，増大する。

４．ハッシュレートと消費電力

前節では，マイナーの最適化行動より，最適なハッシュパワーH^*について分析をおこなった。ここでは，現実のビットコイン価格とハッシュパワー（ハッシュレート），そしてビットコイン・ネットワークの費用である消費電力の動向とそれらの関係について検討しよう。

まず，ビットコインの価格については過去３年間の動向を以下の図で示している。

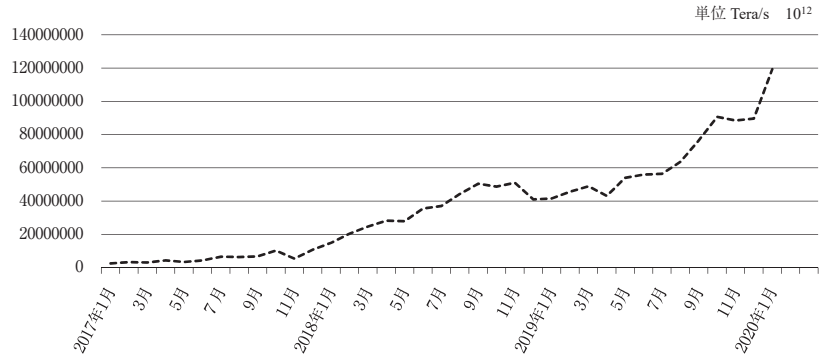
図１　Bitcoin 価格



Bitbank HP　https://app.bitbank.cc/trade より　筆者作成

2017年の１月１日に11万円から始まり12月１日に237万円のピークとなったこと。また2018年12月９日に最安値の35万円となり，現在2020年１月６日は81万円となっている。次にハッシュパワーを数値としてハッシュレートの動きを見てみよう。

図２　Hash Rate

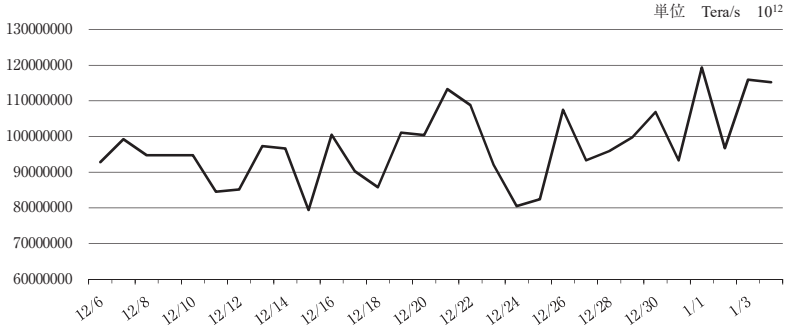


BLOCKCHAIN HP　　https://www.blockchain.com/ja/charts/hash-rate より筆者作成

ハッシュレートとは，マイニングする際の1秒当たりの計算力（採掘速度）のことで，hash/s で表される。図２では滑らかな曲線で描かれているが，日々の変動は次の図のように激しい。

図は2019年12月６日からの30日間のハッシュレートを示している。

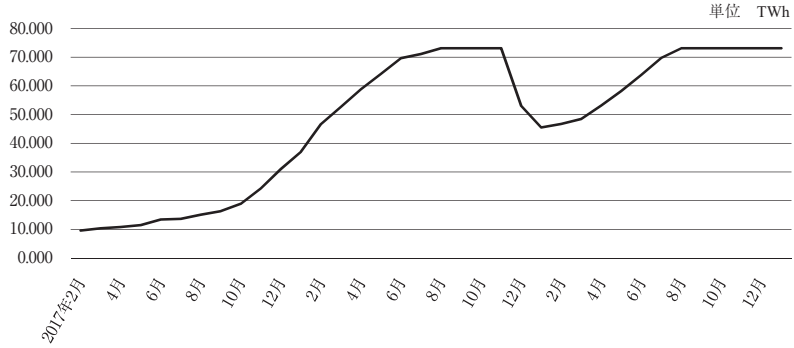
図３　Hash Rate



https://www.blockchain.com/ja/charts/hash-rate?timespan=30days　より筆者作成

図２と３より，ナンスを10分以内で見つけるには高速計算が必要であることがわかる。2020年１月１日には過去最大の毎秒１万２千京（12,000×10^{16}）回の演算処理を行っている。これには膨大な電力が必要となるが，消費電力量を以下の図４に示そう。

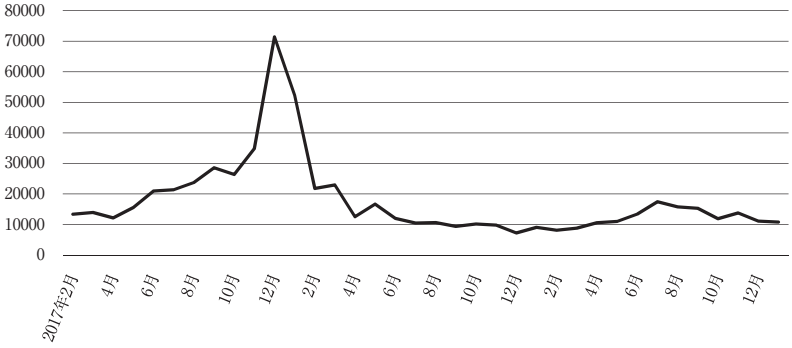
図４　消費電力



Digiconomist HP　https://digiconomist.net/bitcoin-energy-consumption より筆者作成

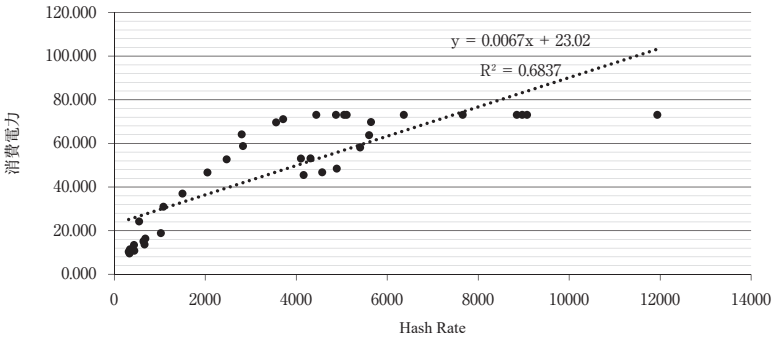
2019年以降７月以降，73.12TWh となっているが，これはオーストリアの年間電気消費量と同じである。これは１回のビットコイン取引に688TWh かかることになる。この消費電力で VISA では455629回の取引ができる。家庭の消費電力でみるならば，夏のエアコンフル稼働で１日最大20KWh かかることより，約34日分である。ビットコイン取引の社会的費用が高いことが理解されよう。次の図５には，１TWh に対するビットコイン価格の動向を示している。

図５　BTC 価格／消費電力



この図より，2017年２月から2018年２月の１年間だけが異様に高くなっており，ビットコイン価格のバブル期に一致することが分かる。他の期間は１万円（１TWh）前後を推移している。次に消費電力とハッシュレートについて単回帰分析[2)]を行うことにする。

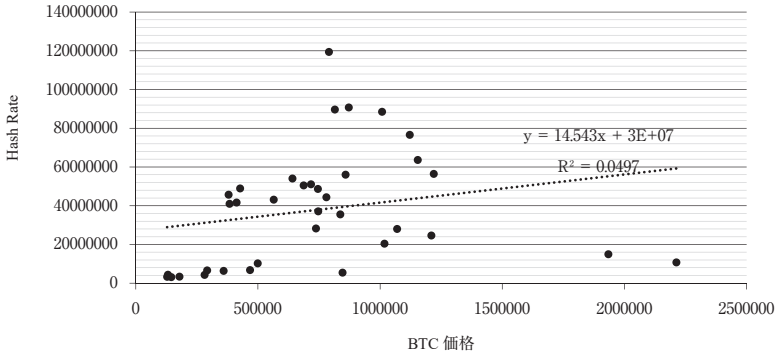
図６　消費電力とHash Rate



この関係は当然であろう。ハッシュレートの上昇とは，マイナーが性能を向上させることではない。１台の計算機が１秒間に処理できる演算数は決まっているので，計算機を大量に増加させることを意味している。それ故消費電力は利用台数

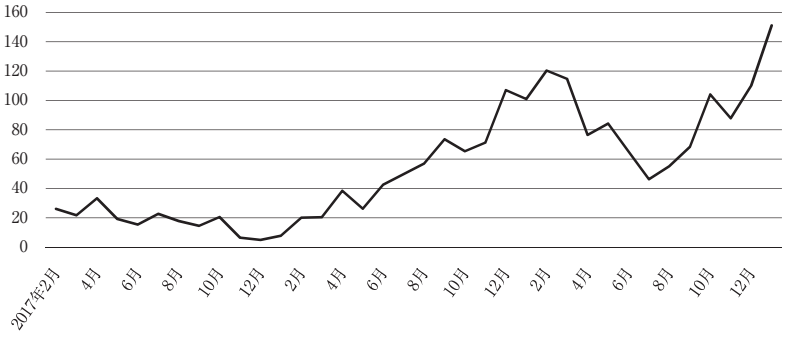
に従い増加する。次にハッシュレートとビットコイン価格の単回帰分析[3)]についてみると，

図７



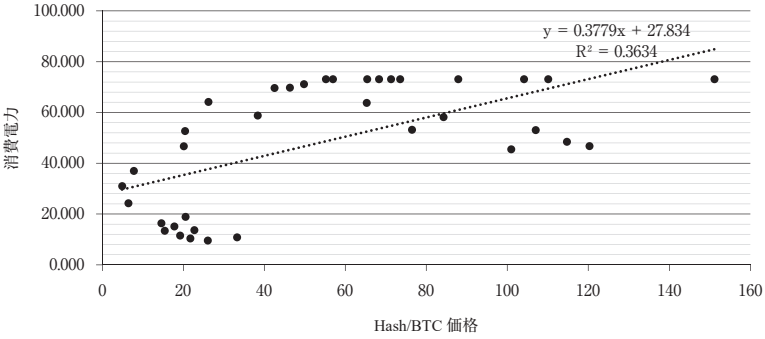
これより，両者には統計的に優位な関係は見られない。価格上昇がハッシュレートを上昇させるという前節のモデルでの結論は支持されない。しかし次の２つの図が示すように，ハッシュレートをビットコイン価格で割った値は意味がある。マイナーが受け取る１ビットコイン価値額に対するマイニング機械のコストとみることができよう。

図８　Hash/BTC 価格



この図より，ビットコイン生成に必要な費用が上昇トレンドにあることは明らかであろう。マイニング機械の計算能力が向上して10分未満に演算課題を処理した場合，より問題を難しくして平均10分となるように設計されているので，マイニング機械の能力向上化と機械の増大（マイニングプールの拡大）の競争が続き，費用は常に上昇傾向を持つことになる。消費電力との関係も次の単回帰分析[4)]で明白である。

図９　消費電力と Hash/BTC 価格



ビットコインネットワークシステムの承認方式がマイニングによる Proof of Work でなされる限り，この Hash Rate と消費電力の上昇は避けられそうにない。Proof of Work は集権的な管理ではなく，自律的で Incentive Compatible な承認方法である。

５．ま と め

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 Satoshi Nakamoto の論文［10］で巧みに結合され，ビットコインという暗号通貨という形になったといえよう。１節では，

Satoshi Nakamoto 登場前のブロックチェーン形成期に触れた。２節では 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した。続く３節では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。そしてビットコインの価格 p と限界費用 c の比率 p /c の上昇がハッシュパワーの増加をもたらし，演算証明の困難度の上昇がハッシュパワーを増大させることを非協力ゲームのナッシュ解より導出した。最後の4節では現実のビットコイン価格とハッシュパワー(ハッシュレート)，そしてビットコイン・ネットワークの費用である消費電力の関係について検討し，以下の３つの結果を得た。１）BTC 価格／消費電力（１TWh に対するビットコイン価格）はピーク時等の例外を除いてほぼ一定である。２）消費電力と Hash Rate は正の相関をもち，Hash/BTC 価格は上昇トレンドにある。３）消費電力と Hash/BTC 価格も正の相関を有し，ハッシュレートの上昇傾向が続く限り，膨大な電力が消費されることになる。通貨としての社会的有用性を無くし，単なる投機対象となったビットコインが，電力浪費という社会的費用を発生していることを大きな問題である。

しかし，このことは Proof of Work を用いない他の暗号通貨には当てはまらない。またブロックチェーンの有用性はビットコインの社会的価値と無縁である。ブロックチェーンを用いたイーサリアムのスマートコントラクトや Facebook の Libra，中国のデジタル人民元など，ブロックチェーンの可能性は大きくこれまでの商取引，公証制度を変えていくと思われる。

付　論

１階微分が正となることの証明

$F_i(t_i|Z,H)=\int_0^{t_i} f(t_i|Z,H)dt_i$ とし，$T_i=\{t\epsilon R_+^m : t_i \le t_j \ i\neq j\}$ とおく。

$$prob(t\in T_1)=[1-F_2(t_1|Z,H)][1-F_3(t_1|Z,H)]\cdots[1-F_m(t_1|Z,H)]$$

$$=\prod_{i=2}^{m}[1-F_i(t_1|Z,H)]$$

$t_1 \sim (Z,H_i)$ は$i.i.d$（独立同分布）なので，$prob(t\in T_1)=[1-F(t_1)]^{m-1}$となる。

$\frac{\partial}{\partial t_1} prob(t \in T_1) = -(m-1)f(t_1)[1-F(t_1)]^{m-2} < 0$ よって

$\frac{\partial}{\partial E(t_1)} \varphi(T_1|Z, H_i, H_{-i}) < 0$

ガンマ分布の性質より，$E(t_i) = \frac{Z}{H_i}$ より

$\frac{\partial}{\partial H_i} \varphi(T_i|Z, H_i, H_{-i}) = \frac{\partial}{\partial E(t_i)} \varphi(T_i|Z, H_i, H_{-i}) \frac{\partial E(t_i)}{\partial H_i} = \frac{\partial}{\partial E(t_i)} \varphi(T_i|Z, H_i, H_{-i}) \left(\frac{-Z}{{H_i}^2}\right) > 0$

となる。

２階微分が負となることの証明

$\frac{\partial}{\partial t_1} prob(t \in T_1) = -(m-1)f(t_1)[1-F(t_1)]^{m-2}$　より

$\frac{\partial^2}{\partial {t_1}^2} prob(t \in T_1) = -(m-1)[f'(t_1)[1-F(t_1)]^{m-2} - (m-2)f(t_1)^2[1-F(t_1)]^{m-3}]$

ここで$f(t_1|Z, H)$の最頻値は(Z－１)/Hであるから，

$t_1 < \frac{Z-1}{H}$ のとき　$f'(t_1) > 0$，$t_1 > \frac{Z-1}{H}$ のとき　$f'(t_1) < 0$

さらに $\forall t_1 \in R_+^m$ に対して　$f''(t_1) < 0$

$t_1 < \frac{Z-1}{H}$ のとき　$|f'(t_1)[1-F(t_1)]^{m-2}| > |(m-2)f(t_1)^2[1-F(t_1)]^{m-3}|$　ならば，

$\frac{\partial^2}{\partial {t_1}^2} prob(t \in T_1) < 0$

$|f'(t_1)[1-F(t_1)]^{m-2}| < |(m-2)f(t_1)^2[1-F(t_1)]^{m-3}|$

ならば，$\frac{\partial^2}{\partial {t_1}^2} prob(t \in T_1) > 0$

$t_1 > \frac{Z-1}{H}$ のとき，$\frac{\partial^2}{\partial {t_1}^2} prob(t \in T_1) > 0$

これより

1階の微分の証明で示した次式より

$$\frac{\partial}{\partial E(t_1)}\varphi(T_1|Z,H_i,H_{-i})<0 \quad \text{よって} \quad \frac{\partial\varphi}{\partial E(t_i)}\left(\frac{2Z}{{H_i}^3}\right)<0$$

上記より，$t_i<\dfrac{Z-1}{H}$ のとき $\dfrac{\partial^2}{\partial {t_i}^2}prob(t\in T_i)<0$ よって

$$\frac{\partial^2\varphi}{\partial E(t_i)^2}<0 \quad \text{すなわち} \frac{\partial^2\varphi}{\partial E(t_i)^2}\left(\frac{-Z}{{H_i}^2}\right)^2<0$$

$t_i>\dfrac{Z-1}{H}$ のとき $\dfrac{\partial^2}{\partial {t_i}^2}prob(t\in T_i)>0$ よって $\dfrac{\partial^2\varphi}{\partial E(t_i)^2}\left(\dfrac{-Z}{{H_i}^2}\right)^2>0$

しかし，$prob(t\in T_i)<1$より

$\dfrac{\partial^2\varphi}{\partial E(t_i)^2}\left(\dfrac{-Z}{{H_i}^2}\right)^2<\dfrac{\partial\varphi}{\partial E(t_i)}\left(\dfrac{2Z}{{H_i}^3}\right)$ となる。そうでないと$prob(t\in T_i)$

$=\varphi$は増加関数となり，

$prob(t\in T_i)>1$となる。以上より，

$$\frac{\partial^2}{\partial {H_i}^2}prob(t\in T_i)=\frac{\partial^2}{\partial {H_i}^2}\varphi(T_i|Z,H_i,H_{-i})=\frac{\partial^2\varphi}{\partial E(t_i)^2}\left(\frac{\partial E(t_i)}{\partial H_i}\right)^2+\frac{\partial\varphi}{\partial E(t_i)}\frac{\partial^2 E(t_i)}{\partial {H_i}^2}$$

$$=\frac{\partial^2\varphi}{\partial E(t_i)^2}\left(\frac{-Z}{{H_i}^2}\right)^2+\frac{\partial\varphi}{\partial E(t_i)}\left(\frac{2Z}{{H_i}^3}\right)<0 \quad \text{となる。}$$

注

1) こうした確率設定は[2] Dimitri, N. (2017)と[5]Houy, N(2016)にみられる。

2) 消費電力とハッシュレートについて単回帰分析

係数	標準誤差	t	P-値	下限 95%	上限 95%
23.02005	3.756016	6.128848	5.86E-07	15.38691	30.65319
0.00672	0.000784	8.572218	5.16E-10	0.005127	0.008313

3) ハッシュレートとビットコイン価格の単回帰分析

係数	標準誤差	t	P-値	下限 95%	上限 95%
27108963	9450767	2.86844	0.007039	7902693	46315234
14.54296	10.90871	1.333151	0.191347	－7.62621	36.71214

4) 消費電力と Hash/BTC 価格の単回帰分析

係数	標準誤差	t	P-値	下限 95%	上限 95%
27.83388	5.709326	4.875161	2.49E-05	16.23113	39.43663
0.377856	0.085772	4.405336	9.99E-05	0.203546	0.552167

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] Haber,S., and Stornetta,W.S (1991) How to Time-stamp a Digital Document. Journal of Cryptology, Vol. 3, No. 2, pp. 99-111,
[5] Houy,N(2016) The Bitcoin Mining Game, Ledger 1, 53-68
[6] Jakobsson,M., and Juels,A(1999) Proofs of Work and Bread Pudding Protocols
Secure Information Networks, Leuven, Belgium pp. 258-272
[7] 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
[8] Ma,J.,Gans.J.S, and Tourky,R Market Structure in Bitcoin Mining
NBER Working Paper No. 24242 Issued in January 2018
[9] Narayanan,A.,Bonneau,J.,Felten,E.,Miller,A and Goldfeder,S (2016)
BITCOIN AND CRYPTOCURERENCY TECHNOLOGIES Princeton University Press.
[10] Satoshi Nakamoto (2008) Bitcoin: A peer-to-peer electronic cash system,
https://bitcoin.org/bitcoin.pdf
[11] Satoshi Nakamoto (2009) Bitcoin v0.1 released
https://www.mail-archive.com/cryptography@metzdowd.com/msg10142.html

参照 HP サイト

Bitbank HP　https://app.bitbank.cc/trade
BLOCKCHAIN HP　https://www.blockchain.com/ja/charts/hash-rate
BLOCKCHAIN HP　https://www.blockchain.com/ja/charts/hash-rate?timespan=30days
Digiconomist HP　https://digiconomist.net/bitcoin-energy-consumption