研究員の眼

「マイニング」とは何か

経済研究部 准主任研究員　髙山　武士
(03)3512-1818　takayama@nli-research.co.jp

1――はじめに

昨年末以降、代表的な暗号資産であるビットコインが乱高下している。

足もとでは米大手電気自動車メーカーのテスラのＣＥＯ（「テクノキング」という肩書も名乗っている）であるイーロン・マスク氏による自社製品へのビットコイン決済への対応（自社製品へのビットコイン支払いを認める）とその取り下げ発言もビットコインの動きに関係しているなどと指摘がなされている。ビットコイン決済を取り下げた背景にはビットコインの「マイニング（採掘）」作業による電力消費の急増、そしてそれに伴う化石燃料の消費の急増といった懸念があるようだ。

では、そもそもビットコインのマイニングとは何だろうか。なぜ電力消費と関係があるのか。ビットコイン自体は10年以上も前に生まれたもので、これまで様々な解説がなされてきているが、足もとで関心が高まっていることもあり、改めて、本コラムでもビットコインのマイニングについて、やや詳細に解説してみたい。

以下ではビットコインではない暗号資産やブロックチェーンという一般概念にも触れているが、主にビットコインの仕組みを中心に説明している[1]。私たちは銀行預金による送金の仕組みを知らなくても銀行預金を利用しオンラインショッピングなどで活用しているように、ビットコインの仕組みを知らなくても、それを利用することは可能である。筆者も、電子機器など仕組みを知らずに使っている物の方が多い。それでも、「マイニング」という比喩表現が具体的に何を表しているかを把握することは、実際に暗号資産を保有したい（あるいは発掘したい）と考える人にとっては参考になり、ビットコイン（やそれを含む暗号資産、ブロックチェーンなど）に関連する報道をより深く理解する助けになると考えている。

2――ビットコインと預金

ではまず、一般に暗号資産とは何だろうか、という点から考えていきたい。

[1] ブロックチェーンのビットコインへの実装については、主に Andreas M. Antonopoulos, Mastering Bitcoin を参考にした。

暗号資産はデータであり、コンピュータ上に記録されている数字の羅列である。

この数字の羅列は、例えばビットコインが暗号「資産」や仮想「通貨」と呼ばれていることから推測できるように、「価値の貯蔵」手段や「決済」手段などとして用いられることがある（ただし、例えばビットコインのドル建て価格は大きく上下に変動することから、価値貯蔵や決済よりも投機的な目的で保有されている印象がある）。そこで、少し暗号資産・仮想通貨の特徴を明確にするため、仮想ではない本物の通貨である現金や預金と比較してみたい。

例えば現金（紙幣や硬貨）はデータではなく、実際のモノである。例えばＡさんが八百屋のＢさんからリンゴを買いたいときはＡさんがＢさんにリンゴの価格分（100 円）の現金と交換することで売買が完了する（決済される）。

一方、預金はデータである。通帳に印字すれば残高を見ることができるが、実体は銀行が管理するシステムの中にある数字の羅列である。例えばリンゴ 10 個を銀行振込で買う場合、Ａさんはリンゴ 10 個を送ってもらう代わりに、銀行に対して価格分（1000 円）の預金をＢさん口座に振り込むように依頼する。銀行はＡさんの口座残高を 1000 円減らし、Ｂさんの口座残高を 1000 円増やすことで売買が完了する（決済される）。

ビットコインはデータであるので、この意味では預金に近いと言えるだろう。ただし、**ビットコインは銀行のように口座残高を管理する特定の管理者がいるわけではない**。これはビットコイン（およびそれに類似する暗号資産）の大きな特徴と言える。

ビットコインは、そもそも銀行のようにデータを管理する特定の人がいないのに、Ａさんは 100 ビットコインを保有している、そのうちＢさんに 50 ビットコインを送金（移転）する、といった保管や取引をすることができるのである。

例えば、次の疑問は単純だが、なかなか興味深い。

「銀行のような管理者がいないのに、Ａの財布にあるビットコインは持ち主でなければ使えないのはなぜだろうか（管理者がＡさんであると本人確認し利用を許可している訳ではないのに）」

「ＡからＢへの送金（移転）取引はどのように承認されているのだろうか、不正取引をどのように防いでいるのだろうか（「管理者」が不正のないように利用者を見張り、取引承認や口座残高データの増減をしている訳ではないのに）」

前者の回答はマイニングと関係ない部分も多いので、解説は別の機会に譲りたいと思う[2]。一方、後者の疑問はマイニングにも関連する。以下ではビットコインの特徴やマイニングの説明をするとともにこの疑問への回答についても解説したい。

なお、ビットコインの財布はＡさん、Ｂさんという人に紐づいているのではなく、あくまでも電子

[2] 前者の疑問への回答は、公開鍵暗号/電子署名に関する仕組みを学ぶことで理解できる。例えば、松澤登（2020）「キャッシュレスを学ぼう(5)－暗号資産（仮想通貨）」『基礎研レター』2020-06-11 には暗号資産の法的位置づけとともに、簡潔に記載されている。

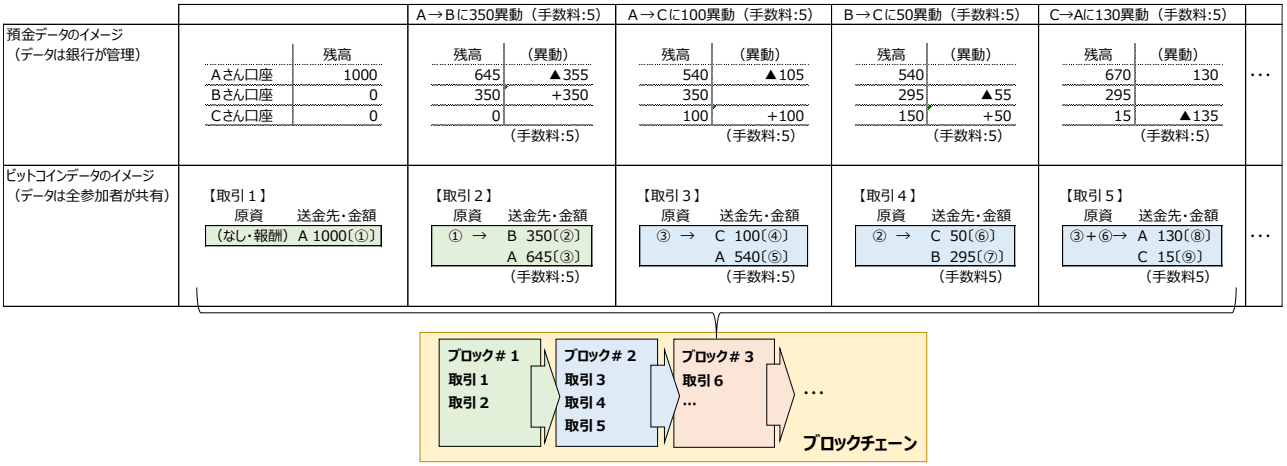
上の宛先（データで示された住所であり、インターネットの「アドレス」やメールの「アドレス」のようなもの）である。実際には「Ａさん」が電子上のＡという電子財布（ウォレット）を作成[3]し、そこに住所（宛先、アドレス）が書かれているのである。Ａの住所宛に送られてきたコインからＢの住所に 50 ビットコインを送金（移転）する、という形になっている。

Ａの電子財布を作成するのと、Ａが銀行に口座開設するのとは似ているような感じもするが、実際には異なる。具体的に、預金データとビットコインを比較してみると、次のような違いがある[4]（図表 1）。

まず、預金は様々な人・企業の口座（残高や口座間の異動）データであり、銀行が管理している（図表 1 の最上段）。Ａさんは自分の口座の残高情報や数年前までの取引履歴を知りたいときには、銀行に依頼して、銀行が保有しているデータの一部をＡさんに開示するという手続きを踏んでいる。

送金や現金の引き出しは、銀行に対して（ＡＴＭカードなどで）Ａさん本人であることを示した上でなされ、また、その取引・残高データは銀行が記録する。

（図表 1）



（資料）筆者作成

一方、<u>ビットコインは、「取引」が連なったデータであり、ネットワーク参加者全員に共有されている</u>（フルノード参加者全員が保有している）。なお「取引」データは、コインがどこからどこに行ったのかを記した、原資（資金源）と送金先・金額が記載されており、「残高」という視点でデータは蓄積されていない。

例えば、図表 1 中央下段の「【取引３】Ａ→Ｃに 100 異動」の「取引」では、送金するための原資（【取引２】〔③〕の取引）と送金先（③からＣに 100〔④〕）というデータが記される。そしてＡの残り 540（手数料除き）も「取引」の一部として（③からＡに 540〔⑤〕）として記される。この後、Ａがこの 540 を原資としてＢに送金する場合は、⑤の原資からＢに△△という取引が続くことになる（原資と送金先はそれぞれ複数で１つの「取引」となることもある（図表１の一番右の例））。Ａが保有す

[3] 財布の作成は、ビットコイン端末を設置しネットワークへの参加すること（「ノード」と呼ばれる）とほぼ同義であるため、本コラムでは、このノードの意味で用いる。ただし、最近は暗号資産の交換や保管（カストディ業務）を行う業者が増えており、ネットワーク参加者でなくてもこうした交換業者を通じてビットコインを保有することができる。

[4] 以下で説明するようにデータとして銀行口座データとビットコインデータには違いがあるが、例えば決済業者にビットコインの保管を委託し、利用するという立場から見ると、預金口座や証券口座を保有するようにビットコイン口座が保有できるため、利用上の感覚は類似する。

るビットコイン（使えるビットコイン）の残高を知りたいと思ったら、これまでの「取引」をすべて集めた上で、まだ送金されておらず原資として使える金額を合計する必要がある。

「取引」データの追加は、ある参加者が正しい（データ上不備のない）「取引」を作成すると、他の参加者にその「取引」データが伝送される形で、全参加者に共有されていく。**参加者なら誰でも自ら「取引」を作成することができ、それが全参加者に共有される仕組みである**（ただし、原資を保有する人しか、その原資をどこかに送金する「取引」を作成することはできないようになっている。これは前述の最初の疑問に関連する仕組みである）。

この「取引」がいくつかまとまって「ブロック」と呼ばれるデータの集合となる。そして、この**「ブロック」の全体がビットコインのブロックチェーンと呼ばれている**（チェーンと呼ばれる理由は後述）。「取引」の共有と同じく、基本的にはこのブロックチェーン（ブロックの集合体全部）を取引参加者全員が保有している[5]。この、ビットコインのような**参加者（ノード）がすべてのデータを共有、管理している仕組みは「分散型」のシステムと呼ばれる**[6]。

「ブロック」のイメージとして、図表 1 の下にそれぞれ数個の取引からなる「ブロック#1」～「ブロック#3」まで記載してみた。実際のビットコインはこんなに単純ではないが、イメージとしてはこのような構造で、ブロックはゼロ番から始まり、執筆時点で 685,000 近いブロックが存在している（図表 2 の「Height」欄、図表 2 ではブロックの#1～#3 を左から順に並べたが、ブロックを下から上に積み上げるイメージもよく用いられ、その番号を示すものとして「高さ（Height）」の標記が使われる）。また、図表 2 を見ると、ひとつのブロックに 1000 から 2000 を超える取引が含まれていることも分かる（図表 2 の「Transactions」欄）。

（図表 2）

Latest blocks View all

Age	Height	Mined by	Transactions	Size
7 minutes ago	684,873		1,337	1.16 MB
15 minutes ago	684,872		2,231	1.26 MB
25 minutes ago	684,871		1,816	1.42 MB
28 minutes ago	684,870		1,594	1.25 MB
an hour ago	684,869		1,681	1.38 MB

Latest transactions

Transaction ID	Output	
e315d514e42fa… 42c0	0.028 557 01 BTC	View details
6794daacfa00f… 621d	0.000 638 07 BTC	View details
e7039c75bca8e… 394b	0.001 360 43 BTC	View details
883f08203b5da… ac66	0.001 256 88 BTC	View details
76e014bc06c13… fb91	0.016 083 11 BTC	View details

（資料）https://explorer.bitcoin.com/btc

なお、昔はブロックに含まれる取引数が少なく、1 ブロックの大きさ（容量、サイズ）も大きくなかったが、近年は全体で 1MB（メガバイト）を超えることが常態化している（図表 3、なお、1 ブロックの容量には制限があるため、1MB を大きく超えることはない）。ビットコインの正体は、最初に稼働してゼロ番目のブロックができた時（2009 年）からのすべての「取引」およびそれを含む「ブロック」の連結であり、執筆時点ではビットコインのブロックチェーンの容量は約 350GB（ギガバイト）に達

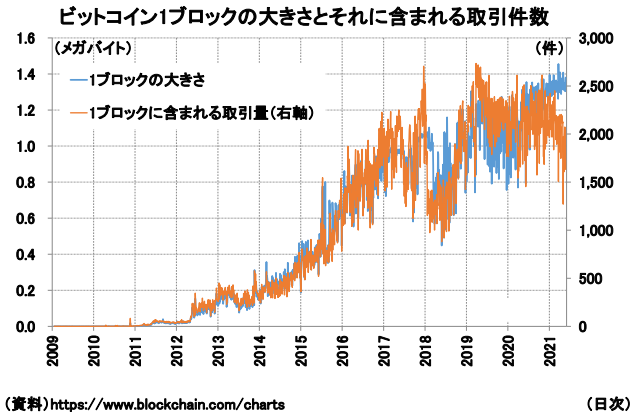
[5] 前述の通り、ここまで参加者によるデータの共有については、いわゆるフルノードの参加者を念頭に説明している。ネットワーク参加者でも、すべてのブロックをダウンロードしない軽量型のノードが存在する（計量型のノードは他のフルノードが持つブロックチェーンの情報を参照することで軽量化を実現している）。

[6] 分散型システムで保有されるこのデータのことを「（分散）台帳」と呼ぶことも多い。なお、共有されているデータは完成されたブロックチェーンだけでなく、「ブロック」になる前の「取引」なども含まれる（承認前の取引の意味であり、詳細は後述する）。また、「分散型」は銀行によるデータの独占のような「中央集権型」「集中型」の対義語となっている。

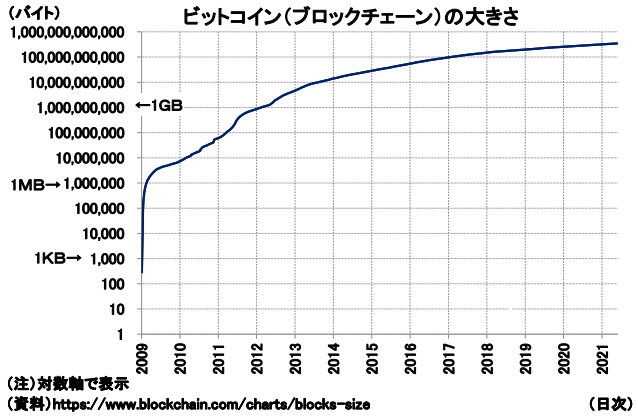
する（図表 4、当然ながらビットコインが生まれてから時間が経過し「取引」が増えるほどに容量はどんどん増えていく。実際、筆者は約 7 年ぶりにビットコインのクライアントを起動させてみたが、容量不足で起動できなかった。7 年前のビットコインの容量は 20 ギガバイト弱であった）。

350GB のデータを大きいと思うかは人によるだろうが、暗号資産とは何か、という問いに対するビットコインの場合の回答は、この大きなデータの塊である。

（図表 3）



（図表 4）



なお、上記脚注 3・4 で少し触れたように、ビットコインの保有者すべてがネットワーク参加者とは限らない。むしろ、近年は交換業者にデータの保管を委託するケースが多いと見られる。また、ネットワーク参加者でも、すべてのブロックチェーンを共有しないケース（軽量型ノード）がある。上記の「参加者」はフルノード参加者を前提に記載しており、保有者のなかでもはブロックチェーンが共有されている層（一部共有も含む）と、共有されていない層がある点を補足しておきたい（なお、フルノード参加者は「マイニング」にも参加している）。

共有されていない層（例えばブロックチェーンの管理を業者に委託している人）にとっては、自分に関連するデータを業者に照会することになる（銀行口座の残高を問い合わせるようなものである）。

また「分散型」と言う特徴も、参加者間におけるデータの共有という意味で用いており、交換業者にデータの保管を委託している人はデータを保有している訳ではない。

3――「マイニング」とは何か

さて、ここまでビットコインのデータイメージについて大まかに説明してきた。ここからは、いよいよ「マイニング」について説明したい。

> By convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. This adds an incentive for nodes to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them. The steady addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended.

上記は、ビットコインを考案したとされるサトシ・ナカモトの論文からの引用である[7]（太字・下線は筆者）。

下線部分を意訳すれば、

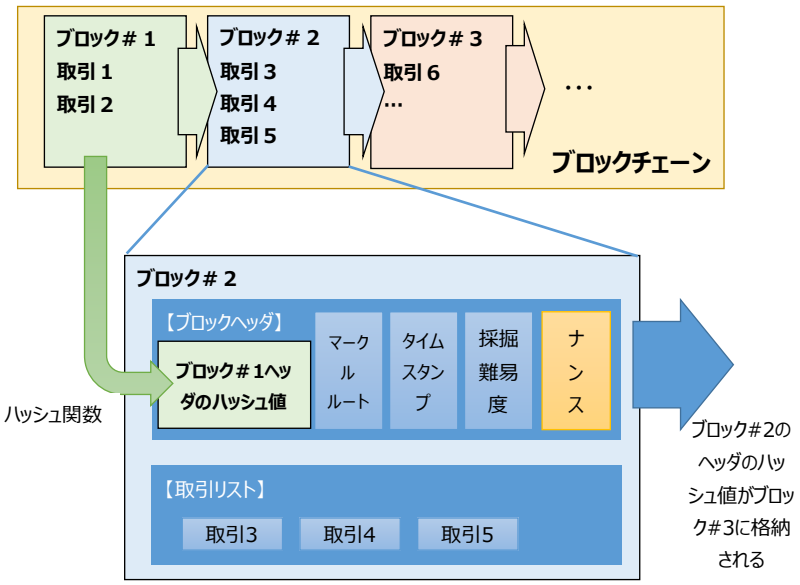
「ブロック」を作成した人が「新しいコイン」を得る事ができ、この「新しいコイン」を安定して獲得し続けることは、採掘者が金を掘って金を流通させていくことに似ている。我々の（コインの）採掘ではＣＰＵの時間と電力が使われる

となる。このサトシ・ナカモトの論文の比喩表現を用いて**今日でも「ブロック」を作成する試みのことを「マイニング」と呼んでいる**と見られる。したがって、マイニングを理解するには、「ブロック」の作成について理解できれば良いことなる。そして、**「ブロックが作成される」ことは、そこに含まれている「取引」の「承認」である**ため、重要な仕組みである。

つまり、この「ブロック」作成の仕組みを理解することが、「ＡからＢへの送金（移転）取引はどのように承認されているのだろうか、不正取引をどのように防いでいるのだろうか」の手がかりになる。

図表１に書いた「ブロック」では、「ブロック」を構成するものは数本の取引だけであったが、実際の「ブロック」にはより多くの情報が記載されている。図表５のように、「ブロックヘッダ」と呼ばれる部分を持ち、この部分がとりわけ重要で、いくつかの情報が付加されている。この情報は、具体的には「親ブロック（図表５の場合はブロック#1）ヘッダのハッシュ値」「マークルルート（Merkle Root）」「タイムスタンプ（Timestamp）」「採掘難易度（Difficulty Target）」「ナンス（Nonce）」である[8]。

（図表５）



（資料）筆者作成

一気に専門用語だらけになってしまったが、順に解説していきたい。

まず、「タイムスタンプ」は現在の時刻のことでイメージは湧きやすいと思われる。「マークルルート」は専門用語で聞きなれない言葉だと思われる。これも重要なデータだが、長くなるため、詳しい説明は割愛したい。簡潔に言えば「マークルルート」は「ブロック」に含まれる取引の束（図表５のブロック#2 の場合は「取引 3」～「取引 5」）から得られる、これらの取引を要約した数値と言える。「採掘難易度」はブロック生成の難しさを表した数値である。そして「ナンス」については後述したい。

そして、先頭にあるハッシュ値は「データから算出した小さな値。各データを区別・表現する目的

[7] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System

[8] これらの先頭にソフトウェアのバージョン情報も付加される。

に用いる」（Wikipedia）などと解説されているが、ブロックチェーンを理解する上では重要な概念と思われるので、例（イメージだが）を挙げて説明してみたい。

そこで、ここでは次のような関数を考えてみる（なお、これはあくまでもハッシュ値のイメージのために筆者が勝手に作成したアルゴリズムで、ビットコインに使われているハッシュ値とは全く関係ない）。

与えられた数値に対して、各桁の数を足し合わせて、その数値でもとの数値を割ったあまり（☆）

例えば、「12345」という数値に☆を適用してみる。まず各桁の数を足し合わせて「1+2+3+4+5＝15」である。次にもとの数値をその 15 でわるので、「12345÷15＝823 あまり 0」となる。したがって「12345」のハッシュ値（ここでは「☆値」と呼ぶことにする）は「0」となる。もとの数値を 1 だけ増やして「12346」として適用してみると、「1+2+3+4+6＝16」となり「12346÷16＝771 あまり 10」なので☆値は「10」である。このように、☆値は元の数値より小さく、元の数値を少し変えただけで☆値が大きく変わることがある。これは（☆値ではない）一般的なハッシュ値にも言える性質である。

さて、ここで再び図表 5 の「ブロック#2」を考えていこう。ヘッダを構成する「ブロック#1 ヘッダのハッシュ値」「マークルルート」「タイムスタンプ」「採掘難易度」「ナンス」はすべて数字である。そこで例えば「ブロック#1 ヘッダのハッシュ値」を「6」、マークルルートは「345」、タイムスタンプは「0525」、採掘難易度は「1」としてみよう[9]。

そうすると、ブロック#2 のヘッダ部分は「634505251???」という数値になる。

ここで、最後の「???」に相当する「ナンス」については説明していなかったが、マイニングでは実はこの数値が重要である。「ナンス」の数値は外部から与えられるものではなく、**「ナンス」はネットワーク参加者（採掘者）が探しあてる数値である**（図表 5 で「ナンス」を黄色にしているのは金発掘のイメージのため）。

では、採掘者はどのような「ナンス」（「???」の数値）を探しているのだろうか。それは、ブロックヘッダからハッシュ値を計算したときに、そのハッシュ値が閾値（target）を下回るような「ナンス」である。この閾値を下回るとブロックが作成される（そこに含まれる取引が承認される）。

これを具体例で示してみたい。ここでは閾値としてハッシュ値（この例では「☆値」）が 10 未満となるような「ナンス」を探している状況を想像してみる。

採掘者がナンスとして「001」を選んでブロックヘッダの「☆値」を計算してみたとする。この場合、「ブロック#2 のヘッダ」＝「634505251001」（下 3 桁がナンスで今回は「001」）となり、この☆値は 25 である[10]。☆値が 10 以上であるためブロックは作成できない。

---

[9] 親ブロックの数値は適当、マークルルートは「取引 3・4・5」が含まれていることから、タイムスタンプは「5 月 25 日」から、採掘難易度は「一番容易」ということから 1 の数値を選んだが、もちろん本物のビットコインのブロックヘッダに格納されている数値はもっと複雑である。ただし、いずれにしても数字の羅列である。

[10] 6+3+4+5+0+5+2+5+1+0+0+1＝32 で、634505251001÷32＝19828289093 あまり 25

次にナンスとして「045」を選んでみる。この場合、「ブロック#2 のヘッダ」＝「634505251045」であり、☆値は 5 となる[11]。☆値が 10 未満であるためブロックが作成できる。

したがって、「ブロック#2」は「ヘッダ部分」が「634505251045」、これに「取引リスト」が加わったものとして作成できる（前掲図表 5）。これ以外の「ナンス」でも☆値が閾値以下になるような「ナンス」であればブロックは作成できるが、どの“あたり”の「ナンス」がブロックとして採用されるかは早いもの勝ちである（1 番早く見つけられた“あたり”の「ナンス」でブロックが作成される）。

また、「ブロック#2」のヘッダである「634505251045」の☆値となった「5」は「ブロック#3」のヘッダの先頭部分[12]の数字となる（「ブロック#2」ヘッダの先頭部分が「ブロック#1」のヘッダのハッシュ値であったことと同じ）。

このように**前ブロックのヘッダ部分のハッシュ値が次ブロックに組み込まれている**ことから、ブロックがチェーン状に繋がっているイメージが持てる。そのため、このブロックの連なりがブロックチェーンと呼ばれる。そして、前のブロックが作成されてはじめて次のブロックのヘッダに格納すべき数値が分かる。そのためブロックは 1 列にしかつながらず、いわば**ブロックのハッシュ値はその前までに繋がっているブロックすべての情報が集約されているのであり、これがチェーンの役割を果たしている**と言える。

このブロック作成で重要なのは、もちろん「ナンス探し」であるが、これは**“あてずっぽう”で探すしかない**（今回の例で「☆値」をやや込み入った計算にしたのは、“あてずっぽう”でしか探せなさそうな雰囲気を出すためでもある）。

また、先ほど述べたように“あたり”の「ナンス」探しは早いもの勝ちである。早くナンスを探せた参加者（ノード）はブロックを作成し、その報酬として新しいコインを得ることができる[13]。それ以外の参加者（ノード）には報酬はなく、次のブロックでナンス探しをしなければならない。

繰り返すと、**「ナンス探し」という仕事（計算）をして“あたり”のナンスを見つけることがブロック生成であり、このブロック生成でブロックに含まれている「取引」が承認されたと見なされる**。こうした仕組みは「プルーフオブワーク（ＰｏＷ：Proof of Work）」と呼ばれている[14]。仕事をしたという証拠（“あたり”のナンスを見つけたこと）が取引を承認させているのである。取引の承認は管理者によりなされるのではなく、**「ナンス」探しという仕事（計算）の結果、ある参加者が適切な結果を得た（閾値以下の「ナンス」を見つけた）という結果でなされている**（そして後述するように、これには大量の電力を消費することがある）。

これで、前述の「ＡからＢへの送金（移転）取引はどのように承認されているのだろうか。」とい疑問の回答が得られた（回答は、「ブロックの作成によりなされている」）。ただし、まだ「不正取引をどのように防いでいるのだろうか」という疑問は解消されないかもしれない。

この疑問についても説明していきたいが、その前に、閾値の設定について触れておきたい。閾値が大きければ適当に選んだ「ナンス」が“あたる”確率は高まり、発見されやすくなり、閾値が小さけ

[11] 6+3+4+5+0+5+2+5+1+0+4+5＝40 で、634505251001÷40＝15862631276 あまり 5
[12] 実際にはソフトウェアのバージョン情報がさらに先頭につく（脚注 8 と同様）。
[13] 取引リストに含まれている取引の手数料も得ることができる。
[14] プルーフオブワークはビットコインに限らず一般的に使われる用語で、ある課題（仕事）に取り組んだこと（そして成果をだしたこと）をもって「証拠」とする（取引の承認根拠とする）という仕組みのことを指す。

れば適当に選んだ「ナンス」はなかなかあたらずに発見されにくくなることから、この閾値の調整をどうするのか、という点は重要であるからだ。

結論を述べれば、ビットコインでは、<u>10 分間に 1 回、どこかの参加者がナンスを見つける、というように難易度が調整される</u>[15]。具体的には 2016 ブロック（1 ブロック 10 分換算で 20160 分、つまりちょうど 2 週間）毎に、想定時間（20160 分）より早くブロック作成されたとすれば難易度が上がり、それより遅ければ難易度が下がるというように調整される（この難易度の数値はブロックヘッダ内にも含まれている（前掲図表 5））[16]。なお、この 10 分という時間の根拠は不明なようだが、「ブロック」がネットワーク参加者に共有されるのに必要な時間といったの意見があるようである。

したがって、ネットワーク参加者が増えたり、マイニング（「ナンス探し」）に使うＣＰＵ・ＧＰＵの性能が向上するなどして、閾値以下の「ナンス」が発見されやすくなると、2016 ブロックを作成する時間が 20160 分（2 週間）より短縮され、閾値の設定が下がり難易度が上がる。<u>マイニングには常に一定の計算時間を費やさなければならないようになっている</u>。

上の☆値は 1 桁や 2 桁の数だったが、実際のビットコインのブロックヘッダのハッシュ値の計算は SHA-2（SHA256）と呼ばれるハッシュ関数（アルゴリズム）が用いられており、その結果の数値（出力）が取り得る値は 2 進数の桁数で 256 桁、16 進数で 64 桁、10 進数だと 78 桁である。桁数（長さ）で見ると長い訳ではないが、数としては相当大きな数である[17]。

具体的に、執筆時点でのビットコインのブロック作成の閾値を見てみよう。

【ブロックヘッダハッシュの閾値（Target）】（以下 2 進数・16 進数・10 進数の 3 種類で標記しているがすべて同じ数値）
「10110011110011101001000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000」（2 進数）
「b3ce900000000000000000000000000000000000」（16 進数）
「1076379879376199359324913638762382564863378102643851264」（10 進数）

これだけ見ると、閾値も大きな数に思えるが、ハッシュ値がとりうる数と比較するとかなり小さい

---

15 したがって 10 分に 1 回新しいコインが誕生している（採掘されている）ことになる。ただし、ブロック生成で誕生する（採掘される）ビットコインは幾何級数的に減少する。ビットコインが生まれた当初（2009 年）は 1 ブロックで 50 ビットコインが報酬として与えられていたが、12 年 11 月には 25 ビットコインに半減、16 年 7 月には 12.5 ビットコインにさらに半減、20 年 5 月には 6.25 ビットコインにさらに半減している。この報酬が半減する周期は半減期と呼ばれる（実際は前回の半減期が高さ 63000 のブロック、次の半減期が高さ 84000 のブロックというようにブロック数で決まっているが、10 分に 1 ブロック生成されるよう採掘難易度がコントロールされていることから半減期が約 4 年周期であることが分かる）。

16 （「ナンス」には桁数制限があるため）難易度が高い場合、すべての「ナンス」を調べても“あたり”が見つからないという可能性もあるのではないか、と疑問を持つ人もいるかもしれない。その通りである。ただし、ブロックヘッダに「タイムスタンプ」があるため、時間が経過してこのタイムスタンプの数値が変わるたびに（たとえば 1 秒毎に）“あたり”が変わるので、延々に見つからないという事はなく、いつかは発見されるだろうという期待が持てる（本コラム上の「タイムスタンプ」の例では月日だけしか使わなかったが、実際のビットコインはもっと細かい時刻を記録している）。ちなみに、ブロックの取引リストの先頭に保管される生成取引（マイニングによる報酬として生まれた取引）にも数値を格納する部分があり、ここも「拡張ナンス（extra nonce）」として使われる。ここに数値を適当に格納することで「マークルルート」の値が変わり、（拡張ではない）“あたり”の「ナンス」が変わる。このように、計算を続ければいずれ“あたり”が見つかるという工夫もされている。

17 $\mathrm{Log}_{10}(2^{256}) \fallingdotseq 77.06$ であり、10 進数では先頭の数値が取れる範囲に制約がでる。なお、10^{12} が 1 兆、10^{16} が 1 京と数えていくと 10^{68} で 1 無量大数（一般的な数え方）となり、78 桁の数は 1 無量大数より大きい。数の表現については後述のテラやペタなども含め、安井義浩（2018）「大きな（または小さな）数字の表し方－単位の話に出てくる数の表記の仕方など」『研究員の眼』2018-10-23 が参考になる。

数であることが分かる。

例えば、2 進数でみると閾値の桁数は（上記枠内の桁数は目で数えるのは大変だが）180 桁となっている。ハッシュ値の総桁数は（2 進数で）256 桁なので、ランダムにハッシュが生成されたとして、256 桁のハッシュがおおよその閾値である 180 桁より小さい数値になれば“あたり”といえる。

この可能性を 256 桁のすべての（2 進数の）数字のうち先頭 76 桁がゼロとなる数字が見つかる割合とみなせば、確率的に $1/2^{76} \fallingdotseq 1.32\times10^{-23}$ となる[18]。また、この逆数は 7.56×10^{22} となる。

つまり、現在“あたり”の「ナンス」を探すには、おおよそ 7.56×10^{22} 回のハッシュ計算（発掘作業）が必要となっていることが分かる[19]。10 分間（600 秒）で“あたり”の「ナンス」が発見されるように難易度は調整されるので、1 秒当たりでおおよそ 1.26×10^{20} のハッシュ計算（発掘作業）が行われていることになる[20]。

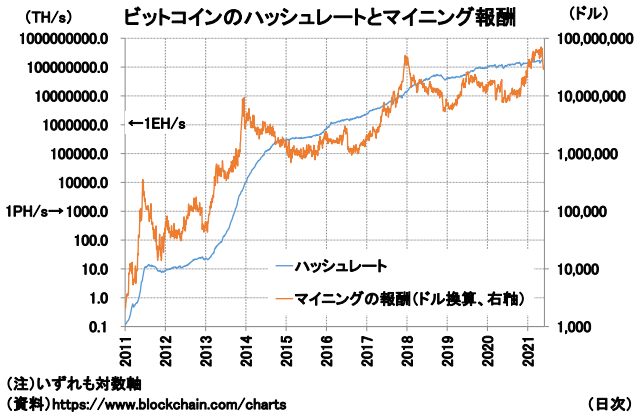
この 1 秒あたりの計算量はハッシュレート（Hash Rate）と呼ばれ 10^{12} を表す単位Ｔ（テラ）や 10^{15} を表す単位Ｐ（ペタ）、10^{18} を表す単位Ｅ（エクサ）を使い、たとえば 126EH/s（エクサハッシュ毎秒）などと表される。実際の「マイニング」に利用されている計算量は、図表 6 の通り激増している[21]。筆者の 7 年前のパソコンでは起動できたとしても、おそらく“あたり”のナンスは発見できないだろうし、宝くじを買って“あたる”可能性の方が高そうだと思える程度に“あたり”は少ない（しかし、誰かが約 10 分に一度“あてている”のも確かである）。

4――「マイニング」のメリット

さて、最後に「不正をどのように防いでいるのだろうか」という疑問について考えていきたい。

不正にはいくつか種類がある。例えば、「自分のものではない電子財布を盗んで使う」「データ上不備のある取引をする（例えば、原資より大きな金額を送金するなど、図表 1 参照）」といったことが考えられる。

（図表 6）



このうち「電子財布を盗んでしまう」という疑問は、前述の「Ａの財布にあるビットコインは持ち主でなければ使えないのはなぜだろうか」という疑問と同じであるため、本コラムでの解説は省略したい。次の「データ上不備のある取引をする」という疑問については、マイニングからやや離れることになるが、重要な点でもあるため少し解説しておきたい。

---

[18] 2 進数では各桁はゼロか 1 の 2 通り取り得るが、先頭 76 桁がすべてゼロである必要があるため $1/2^{78}$ となる。約 100 垓（京の 1 つ上の単位）分の 1 である。閾値がキリの良い数値でないため、例えば先頭 76 桁がすべてゼロでもその後の 2 桁が 11 だと閾値を超えてしまうが、そのあたりは捨象している。

[19] $2^{76} \fallingdotseq 7.56\times10^{22}$（“あたり”の「ナンス」を探すために必要な計算量）

[20] $1.26\times10^{20}\times600$（秒）$=7.64\times10^{22}$。

[21] 図表 6 で示したハッシュレートは直近で約 145EH/s であり、本文中の必要ハッシュレートよりやや大きいのは途中の確率を計算する際に捨象した部分があるためと思われる（脚注 18 参照）。

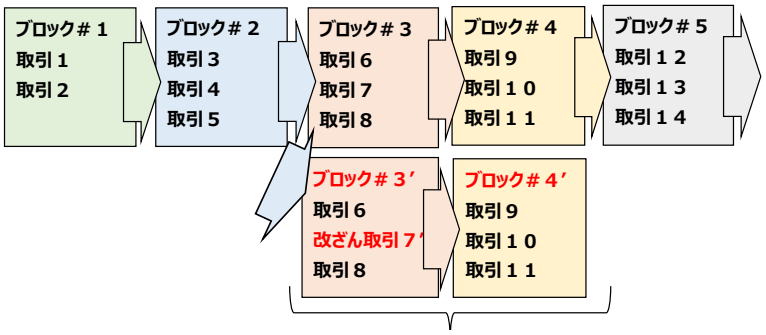
ビットコインにおいて「データ上不備のある取引」を防止させているのは、その「分散性」にあると言える。ビットコインでは、前述の通りネットワーク参加者が同じデータ（ブロックチェーンおよびブロックに取り込まれる前の取引）を持ち、同じルールでデータを更新している。そして、ルール外のデータについては取り除くようになっている。つまり、ネットワーク参加者全員がデータを管理している。したがって、例えば、原資より大きな取引を許可できるように、自分のシステムを変更したとしても、他のネットワーク参加者にそのデータが共有されたときに、他のネットワーク参加者により破棄されてしまうのである。管理者は不在だが、各参加者が管理の一環としてデータチェックを行っており、データ構造上の不備のある取引が共有されないようになっているのである。（ブロック」の作成が「取引」の承認（confirmations）と呼ばれるのに対し、他の参加者から伝送されてきた「取引」の正当性確認は検証（verification）と呼ばれる。検証は承認の前工程のとも言える。取引がネットワーク参加者から検証されているように、ブロックも各参加者同士でその正当性（データ上の不備がないか）が検証されている。）

では、「マイニング」によりブロックをチェーンとしてつなげていくメリットは何かというと、それは（過去の）データの書き換えを防ぐ、という点にある。つまり、データの書き換えという不正に対してブロックチェーンが有効に機能するのである（「耐改ざん性」「不変性」という）。

例えば、不正な取引（データ構造上の不備）が受け付けられなくても、取引を後から修正することができれば、参加者にとってメリットになることがある。例えばＡからＢにビットコインを送金（取引を作成）し、代わりになにかの商品や通貨を受け取った後でその取引とは違う取引で上書きできれば、Ａは不正に得をする（その分、Ｂは損をすることになる）。ビットコインのブロックチェーンはこういった種類の攻撃（不正）に強い。

この改ざんに強い理由は、いままで述べてきた「マイニング」の大変さにある。ビットコインでは（たまたま同じ時間に異なる参加者によって異なる“あたり”の「ナンス」が発掘されるなどして）ブロックチェーンが２つ作成されてしまった（分岐してしまった）場合、長い方のブロックチェーンを正当なブロックチェーンとみなし、短いブロックチェーンは破棄されるようになっている。

（図表７）



（資料）筆者作成　　長短２つのブロックチェーンが作られた場合、短いブロックチェーンは破棄されてしまう

これにより、後からのデータの書き換えがとても大変になる。例えば図表７のようなケースで、Ａが「ブロック#3」に含まれている【取引７】を改ざんしたいと思った場合を考えて見る。そのためには新しい【改ざん取引７’】の「ブロック#3’」を作成する必要がある。これは改ざん取引７’のブロックで“あたり”の「ナンス」を発掘する必要があるということである（これは「ブロック#3」の“あたり”の「ナンス」とは異なる。「マークルルート」と「タイムスタンプ」の数値が異なっている可能性が高いためである）。さらにこのブロック#3’はブロック#4 にはつながらない（「ブロック#4 ヘッダ」の先頭にある値は「ブロック#3 ヘッダのハッシュ値」であり、それを前提に発掘された“あたり”

の「ナンス」となっている)。したがって、ブロック#3’に続くブロック（ブロック#4’）を作成する必要がある。これには、ブロック#4 の“あたり”の「ナンス」を別途発掘することが必要になる（そして、このブロック#3’に続くブロックの“あたり”の「ナンス」は、ブロック#4 の“あたり”の「ナンス」とは異なるため、新たに計算しなおさなければならない)。

書き換えを成功させるには、攻撃者以外の参加者で作成しているブロックの高さを超えるまで新しい“あたり”の「ナンス」を見つけ、ブロックを伸ばさなければならない。つまり、**データの改ざんを成功させるには、攻撃者が、自分以外の参加者全員による「ナンス」探しを上回るほどの計算力を持っている必要がある**。多くの参加者がマイニングをしている場合、攻撃者が他の参加者以上の計算力を得る可能性は難しくなる（ただし、こうしたデータ書き換えは「51%攻撃」と呼ばれ、理論的には不可能ではない)。また、**ブロック（とそれに含まれている取引）が古いほど改ざんするのは難しくなる**のである。これは不正な攻撃ではない場合も同じで、間違って取引を行ってしまった場合でも、後からキャンセルすることは困難になる。**費やされた計算力（≒電力）が耐改ざん性を保証していると言える**[22]。

逆に言えば、新しい取引ほど改ざんされる可能性は高い。特に、承認前の取引（ブロック作成までの 10 分程度）はかなり不安定である。同じ原資の別の取引を記載すると、どちらかが消えてしまうからだ。

なお、承認後であっても、既存の「ブロック」より、長い「ブロック」を伸ばすことができれば、「取引」はすべて長いブロックに含まれているものに書き換えられることになる（上述の通り、ビットコインには「残高」情報は直接的には含まれていないが、採用されるブロックチェーンが変わり、それに含まれる「取引」も変更されれば、利用可能な「残高」も変わる）

最後に、“あたり”の「ナンス」を探すのは難しいが、“あたり”のナンスがあったときにそれが“あたり”であることを確かめることは簡単であることも重要であるので触れておきたい（ハッシュ値を計算するだけである)。ビットコインでは参加者がデータを共有する際に、共有されたデータ自体が正当であることを検証するが、検証作業は発掘作業の負荷と比較すると断然容易である。この**“あたり”の「ナンス」の、「見つけにくいが“あたり”であることを検証しやすい」という性質は、参加者がデータを検証し、共有・管理する（「分散」させつつも、プルーフオブワークという「耐改ざん性」を確保する）上では重要な性質**といえる[23]。

5――おわりに

さて、ここまで「マイニング」とそれに関連する疑問について説明してきた。

結局のところ、**「マイニング」はハッシュ値の計算と、それが閾値以下（“あたり”）かという単純な**

[22] また、不正による暗号資産への信頼喪失というデメリットが攻撃の抑止となっている面がある。51%攻撃をできるほどの計算力を持った人であれば、自らの資産を毀損する攻撃はしないだろう、ということ（プルーフオブステーク（ＰｏＳ）などの概念では重要となる抑止力)。

[23] たとえば、「マインイング」が円周率の小数点以下〇桁目～△桁目の数字を計算する、という計算だったとしたら、〇桁を増やして難易度を挙げると、その“あたり”の数値を計算することも難しくなる。一方で、それが“あたり”であることを確かめることも発見するのと同じ程度に難しくなってしまうだろう。発掘は難しいが検証は簡単ということ複数のノードでデータを管理する（検証してもらう）上では重要と言える。

試行の繰り返しである。そして、この（意味がないように思われる計算に）多くの電力が使われ、マイニングの電力消費量（142.9TWH（テラワットアワー））はノルウェーの消費電力（124TWH）を上回り、世界のデータセンターで消費されている電力（205TWH）に近づく勢いのようである[24]。

冒頭マスク氏が危惧したように、「ナンス」探しという単純計算の電力を生み出すために、多くの化石燃料が費やされているとすれば、気候変動リスクを懸念する立場としては看過できないところだろう。

なぜこの単純計算にこんなにも電力が使われるのだろうか。ナカモト・サトシの「ナンス」探しという単純計算と金の発掘との比喩表現を用いれば、なぜ金の発掘は行われるのだろうか、というころになろう。

理由のひとつは、それはマイニングで得られるビットコインの報酬が魅力的であるため、と言えるだろう。そして、この魅力度を高めているのは、ビットコインがドルなどの別の通貨と交換できる、商品が購入できる、といった点にもあると見られる（金の発掘が、儲かるから行われるのと同じである）。

そのため、現在のところ、ビットコインには相当な需要があり、その需要の高さに応じた電力が使われていると見られる（電力を利用しても、電力使用料がマイニングの報酬を下回れば儲けられる）。

せっかく電力を使うのであれば、もっと有用な計算に活用できないのかといった指摘もできると思う。ただし、ビットコインによる一見“無駄”に見える電力消費でも、“無駄”とは言い切れない面がある。それは、（必ずしも電力である必要はないが）コストのかかる仕事をしているために、後から書き換えることが大変で、それが「耐改ざん性」を高めているという特徴にある。コストがかからないと「マイニング」の意味がなく、大胆に言ってしまえば**“無駄”な「マイニング」だから信頼性が高まっている**のである（それがプルーフオブワークという概念であり、実際に、「電力使用量の大きさ≒耐改ざん性の高さ」がビットコインの魅力を高めている面があると思われる）。

仮に、ビットコインの需要が低下すれば、マイニングして報酬を得たいと思う人が少なくなるだろう。「ナンス」探しに使われる計算力（ハッシュレート）が低下すれば、発掘難易度が下がり、ブロックを作成するのに必要な電力も低下する（ビットコインと同じ仕組みで動いているが、ほとんど電力が使われていない他の「暗号資産」は多いとみられる）。

ただ、図表６で見た通り、現在のところそういった需要が低下する気配は見られない。ビットコインの価格は激しく上下に動いているが、マイニングの計算量は安定的に増えている（もちろん、ＣＰＵ・ＧＰＵなどの性能が良くなっている面もあるだろうが、ビットコインの報酬がマイニング需要を激減させるほど低下していないという面も指摘できるだろう）。

なお、ビットコインはプルーフオブワーク（端的に言ってしまえば、計算力≒電力による承認）を採用したブロックチェーンの例であるが、**プルーフオブワークではない承認の仕組みを採用するブロックチェーンもある**点は補足しておきたい（電力以外の「証拠」で耐改ざん性を担保しようという仕組みといえる）。**必ずしも、ブロックチェーンとプルーフオブワークはセットではなく**、また、一部の

[24] 「ビットコインの電力消費量、多くの国々を超える水準に」Forbes JAPAN（2021/05/12）

暗号資産では既存のプルーフオブワークという仕組みから転換しようという動きもあるようだ[25]。

一方、上述の通り、電力が「耐改ざん性」を高め、信頼性につながるのであれば既存のプルーフオブワークも有用であるという考え方もできるだろうし、気候変動を危惧する視点からはクリーンな電力での発掘なら許せるという立場もあるかもしれない。どの仕組みが「良い」のかは結局、人間により判断されるのであり、将来的に生き残っていく暗号資産が結果として人間にとって「良い」と判断された仕組みということになるのかもしれない。

ビットコインのような（分散型であるため、自律的で耐障害性にも優れている）システムの仕組みを（例えばプルーフオブワークから違うものに）変更するには、すべてのネットワーク参加者が使うシステムを変更する必要があるだろう。暗号資産のシステム保守や管理を行っているコミュニティはこうした力を保有している可能性があり、政治的その他の力を使うことで、システム利用を停止することなどもできるかもしれない。こうしたシステム自体が将来的に変更されていく可能性もゼロとは言い切れない（だだし、すべてのシステムを変更する可能性について言及してしまうと“何でもあり”ということになってしまう）。

本コラムでは脚注で触れるにとどめたが、ビットコインはその発行量が決まっている（金のように希少性がある）といった性質なども後押しする形で、これまで需要は増加する一方であった[26]。現在でもビットコインに対する需要は高く、最近もＥＴＦの組成が検討されているなど、投資対象としての魅力を高めていることに鑑みれば、今後も当面は高い需要が維持されるように思われる。

ビットコインはその価格変動の大きさや、気候変動への関心の高まりにより、最近、多くの報道を目にするようになった。またＮＦＴ（非代替トークン）などの関連技術に関する報道も多くなっているように思う。今後も、こうした技術の動向に注目して行きたい。

[25] 例えば「ブロックチェーンによるエネルギーの大量消費を解消できるか：動き出したイーサリアムと「PoS」の潜在力」WIRED（2021.03.30）など

[26] ビットコインの希少性や経済的な観点からの考察は、例えば、櫨浩一（2018）「仮想通貨と経済～ビットコインを中心として～」『基礎研レポート』2018-03-30を参照。