ITI 調査研究シリーズ
No.56

仮想通貨の基礎知識

国際貿易投資研究所 客員研究員　川野祐司

2017年6月

一般財団法人 国際貿易投資研究所（ITI）
INSTITUTE FOR INTERNATIONAL TRADE AND INVESTMENT

目　次

仮想通貨の基礎知識

川野祐司　Yuji Kawano
（一財）国際貿易投資研究所客員研究員
東洋大学経済学部教授

はじめに

本稿では、Narayanan et al（2016）を主なテキストとして、ビットコイン（bitcoin：通貨記号は BTC）を例に仮想通貨の仕組みを解説する。アントノプロス（2017）は具体的なソフトウェアの動作やスクリプトを紹介しており、ECB（2015）は仮想通貨について金融、経済、金融政策の面から概観している（ただし技術的な理解がやや不足しているように思われる）。さらに、Bitcoin 日本語情報サイト（jpbitocoin.com）などのウェブページからも技術的な情報を入手でき、本章でもこれらを参考にした。統計などは各図表の出所を参考のこと。

1. ますます増える仮想通貨

仮想通貨とは一般的に、硬貨や紙幣のような実体を持たずに、通貨のような働きをするものを指して用いられているようだ。しかし、銀行預金も実体のない電子的な存在であり、我々は銀行の口座の残高という電子データ（特にネット銀行では通帳すらなく、口座の残高を物理的な形で実感することはできない）の取引をしている。一般的な意味では銀行預金も仮想通貨となる。また、マイルなどのポイントや Suica などの電子マネーも仮想通貨ということができる。ECB（2015）では、中央銀行、信用機関、電子マネー機関が発行に関わらず、通貨の代替として用いられるデジタル形式の価値を持つもの、としており、この定義では銀行預金などが仮想通貨から除かれる。

本稿でも仮想通貨の範囲を、ビットコインなどに限定する。自らを担保する経済的価値を持っておらず、人々が通貨として認めて用いることで市場価値を持つというネットワーク外部性に支えられている。法定通貨ではなく、法定通貨との交換も保証されていない。既存の金融サービスにはない利便性のため多くの人々に利用されるようになったことで、市場価値を持つようになってきている。ビットコインの成功以降、仮想通貨は増え続けている。

現在は誰でも仮想通貨を発行することができ、発行をサポートするサービスもある。図表 1 は主な仮想通貨を示している。

図表 1　おもな仮想通貨（発行額上位 10 通貨）

通貨名	通貨記号	発行額（USD）	為替レート（対 USD）
Bitcoin	BTC	35,044,379,839	2142.56
Ethereum	ETH	15,792,537,000	171.67
Ripple	XRP	8,691,434,732	0.227231
NEM	XEM	1,827,045,000	0.203005
Ethereum Classic	ETC	1,535,263,323	16.68
Litecoin	LTC	1,290,139,584	25.15
Dash	DASH	819,395,756	111.90
Monero	XMR	539,441,794	37.12
Bytecoin	BCN	478,891,590	0.002618
Golem	GNT	414,978,256	0.503082

（出所）https://coinmarketcap.com/ より。2017 年 5 月 28 日のデータ。

ビットコインをはじめ仮想通貨には、日本円（JPY）、ユーロ（EUR）のような通貨記号が付けられており、仮想通貨の取引所で利用されている。ビットコインの発行額は約 350 億ドルと他の仮想通貨を引き離している。上位 6 通貨が発行額 10 億ドル以上、29 位までが発行額 1 億ドル以上、上位 93 位までが発行額 1,000 万ドル以上、上位 223 位までが発行額 100 万ドル以上となっている。仮想通貨は金や現金などの準備資産の裏付けがなく発行されていることを考えると、100 万ドル以上の価値を持つ通貨が 200 種以上あるというのは驚くべき現象ではないだろうか。市場価値を持つ通貨は 660 通貨に及び、全通貨の発行額の合計額は約 724 億ドルであり、急速に増加している（2017 年 5 月末からの 1 週間で、全通貨の合計で約 200 億ドル分増えている）。

仮想通貨の多くは暗号化技術を使っているため、暗号通貨（cryptocurrency）とも呼ばれる。仮想通貨の取引はインターネット上で行われるため、暗号化によるセキュリティの確保が欠かせない。仮想通貨は暗号化技術、ネットワークプロトコル、PC 処理速度などの進展により実現化した。ちなみに、ビットコインの取引データの送受信は暗号化されていない。仮想通貨とブロックチェーン技術はセットにして語られることが多いが、全ての仮想通貨がブロックチェーンを用いているわけではない（6. を参照のこと）。

ビットコインのアイデアは、Satoshi Nakamoto（以降、Satoshi[1]）により 2008 年に発表された。わずか 9 ページの論文からビットコインは生まれた[2]。その後、Satoshi が 2009 年 1 月 3 日に一番初めのブロック（#0：genesis ブロックとも呼ばれる）を生成し、その次のブロック（#1）は 1 月 9 日に生成された。ビットコインではブロックチェーン技術を使っており、各ブロックにはナンバー（高さ）が振られている。以降、約 10 分に 1 つのペースでブロックが積まれている。当初はビットコインの生成のみで振り込みなどの取引はなかったが、ブロック#181 で取引が実施されている。ブロック#181 では Satoshi 自身が以前取得したビットコインを 2 つのアドレスに分けたと考えられる取引が記録されている。この時に使われたビットコインアドレス（ビットコインの口座に相当、10 ページ）は「12cbQLTFMXRnSzktFkuoG3eHoMeFtpTu3S」で、その後もビットコインの受け取りに用いられており、2017 年 5 月 1 日までに 37 件の取引で用いられている。その後も断続的に Satoshi 自身の取引と思われるものがあり、2 つのインプットと 1 つのアウトプット、1 つのインプットと 2 つのアウトプットなどの取引が行われている。いくつかのパターンを試しているように見える。

当初はビットコインには Satoshi だけが参加していたが、徐々に参加者が増えていき、現在は仮想通貨の代表格になった。

2. ブロックとブロックチェーン

ブロックチェーンは、積み上げられたブロックのことである。ブロックチェーンはビットコインの参加者（ノードという）がそれぞれ保存しており、1 つのノードがブロックチェーンのデータを失ってもすぐに他のノードからデータをコピーできる。これが分散型といわれるゆえんであり、外部の攻撃者が同時に複数のノードが持つデータを消失させてもすぐ

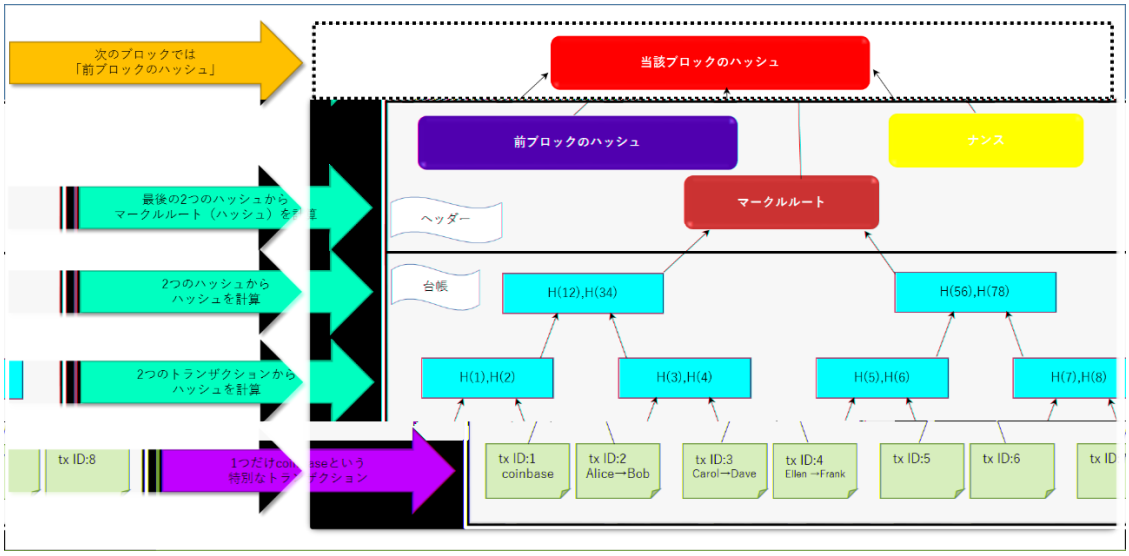
[1] Satoshi Nakamoto を名乗る人物が誰なのかについては諸説あるが、本人は名乗りを上げておらず、現在まで不明である。その理由の一つに、ビットコインの初期に Satoshi が積み上げたブロックから相当量のビットコインを得ていることが考えられる。Satoshi は 100 万 BTC を保有していると見られており、2017 年 5 月時点の為替レートで 3,000 億円相当に達する。本稿で後述するように、ビットコインの使用履歴は誰でも閲覧可能であり、ビットコイン上のアドレスと現実世界の人物とが結び付けられて特定される可能性が高い。Satoshi が保有しているビットコインは使われていないというのが一般的な説であるが、これも現実世界での特定を避けるためではないかと考えられている。

[2] Nakamoto (2008)。Satoshi はこれまで発展してきた暗号理論などをもとにビットコインを提唱している。ビットコインに用いられているすべての技術を創ったわけではない。

にコピーで復旧できるため、ブロックチェーンがネットワーク全体から消失する可能性はほぼゼロといえる。従来から利用されているデータを集中管理する方式では、集中管理サーバーが攻撃を受けることでデータ消失の恐れがある。また、管理が必要なバックアップサーバーを設置する必要があり、管理者の負担と責任が重い。ブロックチェーンはこのような管理の負担を軽減することができる代わりに、集中管理の権限も放棄している。

まずは、ブロックの構成を見てみよう。それぞれのブロックは、ブロックの特徴が記載されているヘッダーとビットコインの取引が記載されている台帳から構成されている。

図表 2　ブロックの仕組み



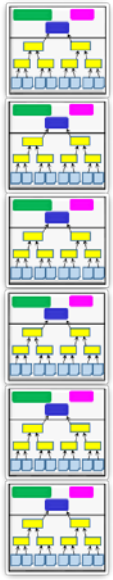
ビットコインを他の人に渡す取引をトランザクション（tx）といい、台帳部分の一番下に並べられている。図表 2 のブロックには 8 件のトランザクションが含まれているが、実際のブロックにはもっと多くの（2,000 件近くの）トランザクションが含まれている。トランザクションのうち、1 つは「coinbase」という特別なトランザクションになっており（図表 2 では tx ID：1）、このブロックをブロックチェーンにつなげたマイナー（miner：ビットコインの採掘者、1-4 を参照のこと）に対して支払われる報酬を表している。その他のトランザクションがビットコインのやり取りを表している。例えば、tx ID：2 には Alice から Bob へのビットコインの受け渡しが記載されている。この分野では「A から B に」という例文で「Alice から Bob に」という表現がよく用いられる。

台帳部分には多くのトランザクションが含まれるが、これらはハッシュという計算をすることでより短い暗号に置き換えることができる。ビットコインでは、2 つのトランザクションを組にしてハッシュを計算し、2 つのハッシュを組にしてさらにハッシュを計算するという方法を採用している。最終的にはハッシュが 1 つにまとめられることとなり、これをマークルルート（マークル木の根）という。マークルルートをチェックするだけで台帳部分の全ての取引の存在を確認することができ、マークルルートからハッシュを辿ることでそれぞれのトランザクションを検索することができる。

ヘッダー部分には、ナンス、マークルルート、前ブロックのハッシュが記載されている。ナンス（nonce：ノンスとも）とは、当該ブロックを積むために必要なパズルの答えである。マイナーはナンスを見つけることでブロックを積むことができ、coinbase トランザクションに記載されている報酬を得ることができる。ナンス、マークルルート、前ブロックのハッシュの 3 つがそろうと、当該ブロックのハッシュを計算することができる。当該ブロックのハッシュは、前ブロックからのつながり、ブロックに含まれる多くのトランザクション、パズルを解いたという証拠＝ナンスから計算されており、ブロックがビットコインのルールに基づいた手続きに従って積まれたことを表している。

このようなブロックの塊をブロックチェーンという（図表 3）。ブロックは 2009 年より約 10 分に 1 つ積み上げられており、2017 年 5 月末ではブロックは 46 万個数を超えている。各ブロックは 1 つ前（1 つ下）のブロックの情報を含んでいるため、単に積み上げられているだけでなく、情報がつながっている。そのため、例えば 1,000 ブロックさかのぼってブロックを書き換えようとすると、1,000 ブロック全てのハッシュを書き換えなければならず、非常に手間がかかる。この手間がブロックチェーンの安全性に寄与している。

図表 3　ブロックチェーン

#450005 #450004 #450003 #450002 #450001 #450000		左図のように、新しいブロックが古いブロックの上に積み重なっていくイメージから、ブロックの番号が「高さ」と表現されている。 古いブロックと新しいブロックは、ブロックのハッシュ値によって紐づけられており、新しいブロックには古いブロックの全ての情報が含まれている。ブロックに含まれるトランザクションの数に関わらずブロックのハッシュは同じ文字列の長さになる。 ブロックチェーンは 2 つに分岐することもあり、フォークという。フォークについては 23 ページを参照のこと。

2.1 ハッシュ関数

ブロックにはハッシュ（またはハッシュ値）という言葉が多く出てくる。ハッシュはハッシュ関数から計算された数値を表しており、ハッシュ関数（Hash function）とは、文字列や数値を入力するとハッシュ値と呼ばれる一定の文字数を持った数値に変換する関数をいう。この数値を 16 進法 [3]に変換して表示すると、入力に対して一定の長さのランダムな文字列が出力されたように見える。

ビットコインでは SHA-256 というハッシュ関数が用いられている。SHA-256 は図表 4 のように入力した文字列を 256 ビットの数値（16 進法では 8×8 文字で 64 文字）に変換する。

[3] 10 進法では 1 つの桁に 0-9 までの記号を使うが、16 進法では 1 つの桁に 0-f までの記号を使う（9 の次は a、b と続く）。16 進法での 10 は 10 進法で 17 を表す。PC プログラミングの世界では、00-ff（10 進法では 0-256）までを 1 まとまりとして扱っており、この 1 まとまりを 1 バイトという。16 進法の数値であることを表すために、数値の前に 0x をつけることもある。このルールを使うと、10 進法の 20 は 16 進法では 0x13 となる。

図表 4　ハッシュ関数（SHA-256）による文字列の変換

元の文字列（入力）	ハッシュ値（出力）
bitcoin	6b88c087247aa2f07ee1c5956b8e1a9f4c7f892a70e324f1bb3d161e05ca107b
bitcoim	2e4b8f2583e165a49186584e4047d7a9669a2463859647f5096e7134c4f42ccf
12c6DSiU4Rq3P4ZxziKxzrL5LmMBrzjrJX	5dbf9a64d84afb212f61aa9af27707c041ad35ccfde402674b5b6046af25de77

（出所）https://webdev.li/hash.php を利用した。秘密鍵は設定していない。

ハッシュ関数には一方向性という特徴がある。図表 4 の「bitcoin」という入力に対して、ランダムに見える複雑な文字列が出力されている。同じハッシュ関数（ここでは SHA-256）を使えば、誰が計算しても入力→出力の結果が同じになる。しかし、ハッシュ関数には逆関数が存在しないため、出力された文字列から、元の入力に戻すことはできない。また、ハッシュ関数を使うと、わずかに異なる入力から予測不可能なほど異なる出力を得ることができる。図表 4 の 2 行目の入力は「bitcoim」であり、最後の 1 文字が n から m に変化しているだけである。しかし、ハッシュ値は 1 行目とは全く異なっており、予測ができない。

ハッシュ関数による変換は予測不能であるにもかかわらず、確認が簡単に行えるという特徴がある。マイナーがパズルを解いてナンスを見つけると、マークルルート、ナンス、前ブロックのハッシュから当該ブロックのハッシュを計算できるが、この計算は誰でも簡単に追試できる。しかし、攻撃者がトランザクションの一部を変更しようとすると（Alice から Bob への支払いを、Alice から攻撃者への支払いに書き換える）、ハッシュ値であるマークルルートが大きく変化してしまうため、書き換えが簡単に発覚する。

ハッシュ関数による変換が予測不能であるということは、偶然、異なる 2 つの文字列の入力から同じハッシュ値が出力される可能性もあり、これを衝突（collision）という。しかし、SHA-256 が取り得る値は 2 の 256 乗個であり、10 の 77 乗に相当する非常に大きな数であるため、現実的な問題として攻撃者がランダムに文字列を選んでハッシュを計算しても意味がない [4]。SHA-256 は SHA-2 世代のハッシュ関数であるが、その前の SHA-0 や SHA-1 世代のハッシュ関数の安全性は疑問視されている。技術の発展や攻撃方法の洗練に

[4] 1 秒間に 1 京回の攻撃を 1 兆台の PC で並列して行ったとしても、3.7×10 の 41 乗年かかる。宇宙の歴史は 10 の 10 乗年であるため、事実上、攻撃は成功しない。

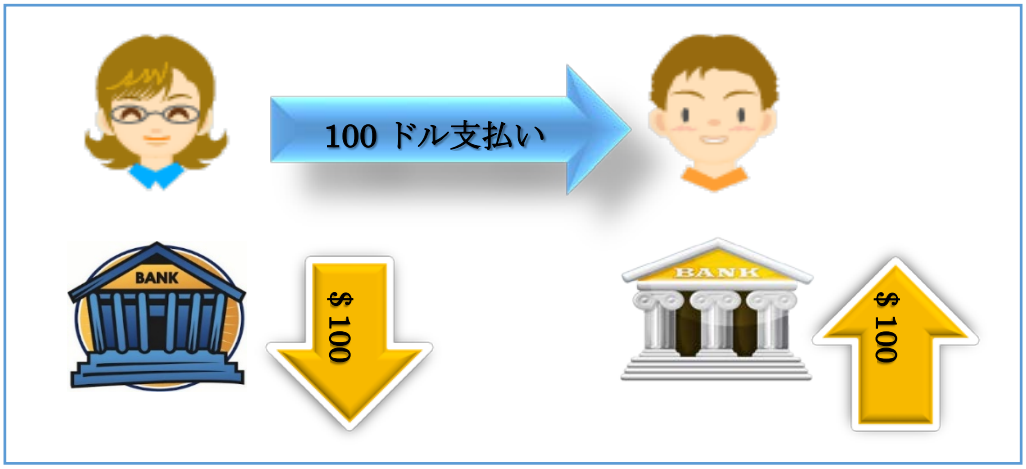
より、SHA-256 が将来に渡って安全とは言い切れないため、新しい仮想通貨の中にはさらに安全性の高いハッシュ関数を採用しているものもある。

ビットコインでは、ハッシュ関数 SHA-256 は二重に使われる 5。一度ハッシュの計算をした後に、その計算結果をもう一度ハッシュ関数にかけている。1 回でも復元が不可能であるが、2 回ではさらに復元が難しくなる。

3. ビットコインの取引（トランザクション）

ここでは、ビットコインのトランザクションがどのように行われているのか見ていく。まず、ビットコインはトランザクションモデル（transaction-based model）であり、アカウントモデル(account-based model)ではないことから始めよう。銀行預金や証券会社の MRF（マネー・リザーブ・ファンド）などは、また、貯金箱に貯めた硬貨も含めて、保有者と保有残高がペアで記録されている。Alice が Bob に 100 ドルを支払うときには、Alice の口座（財布でもよい）から 100 ドルが減少して、Bob の口座が 100 ドル増える。つまり、資金の移動は口座（アカウント）の残高の増減で表現されており、我々はこのようなアカウントモデルに慣れている（図表 5）。

図表 5　アカウントモデルでの支払い



ビットコインでは Alice がインプット（支払い）として自分のビットコインアドレスを提

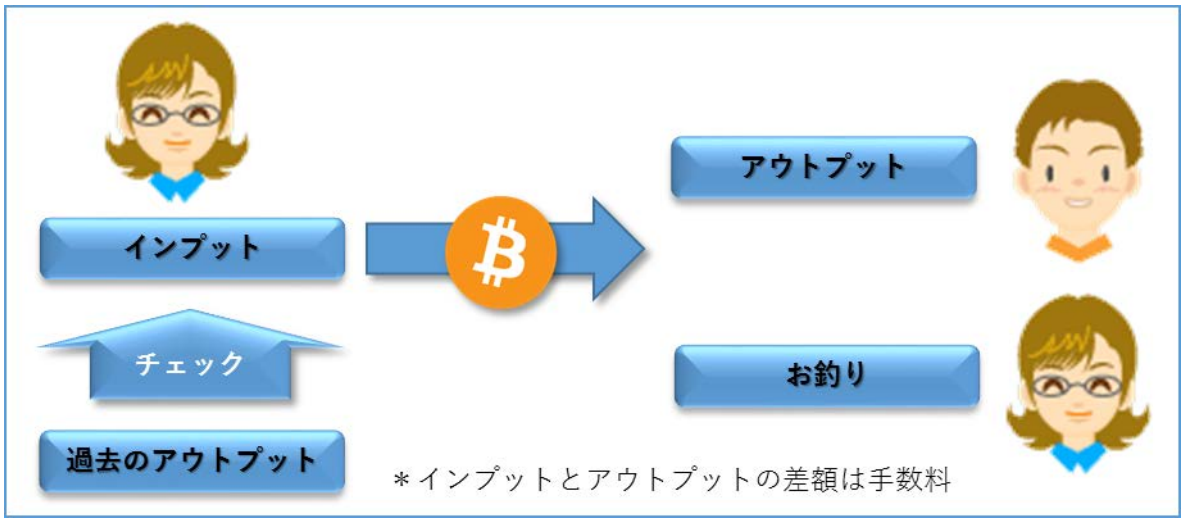
[5] SHA256［SHA256（引数)］のようにプログラムされている。

示し、アウトプット（受け取り）として Bob のビットコインアドレスを指定する。インプットするビットコインの金額とアウトプットするビットコインの金額も提示しておく。Alice がインプットに充てることができるのは、過去にアウトプットとして自分が受け取ったビットコインアドレス（UXTO という、詳しくは 9 ページ）に限られる。

ビットコインではビットコインアドレスに入っているコインの一部だけを支払いに充てることはできない。そのため、4BTC が入っているアドレスから 1BTC だけ Bob に支払う場合には、1BTC を Bob に、3BTC を「お釣り」として自分（Alice）のアドレスに支払う形にしなければならない。アドレスに入っているビットコイン全てを Bob に支払うのであればお釣りは不要になる。

ビットコインの支払いには手数料（transaction fee）が必要となる 6。手数料はインプットの金額とアウトプットの金額の差額で表現されるため、お釣りを少し少なく設定してマイナーに手数料を支払う（図表 6）。

図表 6　トランザクションモデルでの支払い



図表 7 でトランザクションを具体的に見てみよう。図表 7 はブロック#468557 に実際に含まれているトランザクションである。ビットコインや専用アプリを保有していなくても、

6　トランザクションのプログラム（スクリプト）のサイズが小さい（1,000 バイト以下）、全ての支払いが 0.01BTC 以上、優先度が高い（処理されずに長く残っている）という 3 つの条件を満たすとトランザクションフィーは不要になる。しかし、トランザクションを円滑に進めるためにマイナーに対していくらかのトランザクションフィーを払うのが慣例になっている。トランザクションフィーが高ければ高いほどマイナーが処理してくれる可能性が高くなる。

誰もがブロックの中身を見ることができ、受け取りや支払いの全記録を見たり検索したりすることができる。1 つのトランザクションには、トランザクションハッシュ、インプット、アウトプットが記載されている（この他には電子署名も記載されている）。

トランザクションハッシュは ID の役割を果たしている。ブロック#468557 には 1986 件のトランザクションが含まれているが、ID で区別できる。この ID が分かれば、ブロック番号が分からなくてもどの高さのブロックに含まれているのか、https://blockchain.info/などで簡単に検索できる。

図表 7　ビットコインのトランザクション

トランザクションハッシュ： 75c0655a39af050ae1c53dcc9b1a64d652fa17d50ccf3757832eb6ba10777d82		
インプット（支払い）		アウトプット（受け取り）
178BzARKjkszrTyx4TxBKHhzGLZijdE26e	→	1GQSnzh9JRgipxC7btKvD3rBS8Zj8SVnAo
0.06BTC		0.019BTC
	→	178BzARKjkszrTyx4TxBKHhzGLZijdE26e
		0.04BTC

（出所）データは https://blockchain.info/　より。

インプットとアウトプットには複雑な文字列が並んでいる。この文字列はビットコインアドレスであり、口座番号に相当する。数字、アルファベットの大文字と小文字から、間違いやすい 0（ゼロ）と O（大文字のオー）、l（小文字のエル）と I（大文字のアイ）の 4 文字を除いた Base58 というコードが用いられている。ビットコインアドレスは、通常は 1 から始まる[7]。

図表 7 では、インプットから 0.06BTC が払い出されている。ビットコインの補助単位として、mBTC（ミリビットコイン：1mBTC＝0.001BTC）、μBTC（マイクロビットコイン：μBTC＝0.000001BTC）、satoshi（サトシ：1satoshi＝0.00000001BTC）があり、1satoshi は 1 億分の 1BTC である。ビットコインのプログラム上では、ビットコインの計算は satoshi 単位で行われている。2017 年 5 月下旬時点では、1BTC≒30 万 JPY であるため、0.06BTC は約 18,000 円に相当する。

[7] pay-to-script-hash（P2SH）と呼ばれるアドレスは 3 から始まる。最もよく使われるのはマルチシグネイチャという機能（11 ページ）である。

アウトプットには 2 つのアドレスが記載されている。1 行目は支払先と思われるアドレスであり、0.019BTC が支払われている。2 行目はインプットと同じアドレスであり、「お釣り」を自分のアドレスに戻している。2 つのアウトプットを足すと 0.059BTC となり、インプットよりも 0.001BTC 少なくなっている。この差額に相当する 0.001BTC がトランザクションフィーである。ビットコインでは、インプットされた金額はすべてトランザクションに取引に使われてしまう。お釣りのアドレスを指定し忘れると、このケースでは 0.041BTC を手数料として支払うことになってしまう。

図表 7 ではお釣りのアドレスとしてインプットと同じアドレスが使われているが、これは安全上問題がある。先述したようにブロックチェーンではすべての取引が誰でも閲覧できる。図表 6 のインプットに使われているアドレスは、2016 年 12 月から 2017 年 5 月までの間に 3,410 件の取引に使われており、多くが少額取引であることから、寄付などの受け取り用のアドレスだと推測される。ビットコインは匿名性が高いといわれることもある。しかし、悪意ある攻撃者がこのアドレスの使用履歴を分析し、ビットコイン取引所やオンラインショッピングのデータなどと突き合わせることができると、ビットコインアドレスと現実世界の個人（または法人）とが結び付けられることもある。ビットコインの匿名性は決して高くないという認識を持つべきである。ビットコインアドレスからの個人特定は現実的な脅威であるため、このようなリスクを減らすためにはお釣り用のアドレスを別に用意する必要がある。ビットコインアドレスは無限に生成することができるため、個人がビットコインを使う際にはお釣り用の別アドレスを使うべきである。それでも匿名性の問題が解決するわけではない。

ビットコインを使うためには、それよりも以前にビットコインを入手する必要がある。ビットコインを入手するには、取引所でビットコインを購入したり知り合いから購入したり（または譲ってもらう）する。つまり、インプットとしてビットコインを使うためには、それ以前に対応するアウトプットがなければならない。ビットコインのトランザクションはマイナーが処理するが、マイナーはブロックに含まれるすべてのトランザクションが正当なものかどうかをチェックする。正当なトランザクションでは、インプットと同じアドレスが過去のアウトプットにあり、しかもそのアウトプットは未使用の状態になっていなければならない（このようなアウトプットを unspent transaction output：UTXO）という [8]。

[8] UTXO のチェックをすり抜けることができると、同一のアウトプットを複数のインプットに使うことが

図表 8　UTXO の検索

マイナーは、インプット A と同じアドレスの UTXO：A が存在するかどうか、過去の（インプット A より下の）ブロックを検索する。UTXO：A が見つからなければインプット A は無効となり、トランザクションが削除される。

もしブロックをすべて検索してもインプット A に対応する UTXO：A（未使用アウトプット）が存在しなければ、マイナーはそのトランザクションを無効とみなして削除する。つまり、送金することができない。インプット A に対応する UTXO：A が見つかると、UTXO：A は使用済みとみなされる。この点から見ると、ビットコインの支払いは過去の自分の UTXO のビットコインを他人の（または自分の）ビットコインアドレスに移し替える操作といえる。ビットコインでは過去のアウトプットがインプットとして用いられ、口座残高という概念はない。ここから、ビットコインはアカウントモデルではなくトランザクションモデルであるといわれている（図表 8）。

UTXO は口座のような役割をしているが、UTXO の中のビットコインの金額は変更できない。UTXO から一部を取り出したり、付け加えたりすることができない。図表 9 の左側では、0.6BTC の支払いをしたいが 0.6BTC の UTXO がないため、A と B の 2 つの UTXO から合計 0.8BTC をインプットとして用い、残りの 0.19BTC（0.2BTC からトランザクションフィーを 0.01BTC 引いている）をお釣りとして戻している。ビットコインはウォレット（財布）というアプリ（または WEB サービスなど）で管理する。利用者から見ると、ウォレット内にある自分のビットコイン口座の残高が増減しているように見えるが、ウォレットは自分の過去の UXTO をすべて検索してその残高を表示しており、トランザクションがあるたびに検索をやり直して残高が変動したように見せている。ウォレットは図表 9 の左のようなトランザクションを自動で行うため、利用者が UTXO を自分で検索して選択する必要はない。図表 9 の右の取引はビットコインアドレスの統合であるが、このような取

できてしまう。この問題を二重支払い（double spending）という。二重支払いは不正行為であり、二重支払いを試みる攻撃は 1 日に数千件発生している。

引を行う意味はない。

図表 9　様々な金額のビットコインの支払い（トランザクションフィーは 0.01BTC と仮定）

2 つの UTXO から支払う	自分の UTXO を 1 つのアドレスにまとめる
	

3.1 ビットコインアドレスと署名

ビットコインのアドレスは、秘密鍵ー公開鍵の仕組みを使って生成されている。例として、非常に大きな素数を鍵として利用することを考えてみよう。例えば、14757395258967641292 7 は 193707721×761838257287 で計算される [9]。一番大きな数値を公開鍵としてビットコインアドレスに使用する。これまで見てきたように、ビットコインアドレスは誰でも閲覧することができるが、アドレスは個人情報（ここでは 761838257287 とする）を含んでいるものの、14757395258967641292 7 を見ただけではわからない。この公開鍵を開けるには、193707721 という秘密鍵が必要になり、14757395258967641292 7÷193707721 を計算すれば隠されたデータ 761838257287 を簡単に取得できる。しかし、秘密鍵を知らない攻撃者は、14757395258967641292 7 を 2 で割る、3 で割る、4 で割るという計算を繰り返して秘密鍵を探すしかない。秘密鍵があればより大きな素数をかけることで新たな公開鍵（ビットコインアドレス）をいくつでも生成することができ、ブロックチェーンの台帳に書き込んでも個人情報の漏洩の心配がない。現在は PC の計算能力が非常に高いため、このような素数の掛け算による公開鍵は用いられておらず、楕円曲線デジタル署名アルゴリズム（ECDSA）という方式が用いられている。秘密鍵は 256 ビットの大きさを持つため、秘密鍵を決めることは 0 から 2 の 256 乗の間の数値をとることと同じことになる [10]。この秘密鍵に ECDSA の計算を適用し、さらに SHA-256 と RIPEMD-160 というハ

[9] この数値はメルセンヌ数（$M_{67}=2^{67}-1$）である。

[10] この範囲のうちどの数値を採用するかはランダムに決められるが、ランダムに決めるというのは非常に難しく、暗号学的に安全な疑似乱数発生器（CSPRNG）を用いる必要がある。

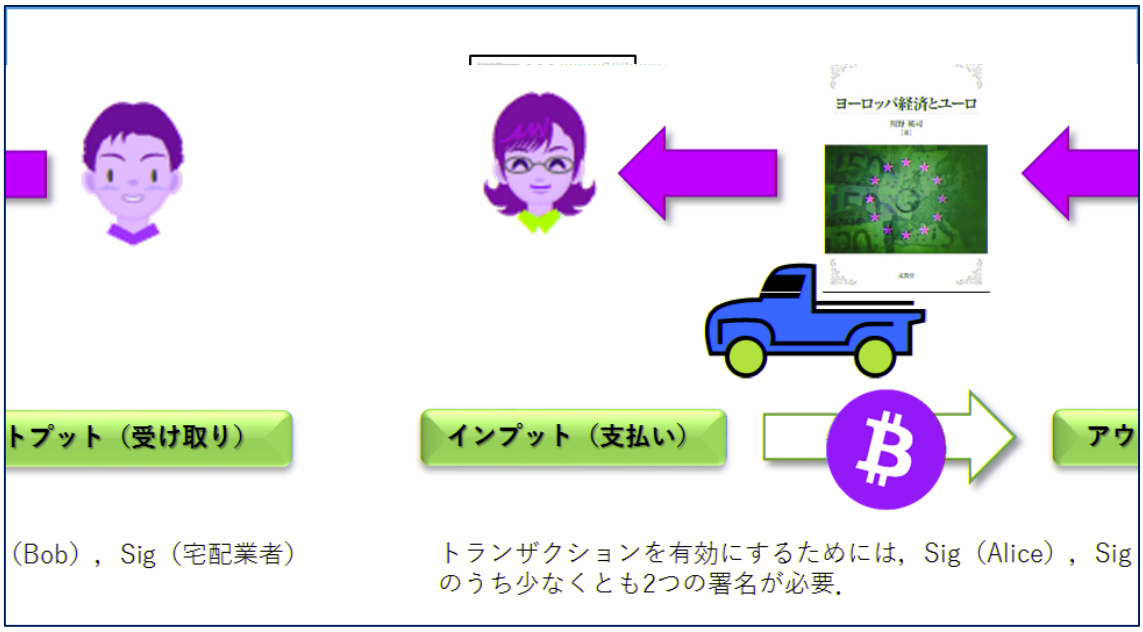
ッシュ関数によって、RIPEMD160［SHA256（公開鍵）］という計算をしてビットコインアドレスを作っている。複雑な方式ではあるが、秘密鍵を使って公開鍵を開けてデータを取り出す基本的な仕組みは先ほどの素数の例と同じである。1 つの秘密鍵からいくらでも公開鍵を創り出すことができるため、数多くのビットコインアドレスを 1 つの秘密鍵で開けることができる。秘密鍵の漏洩はすべての公開鍵のデータの漏洩につながるため、秘密鍵の管理は非常に重要である（21 ページ）。

なお、ビットコインアドレスの中には、1Kawano33u3DQm13TccujQQMmycGVx2oScx のように 1 の次にくる数文字を覚えやすい文字列にしているものもある。このようなアドレスを vanity アドレスという。この例の vanity アドレスを作るためには、秘密鍵をランダムに選んで公開鍵の計算をして、たまたまこのようなアドレスが出るのを待つ。ビットコインアドレスには 58 文字（Base58）が使われるため、6 文字の vanity アドレスを作るためには、計算を 58 の 6 乗回（約 380 億回）試す必要がある。

ブロックの台帳部分に書き込まれた、Alice が Bob にビットコインを支払うトランザクションが本当に Alice によって作られたのか、それとも攻撃者が Alice を装ってトランザクションを作ったのか、確認する必要がある。このような確認のために、トランザクションには電子署名（シグネイチャ）が含まれている。電子署名も秘密鍵から作られる。

ここで、Alice が Bob の運営するオンライン通販サイトで書籍『ヨーロッパ経済とユーロ』を購入するケースを考えてみよう（図表 10）。初めての取引で互いに相手が信頼できないと考えている場合、Alice は本が手元に届くまではビットコインは手放したくないと考え、Bob は本を発送する前にビットコインを手に入れたいと考えるだろう。もしかしたら Alice は本を受け取ってもビットコインは支払いたくないと考えているかもしれない。このようなケースでは、マルチシグネイチャという仕組みが用いられる。1 つのトランザクションの中に、Alice、宅配業者、Bob の 3 つの署名を書き込んでおき、この 3 つの署名のうち少なくとも 2 つが有効にならないとトランザクションが実行されない仕組みである（このケースを 2 of 3 multi signature という）。

図表 10　マルチシグネイチャ



Bob が本の発送前にビットコインを受け取ろうとして Bob の署名を有効にしても、有効数が不足している。Alice が本を受け取ってから署名を有効にするか、宅配業者が本を Alice に引き渡す時に署名を有効にするかしなければ、Bob はビットコインを手に入れられない。また、Alice が本の代金支払いを拒否しようとしても、Bob と宅配業者が署名を有効にすることでビットコインの取引が完了する。Alice と Bob の両者が誠実に行動すれば宅配業者の署名は不要になるが、マルチシグネイチャを用いると、誠実な取引者の保証がなくても正当な取引を成立させることができる。ビットコインでは必ずしもすべての参加者が誠実である必要はなく、誠実か不誠実か不明であっても円滑な取引が行われるような工夫が凝らされている。

トランザクションは作られただけでは意味がなく、トランザクションをビットコインのネットワークに通知する必要があり、通知をブロードキャスト（broadcast）という。ブロードキャストされたトランザクションがマイナーの手によってブロックの台帳部分に取り込まれ、ブロックチェーンの一部になることで取引が完了する。次に、マイナーについて見ていこう。

4. マイニング

ビットコインのネットワークへの参加者をノードという。ノードについては人というよりも、PC、スマートフォンなどの端末をイメージする方がいいだろう。ビットコインのネットワークはピア・トゥー・ピア（peer to peer：P2P）ネットワークであり、ノードが互いにつながりあってネットワークを形成している。P2P ネットワークでは集中管理者はなく、それぞれのノードが情報を交換し合って最新情報を共有している。各ノードは 1 つまたは複数のノードとつながっているだけだが、ネットワークの最新情報は伝言ゲームのように次々に他のノードに伝わっていく。接続環境が良ければすべてのノードに情報が伝わるまでに数秒しかかからない。

PC やスマートフォンにビットコイン関連のアプリをインストールし、インターネットに接続してアプリを実行すると、PC やスマートフォンはノードになる。まずは近隣のノード（地理的に近いとは限らない）からブロックチェーンのデータをもらって最新のブロックチェーンを構築する。シャットダウンなどで PC のインターネット接続を切断するとノードとしての機能も一時停止する。再びインターネットに接続されると、近隣のノードから再び最新データをもらい、他のノードに最新データをコピーしてあげる。攻撃者が複数のノードの攻撃に成功しても、被害を受けていないノードから最新データを受け取ることができるため、ネットワークからブロックチェーンが消去されることはない。ノードはブロードキャストされたトランザクションを他のノードに伝える役割も果たしており、トランザクションがマイナーのもとに迅速に届く手助けをしている。その際、ノードは受け取ったトランザクションがビットコインのルールに従っているか、電子署名はあるかなどのチェックを行い、問題があるトランザクションは消去している。

ノードにはいくつかの種類がある。フルノードと呼ばれるノードは、ビットコインのブロックチェーンを全てダウンロードしてハードディスクなどに保存している。現在ブロックチェーンの全データは 120GB（ギガバイト）以上ある。ブロックチェーンの維持のために常に他のノードと連絡を取り合う必要があるため負担が重い。スマートフォンなどのデバイスは、SPV（Simplified Payment Verification）と呼ばれる軽量ノードとして機能しており、ブロックチェーン全体をダウンロードせずにブロックのヘッダー部分だけをダウンロードしたり、直近のいくつかのブロックだけをダウンロードしたりする。一部のフルノードはマイニング（mining）と呼ばれるビットコインの採掘に従事しており、このようなノードをマイナーという。

ビットコインでは誰もがマイナーになることができ、許可や免許はない。ブロックの書き換えやビットコインの崩壊を望む悪意のあるノードもマイナーになることができる。もちろん個人でマイニングに参加している人もいる。マイニング専用機器を数多く集めたマイニングセンターや数多くのノードでグループを作ってマイニングを行っているマイニングプールも活動している。これらのノードがビットコインネットワークを形成している（図表11）。

図表 11　ビットコインネットワーク（細線はノード間の接続）

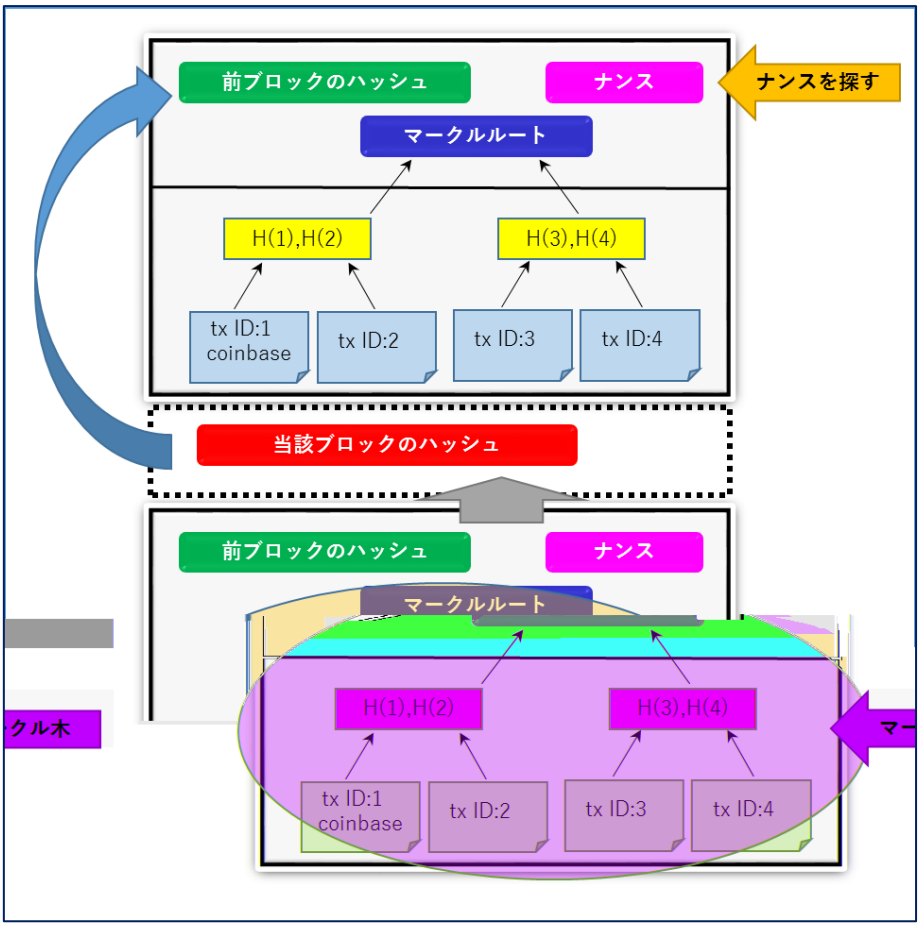
（注）この他にウォレットサービス、取引所、エスクローサービスなども含まれている。

マイナーは互いにブロックを積むための競争している。マイナーたちはナンスを見つけるというパズルに参加しており、最も早くナンスを見つけたマイナーだけが自分のブロックをブロックチェーンに積むことができ、リワード（reward）と呼ばれるブロック報酬を得ることができる。

図表 12 でマイナーの行動を見てみよう。図表 12 では下のブロックが積まれたところであり、マイナーはこのブロックが正しいかどうかを確認する。ブロックの台帳部分は木のような形をしているが、これをマークル木（Merkle Tree）という。マークル木は二分木の一種であり、データを 2 つずつペアにして処理する。自然界の木とは上下がさかさまだが、ト

ランザクションが記載されている部分を「葉」という。葉の一番左は coinbase トランザクションであり、マイナーに対するリワード（ブロック報酬）が記述されている。リワードは 50BTC からスタートし、21 万ブロック（約 4 年）ごとに半減するため、2017 年 5 月末時点では 12.5BTC となっている。

図表 12　マークル木とコインベース、ナンス



coinbase も含めて各段階で上に向かってハッシュを計算すると、最終的にはマークルルートという「根」に到達する。マイナーはこれらのハッシュを確認し、マークルルート、ナンス、前ブロックのハッシュから、当該ブロックのハッシュを検算する。ここまでの過程は非常に素早くできる。そうしてブロックが正しいことを確認すると、次のブロックを積むためのナンスを見つける競争が始まる。各マイナーは、coinbase トランザクションを作り、トランザクションプール（またはメモリープール）というまだ処理されていないトランザクションが集められている場所からいくつかのトランザクションを選んでマークル木の葉と

する[11]。ハッシュ計算をしてマークルルートを算出し、前ブロックのハッシュとマークルルートを所与としてナンスを探す作業を始める。いち早くナンスを見つけたマイナーは、ブロックを公開してブロックチェーンに積む。他のマイナーがブロックの正しさを確認すると、ブロックは正当なものとなり、次のナンスを見つける競争が始まる。

図表 13 はブロックの具体的な情報である。ブロック#468877 には 2065 件のトランザクションが含まれていたが、GBMiners というマイナーが最も早くナンスを見つけ、トランザクションフィーとブロック報酬を合わせて 15.81768445BTC を獲得している。

図表 13　ブロック#468877 の情報

ハッシュ	00000000000000000148b38dfd2d395974ad25a035b60a5375d1198430a96db
前ブロックのハッシュ	00000000000000001b48b837805e085caab620ce79712eba7749094659139de
マークルルート	8abb70271a49b3fcb067e06cb0e4e7a12ca09842ee9486a6f9e64f1baec46951
取引件数：2065	取引手数料：3.31768445 BTC
中継所：GBMiners	タイムスタンプ：2017-05-30 13:26:03
サイズ：998.753 KB	難易度：595,921,917,085.42
ナンス：72840710	ブロック報酬（リワード）：12.5BTC

ここで、ナンスのパズル計算を見てみよう。ブロックを積むためにはハッシュを計算しなければならないが、計算の難易度が設定されている。図表 13 のブロック#468877 では、難易度は約 6,000 億となっているが、2009 年にビットコインがスタートした時には難易度が 1 だったため、当時に比べてナンスの発見が 6,000 億倍難しくなっている[12]。難易度は 2016 ブロック（約 2 週間）ごとに調整されるが、この調整によりナンスの発見に平均 10 分かかる。つまり、ブロックは約 10 分ごとに 1 つずつ積まれていく。難易度は、ハッシュの先頭から決められた数だけ 0 が続く、というようにも解釈できる。#468877 時点では、0 が先頭から 17 個連続で並ぶハッシュを見つけなければならない。まずナンスに 0 を代入してハッシュを計算し、条件を満たしていなければ次にナンスに 1 を代入、次に 2 を、次に 3 をと

[11] 葉の数が奇数になってしまう場合は、どれか 1 つの葉をコピーして偶数にしてからハッシュの計算を始める。

[12] ここには記載がないが、プログラム上はターゲットという数値よりもハッシュが小さくなればブロックを積むことができる、という形式を採用している。

いうように逐次計算を続けていき、0 が連続で並ぶハッシュを探す[13]。図表 14 ではわずか 21 回の計算で 0 が 2 つ並んでおり、理論値（16×16＝256）よりも少ない計算回数でハッシュを見つけている（運が良いケースだといえる）。

図表 14　ナンスパズル

ナンス	ハッシュ値
noncepuzzle0	5214320d729950f8b19feebe49d3831e670b05b26c20642ffc89ebfb59d4c58a
noncepuzzle1	f9512a6f1af2d089a097b48599f207821e3f27ba87b84448bc4dd1dcc1b8731e
noncepuzzle2	87d4c27d160f65e5971311f5bb27dc4689ecd470957ba075c03c24130280dced
:	
noncepuzzle8	0876f321cb79c64fc20ac1f18f68562cf1c1ee35019c506531db9292175285c7
:	
noncepuzzle21	00e6db8e836412388c42bb8e67155f9b16b2470078fd0c1faead9f149579c80f

（注）前ブロックのハッシュ、マークルルート（この例では noncepuzzle で代用）の後にナンスの数字を入れてハッシュ値の計算をする。0 から始めてナンスが 8 の時にハッシュの先頭が 0 に、21 の時に 2 文字続けて 0 となった。条件（0 が連続 17 個）を満たすまでこの作業を続ける。

ハッシュには 16 進法が使われているため、先頭に 0 が来る確率は 16 分の 1 となる。ゼロが 2 つ並ぶ確率は 16 の 2 乗分の 1、つまり 256 分の 1 となる。0 が 17 個の連続で並ぶ確率は約 3×10 の 20 乗分の 1 と非常に小さい。つまり、1 つのブロック積むためには平均で約 3×10 の 20 乗回の計算が必要となる。どれくらいの計算が必要なのか見てみよう。ビットコインのマイナーが使う専用機器[14]に、13Th/s（1 秒間に 13 兆回）の計算能力がある AntMiner S9 があり、約 2,000 ドルで購入できる。この機械を使ってマイニングをすると、平均で 76 カ月（2,278 日）に 1 回の割合でハッシュを見つけてブロックを積むことができる。もちろん運が良ければ 1 日でハッシュが見つかることもあり、運が悪いと 10 年経っても見つからない。その間、専用機器は稼働させ続ける必要があり、機器の電気代（AntMiner S9 の消費電力は 1275W）や機器の冷却（冷房）の電気代、インターネット接続料金などが

[13] #468877 ではナンスは 8 桁だが、0-9999999999 の中からナンスを探す。10 桁のナンスはすぐに使い果たしてしまうが、その場合は coinbase を修正して 0 からナンスを代入し直す。coinbase トランザクションにはメッセージを書き込む領域があり、メッセージが 1 文字変わるだけでハッシュが大きく変化する特徴を利用して多数の計算を行っている。

[14] このような機器はビットコインのマイニング専用に作られており、ASIC（application specific integrated circuit：エーシック）と呼ばれている。

必要となる。マイナーになるためには、一定の初期投資や電気代などのランニングコストを負担する必要があり、運悪くブロックがなかなか見つからないと損益分岐点に達しないままマイニングを断念することにもなりかねない。

現在はブロックを積むためには膨大な計算が必要であり、デスクトップ PC などでは全くブロックを積むことができない（約 20 万年に 1 ブロックの割合）。専用機器も 1 台ではほとんど効果がないため、数千台あるいは数万台をつないでマイニングを行うマイニングセンターが稼働している。例えば、Genesis Mining は電気代の安いアイスランドにマイニングセンターを設置している。数千台の専用機器を用いてビットコインのナンスを探している。これだけの機器を動かすと、機器からの放熱で室温が 50 度近くになるため、冷房が欠かせない。アイスランドは地熱が豊富[15]で地熱発電による安価な電力が利用できるため、ハードウェアと冷房の電気代を節約できる。

4.1 マイニングプールとブロックチェーンのフォーク

図表 11 の右側にはマイニングプールが記載されている。これは、多数のノードが集まって協力してマイニングを行うグループであり、個人でマイニングをするのであればどこかのマイニングプールに参加した方がいいだろう。マイニングプールの運営は様々だが、プールマネージャーがプールの参加者にプログラムを配布してノードが手分けをしてナンスを探す。条件（先頭から 0 が 17 個）を満たすハッシュを見つけるのは難しいため、もう少し簡単なナンス（先頭から 0 が 15 または 14 個つながっているハッシュのナンス）もノードから集めて報酬の算定基準とする。このようなやや簡単なナンスはブロックを積むためには役立たないが、ノードがきちんと計算をしてプールに貢献している証拠として利用されている。プール内のノードが条件を満たすナンスを発見すれば、プールマネージャーがブロックを積んで報酬（リワード＋トランザクションフィー）を受け取り、貢献度に応じてプールメンバーに配分する[16]。

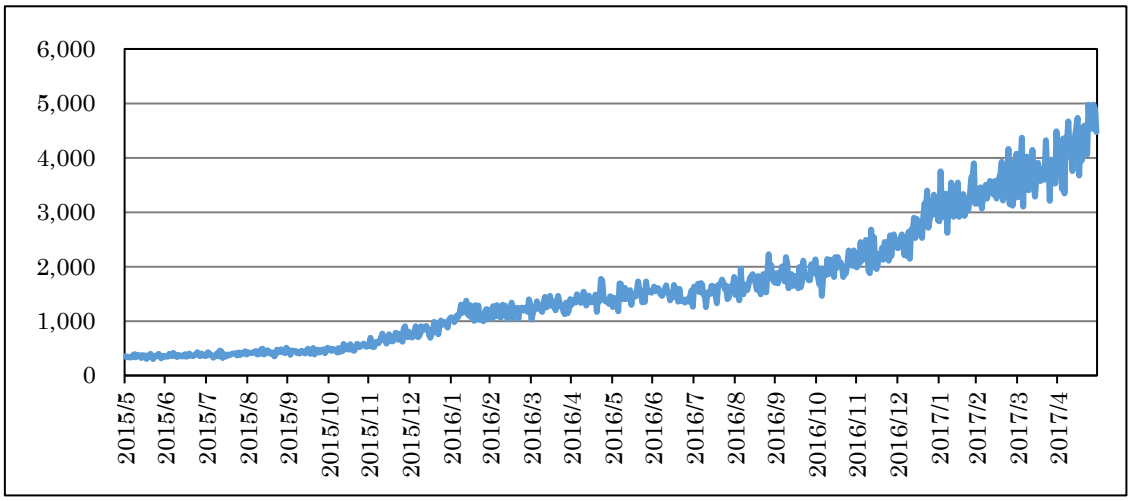
マイニングは世界を巻き込んだ競争の場であり、ハッシュパワー（またはハッシュレート）

[15] アイスランドはユーラシアプレートとアメリカンプレートの裂け目（ギャオ）に位置しており、火山国である。詳しくは川野（2016）。

[16] この時、プールメンバーがプールマネージャーにナンスを報告せずに自分がすべての報酬を受け取ることも考えられる。しかし、coinbase トランザクションにプールマネージャーのビットコインアドレスが記載されているため、プールメンバーは報酬を受け取ることができない。

と呼ばれる世界全体のマイニングの能力は日々増強されている（図表 15）。2017 年 5 月末時点でのハッシュパワーは 5,332.2PH/s（1 秒間に 533 京 2,200 兆回）であり、マイニングを続けるためには継続的な設備投資が欠かせない。

図表 15　ビットコインのハッシュパワー（単位は PH/s、1 秒間に 1,000 兆回）



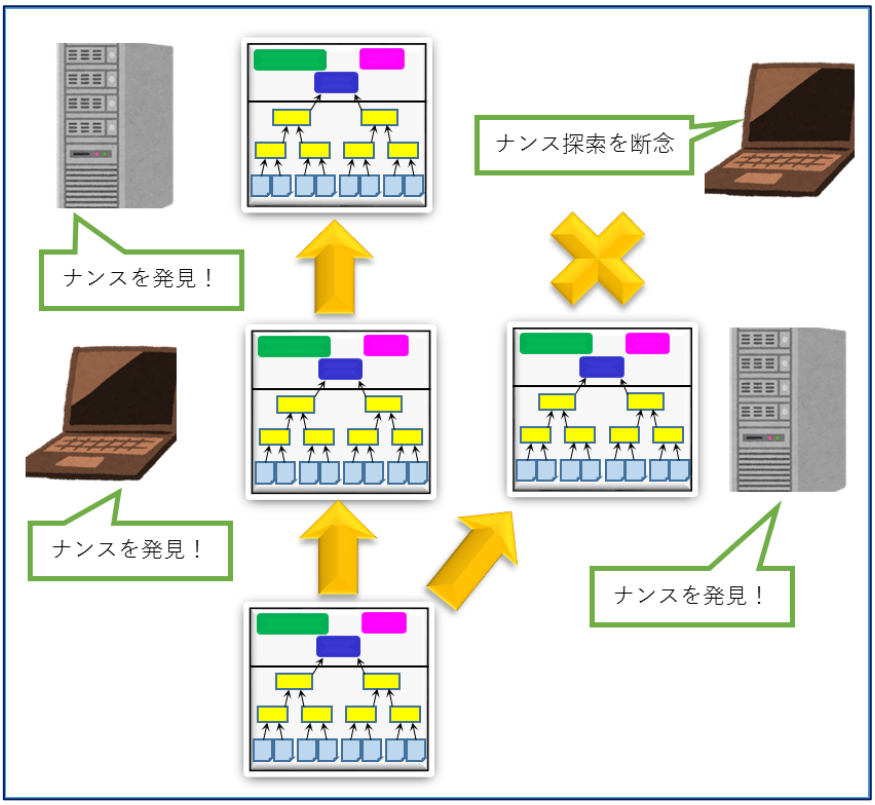
（出所）データは https://blockchain.info/

よく、ビットコインの支払いには 10 分かかるといわれている。これは、1 つのブロックが積まれるまでの時間が平均 10 分であることによる。ブロードキャストされたトランザクションは P2P ネットワークを通じてトランザクションプールに貯められる（図表 11）[17]。マイナーはトランザクションプールからトランザクションを選んでマイニング作業を始めるため、この時にマイナーに選ばれなかったトランザクションは、もう 1 ブロック待つことになる。22 ページで見るように、ビットコインの処理能力は限界に達しており、トランザクションを優先して処理してもらうためには他よりも高いトランザクションフィーを設定しなければならない（0.002BTC を超えるトランザクションフィーも見られる）。マイナーによってブロックに取り込まれたトランザクションは他のマイナーやフルノードにチェックされる。このチェック作業を承認（confirmation）という。ブロックが上に 1 つ積みあがると承認数が 1 つ増える。承認数が多ければ多いほどブロックの書き換えが困難になるため、ブロックの有効性も高くなる。

[17] Blockchain.info によると、2017 年 5 月末時点では約 88,000 件のトランザクションがプールに待機している。

しかし、ブロックチェーンはしばしばフォークと呼ばれる分岐に直面する。もしほぼ同時に 2 つのマイナーがナンスを見つけてそれぞれブロックを積むと [18]、ブロックチェーンは一時的に 2 つにフォークする（図表 16）。

図表 16　ブロックチェーンのフォーク



フォークが発生すると、マイナーはそれぞれどちらかの系列を選択し、次のブロックを積もうとする。いち早く次のブロックが見つかった系列が生き残り、他方のブロックは放置される［放置されたブロックをオーファンブロック（orphan block）という [19]］。ブロックチェーンでは最も長い系列が正当な系列であるというルールに従って形作られ、オーファンブロックに含まれるトランザクションは無効になる。オーファンブロックに含められた

[18] それぞれのマイナーが独自にトランザクションプールからトランザクションを選ぶことにより、マークルルートが変わる。また、coinbase の報酬受け取りビットコインアドレスもマイナーによって異なる。マイナーによってマークルルートが異なるため、探すべきナンスの値も異なる。そのため 2 つのマイナーから異なる計算結果（ブロック）が同時に公表されることがある。

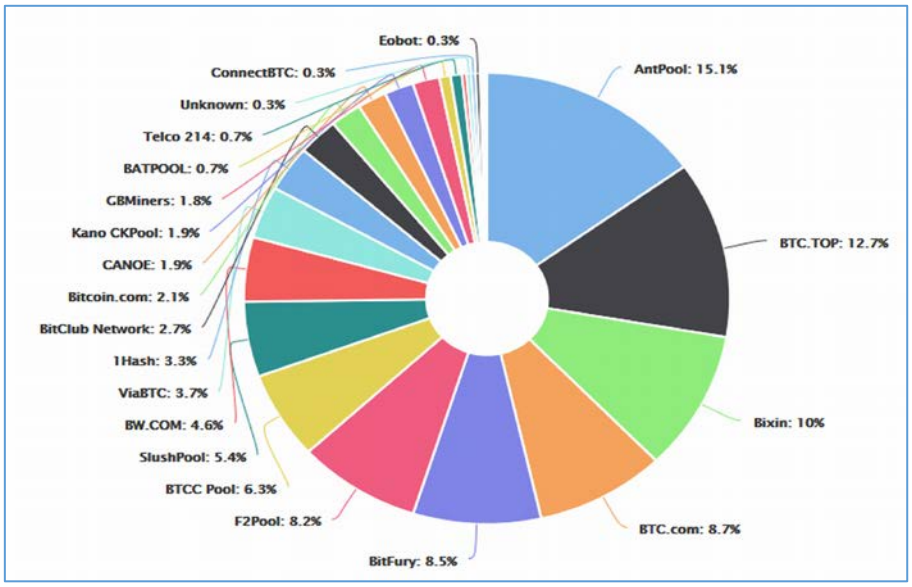
[19] Blockchain.info によると、2017 年 4 月には 6 回、5 月には 9 回オーファンブロックが発生している。

UTXO は検索の対象にならないためである。通常は他のマイナーも同じトランザクションを含めてマイニングしているため、トランザクションは正当な系列にも含まれて完全に無効になる可能性は極めて低い（ただし、トランザクションフィーを低く設定しているとブロックに取り込まれるまで数ブロック待つ可能性はある）。トランザクションがブロックに含まれてブロックチェーンにつなげられただけでは不十分で、そのブロックが正当な系列に所属しなければならない。つまり、上にブロックが続いて承認される必要があるが、ビットコインの慣習では上に 6 つのブロックがつながると（承認数が 6 を超えると）トランザクションが確定する。現在の状況で過去 6 ブロックを書き換えるためには、膨大なハッシュ計算が必要であり、かつ、他のマイナーよりも早く新しいブロックを積まなければならない。理論上はブロックの改竄が可能であっても、世界全体のハッシュパワーの増加がブロックの改竄を妨げている。承認数が 6 を超えた時点で、ビットコインの決済はファイナルになったということもできる。ビットコインはインターネット上の決済であるにもかかわらず、ファイナルまで少なくとも 1 時間はかかる、決済スピードが非常に遅い金融商品であるといえる。

ハッシュパワーの増加はブロックチェーンの安全性に寄与している。マイナー間の競争は激しく、悪意のあるマイナーが競争を勝ち抜くのは簡単ではない。複数のマイニングプールが共謀して不正行為を行うことは可能ではあるものの、マイニングには莫大な初期投資が必要になるため、ビットコインネットワークを破壊する経済的なインセンティブは乏しい。しかしその一方で、マイニングは大量のエネルギーを浪費している。Blockchain.info によると、2017 年 5 月末時点では 25 のマイニングプールが過去 4 日間でブロックを積んでいるが（図表 17）、この 4 日間でブロックを 1 つも積めなかったマイニングプールやマイナーもいる。これらのマイナーは一斉にナンスを見つける作業をしているが、1 つのマイナーがブロックを積んだ時点でその他全てのマイナーの作業は無駄になり、経済的な利益が得られないだけでなく、純粋にエネルギーを捨てていることにもなる。

このようなエネルギーの消費は社会にとって望ましくない。そこで、いくつかの仮想通貨ではより少ないエネルギーでブロックチェーンを維持する方法が模索されたり、ハッシュパワーの有効利用を試みたりしている（6.を参照のこと）。

図表 17　マイニングプールの勢力図（2017 年 5 月末時点）



（出所）https://blockchain.info/

5.　ビットコインは投資の対象になりうるか

筆者の結論を先に述べると、ビットコインは短期的な収益を目指す投機の対象にはなるが、長期の資産形成を目指す投資の対象にはならない。もちろん、少額の決済やクロスボーダーの決済での利用は有用である。通貨には取引単位、交換手段、価値保存の機能がある。ビットコインは交換手段としての機能は有している。為替レート変動が激しく取引単位の機能を満たさないという意見もあるが、ビットコインネットワーク内で活動する限りにおいては BTC が取引単位であり、ここでは機能を満たしていると考えておく。価値保存については、ビットコインが今後も長期的に利用可能であるかどうかによるが、以下に述べるようにビットコインの長期的な利用可能性は高くない。これが、投機は可能で投資は不可の理由でもある。

ECB（2015）はビットコインに限らず、仮想通貨の安全性について 6 点の疑問を呈している。第 1 は透明性の欠如である。仮想通貨のユーザーに対して十分な情報が提供されていないため思わぬ損失を生む。第 2 は法的地位の欠如である。仮想通貨や取引所に対する法的地位が必ずしも確立されていない。第 3 は存続可能性や流動性の欠如である。ユーザーが利用している仮想通貨や取引所が永続的に続くとは限らない。また、仮想通貨の取引量が不十分であるため、自分のタイミングで売買できるとは限らない。第 4 は IT システムへ

の過度の依存である。ハッキングなどの恐れが常に付きまとう。第 5 は匿名性である。仮想通貨では取引相手のアドレスしかわからないため、詐欺に遭っても相手の特定ができない。最後は仮想通貨のボラティリティの高さである。時には、仮想通貨の為替レートの変動幅が非常に大きくなる。

透明性の欠如や匿名性はそのまま仮想通貨の利点でもある。仮想通貨の取引では不要な情報をできるだけ削除し、匿名性を高めることが目的とされている。特にビットコインのような分散型のブロックチェーンでは、中央集権的な管理者がないにもかかわらず安全性を高めるところに利点がある。中央銀行の立場からは自らのコントロールが効かない金融商品が誕生すること自体、容認できないという立場であることは仕方がない。ただし、先述したように、ビットコインを介した取引の匿名性は一般に考えられているよりも低い。ビットコインアドレス自体はランダムな文字列であり、ビットコインアドレスと現実世界の個人（または法人）をつなげることは難しい。しかし、ビットコインを用いてオンラインショップから購入すれば、購入手続きとトランザクションのブロードキャストのタイミングがほぼ等しいため、ビットコインアドレスと商品購入が結び付けられる。オンラインショップのセキュリティが破られるとビットコインアドレスと現実世界の個人の住所とが結び付けられる。手に入れたビットコインをどこかの取引所で円やドルなどの通貨に交換すると、銀行口座などとビットコイントランザクションが結び付けられる可能性がある。ビットコインの多数のトランザクションをビッグデータとして分析することで、現実世界の個人の特定が可能になる可能性もある。また、ニューヨーク市などはビットコイン取引所に規制をかけており、当局の求めに応じてデータを提供する仕組みが整いつつある。仮想通貨や取引所の法的な地位について定義する国や地域が増えつつある。

匿名性への疑問の背景には、仮想通貨が犯罪に利用されるのではないかという危惧がある。実際に、ダークウォレットというサービスでは、Coinjoin という仕組みを使ってビットコインの取引の匿名化を図っている。Coinjoin は複数のノードのトランザクションを 1 つにまとめる仕組みである。1 つのトランザクションに数十件のインプットとアウトプットがあれば、どのインプットがどのアウトプットに関係しているのかが分かりにくい。ダークウォレットでは Tor という匿名化のプロトコルを用いて参加者を募っており、関係者が分かりにくい。ダークウォレットの発明者はダークウォレットを通じて違法な取引が行われても構わないというスタンスを表明しており、ダークサイトと呼ばれる匿名性の高いサイトでは違法な財・サービスが取引されている。

仮想通貨が IT ネットワークに依存していることは間違いない。しかし、ハッキングなどの攻撃に対する脅威という点では、IoT が実現しつつある社会においては仮想通貨に限られた問題ではない。金融機関や企業のサーバーが攻撃されてシステムがダウンしたり、情報が盗まれたりする事件は後を絶たない。ブロックチェーンは従来の集中管理システムよりは攻撃に強いシステムであることはすでに述べた。

仮想通貨の為替レートのボラティリティが高いことも事実であり、筆者が投機に向いていると述べた理由もここにある。ただし、従来の通貨（fiat currency）も誤った政策によりしばしばハイパーインフレーションを起こしており、従来の通貨しか持たない人々は大きな打撃を被ったことは歴史が証明している。財政規律を失った政府がインフレを志向するのも債務問題を解決したいからで、市民の犠牲は厭わない。仮想通貨は市民に選択肢を与えているともいえる。

ビットコインはデフレ的通貨だといわれる。これは、ビットコインの発行量に 2,100 万 BTC という上限が設定されており、ブロック報酬（リワード）が逓減していく仕組みによる。2017 年 5 月末時点では約 1,635 万 BTC が発行されているが、今後はビットコインの新規発行が徐々に少なくなり、2140 年頃には新規発行がゼロになる。新規発行額が減少する中でユーザー数が増えると、ビットコインの需要が高まり、価値が高まる。通貨の価値下落がインフレであるならば、通貨の価値上昇はデフレということになる。もし、ビットコインが長期に渡って存続するのであれば、ビットコインの価値は次第に高くなるといえる。

仮想通貨の存続可能性については、筆者も大いに主張したい。この点については後述する。ECB（2015）で挙げられた疑問点は、多くの識者に共通しているのではないかと思われるが、その一部は仮想通貨の仕組みの理解不足によるものであるといえる。従来の通貨と同じ視点にとらわれると問題の本質を見逃しかねない。

5.1 ビットコインの安全性と存続可能性

ここではより重要なビットコインの安全な管理とビットコインの存続可能性について考える。

ビットコインのトランザクションがブロードキャストされる際、トランザクションの内容は暗号化されずに平文で送られている。インプットやアウトプットはハッシュ化されており、電子署名によりロックされているためである。ビットコインが盗まれるなどの事件の

ほとんどは、秘密鍵のずさんな管理にある。秘密鍵は公開鍵、つまりビットコインアドレスを創り出すために使われる。秘密鍵が漏洩すれば、その秘密鍵から創られた公開鍵はすべて攻撃者の支配下に入る。秘密鍵の安全な管理は重要であるが、多くのユーザーはウォレットサービスに秘密鍵の管理を任せたり、手元で不十分な管理をしたりしている。

ちなみに、ビットコインを保管するだけであれば、秘密鍵と公開鍵から創られるビットコインアドレスだけがあればよく、PC などは必要ない。PC やスマートフォンなどインターネットに接続できる端末をホットストレージというが、ウイルスや攻撃者の脅威にさらされている。そこで、インターネットから隔離されたコールドストレージに秘密鍵と公開鍵をすると安全性が高まる。最も簡単な方法は紙に書いて保存するペーパーウォレットである。もちろん、メモした紙をなくすとビットコインは永遠に失われる。

次に、ビットコインの存続可能性について見てみよう。ビットコインには集中管理者はいないものの、ビットコインコミュニティと呼ばれるグループが細かいルールを決めたり議論したりしている。ビットコインコミュニティは民主的に運営されているといわれているが、実際には激しい非難合戦も起きている。現在最も重要な問題は、ビットコインのブロックのサイズが 1MB（メガバイト）に制限されており、ますます増えるトランザクションを処理できなくなりつつあることである。1MB のブロックでは、4,000 件の取引までしか台帳部分に含めることはできない（複数のインプットやアウトプットを入れるとサイズが大きくなるため、実際には 2,000 件前後が台帳部分に含まれている）。そこで、Satoshi の意向を組んで運営しているといわれているビットコインコアというグループは、Segwit という仕組みを用いて、各トランザクションのサイズを小さくする提案をしている。それに対して、中国の AntPool を中心とするグループは、ブロックのサイズそのものを拡大する提案をしており、ビットコインコアと対立している[20]。彼らはビットコインアンリミテッド（またはエマージェンスコンセンサス）と呼ばれており、アンリミテッドが新通貨、ビットコインアンリミテッド（BTU）を発行するのではないかといわれている。

このような政治的な対立がビットコインの為替レートにも大きな影響を与えている。ビットコインの世界での民主的とは、マイナーたちの支持を意味し、ハッシュパワーによるパワーバランスを意味する。Coindance などのサイトでは、主要なマイナーによるビットコイン改革案を見ることができる。ビットコインコアは保守的な態度を取ることで知られてお

[20] Nakamura and Chen（2017）。AntPool は 2017 年 5 月末時点で世界最大のマイニングプールである（図表 17）。

り、ビットコインの革新を阻んでいるとして批判されることもある。あくまでも噂だが、アンリミテッド陣営はBTUのハードフォークを考えているともいわれている。

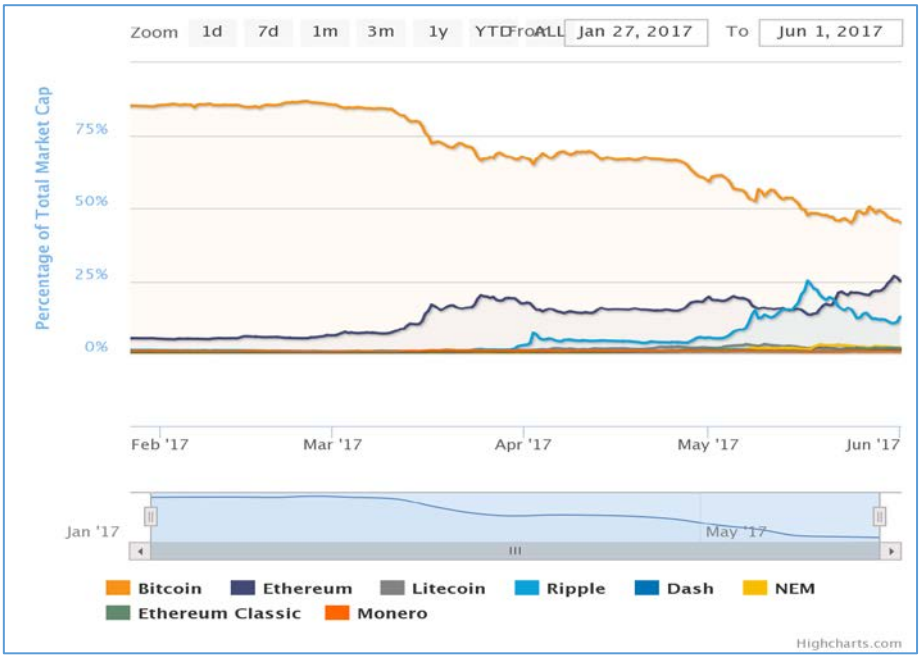
2009年に誕生したビットコインは、セキュリティ対策や利便性の向上などの仕様の変更を何度か行っている。このような変更もフォーク（分岐）というが、互換性のあるフォークをソフトフォーク、互換性のないフォークをハードフォークという。ソフトフォークが実施されてもブロックチェーンには大きな影響がない。マイナーはソフトフォークにより新しいバージョンのソフトウェアを導入すればよいが、ソフトウェアの更新が行われなくてもナンスを見つけてブロックを積むことができる。しかし、ハードフォークが行われるとソフトウェアの更新を行わないマイナーは新しいブロックを積むことができなくなる。当面は新しいルール系列のブロックチェーンと古いルール系列のブロックチェーンが並列することになる。つまり、通貨が2つに分裂する。ブロックチェーンはマイナーが存在する限り存続できる。しばらくして2つの系列がどちらかに収斂することもあれば、2つの系列が長く続くこともある。イーサリアム（Ethereum）は2015年にハードフォークしており、新系列（ETH）と旧系列（ETC）が併存している（32ページ）。ユーザーサイドから見ると、ウォレットが2つの系列に対応していれば両方の通貨を使うことができるが、どちらか片方しか対応していなければ他方の通貨は失うことになる。ビットコインからアンリミテッドがハードフォークすると、BTCとBTUが1：1でフォークすると予想されている。ユーザーから見ると、BTCと同額のBTUを手に入れることができるが、通貨量が2倍になるため円建てで見た価値（為替レート）は半分になると予想されている。小売店も含めて、ユーザーはビットコインコミュニティの動向をある程度知っておく必要がある。

ビットコインなどの仮想通貨の価値は、ネットワーク外部性による[21]。デジタル世界におけるスピードは速く、新しいものが次々に生み出される。ブラウザーやOS、ソフトウェア、SNSサービスなど、古いものが新しいものに駆逐されることはよくあり、そのスピードも速い。人々がビットコインよりも優れたものに移行すれば価値はゼロとなる。

ビットコインは仮想通貨の中で圧倒的なシェアを占めていたが、2017年に入って下落傾向にある。特に、2017年3月には85%だったビットコインのシェアが5月末には46%まで下落しており、イーサリアムやリップルが支持を集めている。今後もビットコインが長く存続するという保証はどこにもない。

[21] ビットコインなどの暗号通貨が人々に信頼される理由の1つに、通貨の発行や取引が数学的に決定されているということがある。従来の通貨やポイントなどは発行主体（政府や企業）が発行量を自由にコントロールできるが、ビットコインでは当事者の一部が発行量をコントロールしようとしても、ブロック報酬を増やしたりブロックを大量に積んだりすることができない。

図表 18　ビットコインが仮想通貨に占めるシェア



（出所）https://coinmarketcap.com/charts/#dominance-percentage

もっと長期の視点で考えてみよう。ビットコインのブロック報酬は約 4 年ごとに半減する。マイナーは多くの資金を投じてマイニングしているが、ブロック報酬が少なくなれば収益率が下がるため、トランザクションフィーを引き上げる可能性がある。そうすると、ユーザーはトランザクションフィーの低い他の通貨に移行する可能性がある。ブロック報酬が次に半減するのは 2020 年頃とみられているが、これを機にビットコインからユーザーが流出する可能性もある。

現在、仮想通貨はバブルの状態にある。バブルはいずれ崩壊し、多くの仮想通貨が消えることになる。バスト（バブルの崩壊）を生き残る通貨を事前に予測するのは難しい。

5.2 ブロックチェーンのビジネスへの応用について

ブロックチェーンはデータベースが堅牢であることからビジネスへの応用が進んでいる。トランザクションにはメッセージを書き込む領域があり、このメッセージを利用して様々な取引を行うことが可能になっている。例えば、1ContractforAandBzzzzzzzzzzzzzzzzzz というアドレスに 1satoshi（1 億分の 1BTC）を送るトランザクションの中に契約書の番号、作成人の署名、要約のハッシュ値などを書き込むことで、この契約書の存在をブロックチェ

ーンに残すことができる[22]。各ブロックにはタイムスタンプが付いており、このタイムスタンプを確認すれば契約の当事者は契約書が交わされた時間をいつでも確認することができる。暗号化された契約書の鍵の一部をトランザクションに含めることも考えられる。

このようなメッセージを利用したカラーコインという方法がある。カラーコインはトランザクションのメッセージ部分を利用してビットコインに「色」[23]を付け、このコインを証明書として使うものである。あるベンチャー企業の全株式を 1BTC のカラーコインとして発行する。この企業の株式の 10%を購入する投資家に対して、0.1BTC のカラーコインを送ることで 10%の株式保有の証明書にできる。このトランザクションはブロックチェーンに含まれ、誰でも確認することができる。このカラーコインには「色」という特別な価値があるため、このコインがオンラインショッピングなどで使われることはないだろう。現実世界の株式の譲渡とカラーコインの譲渡を紐づけることで、ブロックチェーンを使ってこの企業への出資状況を証明することができる。

ビットコインを利用法は次々に生み出されている。ビットコインが 1 億分の 1 まで分割できることで、より低いコストでブロックチェーンを利用することができる。金融機関などによるブロックチェーンの利用が広がっているが、注意点もある。まず、ビットコインなどの既存のブロックチェーンの利用に際しては、これまで述べてきたように秘密鍵の管理を厳重に行う必要がある。また、ある仮想通貨のブロックチェーンの利用が減少するとマイナーが他の仮想通貨に移ってしまうため、悪意のあるマイナーによる攻撃が簡単になってしまう。

独自ブロックチェーンを立ち上げて運用するのであれば、継続的なハッシュパワーの増強が必要になる。ビットコインに参加しているマイナーが悪意をもって独自ブロックチェーンにハッシュ攻撃を仕掛けてくる可能性がある。攻撃者のハッシュパワーは非常に大きいため、誠実なマイナー（ブロックチェーンに参加している企業）たちのハッシュパワーを増強して対抗しなければならない。メディアではブロックチェーンの安全性が過度に報道

[22] このアドレスも vanity アドレスである。A と B の当事者にとっては検索がしやすいが、このアドレスの秘密鍵を見つけるのはほぼ不可能である。そのため、このアドレスを UXTO として 1satoshi を次のインプットに使うことはできず、1satoshi は今後利用不可能になる。このような操作を burn（燃焼、消滅）という。ビットコインは燃えて使えなくなるが、ブロックチェーンに記録を残すための手数料として burn を行っている。自分の名前などを使って vanity アドレスを作り、ブロックチェーンに記録を残すこともできる。

[23] 「色」は比喩であり、実際は当事者間で決めたコードなどを指す。

されている。ビットコイン型のブロックチェーン（proof of work : PoW）のシステムでは、ブロックチェーンの安全性を保つために初期投資だけでなく、継続的な設備投資が必要であり、その額が指数関数的に上昇する可能性があることはあまり知られていないのではないだろうか。Litecoin という仮想通貨では、ビットコインのハッシュパワーの問題点を克服するために scrypt と呼ばれる暗号パズルを導入した。専用機器である ASIC の開発は不可能であると考えられていたが、Litecoin 導入の 2011 年 10 月から 3 年後には Litecoin 専用の ASIC が開発されている。

ブロックチェーン技術は革新的なアイデアであるだけでなく、さらに新しいアイデアが次々に生まれており、イノベーションの場ともなっている。しかし、攻撃者も次々に新しいアイデアを生み出しているため、ブロックチェーンの利用者は技術的な面も含めた十分な理解が欠かせない。トップマネジメント層には新技術を理解できる人材が少ないと想像されるが、現場のセクションに任せきりでは重大な問題を見逃してしまい、将来大きな経営危機に見舞われるだろう。本稿のレベルの理解は最低限のものであり、新しい技術へのキャッチアップも欠かせない。

6. その他の仮想通貨

仮想通貨の世界では、日々新しい通貨が創設されている。その多くはビットコインからハードフォークしたものである。15 ページで見たようにビットコインは 10 分に 1 ブロックしか積めず、トランザクションも 2,000 件前後しか含められない。このような制限を克服するために、ハードフォークした通貨は数多くある。その一方で、新しい通貨を創り出して自分で事前にマイニング（プレマイニング）しておけば、後に大きな利益が得られる可能性があり、創業者利益を目的に創られる通貨も数多くある。そのような通貨は人々の信認を得られず消えていく。2015 年 9 月時点でビットコインから派生した 666 通貨のうち、347 通貨がすでに消えている（Mapofcoins.com）。

ビットコインをヒントに創られたコインはオルトコイン（altcoin）と呼ばれている。近年はコインの創設時に投資家から資金を募り、投資家にコインを配分する方法も用いられている。コインの創設そのものがビジネスになっている。

オルトコインには、ビットコインからフォークしたもの、自ら新しいブロックチェーンを構築しているもの、通貨のように見えるが通貨をいわばトークンとして他のものを取引し

ているもの（本稿ではアントノプロス（2016）に従ってオルトチェーンと呼ぶ)、ブロックチェーンを利用しないもの、がある。以下では、そのうちいくつかを見ていこう。コインの基本情報は Bitcoin 日本語情報サイト（jpbitocoin.com）を参考にした。

6.1 ビットコインからフォークしたオルトコイン

ここには、ビットコインのソースコードを利用して作られたコインも含まれている。

＊Litecoin（LTC：ライトコイン）：2011 年 10 月開始、発行額第 6 位（約 13 億 USD）

Litecoin はビットコインのルールを一部変えることでフォークした。ビットコインのソースコードから創られており、ビットコインと仕組みはよく似ている。ビットコインのブロックが 10 分に 1 度積みあがるのに対して、Litecoin では 4 倍の 2.5 分に 1 度のペースで積みあがる。ハッシュ関数には scrypt と呼ばれる関数を用いており、これは当初はマイニングプールが ASIC を導入しにくいと考えられていたが、現在は ASIC が導入されている。

コインの上限は 8,400 万 LTC であり、84 万ブロックごとにマイナーに対するリワードは半減する（現在は約 121 万ブロックでマイナーへのリワードは 25LTC）こともビットコインの 4 倍という数値になる。ハッシュ計算の難易度の調整は 2016 ブロックごととビットコインと仕組みはよく似ているが、1 ブロックに含まれるトランザクションは数十件で generation（ビットコインの coinbase）のみのブロックも多く、Litecoin の決済はスムーズに進められる。

Litecoin では中国系の F2Pool が 50%近くのハッシュパワーを有しており（ビットコインでは第 6 位の 8.2%)、15%近くのハッシュパワーを保有する第 2 位の AntPool（ビットコインでは第 1 位の 15.1%）と合わせると 60%を超えている。この 2 つのマイニングプールが結託すると、Litecoin のブロックをコントロールできる 51%攻撃が実現可能な状況となっている。

＊Dash（DASH：ダッシュ）：2014 年 1 月開始、発行額第 7 位（約 8 億 USD）

もともとは Darkcoin という名前だったが、2015 年に DASH に変更している。Darkcoin の名前のイメージが悪かったからではないかと思われるが、ここでの Dark とは匿名性が高いという意味である。

ビットコインのようにコインの発行額には上限がある（上限は 1,774 万 DASH から 1,892 万 DASH の間）。ブロック報酬は 1 年間ごとに 7.14%減少していくデフレ通貨である。ブロックは 2.5 分ごとに 1 つ積むことができる。ハッシュ関数に X11（blake、bmw、groestl、jh、keccak、skein、luffa、cubehash、shavite、simd、echo の 11 の関数を用いている）を採用しており、ハッシュの計算に必要なエネルギーを節約できる。

DASH では、マイナーの他にマスターノードと呼ばれるフルノードが存在し、マスターノードはマイニングをせずに送金などの管理を行っている。マスターノードになるためには 1,000DASH を保有していることを証明して、マスターノードリストに登録される必要がある。トランザクションがブロードキャストされるとこのトランザクションを管理するマスターノードがいくつか選ばれ、このマスターノードがトランザクションをロックする。ロックにより、このトランザクションに用いられるインプットはロックが解除されるまで使えなくなるため、二重支払いに対抗することができる。新しいブロックが見つかると、ブロック報酬はマイナーとマスターノードが 45%ずつ取得し、残りの 10%は DASH 管理グループに移される。

DGBB（Decentralized Governance Blockchain Budget）と呼ばれる DASH 管理グループは、DASH の改善（例えばブロックサイズの変更）などの提案や投票の場となっており、管理資金はブロック報酬の 10%が充てられている。提案に対してマスターノードが投票することで賛否がすぐに決まるため、ビットコインのように決定までに長い時間がかからず、争いが起きにくい。

DASH には PrivateSend と InstantSend という 2 種類の送金方法があり、前者は匿名性が非常に高く、後者は決済スピードが非常に速い。

PrivateSend では、トランザクションの匿名性を高めた Darksend という Coinjoin（20 ページ）の技術を用いた方法を使っている。Coinjoin の技術を使って複数のノードからブロードキャストされた複数のトランザクションをまとめるだけでなく、送金額も 100DASH、10DASH、1DASH、0.1DASH などに細かく分割する。Alice による 12.5DASH の送金と Bob による 25.1DASH の送金は、3 つの 10DASH 送金、7 つの 1DASH 送金、6 つの 0.1DASH 送金に分割されてからまとめて送金されることで、それぞれが誰の送金か分かりにくくしている。

InstantSend（2016 年 5 月までは InstantX と呼ばれていた）では、ウォレットから送金されたトランザクションのインプットがマスターノードのネットワークにブロードキャス

トされ、10 のマスターノードに情報が届く。この時点でインプットはロックされ、二重支払いに利用できなくなる。マスターノードがトランザクションをさらに DASH ネットワークにブロードキャストして、マイナーはブロックを積むためのナンスを探す。この過程で 5 つの承認が 1 秒以内に得られることから、ビットコインと異なり、1 秒以内にファイナルまで到達する。ファイナルが先でブロックが後という方式である。

＊Zcash（ZEC：ジーキャッシュ）：2016 年 10 月開始、発行額第 16 位（約 1 億 5,000 万 USD）

2013 年にジョンホプキンス大学の研究者により導入された Zerocoin の後継である Zerocash と MIT の暗号研究グループ、テルアビブ大学の協力により生まれたコインである。Zcash は zk-SNARK（Zero-Knowledge Succinct Non-Interactive Argument of Knowledge）という暗号化技術を採用していることで注目されている。ゼロ知識証明（zero-knowledge proofs）とは、自分が「ある事実を証明した」という情報のみを相手に送ることで、事実の証明ができることをいう。証明するためにどういう方法を使ったのか、などの具体的な情報は不要である。例えば、Alice と Bob の 2 人がパズルを解く競争をしているとする。Alice が制限時間内にパズルを解くが、制限時間が来る前に Bob に答えを教えたくない場合、Alice はパズルの答えをハッシュ関数に入力して出力されたハッシュ値を Bob に送っておけばよい。これで Alice がパズルを解いたことを証明できる。Bob は自分がパズルを解いて（または制限時間後に Alice に答えを教えてもらって）答えをハッシュ関数に入力すれば Alice がすでにパズルを解いていたことを確認できる。Zcash ではブロックのトランザクションに対して四則演算などのいくつかの計算を施して暗号化していく。こうすることで、インプットや金額などを外部から知ることはできなくなる。Zcash の匿名性は仮想通貨の中でもトップクラスである。

Zcash は開発陣の投資を回収するために、現在 12.5ZEC のブロック報酬（開始から 34 日間は不測の問題に対応できるようにブロック報酬はゼロだった）のうち、マイナーに 10ZEC、Zcash 財団に 2.5ZEC が与えられるようになっている。新しい仮想通貨ではプレマイニングといって、公開前に自分たちでマイニングして一定の利益を確保することが多いが、Zcash ではプレマイニングを行わず、ブロック報酬の一部で財団が収益を上げる構造になっている。ブロックは 2.5 分ごとに積まれ、ブロック報酬は 84 万ブロックごとに半減する。ブロックチェーンは 1 から創られているが、Zerocoin の論文がビットコインの匿名性を高める

ためのツールとして書かれており、ビットコインプロトコルのフォークだといえるためこのカテゴリーに入れてある。FAQ には量子コンピューターによる Zcash の安全性についての記述があり、通貨のデザインや Web ページの構成などはいかにも大学の研究者らしい。

Zcash には、transparent address と shielded address がある。transparent addresses はアドレスが t から始まり、ビットコインのように第 3 者がトランザクションの詳細を見ることができる。shielded addresses はアドレスが z から始まり、トランザクションに関する一切のデータが見えないようになっている。トランザクションプールもそれぞれのアドレスに対応して準備されている。https://explorer.zcha.in によると、transparent トランザクションの方が shielded トランザクションよりも 4 倍ほど多い。shielded address や shielded トランザクションに対応していないウォレットサービスが多いことから、匿名性が生かせないでいる。

＊Primecoin (XPM：プライムコイン)：2013 年 7 月開始、発行額第 123 位（約 900 万 USD）

ビットコインのナンス探しはエネルギーの無駄であるという点を改善する目的で作られた通貨である。ナンスを探すパズルがカニンガムチェーン、Bi twin チェーンという素数を探すパズルになっているため、得られたナンスが数学の発展に寄与することになる。

6.2 新しいブロックチェーンを構築しているコイン

このカテゴリーでは、ビットコインのフォークではなく、独自のプロトコルやブロックチェーンを構築している通貨を取り上げる。いくつかのコインにはアセット機能があり、ユーザーが独自通貨を発行することができる。

＊Bytecoin (BCN：バイトコイン)：2012 年 7 月開始、発行額第 8 位（約 4 億 8,000 万 USD）

CryptoNote からフォークした。CryptoNote は匿名性を高めた通貨であり、フォークしやすいように設計されたことから、Monero などもフォークしている。CryptoNote はビットコインのフォークではなく独自ブロックチェーンであることから、Bytecoin もここに分類した。

ブロックは 2 分に 1 つ積みあがる。約 128 万ブロックがこれまでに積みあがっているが、1 つのブロックに含まれるトランザクションは数件～数十件である。ブロック報酬はコイン

の増加と反比例するように線形に減少する設計となっている。

Bytecoin では匿名性を高めるために、受取者のアドレスから 1 回限りの（ワンタイム）公開鍵（アドレス）を作る。この 1 回限りの受け取り用アドレスは、受取者の秘密鍵→受取者のアドレス→受取者の 1 回限りアドレスという流れで作られ、外部から見ると誰のアドレスなのか見分けられないが、受取者は自分の秘密鍵を使えばこの 1 回限りのアドレスのコインを手に入れることができる。その他にも、1 つのトランザクションに複数の人の送金をまとめて、電子署名もまとめる Ring signature という機能も匿名性を高くしている。

＊NXT （NXT：ネクスト）：2014 年 1 月開始、発行額第 43 位（約 7,000 万 USD）

NXT は Proof of Stake（PoS）という方式を導入している。ビットコインなどの多くのコインは PoW（Proof of Work）の仕組みを採用しており、計算をする（work）ことでハッシュ値などを得たマイナーがブロックを積みブロック報酬を得ることができる。しかし、PoS の仕組みでは、NXT の保有比率の多いユーザーがブロックを積むことができる。株式を多く保有する人ほど投票権が多くなる株式会社の仕組みと似ている。

NXT は初めのブロックの段階で 10 億 NXT が発行されており、これ以上通貨が増えることはない。そのため、NXT ではマイニングという言葉を使わず、フォージング（forging：鍛造）という言葉が使われている。フォージャーはトランザクションフィーしか収入がない。10 億 NXT は投資や創業者たちに分配されている。NXT には寄付制度があり、初めて NXT 口座を開いた人や NXT ネットワークに貢献した人（プログラムを創ったり問題点を指摘したりする人）に NXT を寄付できる。

NXT ではウォレットサービスはなく、自分の口座を自分で管理する。口座はパスフレーズ（合言葉）から生成される。たまたま Bob が Alice のパスフレーズを使うと、Alice の口座が使われることになるため、ユーザーは他の人が使わないであろうパスフレーズを用意する必要があり、パスフレーズは変更できない。

NXT にはいくつかの機能がある。Monetary System では、ユーザーは独自にトークン（通貨と呼ばれている）を発行できる。NXT の送金にはメッセージを付けることができるが、メッセージ領域が 1,000 バイトと広いため、文書等を様々なものを送ることができる。マーケットプレイスでは、フリーマーケットのように物の売買ができる。投票システムでは、NXT のユーザーを対象に投票を行うことができる。アンケート調査などが簡単に行え、悪意のある投票を防ぐことができる。Nxt Coin Shuffle 機能では、ブロックの自分のトランザ

クション情報が閲覧できないように設定できる。このような機能の多くは他の通貨でも実装されているが、普通はこの中のいくつかしか利用できない。多くの機能を盛り込んでいることも NXT の特徴の一つである。

＊NEM （XEM：ネム）：2015 年 3 月開始、発行額第 4 位（約 18 億 USD）

NEM は NXT の改良プロジェクトとして始まったが、全く新しい通貨としてスタートした。NEM の重要な特徴は、Proof of Importance（PoI）を導入していることである。NEM は開始時に 8,999,999,999XEM が投資家等に配分され、それ以上は増えない。ブロックを積むための計算はマイニングではなく、ハーベスティング（harvesting：収穫）という。ハーベスティングに参加するためには、少なくとも 1 万 XEM の既得（vested）コインを持つ必要があり、過去 30 日以内に 1 万 XEM 以上のトランザクションを作るなどの条件から重要度が計算される。この重要度の高いノードがハーベスティングを行うことができ、トランザクションフィーを得ることができる。ノード評価システムも取り入れられている。300 万 30XEM 以上を保有するノードがスーパーノードに選ばれると、上乗せ報酬を得ることができる。

NEM では手に入れたばかりのコインは unvested 扱いとなり、PoI にカウントされない。1,440 ブロック（約 24 時間）ごとに未得（unvested）コインの 10%が既得（vested）コインとなり、PoI の計算に用いられるようになる。トランザクションフィーはトランスファーフィーとメッセージフィーに分かれており、公式に従って計算される。

6.3 オルトチェーン

オルトチェーンの通貨は、コインのやり取りが主目的で設計されていない。トランザクションに含まれるメッセージ機能を利用して契約書などをやり取りする仕組みを採用している。

＊Namecoin （NMC：ネームコイン）：2011 年 4 月開始、発行額第 63 位（約 3,000 万 USD）

Namecoin は DNS（domain name system）の機能を持たせたコインである。インターネット上の Web ページのアドレスは、255.255.0.255 のような数字（IP アドレス）で表されるが、これでは人が覚えにくい。そこで DNS の仕組みによって人が覚えやすいアドレス

を IP アドレスに変換している。.com、.net などのドメインはレジストラという団体に管理されているが、Namecoin では集中的な管理者を置かずに分散型の仕組みでインターネットアドレスを管理しようとしている。トップドメイン「.bit」のアドレスは Namecoin で管理される。レジストラ団体が管理している DNS サーバーが攻撃されて情報が失われると Web ページにアクセスできなくなってしまうが、Namecoin を使うとデータベースであるブロックチェーンを書き換えるのは難しいため、データの安全性を高めることができる。

Namecoin はビットコインからのフォークであるため（ビットコインから初めてフォークした通貨）、ブロックチェーンに関する仕組みはビットコインと同じである。ただし、始まった時期が異なるため、Namecoin のブロックは 34 万程度であり、ブロック報酬は 25NMC になっている。

Web アドレスを登録したいユーザーは、トランザクションに name_new、name_firstupdate、name_update などのコマンドを追加する。この場合、トランザクションフィーとは別に登録フィー（registration fee、0.01NMC）が必要となる。マイナーはリワードとトランザクションフィーを受け取り、登録フィーは消滅（burn）して使えなくなる。Web アドレス登録後は、35,999 ブロック（200～250 日）ごとに更新作業が必要となる。更新の際には、登録フィーは不要でトランザクションフィーのみが必要となる。

マイナーはマージマイニングという方法を使うことで、Namecoin のマイニング費用を節約することができる。ビットコインのマイナーは、coinbase トランザクションに電子署名を必要としない。過去の UXTO が存在しないためである（UXTO については 9 ページ）。そこで、この空いているスペースに Namecoin のブロックハッシュを書き込んでおくことで、ビットコインと Namecoin のマイニングを同時に行うことができる。マイナーは同じハッシュパワーで 2 つのコインのマイニングができることになる。

Namecoin では、ビットコインのような通貨の受け渡しと、DNS サービスの利用が混在している。Namecoin Block Explorer（https://namecha.in/）では、どのブロックに更新などのコマンドが含まれているか確認できるが、通貨の受け渡しが約半分くらいになっている。1 ブロック当たりのトランザクションは 1～十数件であり、あまり活発に取引されていない。その理由の一つに、「.bit」に対応していないブラウザーが多いことがある。

＊Ethereum （ETH：イーサリアム）：2015 年 7 月開始、発行額第 2 位（約 158 億 USD）

イーサリアムは契約を付けた取引が可能という点でビットコインと大きく異なっている。

イーサリアムはトランザクションモデルではなくアカウントモデルを採用しており（6－7ページ)、ユーザーは自分の口座の残高を利用して通貨を送金する。ビットコインでは自分の過去の UTXO を分割することはできなかったが、イーサリアムでは可能となる。イーサリアムの通貨単位は ether（イーサー）であり、いくつかの補助単位を持っている。開始時に 6,000 万 ether が発行され、そのうち 1,200 万 ether が開発者やイーサリアム財団に配分された。

図表 19　ETH の補助単位

単位	換算		単位	換算
wei	10^{-18} ether		szabo（microether）	10^{12} wei
babbage（Kwei）	10^{3} wei		finney（milliether）	10^{15} wei
lovelace（Mwei）	10^{6} wei		ether	10^{18} wei
shannon（Gwei）	10^{9} wei			

イーサリアムではトランザクションに複雑な契約を付けることができる。例えば、Alice と Bob の間でさいころゲームをする契約を考えてみよう。両者が 1ether ずつ拠出してさいころを投げる。偶数が出れば Alice が 2ether を受け取り、奇数が出れば Bob が 2ether を受け取る。ビットコインではこのような複雑な取引はできなかったが、イーサリアムでは自由にコード（プログラム）を記述することができるため、さらに複雑な取引も可能となる。このゲームのルールに修正を加えて、日本円の Libor である Tibor1 年物金利が、事前に決めた一定水準（例えば 0.5%）を上回るとその差額分を Alice が受け取り、下回るとその差額分を Bob が受け取るという契約を結ぶことができる。もしある日の Tibor1 年物が 0.6%であれば Alice が差額の 0.1%分の金利を受け取り、0.3%であれば差額の 0.2%分を Bob が受け取る。このような取引は、FRA（Forward Rate Agreement）と同じである。FRA は相対で行われることが多いため、イーサリアムを使えば安全性が高く、低コストで実行できる。

イーサリアムを使うと、オプションなどのデリバティブズを簡単に作り出すことができる。金利や株式指数に関連した従来からあるデリバティブズだけでなく、東京都千代田区の 15 時時点の気温やある交差点の 12 時から 13 時までの車の交通量などのように、これまでデリバティブズの対象にならなかったものも導入することができる。イーサリアムが金融分野での利用が大いに期待される理由がここにある。

トランザクションを実行するためには、燃料（gas：ガス）が必要となる。燃料はトランザクションのサイズやコード（プログラム）の内容によって決められる手数料であり、コードを実行するたびに決められた燃料が消費される。燃料が枯渇するとコードは実行されなくなる。コードをすべて実行した後に残る燃料は返還されるため、ether を送金する際には、この燃料部分を考慮して多めに送る必要がある。先ほどのサイコロゲームでは、掛け金の 1ether と燃料（例えば 1ether）をトランザクションに含める必要がある。燃料方式が導入されることで、コードは無限ループを含むことができる。コード（プログラム）が無限ループに入り込んでしまうと、人がプログラムを閉じるなどして外からコードを止めない限り、いつまでも計算を続けてしまう。このような無限ループはマイナーに対する攻撃として用いられる。イーサリアムでは、燃料が切れた時点で無限ループのコードも止まるため、コードに無限ループを含めることができる[24]。

イーサリアムは 12－15 秒に 1 つブロックを積めるように難易度が設定されている[25]。ブロック生成の速度が速いことは短い時間に多くのトランザクションを実行できる点で優れているが、フォークが発生しやすいというデメリットもある。マイナーにはブロック報酬 5 ether（etherbase という）と燃料が与えられる。ブロック生成速度が速いため、ナンスを見つけたもののネットワークの速度の遅さのために正規のブロックになれないケースもあり、このようなブロックを失効ブロック（stale block）という。失効ブロックを積んだマイナーにも正規ブロックの 7/8（87.5%＝4.375ether）のブロック報酬が与えられる。さらに、失効ブロックの次のブロック（甥ブロックという）を生成したマイナーも 1/32（3.125%＝0.12625ether）のブロック報酬を得ることができる。現在はビットコインのように PoW によるマイニングが実施されており、Ethash という方式が用いられている。ビットコインよりも安全性の高い SHA3 と呼ばれるハッシュ関数のグループを利用している。将来は PoS に移行することが予定されているが、移行時期は未定である。

イーサリアムは機能改善のスケジュールがあり、それぞれコードネームが付けられている。2015 年 7 月の開始時のコードネームは Frontier、それから 115 万ブロック後に自動的に Homestead という改良がおこなわれた。これはハードフォークであり、Homestead に

[24] このような特徴をチューリング完全という。

[25] イーサリアムのブロックでは、マークル木ではなくマークルパトリシア木が用いられている。マークル木よりも木の中のデータの挿入や削除を効率的に行うことができる。ブロック生成速度についてはイーサリアム公式ページ内の説明が統一されていないため、ここでは幅を持った形で記載した。

賛同しないマイナーたちは Ethereum Classic（ETC）として Frontier のイーサリアムを続けている。Metropolis と呼ばれる第 3 段階と Serenity と呼ばれる第 4 段階の内容と実施時期は未定であるが、あと 2 回ハードフォークして 4 種類のイーサリアムが併存する可能性がある。利用者側からすると、ハードフォークの際に当事者同士でどちらの系列で取引を続けるのか決めておく必要がある。新系列に移行するためには、ソフトウェアなどの更新が必要になる可能性が高く、多くの関係者が参加するグループでは全ての参加者のアップデートを待つまでに一定の時間がかかるため、あえて旧系列での取引を続けることも考えられる。

6.4 ブロックチェーンを使わないもの

ここでは、ブロックチェーンではなく分散型台帳システムを採用している通貨から Ripple と Stellar を紹介する。ブロックに取引を記載するのではなく、口座残高を記入する台帳（ledger）の情報を交換することで送金を可能にしている。台帳は口座の残高が増減すると内容が更新されるが、この時に古い内容の台帳を削除せずにそのまま残しておき、新しい台帳を上に積み重ねていく。新しい台帳は古い台帳のハッシュを含むことでそれぞれの台帳がつながっていることを証明できる。ブロックチェーンと似てるように見えるが、台帳には様々な資産情報を載せることができるため、ユーザー側から見た利便性は高い。

Ripple と Stellar では、口座には独自通貨だけでなく JPY や USD などの通貨単位も記帳することができ、金なども含めてあらゆる通貨単位での送金が可能となっている。送金は RTGS（グロス即時決済システム）であり、国際的な送金を数秒でファイナルさせることができる。そのため、これらは仮想通貨というよりは決済システムという方が適している。仮想通貨はブリッジ通貨（為替媒介通貨）として機能し、Alice の口座に入っている USD を Bob の口座に EUR として送金する際に、仮想通貨が USD→仮想通貨→EUR という形で間に入り、円滑な取引を実現している。

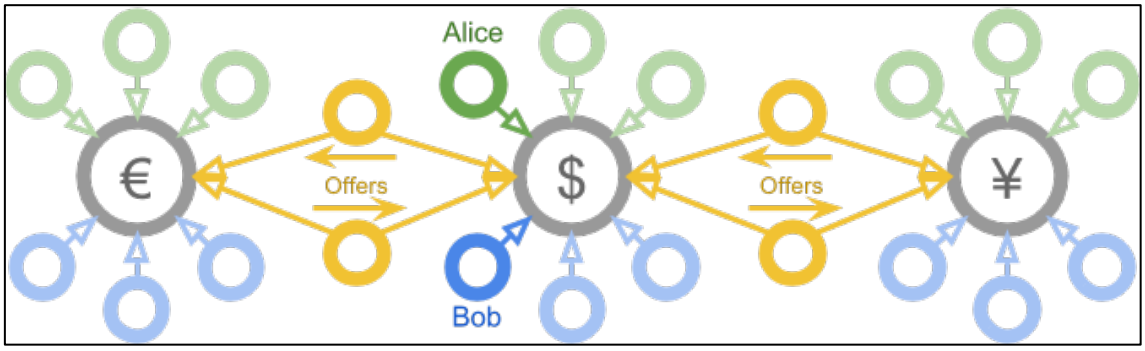
＊Ripple （XPR：リップル）：2013 年 9 月開始、発行額第 3 位（約 87 億 USD）

Ripple は開始時に 1,000 億 XPR が創られており、その多くを Ripple 社が保有している。Ripple 社は XRP を適宜販売することで収益を上げている。100 万分の 1XRP を drop という。XRP は通貨ではなく資産と表現されるが、Ripple 社がその裏付けとなる金などの資産

を保有しているわけではなく、Ripple 社やシステムに対する信用により成り立っている。

Ripple の口座には XRP だけでなく、JPY や USD なども入れることができる。XRP は後述する準備金やトランザクションフィーに利用されるが、必要最低限の残高があればよい。Ripple には、カスタマー、業者（オンラインショップなど）、ゲートウェイ、マーケットメイカーという 4 種類のノードが存在する。ここでは、カスタマーと業者を合わせてユーザーとする。ゲートウェイはユーザーの台帳を管理するノードであり、ユーザーはゲートウェイに JPY などを預けて借用証書（IOU：I owe you）を受け取る。これは預かり証であり、銀行預金の通帳に相当する。ユーザーはゲートウェイに対する預け入れ限度額（与信枠という）を設定する必要があり、普段の利用額よりも少し多めに設定しておけばよい。Ripple での送金は IOU のやり取りという形で行われる。ユーザーは通常 1 つのゲートウェイを使うが、複数のゲートウェイを使ってもよい。この場合、複数のゲートウェイから預かった IOU を統合したり分割したりできる。つまり、ゲートウェイに作った口座間の資金を移動できるが、この操作をリップリング（Rippling）という。ユーザーから見ると、ゲートウェイは銀行として機能している。実際の銀行制度と異なり預金保険制度がないため、ゲートウェイが破綻すると口座残高は失われてしまう。ゲートウェイ選びを慎重に行う必要がある。

図表 20　Ripple のネットワーク



（出所）Ripple wiki ホームページ。

図表 20 での青丸や緑丸がユーザー、灰丸がゲートウェイを表している。ゲートウェイは通常 1 種類の通貨を担当しており [26]、他の通貨への送金をするためには、対応ゲートウェ

[26] ゲートウェイ所在地の通貨を担当し、通貨取り扱いのための現地の法制度に従う。

イを利用する必要がある。ゲートウェイ同士をつなぐのがマーケットメイカー（黄丸）であり、外国為替取引所として機能している。

送金するには、送金金額とは別に 20XRP の準備金が必要になる。20XRP の口座残高は送金するための資格として必要であり、攻撃者が何度も送金してシステムをダウンさせることを防ぐために導入されている。送金の手数料は 10drop（0.00001XRP）であり、これは破棄されてしまうため、長期的には XRP は減少していくことになる。

Ripple にはマイナーはなく、承認者（validator）が取引を承認する。承認者のうち 80%以上が取引を承認すると取引が成立する。承認は数秒で終わる。Ripple は送金にかかる時間は 4 秒だとしている。承認者は相互評価をしており、きちんと機能していない承認者はリスト（ユニークノードリスト：UNL）から削除される。承認者は事実上 Ripple 社が決めるため、承認作業は集中的に行われているといえる。分散型を目指す他の仮想通貨と異なっている。

Ripple は銀行間の決済も仲介している。銀行が Ripple に接続することにより、銀行の顧客は国際送金を銀行→Ripple→相手先銀行という経路で実施することができる。銀行は SWIFT などを用いずに素早く送金できるサービスを提供でき、企業は取引先銀行を通じて国際送金を低コストで実現できる[27]。すでに多くの金融機関が Ripple を導入している。

＊Stellar（XLM：ルーメン）：2014 年 7 月開始、発行額第 13 位（約 3 億 8,000 万 USD）

Stellar は Ripple からフォークして作られたため、Ripple と同じようなシステムを採用している。当初はステラという通貨単位を用いていたが、2015 年にルーメンに改めた。Ripple が金融機関をターゲットにしているのに対して Stellar は個人をターゲットにしているといわれている。 XRP と異なり、XLM は 1%ずつ増加するように設定されている。1XLM は 100 万 stroops。

送金には 100 stroops の手数料が必要で、5×信用枠設定数＋20XLM の残高が口座になければならない。

[27] 送金手数料は銀行が設定するが、Ripple 利用コストが低いため顧客に提示する手数料を低くできる。

参考資料

- アンドレアス・M・アントノプロス（2016）『ビットコインとブロックチェーン』NTT 出版。
- 川野祐司（2016）『ヨーロッパ経済とユーロ』文眞堂。
- George Danezis and Sarah Meiklejohn （2016）、Centrally Banked Cryptocurrencies、：www0. cs.ucl.ac.uk/staff/G.Danezis/papers/ndss16currencies.pdf。
- European Central Bank（2015）、Virtual Currency Schemes。
- Satoshi Nakamoto（2008）、Bitcoin: A Peer-to-Peer Electronic Cash System. Web で入手可。
- Yuji Nakamura and Lulu Yilun Chen（2017）、“Bitcoin Miners Signal Revolt Amid Sluggish Blockchain、” Broomberg、March 13。
- Arvind Narayanan、Joseph Bonneau、Edward Felten、Andrew Miler and Steven Goldfeder（2016）、Bitcoin and Cryptocurrency Technologies、WEB で入手可。

統計・情報サイト

- Bitcoin 日本語情報サイト：https://jpbitcoin.com/
- Blockchain.info：https://blockchain.info/
- Coin Dance：https://coin.dance/stats
- Bitcoin Wisdom：https://bitcoinwisdom.com/
- Map of Coins：https://mapofcoins.tumblr.com/
- CryptoCurrency Market Capitalizations：https://coinmarketcap.com/

仮想通貨公式ホームページ

- Bitcoin：https://www.bitcoin.com/
- Litecoin：https://litecoin.org/
- DASH：https://www.dash.org/
- Zcash：https://z.cash/
- Primecoin：http://primecoin.io/
- Bytecoin：https://bytecoin.org/
- NXT：https://nxt.org/

- NEM : https://www.nem.io/
- Namecoin : https://namecoin.org/
- Ethereum : https://www.ethereum.org/
- Ripple : https://ripple.com/
- Stellar : https://www.stellar.org/