ブロックチェーンと金融取引の革新

淵田　康之

▌要　約▐

1. ビットコインにおいては電子マネーと異なり、取引データを集中的に管理する機関が存在しない。2009 年 1 月のビットコインの誕生以来、ネットワーク参加者がそれぞれデータを管理・更新し続けている。取引記録の改ざんやコインの二重使用の可能性も排除されている。これを可能としているテクノロジーが、ブロックチェーンである。
2. 特定のデータ管理機関を必要としないため、その機関を運営・監督するコストが不要となり、またセキュリティ攻撃が集中するリスクも低下する。また不正が技術的に極めて困難であるだけでなく、不正を試みるよりもデータの管理・更新に正当に貢献する方が、経済合理的となるようなインセンティブ・メカニズムがビルトインされている。
3. ブロックチェーンは、ビットコインのみならず、何らかの価値を持つ物の記録や取引に幅広く応用可能であり、金融分野はもちろん、不動産の登記、各種の契約とその執行、知的財産の保護、投票等、様々な分野で既存の仕組みを代替し、社会システム全体の変革をもたらす可能性がある。既に多くの実験プロジェクトが進行し、実用化の事例もいくつか登場している。
4. 金融分野においては、支払・決済はもとより、証券の発行から売買、清算、決済までの一連のプロセスをブロックチェーン上で処理することに加え、配当や金利の自動的支払い、コーポレート・アクションの自動化、レポ取引、デリバティブ契約の執行や清算、シンジケートローン、本人確認、当局へのレポーティング等の分野への応用可能性が指摘され、各種の取組みが活発化している。バンク・オブ・イングランドでは、中央銀行が紙幣ではなく暗号通貨を発行することにより、マイナス金利の導入を可能とする構想も研究されている。
5. 今日、既存の金融機関やクレジットカード等を通じた金融取引において、コストの高さや不正被害の深刻化が問題となっている。またトレーディングがナノ秒のスピードを競う時代になっているにも関わらず、証券決済には数日を要する状態は何十年経っても変わらないままである。ブロックチェーンは、こうした問題を抜本的に解決し、金融取引に革新をもたらす可能性がある。

Ⅰ　ブロックチェーンの革新性

１．ブロックチェーンとは

ブロックチェーンは、ビットコインの取引を可能としているテクノロジーである。ある期間に発生したビットコインの取引データはまとめられ、一つのブロックと呼ばれる単位で記録されている。2009 年 1 月に最初にビットコインが誕生して以来、今日に至る全ての取引は、こうしたブロックをチェーンのようにつなげる形で管理されており、新たに発生した取引情報を取込んだブロックが、時々刻々と追加されつつある。2015 年 10 月半ばの段階で、最初のブロック（Genesis block）から数えて約 38 万個のブロックがつながっている。

ビットコイン自体は、大幅な価値の変動や一部の交換所における不正の発覚等もあり、幅広い普及には懐疑的な見方もあるが、その背後にあるブロックチェーンという仕組み自体は、画期的な発明と評価され、ビットコイン以外の様々な分野にも応用が期待されている。とりわけ金融取引は、もっとも重要な応用分野となろう。

ワールド・エコノミック・フォーラムは、2015 年 9 月に公表したレポートにおいて、社会を大きく変える可能性のある 21 のテクノロジーの一つにビットコインとブロックチェーンを位置づけ、2027 年には GDP の 10%がブロックチェーン・テクノロジー上で計上されるとするサーベイ結果を紹介している[1]。

ブロックチェーンが画期的であるのは、何らかの信頼できる機関によって取引データが集中的に管理され、過去からの記録の正確性や取引の正当性が保証されるのではなく、誰もが自由に参加・退出できるオープンなネットワーク上で、同様の効果を実現できることにある。

データ等を集中的に管理する機関が不要である結果、その機関を運営したり監督するコストが不要となり、またそうした特定の機関に対してセキュリティ上の脅威が集中する懸念も不要となる。

データの保存・更新、取引の正当性の検証等は、個々のネットワーク参加者のコンピューター（ノード）上で行われる。全てのノードが相互につながっている必要はなく、あるノードが他の 1 つないし複数のノードと相互につながることにより、情報が参加者全体で共有される、いわゆる P2P（Peer to Peer）のネットワークである。世界中に無数に存在する全てのノードが破壊されでもしない限り、過去からのデータは維持され更新され続ける。

取引を記録する台帳（ledger）が一か所で集中管理されていないため、ブロックチェーン・テクノロジーは、より一般的に分散型レッジャーのテクノロジー（distributed ledger technology）とも言われる。取引台帳は、世界中のノードがそれぞれ保有し、新たに発生した取引を追加記帳しているのである。

[1] World Economic Forum, "Deep Shift: Technology Tipping Points and Societal Impact", Survey Report, September 2015.

銀行預金が口座振替等を通じて、支払・決済に利用可能なのは、銀行利用者が銀行システムを信頼しているからである。銀行のような信頼できる機関とそれら機関によって運営されるネットワークが存在しないにも関わらず、ビットコインが支払・決済に利用可能なのは、ブロックチェーンが銀行システムを代替する信頼性を提供するテクノロジーであるためである。

一部のビットコイン交換所で生じたスキャンダルは、主に顧客からのビットコインや法定通貨の預かり分が不正に流用されたものであり、ブロックチェーンの外で生じた問題である。交換所の顧客は、ビットコインの相場変動に応じて、迅速な売買を行うため、自らのビットコインと円やドルなどを、交換所に預託したままにしていたのである。例えばある顧客のビットコイン残高が変動しても、交換所はビットコインの名義変更をその都度ブロックチェーンに登録していたわけではなかったのである。

ブロックチェーンを通じたビットコインの交換自体は、2009 年 1 月にスタートして以来、問題なく継続しており、ブロックチェーンがなんらかの価値を持つ物を交換するテクノロジーとして、現実に機能していることが確認される。

以下、ブロックチェーンとは何かを理解するために、まずビットコイン取引の仕組みを確認することから始めよう[2]。

２．トランザクションの仕組み

X が Y に、10BTC（ビットコイン、2015 年 10 月半ばの時点で 1BTC は 240 ドル台程度）を支払うとする。X は、PC やスマートフォン上で、ビットコインの受取り、支払いを可能とするソフトウェアである「ウォレット」を用い、Y のビットコイン・アドレスと金額（10BTC）を入力し、支払いボタンを押すことで、Y への送金が行われる。ビットコイン・アドレスは通常 1 で始まる 34 の英数字であるため、Y が表示した QR コードを読み取るのが簡単である。

ウォレットには、過去からのブロックチェーン全体の情報が記録されている場合と、ネットワーク上で利用の都度、必要な情報にアクセスする仕組みの場合がある。過去からのブロックチェーンの情報全体は、2015 年半ばに 30 ギガバイトを超えたところであり、PC へのダウンロードには時間がかかり、メモリーも相当使用することとなるため、一般個人の間では簡易なウォレットが利用される場合が多い。

もっとも個々の参加者が、なんらかの機関が提供するデータやサービスに依存しなくても、自ら、過去からの全ての記録を確認した上で取引を行うことが可能な仕組みになって

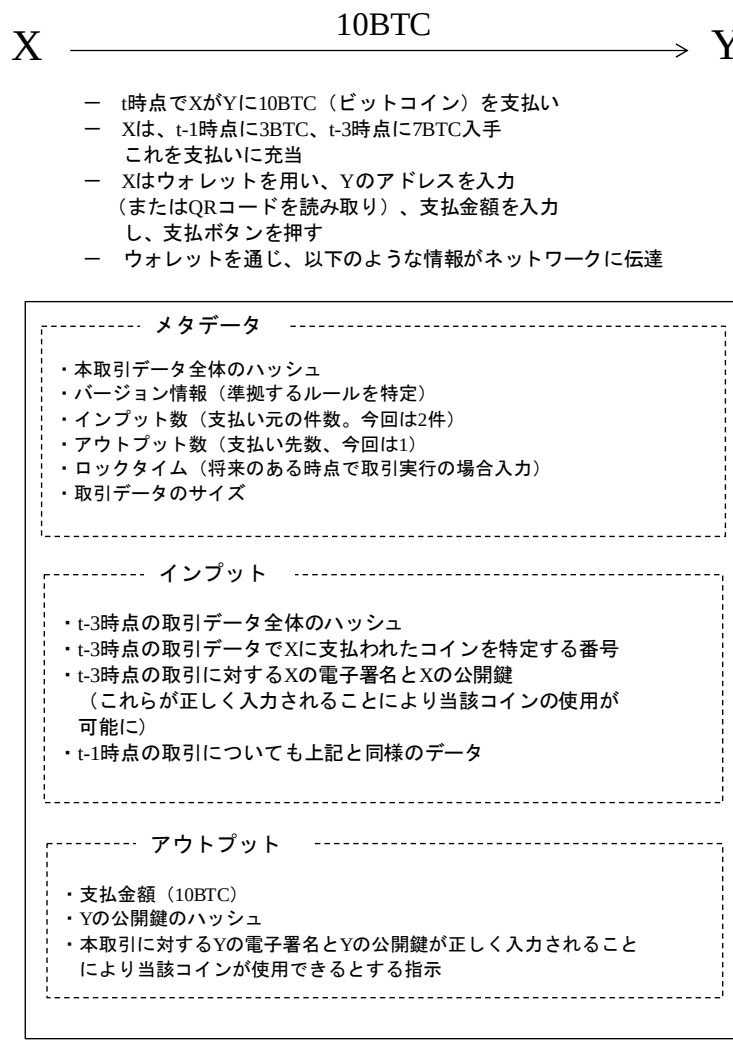
[2] 本稿におけるビットコイン及びブロックチェーンに関する紹介は、Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System"の他、主として Andreas M. Antonopoulos, *Mastering Bitcoin*, O'Reilly Media, Inc. 2013、Arvind Naryanan et.al. "Bitcoin and Cryptocurrency Technologies", Princeton University, 2015、https://enbitcoin.it/wiki/ による。この他、野口悠紀雄『仮想通貨革命』ダイヤモンド社、2014 年、岡田仁志他『仮想通貨』東洋経済新報社、2015 年、http://www.coindesk.com/news/、http://btcnews.jp/、http://www.digitalmoney.or.jp/、http://doublehash.me/等を参照した。

いることが、ビットコインの特徴の一つである。ウォレットをオンラインで提供しているサービスを利用する場合は、そのサービスの運営企業に対する信頼が前提となる。

ウォレット上で上記の簡単な操作を行うと、図表 1 に示すようなトランザクション・データが生成され、ネットワークに共有される。t 時点で X が Y に 10BTC を支払うに当たり、X は、t-3 時点に V から受領した 7BTC と t-1 時点で W から受領した 3BTC を支払いに充当するとしよう。実際にはウォレットには、X が利用できるビットコインの残高が表示されているわけであるが、X が 10BTC と入力すると、この支払いに充当するのに十分な金額を含む過去の取引（X がビットコインの受領者となった取引）が検索され、合計して 10BTC 以上となるような取引のセットが選ばれる。

データ処理の仕組みとしては、過去の取引で入手したビットコインは、支払いに充てられるごとに全額消費され、新たなビットコインが生まれる形となっている。仮に検索で参照された過去の取引における X のビットコイン受領額の合計がちょうど 10BTC ではなく 12BTC であった場合は、Y に 10BTC を支払い、お釣りの 2BTC が X に支払われる形となる。

図表 1　トランザクションとそのデータ（概要）



（出所）野村資本市場研究所

今回の支払いに充てられる過去の取引は、図表 1 のインプットの部分に表示されている。まず「t-3 時点の取引データ全体のハッシュ」とあるが、このハッシュという情報処理の仕組みが、重要である。

ハッシュは、元のデータをハッシュ関数によって処理したものである。ハッシュ関数は、どのようなサイズのデータも一定サイズのデータに変換するものであり、元のデータが少しでも異なれば、ハッシュは全く異なるものとなる。またハッシュから、元のデータを導くことは不可能である。

潜在的には元のデータは無限個あり、その一方でハッシュは有限のサイズであるため、異なるデータが同じハッシュとなる確率はゼロではない。しかし数学的にそれがほとんどありえず、実際にそうした事態が確認されたこともないようなハッシュ関数が採用されている。

今回の X から Y への取引情報がネットワークに流れると、誰でもこのインプット部分にある t-3 時点の取引データのハッシュを使い、自らが保管する t-3 時点の取引情報を参照し、確かに X が 7BTC を受領していることを確認できるのである。

インプット部分で次に重要なのは、X の電子署名と公開鍵の入力である。これは t-3 時点で X が受領したビットコインを、X が支払いに使うことを認めるものである。電子署名は、取引データと X の秘密鍵によって生成される。秘密鍵は X のみが知っており、この電子署名は X のみが作成できる。秘密鍵は公開鍵とペアになっており、秘密鍵自体の情報がなくても、公開鍵と電子署名をセットで処理することで、誰もが、今回の取引で、X が t-3 時点で受領したビットコインを支払いに使うことを X 自身が認めていることを確認できる。t-1 時点の取引で入手したビットコインについても、同様のインプットがなされる。

アウトプット部分では、支払額と支払先である Y のアドレス（実際には Y の公開鍵のハッシュ。このデータ表示形式を変換したものがビットコインのアドレスとなる）、そして Y が自分の電子署名と公開鍵を入力すれば、今回、受領した 10BTC を使用できるようになるという指示が記録される。

t-3 時点や t-1 時点の取引データのアウトプット部分にも同じ指示があり、t 時点でこれらがインプット側に選択され、これに対して電子署名及び公開鍵が入力されたことにより、X は今回、過去に受領したビットコインを使用できたのである。

結局、X から Y に 10BTC が送金されたといっても、何らかの価値を持つ物が電子メールの添付ファイルのような形で X から Y に移動したわけではなく、X の秘密鍵で管理されていたデータが、Y の秘密鍵で管理されるデータとなったのである。X と Y はネットワークで直接つながっている必要もなく、このようにデータのステイタスが変化したという記録が、ネットワーク全体で共有され、そのネットワークに何らかの形で Y がつながることで、X からの支払いが行われたことを知ることができるのである。

なお X がウォレットに入力する必要があるのは、支払金額と Y のアドレスのみである。X の公開鍵や秘密鍵、その他のデータを用いた処理は、ウォレット上で自動的に行われる。

ウォレットへのアクセスにはパスワードが必要であるが、セキュリティをより確実にするため、秘密鍵はオフラインで保管し、電子署名や取引データの入力もオフラインで行うことができる。

３．トランザクションとブロックチェーン

以上の X から Y への支払いは t 時点のトランザクションであったが、同じ時点までに発生した他のトランザクションも合わせて、一つのブロックの形でビットコインのトランザクション・データは管理される。ビットコインの場合、約 10 分間隔で 1 時点が区切られている。

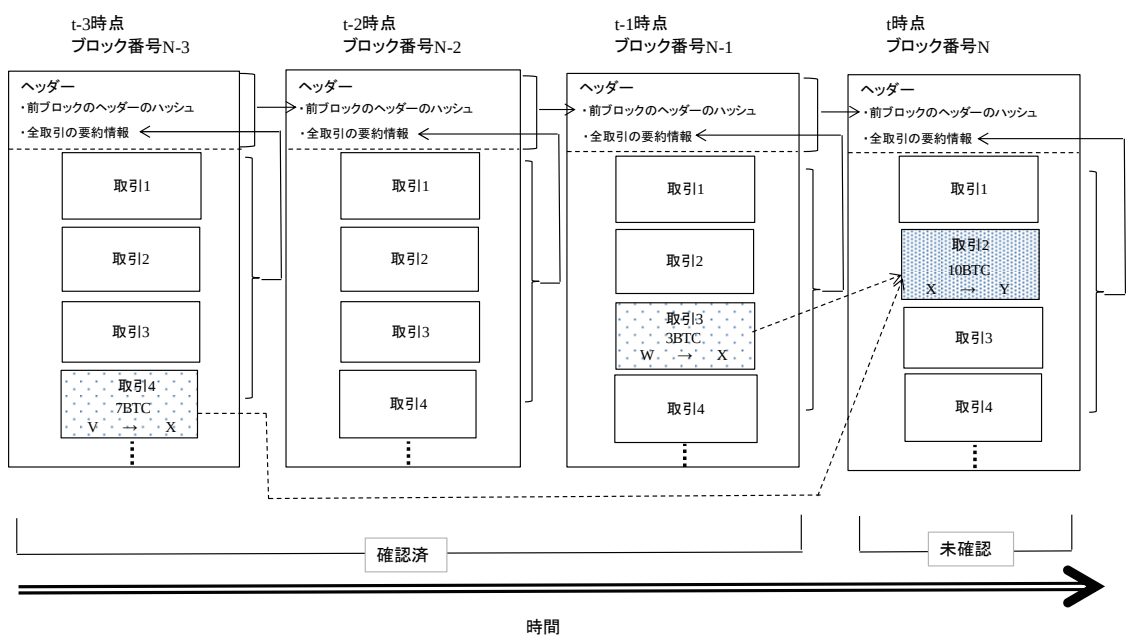
ある時点のトランザクションとその時点のブロックの関係、及びブロック同士の関係は図表 2 のようになっている。

まず t 時点に行われた X→Y のトランザクションは、t 時点のブロックに取引 2 として記録されている。このトランザクションは前記のように、t-3 時点の V→X のトランザクションと t-1 時点の W→X のトランザクションを参照している。こうした過去のトランザクション情報も、それぞれの時点のブロックに記録されている。

また各時点のブロックのヘッダーには、そのブロックに含まれるトランザクションの情報の要約情報と、前のブロックのヘッダー情報のハッシュが含まれる。

ブロックに含まれるトランザクションの要約情報とは、個々のトランザクションの情報のハッシュを、二組のペアにしてそのハッシュを求め、さらにそのペアのハッシュを求め

図表 2　トランザクションとブロックチェーン（イメージ）



（出所）野村資本市場研究所

るということを繰り返して、一つのハッシュとしたものである。奇数個の場合は、同じデータ同士のペアのハッシュを求める。

個々のトランザクション情報を葉とすれば、最後に得られる一つの値は根である。すなわち図表 3 のように、木を逆さまにした形になるが、これは考案者にちなんでマークル・ツリー（Merkle Tree）と呼ばれ、最後に得られる要約情報はマークル・ルート(Merkle Root)と呼ばれる。

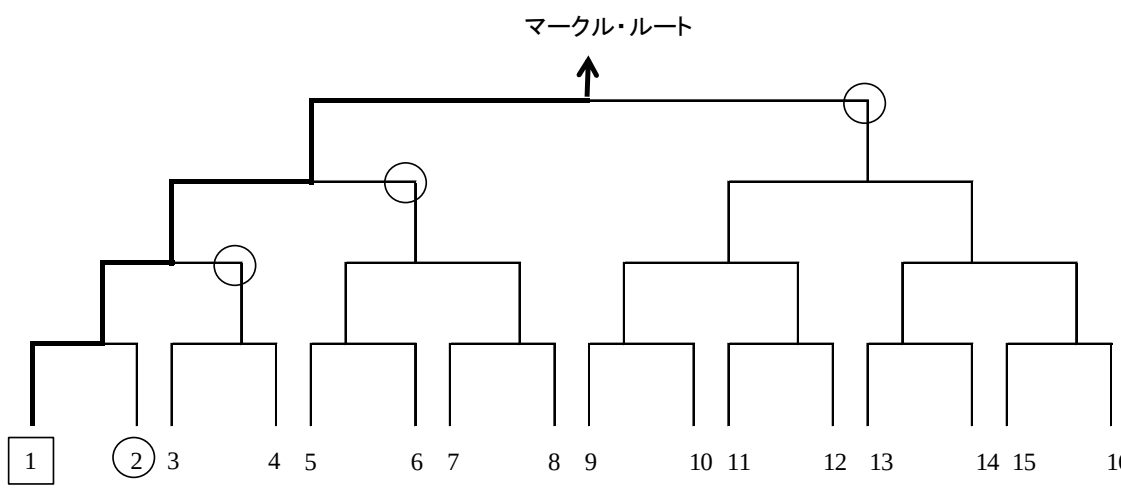
このようなデータ処理の利点は、あるトランザクション・データが確かにそのブロックに含まれているかどうかは、全てのトランザクション・データを検索しなくても、図表 3 に示すようにいくつかのデータのみ利用し、同じマークル・ルートが得られるかどうかを確認すれば良い点にある。

以上の仕組みから次のようなセキュリティ上の特徴が生まれる。まず図表 1 で示したように個々のトランザクションにおいて、使用されるビットコインに関連する過去のトランザクションのハッシュが参照されるため、過去のトランザクション・データが改ざんされれば、ハッシュが変わるため、改ざんの事実が発覚する。

また図表 2 で示したように、各ブロック内のトランザクションのデータが改ざんされれば、そのブロックのヘッダー情報に含まれるマークル・ルートも変化する。そして各ブロックのヘッダー情報には、一つ前のブロックのヘッダー情報のハッシュが含まれているため、過去のあるトランザクション・データが改ざんされ、そのブロックのヘッダー情報が変化すれば、それ以降のブロックのヘッダー情報も全て変化することになる。

過去から現在に至るブロック情報は、ネットワーク上の各ノードが保管しているため、異なる情報を持つブロックの登場は直ちに検知される。

図表 3　マークル・ツリーとマークル・ルート



（注）　取引 1 が本ブロックに含まれることを確認するには、○で囲んだ値のみ入力し、同じマークル・ルートが得られるか調べればよい。

（出所）野村資本市場研究所

P2P のネットワークで取引を行う場合、問題となるのはなりすまし、改ざん、そして二重使用である。なりすましとは、X ではなく他の人間が X になりすまして、X のビットコインを使用することである。ビットコインにおいては、この点は、秘密鍵と公開鍵、そしてこれを活用した電子署名の利用によって対応されている。ただし、この公開鍵暗号のテクノロジーは、1976 年に発案されたものであり、今日、ビットコイン以外でも広く利用されている。

改ざんの防止という点では、前記のように過去のトランザクション・データの改ざんが、そのトランザクション自身のハッシュ、及びそのトランザクションのマークル・ルートが含まれるブロックのヘッダー情報、さらにそれに続く全てのブロックのヘッダー情報の変更をもたらしてしまうという構造の採用が、重要な工夫と言える。

また二重使用の問題についても、例えば t-3 時点のトランザクションで受領したビットコインを t 時点で使用しようとした場合、t-3 から t 時点の全てのトランザクションをスキャンすることにより、同じビットコインが既に使用されていないか容易に確認することができる。

通常、X が利用するウォレットの仕組みとしてこうしたチェック機能が提供されており、そもそも X は二重使用を実行できない。仮に X 自身がウォレットを改変するなどして二重使用を行ったとしても、その情報を受領した他のネットワーク参加者が容易に二重使用を検知できる。二重使用を検知できないように、関連するデータを書き換えようとしても、その影響はそれ以降の全てのブロックの情報の書き換えを必要とする。さらに書き換えられたデータを、ネットワーク参加者に正当なものとして受け入れてもらう必要がある。

しかし逆に言えば、例えば X 自身がトランザクション・データの唯一の管理者であり、他の参加者が全ブロックチェーンの情報をそれぞれ保有して、チェックしていたとしても、例えばその情報は X が管理するデータをコピーしているだけだとすれば、X がデータを全て辻褄が合うように書き換えることができ、さらにそれを参加者が追認してしまうため、二重使用は避けられない。このような可能性があるのであれば、X が銀行のように信頼できる存在でない限り、誰もこのシステムを使わず、P2P の取引システムとしては成り立たない。

ブロックチェーンが真に革新的であるのは、こうしたケースも含め二重使用の脅威を克服したことにある。すなわち銀行のような信頼できる存在が無くても、というより、特定の管理者がいないからこそ、二重使用の恐れがない、P2P の取引システムを実現したのである。

４．ブロックの構造とマイニング

ビットコインにおけるブロックチェーンが画期的であるのは、特定の信頼できる管理者が存在しなくても、ネットワーク参加者が過去からの今日に至る取引データを共有し、またその正当性について合意し、それにつながる新たなブロックについても、正当なものとして合意して既存データを更新する仕組みを実現した点にある。

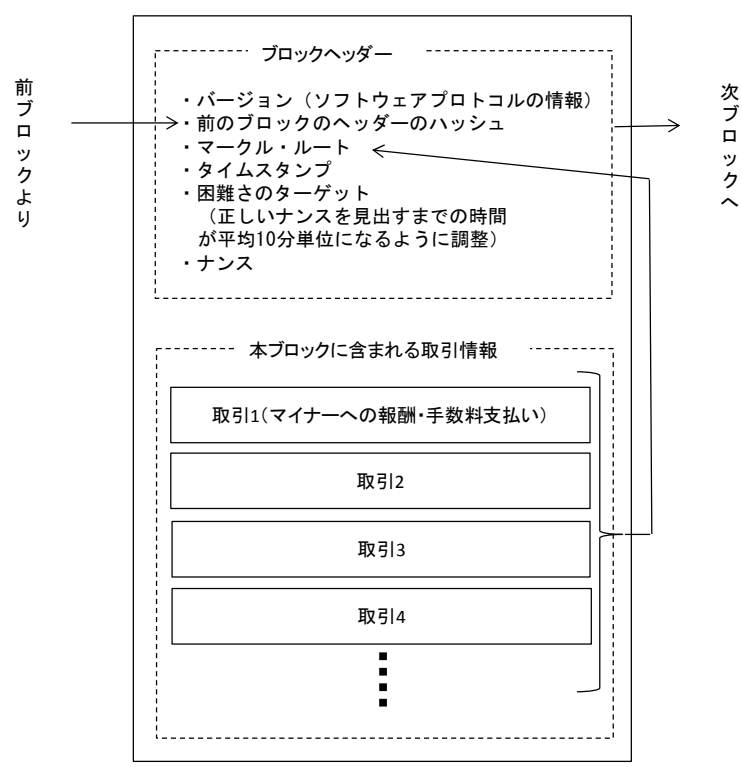
特定の機関が参加者に信頼され、従ってその管理するデータの正当性についても合意することによって成立するのではなく、個々の参加者がそれぞれデータの正当性を信頼し、その利用に合意していることによって成立しているため、この仕組みは分散的合意のメカニズム（distributed consensus mechanism）とも呼ばれる。

このための特徴ある工夫として、単に不正を行うことが技術的に困難なだけではなく、不正を試みる場合の労力が非常に大きくなるプロセスの導入がある。この点を確認するために、図表 4 で各ブロックの構造をより詳しく示してある。

ブロックのヘッダー情報には、前ブロックのヘッダーのハッシュと当該ブロックに含まれるトランザクション・データの要約情報であるマークル・ルート以外に、「ナンス（nonce）」が含まれる。ナンスは、number used once の略であり、32 ビットのデータである。ナンスはヘッダーに含まれる情報であるため、ナンスを変化させるとヘッダーのハッシュも変化する。

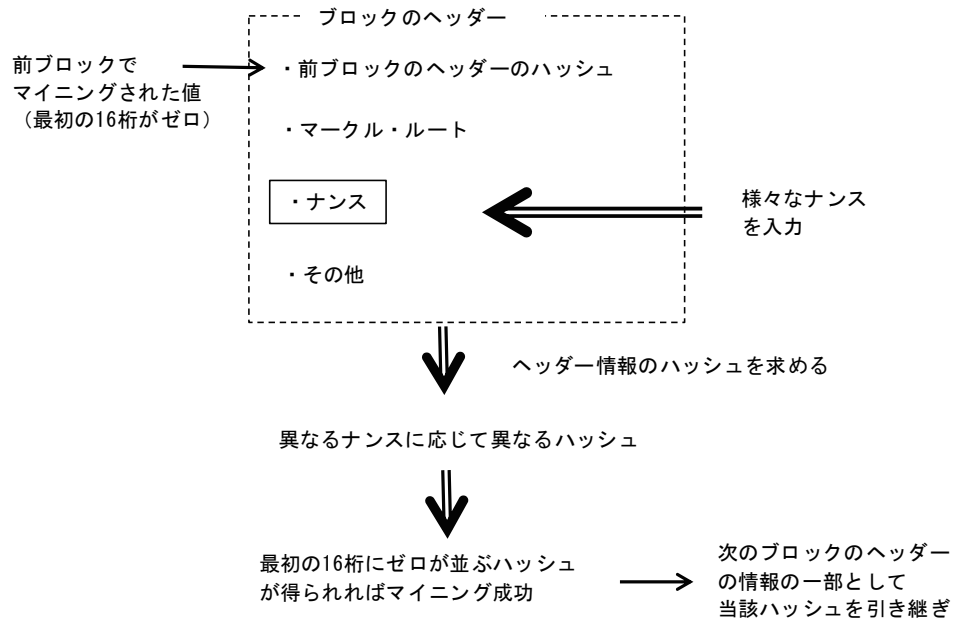
そこで図表 5 に示すように、参加者はナンスを変化させ、ヘッダー情報のハッシュを計算し、ハッシュを 16 進数で示した場合、指定された桁数だけ最初にゼロが並ぶような結果が生ずるナンスを探すのである。このためには、膨大なナンスをランダムに発生させて条件を満たすハッシュを求める作業を繰り返す必要がある。この単純作業をマイニングと呼び、当たりのナンスを見出すための時間が平均して 10 分となるように、発見の困難さ

図表 4　各ブロックのデータ（概要）



（出所）野村資本市場研究所

図表 5　マイニングの仕組み



（注）　ブロックヘッダーのハッシュの最初にゼロが何桁並ぶ必要があるかは、困難さのターゲットで規定される。本事例では 16 桁としている。
（出所）野村資本市場研究所

のターゲットが調整されている[3]。テクノロジーが進化し、参加者の処理スピードが向上すれば、ハッシュの最初に並ぶ必要があるゼロの桁数を多くすることで、当たりのナンスを見つけるのに要する時間を長くするのである。

マイニングを行う者（マイナー）は、単に当たりのナンスを見つけるだけではなく、マイニング作業の大前提としてブロックに含まれる全てのトランザクションが過去のトランザクションと整合的であることをチェックし、全てのトランザクション情報が正当であることを確認する。

マイニングの成功者は、マイニングの成功と新たなブロックの追加を宣言すると、ネットワークの他の参加者が、提示されたブロックの情報とナンスからマイニングの成功を確認し、ブロック内のトランザクション・データの正当性も確認した上で、自らの保有するブロックチェーンに新たなブロックを追加する。

マイニングに成功したと宣言する者が、仮にブロック内の個々のトランザクションの正当性をきちんと確認せず、誤ったトランザクションを含むブロックを追加しようとしていたのだとしても、他の参加者によって誤りが容易に発見される。この場合、マイニングに投入した労力が無駄になってしまう。マイニングという単純作業を経なければ、ブロック

[3] 過去 2016 ブロックの追加（約 2 週間）にかかった時間を計算し、ブロックの追加が平均 10 分間に 1 ブロックとなるように難易度が調整される。10 分という単位を短くすれば、取引確認が迅速に行われるようになるが、一方で、マイニングの成功者が現れやすくなり、ほぼ同じような時間に多数のブロックの追加が宣言され、ブロックチェーンの分岐（fork）が生じやすくなる。こうした点に配慮し、10 分という単位が選択されている。

を追加できない仕組みとすることで、いいかげんにブロックを作成し追加することが高くつくことになるわけである。マイニングは、システムの維持運営にまじめに参加することを担保する作業であり、Proof of Work とも呼ばれる。ビットコインが採用する仕組みは、1997 年に考案されたハッシュキャッシュと呼ばれるもので、スパムメールの防止等に利用されてきた技術である。

一方、トランザクションの正当性をきちんと確認した上でマイニングを成功させた者には、新たなビットコイン及びそのブロックに含まれる個々の取引に対する取引手数料の合計が与えられる。このトランザクション情報は、ブロック作成時に、ブロックのトランザクションの一番最初のトランザクション情報として入力される（図表 2 及び図表 4 の取引 1）。こうした報酬へのインセンティブがあるため、様々な参加者が自主的にビットコインのネットワークに参加し、それを維持・管理する作業に携わる仕組みが出来上がっているのである。報酬として新たに発行されるビットコインは、当初 50BTC であったが、21 万ブロックごとに半減する仕組みとなっている。2012 年 11 月以降、25BTC となり、2016 年中に 12.5BTC となる見込みである。

ある者がブロックの中のトランザクションを書き換えるには、それに係るブロックヘッダー情報を含む全てのブロックを書き換える必要があり、それぞれのブロックにおいて正しいナンスのマイニングに成功する必要もあるため、何ブロックも前のトランザクションの書き換えは事実上困難となる。その間に、同じようなコンピューター・パワーを持つマイナーらによって、正しい過去の情報と整合的な新ブロックが次々と追加されてしまうからである。

改ざんの可能性が多少でもあるとすれば、極めて最近のトランザクションの改ざんであり、そのトランザクションを含むブロックとその後のブロックのマイニングに成功し続け、改ざんされたデータと辻褄の合うブロックを追加し続ける場合である。

マイニングには、膨大な量の数字の入力が必要であり、成功し続けるには他の参加者を圧倒するコンピューター・パワーを持つ必要がある。また仮に異なる内容の二つのブロックが追加され、ブロックチェーンの分岐が生じる場合には、長く伸びたブロックチェーン、すなわちより多くのブロックが追加され、参加者による確認が繰り返されたブロックチェーンが正当とみなされることから、その意味でも他の参加者を上回るスピードでマイニングに成功し続ける能力が必要である。

これを可能とするほどの圧倒的なリソースを持つ者の登場はそもそも想定しにくく、さらにそれほどのリソースがあれば、それを悪事に使うよりも、正直な参加者としてマイニングに活用し、正当な報酬を得る方が、経済合理的となる。

５．トランザクションからその確認まで

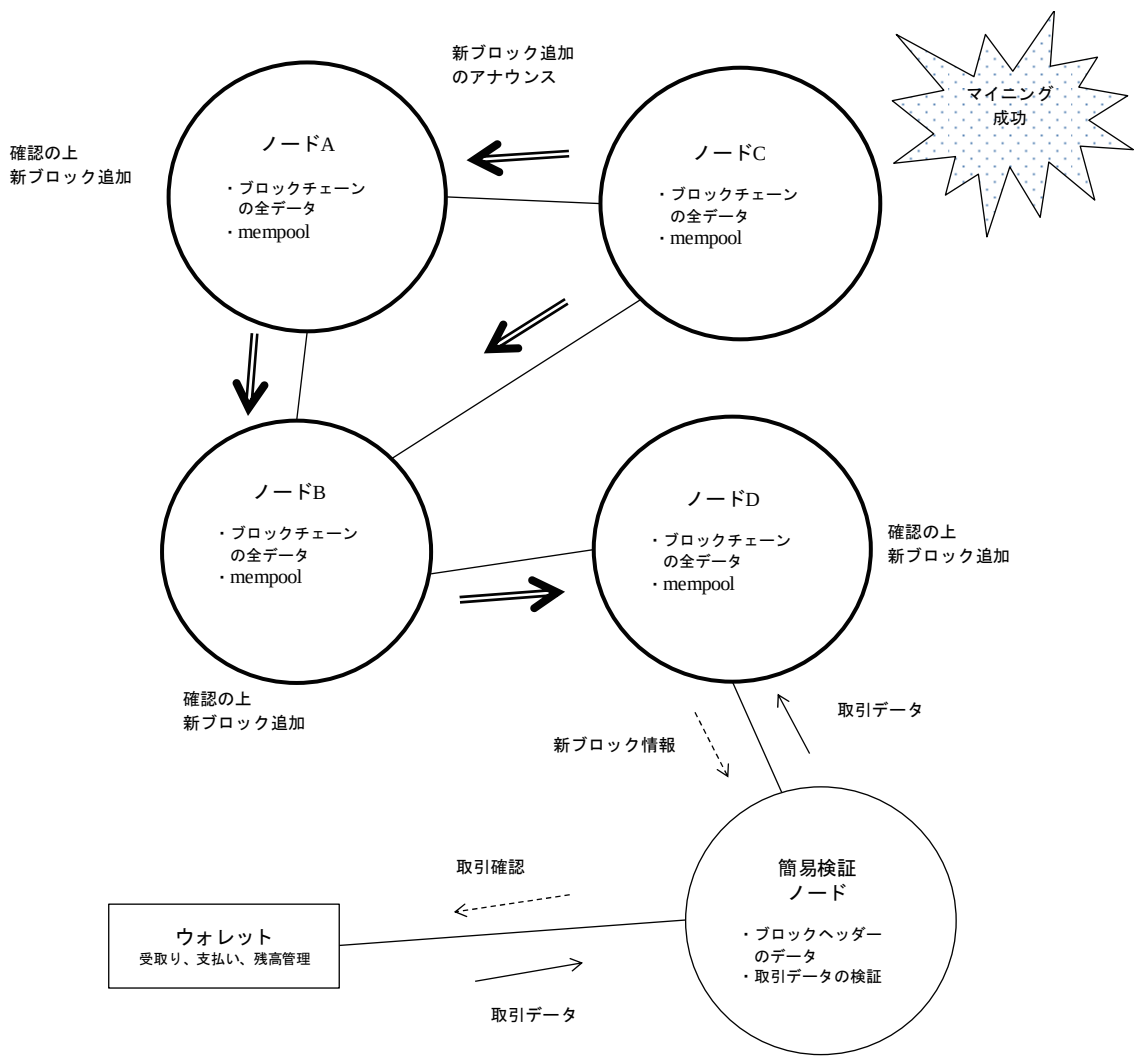
以上で見てきた仕組みを振り返りつつ、一つのトランザクションが、いかにブロックチェーンを通じて参加者全体に認知され、確認されていくか、一連のプロセスを概観して

みよう（図表 6）。

まず個々のウォレットのレベルでトランザクションが発生する。ウォレットの仕組みで、当該トランザクションに使用されるビットコインのどの部分が、過去のどのトランザクションで現在の持ち主に支払われたかが特定され、現在の持ち主の電子署名でそれを使用すること、そして新たにそれを使用できるようにするには Y の電子署名が必要であるという情報が作成される。

この情報をビットコイン・ネットワークに流すと、受け取ったノードは、そのデータ形式がプロトコルに則っているかどうかの他、保有するブロックチェーンの記録に照らし、参照されている過去のトランザクションが正しいものであり二重使用が無いかどうか等を検証（verify）した上で次のノードに伝達する。こうしてネットワーク上の各ノードが新たな取引の情報を共有する。ノードにはブロックチェーンの全データを管理しているフルノードと、ヘッダー情報のみ管理している簡易検証ノードがある。

図表 6　P2P ネットワークによる分散的コンセンサスの形成



（出所）野村資本市場研究所

トランザクションが各ノードにおける検証を経たとしても、これだけの仕組みであれば、何者かが過去のトランザクション情報を含めて改ざんしている可能性を排除できない。過去のトランザクションを含めて改ざん不能となるブロックチェーンに、このトランザクションを追加して登録する作業を行うことで、この取引の正当性がネットワーク全体にとってのコンセンサスとなる。そしてこのトランザクションでビットコインを入手した者も、正当な保有者としてそのコインを将来安心して使用することが可能となる。

このトランザクションを含む新たなブロックの作成は、次のようなプロセスで行われる。新たなトランザクションは、未確認トランザクションとしてプールされ、マイナーは、ここ（memory pool、略して mempool）からブロックに取り込むトランザクションを選択する。高額のトランザクションや取引が行われてから未確認の状態が長く続いているトランザクションの処理は、優先して行うルールとなっている。それらの取引の記録にブロックサイズの一定部分の容量を充てた上で、あとは手数料の大きいトランザクションを選択することが当然考えられる。

ブロックに取り込むトランザクションは、マイナーによって必ずしも一致しない。各自が自らの選んだトランザクションを内容とするブロックを対象にマイニングを行うのである。マイニングに成功した者は、そのブロックの情報をネットワークに伝達する。他のマイナーは、マイニングが成功していることとトランザクション・データが正確であることを確認し、各自、新ブロックを自ら管理しているブロックチェーンの記録につなげる。

自分がマイニング途上であったブロックに含まれていたトランザクションのうち、マイニングに成功した他者が追加する新ブロックに含まれていない部分は、mempool に戻され、また新たなブロックのマイニング作業を始めることとなる。

新ブロックがブロックチェーンにつなげられた場合、そのブロックに含まれていたトランザクションは、「確認（confirm)」されたというステイタスとなる。さらに次のブロックがつながると、2 回確認されたことになる。ブロックがつながっていき、繰り返し確認されるにつれ、改ざんは飛躍的に困難となるため、確認回数の多さが、データの正確性の指標となる。

Ⅱ ブロックチェーンがもたらす社会システム変革

１．様々な応用可能性

様々な法制度や公的インフラによって、その信用が支えられた銀行とその決済システムの存在を必要とせず、ネットワークの参加者が自己の利益を追求するために行う行動により、銀行預金を通じた支払・決済と同様の機能がブロックチェーン技術によって実現するのであれば、この仕組みを、ビットコインの取引だけではなく、現状、特定の信頼できる第三者を介在させることで成り立っている他の様々な分野にも応用していくことが考えられる。

例えば、少額のビットコインをビットコインとしてではなく、有価証券等、より高額の資産を化体したものとして取扱い、これをブロックチェーンで取引することが考えられる。これがカラードコインと呼ばれる仕組みである。

契約をブロックチェーンで扱い、その真正性を確実なものとするのみならず、契約情報に埋め込まれたプログラムにより、一定の条件が満たされることで契約内容を自動的に執行することを可能とするスマートコントラクトという仕組みも考案されている。

各種の応用にあたっては、ビットコインに用いられたブロックチェーンの仕組みそのものではなく、そこから派生した様々な仕組みも考案されている。ビットコインにおいては、特定の機関の信頼が無くても確実な取引が保証されるという、ある意味で究極の姿を実現することが最重視されたが、その一方で、ブロックの作成に 10 分程度必要であるとか、マイニングに膨大な電力と CPU が使用されるといった問題もある。

そこでブロックチェーンの仕組みのメリットを活用しつつ、完全にオープンなネットワークではなく、一定の資格のあるクローズドなメンバーのみが参加するネットワークを使ったり、一定の信頼できる機関を介在させたり、Proof of Work とは異なる仕組みを採用するといった工夫を盛り込んだ様々な仕組みも開発されつつある。

以上のような新たな構想は、ビットコイン 2.0 とも称されている。本稿では、それらの技術的説明は割愛し、様々な応用可能性の紹介に焦点を当てることとする。例えば、以下のような分野での応用可能性が指摘されている。

１）不動産、有価証券、その他財産の登録・移転

所有やその移転の証明を確実なものとするための既存の制度、例えば公証人、不動産の登記、証券保管振替機構、名義書換代理人、自動車の登録といった制度を、特定の機関ではなくブロックチェーンを用いる仕組みに転換できる可能性がある。

２）契約の自動執行

事後的に改ざんされない真正な契約を電子的に締結することができるのみならず、契約内容を自動的に執行するプログラムを契約データに盛り込むこともできる。例えば債券の保有者に、自動的に定期的な利払いや償還金額の支払いが行われる仕組みが考えられる。あるいはデリバティブ契約において、自動的に権利が行使される仕組みが考えられる。

自動車や不動産の所有の移転と共に新たな所有者のスマートフォンにキー情報が送信され、スマートフォンで自動車や不動産の利用が開始できるようになるといった仕組みも考えられる。

３）知的財産の保護

ブロックチェーンで管理されるビットコインでは、二重使用が不可能となる。従って、同じ技術を用いれば、ネットでダウンロードした音楽やプログラムを複製・再販

することを不可能とできる。また動画等の一部を秒、分単位で販売し、課金することも容易になる。

４）投票

二重投票が回避できる。公正な電子投票とその迅速で確実な集票が可能となる。

その他、様々な応用が議論されているが、いずれの場合も、ブロックチェーンを利用し、第三者を介在させない、あるいはその介在を限定的とすることにより、第三者の信頼性を確保するコストやその運営コストを大幅に削減できることがメリットとなる。また特定の国の制度等に依存せず、グローバルに標準化された経済取引を実現しうることもメリットとして指摘される。

２．相次ぐ実用化の試み

こうしたブロックチェーン・テクノロジーの応用に関する各種の構想を実現させるための試みが、以下のように各方面で活発化している。このうち金融分野の試みについては、次章でより詳しく紹介することとする。

１）土地

中米のホンジュラスは、2015 年 5 月、ブロックチェーンの仕組みで土地の登記を管理する仕組みの開発を、テキサスの Factom 社に依頼した。

途上国においては、土地の所有権が公的な文書に記録されていないケースが多く、記録されていたとしても、紙の台帳で管理され、消失のリスクもある。一部の途上国では世界銀行から多額の支援を受け、土地の登記簿のデータベース化を進めたが、不正によりデータが改ざんされるという問題も生じているという。集中的な管理はハッカーの標的ともなり易い。

ブロックチェーン上で登記簿を管理すれば、コストが大幅に削減できるだけではなく、内戦やハッキング、汚職や不正によるデータベースの消失や改ざんの恐れもなくなる。

途上国においては、土地以外の資本の蓄積は少ないため、土地の所有権が明確となり、これを担保として利用することが容易になることは、経済発展のためにも意義があるとされている。土地の所有権が明確となることで、埋蔵資源の利用も円滑化することが期待される。Factom 社によれば、他の諸国においても、ブロックチェーンによる土地登記の仕組みの導入が検討されているという。

２）貴金属

ロンドンの Real Asset 社は、小口投資家の金売買のプラットフォームを提供してき

たが、2015 年 1 月に Goldbloc という仕組みを導入した。Goldbloc は暗号通貨であり、一つの Goldbloc は、専門業者が管理する金庫に保管された金 1 グラムと対応することが、ブロックチェーン上で規定されている。金貨を自ら保有することのリスクやコストが回避でき、また金関連の金融商品と異なり、カウンターパーティ・リスクが無い。同社はこの仕組みを他の金属にも応用していく予定である。

3）ブランド商品・宝石

サンフランシスコの Chronicled という会社は、ブロックチェーンを活用し、ブランド商品が本物であること、またそれを本人が所有していることを証明する仕組みの開発を進めており、2015 年中に事業をスタートする予定である。

具体的には、ブランド物のスニーカーにスマートタグやスマートラベルを取り付けることで、消費者がスマートフォンで偽ブランド商品でないことを確認できる仕組みを導入する予定である。

スマートタグやスマートラベルは取り外そうとすると、アンテナが破壊されるため、これらを偽ブランド商品に付け替えることはできない。購入者は、当該商品を所有していることを、ブロックチェーンに登録できる。ネットオークションでも、ブランドが本物であることを確実に証明できるため、偽物リスクの無い売買が可能になる。

一方、ロンドンの Everledger 社は、大型のダイヤモンドの一つ一つについて、40 種類の特徴を記録し、鉱山で発掘された段階から宝石として個人に所有される段階まで、その所在を追跡できる仕組みを既に実用化している。これにより、いわゆる「紛争ダイヤモンド（blood diamond）」の流通を防ぐこともできる。また証明書の偽造、あるいは盗難、転売も抑止できる。盗難により所有者に保険金が支払われた場合、ダイヤモンドの所有権が保険会社に移るため、大手保険会社もこの仕組みに参加している。オンライン上での売買の際も、商品が本物であることを証明できるというメリットがある。

Everledger 社は、2015 年 6 月、バークレイズ銀行の TechStars fintech アクセレレーターの支援を受け、ロンドンの Eris Industries 社の開発したプラットフォームを利用して、上記の仕組みの実用化を実現した。既に数十万個のダイヤモンドが、この仕組みに登録されている。同社はこの仕組みをダイヤモンドだけではなく、時計やデザイナーバッグ、美術品等、他の高額商品にも応用していくことを計画している。

4）ギフトカード、マイレッジ

POS システムの大手 First Data の子会社で、ディジタル・ギフトカードの会社である Gyft は、サンフランシスコの新興企業で、ブロックチェーンのサービス・プロバイダーである Chain 社と提携し、ブロックチェーン上で管理されるディジタル・ギフトカードの発行を予定している。ブロックチェーンの利用により、現行のディジタル・ギフトカードよりも格段に安くセキュリティを確保できるため、スモールビジネ

スでもギフトカード・プログラムを導入することが容易になると期待されている。

Chain 社は、この他、飛行機のマイレッジ、各種のポイント等、価値を持つ様々なものを、ブロックチェーンを用いて管理するアプリケーションの開発用ソフトウェアを提供している。なお同社は、後述するように NASDAQ OMX のブロックチェーン・イニシャティブのパートナーともなっている。

５）ID カード

カリフォルニア州パロアルトの ShoCard 社は、モバイルで管理できる ID カードを開発中である。個人の各種の情報をブロックチェーン上で暗号化して管理し、各種の本人確認のニーズに対応できる形とする。

例えば、クレジットカードで支払う際に、ShoCard 社のアプリ上で認証を行う仕組みにできる。このため、クレジットカードが盗まれても、本人以外による支払いを避けることができる。この仕組みは、既存の個人認証の仕組みよりも、コストが大幅に低いとされる。

６）音楽

PeerTracks 社がローンチ予定の事業は、音楽のストリーミング・サービスを行い、リスナーが直接アーティストに料金を支払うことを可能にする仕組みである。スマートコントラクトを用いることで、アーティスト以外の関係者、例えば作詞者、作曲者、伴奏者等への収益分配も、予め設定された割合で自動的に行われる。また個々のアーティストが一種の暗号通貨である「トークン」を発行する。これはいわばトレーディング・カードであり、アーティストの人気によって価格が変化する。初期に才能あるアーティストを見出し、トークンを購入した人は、トークンの上昇によって利益を得ることできる。この他、トークンの保有者に対して、特別のサービスを提供することもできる。

Ⅲ 金融分野における取組み

１．高まる関心と進展する取組み

JP モルガン・チェースでクレジット・デリバティブを開発したメンバーの一人として有名な Masters 女史は、2015 年、ブロックチェーン関連の新興企業の CEO に就任して話題を呼んだ。就任して間もなく、彼女はコンファレンスにおいて、金融取引のフロント・エンドでは、ナノ秒単位のレスポンスが競われているのにも関わらず、ウォール街のバックエンド・システムは数十年にわたり根本的な見直しがなされていないと批判し、注目を集めた。

ブロックチェーンは、まさにこうした問題への解決策となりうるテクノロジーとして、

昨今、各国の金融資本市場関係者の間での関心が高まっており、具体的な取組みも進展しつつある。

EU の証券監督当局である ESMA（European Securities and Markets Authority、欧州証券市場監督局）は、2015 年 4 月に仮想通貨やブロックチェーン・テクノロジーを使った投資に関する情報収集を行ったが[4]、これに対する回答の中で、ドイツ銀行は、ブロックチェーンに関して以下のような応用分野がありうるとしている。

- （暗号通貨ではなく現行の）支払・決済
- 証券の発行と売買
- 証券の清算と決済
- 配当や金利の支払い、コーポレート・アクションの自動化
- デリバティブ契約の執行やスマートコントラクトを用いたデリバティブの清算
- 資産の登録
- 本人確認や反マネーロンダリングのための登録や監視
- 顧客向け、規制当局向けのレポーティング

ドイツ銀行は、ベルリン、ロンドン、シリコンバレーの 3 か所にイノベーションラボを立ち上げ、同行のディジタルバンク化のために 2020 年までに 10 億ユーロを投資することを計画しているが[5]、このイニシャティブにおいて当初よりブロックチェーン・テクノロジーに注目しているということである。

この他、バークレイズ銀行では、ブロックチェーンの金融への応用に関し、20 件ほどの実験に取り組んでいるという。またシティグループにおいては、6 つのインハウス実験を行っており、その一環で Citicoin という実験用の仮想通貨も導入しているという。UBS は、2015 年 4 月に、ブロックチェーン・ラボを設置し、25 を超えるプロジェクトに取り組んでいる。

銀行横断的な取組みもある。すなわち、2015 年秋、金融テクノロジーのベンチャー企業である R3 の主導により、世界的な金融機関とのパートナーシップが形成され、ブロックチェーンやその派生技術の業界標準規格を検討し、新たな取引ネットワークの構築を目指すこととなった。

同プロジェクトには、当初、JP モルガン、ゴールドマン・サックス、ステートストリート銀行、バークレイズ銀行、RBS、UBS、クレディスイス、BBVA、コモンウェルスバンクの 9 行が参加を表明したが、その後、新たにシティグループ、ドイツ銀行、三菱 UFJ フィナンシャル・グループ等、13 の金融機関も加わることとなり、世界の主要 22 行が参加する一大国際プロジェクトとしてスタートすることとなった。

---

[4] European Securities and Markets Authority, "Call for evidence, Investment using virtual currency or distributed ledger technology", 22 April 2015.

[5] 2015 年 4 月に発表された Strategy 2020 におき、6 つの key decisions の一つとして、Digitalize DB（Deutsche Bank）が掲げられている。

２．決済業者における取組み

このように大手金融機関においては、ブロックチェーンに関する実験的な取組みが行われている段階であるが、一部のベンチャー企業等においては、実用化の動きや実用化に向けた具体的な取組みの動きもある。

例えば支払・決済の分野では、ロンドンの Earthport 社が、サンフランシスコの Ripple と提携し、2015 年 8 月に、ブロックチェーンを使ったリアルタイムの国際送金ネットワークをスタートさせた。同社の CEO は、ゴールドマン・サックスのグローバルテクノロジー・システムのヘッドであった人物である。

コルレス銀行を経由した既存の銀行間の国際送金の仕組みは、数十年前から利用されているが、時間やコストのかかる非効率なものであった。同社は、この点を解決すべく 1997 年に設立された。銀行は Earthport を通じることにより、コルレス銀行を経由せず、低コストかつ迅速に国際送金を行うことができる。バンクオブアメリカや HSBC、アメリカンエクスプレス等が同社の顧客となっている。同社の従来のサービスでは、リアルタイムの送金は不可能であったが、Ripple のネットワークを使うことにより、今回、これを可能としたのである。

３．資本市場分野の取組み

資本市場分野では、前記のように大手金融機関による取組みも行われつつあるが、以下のように取引所や発行体、ベンチャー企業主導の注目される取組みもある。

１）NASDAQ

NASDAQ OMX は、NASDAQ Private Market においてブロックチェーンの利用に着手している。NASDAQ Private Market LLC は、NASDAQ OMC が 2013 年 3 月に、未公開企業の株式関連の業務をサポートすべく、SharesPost, Inc.とのジョイントベンチャーとして設立した組織である。

近年、米国では、多くのベンチャー企業が IPO を急がず、ベンチャーキャピタル等より潤沢な出資を受けつつ、未公開のままその規模を拡大させているという状況があることを受け、取引所としてもこれら未公開企業への関与を強めていくことが重要となっていることがこの背景にある。

具体的には、未公開企業の株主の管理、ストックオプション管理、IR、ディスクロージャーのサポート、役職員の保有株の売却ニーズへの対応を行う他、2014 年 5 月からは、株式の発行や売買を行うマーケットプレースをスタートさせた。株式の売買は、傘下の ATS（Alternative Trading System）である NPM Securities, LLC を通じて行われる。未公開株専門の証券会社が会員となり、適格投資家が、これら会員証券会社を通じて、未公開株の売買に参加できる。2015 年 5 月時点で、75 社の未公開企業

が同市場に参加している。

未公開企業においては、制度上、投資家となれるのは適格投資家に限定されている他、誰が株主となるかをコントロールするニーズもあり、これらの点の確認作業が必要である。これらの作業は、法律事務所が関与し、多くの書類やスプレッドシートを用いながら、もっぱら手作業で行われてきたという。

ATS を通じた流通市場の設立は、未公開企業の株式の円滑化につながるが、さらなる効率化のための取組みとして、NASDAQ OMX は、2015 年 5 月、ブロックチェーン上のカラードコインの仕組みであるオープンアセット・プロトコルを、Private Market の取引処理に利用する構想を発表した。6 月には、Chain 社との提携を発表し、本年中にシステムを稼働させることを目指している。Chain 社が、同システムで取引される最初の銘柄の一つとなる予定である。

NASDAQ OMX は、ブロックチェーンの活用を組織全体のイニシャティブの一環として位置付けており、Private Market におけるブロックチェーンの活用が成功すれば、このテクノロジーを、他の分野にも応用していくことを予定している。

２）Symbiont

2015 年に発足したニューヨークの Symbiont 社は、ブロックチェーン上で未公開株を、スマートセキュリティという形態で発行し、取引することを目指している。例えば、社債をスマートセキュリティとしてプログラムし、ブロックチェーン上に登録すると、売り手と買い手は清算機関や証券保管機構等を介さず、P2P（Peer to Peer）で売買を T+10 分といったスピードで完結でき、また発行体は利払い日に、クーポンを全ての社債保有者に自動的に支払うことが可能となる。2015 年 8 月に、最初のスマートセキュリティが発行された。

当初はビットコインのブロックチェーンを用いるが、プラットフォームとしては、より進化した将来のブロックチェーンに移行可能なものとなっているという。

同社には、ニューヨーク証券取引所の前 CEO である Niederauer 氏も、役員及び投資家として参画している。

３）Overstock.com Inc.と t0

Overstock.com Inc.は、ナスダックに上場する米国のリテール向け電子商取引会社の大手である。同社は、破綻した 20 社ほどのドットコム企業の在庫や備品等を消費者向けに安売りするプラットフォームとしてスタートしたが、その後、新品の商品の販売も含め、様々な分野の商品のオンライン販売に進出している。

同社は、2014 年 1 月からビットコインによる支払いを受け入れている。これは、大手の小売店によるビットコイン受け入れの第一号であった。同社はビットコインでの売上の 4%を、暗号通貨関連の財団に寄付している。

このように同社は、ビットコイン関連のテクノロジーに対する関心が高い企業であ

るが、ビットコインやブロックチェーンのテクノロジーを証券市場分野に応用すべく、Medici というプロジェクトを立ち上げている。同社は、かつて株式市場における空売り行為を積極的に批判し、訴訟を起こすなど、既存の証券市場のあり方に対する問題意識が高い。そこで新たなテクノロジーを活用し、自ら証券市場を革新しようと考えているのである。

このプロジェクトの一環として、2015 年 6 月、同社は t0.com というブロックチェーンを活用した証券取引プラットフォームを通じ、自ら社債を私募発行（レギュレーション D の Rule506 に基づき適格投資家向けに発行）した。同社債は、5 年債で、500 万ドルを FNY（First New York）Capital の関連会社が購入した。

この社債においては、ビットコインのブロックチェーンをベースとしたカラードコインの仕組みが使われている。t0 とは t+0、すなわち取引が行われると即時に決済されることを意味する。同社は、t0.com を通じた公募発行を行うことを目指し、2015 年 4 月に SEC に公募発行の登録申請書類（FormS-3）を提出しているが、まだ承認は得られていない。

４）Digital Asset Holdings

ニューヨークの Digital Asset Holdings LLC は、不特定多数が参加するブロックチェーンと、クローズドな参加者による分散型レッジャーを組み合わせた技術を開発した Hyperledger 社を買収し、金融機関や金融インフラ組織が、既存のシステムやネットワークも利用しながら、様々な金融取引を飛躍的に効率化する仕組みを普及させようとしている。

同社は 2014 年に設立されたばかりであるが、2015 年、先述の通り、JP モルガン・チェースの Masters 女史が、従業員が 20 名に満たないこの新興企業の CEO に就任したことで、大きな話題を呼んでおり、各種のプロジェクトに大手金融機関を多数参加させることに成功している。

現在、主として取り組んでいるのは、シンジケートローン、米国財務省証券のレポ取引、未公開企業の株式取引であるが、この他、外為取引、金利スワップ、デリバティブ、公開企業の株式、取引報告、ファクタリング、通貨、債券等への応用が構想されている。

現状、シンジケートローンの実行には、多くの手作業や書類、電話やファックスでのやりとりが必要となり、完了までに平均 20 日以上かかるが、新たなテクノロジーの利用により、大幅な効率化が実現し、リードマネジャーのリスクも削減されるという。

また米国財務省証券のレポ市場は、金融危機後、参加者にリスク回避の姿勢が強まったことや、金融機関に対する流動性比率規制が強化されたことから、取引が縮小している。そこで同社の仕組みを導入することで、流動性の向上、リスクの低下が期待されるという。

４．ブロックチェーンがもたらす新しい金融

これまで見てきたように、ブロックチェーンを活用することにより、金融商品の保有や取引に関するデータを管理するという業務が大幅に見直される可能性がある。データ管理を主業務としてきた機関については、そもそも不要とされていく可能性もあろう。

利払いや配当支払い、コーポレート・アクションの自動化が現実のものとなれば、これに係ってきた業界に大きな影響をもたらそう。

この他、いくつかの興味深い可能性も指摘されている。例えば、現状、基本的に 1 日が最低単位となっている付利を、より短い期間、例えば 1 時間単位で付利される金融取引も可能となり、1 時間から 24 時間までのイントラデイ・イールドカーブが実現する。この結果、よりきめ細かく収益機会を追求できるようになる可能性があるという。

また中央銀行が、紙幣ではなくディジタル・カレンシーを発行することも構想されている。2015 年 2 月、バンク・オブ・イングランドは、中央銀行を取り巻くファンダメンタルな変化に対応するためのリサーチ・アジェンダを打ち出したが、そのコアのテーマとしてこのディジタル・カレンシー発行の是非が位置付けられている[6]。これが実現する場合、金融政策のあり方や、銀行預金の位置づけがどう変わるのかも、論点となっている。

これに関連し、バンク・オブ・イングランドのチーフ・エコノミストである Haldane 氏は、マイナス金利導入の必要性を主張するスピーチの中で、中央銀行が紙幣に替えて暗号通貨を発行することにより、マイナス金利を簡単かつ迅速に導入できると指摘している[7]。

Ⅳ 今後の課題

１．ビットコインに係る課題

ブロックチェーンに記録された情報が改ざん不能であり、高度のセキュリティが確保されているとしても、ブロックチェーンを活用した全ての経済活動の安全性・確実性が保証されているわけではない。

まず利用者の秘密鍵の情報が盗まれれば、盗んだ人間が被害者に成り代わって取引の当事者となることができる。ただしこの種のリスクは、他の取引、例えば銀行取引でカードの暗証番号やインターネット取引のパスワード等を他人に知られる場合でも生じるため、ブロックチェーン特有のものとは言えない。秘密鍵はパスワードと異なり、オフラインで電子署名に使うことができるため、パスワードより安全とも言える。

あらゆる取引が完全にブロックチェーン上で完結するのではなく、第三者の信頼性に依存せざるをえない部分があることから生ずるリスクもある。例えば法定通貨をビットコイ

[6] Bank of England, "One Bank Research Agenda", Discussion Paper, February 2015 及び Michael Kumhof, "Response to Fundamental Change", One Bank Research Agenda－Launch Conference, February 2015 参照。

[7] Andrew G. Haldane, "How low can you go?", speech at Portadown Chamber of Commerce, Northern Ireland, 18 September, 2015.

ンに交換する場合、ビットコイン交換所やビットコイン販売所、専用 ATM 等に法定通貨を入金することが一般的であるが、これらの関係者が不正を行ったり、セキュリティ上の問題を抱えているリスクがある。先述の通り、一部の交換所においては、ビットコインと円やドルの間で頻繁に売買する投資家の便宜のため、預り金口座とビットコイン口座を管理している場合が多いが、この不正流用と交換所の破綻という事態が発生し、分別管理も行われていない実態も明らかとなった。

ビットコインにおいては、匿名性を巡る問題もある。ビットコインを取得、使用する上で、ウォレットを導入し、アドレスを取得する必要があるが、その際、こうしたサービスを提供する会社側が、一定の本人確認を行うことが一般的である。しかしこれは必ずしも国際的なルール等により強制されているわけではない。本人確認が適切に行われているか、マネーロンダリング対策が行われているか等、規制も監督も発展途上である。

以上のようなことから、ビットコイン関連のビジネスを行う者に対して登録制や免許制の導入等、制度的な枠組みの必要性が指摘されているのは当然であろう。2015 年 6 月には、金融当局の多国間組織であるマネーロンダリング対策に関する金融活動作業部会（Financial Action Task Force on Money Laundering、FATF）が、仮想通貨の交換所を登録制・免許制にしたり、マネーロンダリング規制を課したりすることを各国に求めるガイダンスを公表している。米国財務省の機関である Financial Crimes Enforcement Network（金融犯罪執行ネットワーク、FinCEN）は、2014 年 10 月、仮想通貨の交換所及び管理者を、マネーロンダリング・テロ資金対策の規制対象とする指針を発表した。またニューヨーク州金融サービス局は、2015 年 6 月、仮想通貨ビジネスに対する免許制を導入した。

ただし仮想通貨ビジネス従事者の信頼性や仮想通貨を用いたマネーロンダリング等の問題は、ブロックチェーンそのものの問題ではない。

またビットコインにおいては、どのアドレスからどのアドレスへいくらのビットコインが支払われているかが 1 件 1 件、全てほぼリアルタイムで公開されている。取引ごとにアドレスを変更するといった工夫がされることもあるが、必要があれば、インターネットの IP アドレス等、他の様々な情報と組み合わせることにより、あるアドレスの利用者がビットコインを武器や麻薬等の取引に利用していることを解明し、かつ本人を特定することも不可能とは言えず、そうした実例もある。むしろ、口座開設に利用された本人確認情報の正確性に依存する必要もなく、また銀行等にデータの提出を強制する必要もないため、ビットコインの取引の方が銀行取引よりも正確性や透明性が高いという評価も可能である[8]。もちろんドル紙幣等の現金を使った取引に比べて、はるかに匿名性は限定される[9]。いずれにしても、この点も、ビットコイン取引のあり方の問題であり、ブロックチェーンの問題とは切り離して考えることができる。

---

[8] U.S. Senate Committee on Homeland Security & Governmental Affairs, "Beyond Silk road: Potential Risks, Threats, and Promises of Virtual Currencies", November 18, 2013 参照。

[9] アドレスが公開されているという意味で、ビットコイン取引は、anonymous（匿名）ではなく pseudonymous（ペンネームの、変名の）の取引とされている。

２．ブロックチェーンに係る課題

ブロックチェーンそのもののリスクや課題としては、次のようなものが指摘されている。ブロックチェーンを用いた取引で、現状、最も活発なのはビットコインの取引であるが、現状、その設計は、少量の取引を想定したものとなっている。すなわちビットコインのプロトコルでは、1 ブロックが最大 1 メガバイトとされている。これは、1 秒間に 7 取引に相当する。これに対して例えば VISA の場合、平均、1 秒間に 2000 取引、1 日のピークでは 1 秒間に 4000 取引を処理しており、最大で 1 秒間に 56000 取引を処理する容量を有している。仮に、多額の経済取引をビットコインやビットコインのブロックチェーンを用いて行おうというのであれば、容量の拡大が不可欠である。

またブロックチェーンで記録が分散的に維持・更新されるのは、そうすることによりマイニング成功者が報酬を得ることができるという、インセンティブ・メカニズムが機能しているからである。仮にこのインセンティブが十分なものでなくなれば、ブロックチェーンは維持されなくなる。ビットコインの場合、現状、主たる報酬は追加的に発行されマイニング成功者に付与されるビットコインであるが、この金額は 21 万ブロックごとに半減していくため、2140 年頃にはビットコインが発行上限に達し、その後は、手数料のみによって彼らの報酬が賄われなければならなくなる。将来的に十分なマイナーの活動が確保され続けるための手数料はどのような水準となるのか、現時点では予測し難い。従って単純なコスト比較において、信頼できる第三者と集中的データ管理機関等に依存したシステムに比べ、ブロックチェーンによる分散型システムが格段に低コストであり続けるとは断定できないとの指摘がある。

この他、ブロックチェーンが改ざん不能であるというメリットは、取引のキャンセルややり直しができないというデメリットももたらすとの指摘がある。信頼できる第三者を介した取引であり、集中記録機関があれば、この仲介者が間に入り中央の帳簿を訂正することも可能かもしれないが、完全な分散型システムでは困難とされる。

以上の問題は、ビットコインのブロックチェーンに依存する場合の問題であり、ビットコインのような完全に分散的でオープンな仕組みである必要がないのであれば、別途、関係者が独自のクローズドなブロックチェーンの仕組みを導入するなどして、これらの問題を回避できる可能性がある。

この他、ブロックチェーン上の資産の法的性格、所有権の行使、会計や税務上の取り扱い等が明確になる必要がある。法的な検討は、既にいくつかの国において取り組まれているとされ、米国においても、バーモント州政府が、2015 年 6 月、州法上、ブロックチェーンを法的な記録の手法として利用しうるかどうかについての検討を諮問している。

ブロックチェーンは革新的なテクノロジーである故、その存在を前提として形作られていない現実の制度・慣行と対峙する際、様々なフリクションが生じるのは当然であろう。しかしその一方、今日、クレジットカードやインターネット・バンキング等を巡る不正行為は、日常的な出来事となっており、そこから生じる損失は毎年膨大な金額に上るという

現実がある。また、既存の金融取引にはコストの高さの問題もある。ナノ秒単位のトレーディングが行われるようになった一方で、取引完了までに何日もかかる状態が過去何十年も変わっていないという問題も深刻と言える。今日の金融取引が抱えるこうした問題の重大性とも対比しつつ、新たなテクノロジーの潜在的問題を評価し、そのベネフィットを追求していくことが重要であろう。