

第8章（講演録）ブロックチェーンと生産性向上

高木 聡一郎¹

【要旨】

ブロックチェーンとは、インターネット技術上に構築される価値（資産）交換の分散型インフラ技術である。ブロックチェーンには3つの要素があり、①データの連結によりデータ改ざんが困難、②情報資産とエンティティ（主体）の紐付けによる情報の所有、流通、用途の管理、③P2Pでのデータ管理・合意形成による信頼性向上と中央管理者が不要となることである。ブロックチェーンのようなリーダーなき分散型台帳の世界では、いかに台帳間の合意（コンセンサス）を取るかが最も難しい点になる。ビットコインでは、報酬を組み込んだインセンティブ付けが設計されている。近年は仮想通貨に注目が集まっているが、海外では政府が社会保障給付や不動産登記・売買を対象に実証実験を行う動きがある。また、電力、モバイルペイメント、地域通貨等、実生活に近いところでブロックチェーン技術が使われ始めている。

ブロックチェーンはマクロレベルでの経済的変容をもたらす。情報の信頼性が組織に依存しないことから、誰もがミクロな経済圏を生み出す可能性がある。個人あるいはスタートアップ企業でも簡単にサービスを立ち上げることが可能となるため、例えばIoTと決済の融合など、よりミクロな経済取引を実現できる可能性が高まる。それにより、今まで顕在化していなかった価値を獲得することが可能となる。ブロックチェーン技術によってミクロの経済取引を底上げし、さらにマクロ経済のプラス寄与につながるような使い方の研究が今後重要である。

1. ブロックチェーンとは:仮想通貨を中心に

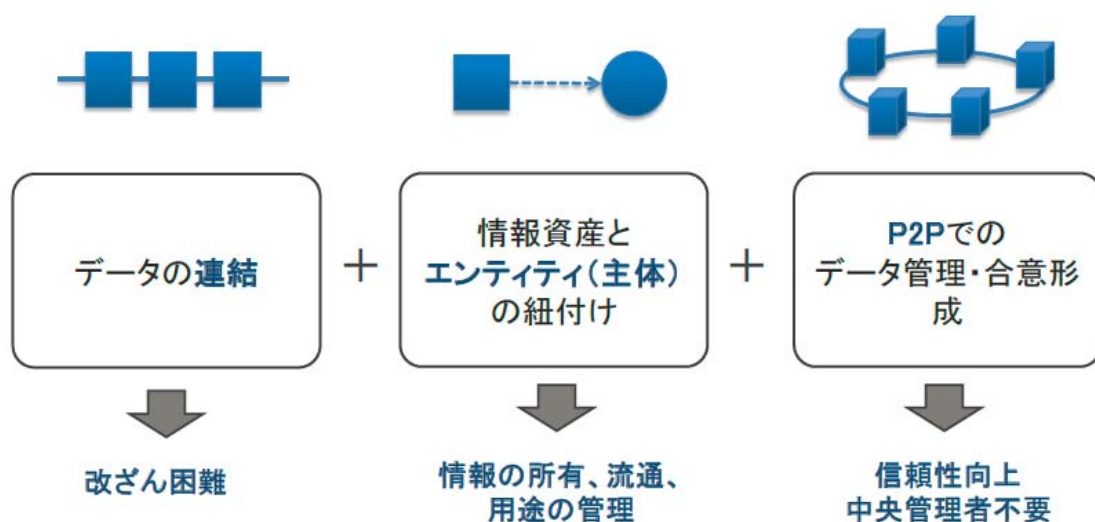
仮想通貨は、判明しているだけで約1,300種類、仮想通貨全体の時価総額は約30兆円にも上り、中小規模の国のGDPに匹敵する時価総額となっている。その時価総額の約半分をビットコインが占めているといわれている。ブロックチェーンを定義するのは非常に難しいといわれているが、通常ブロックチェーンと呼ばれるものには以下の3つの要素が含まれる（図表1）。1つ目はデータの連結によりデータ改ざんが困難になるという特性、2つ目は情報資産とエンティティ（主体）の紐付けによる情報の所有、流通、用途の管理への適応、3つ目はP2Pでのデータ管理・合意形成による信頼性向上と中央管理者を必要としない性質である。

上記3つの要素から考えると、ブロックチェーンとは、インターネット技術上に構築される価値（資産）交換の分散型インフラ技術といえる。現在のインターネット上でも企業

¹ 国際大学グローバル・コミュニケーション・センター准教授／主幹研究員、研究部長

が仲介する形で資産の移転は簡単に行われているが、ブロックチェーンはそのような仲介者が不在であっても資産の移転の履歴を管理することができる点が、現状のインターネットとの相違点である。

図表1 ブロックチェーンの3大要素



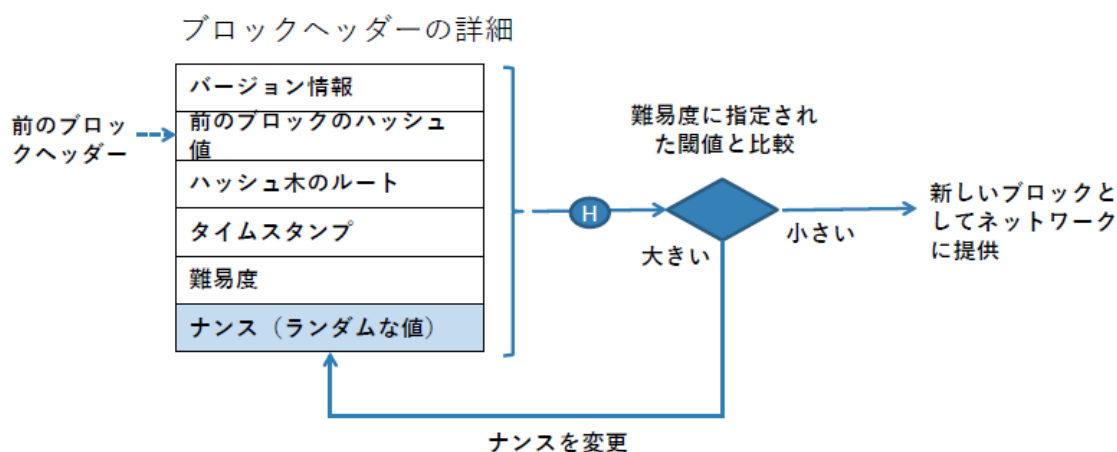
(出所) 筆者作成。

また、もう一つ重要なのがスマート・コントラクトという概念である。ブロックチェーン上のプログラムとしてのスマート・コントラクトという仕組みは、静的データの保存を行うデータベースとしての機能だけでなく、その上でソフトウェアが動作するプラットフォームとしての機能も持ち合わせている。具体的には、自分で作成したソフトウェアを不特定多数のコンピュータに分散しておいて、条件が整えば自動的に起動し、処理を実行することが可能となる。基本的にはどのような処理も記述可能(チューリング完全)であり、外部API(Application Programming Interface)との連携も可能となりつつある。ブロックチェーンは、スマート・コントラクトの仕組みにより、分散されたネットワーク型のコンピュータとして、誰もが使えるインフラへと変化している。

ブロックチェーンのデータ更新は台帳の更新という形で処理される。リーダーなき分散型台帳の世界では、いかに台帳間の合意(コンセンサス)を取るかが最も難しい部分となる。この問題を解決する方法として、分散型台帳の更新は自由競争の中で参加者が新規ブロックを作成し、最速で作成した参加者がそのブロックを共有することで行われる仕組みとなっている(図表2)。例えばビットコインを取り上げると、ビットコインの台帳の更新は、コンピュータの中に溜まっていく世界中のビットコインの取引データを10分おきにブロックという形に固めて台帳の最後に付け足すことで行われている。その最後のブロックを参加者に送る前にProof of Work処理(ハッシュ処理)を行うが、最速でこの処理を解き、

新しいブロックを提供した参加者には報酬としてビットコインが付与される仕組みとなっている²。ビットコインには中央銀行のような機能や決済サービスのような機能もあるが、それを組織ではなく分散化された参加者の間で分担して行うという特徴がある。

図表2 新規ブロックの作成



(出所) 筆者作成。

このブロックを作る作業（マイニング）には大きな課題が存在する。マイニングは単純な計算処理を膨大に行う必要があるため、電気代は重要な問題である。また、マイニングには処理に適した専用のハードウェアがあり、それを所有しているかどうかで競争力に差異が生じる。こうした環境がマイニングの競争を激しくし、従来は不特定多数のコンピュータで分散的に行うことを想定していたが、徐々に寡占状態に陥ってきている。現在マイニング事業は上位5社が全体シェアの約半分を占めているといわれている。最近では日本でもこのマイニング事業に参入する企業が増えてきている。

現在非常に問題になっているのは、このマイニングがエネルギーを非常に浪費しているという点である。ビットコイン価格が高騰し、マイニングへの参入者が増加し競争が激化することで、マイニング難易度が調整され上昇し、計算処理に伴う消費電力が増加し電気代が上昇するという事象を招いている³。現在、ビットコインのマイニングに係る電力消費量は35TWh⁴で、電気代は年間約17億ドルにも上るとも言われている。これはデンマーク等の年間電気消費量を超えている。最終的にはハードウェアの価格を除くと、このビットコインの価格と電気代が結果的に釣り合うようになる（図表3）。これは当初より意図されていたわけではないが、エネルギー価格をベースにビットコインが発行されている状態になっ

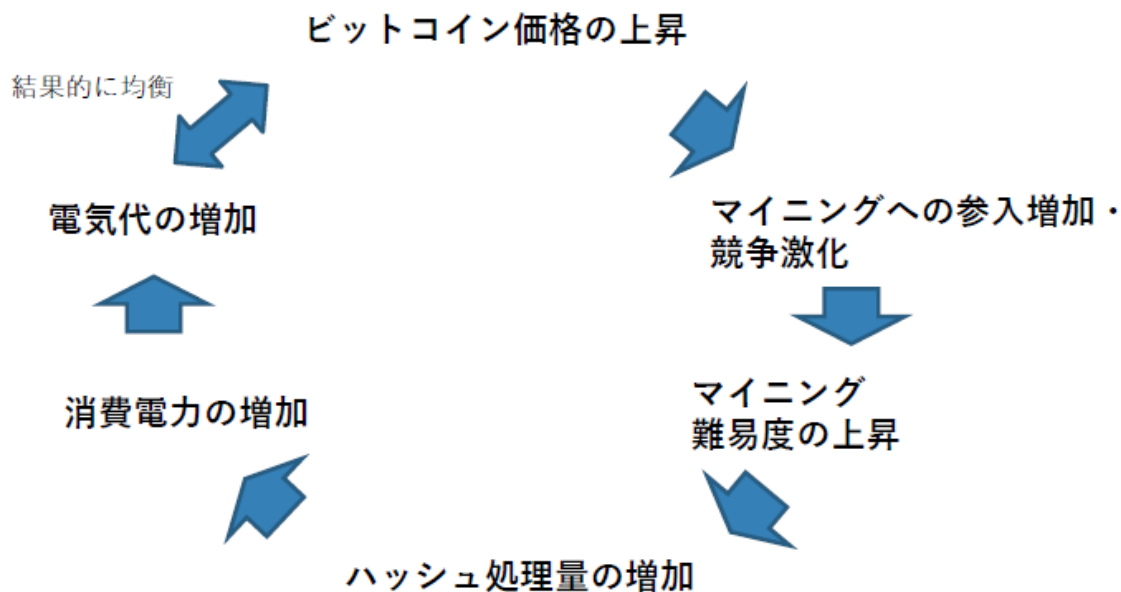
² ビットコインは全くの無から発行されるコインだが、ビットコインの量は4年毎に半分減る設計になっているため、どこかの時点で総発行量は頭打ちになる仕組みとなっている。

³ 逆方向のループもあり得る。

⁴ 出典：<https://digiconomist.net/bitcoin-energy-consumption>

ている。

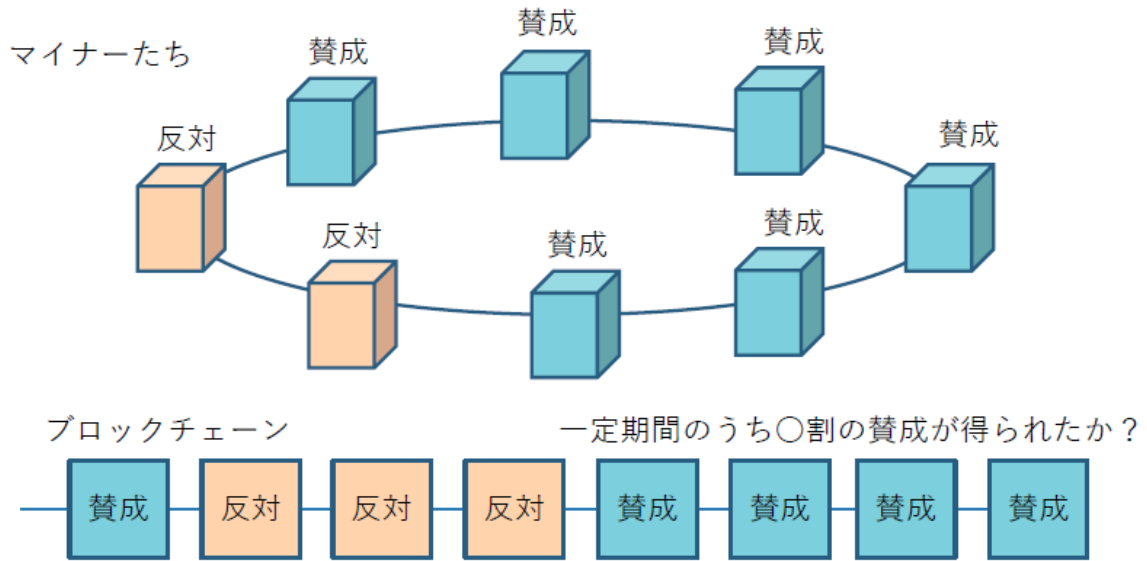
図表3 価格と電力消費の関係



(出所) 筆者作成。

もう一つの問題は、ブロックチェーンには決定事項を強制するメカニズムがないため、仕組みの改善を行う際に合意形成できず、常に分裂のリスクがあるという点である。ビットコインの世界は完全に分散化されており、リーダーが存在しないため、ビットコインの仕組みを改善・バージョンアップする際に参加者の合意形成がスムーズに出来ず、ある提案に対して賛成する者と反対する者に分裂することが起きる。つまり、ブロックチェーンには合意形成の落とし穴がある(図表4)。例えば、2017年8月にはビットコインからビットコイン・キャッシュが分裂した。しかし、分裂後にビットコインの値下がりは見られなかった。例えば、株式分割を考えると時価総額は一定で、中身だけを分割することになるが、ビットコインの分裂の際は、全体の相場が上がっている中で分裂すればするほど全体の時価総額が上がる状況になり、さらに分裂が進んでいった。ビットコインを預かっている取引所は、分裂の度に新たに発生したコインを自動的に保有者に付与させるように管理する必要が出てくるため大変な負担となっている。この点については決済サービスにおける生産性という観点から注意すべき点と考えられる。なお、仮想通貨そのものは価値がなく、何と交換するかで価値は決まるのであり、仮想通貨そのものは交換媒体に過ぎない。

図表4 合意形成の落とし穴



(出所) 筆者作成。

2. ブロックチェーンとは:様々な用途への展開

(1) 様々な用途への展開可能性

ブロックチェーンという技術は当初はビットコインを実現させるために生まれてきた技術であるが、より汎用的な用途への活用が検討されている。例えば、ブロックチェーンの改ざんが非常に難しい特性を使って、学歴の修了証書やダイヤモンドの所有、食品やチケットの転売や偽装防止などの用途への活用がある(図表5)。また、スタートアップ企業が資金調達をする際、株式を新規公開するように、当該企業が行っているサービスのコインを売り出して資金調達するICO(Initial Coin Offering)という方法もある。あるいは、地域通貨、社内通貨、生活保護の支払いに暗号通貨を用いるというアイデアも出てきている。ブロックチェーンが持つ、分散型組織への期待は高いが、実際は暗号通貨機能を別の用途で使うことが多い。

さらには、上述のスマート・コントラクトの機能を用いて電力取引や土地の登記に係る運用をある責任組織が行うのではなく、ブロックチェーン上にばら撒かれているソフトウェアで全て処理する仕組みを作ろうとする試みもある。このように「自律的分散組織」の特性を活用した、新しい組織の作り方やビジネスのやり方を試す動きが出てきている。

図表5 ユースケースの展開

	BC1.0	BC1.5	BC2.0
スマート コントラ クト			<ul style="list-style-type: none"> 電力取引 土地登記 シェアリング クラウドソーシング
台帳		<ul style="list-style-type: none"> ダイヤモンド 著作権 サプライチェーン 学歴 投票、公証 	<ul style="list-style-type: none"> 食品偽装 チケット 医療 難民ID
暗号通貨	<ul style="list-style-type: none"> ビットコイン 	<ul style="list-style-type: none"> カラードコイン オルトコイン 	<ul style="list-style-type: none"> ICO 地域通貨、社内通貨 社会保障 クラウドファンディング データ売買、IoT
プラットフォーム	Bitcoin	Bitcoin, Ethereum	Bitcoin, Ethereum+

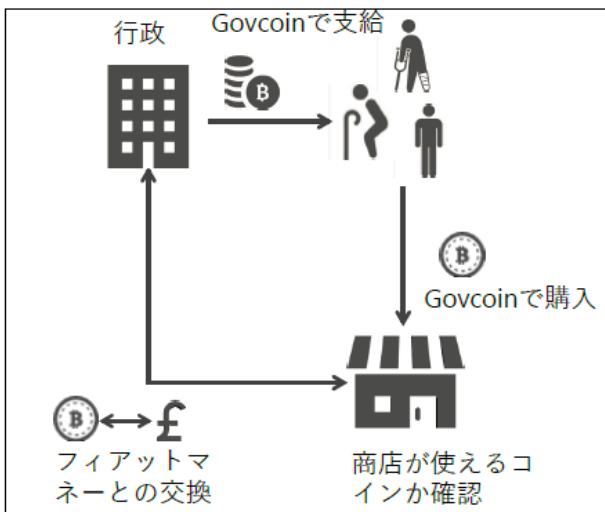
(出所) 筆者作成。

(2) 用途事例

①イギリスの生活保護費の支給の事例

イギリスの労働年金省(Department of Work and Pensions)が、マンチェスター市において生活保護費の給付に仮想通貨を使う実証実験を行っている。生活保護の目的に合致しない支出を制限するために、ポンドと固定レートで交換する Govcoin という暗号通貨を既存のビットコインのブロックチェーン上に新たに発行して生活保護費で購入できる対象を限定している。

図表6 暗号通貨の応用：社会保障給付



- ポンドと固定レートで交換する仮想通貨 (Govcoin) を用いて生活保護費を支給
- 生活保護費で買える対象を限定し、**制度の目的に合致しない支出を抑制**
- Bitcoinベースのカラードコインで実装

(出所) 筆者作成。

この事例で重要なのは、イギリス政府が新しいブロックチェーンを立ち上げて Govcoin を作成するのではなく、図表 6 のように既存のビットコインのブロックチェーン上に相乗りする形で発行するという形態をとっている点である。よって自分たちのコインを発行するためのインフラを新規で作らなくとも、既存のビットコインのブロックチェーン上で自分たちのオリジナルのコインを発行できる部分が新しい。

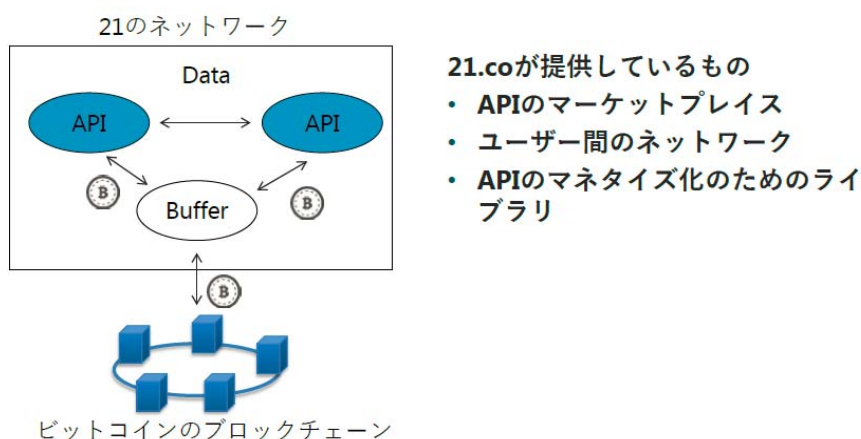
②スウェーデンの不動産登記・売買の事例

スウェーデン土地管理局では、スマート・コントラクトによる土地売買・登記システムを検討している。売り主のリードのもとスマート・コントラクト利用を開始し、売買の交渉・価格決定・銀行によるコミット・登記所による登記変更までカバーするシステムを想定している。対象となるプロパティの指定については公的な ID を利用する。これは不動産取引において幅広いステークホルダーのシームレスな連携を実現することを目的としているシステムである。またこの不動産登記に関するシステムについては、ホンジュラス、ジョージア、ガーナ等の国々でも検討している。

③API のマネタイズ化の事例

暗号通貨は完全なデジタルなものであり IoT との親和性が高い。IoT はデバイス同士が通信するので、人が介在しなくても仕組みの中に課金処理が可能のため、既存の API に課金を埋め込む仕組みの提供が可能となる（図表 7）。このアイデアをもとに、温度、湿度などを測定する環境センサーのデータは、従来であればそれを設置した人しか使えなかったが、ある決められた手順に従って一定のビットコインを支払えば、そのデータを利用することができる仕組みを提供する企業も現れている。つまり、微少のお金を支払うことで、世界中にある様々な環境にあるセンサーのデータをもらうという新しい使い方もある。

図表 7 21.co の Machine Payable Web



(出所) 筆者作成。

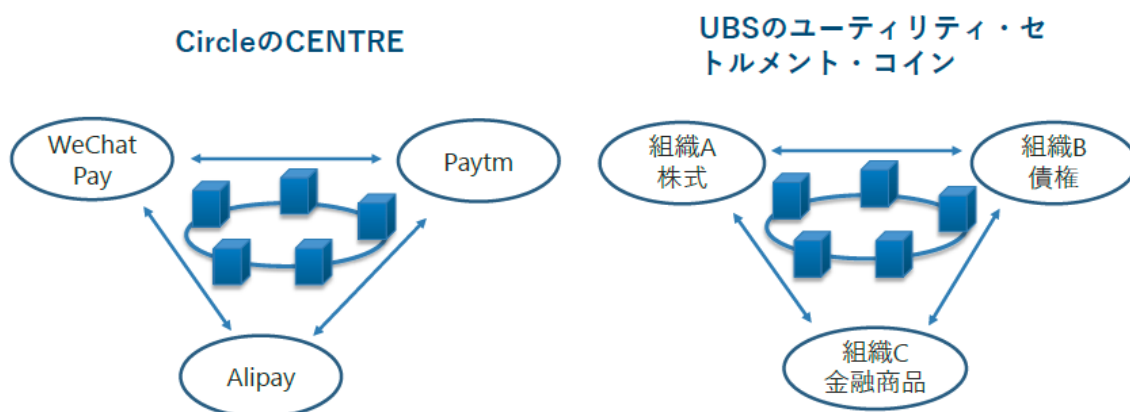
④電力のユーザー間取引の事例

別のIoTの使い方として、電力のユーザー間の直接取引がある。これは電力にIDをつけてどこで発電されたものか仮想的に分かる仕組みを作ること、電力会社を通すことなくユーザー間で直接売買するという取引方法が検討されている。これはブロックチェーンを使うことで、生み出される価値を記録して売買していくことが可能となる。この取り組みはもともと東京大学において、デジタルグリッドという名で研究されているものである。現在同様の試みはEV充電（ドイツ、アメリカ）、地域グリッド（日本・会津若松、アメリカ・ニューヨーク）でも検討されている。

⑤モバイルペイメントの事例

ブロックチェーンの不特定多数の人々の情報を共有しても非常に改ざんしにくいという特性を活かし、縦割りになっていたモバイルペイメントの異なるサービスをつなぐ役割としても期待されている（図表8）。例えばAlipay、WeChatPay、ApplePayなど様々なサービスが存在しているが、ApplePayの会員でなくともApplePayを受け入れているお店でも支払い可能にするなど、ブロックチェーンを媒介することで異なるサービス同士をつなぐという試みも行われている。これと同様に、株式や債券など、他の様々な金融商品間をつなぐという取り組みも検討されている。

図表8 分断されたサービスの「つなぎ役」



（出所）筆者作成。

また、日本では、福島県会津若松市で地域活性化を目的とした地域通貨「萌貨」の実証実験を行った。地域を活性化するためには、まず居住者が知り合い会話することが重要と考え、参加者間のコミュニケーションによりコインが新規発行される仕組みを作った⁵。従

⁵ ビットコインの例であれば、マイニングのような台帳管理をする貢献に対してトークンを発行する。「萌貨」の場合は住民が互いに会話をしたことに対してトークンを発行し、片方の人がスマートフォン振るこ

来の地域通貨は、円と1対1での交換か、自治体が税金で補填をしてプレミアムを出す仕組みであったが、この「萌貨」は0円の価値からスタートさせ、その地域である決済手段としてユーティリティを持たせれば持つほどその価値が徐々に上昇し、その結果地域の活性化に繋がっていくとの意図で行われた。長期的には、住民がその通貨の価値を高めるインセンティブを有するステークホルダーとなる仕組みにより地域内のコミュニケーションを活性化し、「萌貨」が地域の中での交換媒介として利用されることが期待される⁶。

⑥ICO

スマート・コントラクトを使ってサービスを構築する場合、サービスは成り立っているが運営者は不在であるため、結局は誰かが仕組みの開発や維持管理をしなければならないという問題が出てくる。自立分散型組織（DAO）の開発等を行う者へインセンティブを持たせる手段としてICOが注目されている。ICOは自律分散型組織による資金調達方法であり、あるサービスの中で使うトークンを売り出すことで資金調達を行い、その調達資金でサービスの開発を行うことが可能となっている。

実際にそのサービスが多く使われるようになれば、そのコイン（トークン）の値段が将来上昇するとの期待から、ICOへの投資が行われている。ICOによる資金調達は活発化しており、世界中で資金調達が行われている。しかし、ICOの仕組みとして何の責任も負わずに資金を調達できるようになってしまっているが故に、資金を集めたものの何もサービスが生まれなかったといった詐欺的な事例も散見されるようになってきた。そのため昨今各国において規制の是非が議論されるようになってきている。

(3) 用途展開に係るブロックチェーンの特性

ブロックチェーンを様々な用途へ活用していく上で注目されている特性は如何なる点であろうか（図表9）。最大の特徴は、情報の信頼性が組織に依存しないという点であろう。すなわち、アルゴリズム上改ざんされない、情報がなくなるといったことはほぼないために、情報の信頼性が組織に依存しなくても担保できる点に新規性を見出せる。通貨でいえば、中央銀行の信頼性に依存しない形で提供されるということになる。この点が従来と異なる部分である。

とで出現するQRコードをもう一人が読み込むことで互いに一定の萌貨を獲得できる仕組み。

⁶ この実証実験は1日限りのイベントであったため、今後継続的な実証が期待される。

図表9 一般的な活用法からみるメリット・デメリット

ブロックチェーンの要素	使い方の重点	応用例	メリット	デメリット・課題
<ul style="list-style-type: none"> 中央管理者不要性 資産の管理可能性 改ざん耐性 	一般的なデータベースの代わりとして使う	<ul style="list-style-type: none"> 土地・法人登記 サプライチェーン 利用履歴・信用情報 	<ul style="list-style-type: none"> 複数組織で使用する場合に特定の他組織に依存しない <u>情報の信頼性が組織に依存しない</u> オープン型であればコストが安い 	<ul style="list-style-type: none"> スピード、データ量、セキュリティに問題 クローズドで使うならRDBと要比較
	仮想通貨・トークンの機能を中心に使う	<ul style="list-style-type: none"> 仮想通貨 電力取引 銀行間決済 中央銀行デジタル通貨 社会保障支給 IoTデバイス間決済 	<ul style="list-style-type: none"> <u>通貨の信頼が組織の信頼に依存しない</u> 低コスト・スピーディに開発できる <u>決済処理をコード化しやすい (IoTへの応用)</u> <u>マネーに機能を付けやすい (使途制限等)</u> 従来より安いコストで決済・送金できる場合がある 	<ul style="list-style-type: none"> アルゴリズム上の安全性を確認できるか オープンに運用する場合のインセンティブ、クローズ的に運用する場合の信頼の源泉
	自律的なサービス稼働の仕組みとして使う	<ul style="list-style-type: none"> クラウドソーシング マーケットプレイス シェアリング 	<ul style="list-style-type: none"> <u>個人がより自律的に経済活動を行える</u> 手数料が安くなる場合がある 	<ul style="list-style-type: none"> イノベーションの担い手の報酬 運用の担い手、改善の意思決定と実施等

(出所) 筆者作成。

企業がブロックチェーンを活用する場合においては、現在大半がクローズドなブロックチェーンである「パーミッションド」と呼ばれる類型となっている。これは不特定多数の人が参入できるブロックチェーンではなく、企業の中だけで利用可能で、情報が外部から見えないブロックチェーンである。一方、上述のイギリス政府がビットコイン上で独自のコインを発行しようとしている試みは、公開されているインフラの上で自分たちのサービスを作っていくというサービスに該当する。様々な種類のブロックチェーンがそれぞれ互換性がない状態で乱立しているため、これが標準化されたインフラのような形で将来統一されていくかどうかは課題と言えよう。

3. マクロレベルでの経済的変容

ブロックチェーンの新規性は、上述したように情報の信頼性が組織に依存しない形になる点にある。例えば、通貨の信頼性が中央銀行の信頼性に依存しない形で提供されるということも可能である。組織を運用するコストがかからなくなるため、個人あるいはスタートアップ企業でも、ある決済サービス等を簡単に立ち上げることが可能となる。それにより多様でマイクロな経済圏を生み出す可能性がある。今まで顕在化していなかった価値を獲得し、取引を成立させるといったことができるようになり得るといふ点も新しい動きとして注目している。

また、ブロックチェーンは分散化されたインセンティブに基づく仕組みとなっている。

すなわち、トークンの発行により、契約関係のない相手にインセンティブを生じさせて業務を運営することになる。よって、何に対してトークンを発行するかという観点からインセンティブの設計ができるため、組織の在り方が今後変化していく可能性がある。

加えて、IoTやAIが普及していく中、マシンとマシンのやり取りの中に、仮想通貨・トークン、スマート・コントラクトの仕組みに基づく決済サービスが組み込まれることで、自動的・自律的に経済活動が回っていくようになる可能性もある。

4. 生産性を巡る論点

最後にブロックチェーンと生産性を巡る論点として、上述した内容への補足を含め以下に3点述べる。

1点目は、企業体としての組織を不要とするブロックチェーンの特性に係る論点である。ブロックチェーンは雇用契約に係る取引費用や組織運営のための制度設計にかかるコストなど、組織運営にかかる様々なコストを削減し得る可能性を秘めている。仮想通貨を例に挙げると、フィアットマネーと仮想通貨の比較が挙げられる。フィアットマネーと仮想通貨では特徴が異なるため単純な比較はできないものの、フィアットマネーの場合は中央銀行が相当の運営費用を負担している一方、仮想通貨の場合はマイニングに係る電気代を始めとするコストが発生している。ただし、仮想通貨の場合、マイニングの方式次第で、上述した電気代のようなエネルギーコストを改善する余地はある。

2点目は、企業という組織体の中でブロックチェーンを利用する企業の実産性に係る論点である。日本取引所が証券取引システムにブロックチェーンを使うという実証実験を行ったところ、一部のハードウェアやミドルウェアのコストを低下させる可能性が指摘された。現状では、ブロックチェーンの持つ情報の改ざん耐性の強さから情報セキュリティ対策費の一部削減には貢献し得るが、クローズドでオリジナルなブロックチェーンを使って立ち上げたとしても、従来型のシステムと比較して生産性が向上するとは言い切れない。

最後に3点目は、ブロックチェーンの活用が新たな経済活動を促進させる可能性を秘めている点が挙げられる。多様なコイン、トークンを誰でも発行できるようになれば、新たな価値を顕在化し、それを取引可能とすることで媒介手段として提供できる可能性がある。また、IoTと決済の融合など、よりマイクロな経済取引を実現できる可能性が高まる。

ブロックチェーンの技術を用いた研究が、経済全体の底上げにどのようにつながることができるのか、さらに国全体でみた場合マクロの実産性の上昇にプラス寄与になる使い方ができないかについての研究が今後重要である。