ブロックチェインの分類に関する一考察

国立情報学研究所　情報社会相関研究系 准教授　岡田（おかだ）　仁志（ひとし）

1. はじめに

金融と工学を融合したFinTechの分野において、ブロックチェイン技術の可能性が注目されている。ブロックチェイン技術は、分散型仮想通貨を支える技術として提案されたものであったが、その用途に限定されることはない。中心を持たないP2Pネットワークにおいて正確かつ効率的にデータを授受する特性を活かすことによって、あらゆる応用が可能になると期待されている。

こうした特性に着目して、複数の省庁等においてブロックチェインの可能性を議論する研究会が設立された。経済産業省は2016年2月にブロックチェインの産業への応用に関する研究会を開催し、同年3月に報告書を公表した。同年5月には、英文による報告書概要を公表している。

2016年4月には日本銀行にFinTechセンターが設立された。同月には、日本銀行にFinTech勉強会が設置され、情報技術、法律、及び経済の分野から有識者が参加して、ブロックチェイン技術の可能性に関する検討が行われている。

金融のコア技術に関する標準化を担うISO TC68には、2015年にデジタル・カレンシーの通貨記号に関する標準化を扱うSC7にサブグループが設置された。同サブグループは、2016年4月にフランクフルトで開催されたTC68の年次総会においてレコメンデーションを提案し、いずれも了承されている。レコメンデーションは仮想通貨の通貨記号に関する取扱いを規定したものであるが、付帯的な提案として、ブロックチェイン技術の応用可能性を議論する組織の設置がレコメンドされている。

ただし、この付帯的な提案については、オーストラリアの標準化機関であるStandards Australiaから、ブロックチェイン技術の標準化に関する新たなTCの設立が提案されたことを受けて、組織の重複を避けるため設置が見送られている。オーストラリア提案によるTCの設置については、本稿の執筆時点において、加盟国による投票の過程にある。

このように、ブロックチェイン技術の応用可能性については、仮想通貨としての実装だけでなく、FinTechの基幹技術としての活用が提案されている。さらには、金融分野に限定することなく、あらゆる産業分野への応用が検討されている。

2. 仮想通貨の要素技術として

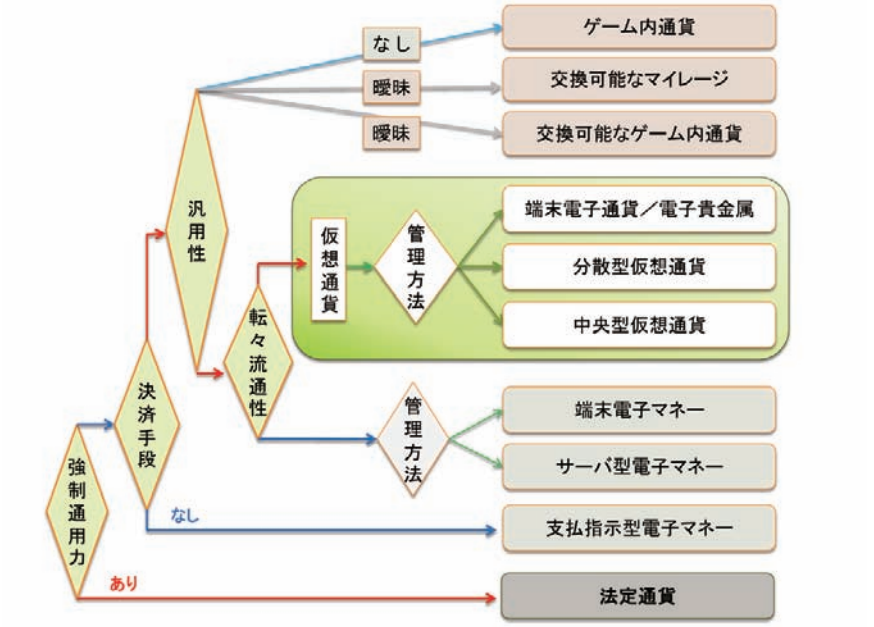
ブロックチェイン技術は、分散型仮想通貨の草分けであるBitcoinシステムの要素技術として実装されたことで注目を集めた。2008年に登場したBitcoinシステムは、取引の記録を不可逆的に記録するブロックチェイン技術、及び、時制的三式簿記と呼ばれる固有の記述方式などの組合せによって、P2Pネットワーク上における貨幣的な価値の流通を実現させた。ブロックチェイン技術はBitcoinシステムに代表される分散型仮想通貨を成立させる要素技術であるから、Bitcoinシステムの特性を理解することは、ブロックチェイン技術を理解するための有用なアプローチである。

ブロックチェイン技術の特性を分析する前提として、仮想通貨の特性を概念的に記述するならば、次のような要素を有するものであると定義することができよう。すなわち、仮想通貨とは、法定通貨のような強制通用力を持たない代替的な決済手段であって、利用場所が限定されない汎用性と、支払いの相手が限定されない転々流通性を兼ね備えるものである。

さらに、発行者との関係で仮想通貨の特性を分析すると、発行者の存在する中央型仮想通貨、管理者が貴金属などを引当てとして発行する電子貴金属、及び、特定の発行者が存在しない分散型仮想通貨の3類型に分けることができる（**図1**）。これらの3類型のうち、分散型仮想通貨においては信頼できる第三者機関が存在しないにもかかわらず、取引を不可逆的に記録する仕組みとして、ブロックチェイン技術及びその他の要素技術が実装されている。

分散型仮想通貨においては、ブロックチェイン技術を実装することは、おそらく不可避的である。これ以外の類型としての中央型仮想通貨、電子貴金属においても、ブロックチェイン技術を実装する場合がある。ただし、これらの2類型においては、ブロックチェイン技術を実装することは必須であるとは言えない。

このように、ブロックチェイン技術の特性は、仮想通貨の機能及び分類との関係で理解する限りにおいては明確である。しかしながら、ブロックチェイン技術を金融のみならず産業界のあらゆる取引の基盤へと展開する過程においては、改めてブロックチェインとは何かを議論する必要



■図1. 仮想通貨の特性と決済手段における位置付けに関する分類

	許可型	自由参加型
市場型	許可型パブリックチェイン	自由参加型パブリックチェイン
非市場型	許可型コンソーシアムチェイン	自由参加型コンソーシアムチェイン

■図2. ブロックチェインの分類（市場と許可の観点から）

がある。これが、昨今のFinTechを取り巻くブロックチェイン技術に関する議論の出発点である。

3. ブロックチェインの分類論

仮想通貨を定義することが容易ではないように、ブロックチェインを定義することも困難な試みである。ここでは、定義に関する議論には言及しないこととし、代わりに、ブロックチェインの機能に着目して、分類を試みることにする。

本章の議論は、『FinTechと金融サービスの将来像』（山崎重一郎）に依拠する。以下は、山崎教授のスライドにヒントを得て著者の解釈を論じたものであり、あり得べき間違いは著者の責任である。

3.1 自由参加型パブリックチェイン

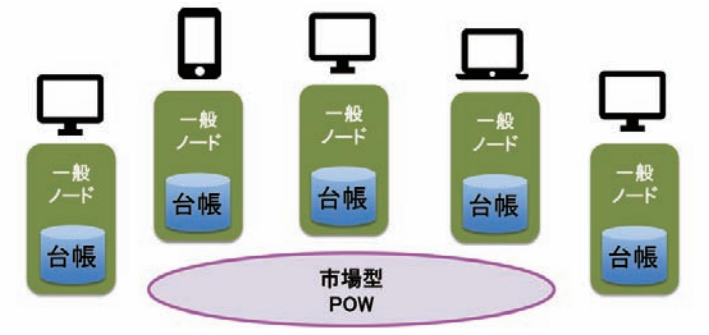
Bitcoinシステムを念頭に置くと、分散型仮想通貨のブロックチェインは、誰もが許可なくして「採掘」、すなわちマイニングを行う主体となることのできる、自由参加型の仕組みであることが分かる。マイニングの報酬として発生する仮想通貨をコインベースと呼ぶが、これを売買する市場が成立して、仮想通貨の価格が形成されている。

このようなブロックチェインは、自由参加型であり、市場型である（図3）。

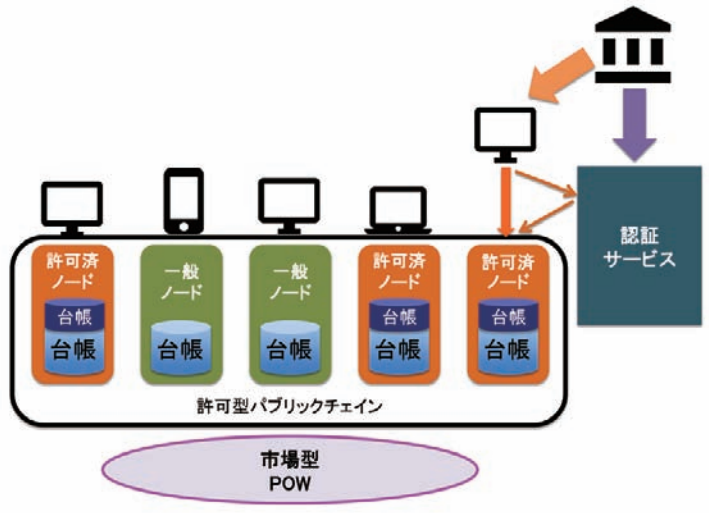
おそらく、自由参加型であることと、市場型であることは、相互に必然的な条件ではないが、理想的な関係にある。なぜなら、何らかの主体による調整を受けない自由参加型のブロックチェインにおいて、マイニングを行うフルノードとして参加するマイナーを維持するためには、価格形成のための市場が成立していて、報酬としてのコインベースを受け取るインセンティブが維持されることが必要とされるからである。

Bitcoinシステムと同様の構造を有するAlternative Coinsと呼ばれる分散型仮想通貨においては、同じく、誰もがフルノードで参加することのできる自由参加型のブロックチェインが採用されており、コインベースを受け取るインセンティブとしての市場と価格が形成されている。ただし、広義のAlternative Coinsにおいては、Bitcoinシステムとは異なる構造を有するものを含む場合がある。

例えば、仮想通貨の市場においては、広義の仮想通貨として、中央集権型仮想通貨に価格が形成されることがある。これらの中央集権型仮想通貨は、中央に発行主体が存在していて、発行量及び取引の承認プロトコルの全てを発行主体が意図的に管理するものである。この場合にも、



■図3.　自由参加型パブリックチェイン



■図4.　許可型パブリックチェイン

効率性の観点からブロックチェインに類した構造をとる場合があるが、1つの主体が唯一のフルノードとして参加するプライベートチェインであるから、そもそもブロックチェインの条件を満たさないと考えられる。これについては諸説あるが、本稿では、プライベートチェインをブロックチェインの分析対象に含めないこととする。

3.2　許可型パブリックチェイン

さて、Bitcoinシステムにみられるように、自由参加型パブリックチェインにはインセンティブとしてのコインベースを流通させる市場が形成されるが、許可型パブリックチェインにも市場が形成される。ここで、許可型のブロックチェインというのは、取引を検証してブロックを生成する権限を有するフルノードが、認証局による許可を受けたノードと、単に実在性だけを認証された一般ノードとの混成によって成立している場合を指す。

自由参加型パブリックチェインと許可型パブリックチェインの違いは、参加するノードが信頼できる第三者による実在性の認証を受けているか否かに存する。そして、認証局の運営を支配する主体が、さらに特権ノードとして何らかの権限を与えたノードのことを、許可済みノードと呼ぶ。

こうしたブロックチェインは、許可型であり、市場型である（図4）。

ところで、自由参加型パブリックチェインの典型であるBitcoinシステムにおいては、信頼できる第三者が存在しなくても記録の正しさが担保されるように、計算量に応じた多数決の仕組みが実装されている。そこでは、無数の高性能コンピュータが計算量に応じた「投票権」を持っており、計算競争の勝利者が多数決の代表者となる。大規模な計算量を保有するほど、勝利者になる確率は高くなる。これが、Bitcoinシステムに特有のマイニングという作業である。

世界中から多数の一般ノードがマイニングに参加して、

計算問題の正解を発見するということは、高性能のコンピュータを含む無数の計算機が大規模な計算量を投入したことの証明が残ることを意味する。この含意から、計算問題の正解となる数のことを、POW（Proof of Work）と呼ぶ。

このように、一般ノードが多数参加することは、計算量を投入したことの結果としてのPOWに意味を持たせるために不可欠である。すなわち、限定された許可済ノードだけで構成されるようなブロックチェインにおいては、POW法に代わる何らかの正当性の根拠が必要となる。

さて、許可型パブリックチェインにおいては、許可済ノードと一般ノードが併存する。一般ノードの役割は、マイニングのために計算量を投入し、POWの発見に寄与することによって、ブロックチェインの分散性と耐改ざん性を高めることである。これに対して、許可済ノードは、認証局を運営する主体によって特権ノードとして設置されており、アセットの発行ノードや監査ノードなどの特権ノードとして特別な役割を果たす。

ブロックチェインの構成に関しては、許可済ノードだけで構成するほうが効率的であるとする見方と、不特定多数の一般ノードが参加することが不可欠であるとする見方とが存在するが、許可型パブリックチェインは、これらの中間型として位置付けられる。

3.3　許可型コンソーシアムチェイン

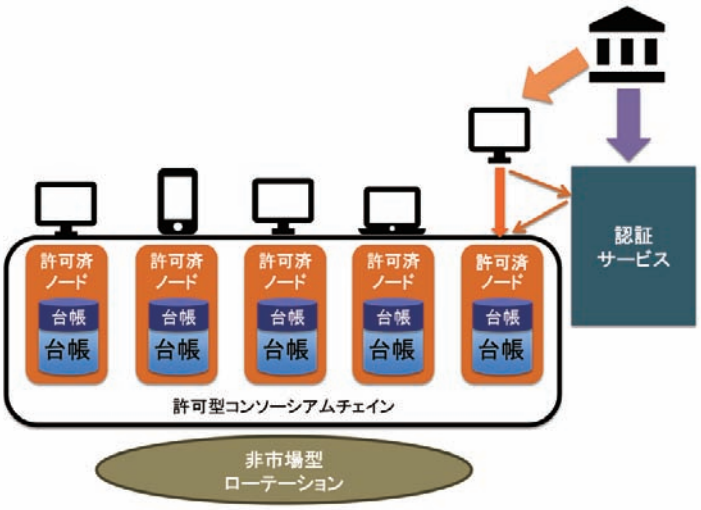
許可型パブリックチェインでは、認証局を運営する主体から特別な権限を与えられた許可済ノードと、認証局から実在性の証明だけを受けた一般ノードが混在しながら、等しくマイニングに参加することが特徴であった。すなわち、許可済ノードと一般ノードが競争的にマイニングを行うことによって、結果としてPOW法が実現されていた。

これに対して、許可型のコンソーシアムによってブロックチェインを構成することも可能である。ここでコンソーシアムとは、ある目的のために形成された企業連合体などの、限定されたメンバーだけがノードとして参加することを指す。コンソーシアムがブロックチェインを構成する場合には、認証局を運営する主体から認められた許可済ノードだけに参加者を限定する。

企業連合体がブロックチェインのコンソーシアムを構成する場合には、参加企業は契約に基づいて権利関係の内容に合意している。この場合、参加する企業群が競争的にマイニングを行うPOW法をとることは必然的ではない。むしろ、合意に基づく省力的な方法をとるほうが賢明である。具体的には、ブロックを検証する順序を予め決定しておき、当番制でブロックを検証していく方法などが合理的である。この検証方法のことを、ローテーション法と呼ぶ。

こうして構成されたブロックチェインは、許可型であり、非市場型である（図5）。

許可型コンソーシアムチェインにおいては、一般ノードが参加することはないため、ブロックを検証するインセンティブを準備する必要はない。従って、ブロックチェインを維持する副産物として仮想通貨を発生させることは必要条件ではなく、また、副産物として何らかの仮想通貨が発生する構成をとった場合であっても、市場を成立させることは必要条件ではない。



■図5：許可型コンソーシアムチェイン

このように見ると、許可型コンソーシアムチェインは、不特定多数の参加者によって維持される自由参加型パブリックチェインや、一定数の許可済ノードと多数の一般ノードによって維持される許可型パブリックチェインなどと比べると、エネルギー効率に優れた手法であるようにも見える。

しかしながら、許可型コンソーシアムチェインには問題点も存在する。コンソーシアムに参加する企業連合体がメンバーの交代なしに長期にわたって存続することは稀であり、参加者の変遷によってはノード間の結託などの不正が起こりやすくなる。また、参加企業が入れ替わる度に権限の設定を変更する必要から、少数の特権ノードが大きな設定権限を握ることになり、そもそもブロックチェイン技術を利用する意義が疑わしくなる。

果たして、許可型のブロックチェインは、ブロックチェインとしての要件を充たすのであろうか。殊に、参加者が限定されている許可型コンソーシアムにおいては、ビザンティン問題と呼ばれるノード間の結託による不正の可能性も懸念される。これに対しては、契約関係によって不正が禁止されていることを以て解決したとする法的アプローチや、POW法に代わる適切なアルゴリズムを実装することで解決できるとする技術的アプローチなどの対案が示されている。

おそらく、これは分類上の特性だけで論じられるものではなく、ブロックの正当性を検証するアルゴリズムの工夫とも密接に関わることであるから、どこまでをブロックチェインと呼ぶべきかという定義についての議論は、マトリクス上の分類論だけによって容易に結論付けることはできまい。

ただ一つ確かなことは、自由参加型パブリックチェインであるBitcoinシステムでは、これまで数年間にわたって、ブロックチェイン運用の根幹に関わるエラーが発生していないとされていることである。これと比較すると、許可型コンソーシアムチェインは閉じた環境となることに起因する弱点を否定することはできず、ブロックチェインとして正確に動作するかは未知数である。許可型コンソーシアムの利点を活かしながら、ブロックチェインとしての性能を維持できるような、最適なアルゴリズムを設定できるかは、今後の実証実験の行方にかかっている。

4. おわりに

FinTechの興隆を受けて、ブロックチェイン技術の可能性が注目されているが、その定義や類型については曖昧なままであった。本稿では、ブロックチェインを2つの視座から論じることを試みた。

本稿では、ブロックチェインを市場型／非市場型という視点と、許可型／自由参加型という視点から分類して論じた。ブロックチェインの分析軸に関しては定説が形成されておらず、これ以外の視点による分類のほうが説明に優れている可能性は多分に残されている。

すなわち、本稿はブロックチェインの分類論を通じて、その可能性と限界について議論する契機に過ぎない。何をもってブロックチェインと呼ぶかという定義の外延は、ブロックチェインの要素技術は何であるかという議論と密接に関連する。さらに、マトリクス上においては、現在の技術による実装を想定できる組合せと、実装例を想定することが容易ではない組合せが存在する。ここで援用したマトリクスにおいても、第4の組合せとして自由参加型コンソーシアムの構成が想定されるが、本稿ではその可能性について言及しないこととした。

新しい技術の定義論は、どのような実装が登場するかに依存して流動的である。従って、分析軸の妥当性についても、実装例を吟味しながら、仮説と検証を繰り返すことになる。こうして、異なる分析軸からブロックチェインの性質を考察することによって、次第に技術の特性が明らかになる。こうした議論が収束に近づく頃には、ブロックチェインの産業への応用が普及し、社会基盤として日常的に利用される技術へと成長していることであろう。

参考文献

[1] Distributed ledger technology: beyond block chain Government Office for Science, United Kingdom（19 January 2016）
https://www.gov.uk/government/publications/distributed-ledger-technology-blackett-review

[2] FinTechと金融サービスの将来像
山崎 重一郎（Mar 30, 2016）
http://www.slideshare.net/11ro_yamasaki/fintech-60247773

[3] 仮想通貨―技術・法律・制度
岡田 仁志, 高橋 郁夫, 山崎 重一郎（May 29, 2015）東洋経済新報社
http://store.toyokeizai.net/books/9784492681381/

[4] 貨幣の歴史にみる仮想通貨の特異性－国家の通貨高権からCODEによる通貨発行へ－
岡田 仁志（May 26, 2016）Nextcom26号
https://www.kddi-ri.jp/nextcom/volume?from=news