ブロックチェーン・エコノミーにおける信頼の構造に関する一考察

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

ブロックチェーンは分散型仮想通貨の基盤として開発された技術であるが、その応用範囲は貨幣的価値の表現に限定されない。分散型仮想通貨の基盤としてのブロックチェーンの特徴は、中心となる運営者が存在しないにもかかわらず、二重送金を防止することができる点に求められる。すなわち、電子的に表現された価値でありながら、これを複製して二重使用することが不可能であり、原所有者から新所有者へと一意に移転する性質を有する。

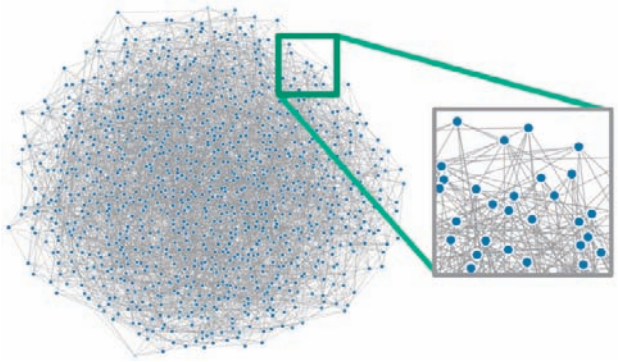
かかる一意性は、電子的に表現された価値がこれまで具備することのできなかった性能であり、それゆえにブロックチェーンは技術的な跳躍であると評される。ブロックチェーンの整合的な性質は、貨幣的な価値のみならず、電子的なアセットとして表現されるあらゆる権利関係の移転を表現できる可能性を示唆する。このような観点から、ブロックチェーンの応用可能性について検討した各種研究会等の調査報告書が公表されている。

本稿では、ブロックチェーン・エコノミーに関する三層構造の仮説を提言しておられる、山崎重一郎教授（近畿大学）の論稿及び資料を端緒として、その社会的かつ経済的なインプリケーションについて考察する。そして、ブロックチェーン・エコノミーの覇権をめぐる国際間の状況について概観し、3つの層から構成されるブロックチェーン・エコノミーにおいて、いずれのレイヤーを把握することが覇権への近道であるのかを検討する。

議論の前提として、はじめに分散型仮想通貨の基礎となる自由参加型パブリックチェーンの構造特性について概観する。そして、ブロックチェーン技術によって経済活動のプラットフォームを構築することの意義がどこにあるのかを考察する。これらの検討を経て、ブロックチェーン・エコノミーの将来について展望する。

2. 自由参加型パブリックチェーンの構造特性

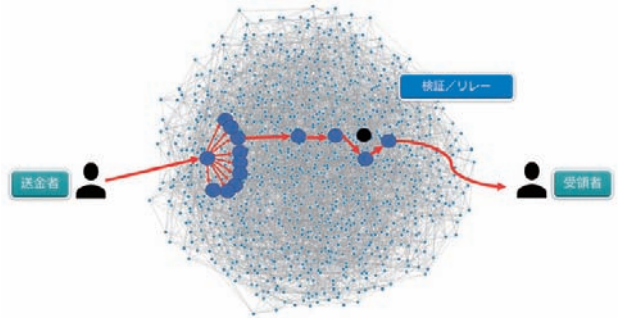
ビットコインに代表される分散型仮想通貨は、自由参加型パブリックチェーンによって構成されている。これは、中心を持たないピアー・ツー・ピアー（P2P）型のネットワークであり、ノードとして参加するために特定の主体からの許可を得ることを必要としない。現時点では、世界中におよそ1万1000個程度のノードが設置されている。各ノードは最大で8個のノードとつながっており、格子状に類似したような構造を持つ。



■図1. ビットコインのP2Pネットワーク

分散型仮想通貨の送金とは、P2P型のネットワークにおいて、ノードからノードへと取引データを伝搬することを意味する。送金者はスマートフォンなどの機器内にウォレットを保有しており、ウォレットには秘密鍵が格納されている。秘密鍵に対応した公開鍵を元に、アドレスが設定される。送金者は、受信者のアドレスに対して送金を行うことを意図する。

このとき、送金者のウォレットは、少なくとも1つのノードを予め知っており、これに対して取引データを渡す。これを受け取ったノードは、つながりのある最大8個のノードに対して取引データを渡す。各ノードは、取引データを検証して、エラーがなければつながりのあるノードへと取引データ



■図2. 送金データのブロードキャスト

を渡す。このようにリレーしていくことによって、最終的には受信者のウォレットへと取引データが届く。

中心を持たないP2P型のネットワークを活用して貨幣的価値を表現することは、一見すると容易に見える。しかしながら、分散型の仮想通貨は早くから構想を持ちながら、長らく実現しなかった。その原因は、電子的なデータの二重使用を防ぐ仕組みを構築することが困難であったことにある。電子的に表現された貨幣的価値においては、二重使用を防止する方法を見つけることが難問とされていた。

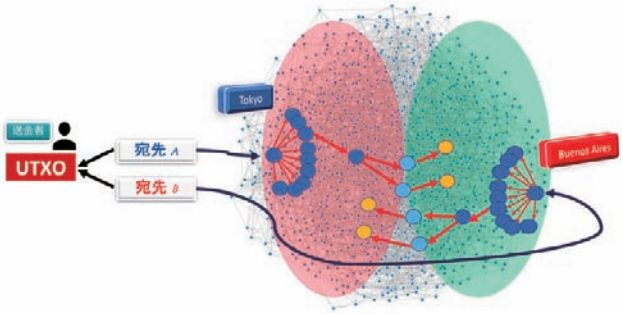
ビットコインにおける貨幣的価値は、UTXO（Unspent Transaction Output：未使用残高）として表現される。いわば電子的に表現されたコインである。UTXOは1か所のサーバに記録されるのではなく、ブロックチェーン上に記録される。では、分散型仮想通貨の台帳であるブロックチェーンはどこに存在するかというと、自由参加型パブリックチェーンに参加する全てのノードが個々に記録する。

分散型仮想通貨の送金とは、送金者の秘密鍵に対応したUTXOを参照し、受信者のアドレスに向けて全部または一部を移動させることである。ウォレットは、このような指示を要素とする取引データを作成し、自己とつながっているノードに対して取引データを渡す。ゆえに、分散型仮想通貨の二重送金とは、1つのUTXOを参照する2つの取引データを不正に作成し、異なる2人の受信者に向けて送金することを意味する。

従来の中央集権型の送金システムでは、1か所において時系列的に取引データを記録するため、二重送金は容易に検知することができた。分散型仮想通貨においては、中心を持たないP2Pネットワークに2つの矛盾する取引データが流れていても、直ちに検出できるとは限らない。P2Pネットワークのノードが地球上に分散しているような場合において、この傾向は顕著となる。

1つのUTXOを参照する取引Aと取引Bが不正に作成され、取引Aのデータは東京付近のノードに渡され、取引Bのデータはブエノスアイレス付近のノードに渡されたと仮定する。このとき、取引Aのデータは東京から徐々に近隣のノードへと伝搬される。取引Bのデータはブエノスアイレスから徐々に近隣のノードへと伝搬される。いずれも正しい取引データとして、ノードからノードへとリレーされる。

こうして、取引Aと取引Bが地球の両側からブロードキャストされる。当初はノード間を矛盾なくリレーされるが、やがて取引Aと取引Bのデータの両方を受け取るノードが現れる。ここにおいて、1つのUTXOを参照する2つの取引が不正に作成されていることが検知される。これが中央集権型のシステムであれば、遅れて到着した取引データをエラーとして扱うなど、何らかのルールに従って取引の正統性を一意に決することができよう。



■図3. 二重送金における2つのデータの伝搬

ところが、地球上に分散したノード間においては、地点によって取引データの到着する時刻が異なる。東京に近いノードは取引Aを先に受け取る蓋然性が高く、ブエノスアイレスに近いノードは取引Bを先に受け取る蓋然性が高い。地球上に分散したノード群においては、ある時刻に観測している風景がノードによって異なる。このことが、中心を持たないP2Pネットワークで貨幣的価値を表現することの難しさの原因であった。

Satoshi Nakamotoが2008年に公表した論稿は、この問題に対する解決策を提示した。その発想は、Proof of Workという方式によって、代表ノードを選定することを内容とする。すなわち、P2Pネットワークに参加するノード群の中から、1つの観測者としてのノードを選定することにより、そのノードが観測している風景は一意に決まるという性質を利用したものである。

ビットコインにおいては、代表ノードを選定するためにProof of Work方式のマイニング方法を導入している。これは、分散性を保つために不可欠なプロセスであるが、資源と時間の浪費であるという批判も存在する。これに対しては、中心を持たないにもかかわらず歴史を記録するための装置、いわばクロニクルを地球上に作り出すためのコストとして容認する向きもある。その是非については論争が繰り広げられている。

3. ブロックチェーン・エコノミーの三層構造

上述のように、ブロックチェーンの存在意義は、中心となる運営者が存在しないにもかかわらず、無数の当事者間における取引を正しく記録し、矛盾なく1つの歴史を作り出

すことを可能にした点に求められる。これまでの巨大な運営者を信頼するネットワークに対するアンチテーゼとして、ボランティアで参加する無数のノードが競争的に協調して、プログラムのコードによる信頼を作り出す仕組みである。

ブロックチェーンは価値の移転を正しく記録することのできる仕組みであるから、貨幣的価値の移転だけでなく、あらゆるアセットの移転を表現できる可能性がある。こうした性質に着目して、あらゆる産業においてブロックチェーン導入の可能性が検討されている。本稿では、これらの動きのなかでも、分散型仮想通貨を支える自由参加型パブリックチェーンを基礎に置いたプラットフォームについて考察する。

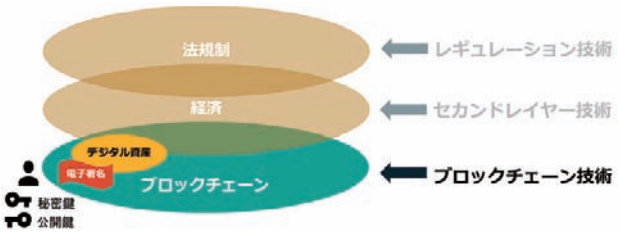
仮説として、ブロックチェーン技術を基礎とした経済活動のプラットフォームは、自由参加型パブリックチェーンによって第1層を構成しながら、その上位レイヤーとして経済活動の第2層と法制度執行の第3層を構築することで形成されるものと想定する。このようなモデルのことを、本稿ではブロックチェーン・エコノミーの三層構造と呼ぶ。

3.1　ブロックチェーンのレイヤー（第1層）

ブロックチェーン・エコノミーの第1層は、分散型仮想通貨に適用される自由参加型パブリックチェーンによって構成される。このタイプのブロックチェーンは、構成要素としてのノードを設置するために何らかの主体による許可を必要としない。なぜならば、許可の主体となるヒトまたは法人はそこには存在せず、ただプロトコルによってのみ規律されるヒトの意思に基づかない空間が広がっているからである。

自由参加型パブリックチェーンは、それがプロトコルに従って正常に動作する限りにおいて、個人から個人へのアセットの移転を不可逆的に記録することができる。個人が保有するアセットの未使用残高はブロックチェーン上に記載されているが、ブロックチェーンは自由参加型のノードによって分散的に保有されている。概念上の設計においては、自由参加型のノードは特定の国家や企業による支配を受けることはない。

ここで、デジタル資産に対する権利を表章するのは秘密鍵である。従来の電子認証基盤では、信頼できる第三者機関の存在が不可欠であった。これに対して、自由参加型パブリックチェーンが創出した空間では、信頼できる第三者機関を必要としない。ブロックチェーンが創出したのは、特定の主体によるコントロールの可能性を排除し、プロトコルによって支配される新しいタイプの信頼空間である。



■図4.　ブロックチェーンのレイヤー（第1層）

ヒトによるコントロールの可能性を排除したことによって、不可逆的な歴史を自動的に記述していくクロニクルが成立した。こうして自由参加型パブリックチェーンは、人間の経済活動の記録を刻む石版としての役割を果たしていく。歴史を刻印するための方式は、あたかもヒエログリフのように特有のプロトコルから構成されている。プロトコルが正しく定義されて実行される限りにおいて、ヒエログリフは正しく歴史を刻んでいく。

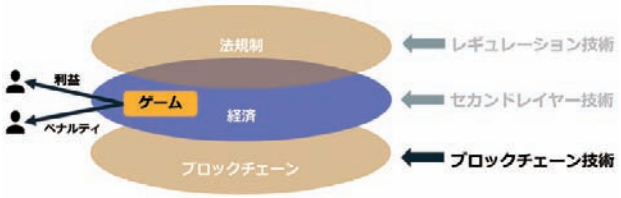
3.2　経済活動のレイヤー（第2層）

自由参加型ブロックチェーンはクロニクルとしての役割を果たす堅牢な仕組みであるが、信頼できる第三者機関を置かないことの結果として、経済活動の主体に関する実在性を担保できないという制約があった。さらに、クロニクルを刻んでいくブロックの1個1個は、ピラミッドの石のようにサイズの上限が決まっているため、ブロックチェーンを基盤とした経済規模の拡大に対応することができないという制約があった。

こうした課題を解決するために提案されたのが、ブロックチェーンのセカンドレイヤー技術である。典型的な方式としては、分散型仮想通貨であるビットコインシステムのセカンドレイヤーとして、ライトニング・ネットワークなどの技術が提案されている。ビットコインシステムにおいては、2017年にアクティベートされた技術文書によって、セグウィット（Segwit：Segregated Witness）のプロトコルが実装された。

Segwit方式は、署名部分をブロックの外部に置くことによって、ブロックに格納できるトランザクション数を増やす効果があり、ビットコインシステムの処理能力を高めるスケーリング策としての意味を有する。Segwit方式のもう1つの効果は、セカンドレイヤーとしてのライトニング・ネットワークの実装を可能にしたことである。これによって、ビットコインシステムは、多層構造の第1層としての位置付けを明確にした。

ライトニング・ネットワークによって記述されるセカンドレイ



■図5. 経済活動のレイヤー（第2層）

ヤーは、第1層としてのビットコインシステムと相互に連携する。これから契約関係に入る2人の当事者は、最初に第1層のビットコインシステム上にデポジット用の共通アカウントを設定する。これを引き当てとしてセカンドレイヤーにおいて契約行為を反復し、契約関係が終了するとビットコインシステムに戻って共通アカウントを閉じ、これと同時に差額を清算する。

ビットコインシステム上における取引をオンチェーンの行為と呼ぶのに対して、セカンドレイヤーにおける経済活動はオフチェーンの行為と呼ぶことができる。オンチェーンの行為はプロトコルによって不可逆性を担保されているが、オフチェーンの行為は不可逆性を当然に備えるわけではない。そこで、オフチェーンの行為にも不可逆性の性質を表現するために、ゲーム理論を応用して契約に反する行為を防ぐことが検討されている。

オフチェーンの行為は、経済活動の行動規範に従って記述されており、その内容は各領域のビジネス・プロトコルに準拠する。しかしながら、契約の一方の当事者が合意の内容を守らなかった場合には、ビジネス・プロトコルから逸脱した行為が発生する。第1層のオンチェーンの行為は、プロトコルが自動的に執行されて逸脱の余地がないのに対して、第2層のオフチェーンの行為は、ビジネス・プロトコルを逸脱する余地がある。

あらゆる経済活動は合理性に関する判断を前提とするため、オフチェーンにおいてビジネス・プロトコルを逸脱することで得られる利益よりも、ペナルティとして受ける損失の方が大きくなるように設計することによって、契約に違反する行為を防ぐことができる。そのための方法として期待されているのが、ゲーム理論を応用したルールの構築である。これが完成すれば、オフチェーンの行為をビジネス・プロトコルに準拠させることができる。

現時点においては、オフチェーンの行為をゲーム理論に従って記述する作業は、いわば手作業によって理論をプログラムに落とし込む段階にある。だが将来的には、ゲーム理論に従って常に契約違反によるペナルティが違反行動による利益を上回るように、半自動的にプログラムを記述するよう改良されるであろう。この段階に至れば、オフチェーンの行為はスケールの制約を受けることなく、広汎に活用することが可能となる。

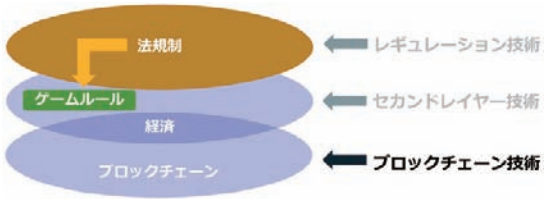
3.3 法規制のレイヤー（第3層）

ブロックチェーン・エコノミーの第1層を規律するのは、プログラムによって記述されたプロトコルであった。第2層の経済活動を規律するのは、ゲーム理論に基づく利益とペナルティの合理的判断であり、第1層と第2層はライトニング・ネットワークなどの仕組みによって相互に連携していた。第1層のルールは、エンジニアによる提案と議論を経て改良され、第2層においては経済学の知見を借りて実効性が改善されていく。

ブロックチェーンにおける経済活動がシステム内で完結するものであれば、これらの二層によって最低限の信頼関係が成立しているように見える。しかしながら、実社会における経済活動を表現するためには、オフチェーンの行為が法律や規範に従ったものであることが必要とされる。契約の両方の当事者が国内に居住するような場合であれば、国内法の規制が自律的に適用されるような装置をシステム内に組み込むことが好ましい。

このような観点から、ブロックチェーン・エコノミーの第3層として、レギュレーションのレイヤーを設計することが提案されている。この構成は、国内法としての強行法を適用する場面よりも、むしろソフト・ローを実装する場面において、より柔軟に機能を発揮する。あるビジネス領域におけるビジネス・プロトコルを業界内で議論して合意に至ったとする。このルールを単に自主的に遵守するのであれば、必ずしも強制力は必要とされない。

これを発展させて、業界団体と規制当局が協調的に関与する方式として、共同規制の手法が注目されている。共同規制の手法によれば、業界団体が中心となって提案したルールが、法適合性を有していて必要かつ十分な内容を具備していることを、規制当局が確認するプロセスを経る。



■図6. 法規制のレイヤー（第3層）

そして、決定したルールに従って経済活動を行っていることを、何らかの方法によって規制当局が検証し、必要に応じて改善のための助言と指導を行う。

ここで、共同規制の仕組みをブロックチェーン・エコノミーの第3層として実装する場合には、第2層の経済活動は第3層のルールの範囲内でしか起こり得ないため、レギュレーションに違反した経済的行動をとることが不可能となる。

およそ共同規制の手法を採用する場合には、過度のレギュレーションによって経済活動の自由を制約していないか、レギュレーションの不足によって契約の不公正を招いていないかを、継続的に検証することが必要となる。共同規制の手法はインターネットに適したレギュレーション手法とされるが、こうした検証のコストが高いことが課題であった。

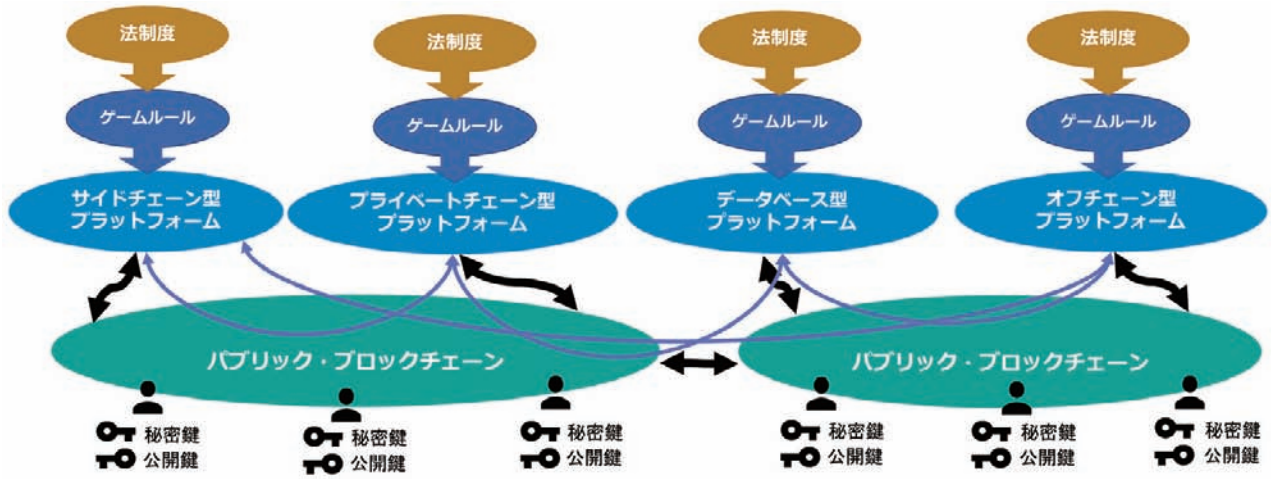
ブロックチェーン・エコノミー仮説では、第2層の経済活動と第3層のレギュレーションを不可分一体で構成することによって、レギュレーションの経済活動における実践を可視化することができる。このことは、共同規制の手法における検証のプロセスを自動化し、さらには協調的にルールを改良するプロセスを支援することが期待される。

4. おわりに

本稿は、ブロックチェーン・エコノミーは三層構造であるとする仮説に対して考察を加えた。その基本形は、第1層を自由参加型パブリックチェーンで構成し、第2層をライトニング・ネットワークなどのオフチェーン技術で構成するものである。ただし、第2層を許可型コンソーシアムチェーンまたはデータベースによって構成することも不可能ではない。オンチェーンとオフチェーンは垂直に連携し、各レイヤーのチェーンは水平に連動する。

こうした階層構造の上位に位置するのが第3層のレギュレーションである。インターネットのルールが主要プレイヤーの集中する国の法律に準拠していったように、ブロックチェーンによる新たな秩序の構築においても、主要なプレイヤーの集中する国が法制度設計をリードする地位を得る。こうした傾向は、三層のレイヤーが密接に関連するブロックチェーン・エコノミーにおいては、より顕著な傾向として現れるものと想定される。

インターネット経済に慣れ親しんだ国では、既存の秩序を重んじてブロックチェーンへの移行を否定する傾向がある。だがインターネット秩序の再構築を試みる国々においては、ブロックチェーン・エコノミーの各レイヤーで存在感を示すことによって、上位レイヤーにおける法制度設計の主導権を握ろうとして競争が繰り広げられている。いま、同時代に起こっている2つの流れの中から、正しく未来を読み取る洞察力が求められている。



■図7. インターブロックチェーン