応般

特別解説

ビットコインの構造と制度的課題
―分散型仮想通貨の提起する論点とは―

岡田仁志（国立情報学研究所）

分散型仮想通貨の登場

ビットコインが世界で流通し，その法定通貨との交換価格の変動幅の大きさや交換所の破たんなどの事件が注目されている．しかしながら，ビットコインは本来，P2P 技術を利用した分散型の仮想通貨であり，どこにも中心を持たないことを本質とする．中継点の１つに過ぎないはずの交換所が大きな役割を果たしていることから，P2P 型の仮想通貨としての実像がゆがんでいるビットコインであるが，原著論文[1]の内容に立ち戻り，分散型仮想通貨の構造とその可能性について考察する．そして，論文の構想とはかけ離れて成長しているビットコインなどの仮想通貨について，その将来性に着目しつつ制度的課題を検証する．

▶ 分散型仮想通貨の構成

分散型仮想通貨を制度論的観点から見たとき，その最大の特徴は中心となる発行主体を持たないことである．一般に我が国の法律構成においては，たとえば電子マネーであれば発行主体の備えるべき特性を定義し，発行主体をコントロールする規制手法として免許制または届出制などのいずれが適切であるかを検討し，具体的な条項の細目をつめていく作業や関係省庁との法令協議を経て，１つの法律が完成していく．

ところが，分散型仮想通貨には発行主体が存在しない．一例としてビットコインの支払情報の伝達過程を図示してみると一目瞭然である（図 -1）．

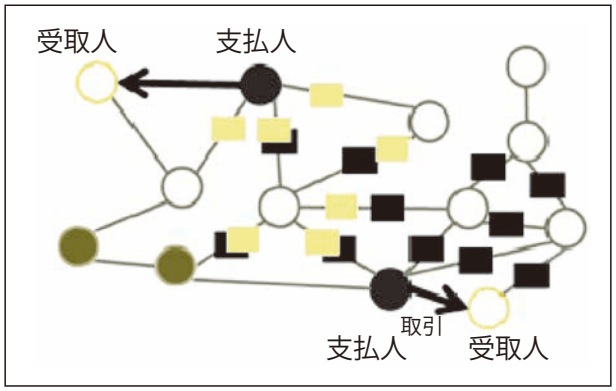

図 -1　P2P 仮想通貨における支払情報の伝達
（出典：山崎重一郎，Bitcoin 勉強会 2，
http://www.slideshare.net/11ro_yamasaki/bitcoin2）

支払人から受取人に対してビットコインが送金されると，支払情報が直近のノードに向けてブロードキャストされ，さらにノードからノードへとバケツリレーで伝わっていく．オフラインになっているノードは，再接続した際に最新の取引情報の束をまとめて受信する．このことは，分散型仮想通貨の第一の特徴であるところの，参加者全員の記憶によって支払情報の正しさを担保し，偽造や変造の困難性を高めるという性質を実装したものである．

中央管理型の電子マネーであれば，すべての支払情報はサーバに書き込まれる．しかし，分散型仮想通貨にはサーバが存在しないため，参加者全員で記録するという方法がとられている．

電子署名の連鎖

分散型仮想通貨を現所有者から次の受取人に渡す手続きは，現所有者の秘密鍵によって，次の受取人の公開鍵に電子署名を行うことによって実現される．このこと自体は従来から存在する電子署名の連鎖の典型例に過ぎず，何らの新規性を有しない．分散型

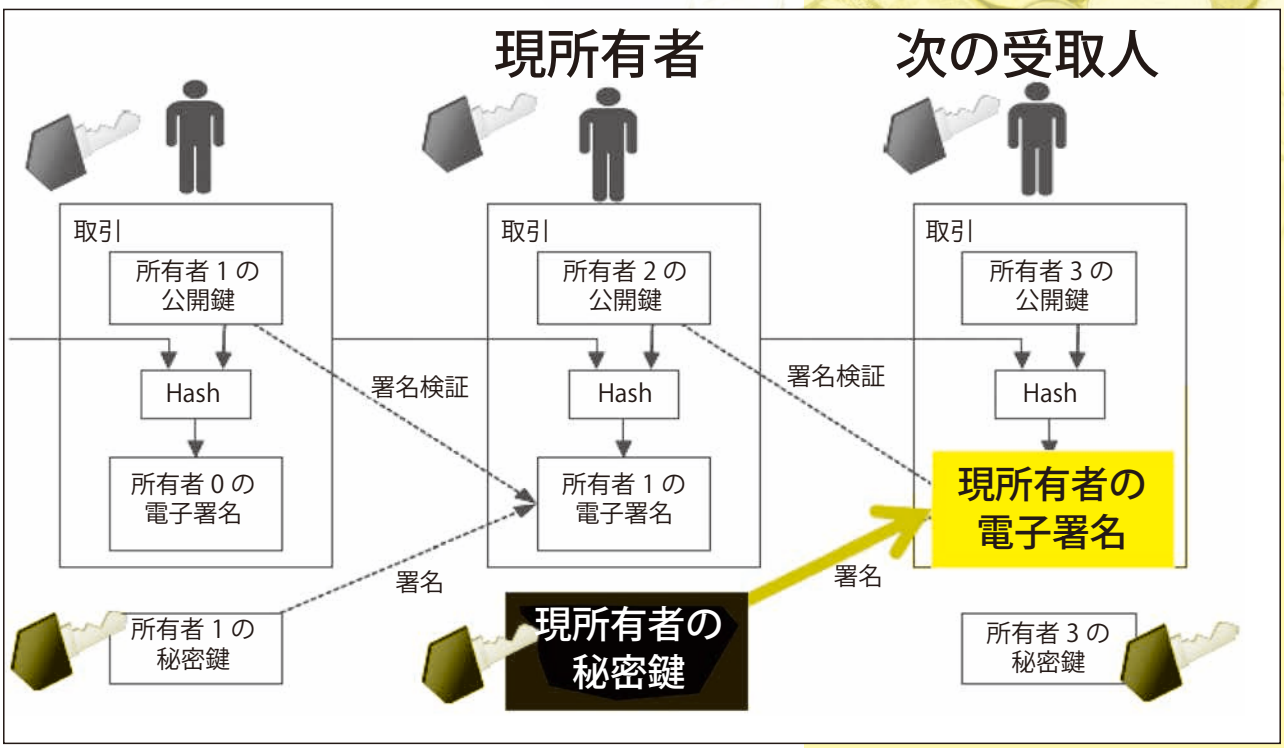

図 -2　Nakamoto 論文が提案する電子署名と取引履歴の連鎖構造
（出典：山崎重一郎，Bitcoin 勉強会 2，http://www.slideshare.net/11ro_yamasaki/bitcoin2）

仮想通貨の可能性を論証した Nakamoto 論文[1] は，**図 -2** に示すような入子構造を示し，現所有者の手元に至るまでの取引記録および次の受取人の公開鍵のハッシュ値に対して，現所有者の秘密鍵で電子署名するという方法をとる．

このような構成をとることの前提として，発行主体を持たない分散型仮想通貨においては中心となるサーバが存在しないため，分散型でありながら取引の正しさを担保しなければならないという要請が存在する．現所有者までの取引情報と受取人の公開鍵のハッシュ値は，単独で存在していれば十分に安全とはいえないが，入子構造の電子署名の鎖がつながっていくことによって，飛躍的に改ざんの難易度が高まっていく．

発行者の存在する電子マネーの歴史においても，転々流通型の構成をとるものは稀である．接触型 IC カードに価値を格納するタイプの前払い式証票であったモンデックス電子マネーは広域実用例が存在しないため実装計画について断定することはできないが，本質的には転々流通型の構成を前提とした電子マネーであった．日本においては，FeliCa 技術による非接触 IC カードを活用した電子マネーが広く流通しているが，これらの多くはオープンループ型の構成をとらず，1 回の取引ごとにサーバにおいて対応する価値を消し込むクローズドループの構成になっている．

オープンループ型であるかクローズドループ型であるかは，単なる価値流通の構成の違いだけでなく，およそ電子的な価値流通の設計思想を強く反映する．クローズドループ型では中心となるサーバにすべての取引記録が残るため，現金と同様の匿名性を保つためには法制度などの技術外手法が必要とされる．これに対して，オープンループ型であれば現金と同じように転々流通しており，匿名性を高めることが可能になる．そもそも匿名購買の自由は基本的人権の 1 つであると解釈する考え方もあり，匿名性の高いオープンループ型の電子マネーを構築することは長年の難問であった．分散型仮想通貨はさらに一歩進んで発行主体を持たず，取引情報がコミュニティ内を縦横無尽に駆け巡る完成度の高いオープンルー

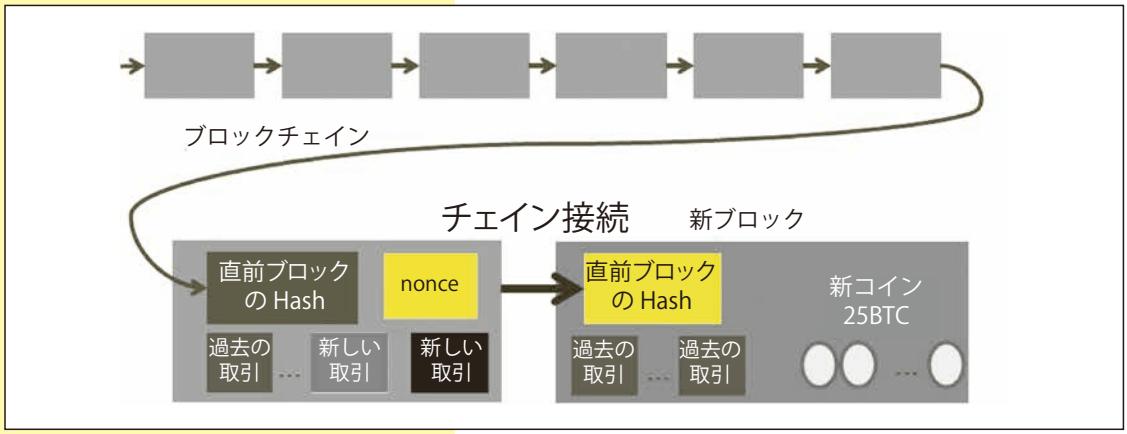

図 -3　生成中のブロックを既存のブロックチェインに接続する手順
（出典：山崎重一郎，Bitcoin 勉強会 2，http://www.slideshare.net/11ro_yamasaki/bitcoin2）

プ型の構成をとるため，高い匿名性を確保できる可能性がある．

採掘という通貨発行

分散型仮想通貨を提唱した Nakamoto 論文の第 2 の特徴は，通貨の発行にあたる作業と取引の承認にあたる作業を兼ねるエコシステムを発見したことである．採掘者は，直近の数百件の取引をブロックに格納する．ビットコインの例では，取引の ID にあたる取引情報のハッシュを格納する．これに，直前のブロックのハッシュを加える．

さらに，乱数を加えながらハッシュ関数の値を取り続ける．最終的に，ハッシュ関数で得られた値においてゼロが一定個数並ぶまで，計算を続ける．この計算の難易度は，過去 2 週間の平均値との不等式により，常に平均して 10 分間になるよう自動的に修正される（**図 -3**）．

ここで，一定の個数のゼロが並ぶハッシュ値が得られると，いま新たに生成されたブロックは前のブロックとつなげられる．こうしてチェインが接続されると，新しいブロックに格納された数百件の取引は承認されたことになる．同時に，計算を行って最初に回答を発見したプレーヤには，報償としてビットコインが発生する．

このとき，ビットコインは誰かから送金されてくるのではなく，新たに生成したブロックに格納された取引群の先頭に，一定数のビットコインを発生させるための，現所有者の存在しない取引が格納される．すなわち，ビットコインを発行するのは発行主体ではなく，アルゴリズムである（**図 -4**）．

発行主体を持たない分散型仮想通貨は，発行主体を持つ管理型の仮想通貨とは大きく異なる性質を有する．発行主体は意思を持つことができるが，P2P というネットワークの全体は自然人または法人格としての意思を持つ主体とはなり得ない．このことが分散型仮想通貨のコントロールを困難にし，言い換えればいかなる政府からのコントロールも受けない独立性を保つことができる．

法定通貨の歴史を振り返ると，通貨の価値を維持する役割を担う中央銀行が，政府の意思によってハイパーインフレーションを誘導し，結果的に通貨価値が損なわれるという例があった．これらを防ぐための方策の 1 つとして，通貨発行自由化論が提唱された．南北戦争の前のアメリカ合衆国の一部の地域には，市中銀行が発行する銀行券が価値を表象する決済手段として流通していた．

国民国家においては，通貨を発行する権限は通貨高権として国家が独占するものであり，国家の存立そのものにかかわる重大な権力である．通貨自由発行には確かに一定の効果もあるが，金融政策の効果を減殺し，財政政策の実効性を失わせる．

小さな連邦政府を標榜するリバタリアンの思想に合致する通貨発行自由化論は思考実験として興味深

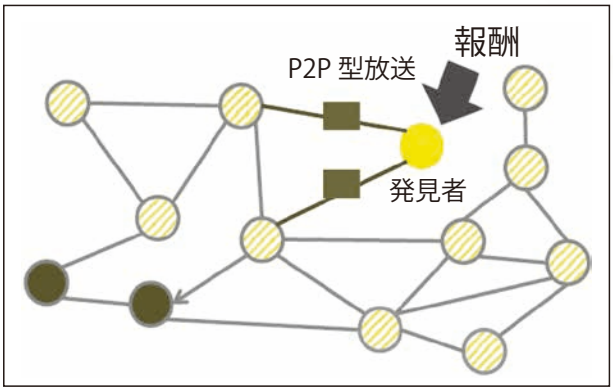

図 -4　P2P 仮想通貨における支払情報の伝達
（出典：山崎重一郎，Bitcoin 勉強会 2，
http://www.slideshare.net/11ro_yamasaki/bitcoin2）

いが，金融政策に影響を及ぼす規模での実施は実際には困難であると考えられていた．分散型仮想通貨は発行主体を持たないため，政府の発行者規制を受けることが構造的に困難であるように設計されているのである．

▶ ビットコインは分散型仮想通貨か

完全なる分散型仮想通貨は，いかなる政府のコントロールを受けることもなく，あたかもインターネットの存在そのものと同じように，自律的な存在として成長していく．こうした自由発行通貨が世界で流通するようになっても，基軸通貨に与える影響は限られているが，政情不安を抱える小国においては法定通貨にとって代わられる可能性も否定できない．キプロスの財政が破たんし，銀行預金に預金税を課す議会案を嫌って人々が預金資産を仮想通貨に避難させたことは，政府を持たない仮想通貨に対する需要というものが，一部には確実に存在することを示した．

完全なる分散型仮想通貨は，発行主体の意思に左右されない，フラットな金融ネットワークを実現しようとする思想を反映している．少なくとも，Nakamoto 論文から読み取ることができるアイディアは，どこにも中心が存在しないフラットな社会であり，P2P ネットワークのどこにも中心となるプレーヤが出現しないはずであった．ビットコインの実装においても，当初はウォレットごとに採掘の機能がついており，誰もが支払人であり，誰もが受取人であり，誰もが採掘者すなわち発行者になることができる構成であった．

しかし，現在のビットコインは決してフラットな P2P ネットワークではない．採掘すなわち発行の計算は誰もが行うことができるが，実際には特定のマイニングプールが 40% 近くを寡占する規模に至っており，特定の発券銀行を置くような構成と近づいている．プルーフ・オブ・ワークを覆すとされる 51% 攻撃の可能な数値に近づいており，もはや論文が前提とする分散性はおびやかされつつある．

さらに，法定通貨と現金の交換を行うための取引所が，P2P ネットワークの取引の大半をコントロールするようになった．もはや取引所を頂点とするピラミッド型の構造に近づきつつあり，無数の取引がフラットに流通する前提が崩れようとしている．ここにおいて，法律は発行者規制に代わるものとして，取引所を規制する必要があるか検討を開始することになる．

ビットコインは分散型仮想通貨の時代を拓く先駆者であるが，完全ではない．あらゆる意味で発展の余地を秘めており，価値を担保する技術的な仕組みにおいても，それを支える法制度の側面においても，さまざまな改善の余地がある．技術と法律が手を携えて，理想的な分散型仮想通貨の実現に向けて一歩ずつ前進し，やがて日本発の完全なる分散型仮想通貨が普及することを願いたい．

参考文献

1) Nakamoto, S. : Bitcoin : A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf（The Bitcoin Foundation の公認する団体が公開する論文．著者の実在性については未確認とされる）

（2014 年 3 月 9 日受付）

▶岡田仁志（正会員）okada@nii.ac.jp

国立情報学研究所情報社会相関研究系准教授．東京大学法学部第一類・第二類卒業．大阪大学大学院国際公共政策研究科博士後期課程中退．博士（国際公共政策）．専攻は情報制度論．2011 年度優秀教材賞．