暗号通貨「価値の移動と保蔵」

＜はじめに＞

人類は価値の経済的表象としてマネーを創造し、これを扱う手段として通貨を発明した。

現代におけるマネーは、モノの経済価値だけでなく、信用そのものによって創造される。一方通貨は、価値が化体した有体物として、特殊な形や材質を有する貝殻や石から始まり、その後希少性のある金属に変わり、中世末期のイタリアにおいて信用をベースにした紙幣が考案された。そして、現在、偽造も不正使用もできない、最も安全で使用方法や場所を問わない究極の通貨として、「Crypto Currency（暗号通貨）」が生まれた。

通貨の基本機能は「決済手段」、「価値の保蔵手段」、「価値尺度」の３つであり、信用によって裏打ちされた債務として譲渡が可能である。人類の経済活動において、常に価値の移動と保蔵が必要であり、通貨はその主たる手段として中心的役割を担っている。

通貨は、①取引記録や残高を記帳し、その台帳を根拠として発行する方法（台帳方式）と、②台帳は持たず、金属や紙などに特殊な方法で偽造できないようにしたモノ（実体貨幣）を発行する方法（現金方式）があり、いずれの方法においても通貨の３つの基本機能を実現できる。

ところで、現代の経済活動においては、空間的または時間的な変化に伴い、通貨自体の表す価値を変化させることを必要とする場面が少しずつ増えている。例えば、地域通貨はある地域のみで有効であり、通貨に似た地域振興券には有効期限がある。シルビオ・ゲゼルによって考案された自由通貨※1（スタンプ通貨）も電子マネーを用いることで実験的使用が始まっている。従来の通貨は、この現代の要求に十分に応えられるだろうか？

以下、通貨の３つの基本機能である、「価値の移動（決済手段）」、「価値の保蔵手段」、「価値尺度」のうち、現代の暗号通貨が担い得る役割について、特に、価値の移動と価値の保蔵の焦点を当てて、その上で価値そのものについて論じる。

＜台帳方式通貨＞

台帳方式の代表的な例として、銀行口座を用いた銀行取引を考察する。人々が銀行に預けた（または、借り入れた）法定通貨（日本の場合、円）は銀行の台帳に記録され、実体は喪失し、口座にしか存在しない一種の仮想通貨となる。それでも利用者は、その後の取引によって金額は増減するものの、その残高は銀行により保証されているので、全く心配せずに価値の保蔵手段として用いている。価値の移動は、銀行の窓口に自分の通帳と振込内容を記載し押印等した振込用紙を提示し依頼すれば行える。もちろん ATM（現金自動預け払い機）を用いてもよい。最近はインターネットを介して振込手続きをする人も増えている。この過程を以下箇条書にする。

予め、インターネットバンキングの口座を開設して、ID とパスワード（PW）を登録し、ワンタイムパスワード（OTP）のトークンを入手し、入金を済ませる。

① インターネット上のインターネットバンキングサイトに SSL 通信で接続する。
② ID、PW、OTP を入力し認証の上、自身のページ（口座）にログインする。
③ 送金先の口座情報、金額を入力し、手数料を確認して、送金ボタンを押す。
④ 送金手続きが終わったことを示す情報と、自身の銀行口座から送金した金額と手数料が差し引かれた

ことを確認し、しばらく待つ。

⑤ 送金元の銀行台帳に送金情報が書き込まれると同時に、全国銀行データ通信システム（全銀システム）を使って送金情報が送金先の銀行台帳に送信される。

⑥ 送金情報（送金先にとっては着金情報）が送金先に届き、送金先の銀行台帳に書き込まれ、送金相手は送金先の銀行口座に金額が加算されたことを確認する。

このように、銀行に預けた（または、借り入れた）法定通貨は実体をもってないものの、台帳に記載された記録によって、価値の移動も価値の保蔵も行うことができる。

それでは、ビットコインに代表される仮想通貨の場合はどうであろうか？

実は、仮想通貨も全く同じなのである。違うのは、銀行が銀行毎に１つの台帳（バックアップ用途の台帳は考慮しない）を用いるのに対し、ビットコインではブロックチェーン（BC）と呼ぶ大量の同一複製台帳を用いる点だけである。ビットコインは、ビットコインを信じるコミュニティの中だけで価値があるとされる仮想通貨であり、BC に記載された取引記録から辿ることのできる残高として、価値を保蔵できるとされている。また、価値の移動は、移動記録を BC に書き加える（繋げる）ことで実施する。以下、この過程を箇条書にする。

予め、仮想通貨取引所に口座を開設して、ID とパスワード（PW）を登録し、ワンタイムパスワード（OTP）のトークンを入手し、入金を済ませる。

① インターネット上の仮想通貨取引所サイトに SSL 通信で接続する。

② ID、PW、OTP を入力し認証の上、自身のページ（口座）にログインする。

③ 送金先のアドレス、送金するビットコイン（BTC）の量を入力し、手数料を確認して、送金ボタンを押す。

④ 送金手続きが終わったことを示す情報と、取引所の自身の口座から送金した BTC 量と手数料が差し引かれたことを確認し、しばらく待つ。

⑤ 公開鍵暗号方式を使って、取引所のアドレスから送金先のアドレスにどれだけの BTC を送付したという送金情報がブロックチェーンに送られる。

⑥ 送金情報（送金先にとっては着金情報）が送金先に届き、ブロックチェーンに書き込まれ、送金相手は送金先の口座に着金した BTC 量が加算されたことを確認する。

以上の通り、具体的な手続きは、ほぼ同一（異なるのはアンダーラインの部分のみ）である。

一方で、ビットコインの場合は、仮想通貨取引所を利用しなくても自身の持つウォレット（Wallet※2）から直接送金できる。この場合の過程を参考までに以下箇条書にする。

予め、ウォレットアプリをインストールして、パスワード（PW）を登録し、入金を済ませる。

① PC（またはスマートフォン）上のウォレットアプリを起動する。

② PW を入力し認証の上、ウォレットを開く。

③ 送金画面にて、送金先のアドレス、送金するビットコイン（BTC）の量、手数料の 3 つを入力し、送金ボタンを押す。

④ 送金手続きが終わったことを示す情報と、ウォレットから送金した BTC 量と手数料が差し引かれたことを確認し、しばらく待つ。

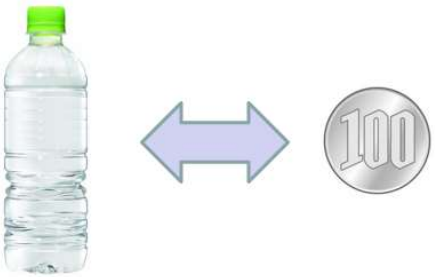
⑤ 公開鍵暗号方式を使って、ウォレットのアドレスから送金先のアドレスにどれだけの BTC を送付したという送金情報がブロックチェーンに送られる。

⑥ 送金情報（送金先にとっては着金情報）が送金先に届くとともに、ブロックチェーンに書き込まれ、送金相手は自分のウォレットに着金した BTC 量が加算されたことを確認する。

以上、仮想通貨の場合においても、台帳方式の価値の移動は、台帳にその価値の移動記録を追記するだけであり、法定通貨を扱う銀行の場合と全く同一の行為として実現される。それではなぜ多数の同一台帳を使用する必要があるのであろうか？

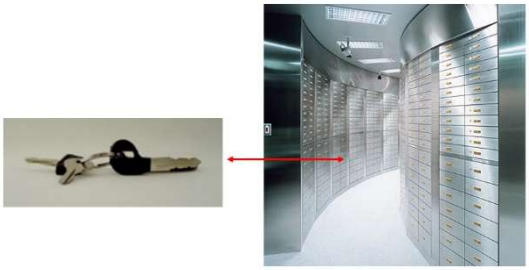
異なる銀行の口座間振込の場合はそれぞれの台帳にそれぞれの内容を書き込めばよい。振込元は送金、振込先は着金情報である。各銀行の信用により、各銀行の台帳の記載に改ざんがないことは保証されている。ビットコインの場合は､すべての口座の所有者の中に台帳の記載を改ざんする者が存在する可能性があるため、すべての口座の所有者が対等に同一の台帳を持つことで、大量の台帳を統一的に改ざんすることはできないという事実に基づいて、価値の移動という情報（取引内容）を巻き戻しができないように永遠に固定化することを保証する。その目的のためには、膨大な電気量と通信量を負担して自分には関係のない取引も含めたすべての取引内容を、すべての台帳に記録しなければならない上に、価値の移動に時間がかかるという負の側面が存在するものの、少なくとも、国家や銀行という特殊機関でなくても、国境を越えても、価値の移動が可能になった。このように、実体がなく、台帳上にしか存在しない、法定通貨でないものが仮想通貨と呼ばれている。コミュニティの参加者にとっては価値があり、参加者の間だけでは、上記のように「価値の移動」ができ、法定通貨との比較価値が乱高下するものの「価値の保蔵」もできる。

＜現金方式通貨＞



現金方式における通貨は通常「貨幣」と呼ばれる。貨幣は価値そのものを表し、貨幣を授受することで即座に価値の移動が完了する。例えば 100 円相当の価値のあるペットボトル入りの水を購入する際、100 円硬貨を替わりに差し出せば水は即、自分のものになる。さらに、匿名の貨幣は保有者が次々に変わる「転々流通性」という特徴を持つ。銀行の窓口や ATM、インターネットがなくても貨幣の交換で決済が行え、その貨幣は回収されるまでの間、転々と所有者の間を流通する。

一方、貨幣は紛失するというリスクのほかに、偽造されるという決定的な弱点を持っている。どんなに特殊な紙や金属を使って、高度な印刷を施しても、偽札・偽貨はなくならない。発展途上国では紙幣の真贋を判定するための判定機が一般の店舗でも備わっている場合がある。この真贋判定を容易にするのが現代暗号※3を使った「暗号貨幣技術」であり、究極の貨幣こそが「CryptoCash（暗号貨幣)」である。



貨幣の本質とは一体何か？貨幣の発明以来人類は長い時間をかけてこの問いに答えようとしてきた。そして 1 つの答えとして､「価値の引換券」という考え方が生まれた。例えば、貸金庫に 100 万円の日本円が入れてあることを A と B の 2 人が知っており、かつ、その貸金庫の鍵を保持するものがこの貸金庫の中身である 100 万円の所有者であることを合意しているなら、この貸金庫の鍵はこの 100 万円の引換券であり、2 人にとっては貨幣そのものと考えられる。貨幣とは関係者間で合意された「価値の引換券」なのである。

このように、CryptoCash は貨幣の本質を表現することで生み出された。CryptoCash は発行者、価値、発行日などの情報が現代暗号で暗号化された記号列である。CryptoCash が特殊な紙や印刷などの偽造防止対策が施された媒体を持つ場合は、複製を作ることは難しく二重譲渡を考慮する必要は基本的に無いので、その使用時に、真贋チェックだけ行えばよい。希少金属に刻印された場合も同様である。ところが、紙や金属などの媒体を持たない場合、つまり CryptoCash が単なる情報である場合、二重譲渡を考慮する必要があるため、そ

の使用時において、真贋チェックに加えて、二重使用のチェックが必要になる。いくら暗号化されているとはいえ、記号列の複製は容易で二重譲渡の危険性を排除できないからである。
実は、台帳方式通貨を利用して、現金方式通貨を作ることは不可能ではない。銀行口座を利用する場合、口座内の残高をそのまま譲渡することで「価値の移動」は可能である。具体的には、例えば、この口座の通帳と印鑑を貨幣に見立てて譲渡する。しかし実際には口座は銀行が認めた個人または法人のみが使用できるものであり合法的には譲渡できない。一方、ビットコインなどの仮想通貨であれば理論上いくつでもウォレットを保持できるので、ウォレット丸ごとの譲渡も可能である。実際、予め仮想通貨の口座に必要額（量）を入金しておき、この口座情報を入れたハードウエアウォレットを譲渡可能な実体として用意して、貨幣同等に使用する試みが始まっている。

＜価値と価値の創造＞
人類の経済活動にとって価値とは何であろうか？直接的には需要と供給の関係で決まる譲渡価格に相当するものが価値である。ある場所である時点での物々交換が基本的な人類の経済活動である。しかし、価値は場所や時間などの条件によって変動するので、人類は経済活動範囲を拡大して、物と物を空間と時間を超えて交換することで交易活動を行う。そのために、経済活動を行うすべての人々が価値を認める代替物として、持ち運びが容易な貨幣が発明された。当初は希少な貝殻や石、金属を、価値の明確な引換券として選び、その後、発行者の権威や信用を証書にした引換券を、貨幣として用いるようになった。このように証書を貨幣（引換券）とすることは、人類の経済活動にとってのパラダイムシフトといってよいほどの大転換であり、引換券の担保が権威や信用に限られた時代を超え、様々な価値を担保にするように進化した。今では誰でも等しく受けることのできる太陽光エネルギーや、１日に等しく与えられた時間を担保とする通貨が生まれている。例えば、時間貨幣では、ある人が１時間で与えることのできるサービスを別の人が同じ１時間で提供できるサービスと交換する。クラリネットの演奏方法の教育１時間と折り紙の勘所を教える１時間を交換するのである。さらに最近では、貨幣自体の価値が様々な条件次第で変化する必要性が生じており、地域振興や経済行動の加速化などの特定の目的に使用される。沖縄県の離島観光振興のための地域通貨を考えるなら、沖縄本島では 100 の価値しか持たない貨幣を離島では 200 の価値として使用できるようにすれば、離島観光を促すインセンティブとなる。国家や地方が発行する公債や企業の発行する社債は貨幣ではないが、貨幣と似たような性格を持ちながらも満期や利息が存在する。近い将来には、貨幣に付帯した契約を実行することで消費される貨幣も生まれてくると予測される。家を建てるために大工に支払われる未来型貨幣は、予め合意した契約に従って、工事に取り掛かる際に 3 分の 1 が大工に価値が移転し、中間検査が終わり次第残りの 3 分の 1 が移転し、最終検査が無事に終われば残金が移転するというような「スマートコントラクト」と連動した自由度の高い貨幣が登場することであろう。CryptoCash は、以上のような様々に変化する価値や条件を暗号化した記号列とすることで貨幣という引換券に変換し発行する技術であり、究極の貨幣とされる暗号貨幣そのものである。
ところで、当初、物やサービスの交換に必要な代替物（引換券）として登場した貨幣が、管理通貨制度の下、国家や金融機関による信用創造によって、今では主従入れ替わり貨幣そのものに価値があるとされるようになっている。今後 CryptoCash によって、国家以外の誰でもが、様々な価値を担保として貨幣を発行できる時代となると予測されるが、この貨幣の発行者や管理者によって、法定通貨と同様に信用創造が行われることも起こり得るであろう。実際、仮想通貨であるビットコインにおいても、ビットコインを扱うコミュニティの外の世界では何の価値をも表象するものではないが、予め定められたルールに従ったプログラム通りに運営することで、ビットコインコミュニティの中では信用創造が行われている。

近未来においては、国家が発行する法定通貨が基本的な価値基準を提供することは変わらないとしても、CryptoCash を使って、多種多様なコミュニティや個人が、それぞれに異なる価値を共有し、これを担保として貨幣を発行する時代がやってくる。そして、それぞれのコミュニティの中では信用創造さえ行われるであろう。新たな時代の経済学、貨幣学、資本主義が求められている。

※1. 自由通貨

自由貨幣は、シルビオ・ゲゼルがその代表作『自然的経済秩序』で提案した通貨制度。中立貨幣あるいは減価する貨幣とも呼ばれる。財やサービスの多くが時間の経過とともに劣化するのに対し、インフレがないと仮定すると貨幣は価値が減らない。そのため、融資する際に債務者に対して金利を請求できる。こうして、通貨を大量に保持している人間は金利収入だけで生活が可能になる。その一方で、債務者は稼ぎのかなりの部分を金利という形で吸い取られていくことで富の格差が拡大したり、利息ぶんの利益が出ない事業に対して投資が回らないなどの問題が発生する。これを解決する手段として、徐々に貨幣価値が下がる通貨の導入をゲゼルは提案した。現在、ドイツ・バイエルン州のプリーン・アム・キームゼーを中心とした一帯で地域通貨として流通しているキームガウアーなどが存在する。

（出典：Wikipedia https://ja.wikipedia.org/wiki/自由貨幣）

※2. Wallet

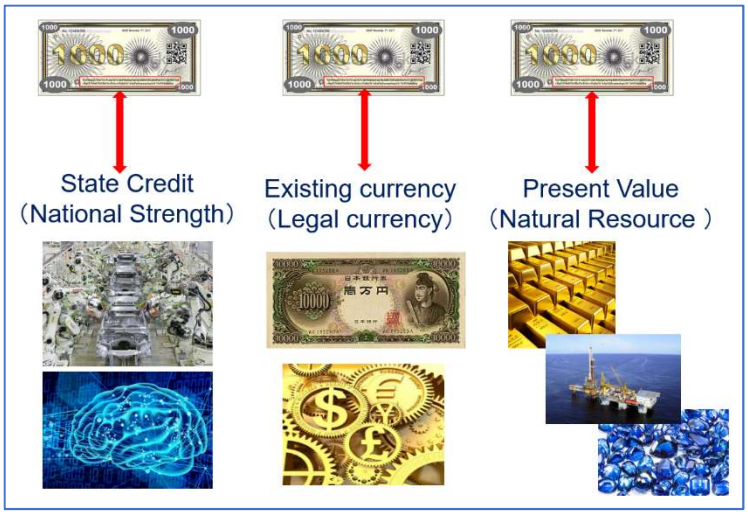
ウォレット（Wallet）とは、仮想通貨を保管するための財布のようなもので、購入した仮想通貨を保管するところと説明されることが多いが、実際はブロックチェーンなどの台帳において識別可能なアカウントと同等の働きをするプライベートキー（秘密鍵）を管理するものである。ブロックチェーンそのものをすべてダウンロードするタイプ(フルブロックチェーンウォレットとよばれる)、ブロックチェーンそのものはダウンロードしないが API（Application Programming Interface）を用いて公開されているブロックチェーンを操作するタイプ(ライトウォレットとよばれる)がある。通常、台帳上にいくらの仮想通貨が存在するか見られる機能や取引所にアクセスする機能などを有する。

※3. 現代暗号

米国国立標準技術研究所（NIST）が，弱い暗号技術の使用を 2010 年に停止する方針を発表した。従来の暗号技術は，1)暗号鍵が十分長い，2)解読の近道がないようにして，現実的な時間で解けなくすることで安全性を確保しており、2010 年、暗号アルゴリズムをより難解なものに、また暗号鍵をより長いものにすることで一時的に安全な状態に変更した。しかし，現代では，高速並列計算を可能とする量子コンピュータの出現を前提としなければならず，解読時間による安全性の確保は意味をなさない。従来暗号技術の解決すべき 2 大問題である①暗号鍵の配送問題と，②解読不可能な暗号アルゴリズム問題を根本的に解決しなければならない。現代暗号では，①については，かつてこれを解決したとされその後欠陥が見つかった公開鍵方式や量子暗号鍵配送方式ではなく，完全にこの問題を解決する新しいソリューションを，②についても、数学的に解読不可能を証明されたアルゴリズムを，それぞれ使用しなければならない。

コラム

法定通貨の発行と資本主義



昨年終わりに、中東とアフリカを訪問させて頂く機会を得た。その中で、かつての帝国主義の名残がいかに現地の人々の生活に影を落としているかをまざまざと見せつけられ、これらの発展途上国の未来を案じるとともに、この旅行中に起こった米国と欧州の移民問題や、フランスでの現政権の燃料税引き上げに対する大規模な抗議運動について聞き及ぶにつれ、旧来の資本主義が限界を迎え、新しく生まれ変わろうとしているという小さな息吹を感じた。そして、暗号通貨はその変革の道具となる可能性があると思い至った。

法定通貨は本来、国力があれば国の信用で、無ければ他国の通貨の信用を利用して発行する。それゆえ発展途上国では、旧宗主国との関係を大事にすることが貨幣経済の安定化に不可欠とされてきた。旧宗主国はこの関係を最大限に利用することで、古い帝国主義時代の利益の移転を現在まで続けることができたといえる。それゆえ、貧しい国から富める国への移民は後を絶たなかった。ところが、移転できる利益が減少し、旧来の資本主義が変調を来し始めたようである。その結果、先進国において国民全体に富を配分できた時代が過ぎ去り、貧富の差が拡大した。暗号通貨の発行が可能になったことで、自国に存在する天然資源などを担保として貨幣を発行する国が現れてきた。さらにこれを暗号通貨で行えば、従来の金融ネットワークを介さなくてもインターネット上での取引に用いることができ国境を越えて流通する。資源などの担保によって十分な信用が得られれば、宗主国との関係を見直すことができる。これは、旧宗主国にとっても今後これらの発展途上国を支援しなくてよい状況になれば、何もマイナスの効果ばかりではないであろう。新たな暗号通貨が新しい資本主義を創造し平和に貢献できると考えている。