仮想通過で銀行が消える日　真壁昭夫

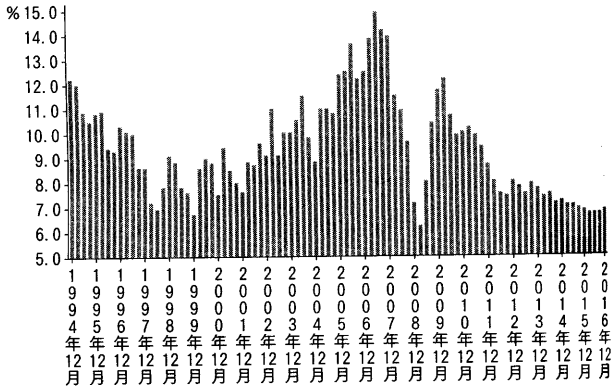
思ったよりも面白かった。銀行の生存が問われていく時代になる。

仮想通貨のタイプは大別して 2 つある。**マイニング**＝採掘によって発行される仮想通貨と、発行者がいるタイプの仮想通貨（**アセット型**）だ。
まず、マイニング型の仮想通貨を説明しよう。ビットコインはこの代表例だ。マイニグ（Mining）とは、金などの鉱脈を掘り当てることを意味する。一言で言うと、マイニングとはビットコインを〝当てる〟ことだ。ビットコインのマイニングは、一種の計算ゲームに勝って、コインの新規発行を行なうことをいう。
ビットコインの発行は、ビットコインを手に入れたいと思う、一部の有志（マイナー）が行なっている。この人たちは、ブロックチェーンの中にあらかじめ設定されている計算問題を競争して解く。そして、一番早く正解した人には、12・5 ビットコインと一種の手数料が与えられる。これが、ビットコインの発行を支える経済的なインセンティブだ。
・・・
アセット型の仮想通貨は、トークン型の仮想通貨と呼ばれることもある。トークンとは〝代用通貨〟を意味する。このタイプの仮想通貨には、コインを発行する人（企業）がいる。この発行者がコインの供給量を決めているが、発行数が決められていても、後で変わることもある。
アセット型の仮想通貨は、株式への投資によく似ている。株式は企業が発行する。新しい株券を発行すると、発行済みの株式数は変動する。そして、投資家はその企業の増益などを期待して投資する。期待した通りに企業が成長すると、株価が上昇したり、配当が支払われる。こうして投資家は儲けを手にする。

特に、中国の資本規制はきつい。中国の政府は、銀行が参加する為替の市場で、為替レートの変動率に制限を設けている。ドルに対して、人民元は基準となる為替レート（中国外貨取引センターが発表する米ドルの取引仲値）から、上下 2%以内に収まらなければならない。**上下 2%を超えて為替レートが動くと、当局は為替介入**を行なう。その他の通貨に対する変動幅は、ドルよりも緩い。ここから、中国の政府がドルと人民元の為替レートの安定を重視していることがうかがえる。
また、中国は個人が外貨を購入できる額を、1 年間に 5 万ドルと定めている。そして、企業に対しては、海外の企業の買収に対する取り締まりが強化され、5 万ドル以上の利益を海外に送る場合には、決算に関する書類などを銀行に提出しなければならない。

こうした規制の強化を通して、中国はお金を国内に強制的にとどまらせようとしている。先行きの経済への懸念から、中国から海外にお金が流出しやすくなっているからだ。
2011 年の半ばを境に、中国の経済成長率（実質 GDP＝国内総生産の成長率）の低下傾向が顕著になっている。今でも、不動産バブルの崩壊や、鉄鋼や石炭など、多くの業種で過剰な生産設備といった問題がある。そのため、企業の財務内容が悪化し、借金が返せなくなるなど、先行きへの不安は高まりやすい。地方政府の財政も悪化している。

中国の実質ＧＤＰ成長率の推移



データ出所：中国国家統計局

IMF（国際通貨基金）によると、2017 年、**ベネズエラの経済成長率はマイナス 4・5%、インフレ率は 2200%に達する**と見られている。このような破滅的な状況の下でベネズエラの通貨〝ボリバル〟は交換の手段としての機能を十分に果たせなくなっている。政府は、ゼロが何桁もくっつく高額の紙幣を準備しているが、物価の上昇スピードが速いため、高額紙幣の印刷が追い付いていない。こうしてベネズエラでもビットコインへの人気が高まっている。今後も、資本規制や通貨危機への不安が高まった場合には、自分の国の通貨よりも仮想通貨を使って資産の価値を守ろうとする人は増えるだろう。「仮想通貨なんてインチキだ」とは言っていられない状況に置かれている国は世界に多くあるのだ。

ナカモトがビットコインの基幹システムに**ピア・トゥ・ピア**（peer to Peer = P2P）を採用したのは、画期的な発想だった。peer とは、同じもの、同僚や仲間を味する。ピア・トゥ・ピアとは、仲間同士、対等な関係と考えればよい。

この意味をコンピューターネットワークに落とし込むと、ネットワーク上にある端末同士が、お互いに通信し、履歴などのデータを送ったり、受信したりすることに置き換えられる。端末間に主従の関係はなく、〝分権的〟なシステムが構築される。そのため、データを一カ所にとどめて管理する必要はなく、システムの運営コストを抑えることができることになる。これは通貨の発行コストを抑えることに他ならない。

ビットコインの発行は制限されている。今のところ、2100 万コインと定められている。そして、この制限に近づくほど（ビットコインの発行が進むほど）、採掘できるコインの量は少なくなる。マイニングの難度も上がる。その分、マイニングにかかる電気代などのコストは増えてしまう。こうなると、発行するのにコストのかかるお金を誰が欲しがるだろうかという疑問が残る。これは、ビットコイン、そしてその他の仮想通貨が解決すべき問題点だ。

このように、量に限りがあると、一部の愛好家などの買い占めが起きやすい。歴史を紐解けば、オランダのチューリップバブルはそのよい例だ。そのため、どうしても**ビットコインの価値は安定しづらい**。

欧州ではギリシャが財政の状況を虚偽報告していたことを皮切りに、南欧諸国の財政への懸念が高まった。一時はユーロの持続性への懸念も高まったほどだ。この状況に対して、ドイツは一貫して財政の立て直しを各国に求めた。その結果、失業率が急増し、各国経済の消費や投資は低迷した。そして、2014 年 6 月、欧州中央銀行は政策金利をマイナスに設定し、短期金利の低下圧力を高めようと〝マイナス金利〟を導入した。わが国も 2016 年 1 月に、「検討していない」と言っていたにもかかわらず、マイナス金利を導入した。

ブロックチェーンに不可欠な技術として、**スマートコントラクト**、改ざんを防ぐ技術（暗号化など）、**合意アルゴリズム**、P2P がある。ビットコインに関する説明でも紹介した技術だが、とても重要なため、復習を兼ねて、今一度確認しておこう。

まず、**スマートコントラクト**は一定の条件を満たした時に契約を自動で成立させるプログラムのことを言う。あらかじめ、一定の約束事を決めておき、その内容に合致したイベントが発生すると、自動で契約が成立する。これが取引プロセスの自動化や効率化を支えている。

次に必要なものが、改ざんを防ぐ技術だ。具体的には公開鍵暗号方式、ハッシュ関数が使われている。データの送信者は、ハッシュ関数を使って送るデータの**ハッシュ値**（データに演算処理を施して得られる固定長のデータ）を求める。これは、データの指紋と考えればよい。一人一人の指紋が違うように、データごとにハッシュ値も違う。そして、ハッシュ値からもともとのデータを逆算することはできない。

その上で、求められたハッシュ値を暗号化する。それによってハッシュ値の改ざんを防ぐ。その結果、データ一致の信頼度が高められる。

ブロックチェーンは〝分散された台帳〟と言われる。これは、ネットワーク上にあるデータ＝台帳の中身がまったく同じであることを指している。そこで**合意アルゴリズム**が登場する。ビットコインの場合、計算に平均 10 分かかるように設計されている。ハッシュ値が規定の条件を満たすまでランダム（Nonce……ナンス、ノンスともいう）な値を入れ続けて作業を繰り返さないといけない。これが合意アルゴリズムを用いた〝プルーフ・オブ・ワーク〟である。そのほかにも合意アルゴリズムにはさまざまなパターンがある。誰かがブロックを改ざんすると、チェーン状に隣のブロック、そのまた隣のブロックと、すべてのブロックのハッシュ値が変わってしまう。

そして、P2P がデータを管理する。

ビザンチン将軍問題とはどのようなものかを、説明しよう。ビザンチン帝国の将軍 9 人が、それぞれの軍勢を率いてある町を攻撃しようとしていた。ここで、将軍たちはどう町を攻め落とすか、攻撃計画の合意を取り付けたいと考えている。町を手に入れるためには、過半数以上の将軍が攻撃に参加しなければならないとしておこう。単純な多数決で全体の意思決定を成すことが最善の方法である。

そこで、将軍たちは互いに攻撃するかどうか、メッセンジャーを送り合って、それぞれの考えを伝え合う。その結果、4 人の将軍は攻撃に賛成し、別の 4 人は撤退したいと考えていることが分かった。

ここで 9 人目の将軍が、裏切者だったとする。彼は、攻撃に賛成の将軍らには「攻撃に加わる」と伝える。一方で撤退したい将軍には「自分も逃げたい」と伝える。これを聞いた攻撃賛成派の将軍たちは、過半数の将軍が攻撃に加わるから町を落とせると判断して、攻撃を行なう。しかし、実際には攻撃に加わった将軍は 4 人だけであるため、戦に負けてしまう。これは、裏切者によって他の将軍が欺かれることを意味する。

このように、複数の人が混ざって一つのことを決定する場合、悪意のある人が周囲をだます恐れがある。そのため、**信用できない人同士が一緒に、一つのことを作業するのは困難だと考えられてきた**。多数決ではなく、全員が合意＝データが一致することが欠かせない。

これを P2P ネットワークに当てはめると、一部のノードが故障したり、悪意ある者によって情報が書き換えられてしまうと、ネットワーク全体にウソの情報が広がる恐れがある。その結果、正しく行為できるかどうか、不安が残る。ビットコインのために設計されたブロックチェーンでは、プルーフ・オブ・アークを採用することで見事に〝ビザンチン将軍問題〟を解決した。

分散型のネットワークの制約に関する定理として、〝**ブリュワーの定理**〟がある。これは CAP 定理とも言われる。この定理は、すべてのノードで次の 3 つを同時に成立させることはできないという考えだ。その 3 つの機能は、データの一貫性

（Consistency……同じ情報でなければならない）、可用性（Availability……単一障害がなく、一部のノードがダウンしてもそのほかのノードが常に応答する）、分断耐性（partition tolerance……通信障害によってメッセージが損失されても、システムは機能する）ことを指す。
一般的に、**ブロックチェーンは可用性と分断耐性を満たしている**と言われている。その一方で、一貫性については、常に成立しているとは言い切れない。それは、確率論的にデータの一貫性が保たれていると考えられるからだ。
100%データの一貫性が確立されていないと考えられることは、ソフトフォークのリスクがあることと言い換えられる。**ソフトフォークとは、新しいルールが導入された時に以前は有効だったルールが無効になることをいう**。

~~~~~~~~~~
ソフトウェア開発におけるフォークとは、あるソフトウェアパッケージのソースコードから分岐して、別の独立したソフトウェアを開発することである。
~~~~~~~~~~

支払いの指図
~~~~~~~~~~
指図
㋑甲が乙から給付を受け丙に給付する場合、三者間の支払い関係を簡易にするため、甲（指図人）が乙（被指図人）に指図して丙（受取人）に給付させること。
~~~~~~~~~~

こうした取り組みの背景には、「銀行がつぶれると社会に大きな混乱が広がって大変だ」という、一種の思い込みがある。銀行は守らなければならないという考えは、どこの国でも強い。それは、預金者を守らなければならない、ということと同じだ。欧州では、銀行が破綻した際には、まず、銀行の株主や債権者に損を負担させることが取り入れられた。
これを〝**ベイルイン**〟という。その対義語が、公的資金＝税金を使った銀行の救済を意味する〝**ベイルアウト**〟だ。ベイルインが取り入れられた背景にも、銀行の内部に損を負担させる仕組みを作っておけば、過度なリスクテイクが進まず、銀行危機は起きない、という発想がある。

そして、世界全体の需要は供給を上回っている。どの国も、できることなら海外の需要を取り込んで自国の経済基盤を強化したい。その中で、世界の政治、経済の中心的役割を担ってきた米国が保護主義政策を重視すると、世界各地で需要の囲い込みが進む可能性がある。それは、1920 年代後半の世界恐慌を経た 1930 年代、列強がブロック経済を形成し、植民地の取り合いをしたことに似ている部分がある。

通常のインターネットでは閲覧できないトーア（Tor、深層ウェブとも呼ばれる）

金融の基本的な理論を理解していれば、個人の長期的な資産形成を考えた場合、分配ではなく、**再投資を行ない、複利の効果を享受**していくべきだ。それが、中長期の観点で資産を増やすということである。

DAO（Decentralized Autonomous Organization〉は自律分散型組織とか、単に分散型組織と呼ばれる組織運営システムに関する考え方だ。すでに、このコンセプトを使つたドイツ企業のネットワークに対するハッキング攻撃によって、資金が流出したことは述べた。そのため、DAO とはいまだ未熟なコンセプトだ。
DAO は意思決定を行なう責任者がいないシステムだ。このシステムは、分散型台

帳のネットワーク（P2P）上で自律的に投資先を決め、実際に投資（ビジネス）を行なうことを目指していた（ファンドマネージャー不在の組織が、自律的に投資先を決めて資金を運用することをイメージすればよい）。具体的には、**スマートコントラクトの技術を使い、どこに投資するかをシステムが賢く自動で決める**。これは指揮者がいないオーケストラのようなものだ。

DAO は企業のビジネスモデルを大きく変える可能性を秘めている。