連載: テクノロジーが変える私たちの生活

～私たちの身近なテクノロジーの未来をレポートします～

仮想通貨がお金になる日

副主任研究員　柏村　祐

現在､話題の仮想通貨は我々が使っているお金と共存または代替になる可能性があります。そこで今回はお金の歴史や国内外の現状をふまえてレポートします。

1. 仮想通貨誕生までのお金の歴史

最近、仮想通貨が世間を騒がしている。騒ぎになった要因は2017年４月に改正資金決済法が施行され、企業の参入が相次ぎ有名タレントを起用したテレビＣＭや､「億り人」と言われる人が雑誌やメディアで紹介されたことである。仮想通貨を語る前に、そもそもお金とは何なのか歴史を紐解いてみたい。大昔、人々は物々交換をして取引をしていた。例えば、漁師は獲った魚を農家に渡しお米を得て、農家は魚を得るためにお米を渡す物々交換が成立していた。しかし、両者の欲しいものが一致している場合のみ物々交換は成立するため、魚や米のどちらかが余ってしまう（または腐ってしまう）ケースが発生していたのである。

そこで生まれたのが「お金」である。「お金」の３要素は「価値の尺度」「価値の交換」「価値の保存」と言われている。最初に生まれた「お金」は物品貨幣と呼ばれ、組織やコミュニティー内で価値があると認められた物品によって交換することができるものであった。そのひとつとして貝貨や石貨などが幅広く浸透していた。例えば、漁師は貝貨を得るために魚を渡す。漁師は貝貨や石貨というお金によって農家からお米を受け取ることができる仕組みが出来上がったのである。しかし貝貨や石貨は容易に作れてしまう。そこでつぎに人々が目を付けたのが金属（とくに金、銀、銅）である。金属は「価値の尺度」「価値の交換」「価値の保存」においてお金に適した性質があり、金貨、銀貨、銅貨などが作られた。その後、人類は長年、金（ゴールド）を価値があるものと信じてきた。第二次世界大戦後には金本位制が強化され、１ドル（360 円）で一定の金に交換できる兌換紙幣（だかんしへい）を前提とした固定相場制の流れが進んだ。兌換紙幣は近年に至るまでまさに「お金」そのものであった。

しかし金（ゴールド）の量には限界があるため、そこにレバレッジ*[1]をかけることはできなかった。その制約を完全に取り払ったのが、1971 年に発生した米国のニクソンショック*[2]である。それ以降、変動相場制へ移行したことにより不換紙幣、つまり現在の法定通貨（ドルや円）が誕生したのである。

法定通貨の価値を担保しているものは金（ゴールド）ではなく、国家の信用である。国家の信用という目にみえないものに基づいて法定通貨は成り立っている。

そうした時代に突如現れたのがビットコインを代表とする仮想通貨である。2008 年 10 月

31 日、ビットコインに関する論文『Bitcoin: A Peer-to-Peer Electronic Cash System』が、サトシ・ナカモト（Satoshi Nakamoto*3）によって暗号理論に関するメーリングリストに投稿された。『Bitcoin: A Peer-to-Peer Electronic Cash System』の概要部分には、「本システム（ビットコイン）によるＰ２Ｐ電子決済により、金融機関を介さない直接的オンライン取引が可能になる」と書かれている（図表１）。

図表1　Bitcoin: A Peer-to-Peer Electronic Cash System

ビットコイン：　Ｐ２Ｐ電子通貨システム

中本 哲史
satoshi@gmx.com
www.bitcoin.co.jp

概要 真のＰ２Ｐ電子通貨が実現すると、金融機関の介在無しに、利用者から利用者へと直接オンラインで支払いできるようになるだろう。電子署名によって、その機能の一部は実装可能である。だが従来の方法では、多重使用を禁ずるために第三者機関を設置する必要があり、電子通貨の利点を生かせなかった。本論文で提案するのは、多重使用問題をＰ２Ｐネットワークで解決する方法である。このネットワークは、ハッシュ関数による演算量証明を利用する。その証跡をチェーンでつなぎ続けることにより、いつ、どのような取引が行われたかを証明可能にする。チェーン内の取引履歴を改ざんしようとしたら、時間をかけて演算量証明をやり直さなければならない。過去の出来事を時系列的に確認する場合には、ネットワーク上で最長のチェーンを調べれば良い。さらに、最長チェーンは、ＣＰＵ能力を最も費やした計算結果でもある。ＣＰＵ能力を持つ者の大半が、ネットワークへの攻撃者を無視していれば、その善良なノード群が作るチェーンは、攻撃者のそれを長さで上回り続ける。このネットワークに必要な規則は、極めて簡素である。メッセージはベストエフォートで拡散すれば良いし、各ノードはいつ離脱・再接続しても構わない。再接続時に最長チェーンを受け取ることによって、離脱していた間に何が起きたかを把握できるからである。

資料：Bitcoin: A Peer-to-Peer Electronic Cash System（英語）１ページ目より筆者和訳

2. 仮想通貨を利用する人々

多くの日本人は何の疑問もなく日本円を使っている。だが世界の人口 76 億人のうち、国家を信用できないため自国通貨を使用していない人は沢山いる。例えば南アメリカ北部に位置するベネズエラは 2010 年代に入ってからハイパーインフレーションが慢性化している。2018 年５月に南米ベネズエラの国会は４月時点の物価上昇率が前年同月比 13,779%に達したことを明らかにしている。日本円で例えれば１年前に 100 円だったものが 13,779 円払わないと買えないということである。ベネズエラのようにハイパーインフレーションに苦しむ国の人々は自国の法定通貨を信用していない。

同様にアフリカ大陸の南部に位置するジンバブエでは 2008 年に起きた凄まじいハイパーインフレーションへの対抗策として自国通貨を廃止し大半の商取引を米ドルで決済してきた。しかし現在は外貨不足が深刻化し、政府は米ドルと等価の「ボンドノート」*4と呼ばれる銀行券を発行し何とか対処しようとした。ところが、近年ではボンドノートの相場は闇市場で下落していることから国家への不信感が高まり仮想通貨の使用が一般に広く浸透しつつある。つまり、自国の通貨を信用できない状況で、必然的に財産を守りたいと思う人々が仮想通貨

を使っているのである。

3. 仮想通貨を維持する仕組み

仮想通貨の特徴を一言で表すとすれば、中央管理者が存在しない非中央集権的なシステムである。法定通貨は中央銀行が発行・管理をしており中央組織が管理をしなくては維持できない。例えば「ＡさんがＢさんに１万円送金した」「Ｂさんが銀行から５万円出金した」という取引履歴は銀行が管理している。銀行の巨大な中央集権的なシステムは、維持コストが膨大であると同時に度々発生するシステム移行に伴うＡＴＭやオンラインサービスの休止が発生したりする。

一方仮想通貨はネットワークが止まらない限り24時間365日動き続ける自走式のテクノロジーである。ネットワークに参加するノード*5同士が、それぞれ仮想通貨を維持する拠点となり「ＤさんがＡさんに１ビットコイン送金した」「ＣさんがＢさんに３ビットコイン送金した」という取引を記録し、不正がないかを検証し維持されている。取引を記録した台帳は「分散型台帳技術」と呼ばれ誰でもみることができる。仮想通貨の代表格であるビットコインを例にとれば約10分ごとに世界中でおきた取引情報を記録している。この10分ごとの記録は「ブロック」と呼ばれ、検証が終わったブロックが鎖のように繋がっていくことを「ブロックチェーン」と呼んでいる。2009年１月４日に最初のブロック（ジェネシス・ブロック）が生成されてからすでに53万以上のブロックが生成されている（図表２）。

図表2 ビットコインのブロック生成数

ブロック番号	タイムスタンプ	合計送金額（ＢＴＣ）	マイナー	サイズ（ＫＢ）
532549	2018-7-19 00:42:10	2,550.38	BTC.com	523.03
532548	2018-7-19 00:37:33	657.06	AntPool	16.65
532547	2018-7-19 00:37:03	3,391.51	BTC.TOP	1,034.83
532546	2018-7-19 00:28:34	57.31	AntPool	26.03

注　：マイナーとはマイニング（採掘）を行う人あるいは組織
注　：ブロック番号とはビットコインの送受信記録が保管された塊
資料：https://www.blockchain.com/より筆者作成

参加しているノードはボランティアでブロックに不正がないかの検証をしているわけではない。最初にブロックの検証を完了したらネットワークから新たに発行されたビットコインを報酬として貰えるのである。この検証作業を金の採掘になぞらえてマイニングと呼ばれる。報酬については４年ごとにマイニングによる報酬が半減していく仕組みが導入されており、

2009年当初は１ブロックあたり50ビットコイン貰えた報酬は現在１ブロックあたり12.5ビットコインとなっている。ビットコインはブロックチェーンという堅牢な仕組みとマイニングという報酬を与えることによって維持されている。システムで設定されている発行上限の2100万ビットコインが全て採掘されるのは2140年頃と言われている。ビットコインと法定通貨の違いは以下の通りである（図表３）。

図表3 ビットコインと法定通貨の違い

特徴		ビットコイン	法定通貨
発行・管理	発行者	システムが自動的に発行	日本政府（通貨） 日本銀行（紙幣）
	管理者	Ｐ２Ｐネットワーク参加者が分散管理	同上
価値	発行上限	2100万ＢＴＣ	なし
	価値の裏付け	システムへの信用	日本政府への信用
送金処理	送金の方向	双方向	双方向
	送金の処理時間	約10分間隔でブロックを作成	直接の受け渡しであれば即時 長距離、大量だと時間がかかることもある
	送金の手数料	少額 送金者負担	高額 場合によって両方負担
匿名性	取引の匿名性	取引履歴は明らかだが、匿名性あり	高い
	取引履歴の公開	公開	非公開

資料：平成27年度 我が国経済社会の情報化・サービス化に係る基盤整備（ブロックチェーン技術を利用したサービスに関する国内外動向調査）報告書（経済産業省ウェブサイト）

4. 仮想通貨という革命

仮想通貨はブロックチェーンを利用したイノベーションである。インターネット革命に匹敵するインパクトのあるテクノロジーと考えられる。1990年代にインターネットを初めて使ったときに、まだアナログの電話回線を通じた非常に脆弱な通信インフラだったためホームページのダウンロード時間が異様にかかり正直こんなテクノロジーは使えるのか？と思ったものである。それから20年経過し今では、電車に乗れば老若男女問わずスマホで動画や漫画、ＳＮＳやゲームに没頭する光景が当たり前になっている。仮想通貨はまさに20年前のインターネットと同じように黎明期にある。いずれインターネット革命のように我々の生活スタイルを一変させる可能性を秘めている。

日本では 2018 年１月に発生した取引所からの仮想通貨流出事件や監督官庁による相次ぐ取引所への行政処分といった報道がされている。当該事件の原因はセキュリティが万全でないのに金融サービスを運営、取引を開始したリスク管理の「甘さ」にあろう。再確認したいのは仮想通貨そのものの問題があったわけではないという点である。われわれの生活を便利にしてくれる新しい「お金」と捉え未来に向かってポジティブな見方もできるのではないだろうか。20世紀を代表するノーベル経済学者のフリードリッヒ・ハイエク*[6]は「貨幣発行自由化論」（1976 年刊行）において、通貨の脱国営化論を提唱している。市場を通じた通貨の

自由競争によって、最も健全で安定した通貨が発展するというアイデアである。仮想通貨は金融既得権益に左右されない公平で透明な「お金」になる可能性を秘めているのではないだろうか。

【注釈】

*1　「てこ」の意味。少ない資金で大きな金額を取引できる事をレバレッジ効果と呼んでいる。
*2　アメリカ第37代大統領リチャード・ニクソンが1971年8月15日に発表した金とアメリカ・ドルの兌換停止宣言のこと。
*3　インターネット上の仮想通貨「ビットコイン」を創設した人物の名義。正体は不明だが、暗号理論やP2Pのシステムに精通した人物と言われている。
*4　ハイパーインフレーションの再来に対する懸念が広まる中、深刻な現金不足を緩和するため、発行された米ドルと等価の自国版紙幣のこと。
*5　ネットワークに直接接続されているコンピュータのこと。
*6　フリードリヒ・アウグスト・フォン・ハイエクは、オーストリア・ウィーン生まれの経済学者、哲学者。経済学、政治哲学、法哲学、さらに心理学にまで渡る多岐な業績を残した。20世紀を代表する自由主義の思想家。