ARCJ定例会
「ビットコインの思想史」

開催日：2020年11月２５日
会場：銀座中央区民館３号室
講師：三上哲寛

I. プレゼンテーション

こんにちは、今回の定例会は「ビットコインの思想史」についてです。

ビットコインの歴史

まず、ビットコインの歴史から見ていきましょう。2008年10月31日、謎の人物サトシ・ナカモトがインターネットでビットコインの仕組みを説明するホワイトペーパーを発表します。これはネット上で誰でも見ることができ、2009年1月3日には「ジェネシスブロック」が生成されます。ブロックチェーンとは文字通り、ブロックが鎖のように繋がっていく仕組みですが、この日に最初のブロックが創世され、稼働し始めました。

2009年1月10日に二人目のユーザーとなるハル・フィニーがビットコインネットワークに参加します。フィニーは実在の人物で、アイン・ランドの思想の影響も受けていました。

同年10月に1ドル1,000ビットコインで、ビットコインが初めて法定通貨と交換され、2010年5月22日には初期の採掘者ラズロ・ハニエツが10,000BTCでピザ2枚を購入します。2020年11月25日現在で、1ビットコイン2,000,000円に迫っていますから、ハニエツが買ったピザは現在のビットコインの価値で換算すると２０億円にもなり、史上最も高価なピザでしょう。ですが当時の開発者にとっては、10,000ビットコインはピザ2枚の価値しかなかったわけです。

2010年12月12日にサトシ・ナカモトが最後の投稿をして、インターネット上から姿を消します。彼が誰かは大きな謎として残ったままですが（日本人ではない説、複数人のチームである説も有力）、それとは関係なく、ビットコインは様々な技術者やユーザーの努力によって発展してきました。

先ほど言及したハル・フィニーについては以下の記述があります。

…「エレクトロニクス時代の開かれた社会に、プライバシーは欠かせない」
こうした発想は1970年代と80年代のカリフォルニアで広まった政治的自由主義の延長と考えられる。この政府に対する不信感は、日々コードを書いて独り新たな世界を生み出しているハルのようなプログラマーにとって、なによりしっくりくるものだった。ハルはカルテックとアイン・ランドの小説を通じて、こうした考え方を身につけた。ただプライバシーの問題は、リバタリアン（自由至上主義者）だけでなく、人権活動家をはじめ反体制運動家にとっても関心のあるテーマだった。…（ナサニエル・ポッパー、土方奈美訳『デジタル・ゴールド―ビットコイン、その知られざる物語』から引用）

ビットコインの最初期の開発者であるハル・フィニーはアイン・ランドの小説（おそらく『肩をすくめるアトラス』？）の影響を受けていたようです。ビットコインの仕組み自体にもアイン・ランドの思想との親和性が見られます。

先ほど言及した「ジェネシスブロック」には、サトシによって以下のメッセージが付されていました。

The Times 03/Jan/2009 Chancellor on brink of second bailout for banks
（財務大臣は銀行を二度目の救済へ）

The Timesはイギリスの新聞なので、当時サトシはイギリスに住んでいたのではないかという推測もあるのですが、それはさておき、リーマンショックのさなか、国家が短期間に二度にもおよぶ銀行救済によって自由市場に介入することにサトシはネガティブな感情を抱いていたわけです。それはビットコインの設計にもあらわれているのですが、ここからはビットコインの仕組みついてざっくりと見ていきましょう。

ビットコインの仕組み

ビットコインは「お金」なので、私が友人から絵画をもらった対価にビットコインを支払う場面を、集合ポスト（パワポ参照）のアナロジーで説明します。雲の上に巨大な集合ポストがあるのを思い浮かべてください。208号室とか301号室というふうにそれぞれのポストに付されている番号が「ビットコインアドレス」です。私は301を、友人が208を使っているとしましょう。

私が301の暗証番号を入力し、扉を開けてビットコインを取り出し、それを208に入れたら、私は友人にビットコインを支払ったことになります。この暗証番号がビットコインの「秘密鍵」です。私は301のポストを自分のもののように使っていましたが、301の暗証番号（秘密鍵）を知っている人なら誰でも301にあるビットコインを使えます。ですから、ビットコインを使う人は秘密鍵を厳重に管理しなければいけません。他人に教えるのはもっての外です。

301から208へビットコインが移動したら、それを記録する必要があります。実は、ビットコイン以前にもデジタル通貨の試みは多くありましたが、ことごとく失敗に終わっていました。それは「二重払い」と「中央集権」の問題があったからです。

「二重払い」問題とは、例えば私が301から208へ支払ったビットコインを、301から507にも支払うことができてしまう問題です。現金であれば同じ千円を2回使うことは物理的に不可能ですが、デジタル通貨は「情報」をやりとりするので、「二重払い」の可能性を排除することが難しかったのです。

「中央集権」の問題とは、デジタル通貨のやりとりを一箇所で管理していると、そこがハッキングされたらシステムが壊滅的な被害を被るという問題です。それまでのデジタル通貨は中央管理者と運命共同体だったわけです。ビットコインはこうした問題を以下の仕組みで解決しました。

まず、ブロックチェーンという「改竄を防ぐ」仕組みです。ノートに記録するアナロジー（パワポ参照）で考えましょう。301から208へビットコインが移動したら、それをノートに記録することになりますが、一旦記録されたらそれを改竄することはできません。でも、ノートに記録する人がいつも同じ人なら、その記録は信用できません。

そこで出てくるのが、マイニングの仕組みです。ノートに記録する権利を、計算問題の答えを最初に見つけた人に与えるのです。今この瞬間も世界中のマイナーたちが大量のコンピュータを稼働させて計算問題を一生懸命解いています。その努力によって答えを見つけた対価としてビットコインの報酬をもらうので、答えを見つけたマイナーはビットコインの信用を傷付けないために、ちゃんとノートに記録するのです。

言い換えれば、「改竄できないノートをみんなで書く」仕組みを作ったことで、ビットコインは「二重払い」と「中央集権」というそれまでのデジタル通貨が抱えていた問題を解決したのです。（他にも「ノード（Node）」などの重要な仕組みがありますが、ここでは省略します）

ビットコインの３つの特徴

以上の仕組みにより、ビットコインには大きく3つの特徴があるといえます。「非中央集権」「プライバシー」「希少性」です。

まず、「非中央集権」とは、中央管理者を信用せずに送金できることです。例えば私がアルゼンチンの友人にお金を送るとき、銀行やクレジットカードを通じて支払うと、そうした仲介者を信用する必要がありますが、ビットコインなら誰も信用することなく直接アルゼンチンの友人に支払うことができます。これはビットコインが「非中央集権」の分散型ネットワークだからです。

次に、ビットコインは「プライバシー」を保障するように設計されました。ビットコインを使うために身分証明をする必要はありません。さらに、所有には「物理的所有」と「名前による所有」がありますが、ビットコインは「情報による所有」ができる資産としても画期的です。秘密鍵という「情報」さえ知っていれば、ビットコインを所有できるのです。あるベネズエラ人は、秘密鍵だけ暗唱して身一つで国外逃亡したそうです。「物理的所有」しかできない金塊や「名前による所有」しかできない銀行預金は持ち出せないため、ビットコインの秘密鍵という「情報」だけを持ち出したのです。もっとも、ビットコインはpseudonymousであり（集合ポストのアナロジーでいえば、301の所有者が誰かは分かりませんが、コインの動きは世界中に公開されています）、現金のようにanonymousではないので完全にプライバシーが保障されているわけではありません。（モネロなど匿名性が非常に高い仮想通貨は他にあります）

最後に、ビットコインは供給量の上限が定められているので、「希少性」があります。もともとサトシはビットコインを支払手段として想定していましたが、現在ではビットコインはむしろ金のような「資産」と捉えられることが多いです。これは、紙幣を恣意的に増刷できる中央銀行を中心とした法定通貨のシステムに対する不信感のあらわれでもあります。前述したジェネシスブロックのメッセージもそうした不信感を示していたといえるでしょう。

希少性を担保し、インフレを抑えるビットコインの設計はすべての分散型の仮想通貨に共通ではなく、供給量の上限が定められていないものも多くあります。ただし、仮想通貨の元祖たるビットコインが誕生から10年以上経った現在でも価値を保持しているのは、供給量の上限があるシステムを人々が支持しているからでもあります。ビットコインの思想は、その設計者だけでなく、支持者の価値観も反映されているところが面白い。

ビットコインの思想

「ブロックチェーン」はまだまだ試行錯誤の段階ですが、「法定通貨の世界で私たちは本当に自由なのか？」という強烈なメッセージを投げかけたビットコインは、世界に大きなインパクトを与えたと思いますし、このような「私的かつ無国籍な通貨」への動きは、アイン・ランドの思想を色濃く反映しています。

通貨の世界における中央集権的なシステムから脱却を図る、という理念は多くのビットコイン支持者の間で共有されています。ランド思想に共感するオブジェクティビストにはビットコインの支持者も多く、今日でも真面目にFED（連邦準備制度）不要論が語られていると言います。そうした議論が現実的なのか、理論的に正しいのか私にはまだ分かりません。ドルや円はすぐにはなくならないでしょう。

ただ言えることは、ビットコインの登場によって、法定通貨を前提とした世界をより相対的に見られるようになったことです。既存の中央集権型の通貨で私たちは本当の自由を獲得できるのかと誰もが考えるようになった時点で、サトシ・ナカモトの試みは半分成功しているのではないでしょうか。

今後の展望

ビットコインは構造上、「オタクか犯罪者しか使わない」とか「信用に値しない」と、当初から言われ、ウォールストリートからも懐疑的な目を向けられていました。やはり従来の中央集権的システムとは「水と油」の関係なのです。

そこで出てきた考え方が、「大事なのはビットコインではなくてブロックチェーン技術だ」というものです。ブロックチェーンは世界を大変革する技術だと言われることもありますが、本当にそうでしょうか。

ブロックチェーンの本質は「みんなで書いた改竄できないノート」です。

例えば、戸籍はブロックチェーンで管理するべきでしょうか。男の子が生まれ、ブロックチェーンに記録されて、後で女の子だと分かったらどうでしょう。従来のアナログな管理の方が融通が利くのではないでしょうか。

また、スマートコントラクトという仕組みを備えた仮想通貨がイーサリアムを皮切りに数多く登場し、将来を期待されています。スマートコントラクトとは契約を自動的に執行する仕組みのことで、駄菓子屋のおばあちゃんがジュースを渡してくれるプロセスを自動化させた自動販売機のようなものです。

しかし現状、スマートコントラクトの仕組みだけでは、誰かの判断を排除することが難しい。例えば農家と保険会社が「雨が30ミリ降ったら保険金を支払う」という契約をスマートコントラクトで結んだとします。「雨が30ミリ降った」とは誰がどのように決めるのでしょうか。中央集権を排除しようとするブロックチェーンのそもそもの目的が達成されていないことにもなります。

ブロックチェーンを現実世界に応用しようとすると、現実世界とブロックチェーンをリンクさせる難しさがあります。また、現実世界では他にも自然法則、法律、道徳などの「現実世界の論理」があり、ブロックチェーンの論理との違いを克服するには単なる技術以上の問題が潜んでいます

また、中央集権と非中央集権は善悪の問題とも限りません。民主的に決めたほうがいいか、カリスマの独裁が効率が良いかは場合によります。非中央集権（decentralization）が万能なわけではない。ブロックチェーンは、将来性は非常にあるけど得意分野が限られてくる技術かなと個人的には思います。

一方、「お金」や「ゲーム」など仮想世界で完結している分野であれば、「ブロックチェーンの論理」に支配されても問題はありません。（集合ポストのアナロジーでは、301から208へお金を送ったら、たとえ騙されていようが宛先を間違えていようが、208にお金が渡った事実を受け入れるしかなく、みなが「ブロックチェーンの論理」に従っているからシステムが成り立っています）

今のところ、ブロックチェーンの良さが一番発揮されているのは「お金」や「ゲーム」など仮想世界で完結している分野に限られているようです。

II. ディスカッション

1. 仮想通貨は、犯罪防止の観点から規制すべきかどうか

各国政府の中には、匿名性の高い仮想通貨は犯罪防止の観点から規制すべきという方向性が議論されているところもある。

＝＝＝＝＝＝
　…銃の所持規制を求める声が上がると、全米ライフル協会は決まって、「銃が悪いわけではない。銃そのものは何も悪いことはしない。悪いのは銃を使って犯罪をする人間である」と声高に主張する。
このような愚かな主張を真に受けているアメリカ人が多いというわけではない。…（中略）…
　タックス・ヘイブンも同じである。「タックス・ヘイブンが悪いわけではなく、タックス・ヘイブンを利用して悪事をはたらく人間が悪い」などという、愚にもつかぬ理屈が成り立つはずがない。タックス・ヘイブンはその存在自体が悪である。そこを見誤ってはならない。…（志賀櫻『タックス・ヘイブン―逃げていく税金』から引用）
＝＝＝＝＝＝

という記述を参照しながら、銃・タックス・ヘイブンを仮想通貨に置き換えて「仮想通貨は悪くなく、悪いのは仮想通貨を使って犯罪をする人間である」という理屈の肯否について議論した。これについては、「人間が悪いか媒体が悪いか」という二項対立で考えることは不適切であり、歴史的事情や媒体の性質などの個別事情を考慮しないと議論することは難しいとの意見があった。また、アイン・ランドのお金に関する記述を踏まえて、お金はもともとニュートラルなものだから、それを規制すべきではない、という意見もあった。

2. ドキュメンタリー　「泣きながら生きて」（２００６）

作品の紹介。ある中国人夫婦の物語。
お金の本来の価値とは何か。

３．『肩をすくめるアトラス』ラグネル・ダナショールドの引用

ダナショールドの引用から国家と税金の正義について。