WIDE Technical-Report in 2013

# ビットコイン — 人間不在のデジタル巨石貨幣

wide-tr-ideon-bitcoin2013-00.pdf


WIDE Project : http://www.wide.ad.jp/

*If you have any comments on WIDE documents, please contact to board@wide.ad.jp*

Title: ビットコイン — 人間不在のデジタル巨石貨幣
Author(s): 斉藤 賢爾 (ks91@wide.ad.jp)
Date: 2013-12-31

# ビットコイン — 人間不在のデジタル巨石貨幣

斉藤 賢爾
ks91@sfc.wide.ad.jp

2013 年 12 月 31 日

**概 要**

本稿は、2013 年末の時点で日本でも一種の社会現象となったデジタル通貨 (デジタル技術により創られたオルタナティヴ通貨) である**ビットコイン (Bitcoin)**[4, 15] について、概要を解説し、その誕生と設計の背景を探るとともに、技術とポリシーの統合的観点から問題点をまとめ、「人間不在のデジタル通貨」に対して「人間のデジタル通貨」を提案するものである。

ビットコインの誕生の背景には、各国の中央銀行が発行する法貨 (円、ドル、ユーロ等) への不信があると思われる。ビットコインは、技術的には、いわば「デジタル貝殻貨幣」あるいは「デジタル巨石貨幣」を暗号および P2P (peer-to-peer) 技術の応用により生み出したものだと考えることができる。貝殻貨幣や巨石貨幣そのものは、人間の知恵が生み出した尊い文化であるが、それらが人間の信用に基づかず、現代社会のグローバリズムとともに使われるとき、現代の法貨に由来する社会の諸問題を解決するよりも、むしろそれらを助長する恐れがある。

ビットコインは「信用ではなく、暗号学的な証明に基づく支払いシステムをつくる」という宣言の下で開発されたが、人間の信用に基づくセキュリティという考え方を持たないが故に、秘密鍵の紛失や漏洩に対する保障がない。一方で、コインの二重消費 (double spending) の回避を設計の中核と置きつつも、二重消費により不利益を被るのが誰かが不明確であり、システムの健全な運用は結局のところ善意 (システムの信用を保とうとする意思) と惰性に頼っているという危うさがある。また、ビットコインの設計には、3 層のギャンブルの構造が組み込まれていると言え、人々がそのことに無自覚に自らの人生を賭けていくとすれば、社会は何らかの対策を持つ必要があると考える。

以上のように多くの問題を抱えるビットコインであるが、法貨の絶対的な地位に対してオルタナティヴを示せたという意味で、今後、起こり得る変化の予兆としての意義は大きいと考える。

## 1 はじめに

### 1.1 ビットコインとは何か

ビットコイン (Bitcoin)[4, 15] は、サトシ・ナカモトという仮名をもつ匿名の人物により 2009 年に提唱されたオルタナティヴな貨幣の仕組みであり、かつそのオープンソースソフトウェア (MIT ライセンス [16]) である。コンピュータの計算パワーさえ十分にあれば、誰でも「無」から電子的なコインを作れ、実際の商取引に利用できる。

**用語** ビットコインは、円やドルなどのいわゆる「リアルマネー (real money)」に対して「仮想通貨 (virtual currency)」と呼ばれることもある。しかしこれらの用語は不正確である。貨幣 (交換の媒体) や、通貨 (通用力をもつ貨幣) は、円やドル、金(きん)なども含めて、そもそも仮想的な存在である。貨幣は、それとは物理的に異なる商品と「等価」であると「見なす」、いわば心理現象に則った事物だからである。

「仮想通貨」に代わる用語では、ビットコインは「デジタル通貨 (digital currency)[1]」[24] あるいは「暗号学的通貨 (crypto-currency)」などと呼ばれる。前者は、「デジタル技術により創られたオルタナティヴ通貨」を意味する。これは後者よりも包括的な概念であり、暗号学的通貨でない (すなわちその本質的な部分に暗号技術を用いない) デジタル通貨は可能である。

本稿では、デジタル通貨に対して、政府や中央銀行が発行する貨幣を「法貨」(法に拠る強制通用力をもつ貨幣) という言葉で区別する。また、通貨システムに言及する際は「ビットコイン」、支払いに使われる実際の貨幣に言及する際は「BTC」という用語を用いることでこれらを区別する。

**デジタル通貨の小史**　2013 年 12 月現在の Bitcoin Project のウェブサイト [4] に掲載されている動画では、「最初の非集中デジタル通貨 (first decentralized digital currency) 」という言葉が使われているが、これは正しくない。

当該ウェブサイトの FAQ にも記載されている通り、ビットコインのような暗号学的通貨のアイデアは 1998 年に既に提案されている。

2000 年には、ファイル共有システムである Mojo Nation[1] が「Mojo」という通貨単位を導入していた。これは単一のサーバにより発行されるトークンに基づいていたため、非集中とは言い難かった。

2003 年には、分散ハッシュテーブル [37] 上に置かれた「バンク集合」に基づく支払いシステムである Karma[23] が提案された。これは同年に提案された種々の非集中的デジタル通貨システムのひとつだと言える。

同じく 2003 年には、遠隔のストレージ領域を互いにフェアに使用するための仕組みである Samsara[7] が提案された。これは通貨ではないが、ストレージ領域という共通の計算機資源に基づく商品貨幣[2]の可能性を示唆するものだった。(実際、2008 年に本稿の筆者が「ストレージ本位通貨」を提案・実装している [22]。)

また、同じく 2003 年には、コインの発行と回収を参加者が自律的に行うことができる PPay[32] が提案された。

本稿の筆者も、債務証書の発行と回収を参加者が自律的に行うことができる形式の地域通貨 [26] である「ワットシステム」をデジタル化した *i*-WAT[20, 21] を 2003 年に発表し、運用を開始した。

また、遅くとも 2006 年までには、バケツリレー的に支払いを行うシステムである Ripple[9] が萌芽的に提唱されている。

2009 年のビットコインの発表以降は、ビットコインと同様のプロトコルに基づき、セキュリティと後述する《採掘》のコストの面で改良された Litecoin[13]、Litecoin の変形であると考えられ、柴犬のキャラクターを用いた冗談から始まった Dogecoin[17] 等、言わばビットコインの「亜種」が数多く生み出されている。本稿ではビットコインの設計について批判を加えるが、その批判は押し並べて、これらの亜種に対しても等しく適用できる。

## 1.2　ビットコインが注目される背景

以上のように、2003 年以降の 10 年あまりで、数々の非集中型・分散型のデジタル通貨が提案・実装・運用されているが、中でもビットコインが最も普及していることは間違いない。

ビットコインの貨幣である BTC は法貨で購入できるが、日本円などで固定された価格をもつものではなく、現代の各国の法貨が互いにそうであるように (あるいは金(きん)がそうであるように)、交換レートが変化し、値動きがある。レートは安定せず、最初は無価値と言えたものが、最近 (2013 年 12 月 3 日現在) では 1BTC の価格が 10 万円を超えるなど、当初と比較して高騰が続いている。

[1]デジタル通貨という用語も奇妙ではある。「デジタル」は量を数字列で表現することであり、通貨は押し並べて価値の尺度・交換・保存の機能を満たすために数字列により価値を量的に表すものだからである。しかし、対義語である法貨を暗黙に「現実的」ないし「物理的」であると見なす「仮想通貨」よりも用語として正確なので、本稿では「デジタル通貨」を採用する。

[2]例えば米など、共通性の高い商品自体を貨幣として用いる仕組み。

そのことから、最近にわかに社会的な注目を集めることになり、日本のテレビメディアや新聞でも盛んに取り上げられるようになった[3]。

後述するように、ビットコインは現金 (特に金貨) を模した仕組みであるため、ある程度の匿名性を持ち、一部では犯罪に使われた例もある [14] (この点で注意が必要なのは、少なくとも日本での報道には、「現実」の法貨と異なる「仮想的」な通貨が現れ、法貨と異なるが故に犯罪に使われているという印象を与えるものが多いが、むしろ法貨に似ているから犯罪に使われるのだという点である)。また、投機的な興味も集めているので、各国政府も無視できない状況になってきており、2012 年 12 月のフランス [2] を筆頭に、2013 年 8 月のドイツ [11] 等、通貨当局が何らかのかたちで認可し、規制の対象にする動きが出ている。

### 1.3 本稿の動機と目的

筆者は、前述したように主として地域通貨の電子化の観点からオルタナティヴな貨幣について研究を続けており、ビットコインの誕生と同じ 2009 年には一般向けの書籍 [36] を上梓した。『誰でも「無」から貨幣を作り出せるようになること』について、10 年以上、研究してきた身としては、ようやく、貨幣のこうしたオルタナティヴな在り方について注目が集まるようになったと感じ、そのこと自体には感慨深いものがある。

しかし、ビットコインやその亜種には技術的・ポリシー的な問題点が散見される。ビットコインに対しては、これまで多くの批評や批判があったが、それらに欠けているのは**通貨を実現するソフトウェアを設計する者からの視点**である。筆者には、計算機科学者として、地域通貨をデジタル技術で実現する研究を続けてきたというユニークなポジションから、世界に向けて発信すべき内容があると考え、本稿をまとめることにした。

本稿は、ビットコインの概要を解説し、その誕生と設計の背景を探るとともに、技術とポリシーの統合的観点から問題点をまとめることを目的とする。また、ビットコインを「人間不在のデジタル通貨」と考える場合の対立概念である「人間のデジタル通貨」を、これまでの研究成果を元に提案する。

## 2 貨幣はなぜ使えるか

ビットコインが中央銀行や政府に依らずに貨幣を生み出す仕組みは、実のところ、その本質的な部分では、中央銀行や政府による行いと変わりがない。それは「これは貨幣として使用できる」という共通の信念 (あるいは共同幻想 [41]) を創り出すということである。

ここで、「なぜ貨幣は使えるのか？」という素朴な疑問を振り返りたい。A 氏から B 氏に例えば千円札なりの紙幣を渡し、A 氏が B 氏から何かを買えるのは、紙幣を受け取る B 氏が、受け取った後に、その紙幣を他人、例えば C 氏に対して使えると信じているからである。その信念がなければ、B 氏には A 氏から紙幣を受け取る理由がない。**貨幣が使えるのは、皆からそれが貨幣であると信じられているからである**[4]**。**貨幣が貨幣であるために、それ以上の条件はない。逆に、その条件が満たされるなら、何であれ、貨幣になることができる。このことは直観的でないかも知れないが、詳しくは、例えば [33, 39] を参照されたい。

「これは貨幣として使えるものである」ということを「信じてもらう」やり方は、中央銀行や政府の方法と、ビットコインの方法とでは大きく異なる。だが、基本的には、前者が「国家という物語」、後者が「数学的な証

[3] 2013 年 11 月末から 12 月にかけて、少なくとも NHK 総合「NEWS WEB」、「ニュースウォッチ 9」、日本テレビ「NEWS ZERO」、フジテレビ「スーパーニュース」等で報道された。また日本経済新聞が 2013 年 12 月末に詳しい記事を掲載している [42]。

[4] 貨幣の本質を突くこの議論について、政府が担保する法貨に対してはそのまま適用できないと指摘する向きもある [35]。しかし、法貨は政府の徴税能力により担保された債務証書であり、税もまた法貨で収められる以上、同語反復しているという指摘は免れない。

明をベースに貨幣が作られたという物語」を打ち出すことだと言え、何か多くの人々が信じられる物語をつくる、という点では共通している。

次節で述べることは、したがって、BTC が貨幣として使えることの本質的な仕組みではなく、BTC が貨幣として使えると信じる人々の、その信念を支える物語の一部である。

# 3 ビットコインの仕組み

## 3.1 電子コインとその所有の表現

電子的にコインを作ったとする。それはその一番コアな部分では、単なるデジタルデータである。単なるデジタルデータは、コピーすれば誰でも同じものを所有できる。それでは、貨幣としては信じられにくい (貨幣になれないわけではない)。

ビットコインでは、「デジタル署名 (digital signature)」[25] の技術を用い、コインの現在の所有者が誰であるかを明確にする。

ここで、デジタル署名の仕組みを簡単に振り返りたい。各自は「公開鍵」$K$ と「秘密鍵」$K^{-1}$ の「鍵ペア」$< K, K^{-1} >$ を持ち、公開鍵 $K$ は公開し、秘密鍵 $K^{-1}$ は隠し持っておく。秘密鍵で暗号化したデータは、ペアとなる公開鍵でしか復号できない。

**署名** あるデータ $m$ に対しデジタル署名を施す際は、まず $m$ に「暗号学的ハッシュ関数[5]」$H$ を適用した固定長 (実際の関数により異なるが 160bit, 256bit 等) の値である $H(m)$ を計算する。この値を「ハッシュ値」と呼ぶ。ハッシュ値を秘密鍵 $K^{-1}$ で暗号化した $\{H(m)\}_{K^{-1}}$ を「デジタル署名」または単に「署名」と呼び、$m$ とともに相手に送る。

**検証** 相手も $m$ からハッシュ値 $H(m)$ を計算し、それが署名を公開鍵 $K$ で復号して得られる内容と一致するかを確かめる。このことを署名の「検証」と呼ぶ。一致しているならば、次のふたつのことが言える。

1. 間違いなく本人が署名を行った (秘密鍵は本人のみが使用できるように隠されているため)。
2. 署名された後、データは改竄されていない。

ビットコインでは、デジタル署名を図1のように使用し、署名のチェイン (連鎖) によりコインの取引履歴を表現する。コインの現在の所有者は、相手にコインを支払う際、現在のコインのデータ (自分が受け取ったときのコインのデータ) と相手の公開鍵を合わせたデータに対して暗号学的ハッシュ関数を適用し、自身の秘密鍵を用いて署名を施す。コインを受け取った相手は、そのひとつ手前の取引における受け手の公開鍵を用いて署名を検証するとともに、ハッシュ値を再計算することで、コインが正当な所有者 (すなわち、そのコインの直前の取引における受け手) から渡されたことを確かめる。

[5]暗号学的ハッシュ関数 $H$ は、データ $m$ が与えられた場合、$H(m) = H(m')$ となるような $m'$ (ただし $m' \neq m$) を現実的な時間内に計算により求めることができず、したがって、ハッシュ値 $H(m)$ が与えられても $m$ や $m'$ を現実的な時間内に計算により求めることができないという性質を持つ。

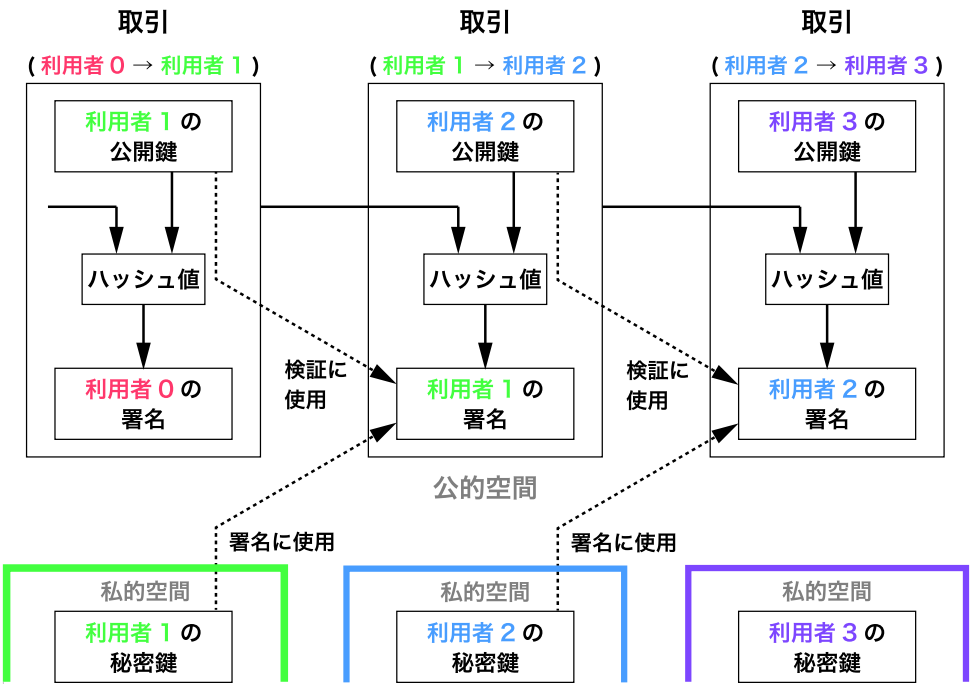


図 1: 署名チェインにより表現された電子コインの取引

### 3.2 取引主体の匿名性

上記のような仕組みであるので、コインの所有者は公開鍵によって識別される (BTC の「送金」に用いられる「アドレス」は、公開鍵のハッシュ値である)。その公開鍵が実際には誰のものであるかを隠し通すことができれば、ビットコインは匿名で使えることになる。

後述するように、ビットコインにおける取引の履歴は、そのすべてがビットコインのネットワーク内で共有されている。ビットコインのネットワークはオープンであるので、誰でもそのデータを取得できることになり、実際に例えば [5] にて閲覧できる。特定の公開鍵が、いつ、どこで[6]、何 BTC を受け取り、あるいは使ったかということが、常に明らかとなるが、このことは高い追跡可能性をもたらす。

一方で、ビットコインは後述するように権威や管理からの自由を指向しているため、匿名性に重きを置いている (この点で目的と設計に乖離が見られる)。そのため、ビットコインでは現在、取引毎に受け手が新たな鍵ペアを生成し使用することを奨励している。後述するように、このことは鍵ペアと人間を分離するため、多くの問題をもたらす。

### 3.3 二重消費 (double spending) への対策

デジタルデータを、言わば貨幣化するためには、所有の表現の他に、もう一工夫が必要である。それは、相手にコインを渡しても、手元にコインのデータのコピーを残しておいて、それを別の相手に対して使うような利用者がいたらどうするか、という「二重消費 (double spending)」の問題に対する対策である。二重消費は、図 1で

[6]取引のデータはブロードキャスト (次の注釈を参照) されるが、その起点となる IP アドレスがもし特定できれば、大まかな地理的位置を推定できる。[5] では、最初に観測された IP アドレスから推測される物理的位置を表示しているが、おそらく不正確だろう。

考えるなら、取引の履歴が分岐することに相当する。分岐した場合でも、ハッシュ値や署名は正しく計算でき、不正な取引が正しいと検証されてしまうため、別途、機構が必要となる。

この二重消費の問題は、電子的な貨幣を設計する際にはつきものであり、ありふれた課題だが、ビットコインではその対策がかなり特殊に見える。

ビットコインでは、全世界でのすべての BTC による取引の順序が一意に定まるように、ビットコインのネットワークに参加するコンピュータの間で合意形成し、二重消費を監視することにしている。取引のデータはネットワーク内にブロードキャスト[7]され、ネットワークに参加するコンピュータ群は、複数の取引をまとめてデータのブロックに格納し、ブロックを時系列に並べていく。このデータ構造をブロックチェインと呼び、全世界で唯一のものをネットワーク内で維持する[8]。すなわち、ネットワークに参加するすべてのコンピュータが、同じブロックチェイン (の部分) のコピーを持つ。ブロックチェイン内の取引はネットワークにより「承認」されていると見なされ、二重消費の場合等、それらに照らして正しく検証できない取引は拒否される。

ビットコインでは、一度承認された取引が改竄されることを困難にするため、ブロックチェインへのブロックの追加にコストを設けている。具体的には、ブロックは数学的な方法で言わば**《採掘》(mining)** されなければならないことになっており、そこに大きな計算パワーが必要になる。《採掘》は競争的プロセスである。

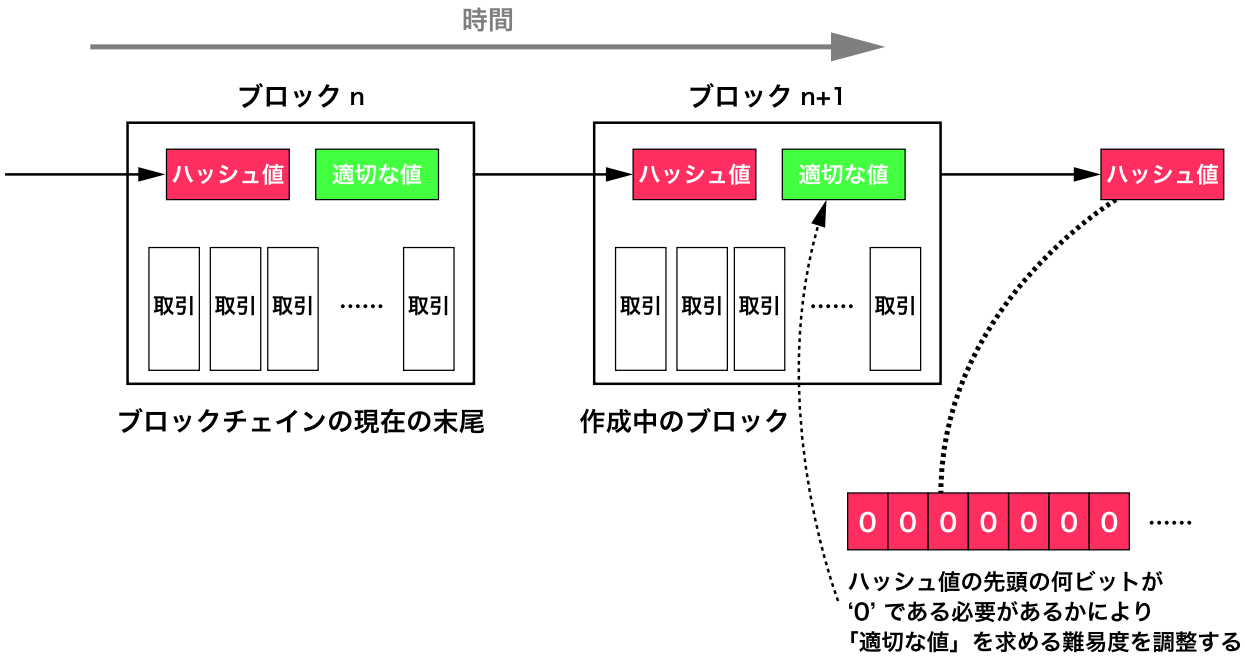


図 2: 二重消費や改竄の防止機構としてのブロックチェイン

図 2に《採掘》の考え方を示した。《採掘》に参加するコンピュータは、それぞれが作成中のブロックに、収集した複数の取引のデータと、チェインの現在の末尾のブロックのハッシュ値 (256bit) を格納する。そして、作成中のブロックに対して同様に暗号学的ハッシュ関数 (SHA-256) を適用した場合のハッシュ値の先頭の $k$ ビット

[7] コンピュータネットワークにおけるブロードキャストとは、ネットワークに参加している近隣のコンピュータに向けてデータのコピーを転送し、中継を重ねることにより、全員にいずれ到達することを期待するという方法である。

[8] 不正な取引データを監視するためには、コイン毎の取引履歴が一意に定まればよいだけであり、全コインの履歴を順序づけることがオーバースペックであることは論をまたない。

がすべて '0' になるように、図中の「適切な値」(32bit) を 0 から順に変化させながら試していく[9]。正しい「適切な値」($2^k$ 回に 1 回の確率で発見できる) が見つかったら[10]、チェインの末尾に追加されるべき新しいブロックとしてブロードキャストする。他のコンピュータは、到着したブロックが正しく作られているかを検証し、正しければ、チェインの新しい末尾として承認する。

$k$ を大きくすると、正しい「適切な値」が見つかるまでの時間が長くなるが、このことにより、参加するコンピュータ群の計算パワーが変化 (典型的には増大) しても、新たなブロックが作られるまでの時間が一定 (10 分) になるようにネットワーク全体で調整する。調整は 2016 個のブロックが生成される毎に行われる。これは、調整が完璧であれば 2 週間ちょうどの間隔になる。したがって、ビットコインの取引が承認されるには、平均して約 10 分の時間がかかることになる。

ビットコインにはネットワーク全体を管理する仕組みは入っていないため、以上のことは競争的かつ協調的なプロセスとして自律的に進行する。そのため、別々のブロックが同時にブロードキャストされたり、ブロードキャストされた取引やブロックが通信の障害や遅延などの理由でネットワークの一部に届かなかったり、到着の順序が前後したりすることで、チェインが分岐する場合も出てくる。その場合、常に最長のチェインが採用されることになっており、ブロックが再計算され、改めて最長のチェインの末尾に追加されていくことで、いずれ問題は収束するとされる。

悪意のある利用者が、二重消費が検出されることを防いだり、その他の理由で取引を偽造したいとしたら、承認済みの取引の内容を改竄しなければならない。そのためには、単に取引のデータを変更するだけではなく、その取引を含むブロックの《採掘》の手続きをやり直さなければならない。ブロックの内容の変更は、そのハッシュ値が変わることを意味するので、そのブロックがチェインの末尾にないとしたら、チェイン上でそのブロックに続く以降のブロック列を、末尾まで《採掘》し直さなければならなくなる。そのことは、ブロックチェインが伸張するにつれ困難になる。

ブロックチェインが健全に保たれるかどうかは、したがって、チェインが正しく伸張していけるかどうかに懸かっている。善意 (システムを健全に保とうとする意思) の計算力が、悪意 (システムを破壊しようとする意思) の計算力を上回っている限り、システムの健全性は維持される[11]。

このように、手続き上の (計算) コストにより悪用を防ぐ方法は、一般に「POW (Proof of Work)」と呼ばれる[12]。ビットコインをはじめ、現在、運用されている多くのデジタル通貨のシステムが POW を採用している。

### 3.4 参加への動機づけとコインの発行

前節で述べた《採掘》の手続きに、多くのコンピュータ (の善意の所有者) が参加しなければ、ビットコインがそもそも成り立たなくなる。しかし、計算には電力が必要になるし、自分のコンピュータの計算資源を割かれることにもなり、そのままでは、あえて参加する動機がない。そこでビットコインでは、ブロックを《採掘》したユーザが、報酬として新たなコインを獲得できる仕組みを採用している。つまり、計算パワーさえあれば、言わ

[9] 0 から順である必要はないが、暗号学的ハッシュ関数の性質上、予めどんな数を入れれば正解かは分からず、また、それぞれが試すブロックのデータは後述する「先頭の取引」が異なるため必ずユニークであり、他の順序で試すメリットがないため、0 から順、あるいは最大の数から逆順に試すのが最も簡単な方法である

[10] 「適切な値」は 32bit だが、現在の $k$ は 32 を超えているため、すべての数を試しても正しい値が見つからないことは実際には頻繁に起きる。その場合、後述する「先頭の取引」のデータ内のフィールドを変更し、再度チャレンジすることになる。

[11] 2013 年 11 月、コーネル大学の研究 [8] がブロックチェインの脆弱性を示唆し、改修したとしても $\frac{1}{4}$ 以上の参加者が共謀すれば乗っ取りが可能との見方を示した。

[12] 日本語では「労働証明」ないし「仕事証明」と呼ばれるべきかも知れないが、ビットコインにおける《採掘》は生産的ではないという意味で「労働」ではないし、日常的な意味での「仕事」でもない (ワット時ないしジュールで測れるという意味では物理学的な「仕事」である)。

ばコインを「掘り出す」ことができることになっているのである。具体的には、ブロックに格納する先頭の取引を、「無」から自分の公開鍵に宛てられた取引 (BTC の生成取引) とすることが許される。

ただし、BTC は総量が決まっており (現行システムでは約 2,100 万 BTC)、全部が「掘り出された」あとは、取引手数料がブロックの《採掘》の報酬となる。

《採掘》の報酬として得られるコインは、2009 年当初は 50BTC だったが、4 年毎に半分になると定められており、本稿を書いている 2013 年 12 月現在では 25BTC となっている。これは、金(きん)などの鉱物資源が、採掘が容易なところから先に掘り出され、徐々に採掘が困難になり、コストが上昇していくことに対応していると考えられる。

このことが示すように、ビットコインは恐らくは金貨をモデルにしており、現代の不換紙幣や、現実の金貨では歴史的に生じた品位 (含有率) の低下等について問題意識を持っていると考えられるが、ビットコインの設計は、後述のように本質的に問題を解決するものではない。

### 3.5 その他の仕組み

ビットコインでは、システムをより実用的にするために、他にも幾つかの興味深いアイデアが採用されている。

ビットコインの設計では、BTC の寿命は永遠であり、秘密鍵の損失等の理由でコインが実質的に無効とならない限り、取引の履歴は伸張し続ける。ネットワーク内でデータが際限なく増え続けることを避けるため、参照されなくなった過去の取引データを適宜、破棄できるようにブロックのデータ構造が工夫されている。

取引自体のデータ構造も、複数枚のコインの同時使用および釣り銭を表現するために工夫されている。ただし、匿名性の観点からは、複数枚のコインを同時に使用すると、それらの所有者を示す公開鍵同士が同じ主体に結びついていることが露見し、追跡がより容易になるという問題が認識されている。

## 4 ビットコインは法貨が生む諸問題を解決するか

### 4.1 ビットコイン誕生の背景

計算機システム・情報システムに詳しい読者なら、「なぜ (Mojo のように) トークンサーバでコインを管理しないのか？」という疑問を抱くかも知れない。確かに、第 3節で示したような、コインの所有の移転や二重消費の問題は、電子的な貨幣をウェブサービスとして提供して、利用者がそのサービスにアカウントを持つようにすれば、なんら困難な問題ではない。暗号学的通貨である必要がないかも知れないし、匿名性を確保したいのであれば、そのための暗号学的な方法も過去に提案・実装された経緯がある [6]。

ビットコインがそうした方法を採っていないのは、そもそも、それが何を目的として作られたか、ということに関係するはずである。

おそらく、サトシ・ナカモトを名乗る計算機科学者とその仲間たちがビットコインを発案するにいたった動機は、現在の貨幣システムのもつ問題を解決したい、という問題意識にあったに違いない。その点は、例えば、地域通貨が生まれた理由と共通していると言える。

そのためには、信条として、中央銀行や市中の銀行、政府といった「信用のある第三者」を介在せずにシステムを成り立たせる必要があり、第 2 の「銀行のようなもの」を生んでしまわないために、サーバにさえ頼らず、すべてが「ピア (対等な相手)」とのやり取りのみで終始するシステムとして作り上げる必要があったのだと思われる。この点でビットコインの基本的な設計は成功していると言える。

しかし、ビットコインの設計の随所に見られるのは、「貨幣は希少でなければならない」といった、貨幣に対するナイーヴな理解である。ただし、ナイーヴな理解、あるいはポピュラーな誤解といったものは、多くの人々に理解されやすく、共有されている認識に他ならず、ビットコインがデジタル通貨として広く信用を得ることができる一因ともなっていると想像できる。このことは、通貨の設計を考える上で示唆に富む。

さて、ビットコインの開発者たちが、実際には現代の貨幣システムの何を問題にしているのかは、ビットコインの設計から逆に推察が可能である。ビットコインの設計上の特徴をまとめると、以下のようになる。

1. プログラムコードによる規制で固定された総量を持ち、デフレーションが組み込まれている。
2. 国家の枠組みに囚われずにグローバルに使える。
3. 「信用のある第三者」を仮定せず、競争によって誰もが獲得できる可能性を持つ。

このことから逆に導かれる、ビットコインの開発者たちが考える現代の貨幣システムの問題は次のようになる。

1. 銀行による信用創造でいわば無尽蔵に増え、インフレーションが組み込まれている。
2. 国家の枠組みによる垣根がある。
3. 経済的な自由が国家や銀行に預けられており、不自由である。

これらは確かに問題かも知れない。しかし、ビットコインの設計におけるこの問題と解決策のセットは、実は、現代の貨幣が生んでいるのと何ら変わらない問題を、もう一度生み出すのに過ぎないと筆者は考える。

### 4.2 ビットコインが助長する諸問題

「グローバルに使え」、そして「競争により万人に開かれている」といったことは、新自由主義/グローバリズムが世界にもたらした諸問題 [38] に目をつぶるのであれば聞こえがよいのかも知れない。また、[42] が指摘するように、権威を嫌う者たちにとっては、国家の枠組みから自由であることを示唆するこれらのことは、魅力的にさえ聞こえるだろう。だが、その背後にある意味は、「**弱者を搾取するための仕組みを持つ**」ことに他ならない。

弱者が、自分も勝者になれるかも知れないという誘惑に乗って国際的な競争の場に駆り出され、その結果、地域の貴重な資本や資源が、国家の垣根を超えて、少数の持てる者たちへとさらに集中していくのが、グローバルな競争を推進することの重要なネガティブな帰結である。

米国ニューヨーク州の地域通貨イサカ・アワーズの創始者であるポール・グローバー氏は、かつてインタビューに答え「...連邦 (訳注: アメリカ合衆国のこと) のドルは街にやってきて何回か人々と握手したかと思うと、この地域を離れ、熱帯雨林から伐採した木材を買ったり、戦争を戦うために使われていく」と述べている [10]。

グローバルに流通するビットコインは、この点においてドルと同じように振る舞うだろう。仮に、ビットコインの開発者たちが、自分たちが稼ぎ、消費した法貨が、例えば戦争や環境破壊に使われることを憂い、それとは別のことに使われることを夢見てビットコインを作ったのだとしたら、それは失敗と言える。

現代の貨幣の大きな問題は、国家の垣根を超えて使いにくいことよりも、むしろ、交換によってその垣根を超え、グローバルな資本として集中しやすいことにあるのではないだろうか。ビットコインは、その問題を助長することはあっても、解決には導かないと筆者は考える。

また、ビットコインにおいては、BTC を希少にするための様々な仕組み (総量の固定や、約 10 分という生成間隔、および生成時の額面の段階的な縮小化) が組み込まれているが、貨幣が希少であることは、問題の解決で

はなく、問題そのものである。ひとりひとりの人にとって、多くの場合、貨幣の一番の問題は、それが必要とされているのに手元にないことだからである。

ビットコインは、その開始当初は《採掘》の競争相手も少なく、利用者らは、法貨に代わる支払いの媒体として BTC を容易に入手できたかも知れない。しかし、競争が激化している現状では、そもそも資本を持たない人たちにとって、入手しやすいものではない。従って、貨幣のこの重大な問題を解決するものでは、もちろんあり得ない。

# 5　人間不在のデジタル通貨

## 5.1　貨幣と信用

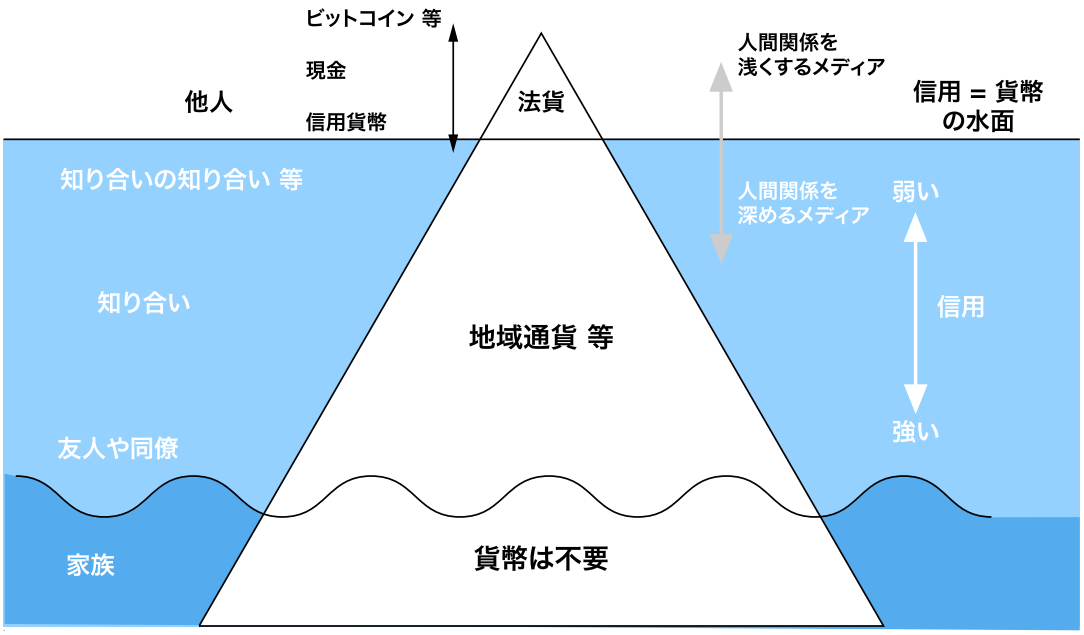


図 3: 貨幣と信用の氷山モデル

ビットコインは、「信用ではなく、暗号学的な証明に基づく支払いシステムをつくる」[15] という宣言の下で開発された。これは、貨幣の在り方に照らして妥当だろうか。経済学者である東京大学の安冨歩教授は、[40] の中で「貨幣はそもそも信頼関係の代替物に過ぎない」と述べている。家族や親しい友人同士のように、信頼で結ばれている人間関係の中では貨幣は不要である。人々は往々にして、「仕事や生活には、信頼関係があっても貨幣がなければ成り立たない局面がある」と考えがちだが、第 2節で見たように、その貨幣も信頼・信用の産物である。したがって、逆に「貨幣 (の物理的な表現型) があっても、信頼・信用がないのであれば (貨幣として) 成り立たない局面がある」と考える方が正しいだろう。

図 3は、さまざまな貨幣と信用との関係を氷山に喩えた図である。[39] で詳しく見ているが、法貨は、それを使う人ではなく、それそのものに信用が置かれるように設計されている。その性質が最もストレートに現れているのが現金であり、買い物において、現金を持ってくれば、持ってきた人の信用は普通、問われない。ビットコインは、プログラムコードによる規制と自動化により、法貨、特に現金のもつその性質を強化したものだと言える。

しかし、法貨は文字通り法によりその通用力が与えられているものであるが、法は、現金の紛失時、拾得時における対応や、盗難時の対応、あるいは、そうした問題を回避するための、現金に代わる小切手等の信用貨幣といったように、現金自体に信用が置かれることの負の面をカバーする、社会的なセキュリティ (安全) の仕組みを同時に規定している。一方、ビットコインには、少なくとも現状はそうしたセキュリティがない。

ビットコインの設計には、表面上、人に対する信用という概念がなく、言わば人間が不在である (深層的には、人々の競争意識や善意に依存している)。二重消費への対策と貨幣の生成を統一した仕組みで行う等、ビットコインの設計には見事と思える点も多いが、最初の前提を取り違えているように思えて仕方がない。

表 1: 人間不在のデジタル通貨 vs. 人間のデジタル通貨

| 人間不在のデジタル通貨 | 人間のデジタル通貨 |
|---|---|
| グローバルなデータ構造を持つ | グローバルなデータ構造を持たない |
| 鍵ペアを個人に帰属させない | 鍵ペアを個人 (または法人) に帰属させる<br>(頻繁な再生成を奨励しない) |
| POW システムを採用する | POW システムを採用しない |
| 貨幣の発行量を制限する | 貨幣の発行量を制限しない |
| 貨幣は同語反復的 | 貨幣が根拠 * を持つようにする<br>(ex. 同語反復しない債務証書) |

* かつ、その根拠が時を経るにつれ減額するようにする。

**人間のデジタル通貨のための提案**　ビットコインが「人間不在のデジタル通貨」だとすれば、その対立概念である「人間のデジタル通貨」は可能だろうか。筆者は、それは十分に可能だと考える。基本的に、「人間のデジタル通貨」を設計するためには、ビットコインとは真逆の提案を行うことになる。そのことをまとめ、表1に示した。

以降の節では、ビットコインが持つ様々な問題の詳細について議論するとともに、その各々について、「人間のデジタル通貨」における対案を示す。

### 5.2　紛失・盗難等への保障の欠如

2013 年、英国で 7 億円相当 (2013 年 11 月末現在) のビットコインのデータが入ったハードディスクをうっかり捨ててしまった男性のニュースがあった [3]。ここには、データ (コインの所有を主張するための秘密鍵) が失われたくらいでコインが使えなくなってしまうという、システムとしての危うさがある。本来であれば、本人性を確認するための社会的な別の手段が用意され、それを注意深く適用した上で、新しく公開鍵と秘密鍵のペアを生成して、所有権をそれと切り替えるといった手続きが可能であって然るべきである。

同じく 2013 年、米国のケーブルテレビの番組で、米ドルで $20 相当のビットコインの秘密鍵をエンコードした QR コードが画面に映ったとたんに盗難に遭うという事件もあった [19]。小切手やトラベラーズチェック等、貨幣に宛先を含めたり、使用時に所有者の署名を必要とすることは、貨幣の盗難による不正利用を防ぐために人間の知恵が生んだ文化である。ビットコインは、手続き上は、そうした文化を引き継いでいるように見えるが、鍵ペアが人間に結びつかないのであれば、その知恵は活かされない。

これらは、鍵ペアが個人と結びついていないことの弊害である。

**人間のデジタル通貨のための提案**　鍵ペアを個人と結びつけることには、権威による管理・追跡の懸念があると思われている節がある。PKI (公開鍵インフラストラクチャ)[28] を前提とすれば、確かにそうかも知れない。

しかし PGP (Pretty Good Privacy)[27] が個人の自由を指向して発案され、使われているように、そのことは必ずしも当てはまらない。PGP では、信用の輪 (web of trust)[31] を用いることにより、権威に依らず、個人の責任において、相手の公開鍵が本人のものであることを確認できる。

筆者が開発した *i*-WAT の実運用では、実際に秘密鍵が紛失される事案が発生している。しかし、*i*-WAT では利用者を公開鍵 (やそのハッシュ値) そのものではなく、PGP の公開鍵ユーザ識別子 (メールアドレス等) で識別しているため、同じユーザ識別子を持つ鍵ペアを再生成し、信用の輪を再構築することで無事に回復している。

識別を、鍵ではなく、人間に対して行うことが、「人間のデジタル通貨」のための提案である。そのことと、プライバシーの議論は独立させて行うことができる。

### 5.3　システムの健全性の維持は誰がどう担うのか

現在、BTC の《採掘》の競争は激化しており、参加するコンピュータ群の中で計算パワーを優位に保てなければ、なかなかコインを得られなくなっている。したがって、他の参加者が計算パワーに投資するなら、自分はもっと投資しなければならなくなり、その競争の行き着く末に、遂に高性能で低消費電力な BTC《採掘》専用マシンが誕生した[13]。他の何の用途にも使えず、ただ純粋にハッシュ値を繰り返し求めることで新たなブロックを生成し、BTC を作り出すだけのことに電力を消費するコンピュータである。いかに低消費電力化が進行しているとは言え、ビットコインのシステムを維持するためだけに、社会的に見て多大な非生産的活動が行われているという点は否めない[14]。

ここで、《採掘》はそもそも必要なのかという疑問を提起したい。

ビットコインにおける《採掘》は、不正に対する POW システムと、BTC の生成ペースの制御のふたつの意味を兼ねる。そして、その前提として、グローバルなデータ構造であるブロックチェインがある。

不正行為を監視したいだけであれば、全世界の取引を一意な順序で並べる必要はなく、各コインについて取引系列が一意に定まればよい。分散ハッシュテーブル等の既知の方法を用いれば、そのことを管理主体を置かない分散データ構造として実現することは可能である。ビットコインにおいて、そうなっていないのは、安全性の面でも問題と考えられ、[8] が示唆したように、ブロックチェインへの攻撃が必ずシステム全体への攻撃になる。すなわち、攻撃が成功すれば、全世界のビットコイン利用者全員が被害を被りうる。

また、取引にはデジタル署名を施してあり、否認が不可能であるのだから、不正があった場合、本来は署名者を追及できるはずである。そのためには公開鍵から特定の主体を参照できなければならないが、ビットコインでは鍵ペアを人間と切り離しているため、それができない。そのため、本来は追及可能性をもって不正を抑止できるところを、POW によって力技で抑止していると考えることができる。ここにも、人間不在であるビットコインの設計の弊害がある。

より本質的には、ビットコインにおいては、二重消費をはじめとする、BTC を見かけ上増量させる不正行為が誰にとって不利益となるかが明らかでない。アンフェアであることはわかるが、それがシステム全体の挙動に

[13] 計算機システムの高速・低消費電力化に興味のある向きには、GPGPU (General-Purpose computing on GPU) → FPGA (Field-Programmable Gate Array) → ASIC (Application-Specific IC) という流れで進んできたことを特に書き記しておく。

[14] この点に関し、ビットコインの開発者らは、法貨のシステムの維持のためにも多くの人間たちが働き、多大なエネルギーが消費されている (対してビットコインは自動化されている) と反論している。それは確かにそうであり、貨幣システムの (省人員化を含む) 省エネルギー化は追究されるべきだろう。だが、であるのなら、《採掘》を不要にするシステム設計も当然、追究されて然るべきではないだろうか。

どう影響し、自らがどんな具体的被害を被るかを利用者は簡単には判断できない。だからこそ、全体がその抑止コストを共有しているとも言える。

アンフェアな利用者に対するコストを全体が共有する状態だということは、「共有地の悲劇 (tragedy of the commons)」[12] のための舞台が用意されてしまっていることを示しており、[8] が示唆するように、参加者が善意や惰性よりも合理性を追求し出したとたんに、全体が破綻しうることを意味している。

**人間のデジタル通貨のための提案**　仮に電子コインが信用貨幣であれば、すなわち何らかの債務証書であるならば、二重消費は債務が倍増することを意味する。したがって、貨幣が増量するような不正が行われた場合に不利益を被るのは発行者であり、発行者にその抑止コストを負担する理由がある。また、貨幣を無軌道に発行すると、それだけ発行者の負債が増えるので、貨幣の発行量は自律的に制御されることになる。

もちろん、貨幣の発行が適切かどうか (履行できる債務の範囲に収まっているか) を周囲が監視する機構は必要であり、そのために、発行された/発行されつつある貨幣に関わる範囲内で取引の履歴が局所的に共有されることには意味がある。また、発行者が死亡/逃亡したり、あるいは他の理由により債務を履行できなくなった際に、どう対応するかというセキュリティの設計も必要である。ただし、債務の不履行の影響は局所的に留まる。

*i*-WAT は以上のことを考慮して設計されているシステムの例である。

責任が宙吊りにならず、サボタージュが、どんなに大規模なものであっても、システム全体を停止させるに至らないような設計を行うことが、「人間のデジタル通貨」のための提案である。

### 5.4　3 層のギャンブル構造

筆者は、ビットコインの設計に潜むグローバリズムへの信奉には、実は根深いものがあるのではないかと疑っている。グローバリズムが発するメッセージは「世界には唯一の正しい生き方がある」というものだと思うが、ビットコインの設計の中核にあるのは、「世界には唯一の正しい取引履歴がある」ことを実現し、維持することだからである。

現在、その中核に沿って、地域の垣根を超えた競争が繰り広げられている。BTC の《採掘》に向けられる人々の熱意は、ゴールドラッシュに喩えられることもある。しかし、金(きん)が鉱物資源でもあり、それ自体が何かの素材として使われ、人類にとって価値があるものなのに対して、ビットコインのブロックや BTC は、単なるデジタルデータであり、数字列であって、それが何であるかの「決まりごと」、いわばゲームのルールによって意味づけられているものに過ぎない。

このように、客観的に見て、無意味な行為に見えるのに、自分が勝つことの幻影に打ち克つことができず、それに熱中する行為は、ギャンブルによく似ている (それなら現代の貨幣経済も同じではないか、と読者が思うなら、筆者と問題意識を共有している)。ただ、これを個人の問題に帰結させるのは酷であり、こういうものこそ、社会が協力してその構造を明らかにして、無自覚に巻き込まれる人々が出ないようにする必要があると筆者は考える。

ビットコインは、したがって、全体がギャンブルの構造を持つと思うが、そのギャンブル性は 3 つの層を持っていると考えられる。

1. グローバリズムというギャンブルへの加担
2. 投機というギャンブルの助長
3. 《採掘》というギャンブルの構造

まず、グローバリズムは、それ自体が弱者が勝者になることを夢見るギャンブルによって成り立っていると言える。グローバルな通貨を標榜するビットコインは、その構造に加担している。

次に、ビットコインは BTC の価格が高騰していることで、現在、話題になっているわけだが、その仕組み自体に投機的な興味を助長させる部分がある。それは、BTC の総量が予め決まっており、すべてのコインが「掘り出された」あとも (あるいは、《採掘》による生成率が低下し、市場に新たな BTC が供給されにくくなっても) ビットコインの経済圏が拡大することを期待するとすれば、デフレーションが継続して起きなければならないという点である。つまり、同量の BTC でも、より多くの財やサービスと交換できるように、BTC の価値が上がりつづけなければならない。貨幣の価値が上がることが期待される場合、人はそれをあえて今、交換の媒体としては使わず、投資の対象とする。したがって、ビットコインがこれから普及することを期待する人ほど、それを実際には使わない、ということになるが、それはもはや普通の意味では通貨でも貨幣でもあり得ない。

最後に、ビットコインの《採掘》自体がギャンブルの構造を持っていることは、あまり気づかれていないかも知れない。

ギャンブルは、「金銭や品物などの財物を賭けて偶然性の要素が含まれる勝負を行い、その勝負の結果によって賭けた財物のやりとりをおこなう行為」と定義される (広辞苑)。何であれ活動にはコストがかかる (賭けているものがある) ので、それはさておいて、ここで重要なのは「偶然性」によりアウトプットが得られるという部分である。この部分が人を夢中にさせることが、さまざまな方面から指摘されている [18, 34]。例えばそれは、双六がなぜ面白いか、ルーレットやスロットマシンがなぜ面白いか、ということに関わってくる。

ビットコインにおけるブロックの《採掘》では、大きな電力と計算パワーを賭けたとしても、アウトプットが得られるのは (=正しいハッシュ値が得られるのは) 確率的である。おそらく、ビットコインの《採掘》に励む人々は、ギャンブルに興じているときのような高揚感を感じていると筆者は想像する。

**人間のデジタル通貨のための提案**　上記のようなギャンブルの構造を通して、ビットコインは (そして法貨も)、他の商品に対して絶対的な優位性を持つものとしての貨幣を集めることに人々を夢中にさせている。

「人間のデジタル通貨」のためには、法貨やビットコインが持つ絶対的な優位性から、貨幣の地位を一般の商品のレベルに押し下げ、「信頼関係の代替物」としての適正な地位に回帰させる必要がある。そのためには、デフレーション傾向を持つのではなく、一般の商品と同様、貨幣の価値が減少していく仕組みを採用するのがよいかも知れない。*i*-WAT では、そのような仕組みを実験し、標準システムの中に組み入れている。

「人間のデジタル通貨」では、人と人の間の、より強い信用に向けて、通貨の役割が次第に縮小していき、新しい人間関係の形成の中で限定的に使われていくような世界を目指したい。そのことが、貨幣に由来する諸々の社会的課題の解決に寄与すると信じている。

## 6　おわりに

筆者は、当初、ビットコインは貝殻貨幣 [30] のようなものだと考えていた。貨幣として使われる貝殻自体に、何かの価値があるわけではない。そしてそれは、そうしようと思えば拾ってくることができる。その性質は、ビットコインとまったく同じに見えた。

現在、筆者は、ビットコインはむしろ巨石貨幣 [29] と似ていると考えている。巨大な石の貨幣が価値を持つ (それでものが買える) のは、離れた島で石を切り出してカヌーで運んできたという苦行の物語があって、それがコミュニティの中で共有されるからである。ビットコインでも、計算機資源を投入してブロックを《採掘》したという物語が共有されることで、コインは価値を持つ (それでものが買える — 現状、ものを買うのに使う人は少数

派かも知れないが)。どちらも物語の核となる行いは実体経済の目から見て決して生産的ではない。また、巨石貨幣は持ち運ばず、所有権の移動のみが石に刻まれていくが、BTC もネットワーク上に存在し続け、所有権の移動のみがブロックチェインに刻まれていく。

筆者は、貝殻貨幣や巨石貨幣が悪いとは思わない。自然の恵みにあふれた社会の中でなら、それらはうまく使われていくだろう。しかし、貨幣が絶対的な優位性をもち、それを基準としてものごとを判断することが「世界での唯一の正しい生き方」として推進されているような、私たちの現代の社会の中に、貝殻貨幣や巨石貨幣を投入したら、どうなるだろうか。私たちは、その行く末を今、目撃しつつあるのかも知れない。

ビットコインは、「信用ではなく、暗号学的な証明に基づく支払いシステムをつくる」という宣言の下で開発された。しかし、それもまたひとつの物語である。そして、その物語への信用なくしては、それが貨幣として機能することはあり得ない。にもかかわらず、あたかもそのことに無自覚であるかのように、「人間の信用」に関わる仕組みをビットコインは持たない。このことから、ビットコインが「人を信じていない」という点が仇となる事件が今後も起きうる危険性があると筆者は考える。社会的な「セキュリティ」の必要性に応えず、暗号学的なセキュリティに終始しているビットコインは、社会を支えるインフラとしては、かなり未熟な段階にあると言えるだろう。

ただし、中央に依存しない貨幣システムを独自に実現させ、さらには大勢の人々を巻き込み、オルタナティヴな貨幣としてのムーブメントを興したことについては、筆者はビットコインの作者らを尊敬する。また、法貨の絶対的な地位に対してオルタナティヴを示せたという意味で、今後、起こり得る変化の予兆としての意義は大きいと考える。

本稿の執筆を通して、筆者は自身の研究成果を改めて「人間のデジタル通貨」として見直す機会を得た。筆者には、そのより高度な実現と普及に向けた責務があると考える。知っていて事を為さないほど無責任なことはないからである。ビットコインやその亜種から学べるところは学び、現代の世界の多くの問題の根源にある、貨幣の問題を解決するべく、これからも努力を続けたい。

## 参考文献


[1] AZI. Mojo Nation technology overview. Online archive. Available electronically at http://web.archive.org/web/20020127125928/ www.mojonation.net/docs/technical_overview.shtml.

[2] BBC. Virtual cash exchange becomes bank, 2012. Hypertext document. Available electronically at http://www.bbc.co.uk/news/technology-20641465.

[3] BBC. James howells searches for hard drive with £4m-worth of bitcoins stored, 2013. Hypertext document. Available electronically at http://www.bbc.co.uk/news/uk-wales-south-east-wales-25134289.

[4] Bitcoin Project. Bitcoin - Open source P2P money, as of 2013. Hypertext document. Available electronically at http://bitcoin.org.

[5] Blockchain.info. Bitcoin Block Explorer - Blockchain.info, as of 2013. Hypertext document. Available electronically at http://blockchain.info.

[6] David Chaum. Blind signatures for untraceable payments. In *Advances in Cryptology – Crypto '82*. Springer-Verlag, 1983.

[7] Landon Cox and Brian Noble. Samsara: Honor among thieves in peer-to-peer storage. In *Proceedings of the ACM Symposium on Operating Systems Principles*, October 2003.

[8] Ittay Eyal and Emin Gün Sirer. Majority is not enough: Bitcoin mining is vulnerable, 2013. Hypertext document. Available electronically at http://arxiv.org/pdf/1311.0243v2.pdf.

[9] Ryan Fugger. Money as IOUs in social trust networks & a proposal for a decentralized currency network protocol. Hypertext document. Available electronically at http://ripple.sourceforge.net/.

[10] Paul Glover. Creating community economics with local currency, as of 2013. Available electronically at http://www.paulglover.org/hourintro.html.

[11] Guardian News and Media Limited. Bitcoin now 'unit of account' in Germany, 2013. Hypertext document. Available electronically at http://www.theguardian.com/technology/2013/aug/19/bitcoin-unit-of-account-germany.

[12] Garrett Hardin. The tragedy of the commons. *Science*, Vol. 162, , 1968.

[13] Litecoin Project. Litecoin - Open source P2P digital currency, as of 2013. Hypertext document. Available electronically at https://litecoin.org.

[14] Stephen Mihm. Are bitcoins the criminal's best friend?, 2013. Hypertext document. Available electronically at http://www.bloomberg.com/news/2013-11-18/are-bitcoins-the-criminal-s-best-friend-.html.

[15] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. Available electronically at http://bitcoin.org/bitcoin.pdf.

[16] Open Source Initiative. The MIT License (MIT), as of 2013. Hypertext document. Available electronically at http://opensource.org/licenses/mit-license.php.

[17] Jackson Palmer and Shibetoshi Nakamoto. Dogecoin, as of 2013. Hypertext document. Available electronically at https://litecoin.org.

[18] Daniel Quinn. *The Story of B.* Bantam, 1996.

[19] Sam Ro. A bloomberg tv host gifted bitcoin on air and it immediately got stolen, 2013. Hypertext document. Available electronically at http://www.businessinsider.com/bloomberg-matt-miller-bitcoin-gift-stolen-2013-12.

[20] Kenji Saito. Peer-to-peer money: Free currency over the Internet. In *Proceedings of the Second International Conference on Human.Society@Internet (HSI 2003), Lecture Notes in Computer Science 2713.* Springer-Verlag, June 2003.

[21] Kenji Saito. *i-WAT: The Internet WAT System – An Architecture for Maintaining Trust and Facilitating Peer-to-Peer Barter Relationships –.* PhD thesis, Graduate School of Media and Governance, Keio University, February 2006.

[22] Kenji Saito and Eiichi Morino. Local production, local consumption storage economics for peer-to-peer systems. In *Proceedings of 2008 International Symposium on Applications and the Internet (SAINT 2008) Workshops*, July 2008.

[23] Vivek Vishnumurthy, Sangeeth Chandrakumar, and Emin Gun Sirer. KARMA: A secure economic framework for p2p resource sharing. In *Proceedings of the Workshop on the Economics of Peer-to-Peer Systems*, June 2003.

[24] Wikipedia contributors. Digital currency - Wikipedia, the free encyclopedia, as of 2013. Available electronically at http://en.wikipedia.org/wiki/Digital_currency.

[25] Wikipedia contributors. Digital signature - Wikipedia, the free encyclopedia, as of 2013. Available electronically at http://en.wikipedia.org/wiki/Digital_signature.

[26] Wikipedia contributors. Local currency - Wikipedia, the free encyclopedia, as of 2013. Available electronically at http://en.wikipedia.org/wiki/Local_currency.

[27] Wikipedia contributors. Pretty Good Privacy - Wikipedia, the free encyclopedia, as of 2013. Available electronically at http://en.wikipedia.org/wiki/Pretty_Good_Privacy.

[28] Wikipedia contributors. Public-key infrastructure - Wikipedia, the free encyclopedia, as of 2013. Available electronically at http://en.wikipedia.org/wiki/Public-key_infrastructure.

[29] Wikipedia contributors. Rai stones - Wikipedia, the free encyclopedia, as of 2013. Available electronically at http://en.wikipedia.org/wiki/Rai_stones.

[30] Wikipedia contributors. Shell money - Wikipedia, the free encyclopedia, as of 2013. Available electronically at http://en.wikipedia.org/wiki/Shell_money.

[31] Wikipedia contributors. Web of trust - Wikipedia, the free encyclopedia, as of 2013. Available electronically at hhttp://en.wikipedia.org/wiki/Web_of_trust.

[32] Beverly Yang and Hector Garcia-Molina. PPay: micropayments for peer-to-peer systems. In *Proceedings of the 10th ACM conference on Computer and communications security (CCS '03)*, October 2003.

[33] 岩井克人. 貨幣論. 筑摩書房, 1993.

[34] 内田樹, 中沢新一. 日本の文脈. 角川書店, 2012.

[35] 小林慶一郎. 「ゲーデルの貨幣」-自由と文明の未来- 危機編　第十二回「貨幣論の本質とは何か」. 一般社団法人 金融財政事情研究会, 2009. 『週刊金融財政事情』 2009 年 11 月 2 日号に掲載, http://www.canon-igs.org/column/macroeconomics/20091111_198.html.

[36] 斉藤賢爾. 不思議の国の NEO — 未来を変えたお金の話. 太郎次郎社エディタス, 2009.

[37] 斉藤賢爾, 高野祐輝. 現実世界の条件に適応する分散ハッシュテーブル. 電子情報通信学会論文誌, Vol. J96-D, No. 6, pp. 1433–1446, 2013.

[38] 中山智香子. 経済ジェノサイド: フリードマンと世界経済の半世紀. 平凡社 (新書), 2013.

[39] 森野榮一, 斉藤賢爾. ぼくらのおカネをつくろうよ (上・下). ぱる出版, 2011-2012. 自由経済研究第 36・37 号に掲載.

[40] 安冨歩. 生きる技法. 青灯社, 2011.

[41] 吉本隆明. 共同幻想論. 河出書房新社, 1968. 角川書店より改訂新版発行 (1982).

[42] 日本経済新聞. ビットコイン、ギークが育てた無国籍通貨, 2013. Hypertext document. Available electronically at http://www.nikkei.com/money/features/32.aspx?g=DGXNMSFK1803U_18122013000000.