踊るバズワード ～Behind the Buzzword（8）ブロックチェーン（2）：

ビットコインの運命 ～異常な価値上昇を求められる“半減期”

https://eetimes.jp/ee/articles/2011/27/news046.html

「ブロックチェーン」を理解するために「ビットコイン」の解説を続けます。今回の前半はビットコインの“信用”について取り上げます。後半は、ビットコインに組み込まれている「半減期」という仕組みを解説します。これは、“旗取りゲーム”による賞金が、約4年単位で半分になること。ここに人間の力が介在する余地はなく、言ってみればビットコインの“逃れられない運命”なのです。

2020年11月27日 11時30分 更新

[江端智一, EE Times Japan]

「業界のトレンド」といわれる技術の名称は、“バズワード”になることが少なくありません。“M2M”“ユビキタス”“Web2.0”、そして“AI”。理解不能な技術が登場すると、それに“もっともらしい名前”を付けて分かったフリをするのです。このように作られた名前に世界は踊り、私たち技術者を翻弄した揚げ句、最後は無責任に捨て去りました――ひと言の謝罪もなく。今ここに、かつて「“AI”という技術は存在しない」と2年間叫び続けた著者が再び立ち上がります。あなたの「分かったフリ」を冷酷に問い詰め、糾弾するためです。⇒連載バックナンバー

紙幣の価値は、がっつり信じてるよね？

「ねえ、マスター……私もう、世の中の何もかもが、信じられないわ……」

4杯目のボルドーのメルロのグラスを空けて、彼女はカウンターに俯しながら呟いた。しばらくして、顔だけを上げて、上目づかいに5杯目をマスターにねだるが、マスターはそんな彼女を無視して、グラスを拭き続ける。

彼女は、溜息を一つつき、髪を上げながら、いつもより1枚だけ多い紙幣をカウンターに置いて、立ち上がった。最初の2～3歩、足元がおぼつかない感じではあったが、それでも、背筋を伸ばして、ドアに向かって歩き出した。

―― と、ここまで読んで、私は思いました。

「世の中の何もかもが、信じられない」と言っていたけど、彼女、**「テーブルに置いた紙幣の価値」だけは、ガッツリ信じているよね？**

と。

バーのカウンター置かれた紙幣は、つまるところ「紙切れ」に過ぎませんが、それでも、バーのカウンターで出される、ボルドー産のメルロー、グラス数杯分の価値に相当する「信用」はあるのです。

私たちは日常の中で、恋愛、友情、家族、仕事、いろいろなものを信用して生きていますが、多分、貨幣ほどは信用していないと思います ―― 私たちは、かなり高い頻度で、愛していた恋人に裏切られ、長年連れそってきた伴侶からは離婚を切り出され、人生をささげてきた会社からは辞令1枚で出向させられます。

これに対して、貨幣に信用は、比較にならないほど高い ―― これは、貨幣の価値を守る者たちの「**日々の闘い**」と、そして、貨幣（日本円）の価値を何の疑いもなく信じ続ける私たちの「**貨幣信仰**」のコラボによる奇跡です。

少なくとも、世の中の「全て」に絶望しカウンターで酔い潰れている女性が、その「全て」の「枠外」にしてしまうほど、通貨には**絶対的な信用が化体している**のです。

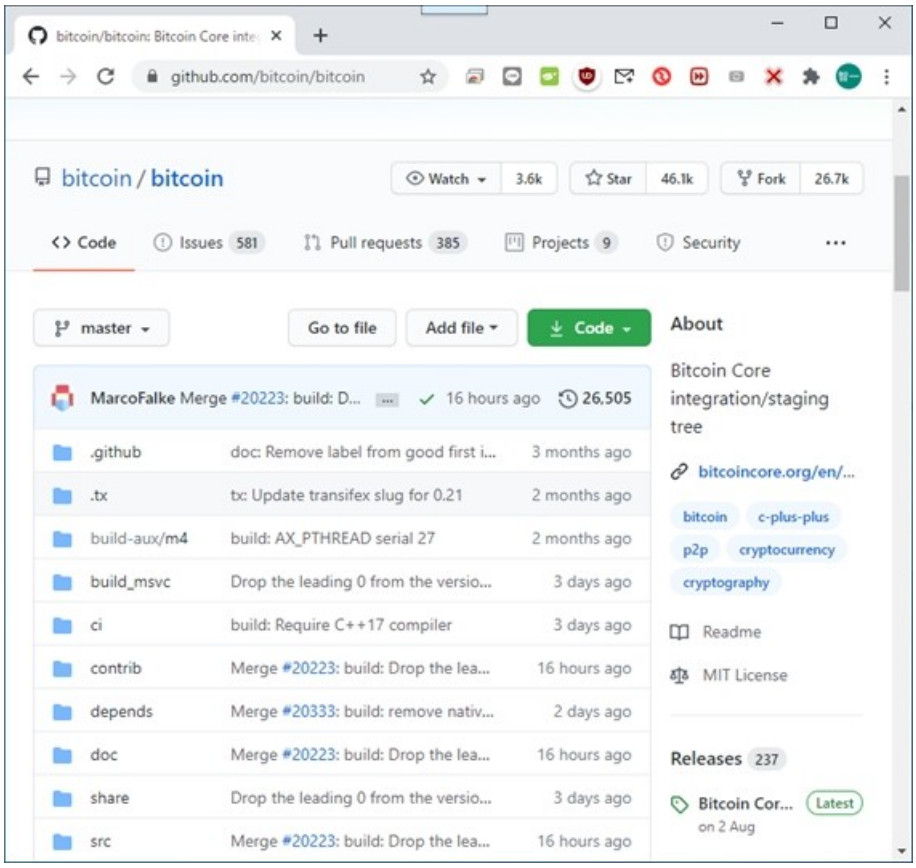
「エバコイン」も作れそうだ

私、この連載の開始時から、ビットコインのプログラム（ソースコード）を調べています。

ビットコインは、国の定めた造幣局や印刷局で製造される訳ではありません。電気料金の安い中国（大陸）奥地のマイニング（発掘）向上でなくても、あなたのパソコンで作り出すことができますし、あなたが使うこともできます（「ビットコインの正体 ～電力と計算資源を消費するだけの“旗取りゲーム”」を参照）。

ビットコインのソースコード（アルゴリズム）は100%無償で公開されています。これは、造幣局や印刷局で秘匿されている、超高度の造幣技術や印刷技術と同じようなモノが、100%余すところなく公開されていて、**誰もが誰の許可も必要とすることなく、勝手にビットコインを作ることができる**、ということです。

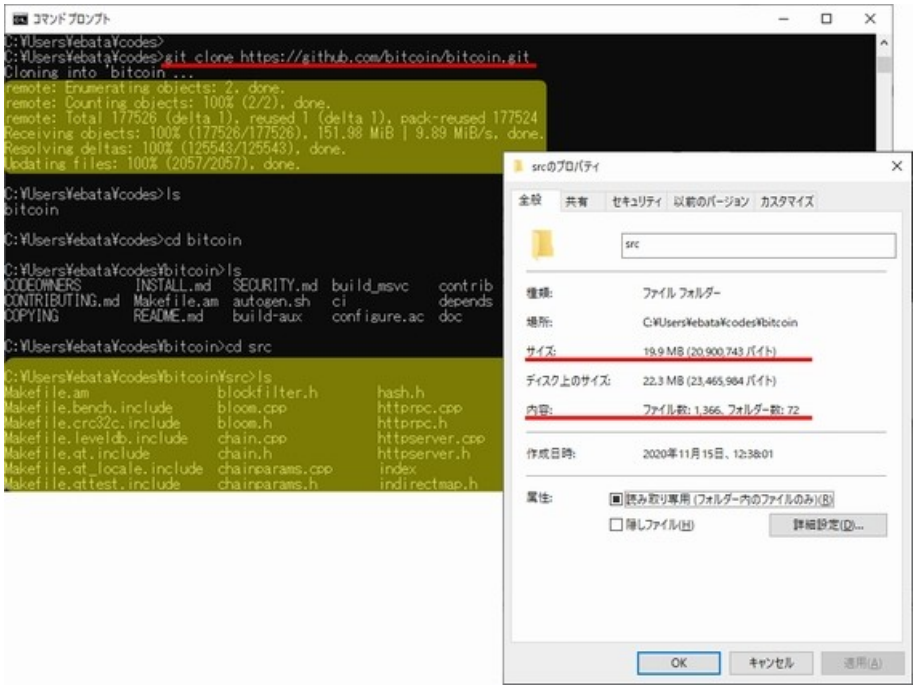
このソースコードは簡単に入手できます。こちらのサイトからダウンロードできます。



または、コマンドプロンプト（又は、適当なシェル）から

> git clone https://github.com/bitcoin/bitcoin.git

と入力するだけで、ソースコードが、自動的にあなたのPCにダウンロードされてきます。



ソースコードは、”src”のディレクトリに格納されています。使用されているコンピュータ言語は、私の十八番であるC/C++が全体の75%、pythonが20%弱、ソースコードのフォルダ数72、ファイル数が1366、全部のソースコードは69,617ステップでした。

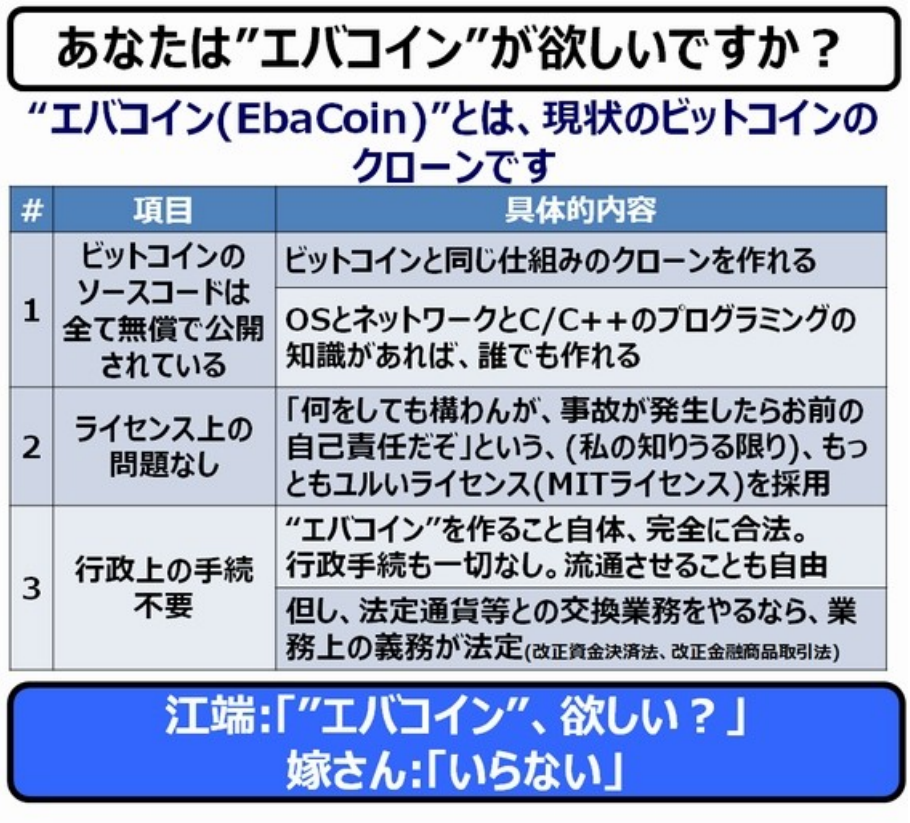
私がこれまで、単体のプログラムとして、スクラッチから自作したソースコードは、最大10K（10,000）ステップ程度でしたので、このビットコインのソースコードを稼働させるだけなら、私でもなんとかなると思いました。（実際、先日、私は139,464ステップのコードの移植を完了したところです*）。

*）ただし、改造した部分は、200ステップにも至りませんが（筆者のブログ）。

うん、これなら作れそうだな ―― 「エバコイン（EbaCoin）」

これは、たとえではなく、完全に同一のビットコインを、私が作り出して、それを運用することが可能であるということです。それでは、ここでは、このビットコインと完全に同じ仕組みであるクローンである、**江端が作成／運用／管理する通貨を「エバコイン」**と呼ぶことにします。

そして、私は嫁さんに尋ねてみました ―― **私がエバコインを作ったら、それ欲しい？** と。



なぜ、嫁さんは（そして、間違いなくあなたも）「**エバコインなんかいらない**」と即答したのか。そして、ビットコインとエバコインは何が違うのか？ ―― 繰り返しますが、エバコインはビットコインのクローンです。送金に使えるし、コストも安く上げられるし、マイニングの仕組みも全く同じです。

ビットコインは、2009年からの商用からのオペレーションのノウハウ（サービス窓口、ネットインタフェース、ノウハウ、トラブルシューティング）が蓄積されていますが、エバコインであったとしても、これからビットコインと同じような運用への投資と経験を重ねることによって、いずれは同じレベルにたどりつくことは（論理上）可能です。

結論から言えば、ビットコインとエバコインの「通貨としての性質／性能の違い」ではなく、ビットコインという **名称に化体したネームバリュー（ブランド）** が違うからです。

さらにダメ押しなのは、**法定通貨との交換の可否** でしょう。エバコインは、金融庁に対しての手続を行い、認可を得なければ、円やドルとの交換はできません（逆に言えば、それ相応の実績を作れば、できないことはないのです）。

なるほど ―― ビットコインとエバコインの根本的な違いは、「ブランド」と「法定通貨との交換」の2つであると。これはもっともな話です。

しかし、同時に、これは奇妙な話です。

ビットコインが、それ自体に価値があるのであれば、法定通貨との交換などは「さまつな話」になるはずです。ビットコインがインターネットの世界で信用を得て、流通が可能であるなら、それだけで十分であるはずです。

なのに、なぜ、ビットコインが、いつも法定通貨の価格との交換レートとともに表示される必要があるのでしょうか。

現在、世界中で確認されている、ビットコインのような仮想通貨は、1000種以上もあります。これらの仮想通貨間での交換ができるのであれば、**法定通貨に依拠しなくても**、世界中どこにいっても不便のない世界共通通貨として通用するハズです。

―― ビットコインの暴落や高とうが、法定通貨との換金比率で語られること自体、おかしい

他の仮想通貨とのレートか、あるいは現存しているインターネット上のサービス商品（例えば、Amazon Web

Service（AWS）等）への値付け等で比較されるなら分かりますが……**そんな風に考えてしまうのは、私だけなのでしょうか？** ーー どうも、そうでもないようです（後述）。

「信用」こそが最大の価値

　こんにちは、江端智一です。

　今回は、「踊るバズワード ～Behind the Buzzword」の「ブロックチェーン」シリーズの第2回です。

　本来、ブロックチェーンの技術的な話から、バズワード批判を行うのが、この連載の目的なのですが、今回もまた、前回に引き続いて、ブロックチェーン技術のベースとなったビットコインについて、多くのページを使わせて頂く予定です。

　実は、ブロックチェーンも、ビットコインも、そして通貨も、目指しているのは「信用」です。”1”と”0”だけからなるビット列の通信や無体物を取り扱うインターネットの世界においては、**「信用」こそが最大の価値があるもの** なのです。

　身近な例で言えば、指1本でコピペが作れる電子情報財（単に”デジ絵（デジタル絵画）”でいい）のオリジナルを、どうやって証明するか、です。これを仮想通貨にあてはめれば、「コピペで無限の複製が可能な仮想通貨の**最初の1枚**をどうやって証明するか、いかにして世界に納得させるか」ということです。

　しかし、貨幣における「信用」とは、そのような「最初の一枚」の「信用」とは、全く違った「信用」なのです。

　今回は、このお話をさせてください。

なぜ「エバコイン」は、うさんくさいのか

　さて、冒頭の、「エバコインは信用できない」の話に戻ります ーー ウザいかもしれませんが、ちょっと我慢してお付き合いください。

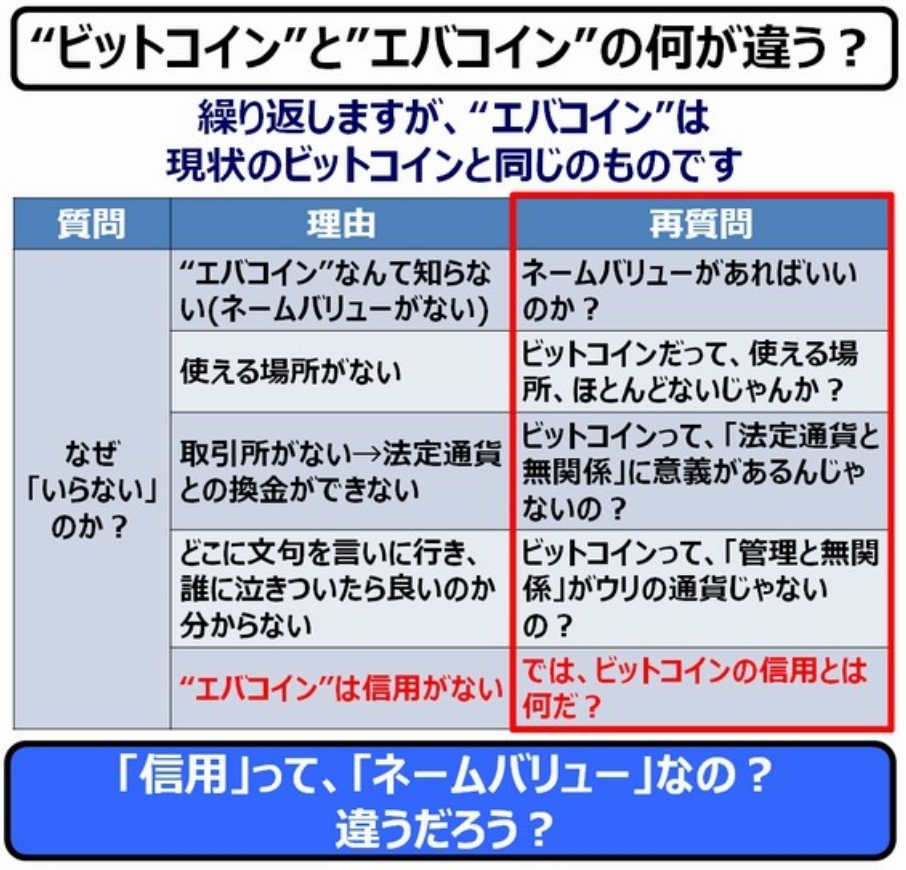
　「ビットコイン」は、最初から今の「ビットコイン」として存在した訳ではありません。「ビットコイン」は、10年の月日を経て、「今のビットコイン」になっていったのです。

　「エバコイン」が「うさんくさい」のは当然ですが、忘れないでいただきたいのは **「エバコイン」は「ビットコイン」の初期状態である** ーー つまり、ビットコインも「うさんくさい」からスタートしたのだということです。

　ちなみに私、今回、ビットコインの論文を一通り読みました。この論文にPoW（プルーフ・オブ・ワーク）（前回ご参照）の話が登場してこないこととか、それがブログの方で展開されているとか ーー なんというか、フィールド系の「研究者」や「開発者」としての、同じニオイを感じました。

　「うさんくさい」のではなくて、そもそもビットコインの論文の目的は、**アカデミズムやエンジニアからなる小規模な世界でのPoC（Proof of Concept: 検証のために行う社会実証実験）が目的だったのではないか**、と思えるのです（後述します）。

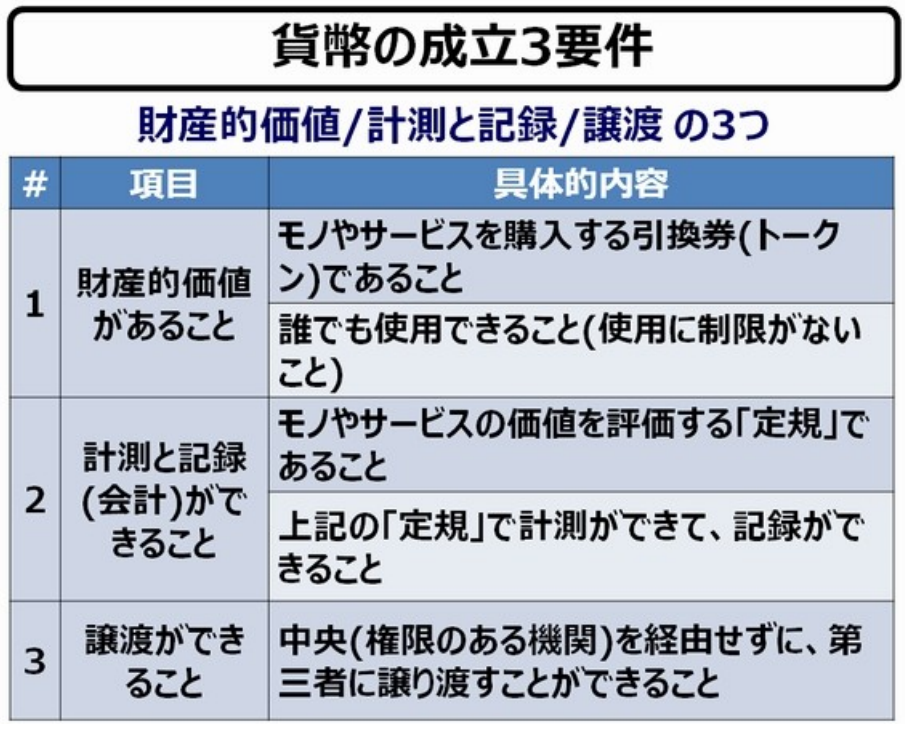
　下記の表は、エバコインを頭の中で鋳造/印刷することで、「エバコイン（=初期のビットコイン）」が、どうして「うさんくさいか」を記載したものです。



引っくり返せば、上記の「エバコイン」の問題点こそが、「信用」の混乱の源（みなもと）になっているということです。

そもそも「貨幣」とは？

まず、「貨幣」とは何かという、超基本的なお話から始めたいと思います。



貨幣とは、まあ、レンタカーのようなものとして把握しても良いと思います。

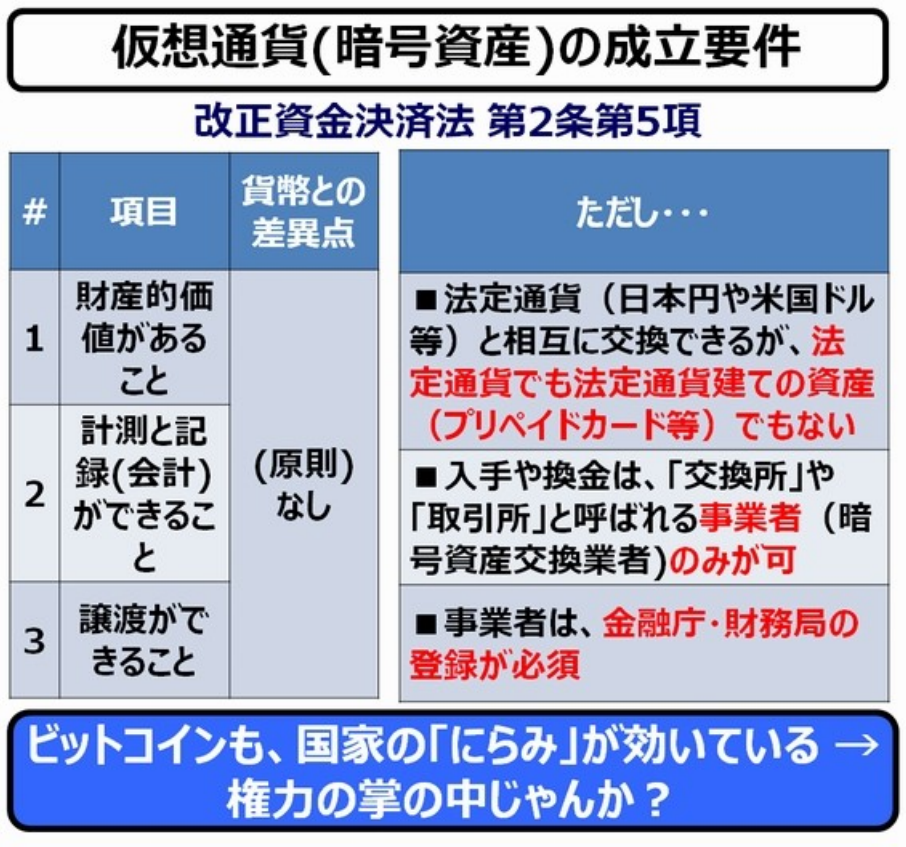
（1）誰でも利用可能な「財産的価値」という荷物を乗せる自動車（ビークル）であり、
（2）走行距離を単一の単位（km）で測定でき、
（3）双方の合意だけで、所有者を換えることができる

という3つの条件がそろえば、成立します。

　で、この通貨の3定義に対して、いわゆるビットコインなどの仮想通貨がどうなっているかというと、**立派に貨幣の条件を満たしています**[*)]。

*）実は、最近の法改正によって、「仮想通貨（Virtual Currency）」は、国際的に共通の名称として、「暗号資産（Crypto Asset）」と名称変更されています。これは、日本円やドルなどの法定通貨との混同を回避することが目的なようです。本連載内では、「仮想通貨」で統一することとします。

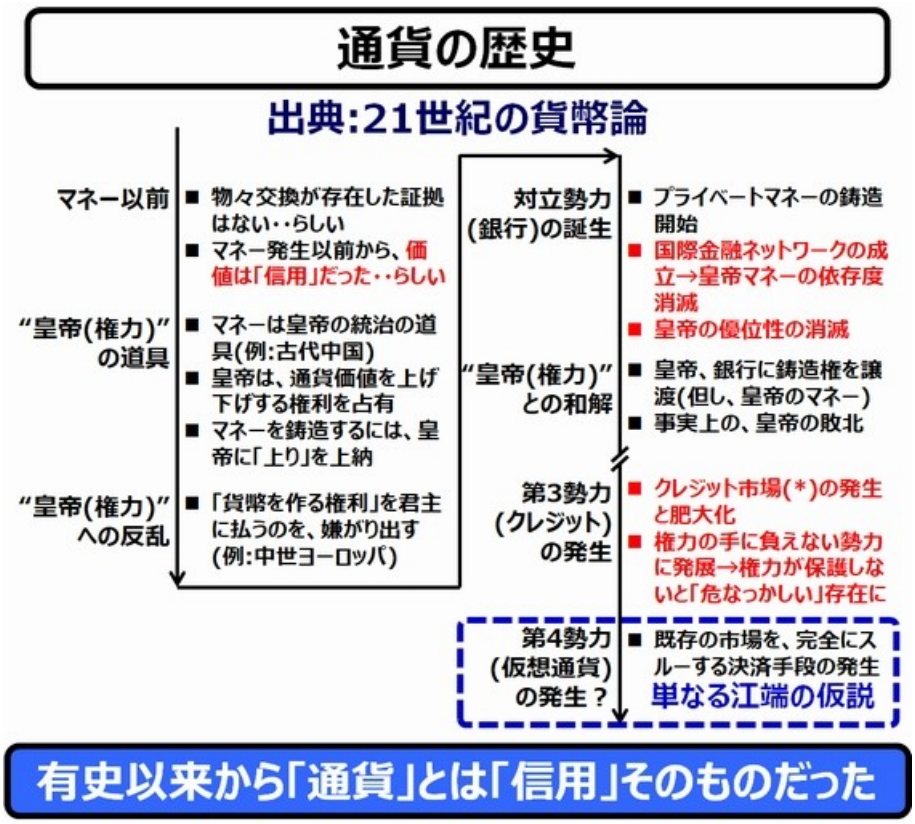
　ただ、「権力の干渉を受けない自由な通貨」という、うたい文句は既にボロボロです。まあ、これは法定通貨との交換とのバーター（交換条件）と思えば、やむを得ない（というか当然の）ような気もしますが。



　実は、各国は、国家や権力の手を離れた「影の銀行（シャドーバンキング）」によって、既に危機的な状況にあります（後述）。「影の銀行」の市場規模に比べれば、ビットコインの影響などは取るに足らないものですが ーー しかし、1980年代、その「影の銀行」も、「取るに足らない」と嘲笑されていたのです。

通貨の「信用」って？

　さて、ここからは、通貨の「信用」とは何か、について説明してみたいと思います。今回は、後輩に勧められた「21世紀の貨幣論」を読み込んで、そこから自分なりに年表（というかチャート）を作ってみました。



この本は、「マネー(貨幣)の発生以前であっても『物々交換』はなかった」という、驚がくの説明から始まります。この本では、物々交換が存在していた証拠が「確認できていない」とまで言い切っています(p.17)。

歴史上、貨幣がどのような意義をもってきたかを並べてみると、こんな感じです。

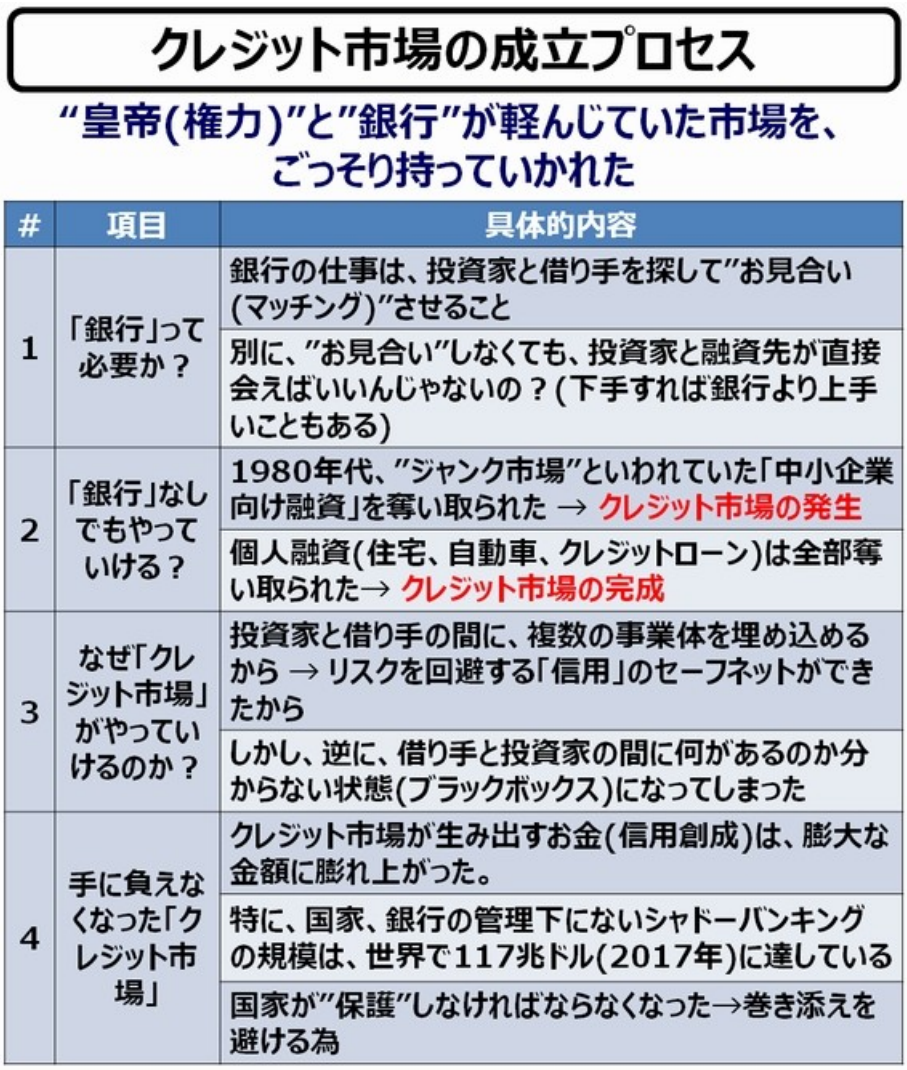
(Step.1) 皇帝(権力)の統治の道具として使われていた
(Step.2) 皇帝(権力)の無策な貨幣政策に嫌気がさした大衆が、勝手に通貨を作り出した(プライベートマネーと銀行の発生)
(Step.3) プライベートマネーと銀行が、独自の国際ネットワークを作ってしまって、皇帝(権力)の貨幣を無力化させてしまう
(Step.4) 皇帝(権力)が民間に、お金を製造する権利を譲渡し、権力と銀行の蜜月時代が始まる

―― と、まあ、ここまでは、**貨幣というものが、権力の制御下にあったこと** を説明しています。

ところが、「権力と銀行のカップル」が、中小規模の市場規模を侮っていた間に、そのカップルを当てにしない第3の貨幣勢力 ―― クレジット市場*) ―― が、最初は見えないほど小さく始まり、そして、現在は無視できないくらいに、大きくなってしまいました。

*)「クレジット市場」とは、「信用リスク(資金の借り手の信用度が変化するリスク)」を内包する商品(クレジット商品)を取引する市場の総称です。

1970年ごろから始まった、分業化、アウトソースが、銀行(金融)の世界にも及び、そして、皮肉なことに市場が「**別に、銀行、なくても良くね?**」ということに気が付き始めてしまいました。



借り手と貸し手を探し出すことや、融資の審査、在庫保有、管理を、アウトソースしまくった結果、銀行から、有価証券市場への移行が行われ、クレジット市場は今も凄い勢いで大きくなり続けています。

そして、「大きくなりすぎて、もうつぶせない」というくらいにまでに成長してしまい、**クレジット市場がつぶれる時は、国家も道連れ**、という状態にまでなってしまっています。

今や、国家権力は、（大変不本意で、本末転倒だろうとは思うのですが）クレジット市場をつぶさないように、「クレジット市場を保護する政策」を取らざるを得ない状況になっているのです*)。

*）後述しますが、このクレジット市場は「エゲつない仕組み（=複雑なサプライチェーン）」が組み込まれています。この問題が最悪の形で顕在化したのが、例の「サブプライムローン問題」であり、そして、これが、今回のコロナ禍以前の災厄としては、最悪の金融危機「リーマン・ショック」を発生させることになりました。

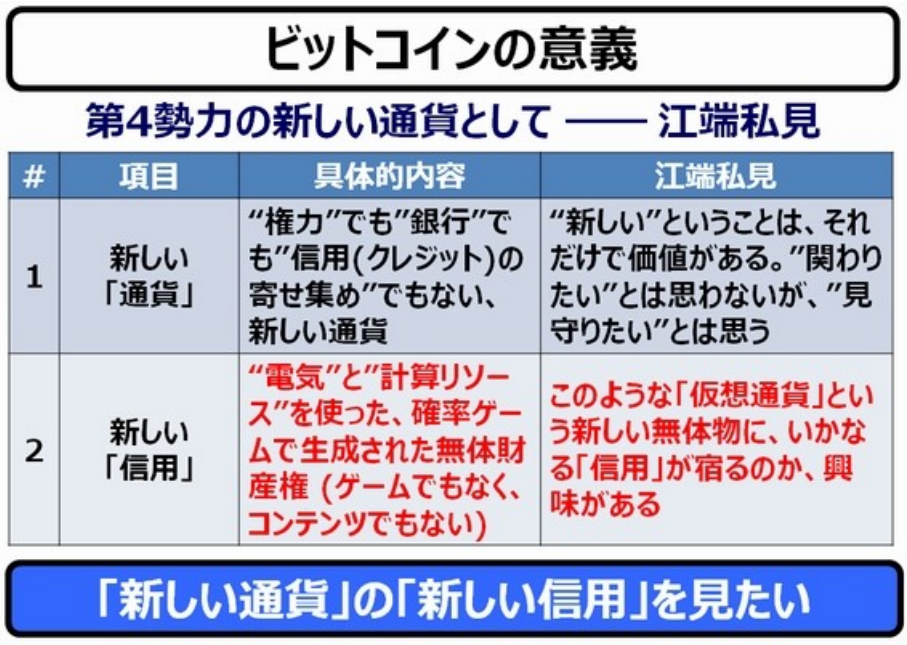
まあ、いずれにしても、通貨発生前、皇帝（権力）、銀行、そしてクレジット（のサプライチェーン）も、何をやってきたかというと、「信用」を作り、「信用」を維持する —— **バーのカウンターに彼女が置いた紙幣を使って、翌日にバーのマスターが、ジン、ウオッカ、ウイスキー、そして、ナッツ、チーズ、ビーフジャーキーを、昨日と変わらない値段で購入できる世界を守る** —— ことをやってきた訳です。

「ビットコイン」の意義とは？

ビットコインなどの仮想通貨は、—— これは私の主観（というか仮説）なのですが —— クレジット市場のカテゴリーには入れることのできない、**新興の第4勢力**のように見えるのです。

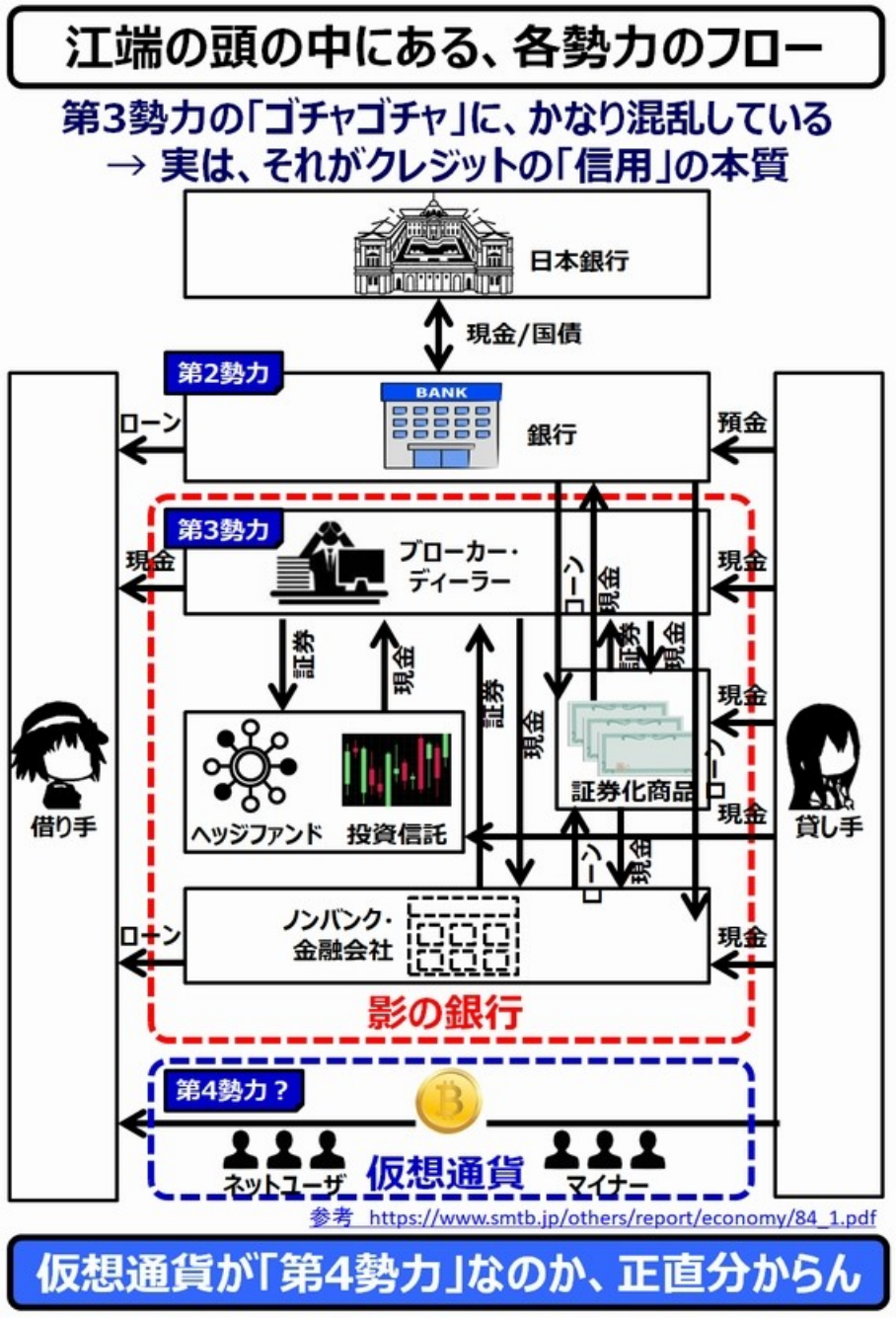
もし、このビットコインのような仮想通貨が第4勢力として成立するのであれば、以下のような意義が求められると思いま

す。



　権力と蜜月の銀行という第2勢力でもなく、複雑なサプライチェーンを前提とするクレジット市場という第3勢力でもなく、そういう全てを全く無視して、「ほとんど友人との間で金の貸し借りをするノリで、電子的に通貨を直通させる通貨」に、**どのような「信用」が乗っかるのか**、私はとても興味があるのです。

　で、まあ、私なりに、このゴチャゴチャする勢力のフローを書き下してみたのが下の図です。



参考:三井住友信託銀行 調査月報(2019年4月号)

詰まるところ、貸し手から借り手に、現金(でいいのかな?)が流れればいいだけのことなのですが、そこに「信用」を作り出すために、かなり面倒な金融のサプライチェーン ―― 責任(リスク)回避システム ―― が組み込まれているのです。

ところが、ビットコインのような、貸し手と借り手の一直線のチェーンでは、どっちかが債務不履行をかましたら、その時点で破綻→信用崩壊→終了です。ただ破綻するのは、貸し手と借り手のペアだけですので、市場全体への波及は(多分)ないはずです。

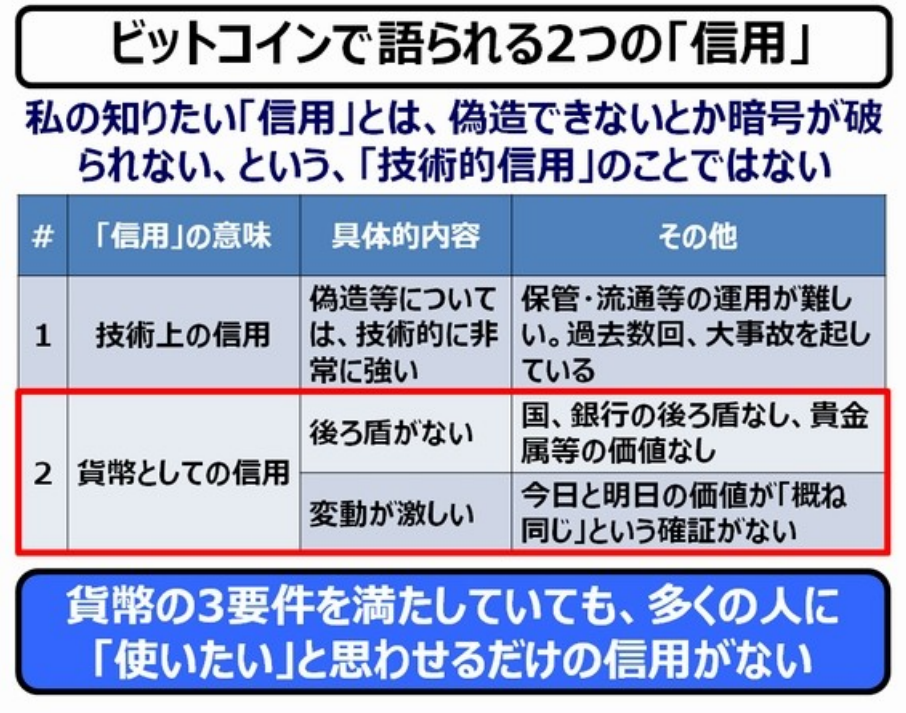
ただし、ビットコインが、「影の銀行」の一部として組み込まれたら話は別ですが。現状の、ビットコインのレートを見ている限り、「**こんなに不安定な金融商品は、見たことがない**」というくらい不安定なものですので、そういうことは、現時点ではないだろうなぁ、と思っています(ただのカンです。裏は取れていません)。

というわけで、慣れない本(私は普段、技術書しか読んでいないので、金融の本や資料を読みこなすのは正直苦痛です)を読んで、貨幣の歴史と、その仕組み(サプライチェーン)を俯瞰してみたのですが、これを見ても、**「ビットコインの信用」というものにたどりつくことはできませんでした。**

ビットコインで決済できる店舗がない

さて、ここで、前述した、意味の異なる2つの「ビットコインの信用」のお話をしたいと思います。

ビットコインで使われている「信用」とは、もっぱらブロックチェーンの技術的な信用です（ただし、運用上の信用は、これまでの事故で、かなり信用が毀損されています）であって、貨幣としての信用が語られることはありません。



貨幣にとって一番大切な信用とは、『「今日のパンの値段」と「明日のパンの値段」が同じである』を担保することです。これは簡単に説明できます。

（今の1BTCは、法定通貨で120万円くらいなので、0.0001BTC=120円と考えて）、今日、0.0001BTCで購入できるパンが、明日はその2倍になるとしたら、

（1）パンを買う人は、今日中にパンを買う
（2）パンを売る人は、今日は休業して、明日パンを売る

となります。

逆に、明日、パンの価格が半分になるとしたら、

（1）パンを買う人は、今日はパンを買わずに、明日買う
（2）パンを売る人は、今日は営業するが、明日は休業する

となってしまいます。

言うまでもないですが、こんな不安定な通貨を使っている国家の経済は、簡単に破綻します。

今回は見送りますが、実はビットコインって、ほとんど市場に流通していません（私には、かなりショッキングな事実でした）。皆さんの周りで、**ビットコインで決済できる店舗、ありますか？**　私、この連載を始めてから、かなり注意深く見ているのですけど、一店舗も見つけられていません（試しにネットで調べてみてください。がく然とすると思います）。

まあ、それはさておき、私の言っている信用とは、「技術的な安全性としての信用」ではなく、「**みんなが使ってみたい気持ちになれる通貨としての信用**」のことです。

ビットコインの“信用”を探し求めて

「歴史」でも「仕組み」でも分からなかったので、仕方がありません。私は、「みんなが使ってみたい気持ちになれる通貨としての信用」を求めて、泥臭い地道な調査を開始することにしました。

大きな書店の中にある、ビットコイン、仮想通貨に関係する本が集っているコーナを写真で取ったものです。私、この本の全てに目を通しました（本屋には大変迷惑な客だったと思いますが）。そして、ビットコインの「通貨としての信用」に言及している本は ーー 嘘偽りなく「1冊だけ」でした。

本棚の前でウロウロする江端

Google Scholarを使って、"ビットコイン"&"信用" & "創成"で、検索をかけたところ、15件がヒットしました。そして、私と同じような疑問に至っている論文を多数発見しました。

さらに、Google Searchで検索してみたところ3万件ほどヒットしたので、上位100件に全部目を通しました。その結果、それらのほとんどが、「通貨としてのビットコイン」に否定的、または、懐疑的な記述であることを知り、正直ショックを受けました。

現時点での暫定的な私なりの結論は、

――現時点のビットコインは「通貨」として使用できる状態にない

です。

ちなみに、私はビットコインをおとしめたい訳ではありません。**逆です。**私は、**ビットコインなどの仮想通貨を、上手く生活の中に取り込んで、早いところ日常的に使い倒したいのです。**

理由は2つあります。

(1)町内会の集金作業をするのに、町内を歩き回って、各世帯を訪問するような、気の重い、うっとうしい作業をとっとと止めて、パソコンやスマホから簡単に集金/送金できるようにしたい
(2)コンテンツを作成してくれた方に御礼に、Amazonギフトカードを送付するというような、Amazonサービスの利用者であることが前提である手段を使うのは嫌だ

「メールに電子ファイルを添付する程度のノリで、送金／集金したい」―― 本当に、私の希望は、本当にこれだけのことであり、これだけのことができない現状に、イライラしています。

ちなみに上記(1)(2)に関しては、町内会のWebサイトを作っていた時に、クレジットカードを使った年会費集金システムを検討したことがあったのですが、クレジットカードのシステム使用料の高額さにがく然として、断念したことがあります(PCの前で「ふざけるな!」と叫んだ記憶があります)。

さて、ここからは、かなり本気のお願いなのですが ―― **ツイートで、私のこのコラムに「勉強不足」とディスるメッセージを書き込む時間があるなら、私に「教育」を施してください。**私は、自分が納得できる”論”や”証拠”に出会いさえすれば、**”3秒”で自分の主張を180度引っくり返すことができる**ように作り上げられた研究員&エンジニアです。

今回の調査では、私は見つけることができませんでしたが、ビットコインの「貨幣としての信用」について、肯定的で、ロジカルに説明された(×観念的、×思い込み、×希望的観測、×根拠のない未来、×エビデンスがない、×エビデンスにたどりつけない)書籍、論文、その他資料、あるいは自説(ただし”証拠”に基づく”論”として成立しているものに限る)があれば、ぜひ、私に紹介してください。連絡先はこちらをご利用ください→”blockchain_20201122@kobore.net”。

頂いたメールは、個人情報を完全に抹消した上で、一文字も改ざんせずに、メール全文を本連載で公開することをお約束致します。ご安心ください*)。

*)公開例としては、こちらが参考になると思います。

特に、数式で記載されたものでご紹介頂ければ、直ちにコーディングしてPCでシミュレーションを実施します。**大好物です*)。**

*)「大統領選、連続1万回シミュレーション」とか「1/100秒単位の飛び込み自殺シミュレーション」のようなものになると思います。

個人的な感情であることは分かっているのですが ―― ビットコインを「投機目的として勧めるような入門書」を読んでいると、私は、非常にムカムカしてくるのです。

閑話休題。

ビットコインの信用=ブランド力?

このように、「貨幣論」からの「ビットコインの信用」へのアプローチに失敗しましたので、ここで一つの仮説を置いてみようと思います。

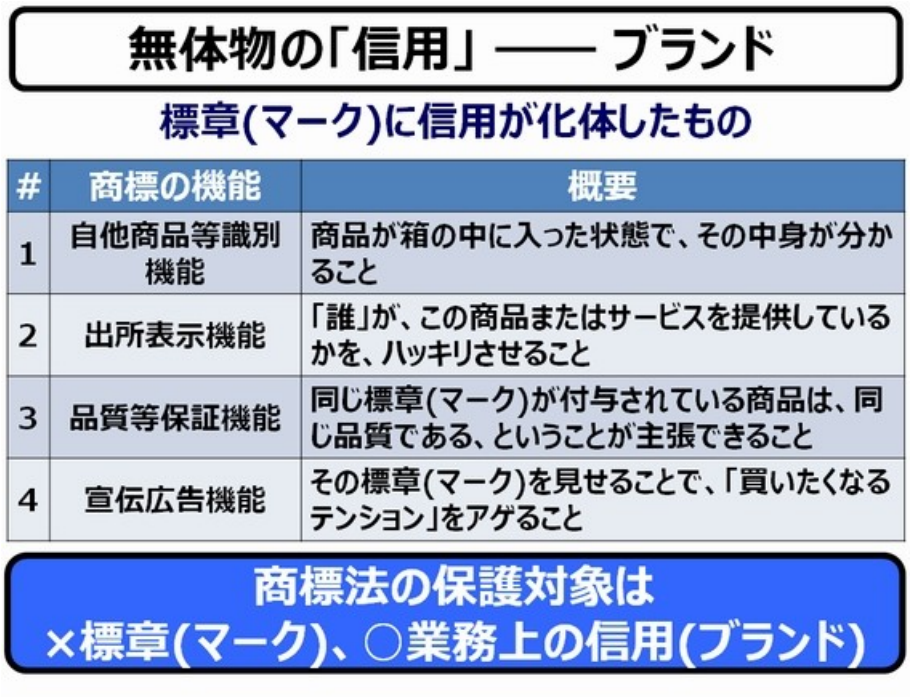
「そもそも、ビットコインには(エバコインと同様に)貨幣としての信用はない。それはそれで良い。なぜなら、ビットコインの信

用とは、ブランド価値として、後発的に発生しているものであるからである」

という、「ブランド論」からのアプローチです。

　実は、無体物の財産権には、特許権、意匠権、著作権などがありますが、その中でもブランドの保護を行っているものに「商標権」があります。

　商標権というと、標章（マーク）が保護対象のように思われているかもしれませんが、実は、商標を利用する法人や個人の、業務上の信用を保護するものです。で、その業務上の保護をする手段として、商標の機能を4つに特定して、それぞれの機能を最大限発揮できるように法定しています。



　ここで重要なのは、**初期状態の標章（マーク）には、ひとかけらの価値もない**、という前提に立つということです。これが、特許法や意匠法と決定的に異なる点です。

　特許発明（技術アイデア）や意匠（物品デザイン）は、厳しい基準をパスした、突出した価値のあるアイデアやデザインだけを保護対象として認めた上で、国家によって徹底的に保護する、という形式を取っています。

　比して、商標法は「**最初は無価値でも構わんが、そのうち、その商標を見ただけで、みんなに『あ！　あの会社だ！』と気がついてもらえるようにガンバレ！！**」という形で応援（保護）し、商標の使用によってその商標に化体した信用（**顧客吸引力**）を保護します。

　さらには、がんばっていない会社の商標は保護期間であっても、保護を止めてしまう規定まであります（不使用取消）*)。

*）ちなみに、特許庁の検索エンジンで調べてみたところ、「ビットコイン」も登録商標になっているようです。

　つまり、ビットコインは、ビットコインをブランド化すべく、これまで営業努力を続けてきたということであり、「通貨としての信用」の有無はさておき、「業務上の信用」の確立には成功していると言えます。

　なにしろ、「ビットコイン」というものがどういうものであるかを知らない人が圧倒的多数であるとは思います。しかし「ビットコイン」という言葉を知らない人は、絶無であると思えるからです（いわゆる、”AI”と同じです）。

　ご存じの通り、ブランドというものは、それを構築するのに多大な努力と10年オーダの時間を必要とする一方で、それが失墜するのは1日あれば足る、といわれるほど、脆いものです。

　実際に、ビットコインのブランド価値を毀損する事件は、結構あります。「（1）シルクロード事件」「（2）マウントゴックス事

件」がありますし、身代金をビットコインで要求された「（3）ランサムウェア事件」については、ひとごとではありませんでした。実際に私の知人のIT関係者の多くが、「ランサムウェア」の被害にあい、仕事が全くできなくなっている状況をリアルタイムで見てきたからです。

さらに、ビットコインそのものではありませんが、同じ仮想通貨（のプラットフォーム）であるイーサリアム（Ethereum）での「DAO Attack事件」、そしてそれに伴う「（4）ハードフォーク」という処理は、「その気になれば、**運用主体がブロックチェーンの『非介在性』に介在できてしまう**」という事実を示してしまいました。

上記の「（1）シルクロード事件」「（3）ランサムウェア事件」は、ビットコインの最大のウリである「匿名性」を、最悪の形で使われたされたものであり、ビットコイン（という技術）には1mmの非もありませんが、現時点で、この手の犯罪への利用を防止する手段がないのも事実です*）。

*）実は、防止する手段がないわけでもありません ーー 例えば、「インターネット利用者全員に対する、完全な実名登録性の導入」をして、利用者の利用状況の100%モニタリングを可能にする、とか ーー まあ、非現実的ですが。

また、上記「（2）マウントゴックス事件」は、ビットコイン自体がどんなに堅固なであったとしても、その運用主体の内部からであれば、いともたやすくビットコインを盗めることを証明してしまいました。

そして上記「（4）ハードフォーク」に至っては『それを言っちゃあ、おしまいよ』と、みんながブロックチェーンに関して思っていたことが『やっぱりできちゃうんだ』と実証して見せた点において、**ちまたの「ブロックチェーン万能神話」を、程よくぶっ壊した**、と思っています。

話が逸れてしまいましたが、結論を言えば、「**ビットコインは、これまでの営業努力に加えて、上記のような醜聞（スキャンダル）も加わって、ブランド（？）を確立した**」と言える訳で、これが冒頭の「ビットコインとエバコインの決定的な違いである」と言えそうです。

ただ、このビットコインのブランドは、商標法の保護対象である「**顧客吸引力**」だけでなく、その真逆の「**顧客嫌悪力**（江端が命名）ーー『なんか、うさんくさい』」というものも発生させている点において、ちょっと違う感じもします。

「ビットコイン」とは、そもそも仮想通貨を成立させる「技術の名称」なのですが、世間一般的には、仮想通貨（暗号資産）という”モノ”を示す言葉としても使われています（これに対して、「ブロックチェーン」は「技術の名称」です）。

さて、「ビットコイン」も「ブロックチェーン」も、その技術内容が理解されないまま、用語だけが乱用されているという意味においては、「バズワード」であることは間違いありません。ですが、「ビットコイン」が、前回のテーマである「量子コンピュータ」と違うのは、（1）既に実運用されている、（2）吸引力と嫌悪力が併存している、（3）普通、2〜3年で消えていくバズワードと異なり、**かなりしぶとく生き残っている**、という点です。

そして、今回、深くは言及しませんが **（4）本来の目的（通貨）から離れて、別の目的（投機）に変質させられている** という点において、**極めて危険なバズワード**とも言えます。

これまでのバズワードは、私たちのような研究者やエンジニアを翻ろうした揚げ句、最後は無責任に捨て去りましたが、逆に言えば、バズワードの被害者は、研究者やエンジニアだけでした。

しかし、「ビットコイン」はちょっと違います。このバズワードは、**取り扱いを間違えると、人生を台無しにしかねないリスク**があります。

もしあなたがこのバズワードに関わることを決めたのであれば、どんなに面倒くさくても、**ビットコインと利害関係のない立ち位置にいるIT技術者**をとっつかまえて、説明させることを強くお勧めします ーー 私（江端）なら、昼飯をおごってもらえれば応じます。

ブラック企業も驚く給与形態「半減期」

さて、ここから後半になります。

私は、ビットコインの根幹技術は、以下の6つと認識しています（ブロックチェーンは、（A）〜（D）の4つ）。

そんでもって、(A)～(D)については、解説をサボらせてもらおうかと思っています。

理由はいくつかあるのですが、

(1)「ビットコイン」とか「ブロックチェーン」の名前が付与された書籍であれば、必ず解説がされていて「今さら、解説することあるかな?」と思ってしまったこと

(2)それらの技術は、多くの人にとっては気が付かないだけで、日々使い倒している技術であり(例えば、"http s://"の利用等)、それ故、解説がしにくいこと、そして、

(3)特に、ここ1～2年の間、某クラウドでの開発、実装、運用で、結構な"修羅場"を体験してきて、個人的に腹を立てていること*)(本当に個人的理由ですが)

に因ります。

*)例えば、最近ならこれなど

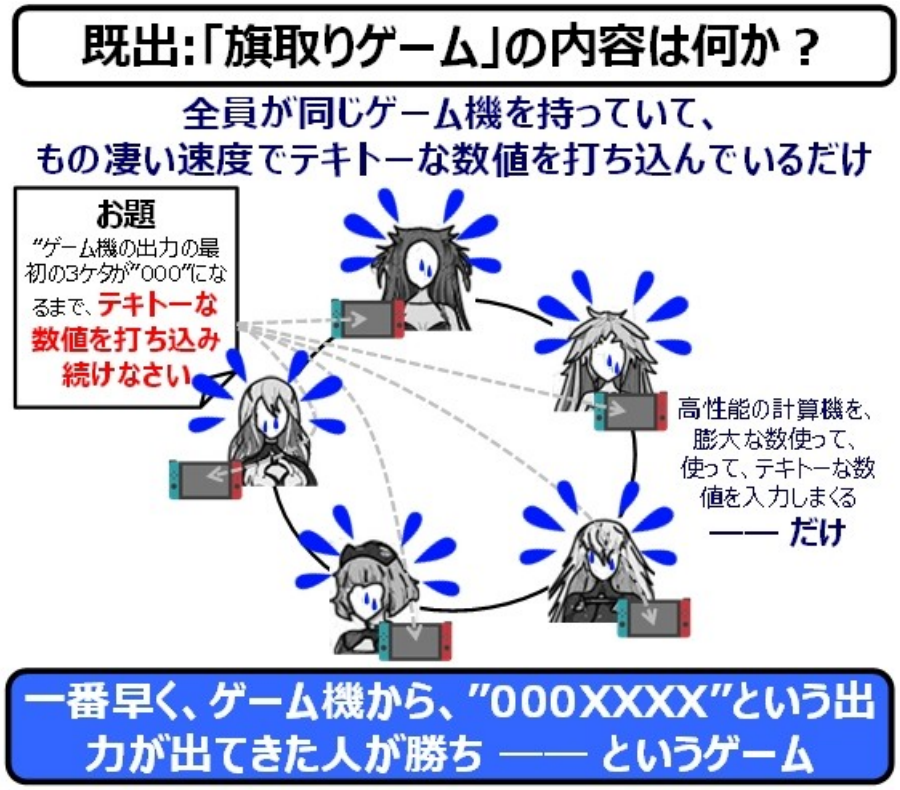
というわけで、今回も(そして、いつも通り)、もっぱら私に興味があることを、もっぱら私のためだけに検討した内容についてのみ、お話したいと思います。

前回、「(E)コンセンサスアルゴリズム」については、バーっと説明しましたので、今回は「(F)の半減期」について、同じくバーっと、私らしく説明したいと思います。

さて前回、ビットコインのマイニング(発掘)が、電力とコンピュータのリソース(それも、単なる乱数生成計算)を消費するだけの、旗取りゲームにすぎず、その旗を取った者に、単なる"数字"が付与されるだけのこと ―― **一体どこが"発掘"やねん!** と突っ込みそうになる代物である ―― というお話をしました*)。

*)ちなみに、私、この旗取りゲームが「乱数生成計算」ではなく、ゲームの度にお題が代わる ―― 例えば、『現時点における、〇〇地区の人身事故による交通ダイヤ回復の最適計画の計算』というものに使われるような仕様になっていれば、**ビットコインの仕組みを社会に定着させるために、私の人生をささげても構わない**、と思っているくらいです。

私が心底腹を立てていることは、「数当てゲーム」ごときのために、**一国分に相当する電力が消費され続けて、コンピュータリソースが食いつぶされている**ことです。

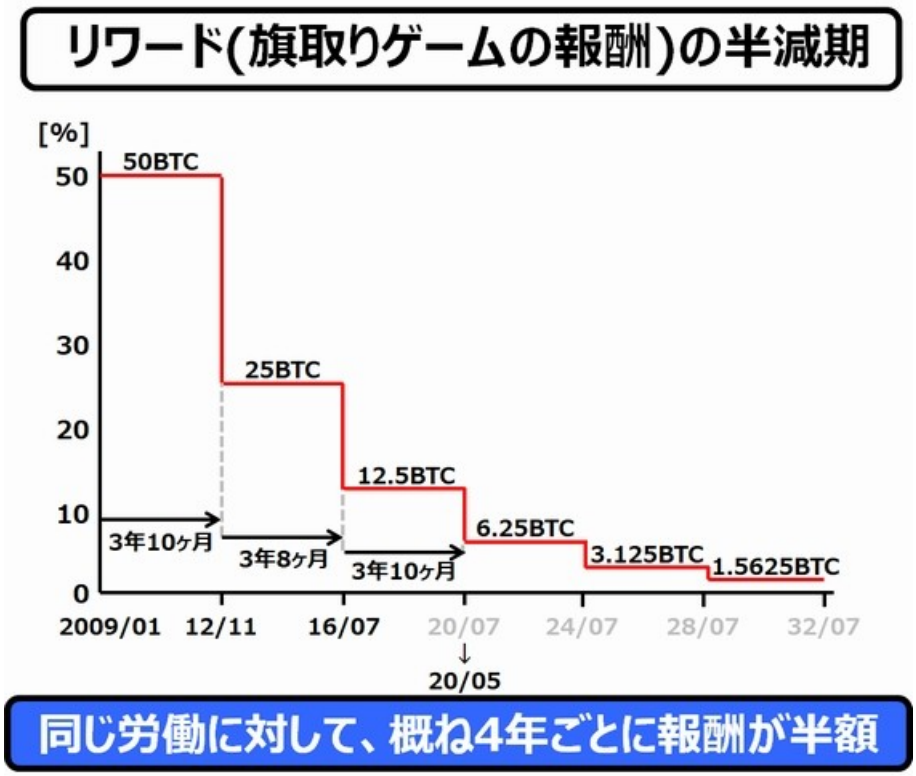


しかし、誰でも「マイニング」に参入できて、ゲームの勝者を公平に維持するのであれば、「数当てゲーム」くらいしか、やりようがないことも分かってはいるのです ーー 本当に悔しいのですが。

さて、半減期の話に戻ります。

ビットコインにおける「半減期」とは、ブラック企業も真っ青の、驚愕動転（きょうがくどうてん）の給与形態にあります。

―― 勤続年数が増えれば、給料がどんどん減っていく



つまり、上記の旗取りゲームによる賞金が、おおむね4年単位で、きっちり半分になる（ように設計されている）のです。

なぜだ！　理不尽だ！　ストライキだ!! と叫んでも無駄です。それはビットコインという仕組みに組み込まれていて、変更することができないからです*）。

*）まあ、公開されているソースコードをハックすることはできますが、マイニング（旗取りゲーム）に参加できなくなるので、意味ありません。

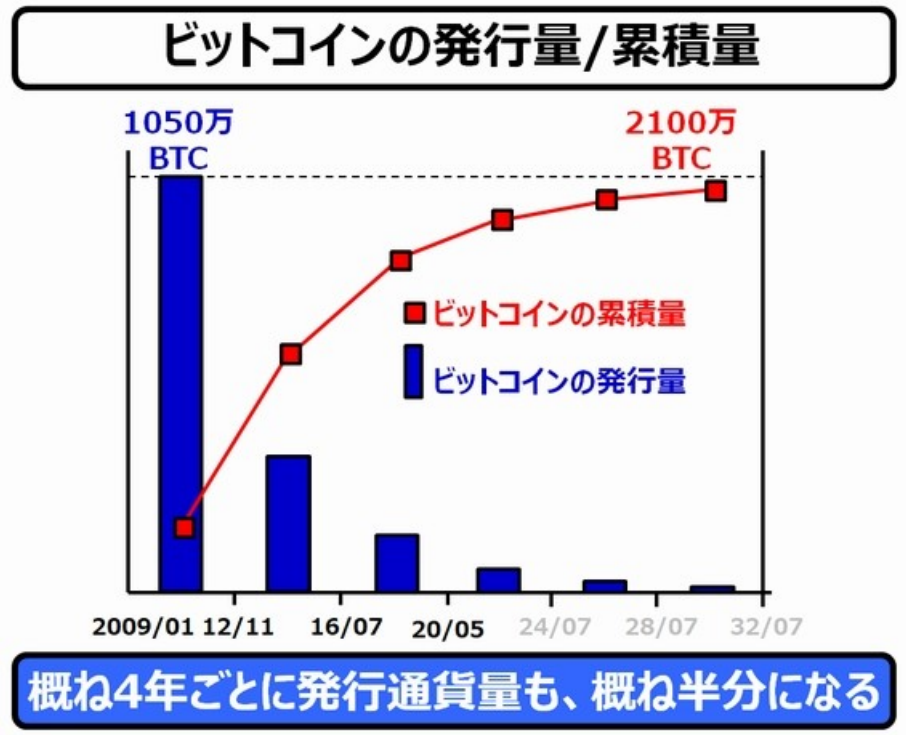
この半減期のタイミングで、ビットコインの発行量も半分になります。

ここで結構勘違いしてしまう人も多いと思いますが（私もそうでした）、発行量が半分になる理由は、ビットコインのマイニング（旗取りゲーム）の勝負の内容が難しくなるとか、そういう訳ではありません。

勝負の時間は、マイナー（発掘者）が増えようが、減ろうが、”約10分間”で調整されつづけます*）。これは、ビットコインの発行開始から終了まで変わることはありません。

*）この”約10分間”をキープするために、ゲームの内容を難しくしたり、簡単にしたりすることはあります。といっても、そのやり方は簡単で、例えば、これまで「上3桁の数が”000”になったら勝者」とした条件を、これからは「上4桁の数が”0000”になったら勝者」とだけ変更すれば、「難しく」できます。

しかし、半減期ごとに発行される賞金（BTC）が半分になるので、その結果として、ビットコインの発行量も半分になってしまうのです。



なぜビットコインがこんなこと（半減期）を設けているかというと、（1）ビットコインの通貨量を2100万BTCで打ち止めとするためと、（2）その打ち止めまでの時間を可能な限り引き延す作戦のためです。

いつも通りの仕事をやっているのに、4年後には給料を半分にさせられる —— 誰が、こんなゲームをやり続ける？と思って調べてみたら、今や、電力の安い中国の奥地だけでなく、今頃になって欧州や日本で参入している法人もいると知り、目を疑いました。

—— おーい、みんな正気かぁーー？

って、普通、思いますよね*）。

*）もっとも、参入しているのはビットコインではなく、他の仮想通貨（イーサーリアムなど）である場合は、ちょっと話は変わってきます（ビットコインは、世界中にある1000種以上の仮想通貨の一つです）。

「正気」で続けるたった一つのシナリオ

ところが、これを正気で続けるシナリオが一つだけあるのです —— **ビットコインのレートが、無限に上がり続けること**です。

簡単に言えば、ビットコインの発行量を半分に抑え込まれたとしても、ビットコインの法定通貨とのレートが2倍になればトントン。それ以上なら、このゲームを続けていても「もうかります」。

加えて、レートが上がれば、既に所有しているビットコインの価値も雪だるま的に上がるので、ビットコインを所有しているだけで、どんどんお金持ちになっていきます。

もうお分かりかと思いますが、そんな状況の中にあれば、**ビットコインを貨幣として流通させて、支払いに使う奴は、はっきりいって阿呆**です。ほっといても価格の上がるものが、財布の中に入っているのに、それを他人にくれてやって、どうするというのでしょうか？

つまり、今のビットコインは、「便利な支払いの道具として使いたい」という私の願いの真逆の「投機物件」に成り下がっているのです —— 誰も手放さそうとせず、それ故、市場に流通せず、ビットコインを取り扱える店舗を、ネットで探さなければ見つけることすらできないという、現状の歪（いびつ）なビットコインの流通市場が完成する —— というわけです。

では、ビットコインのマイニングで、現時点の1BTCあたり120万円の利益を確保し続けるためには、今後、ビットコインの

レートがどの程度上がり続けなければならないのでしょうか。簡単なプログラムを書いてシミュレーションをしてみました*)。

*）現在C/C++言語からGo言語へ乗り換え中です。

```
package main
import "fmt"
func main（） {
 reward := 50.0
 total_bc_issued := 0.0
 passed_year := 2009.0
 next_year := 2009
 for i := 1; i < 21000001; i++ { //2100万ブロックで終了
  if i%210000 == 0 { //21万ブロック単位で報酬が半分になる
   reward /= 2.0
  }
  if int（passed_year） == next_year {
   next_year++
   //fmt.Printf（"reward = %.8f total_bc_issed = %.8f passed_year = %.1f¥n", reward, total_bc_issued, passed_year）
   //fmt.Printf（"%.8f,%.8f,%.1f¥n", reward, total_bc_issued, passed_year）
  }
  total_bc_issued += reward                  // 報酬の加算
  passed_year += 9.6 / 60.0 / 24.0 / 365.2422 //9.6分に一回発行 1年を365.2422日として計算
  if i%1000 == 0 { //1000ブロック単位でデータ表示
   fmt.Printf（"%.3f,%.8f,%.8f¥n", passed_year, reward, total_bc_issued）
  }
 }
}
```

まず、計算結果と、2009年からのビットコインの半減期の時間などから、パラメータチューニングを行ってみました。

シミュレーション結果から見た全体像

実データと比較しながら、シミュレーションのパラメータを補正してみた

#	項目	公称	シミュレーション（チューニングを含む）
1	1ブロックの発掘に調整されている時間	10分	9.6分
2	半減期に至るまでのブロック数と期間	21万ブロック（3.99年）	21万ブロック（3.83年）
3	2100万ブロックに至るまでの半減期の回数	理論的には100回（2100万ブロック÷21万ブロック）	1Satoshi=0.00000001BTCで、桁落ちしてしまうまで、34回
4	2100万ブロックに至る年（ラストデー）	理論的には、西暦2408年（388年後）	シミュレーション上では、2139年3月24日（119年後）

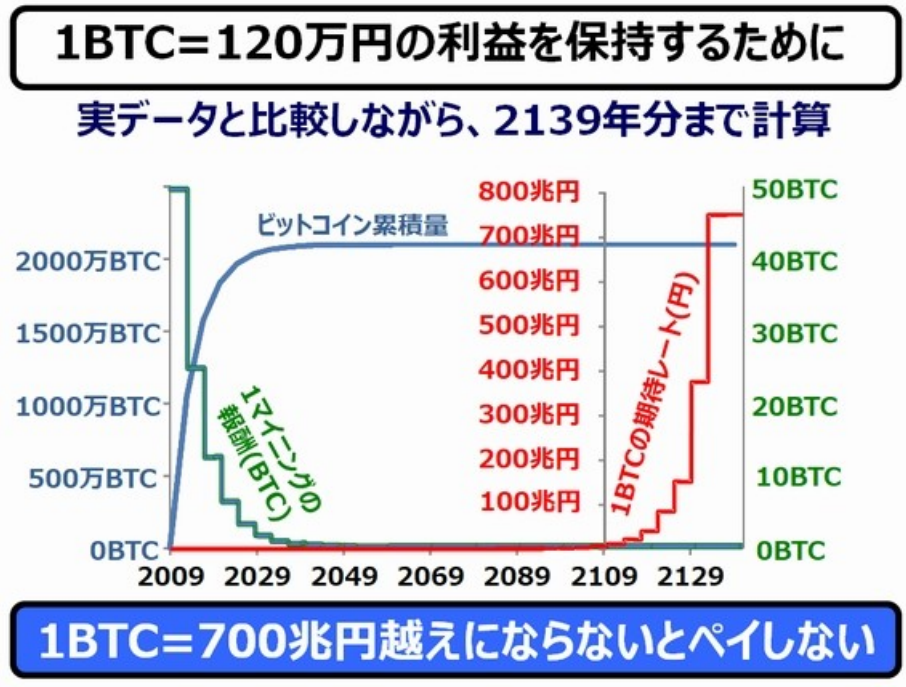
計算結果からでは、10分に1ブロックのマイニング（1回の旗取りゲーム）が完了しているとされていましたが、実際には、平均9.6分ぐらいのようです。

また、21万ブロックで半減期が発動することから考えて、100回の半減期が、2408年（388年後）まで続くように思えますが、実際には、ビットコインの最小単位1Satoshi=0.00000001BTCが桁落ちしてしまう日が、119年後の2139年の3月24日となりました。

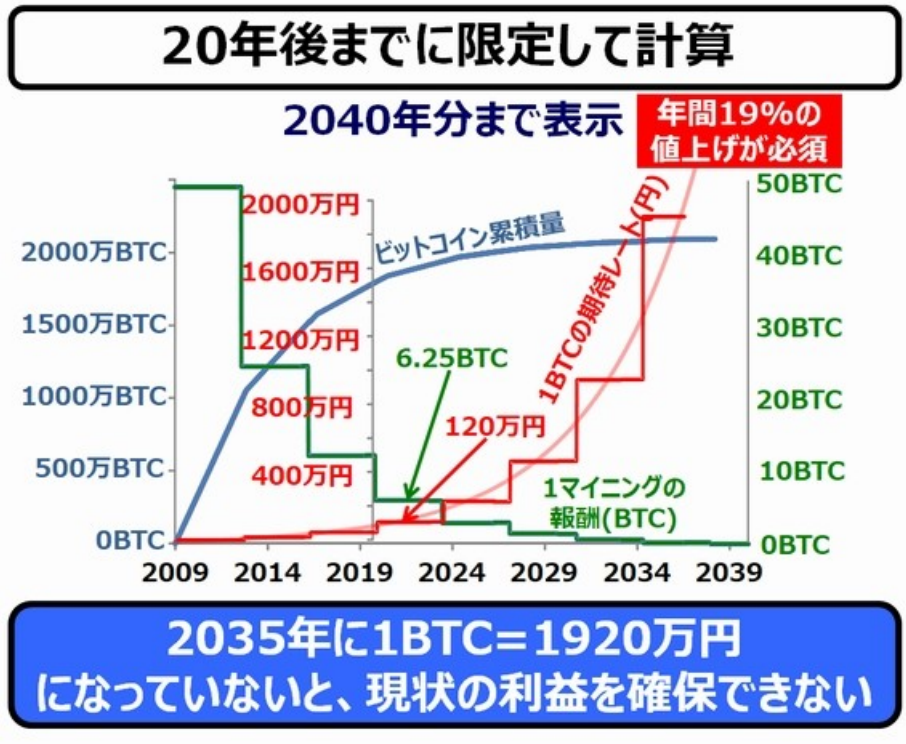
この日（ラストデー）から先、ビットコインのマイニングは行われなくなりますが ーー まあ正直、そのへんは、皆さんにとっても私にとっても、**どーでもいい世界**です（とっくに、私たちは「鬼籍の人」です）。

まあ、このどーでもいい世界でも、ビットコインが動き続けているとしたらどうなるかの計算を続けてみたんですが、なかなか凄いことになっています。

現時点において、「現状の”1BTC=120万円”のマイニング利益を得る」ためには、マイニングの最後の年である2139年に、**1BTC=750兆円**に値上がりしていなければなりません（シミュレーション結果のデータは[こちら]です）。



さすがに、119年後のことを考えても現実的ではないので、現在から20年間、2040年までのシミュレーションをしてみたのですが、これでも、かなり凄いことになっています。



現在のビットコインは、3.83年で半減期を迎えますので、常に値上がりし続けなければ、マイニングは今と同程度の利益を確保できません。

年率19.8%で成長を続けなれければ、ビットコインのマイニングビジネスを現状のレベルでは維持できません。これはビットコインの半減期を使えば、以下の計算で簡単に算出できます。

$$2^{\left(\frac{1}{3.83}\right)} = 1.198389265$$

そんな成長を、**あと119年間も続けなければならないなんて無茶**です。20年間に限定しても、無理でしょう。

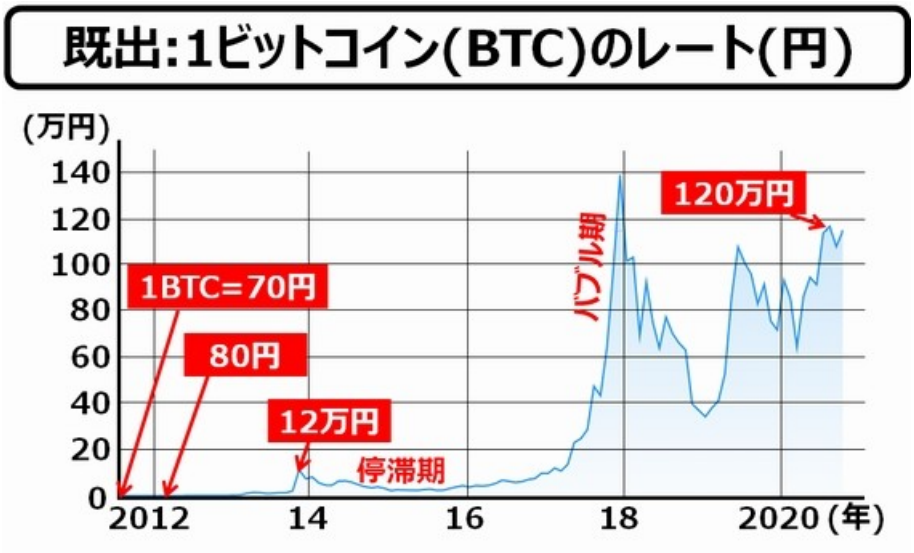
ちなみに普通の株式や通貨では、こういう計算はできません。株式や通貨の流入量は、様々な景気判断の後、企業や日銀関係者の判断によって調整が行われるからです。

しかし、コンピュータのアルゴリズムであるビットコインには、そのような **人間的な恣意が介在する余地はありません**。世界の景気がどうなろうとも、半減期は、21万ブロック単位、3.83年ごとに確実にやってきます。それゆえ、ビットコインは必ず年率19.8%で、ビットコインの価値を増やし続けなければならない運命にあるのです。

いずれにしても、ビットコインの「マイニング（旗取りゲーム）」に明け暮れている人や、ビットコインを大量に保有している人にとって、このビットコインフェスティバルは、**終了させることのできないイベント**なのです。

うっすらと見えてきた、ビットコインの需要

ビットコインは2100万BTCという発行制限が定められているため、そのレートは需要によって決定されることになります。需要が増えれば、当然にレートは上昇することになります。つまりビットコインは、その性質上、レートが上がりやすい、とも言える訳で、実際にそうなっています（というか、恐ろしく不安定という感じです）。



ただ分からないのは、ここで言う**「需要」とは何か**、ということです。

普通「需要」と言えば、市場での貨幣の使用のニーズとなりますが、何度も説明している通り、ビットコインで決済できる店舗（実世界もインターネットも）を、私は知りません。

最近は町内の小売店舗の入る度にチェックしています。また少なくとも、AmazonやMonotaroでの支払いはできないし、楽天はビットコイン自体の購入や交換はできるけど、ビットコインを使った支払いはできないことを、自分のポータルサイトから確認しました。

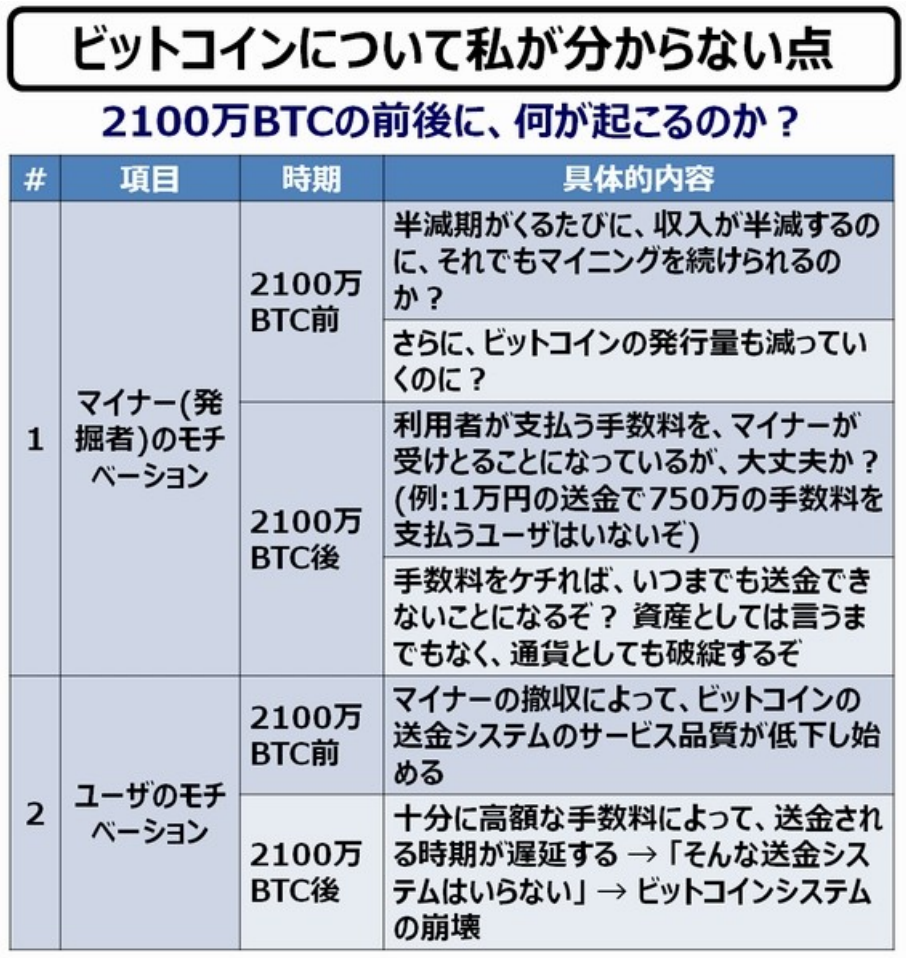
とすれば、残りは、「投機のための『投機需要』」という、実に不吉なものが見えてきます ―― が、これは次回以降にお話したいと思います。

「2139年」付近では何が起こるの？

では、2100BTCが全部出揃った、2139年3月24日（江端試算）の直前と直後に何が起こるのか ―― これを考える

と、**結構怖い**です。

下記の表は、私が思いついたことを書き出したものです。



ビットコインについて私が分からない点

2100万BTCの前後に、何が起こるのか？

#	項目	時期	具体的内容
1	マイナー(発掘者)のモチベーション	2100万BTC前	半減期がくるたびに、収入が半減するのに、それでもマイニングを続けられるのか？
			さらに、ビットコインの発行量も減っていくのに？
		2100万BTC後	利用者が支払う手数料を、マイナーが受けとることになっているが、大丈夫か？(例:1万円の送金で750万の手数料を支払うユーザはいないぞ)
			手数料をケチれば、いつまでも送金できないことになるぞ？ 資産としては言うまでもなく、通貨としても破綻するぞ
2	ユーザのモチベーション	2100万BTC前	マイナーの撤収によって、ビットコインの送金システムのサービス品質が低下し始める
		2100万BTC後	十分に高額な手数料によって、送金される時期が遅延する → 「そんな送金システムはいらない」 → ビットコインシステムの崩壊

2139年3月24日のラストデーを迎えると、マイニングに対して新しいコインが発行されません。もちろん、それ以降もブロックチェーンを追加され続けることで、ビットコインのサービスは継続することができますが、「コンピュータを回し続けるだけでお金儲けできる*)」ビジネスは終了です。

*）毎日壊れ続けるコンピュータを入れ替えて、電力を安定に供給して、マイニングシステムを安定稼働させ続けるその作業（特に運用面）が、ラクではないことは知っています。

ビットコインは得られない、電気料金はかさむ、コンピュータは壊れ続ける ―― そんな中で、マイナーの設備を稼働し続けるモチベーションがあるでしょうか ―― **いや、ない**。

彼らが業務を撤収したらどうなるか ―― ビットコインの送金は、ブロックチェーンを作る作業なくして行うことはできません。マイナーが事業から撤収したら、ビットコインの取引は破綻します。仮に全部のマイナーが撤収しなくとも、取引に必要なブロックの生成は10分間（私の試算では9.6分間）から、もっと遅延することになるかもしれません（例えば10日間とか）。

そんな取引サービスを誰が使い続けるでしょうか？ そして使い道のなくなった2100万のビットコインは、通貨として使えないまま死蔵し、やがて、ビットコインの大暴落と同時に、システムが完全に破綻に至る ―― これは、**ビットコインのシステムを普通に考えれば、普通に出てくる、普通の解**です。

2139年3月24日（江端試算）後に、もしビットコインシステムが破綻してしまうのであれば、破綻の前倒し連鎖が発生するかもしれません。『どうせ破綻するシステムの仮想通貨を持っていてもしょうがない』が、2139年から、どれくらい前まで遡行してくるか ―― これが問題です。

10年か、20年か、あるいは、100年遡ってくるかもしれません。100年前まで遡ってくれば、119年（現在）まで遡るのも同

じことです。

「現時点で、発行スケジュールが確定してしまい、発行量に上限のあるビットコインには未来はない」「それならば、別の仮想通貨に乗り換えてしまおう」というモチベーションが発生しても不思議ではありません。その日は、「今日」かもしれません。

ビットコインは、現時点から未来を俯瞰できる、稀有なシステムであり、それ故に、ユーザに大きな安心を与えていることは間違いありません。しかし、同時に確定した未来は、「**普通なら考えなくて良いことまで考えることができてしまう**」という、負の要素があるのも事実なのです。

ちょっと怖い話をしすぎました。

実際のところは、発行量が上限の2100万ビットコインに達した後は、利用者が支払う取引手数料をマイナーが受け取れることでインセンティブになる、という仕組みが組込まれています ―― ビットコインというものは、私程度の人間の考えることには、既に先行して答を出していて、本当にすごいと思います。

ただそれでも、実際にこれでシステムの維持ができるのは、そのラストデー以降になってみないと分からないのも事実です。

その他の解としては ―― 「それを言ったらおしまいよ」という感もありますが ―― ビットコインの発行の上限を取り払って、現在のようにマイナーが業務を継続し続けるように、アルゴリズムを変更してしまうという「**禁じ手**」もありえます。

あるいは、国家や企業が、**直接、マイニングに介入してくる**という未来も ―― もう、それはビットコインと呼べるものではない何かになってしまいますが ―― そういう未来もあると思います（イーサリアムのハードフォークのように）。

「小市民的ビットコイン」への回帰

私としては、ビットコインを投機対象とする現在の仕組みを、今から少しずつ改めて、本来あるべき**「通貨としてのビットコイン」にシフト**していくことを期待しています。

マイニングは立ち上げっぱなしのPCが、勝手に参入し、運が良ければ、一日100円程度のお金が手に入る、というような、**高性能のゲーミングPCの余った計算能力を、ささやか小金稼ぎに使う**ような、そういう

―― “神田川”、“下宿”、“3畳1間”のような、小市民的なビットコインへの回帰（？）

が実現されるといいなぁ、と思っているのです。

では、今回の内容をまとめます。

【1】ビットコインのソースコードレビューを行い、「ビットコイン」と完全同一の別の仮想通貨「エバコイン」を作れる確信を得た後、仮に「エバコイン」を作ったとしても、誰も使いたいと思わない、と考えました。その理由の一つに「信用」があるという仮説に基づき、**ビットコインを含む仮想通貨の「信用」**について検討を行いました。

【2】まず貨幣の成立3要件をあげて、ビットコインがこれらの要件を満たしていることを明らかにしました。同時に、今のビットコインは、すでに当初の理念『**いかなる権力のコントロールを受けることなく存在する、自由な通貨**』という枠組みでは存在していないことも説明しました。

【3】次に貨幣の歴史を俯瞰して、貨幣の「信用」がどのように発生し、構築されていったのかを、（1）皇帝（権力）、（2）銀行、（3）クレジット市場の、それぞれの観点から説明し、さらに、**ビットコインが、過去のいずれの貨幣の「信用」の形態に当てはまらない**ことを、明らかにしました。

【4】「ビットコイン」の信用は、いわゆる、これまでの貨幣の信用とは異なり、その発生から現在に至るまでの運用の実績に加えて、**数奇な歴史や事件や誤解や偏見などによって、その著名度を獲得する**ことで作り上げられた、これまでの通貨とは完全に異なる「信用」である、という持論を展開しました。

【5】ビットコインの根幹技術である「**半減期**」の概要を説明し、シミュレーションによる検証結果から、人間の恣意的介入を許さないビットコインは、「半減期」によって決定される「発行通貨の上限」によって、その**投機的価値を高めている**ことを説明しました。同時に、その「半減期」が**通貨的価値を毀損している**という実情を説明し、ビットコインのサービスを維持するためには、**年率19.8%という常識外れの価値の上昇を実現しなければならない**という事実を計算で導き出しました。

【6】ビットコインのラストデー（マイニングの最終日）を、シミュレーションより2139年3月24日（江端試算）であるとし、このラストデーの前後で発生する、ビットコインの最悪のシナリオを検討してみました。さらに、その最悪のシナリオが、過去に遡って、今、**現在のビットコインの運用すらも破壊しかねない脅威となり得る**ことを、説明しました。

以上です。

ビットコインが生み出された“本当の背景”

サトシ・ナカモト（Satoshi Nakamoto）は、ビットコインに関する基本的な論文を発表し、冒頭で紹介したビットコインプログラムのプロトコル設計と実装を行ったと言われているという人物ですが、**正体は不明**です。本名なのか、法人/個人であるかも分かっていません。でも、

―― その気持ち、よく分かる。

正体が知られたら、どんな酷い目に合わされるか知れません。特にビットコインのレートが暴落する度に、ビットコインの仕組みを理解しないままに投機目的に購入するような人間から、言われもない非難を受けることは、想像に難くありません。

「ナカモトって奴が悪い。私が破産したのは、奴がこんなもの（ビットコイン）を考え出したからだ。私は悪くない」と言うでしょう。人間はいつだって、自分の損害に対して、自分以外の誰を責め立てる生き物です ―― 少なくとも”私”はそうです。

それはさておき。

今回、いわゆる「サトシ・ナカモト論文」”Bitcoin: A Peer-to-Peer Electronic Cash System”を読んだのですが、非常に短い（それでも9ページあるけど）、内容も簡易で、論旨が明快な論文でした。正直、拍子抜けしてしまうほどでした。

特に、私がビットコインの心臓部と考えている「コンセンサスアルゴリズム」については、第4章で1ページ程度記載されているだけで、「半減期」に至っては記載すらありません。どうやら、ビットコインの全容を明らかにする論文ではない、ということは、後にサトシ・ナカモト自身が認めているようです（参照）。

ビットコインは、上記の掲示板やら、世界中のコントリビュータが集って、考えて、現在の形にまで持ってきたのだと思います。

ただ、私が、ビットコイン誕生のきっかけとなったこの論文の、（1）リリースされた時期（2009年5月24日）、（2）第7章の「ディスク・スペースの節約」、（3）第11章の「数学的根拠」を眺めているうちに見えてきた風景は ―― **仮想化**でした。

仮想化というのは、超乱暴に言えば、PCの性能が上がりすぎて、そのリソースが持て余されるようになったから、**1台のPCの中に、何台ものPCを作って運用してしまえ**、というものです ―― 今となっては、あたりまえの技術ですが*）。

*）例えば、私の場合なら**こちら**。

ぶっちゃけて言えば、あの頃**コンピュータリソースのインフレ状態が発生していた**、と見ることができます。これは、あくまで私の仮説ですが ―― ビットコインは、**計算リソースのインフレに、うまく乗っかるつもりだった**のではないか、ということです。

WordやExcelの使用時のコンピュータリソースの使用量など知れています。シミュレーション計算とは異なり、CPU消費電力は小さいです。それでも、PCの電源が入れっぱなしの状態では、あまり「節電」の意義はありません。

それなら、WordやExcelで仕事をしているPCのバックエンドで、終日、ビットコインプロトコルを動かしていればいいのです。そうすれば、

（1）PCのリソースの有効活用ができ、
（2）費用対効果の高い省エネ対策にもなり、

(3)ユーザには小金稼ぎのチャンスとなり、
(4)既存の(クソ高い)クレジットサービスの使用料を払う必要もない、

新しい通貨によるネットビジネスが簡単に立ち上げられる世界の誕生 ――

　こんな感じの、「**素晴らしい次世代インターネットビジネスの金融基盤を作る**」という壮大なビジョンがあったのではないかと思うのです。

　しかして、その実体は ――

(1)何の役にも立たない「数当てゲーム」のためだけに、一国の消費電力に相当する電力が使われ続け
(2)将来、流用することもなく、廃棄されることが確定している専用(×汎用)PCが量産され続け、
(3)流通されることなく、自分のサイフの中から出ていかない投機目的の、通貨とは名ばかりの暗号資産が、せっせと製造され続けている

　サトシ・ナカモトなる方が、どのように考えているのかは分かりませんが、もし私がビットコインの発明者であったとしたら、

どーして、こうなったぁーーーーー!?

と、叫び出すだろうなぁ、と思うのです。

「今回は特に言うことありません」

後輩:「**今回は特に言うことありません。大変、良くできていました**」

江端:「おい」

後輩:「いや、本当にそう思うんだから仕方がないでしょう。江端さんは『貨幣や経済のことを知らんくせに』とか言ってディスってくる奴に対抗すべく、貨幣の権力闘争の歴史、クレジット市場のサプライチェーン、知的財産権法から最近の資金決済法に至るまで調べまくって、それでも足りず、ビットコイン論文を読んで、ビットコインのソースのコードレビューをして、半減期のシミュレーションまでやったのけた訳ですよね ―― 「**ビットコインは通貨として信用がない**」の、この一言を言いたいがためだけに」

江端:「結果としてはそういうことになってしまったが、動機が違う。私は、「**ビットコインの通貨としての信用を見つけたかった**」だけだ。第一、私は、ビットコインを貶めたい訳じゃない。普通の通貨として使いたいだけなんだ」

後輩:「で、どうでしたか」

江端:「どうもこうも、今回記載した通りだよ。これ以上、付け加えることは何もない」

後輩:「私は、貨幣というのは「信用」というよりは「信仰」に近いものじゃないかと思うんですよ。ほら、神サマってやつは、ロジックでは説明できないでしょ?」

江端:「そうだな。自分の親と友人と町内の人間が信じている宗教が近くにあれば、信仰はそこから始まるのだろうな。そういう意味では、宗教は『同調圧力』で発生しているのかもしれない」

後輩:「我が国においては「特定宗教への純粋な ―― あるいは熱狂的な ――信仰」というのは、敬遠(あるいはドン引き)される傾向にあるじゃないですか」

江端:「そういえば、そういう感じの人間はあまり見たことがないような気がする」

後輩:「それは、江端さんが悪い*)」

*)詳しくは筆者のブログ

江端:「まあ……そこは、認めてもいい」

後輩:「日本の宗教って、ハロウィンとクリスマスで騒ぎながら、新年には神社に参拝し、葬式には御釈迦様の言葉で説教される、という、**複数の金融商品を組み合わせて作られている金融商品**のようなモノじゃないですか。でも、**それって悪いことですかね?**」

江端:「何が言いたい?」

後輩:「私たちは、キリスト教を信じて、神道を信じて、仏教を信じて、同時に、それらの全てを信じていないのですよ。私たちが、ある宗教や政治や信念で集団を作るのは、同時にその集団を”**全てを完全に信じていないからだ**”とは思いませんか?」

江端:「まあ……思う」

後輩:「貨幣が信用の完了形であるなら、貨幣は世界中に1つだけあれば足ります。そして、その唯一の貨幣は、コンピュータ上で単なる帳簿として管理されれば、それだけで足ります。運用コストは、めちゃくちゃ安くすみますし、トラブルも最小数になるでしょう」

江端:「で?」

後輩:「つまり、貨幣の信用というのは『不信という不純物が含有』することで成立するものなのです。そして、その不信とは人間の感情を反映したものです。そう考えれば、**通貨の本質とは、人間の感情 ーー それもネガティブな方のやつ ーー が具現化したものと考えることができる**と思うんですよ」

江端:「つまり、通貨の信用とは、”1”か”0”かというような単純な二値化で判断されるものではなく、比率であると?」

後輩:「さらに、”主観的なものである”と付け加えましょうか。もし、貨幣の信用を、信仰と同義と考えるなら、ですけどね」

江端:「ならば、この原稿の執筆で、私の「ビットコイン神」に対する信仰……もとい、信用は、0.0000……と、いつまでも0が続きそうなくらい小さくなったなぁ、と思う」

Profile

江端智一(えばた ともいち)

日本の大手総合電機メーカーの主任研究員。1991年に入社。「サンマとサバ」を2種類のセンサーだけで判別するという電子レンジの食品自動判別アルゴリズムの発明を皮切りに、エンジン制御からネットワーク監視、無線ネットワーク、屋内GPS、鉄道システムまで幅広い分野の研究開発に携わる。

意外な視点から繰り出される特許発明には定評が高く、特許権に関して強いこだわりを持つ。特に熾烈(しれつ)を極めた海外特許庁との戦いにおいて、審査官を交代させるまで戦い抜いて特許査定を奪取した話は、今なお伝説として「本人」が語り継いでいる。共同研究のために赴任した米国での2年間の生活では、会話の1割の単語だけを拾って残りの9割を推測し、相手の言っている内容を理解しないで会話を強行するという希少な能力を獲得し、凱旋帰国。

私生活においては、辛辣(しんらつ)な切り口で語られるエッセイをWebサイト「こぼれネット」で発表し続け、カルト的なファンから圧倒的な支持を得ている。また週末には、LANを敷設するために自宅の庭に穴を掘り、侵入検知センサーを設置し、24時間体制のホームセキュリティシステムを構築することを趣味としている。このシステムは現在も拡張を続けており、その完成形態は「本人」も知らない。

本連載の内容は、個人の意見および見解であり、所属する組織を代表したものではありません。