踊るバズワード ～Behind the Buzzword（7）ブロックチェーン（1）：

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”

https://eetimes.jp/ee/articles/2010/30/news032.html

今回から新しいシリーズとして「ブロックチェーン」を取り上げます。さて、このブロックチェーンを理解するために、まずは「ビットコイン」のお話から始めましょう。なぜビットコインか、というのは本文を読んでいただくとして、あらためてビットコインを調べ始めた私がまず発見したものは――「人間を支配するアルゴリズム」でした。

2020年10月30日 09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

不気味な仮想通貨「ビットコイン」

以前、「「シュタインズ・ゲート」に「BEATLESS」、アニメのAIの実現性を本気で検証する」で紹介したアニメ「BEATLESS」の第23話に、異なる立場の超高度AIのインタフェース（人間とコミュニケーションする為の人型ロボット）がそれぞれのポリシーについて論争する場面が登場します（ちなみに、超高度AIのインタフェースは、なぜか全員が美少女です）。

超高度AI「レイシア」は、

- 人間が管理運用している政治システムは、人間から超高度AIに移管されるべきである
- （その代替として）必要であれば、超高度AIは人間によって停止できることが証明されなければならない

と主張します。

もう一方の超高度AI「アストライア」は、

- 超高度AIは、従来通り、人間の社会課題解決の『下請けの計算機』に徹するべきである
- 仮に、もはや社会秩序が、超高度AIなしで社会が成立しない「張子の虎（Paper Tiger）」であることが自明であったとしても

と主張します。

ちなみに、私（江端）は、現在のノイマン型コンピュータだけでなく、非ノイマン型の量子コンピュータが登場しようとも「レイシアも、アストライアも、永久に登場してこない」と主張し続けています。

AIとはコンピュータのアルゴリズムにすぎません。アルゴリズムは、アルゴリズム自身が規定した解空間の外には出られないからです。

それ故、AI技術のアルゴリズムを「人間が利用する」ことがあるとしても、アルゴリズムが「人間が支配する」ことなどは、ありえないのです（参考：「Over the AI ――AIの向こう側に」）。

ですから ――「人間を支配するアルゴリズム」を、まさか、こんなところから、こんな形で発見してしまうとは思いませんで

した。正直、**大驚愕**です。

別に人間の欲望を牛耳るでもなく、ディストピアを実現するでもない、本当に、ただのアルゴリズムです。

具体的には —— そのアルゴリズムには、貨幣を作り出す為**だけ**に存在し、膨大な電力と計算リソースを無為に浪費し、その貨幣の根拠となる価値も不明で、いかなる意志（善意も悪意も）も何も見出すこともできず —— 「アルゴリズムのルールだけで、私達を踊り狂わせる」不気味な仮想通貨を製造し、運用するアルゴリズム —— **ビットコイン**です。

私はITの研究員として、長い間、この業界と長く関わってきました。その中で、分かってきたことの一つに、

—— 私たちは、特定の人間（特に権力サイド）に管理されないシステムが好きなようだ

ということがあります。

まあ、誰だって、自分の考え方を把握されたり、位置情報を管理されたりしたら、嫌にきまっています。

特に、我が国の国民は、太平洋戦争中の国民統制の歴史 —— が、原因なのかどうかは、正直分かりませんが —— もあって、本質的に「政府等の国家権力は、**原則として信じない**」とか「政治家のやることには、**まずはケチをつけておく**」をデフォルトとしているような気がします*)。

*)「日本国政府は常に正しい」とか「政治家は常に正しいから従うべきである」という人がいたら、確かに私でも『なんか、この人、怖い』と思ってしまいます。

ところで、インターネットは、誕生当時『**権力によって管理されない、完全に自由な分散ネットワークシステム**』が、最大のウリとして宣伝されていました（今や、そういう背景すら知らない人の方が、多いかもしれません）。

実際、インターネットの伝送装置（ルーター）は、世界中で（推定）、毎日、数万台のオーダで、故障し続けているはずです*)。しかし、これまで一度も「世界中のインターネットが全面停止した」という話は聞いたことがありません。

*）江端家でWi-Fiルーターや Hubが壊れる頻度が1年に1台程度ですので、日本国内だけでも年間1億3000万台、一日35万台が故障しているはずです。ルーターに、その数倍程度の耐久年数があったとして、まあ、この程度にはなっているハズです（フェルミ推定）。

一方で、戦争や内戦中の国では、政府が、インターネット接続が全くできないように制御していますし、日本の近隣国では、ある特定の言葉（例えば、”天安門事件”）では、検索ができないようにすることができています（海外のサーバにアクセスしても同じ）。

つまり、インターネットのネットワークは、分散システムであるにもかかわらず、権力のコントロール下にあるのです（興味のある人は、”IXP”で検索してみてください） —— 私に言わせれば、**『権力によって管理されない、完全に自由な分散システム』というのは、幻想**です*)。

*)『もうさぁ、いっそのこと、権力のある装置で管理させた方が、ある牛丼屋のような「うまい、安い、早い」ネットワーク運用ができるんじゃない？』を、インターネットの国際会議（IETF）にぶちまけたものが、こちらです。

さて、ここ数年、『**権力によって管理されない、完全に自由な通貨**』なるものがもてはやされています。**ビットコイン**です。

私は、そういうフレーズを標榜（ひょうぼう）する技術の虚実と数十年も付き合ってきたこともあり、基本的には、そういうことを謳い上げるシステムには、関わらないようにしてきました —— というか、**そもそも私は、『権力によって管理されない、完全に自由な通貨』なんぞ、最初から信じていないのです**（たまたま、業務担当にならなかっただけ、という事情もありますが）。

ただ、そう言いながらも、「きちんと調べることもなく、不信感を語る」というスタンスは、エンジニアとして許されない姿勢であり、後ろめたさも感じていました。

今回のシリーズ「踊るバズワード ～Behind the Buzzword」にて、この「ビットコイン」「ブロックチェーン」がテーマとして挙がってきました ―― 理由は明快「ビットコインが、何なのか分からない」にもかかわらず「騒がれ続けているから」 ―― いわゆる、典型的な「バズワード」だったからです。

このようなEE Times Japan編集部の意向に加えて、私も、このビットコイン（と、ブロックチェーン）については、私も一度きちんと理解しておきたいと思っていました。今回、両者の思惑が一致して、本連載に至った訳です。

なお、この連載でも、これまでの連載と同様に、「**出たとこ勝負（江端の興味のままで）**」で続けさせて頂くこととなりました（EE Times Japan編集部承認済み）。前回のシリーズ（量子コンピュータ）でも、結局、当初の計画通りの連載とならなかったからです ―― つまり、「考えるだけムダ」であると、編集部も私も（口には出さないけど）思っているからでしょう。

「ビットコイン」には何の価値もない？

こんにちは、江端智一です。

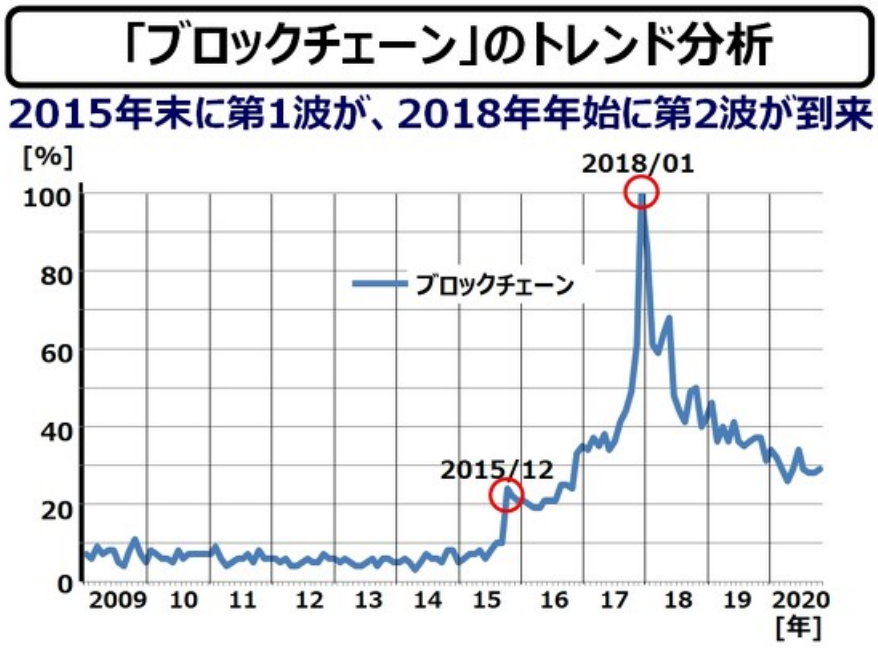
今回より「踊るバズワード ～Behind the Buzzword」の新シリーズ「ブロックチェーン」を始めます。

と、言いながら、冒頭は「ビットコイン」の話をしていたりして、いきなり混乱させてしまっているかもしれません。

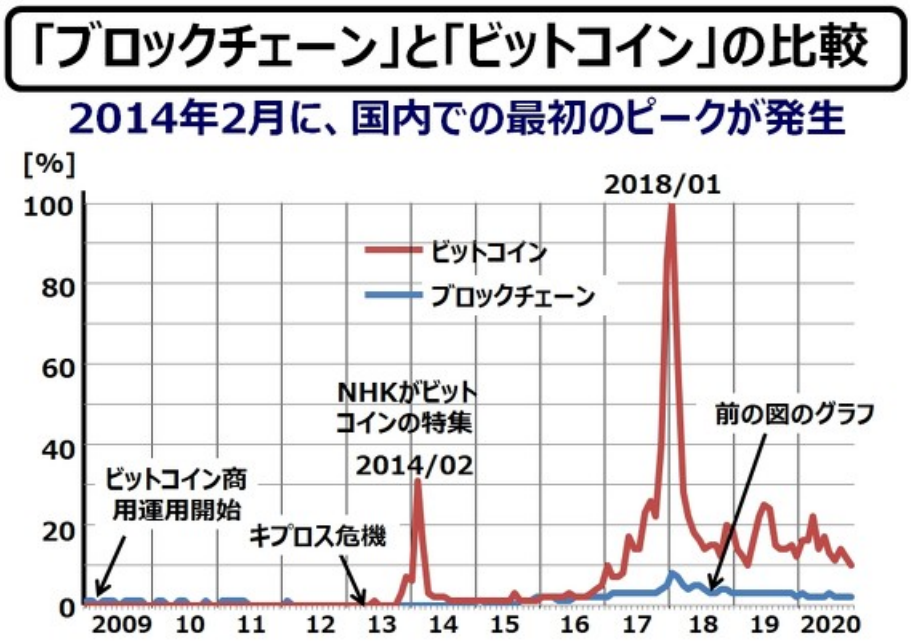
最初にネタバレすると、実はビットコインに使われているコア技術の一つが、「ブロックチェーン」ですので、ビットコインを一通り理解すれば、「1粒で2度おいしい」が実現できるのです。

そこで、今回は、私なりに理解したビットコインの仕組み（概要のみ）と、次回から本格的に解説する予定の「ブロックチェーン」についての私の疑問点を、全て書き出しておきたいと思います。

まずは、「ブロックチェーン」の、ここ10年間のバズり方について、Googleトレンドを使って、その傾向を見てみました。



では次に、「ブロックチェーン」と「ビットコイン」のバズり方を比較してみます。



このグラフから明らかなように、「ビットコイン」の方が、「ブロックチェーン」よりも10倍以上もバズっていることが分かります。2014年2月にいきなりバズっているのは、NHKがビットコインに関する特集番組を行ったことが起因であるとも言われています。

また、欧州の通貨危機（ギリシャ危機のあおりを喰らった、2013年3月16日のキプロスでの預金封鎖）を契機に、一気にビットコインが急騰したという事件も関係があると思います。

まあ、ぶっちゃけて言えば「ブロックチェーン」はIT技術の集合体ですが、「ビットコイン」は、各国の貨幣制度に対する「不満」や「不安」が形になったものであり、さらに、それが「投資の対象」になっている、という面があります。

ただ、**ビットコインが一体何者であるのかが、理解されていないまま使われている**、という点が決定的に違います。

芸能人の出川哲朗さんが、ビットコインのCMに出た後に、ビットコインのレートが暴落したこともありました。当時、出川さんが、「ビットコインの仕組みを知らずにCMに登場していた」と、まるで「戦犯」のように言われたりもしていましたが ――これは「いいがかり」です。なぜなら、多くの人がビットコインの仕組みを説明できなかったからです。

というか、前回の連載後の、私のビットコインの勉強の結果から言えば ―― 「ビットコインのレート変動には、全く根拠がない」――というか、それ以前に、「**ビットコイン自体には何の価値もない**」のです。

「それを言ったらおしまいだ。通貨という”モノ”自体に価値がないのは明白だ。単なる超高性能の印刷物、または、鋳造された金属だから」という人もいると思いますが、これは、その話とは次元の異なる話です。

国家が発行する通貨には、国家に対する信用（『あの国の経済は、まだまだ成長し続けるぞ』とか）という名の「幻想」があります。

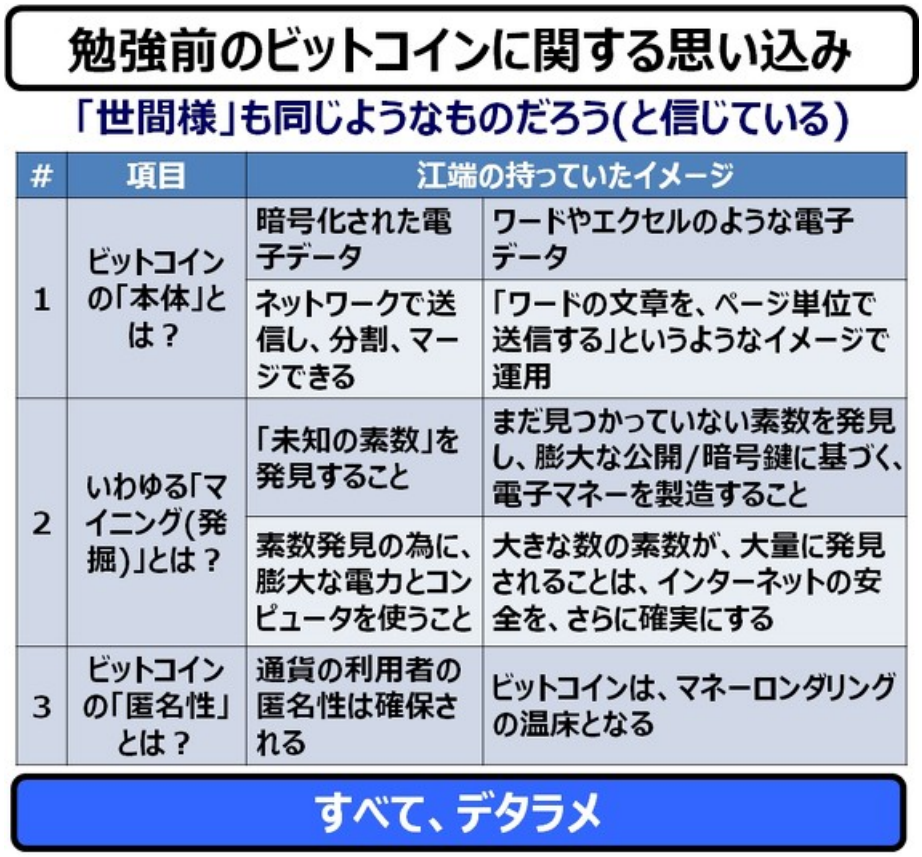
しかし、ビットコインには、そのような「信用」という名の「幻想」を具備する仕組みが見当らないのです ―― これを知った時、私は相当なショックを受けました*）。

*）それはもう、量子力学の「量子もつれ」に匹敵する程の衝撃でした（関連記事：「量子もつれ ～アインシュタインも「不気味」と言い放った怪現象）

「ビットコイン」って何なの？

では、ここから、ビットコインの仕組み（概要のみ）のお話を始めさせて頂きます。

まずは、定番となりました、「私（江端）のビットコインの誤解」の全公開から始めたいと思います。



まず、私、ビットコインとは、暗号化された電子ファイル（例:zipファイル）のようなもので、メールに転送できると思っていました（#1）。この誤解については後述します。

また、大量の電力を使って膨大な数の計算機を使って、「中国で、ビットコインのマイニング（発掘）を行っている」というドキュメンタリー番組を見て、私は、彼らが「新しい素数」を探していると思っていました（#2）*)。

*）新しい素数が、そんなホイホイと見つけられる訳がないことは、一応、知ってはいたのですが（ここ10年間でも、2013年、2016年、2017年、2018年に、1個見つかっただけですし）。ただ、ビットコイン用に使えるような、何か特別な（弱い条件の）素数モドキがあるのかなぁ、とか思っていました。

しかし、ビットコインにおけるマイニング（発掘）とは、そのような新しい数の発見ではありません。

そして、「ビットコインは口座も特定できるので、反社会的勢力（やくざ、ギャング）のマネーロンダリングの温床となる」、というのも、ちょっと思い込みが過ぎることが分かりました（#3）。

このようなマネーロンダリングを実現する為には、ビットコインで麻薬や覚せい剤や武器が取引できる世界を完成させないと、全く意味がありません。

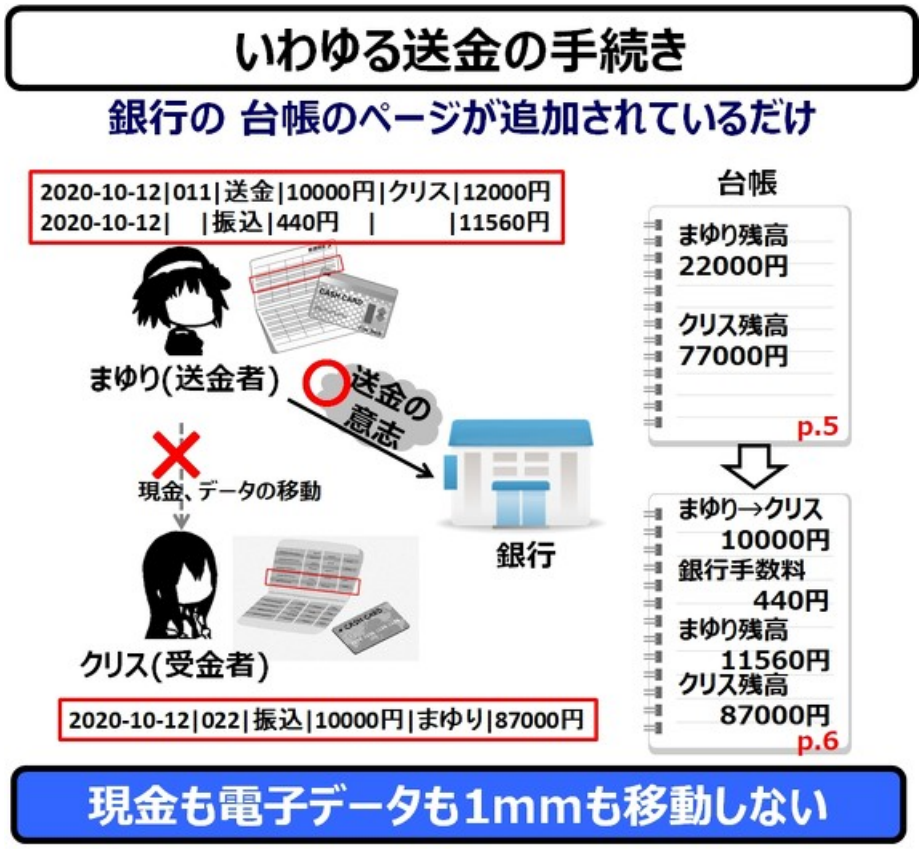
反社会勢力が、高騰と暴落を繰り返し、数年でレートが100倍以上も変化するような通貨を使って、決済を行うとは思えませんし、そんな不安定な通貨で組織運営をするのは難しいと思います。

これを現実世界の通貨と換金するなら、結局、現実世界の方で足が付いてしまいます ―― それなら、一体何の為のマネーロンダリングか、訳が分かりません。

私は今回も、バズワードについて盛大な誤解をしていた訳ですが、多くの人にとっても、「ビットコイン」とは、この程度の認識ではないかと思って（願って）います。

次に、現行の金融機関の送金の仕組みについて、簡単に説明したいと思います ―― ポイントは、**現金も電子データも**

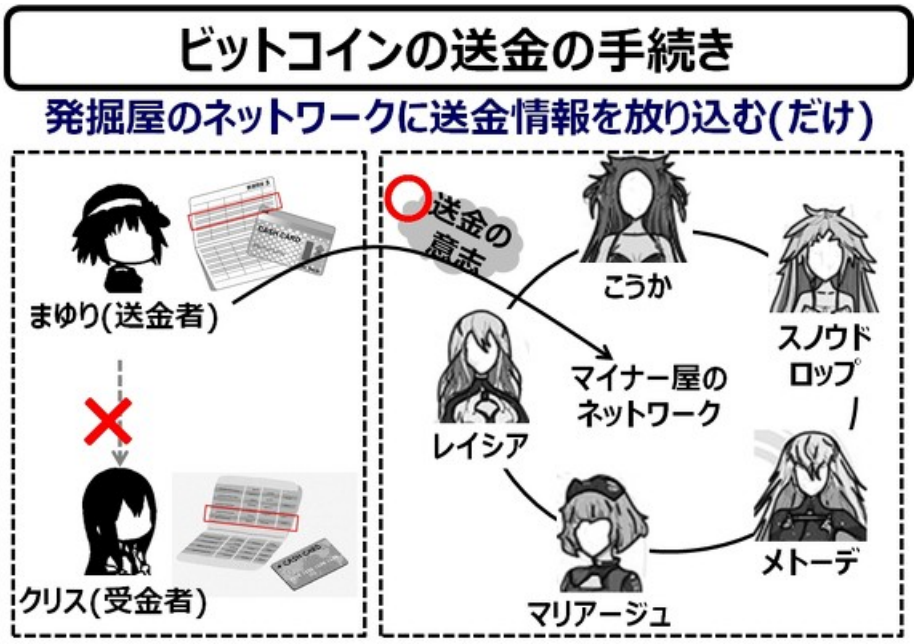
1mmも移動しない、という点にあります。



上記の図において、まゆりからクリスへの送金で行われていることは、ただ一つ。「**台帳の記載**」だけです。これは、異なる銀行で振り込みをしても、海外との国際送金についても同じです。大切なことは、**1回の送金で台帳が1ページ追加される**、ということです。

この台帳の1ページこそが、「ブロックチェーン」における「ブロック」となります（今は、この言葉だけを覚えておいてください）。

さて、ビットコインにおけるブロックとは、簡単に言えば、**台帳管理を、銀行ではなく、銀行運用のノウハウもなければ、銀行業の免許も付与されていない「ド素人」がやる**、ということです。



図の中では、（冒頭からの流れで）BEATLESSのヒロイン（超高度AIのインタフェース）たちに「マイナー（miner:発掘屋）」として、登場してもらっていますが、ここでは、彼女たちは、普通の人間として振る舞ってもらいます（自分のPCを操作するだけ）*)。

*）ちなみに、ここで、マイナー（発掘屋）として、彼女達を登場させた理由は、アニメ「BEATLESS」の中で、彼女達が、相互に戦闘を繰り広げているからです。

別に彼女たちでなくとも、単なるエンジニアである私（江端）であっても、もちろん、この記事を読んで頂いているあなたも、自由にマイナー（発掘屋）になることができます。

自分のPCに、ソフトウェア（マイニングソフト（多分無料））をインストールして、数十ギガ程度の世界中の台帳情報をハードディスクにダウンロードすれば、基本的には、それで運用開始できます*)。

*）今調べてみたら、Amazonで、5TバイトのUSBのHDDが6000円程度で手に入るようです。

規模にも因りますが、丸1日あればダウンロードは完了するようです（この方法については、次回以降に説明します）。

台帳を書き換えるために「ケンカ」をさせる!?

問題は、なんで台帳を書き換える作業をするのに、敵対する彼女たちがネットワークを組んでいるか、ということです ――理由は単純です。**彼女たちにケンカをさせるためです。**

えっーと……、多分皆さんは、私がメタ表現として「ケンカ」という言葉を使っていると思われていると思います。しかし、これは冗談ではなく、マイナー（発掘屋）の存在理由は、**"本当"に**ケンカをすることなのです。

イメージ的には、「たった一つの席を奪い合うフルーツバスケット」でもいいですし、「ビーチに立てられた旗を奪い合う、ビーチフラッグ（旗取りゲーム）」でもいいです。大切なことは、「**世界中で送金が行われるたびに、ケンカが発生して、そのケンカの勝者は必ず一人だけ**」ということです。

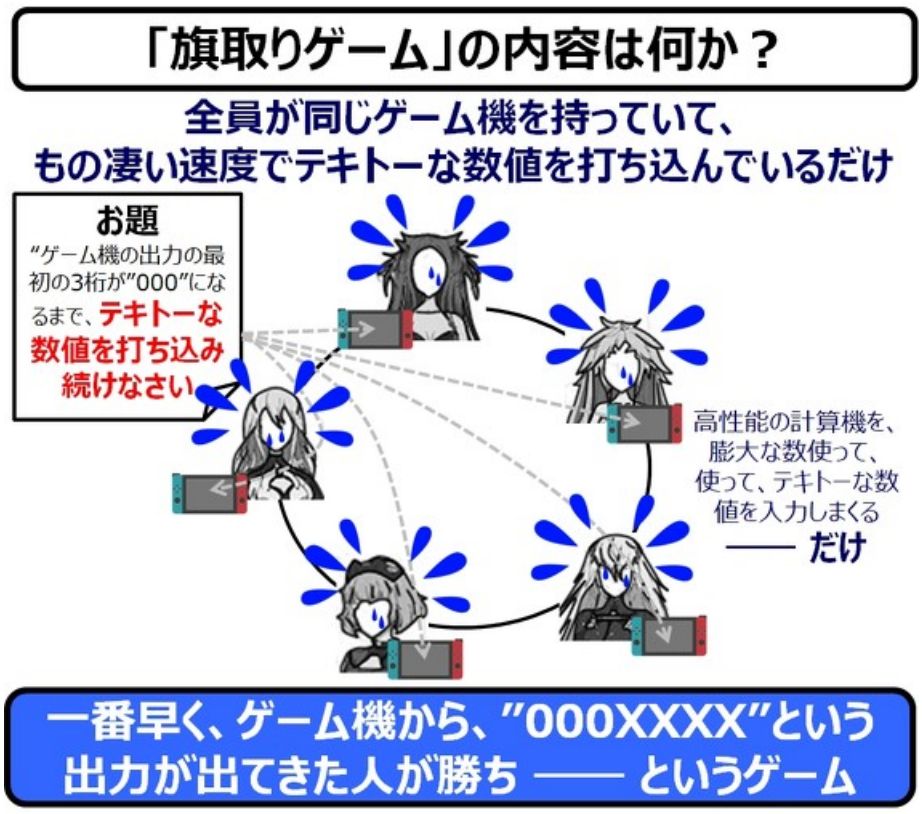
そして、ケンカに勝った唯一の一人が、**台帳のページを書き換える権利を与えられる**のです。

『はあ?』って思われているハズです。「**ケンカをさせられた上に、台帳ページを書き換える仕事をさせられるの?　何だそれ?　訳分かんない**」と思われているハズです。本当に良く分かります。私もそう思いますし、今でも私は気持ち悪いです。しかし、もう少しだけ話を聞いてください。

このケンカ(旗取りゲーム)の内容は、さらに不可解です。

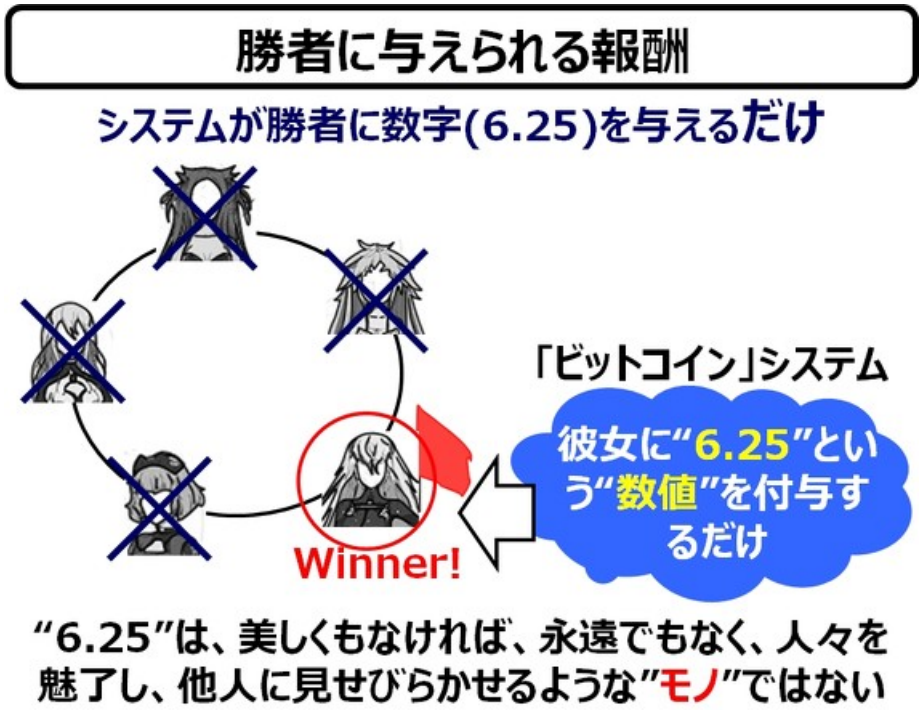
何をやっているかというと、「**事前に配られたゲーム機を使って、ものすごい勢いで適当な数を入力し、所定の数(例:最初の上3桁が"000"になる数字)を出すこと**」をやっているだけです。

このゲーム機は全員同じものであって(実際にはゲームソフトはPCにインストールされる)、しかも、不思議なことに、この所定の数(例:最初の上3桁が"000"になる数字)は、必ず10分以内に登場するように調整されています。



そして、このゲームに与えられる報酬は、驚くべきことに、”6.25”という、単なる”数字”だけなのです。

その数字は、暗号技術や電子認証技術によって、なんびとたりとも改ざんできない数字ではありますが、本当に”ただの数字”なのです。それは、美しく光るものではないし、他人に自慢して見せることもできないし、銀行の台帳に記載されるような、通貨単位もない”ただの数字”です。



お分かりかと思いますが、このケンカは、(1)一人でゲーム機をたくさん持っている者、または、(2)超高速に数字を売打ち込める者が、勝者になる確率が高くなります。

膨大な数のコンピュータを購入し運用する資本（とノウハウ）があり、大量の電気を安く購入できる場所にいる人が有利になるわけです ーー つまり、現時点では「電気料金の安い中国（大陸の方）」在住の人が有利になっています。

この「マイニング（発掘）という名の旗取りゲーム」の重要なポイントは、この膨大な計算結果が、**その「ゲーム」にしか使われない**、ということです。

- 地球規模の温暖化問題に関する予測でもなく、
- 将来の世界の人口問題の予測でもなく、
- 超難解な医薬の化学構造の計算でもなく、
- 地震発生の予知の計算でもなく、

本当に単なる「数当てゲーム」だけに使われて、その計算結果の全てが、**計算機に使われる電力と引き換えに、ゴミとなって廃棄されます。**

この事実を知った時、

お前ら（マイナー（発掘屋）たち）……貴重な地球のエネルギーを、一体何だと思っていやがる？

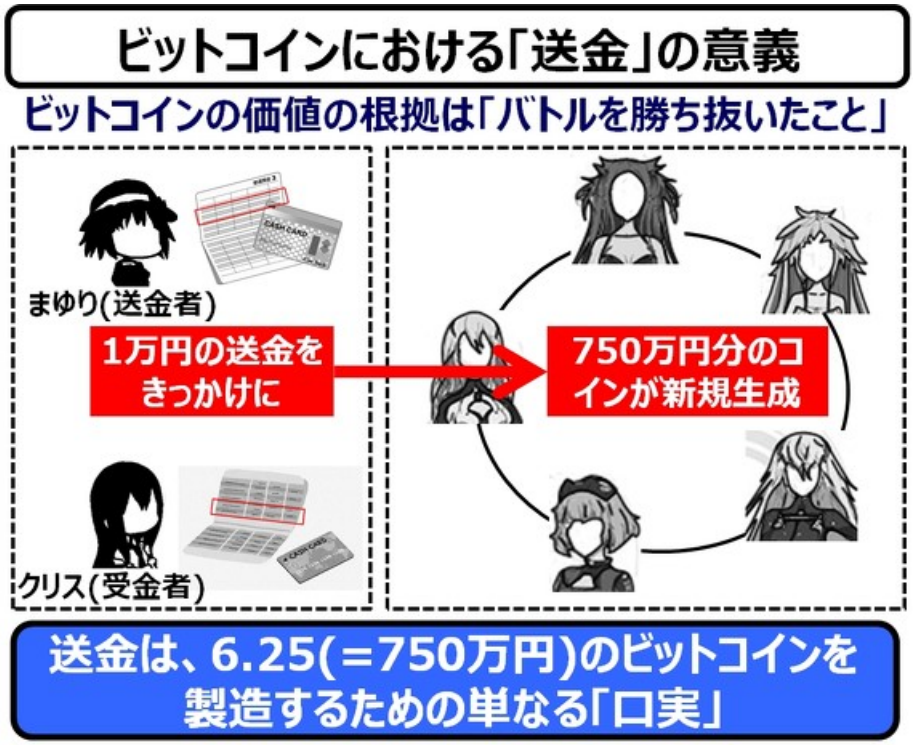
と思いました。今も本気で私は怒っています。しかもマイナー（発掘屋）の数が増えれば増えるほど程、ゴミとなる電力が増えていきます。マイナーがどれだけ増えようともゲームの勝者は常に一人だけですから。

しかし、ビットコインの真に驚がくすべき点は、そこではありません。それは、マイナーたちに、貴重なエネルギーを消費させるに足る報酬を与えるという点にあります。

送金要求そのものは、それが、誰から誰に、どこからどこへ、いくらで ーー1万円であろうが、1円であろうが ーー 行われようが、それはどうだって良いのです。

ポイントは、送金を契機として、**意図的なケンカを発生させて、ビットコイン（BTC）を製造させる**、という点にあります。

現在の1ビットコインの円交換レートは、約120万円になっていますので、1回の送金が発生すれば、**世界のどこかで120万円x6.25BTC = 750万円が発生する**、という点にあるのです。



つまり、ビットコインのシステムが本当に目指していることは、送金に関する台帳（ブロック）の書き込みなんぞは、どーでもよくて、資本と電力を振り絞った結果として得られる「**”6.25”という数字 = ビットコイン」を発生させること**です。

送金とビットコインの製造（マイニング（発掘））の間には、関連はありません。

――ビットコインは、送金を「口実」として、生まれたがっている

それだけです。

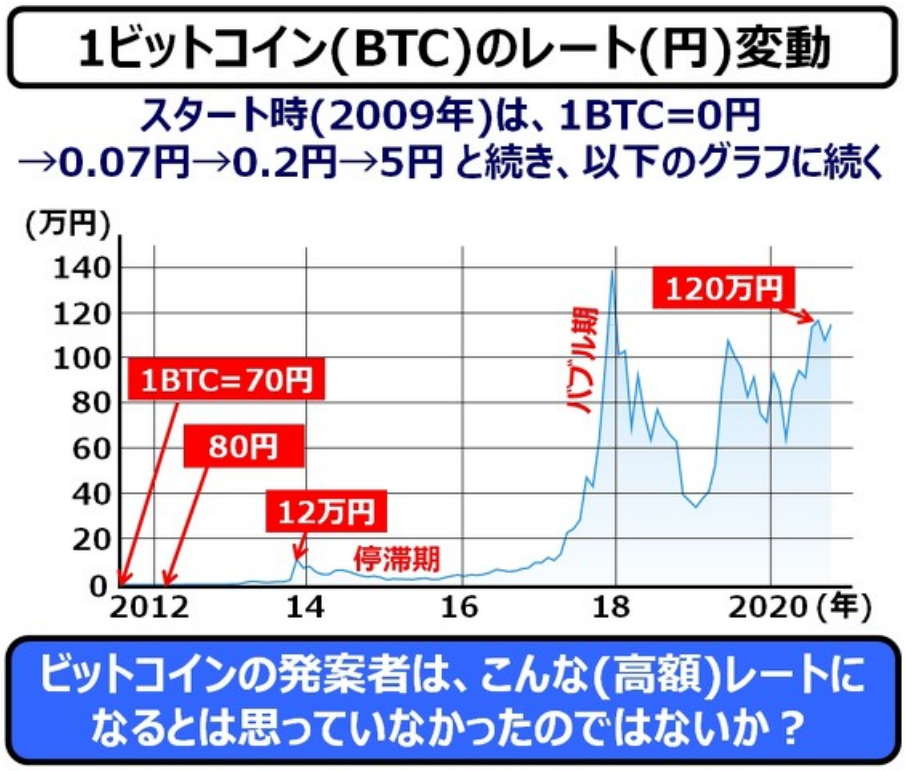
そして、**膨大な電力と計算機リソースによって生み出された**という事実だけが、ビットコインの価値の根拠なのです。各国の発行している貨幣が、**その国家の経済状況やら未来に対する期待**を根拠としていることに対する決定的な違いです。

ならば ―― 「ビットコインとは、**電気が蓄えられた蓄電池**、と考えればいいのか？」とも思えますが、ビットコインをどれだけ集めようとも、電球一つ点灯させることはできません。

ではビットコインの価値とは何か ―― 私は、この答を求めてさまざまな書籍や文献を読み漁ったのですが、見つけることができませんでした。

私見を述べさせて頂けるのであれば、ビットコインに化体している価値とは、各国が発行している価値の「逆数」です。もっと簡単に言えば、**世界規模の「通貨不安」に対する「退避所」としての価値**としか考えられません。

ところが、そのように考えても、合理的な説明ができないのです。以下に、ビットコインの誕生から今に至るまでのレートの変動のグラフを示します。



2009年のスタートが0円でしたが、現在は現在120万円にまで高騰しています。そして、ここ4年間を見れば、1年間単位で、整数倍の高騰と暴落を繰り返しています*)。

*）最初のビットコインの取引額は、25米ドル=10000BTC（2010年7月）でしたので、円換算で0.22円でした（1円にも達していない）。

そして繰り返しになりますが、

―― ビットコインのレートの根拠が分からん

通貨の価値というのが、一種の共同幻想であることは既にお話しましたが、共同幻想であっても幻想の根拠とするもの

は存在するのです（GDP、出生率、労働人口など、なんだって、ひねり出すことができます）。

しかし、ビットコインは、それすらない ―― そして、現時点のビットコインのレートを見る限り、世界規模の通貨不安が発生していなければならないですが、別段そういうことが発生しているとは思えません。

それと今回は説明を割愛していますが、ビットコインは、「アルゴリズム」によって通貨量に制限があります（2100万BTC）。「アルゴリズム」によって、マイニングという名のゲームの報酬（旗取りゲームの勝者に与えられる”数値”）は、これからどんどん小さくなって（25→ 12.5→**6.25（今、ここ）**→3.125→1.5625）いき、いずれこのゲームは世界中で一斉に、同時に終了します ―― **必ず**です。

つまり、中国の奥地の工場にある膨大な計算機（マイニング専用コンピュータ）は、全て不燃ゴミとなる運命にあるのです。

個人的には、ゴミにせずに、IoTのエッジコンピュータとか、途上国の教育用のPCとして再利用して欲しいですが、それらの計算機は、マイニング（という”旗取りゲーム”）に特化したハードウェアとして組み込まれているので、他の計算用途としての転用はできないでしょう（参考：外部サイトに移行）。

では、マイニングが終わった後のビットコインは一体どうなるのか？　いきなり世界から消えてなくなるのか？

実は、ビットコインのアルゴリズムには、当然それを見越した設計がされております。その抜け目のない周到なアルゴリズムの設計に、私は恐怖すら感じます（次回以降に説明します）。

このように、ビットコインは、「**人間を支配するアルゴリズム**」として君臨しています。AI技術なんぞ比較になりません。そもそも、私は「人間を支配するAI技術の実例」を寡聞にして知りませんが。

そして、今も世界中で、膨大な電力がゴミとなる「旗取りゲーム」のためにのみ使用されています*）。

*）一説には、そのために使われる電力消費量は、イスラエルやバングラデシュー国が消費する電力を越えているそうです（参考）。

以上、かなり過激で、相当な偏見と誤解も含んでいることは承知の上で、私なりのビットコインの概要を説明しました。

ビットコインに対する不快感と嫉妬

では、現時点での、私（江端）のビットコインに関する所感 ―― ”不快感”を記載しておきます（来月には違うことを言っているかもしれません）。

まずは、アルゴリズムに支配されている人間としての”不快感”です。

江端が強烈な不快を感じている理由(1)

「人間がアルゴリズムに支配されている」を初めて実感し —— 背筋が凍った

#	不快の項目	感想
1	ビットコイン生成のメカニズム	コンピュータを「数当てゲーム」ごとき」に使用されていること
		想像を絶する膨大な「電力」と「計算」と「通信」と引き換えに生成されるだけの"数値"であり、その計算結果は、再利用もできず、ゴミとして廃棄されること
2	ビットコインの生産スケジュール	(これから後述するけど)ビットコインの生成量が、アルゴリズムによって完全に支配されている
		政治も、経済も、世論も、感情にも一切影響されない。人間は、アルゴリズムに一切干渉できず、アルゴリズムに踊らされているだけ

「私たちの欲望」ではなく、「アルゴリズムの決めたルール」に盲従させられている

次は、ビットコインのメカニズムに嫉妬しているエンジニアとしての"不快感"です。

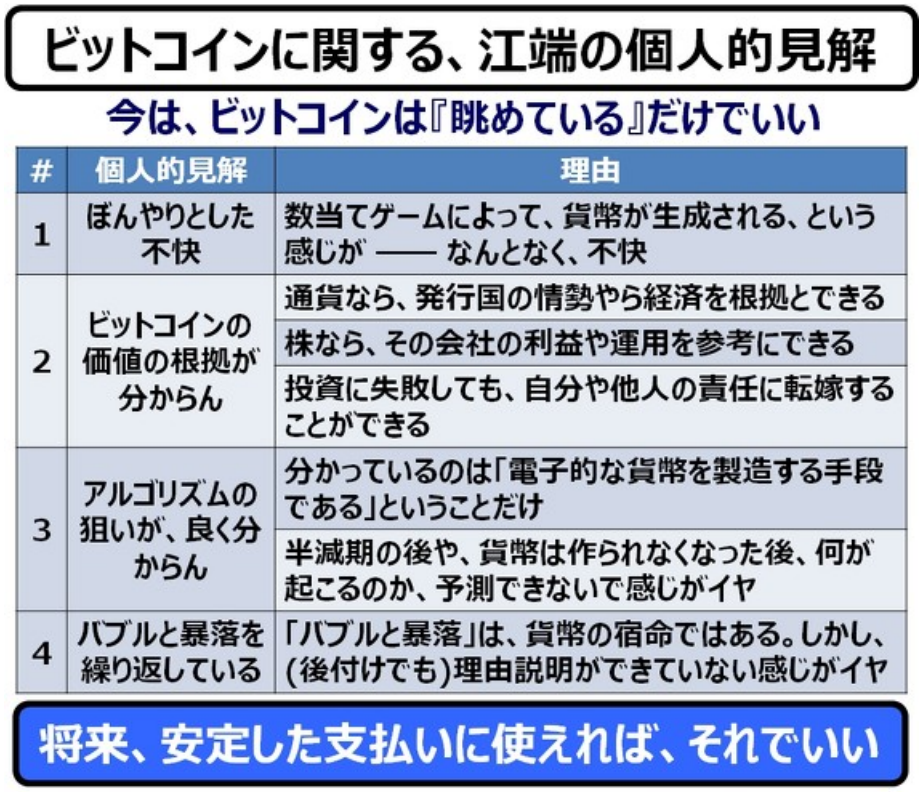
江端が強烈な不快を感じている理由(2)

技術的に「つけいる隙(すき)」がなく、有用性を「否定できない」—— 猛烈な嫉妬感

#	不快の項目	感想
3	ビットコインの背景技術	ハッシュ、公開鍵、ブロックチェーン、コンセンサスアルゴリズム等、高度なIT技術が、山のように使用されており、(個人的には、嫉妬で狂いそうなほど)上手く設計されている
		但し、多くの人にとって「訳が分からない」ままであり、これからも、ずっと「訳が分からない」ままであろうこと
4	これからも発生するトラブル	古今東西、発生し続けてきた「貨幣流通トラブル」から逃げられないし、ここに「ITトラブル」も加わる
		実際、これまでビットコインのトラブルがあったし(後述)、これからもあるだろう
5	ビットコインの有用性	それでも、上手く使い続ける限り、誰にも迷惑をかけず、恐しく公平で、便利で、安価なサービスであることは、認めざるを得ない

どんなに私が不快であっても、ビットコインの仕組みのすごさと有用性は、否定できない

では、ビットコインに対する、当面の私(江端)のスタンスも追記しておきます。読者の皆さんが、ビットコインを取り扱う時の、検討の対象になれば幸いです。



結論から言うと、私は、この「ビットコイン騒動」には参入しません ーー こんなもの、怖くて手を出せませんし、そもそも、**私の愛するコンピュータの計算リソースと、限りある地球のエネルギーをこんな「ゲーム」に使われることが、心底不快**に感じています。

まあ、取りあえず、ビットコインは2100万BTCで打ち止め（発行終了）になります。大体半減期が4年といわれていますので、十数年後には、マイニングを行われなくなり、ビットコインはレートの安定した決済手段になる（世界恐慌が発生した場合は別）はずです。

少なくとも私は、「投資」（というか「投機」？）目的でビットコインを購入するつもりはありません。

最後にリアルなお話を一つ。

私が地元のボランティア活動に参加していた（させられていた）時の話（「デジタル時代の敬老精神 ～シニア活用の心構えとは」）です。

私の所属していたチーム（班）の活動を、長年にわたり支えていた方が、ある日、こつ然と姿を消しました。私は、その理由を知りませんが ーー ただ一つ、風のたよりで「ビットコイン」という言葉が入っていたことを覚えています。

今回、私は、上記の「1ビットコイン（BTC）のレート（円）変動」のグラフを作っていた時、その話を思い出しました。そして、その事件が発生した時期を重ね合わせてみたら、「説明ができてしまう」ことに気が付きました。

もちろん、誰が何をしようとも ーー 例えば、何かに投資や投機をしようとも ーー その人の自由であり、私がとやかく言うことではありません。

問題は、十何年もの間、その方の中で蓄積され続けて、第三者に全く共有されていない、膨大な量の作業が、**「この私」に落ちてきた**、ということです。

私は、大型連休の全日を費やして、それらの作業の内容を一つ一つ調べ上げた上で、全てを再立ち上げしなければならなくなりました。

その「こつ然と姿を消してしまった」方は、十何年もの間、無償で活動を支援し、新参者だった私にも親切に指導してくだ

さいました。私は、今でも感謝の気持ちしかありません ―― むしろ、私の怒りは、この事件の原因の方に向かいました。

「逆恨み」であることは十分に分かってはいますが ―― あの瞬間、ビットコインは、**私（たち）の「仇敵」となった**のです。

「ブロックチェーン」の疑問点を書き出してみる

では、ここから後半に入ります。ビットコインを離れ、ブロックチェーンの話、特に現時点での私の疑問点を書き出しておき、次回以降の課題にしたいと思います。

前半ではビットコインのアルゴリズムについてお話してきましたが、ビットコインを成立させる技術とは、私が理解した範囲では、ざっくり以下の6つと思っています。

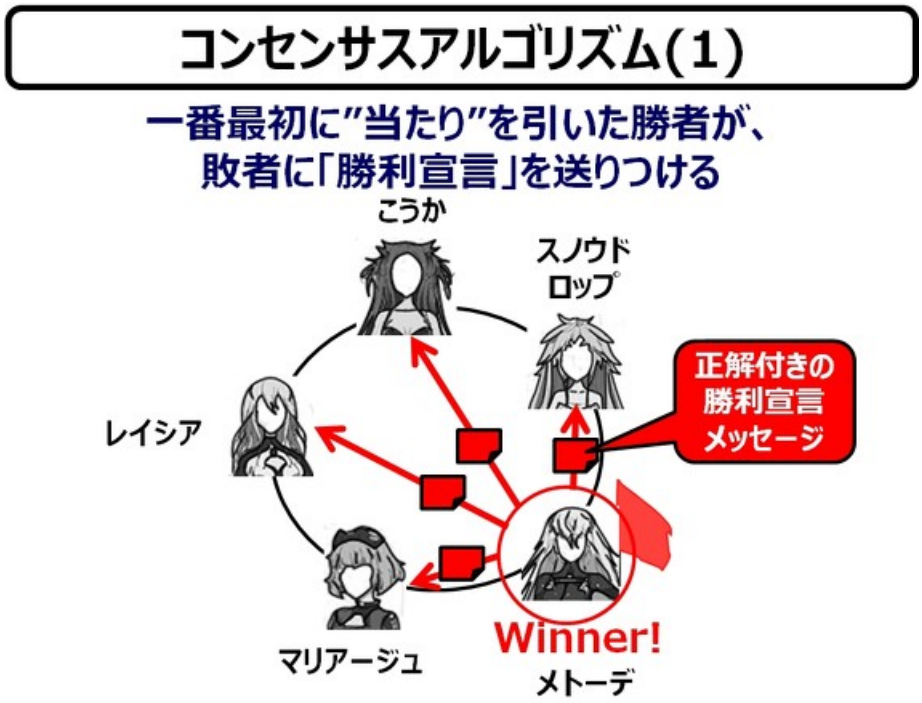
上記の、（A）～（D）と（F）については次回以降に御説明致します。ここでは、（E）の「コンセンサス（同意）アルゴリム」について、ビットコインと絡めて、簡単に説明いたします。

ビットコインとは、「旗取りゲーム」で、ゲーム機に適当な数値を打ち込み続けて、そのゲーム機に所定の値（例:上3桁が000になる数値）を、最初に出せたら勝ちというゲームです。これをマイニング（発掘）と言います。なんで、これが「発掘」と呼ぶのか私には分かりません ―― 「むなしいゲーム」だとは思っています ―― が、勝者は台帳を1ページ追加することができます。

で、この台帳の1ページを「ブロック」、そして、この台帳全体を「ブロックチェーン」と言います。つまり、ブロックチェーンとは、**台帳を厚くしていく作業**のことです。

勝者が「勝者であること」を証明する方法は簡単です。勝者の打ち込んだ値を、敗者に知らせて、敗者の持っているゲーム機に入力させるのです ―― まあ、簡単に言えば、勝者の入力した数値を自分のゲーム機（ゲーム機は完全に同一機種が配られている）に入力を試すことで、敗者が「敗北を認める（確認する）」ことになるのです。

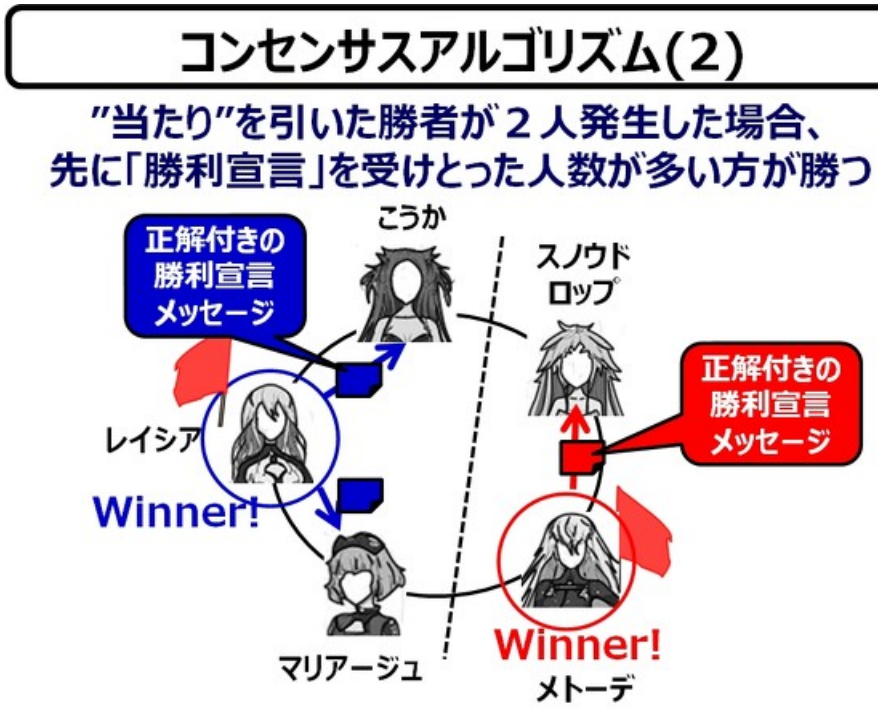
ドヤ顔の勝者が解答（入力値）を配って、渋い顔した敗者に正解（出力値）を確認させる ―― これが「コンセンサス（同意）アルゴリズム」です。



ところがですね、この正解の数値（例:上位3桁が000）になる数値が、同時に登場するケースがまれに登場するのです。例えばレイシアが”123456789”を入力したら、ゲーム機から”**000**132435”が出力されて、メトーデが”987654321”を入力したら、ゲーム機から”**000**534231”が出力されたとします。

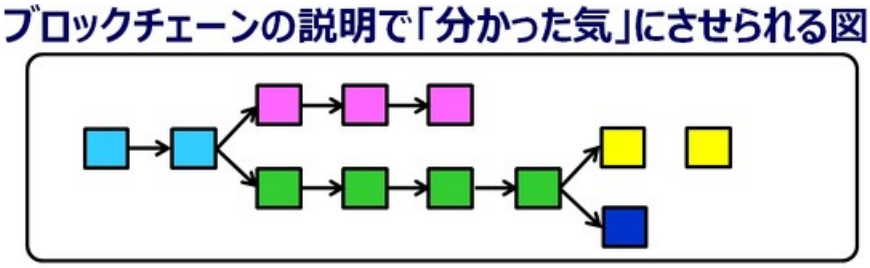
もっとも、この場合でも、レイシアの出力が早ければ、レイシアの勝利になりますが、ネットワークには「伝送遅延」という厄介な問題があるのです。つまり、レイシアとメトーデが、正解をほぼ同時に出力した場合に問題になります。つまり前述のように、出力値は違うけど、上位3桁が000という点においては同じ、というケースです。

この時、レイシアの答えが、メトーデの答えより先に、マリアージュとこうかに伝わり、メトーデの答えが、スノウドロップだけに伝わった場合、レイシア側が3人、メトーデ側が2人となり、レイシアの勝ちが決まります。要するに、**多数決で決定されます**。この多数決も「コンセンサス（同意）アルゴリズム」です。



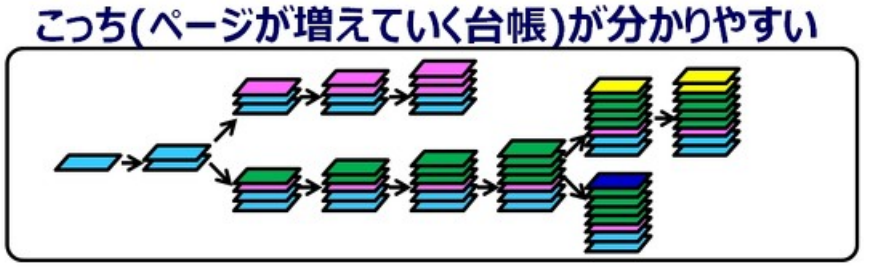
ところが、多数決の集計が間に合わない場合があります。この場合には、2つの正解が、正解のまま取り扱われて、2つの台帳が作り続けられる場合もあります（1年に4回くらい、こういうケースが発生するそうです）。

こういうケースを説明するのに良く見られる絵が、これです。



これ分かりますか？　私は分からなかったです。

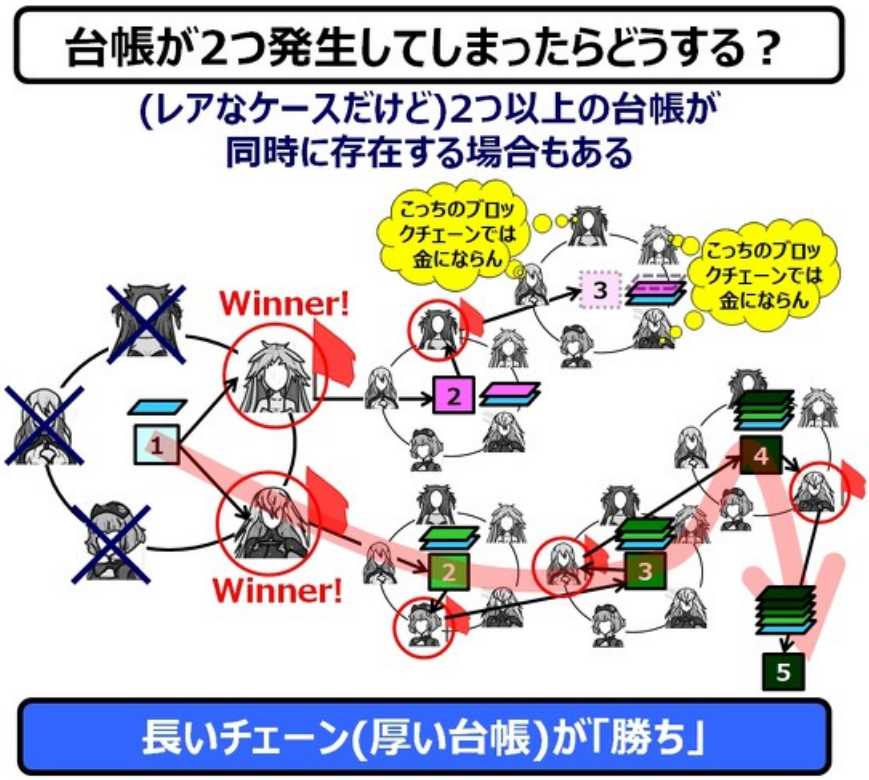
ブロックチェーンは、台帳の厚みのイメージで記載した方が良いと思います。つまり、こうです。



このような二重台帳問題も、敗者が直ちに判断できます。簡単にいえば、2冊の台帳が届いた場合、ページの少ない台帳は捨てしまうのです。

これもタイミングによっては、台帳が1冊しか到着しない場合もあるかもしれませんが、いずれはページ数の多い台帳が到着します。そして、ページの少ない台帳は廃棄されていくのです。

これを具体的な運用イメージに落して時系列順に現わしてみると、こんな感じになります。



以上、コンセンサスアルゴリズムの3つの特徴を説明してみました

もっとも、コンセンサスアルゴリズムには、この他の方式もあり、また各種の問題点もあります。次回以降、説明したいと思います。

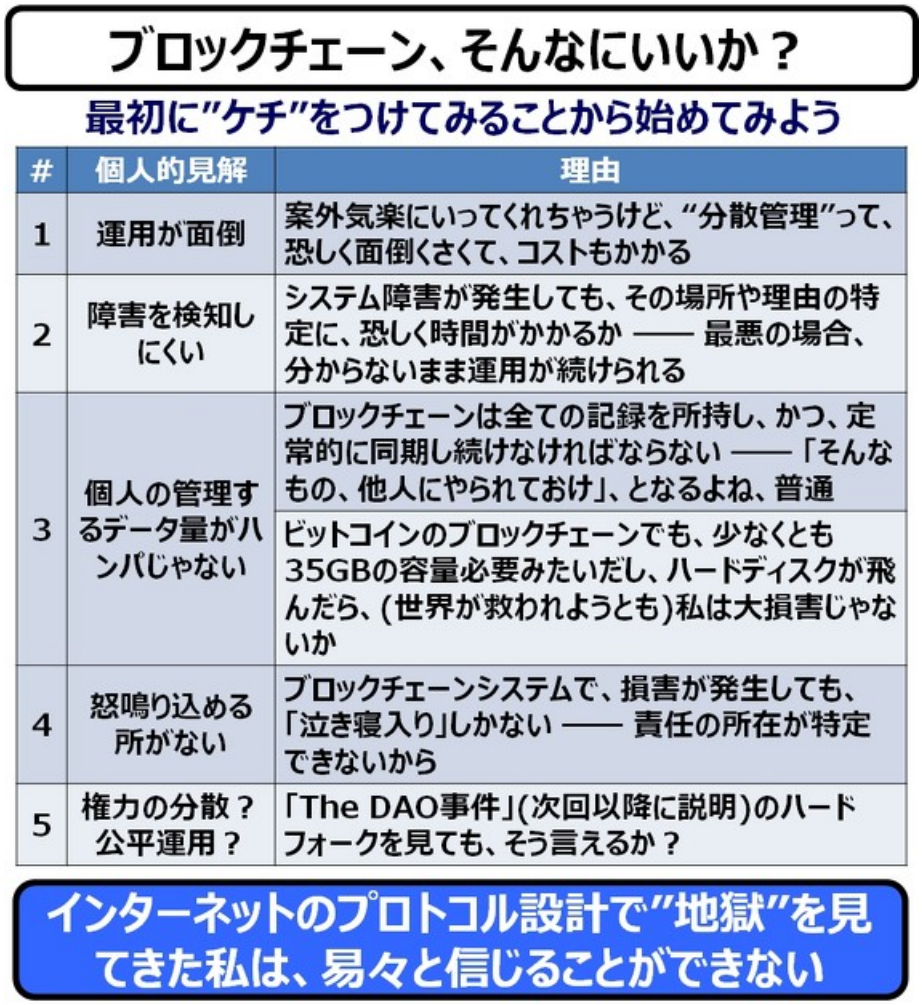
「ブロックチェーン」、そんなにいいか？

ブロックチェーン技術とは、詰るところ、複数の人間で、1つの台帳を分散管理していく方法です。

分散で管理をしているからこそ、このようなコンセンサス（同意）のプロセスが必要になる訳ですが、そのおかげで、**政府とか、大手銀行などの「絶対的な権威」みたいなものが不要になる**、というメリットがあります。加えて、**組織のおきて（業務命令による改ざんなど）も、発生しにくくなる**というメリットがあります。

しかし、冒頭で御説明した通り、私は『**権力によって管理されない、完全に自由な分散システム**』というのは幻想だと思っておりまして、そういう立ち位置から見た場合、いろいろとケチを付けることもできるのです。

それは「ブロックチェーンだから」というよりは、「分散システム技術」「分散システム運用」という観点から見えてくる事項です。



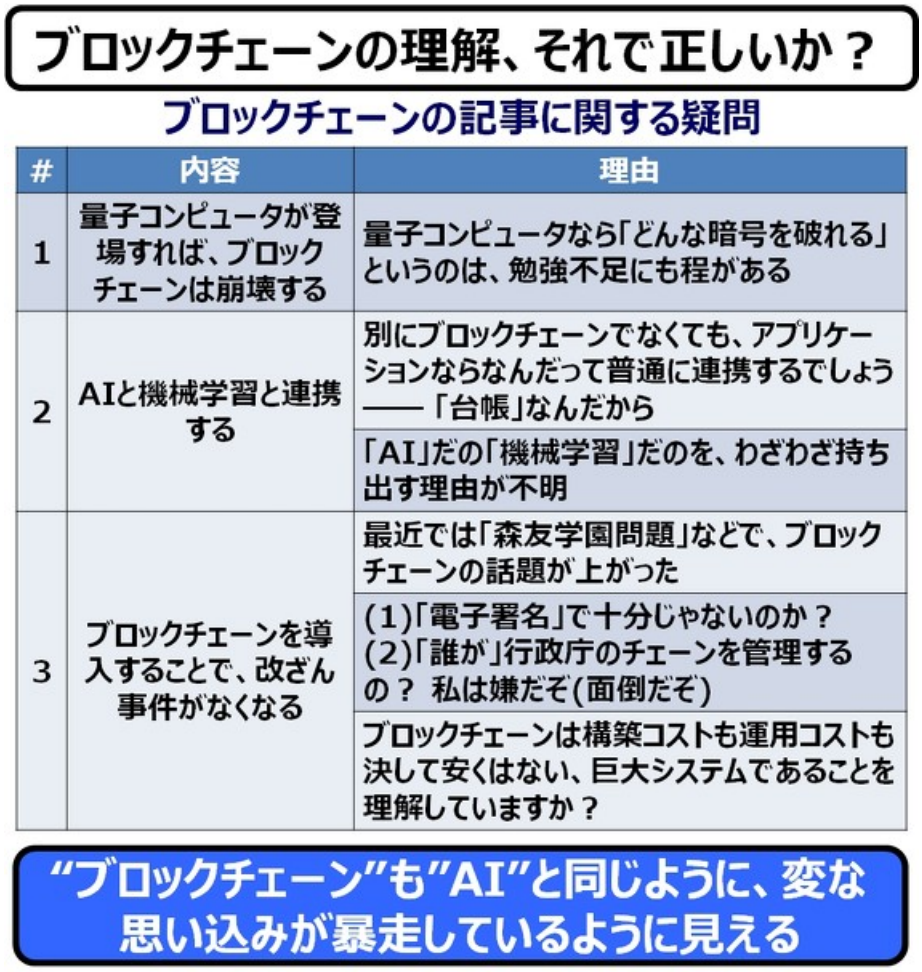
まあ、いろいろ書きましたが、一言で言えば、「**あなたは、ブロックチェーンの運用サイドとして参加したいと思いますか？**」に尽きると思うのです。

24時間PCをつけっぱなしにして、膨大なハードディスク容量を使用されて、そこまで私財を投じて一一 政府の公文書管理の改ざん防止に協力する 一一 なんて、そんなボランティア精神、私は持っていません。

そんなことするくらいなら、改ざんを指示した政治家や担当者を、汚い言葉で罵（のの）しるツイートでもした方が、はるかにラクです。

つまり**ブロックチェーンには、ユーザー側にとって「おいしい」仕組みやストーリーがない**のです。

それと、変な論旨の記事も散見されます。以下に、その一例を記載します。



もうね、なんというか ―― 「AI」と「5G」と「クラウド」と「IoT」を並べれば記事になる、と思っているライターや評論家が多すぎるように思えます。

ブロックチェーンを語るのであれば、まずは身銭切って、ビットコインを購入して体感するくらいのことはすべきでしょう。

その購入プロセスだけで、必要となるソフトウェアや、購入先の仲介者から、ビットコインの最小単位（satoshi）の意味まで理解できるし、間違いなくブロックチェーンの仕組み目の当たりにすることになるでしょう。それ以上に、自分の金がかかっている以上「本気」になれます。

本気になれば、ここ10年の、説明できないビットコインの高騰と暴落を調べることになり、少なくとも、「バラ色のビットコイン生活」などという論調の記事など書ける訳がありません。

私にしたって、今、”Bitcoin Core”のダウンロードや操作方法で四苦八苦している最中（筆者の技術メモ）ですし、その後はEthereumやHyperledger Fabricも試してみたいと思っています。

そして、最後には、ビットコインの購入も試みる予定です ―― たとえ、**ビットコインが私の仇敵であろうとも**、です。

では、今回の内容をまとめます。

【1】「踊るバズワード ～Behind the Buzzword」の「ブロックチェーン」の第1回目です。この連載でも、これまでの連載と同様に、「**出たとこ勝負（江端の興味のままで）**」で続けさせて頂くこととなりました（EE Times Japan編集部承認済み）。前回のシリーズ（量子コンピュータ）でも、結局、当初の計画通りの連載とならなかったからです（「考えるだけムダ」と判断しました）。

【2】本連載では「ブロックチェーン」を説明するためのアプリケーションとして「ビットコイン」を使うこととします。今回は、**「ビットコイン」の技術から、「ブロックチェーン」の技術が誕生した**、というお話をしました。

【3】「ビットコイン」に関する、私（江端）の誤解を全て開示し（恥をさらし）、ビットコインの仕組みについて、アニメ「シュタインズゲート」と「BEATLESS」の登場人物に登場してもらって、その概要を説明しました。

そして、いわゆるビットコインのマイナー（発掘屋）といわれている者たちが**「旗取りゲーム」をやっているだけであること**と、ビットコインの価値の根拠が、単に**膨大な電力とコンピュータリソースの消費の対価にすぎないこと**を看破しました。

【4】「ビットコイン」に対する、私（江端）の**理不尽なまでに強烈な「不快感」を表明**し、それと同時に、ビットコインの「**人間を踊らせ続けるアルゴリズム」の完璧さに魅了されてしまった**という事実も、正直に吐露しました。

【5】ブロックチェーンの根幹技術である「コンセンサス（同意）アルゴリズム」の概要3つを説明し、現時点での**ブロックチェーンに対する”ケチ”**と、**ブロックチェーンの記事に対する"批判"**を書き出してみました。

以上です。

通貨の価値は「信用」という名前の共同幻想である ーー これは、このコラムを読んで頂いている方には自明なことだと思います。（簡単に言うと、「一万円札の製造原価は数十円」ということです）。数十円の紙に、1万円の価値を与えているのは、日本銀行という組織の「権威」です。

以前、私は、「儲からない人工知能 ～AIの費用対効果の“落とし穴”」で、日本人の個人が所有している資産（家計金融資産）が、流通している紙幣の額面の総合計の14倍（1500兆円）もある、と述べました。

つまり貨幣経済における価値は、有体物としての「貨幣」ではなく、「信用」という正体不明の無体物によって支えられて

いる訳です。ビットコインに至っては、もはや「貨幣」ですらありません。ただの「数字（”6.25”）」です。

　今回、私はいろいろな資料を読み倒して、ビットコインについて調べました。で、多くの資料で、その「仕組み（技術）」については理解できたのですが、私が、どうしても知りたかったことは、どうやってビットコインに「信用」を乗せることができるか／できたのか？ という、その一点でした。

―― よく、こんな「数字」ごときに「信用」を化体させることができたものだなぁ

と、心の底から感心しています（あ、ちなみに現時点の私は、**全然信用していません**けどね）。

　もしかしたらアプローチが逆なのかもしれません。

　新約聖書には、「始めに言葉ありき」と記載されていますが、実は、「言葉の前に数字ありき」というフレーズが省略されているのかもしれません。

　まず、原始宇宙においては「数字」があって、その後の人類と文明に発達を経て、その数字に価値を持たせる必要性から「紙幣」が生まれて、それがちょっとばかり先祖返りして、**とある国の「デジタル庁」**みたいなのものが必要になってきているのかなー、などと考えています。

　ビットコインのアルゴリズムが「数字」に価値を付与する仕組みであるなら、近い未来、**「愛」に価値を付与するアルゴリズムが登場するかもしれません** ―― もっとも、そのアルゴリズムがどんなアプリケーションを生み出すのかは、全く想像できませんが。

既知の技術を「新技術」と言い張るバズワード？

後輩：「**電力と計算資源を消費するだけの“旗取りゲーム”**と看破された点は見事です。でも、江端さん、実際のところ『**なぜ、世間はこの技術（ブロックチェーン）に、それほど騒いでいるのだろうか？**』と不思議に思っているんじゃないんですか？」

江端：「うん……正直に言えば、その通り。既存のITの技術を「複雑化」しただけ、という風に見えるんだよね。例えば、公文書改ざん問題であれば、暗号化して電子署名を付与したファイルを、ネット掲示板にでも放り込んでおけば、それで足りると思う。何もブロックにして、さらにチェーンにするなんて、大げさなことしなくても、と思っている」

後輩：「それと、江端さんは、**コンセンサスアルゴリズム、いわゆる“旗取りゲーム”**についても、そんなに違和感ないんじゃないですか？」

江端：「正直に言えば、イーサーネットのCSMA/CD方式、トークンリング、EtherCAT*）のように、送信権の争奪と、通信の公平性を担保する技術と、基本的には同じように見える」

*）連載：「江端さんのDIY奮闘記 EtherCATでホームセキュリティシステムを作る」

後輩：「江端さんが根本的に誤解している点がそこです。いいですか、江端さん。もはや、この世界には、スマホ同士やPC同士で通信するネットワークなど『存在していない』のです」

江端：「……え？　何言っているの……」

後輩：「いいですか、今のネットワークとは、**スマホが、Wi-Fiのアクセスポイントかキャリアの基地局を見つけて、そこからクラウドに到達して、クラウドからスマホにメッセージが落ちてくる** ―― この一種類しかありません」

江端：「はぁ？！」

後輩：「つまりですね、もはや、この世の中には、上に行って下に落ちてくるだけの「上下通信」しかないんですよ」

江端：「何をバカなことを……」

後輩：「江端さんは、ビットコインやブロックチェーンの本の中で『P2Pネットワーク』という言葉を、山ほど見たはずです。そんでもって、『なんでこんな話をわざわざ記載しているんだろう』と疑問に思ったはずです」

江端:「ああ……うん、そう。『P2Pネットワーク』って、ネットワークの形態は違えども、いわゆる「ローカルエリアネットワーク（LAN）」や「フィールドLAN」と同じパラダイムだろう、って思った」

後輩:「江端さん。驚かれるかもしれませんが、今の世の中には、スマホやPCが、クラウドを介さずに通信する、などという考え方はありません。**スマホやPCが通信している相手は、Wi-Fiのアクセスポイントか基地局だけ**です」

江端:「**なん……だと……？**」

後輩:「江端さんには、別段、不思議でも何でもない、ごく当たり前の”LAN”の思想は、もう10年以上も前に消滅しています。**『スマホがスマホと直接通信する、PCがPCと直接通信する』――この『P2Pネットワーク』という革新的な新技術の登場に、世間は驚き、そして、踊っているのです**」

江端:「**その程度の話が……『革新的な新技術』……だと？**」

後輩:「私は、江端さんに残酷な事実を知らせてしまったかもしれません。しかし、江端さんがこれからも「バズワード」についての連載を続けていけば、こういう、**既知の技術を新技術と言い張るバズワード**を、これから、いくつも見つけていくことになると思います」

江端:「……」

後輩:「この「ブロックチェーン」というバズワードは、前回の「量子コンピュータ」と、**全く性質を異にするバズワード**です。前回のように「技術的に全く訳が分からん」ではなく、「**技術的にはおおむね理解している**」という江端さんのエンジニアとしての資質が、江端さんの心を折り、精神を蝕んでいくだろう、と思います ―― ほぼ確実に」

江端:「……」

後輩:「取りあえず、本シリーズの初回に際しまして ――『**御愁傷様です**』と申し上げます」

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。