Blockchain の真実と新しい暗号通貨
-前編-

情報セキュリティ研究所　所長　　中村宇利

＜はじめに＞

筆者はかつて外資系トップコンサルティングファームの戦略コンサルタントとして、ICT 企業、機械製造会社、商社、製薬会社等に対するコンサルティングを行っていた。その後日本でも世界でも多くの人々に利用され、皆さんにとって不可欠のサービスとなったものも少なくない。その中に、1996 年大手運送会社と共同で日本で初めて実施した“宅配便時間指定サービス”や、これと連動した“配達前の一時預かりサービス”がある。これは発荷主と着荷主そして荷物情報を時間情報と合わせて管理するだけで、従来とは比較にならないほどの利便性をもたらした。いつ配達されるか分かるので着荷主は長時間待つ必要がなく確実に荷物を受け取れるようになる、と発着両荷主に大変好評で瞬く間に日本全国に広がった。筆者も効果を実証するため、１年間ドライバーを務めたが、担当地域での苦情は１年間で１件だけ、それも１分弱お届け時刻を早めに間違えたことを冗談交じりにお話し頂いたのみであった。実はこのサービスは、お客様の利便性向上も大きな目的であったが、主たる目的は、不在時には訪問せず在宅時のみに配達する、という当たり前の事を行うことによるコストダウンであった。その結果、その後の 20 年間で数兆円にのぼるコストダウン効果があり、全国の運送会社の利益増大に貢献し税収増効果があっただけでなく、配送料金の据え置きによって利用者にも利益還元されたものと自負している。しかしながら、国内総生産という観点から考えてみると、利便性が高まったので荷物量は増えたが、配達料金据え置きのため総生産拡大としては限定的であったと言わざるを得ず、無駄を排除することで莫大な経済効果があっただけに、何とも釈然としない気がする。不動産の値上がりだけで経済成長をうたっている国がある中、どちらが国民を豊かにしているのか、答えは明白である。アベノミクスも、経済成長だけを目標にすると、国民の豊かさを置いてきぼりにすることになりかねない、と危惧している。

ところで、この経済を測る最も重要な指標の一つが通貨である。通貨は信用によって裏打ちされた債務を譲渡可能にするものであり、残高を証明する取引記録、または、譲渡可能な証書によって表現される。例えば、法定通貨は各政府の信用を元に発行される譲渡可能な債権（政府にとっての債務）であり、貨幣（硬貨または紙幣）という通貨を実効あらしめる実体として提供される。長い歴史の中で、様々な通貨が試されてきた。通貨によって、表面価値、価値の裏付け、表現方法は異なるものの、現在通貨の基本機能は「決済手段」、「価値の保蔵手段」、「価値尺度」の３つと言われている。最近では、「抽象的な価値単位」と「その存在と移転が認識できる仕組みが保証されているもの」と云うことが受け入れられるようになってきた。これは、情報こそが通貨の本質であると理解されはじめたと言えるし、その結果“仮想通貨”までも社会的に認知されつつある。

＜ビットコイン論文＞

最近 ICT 技術を利用しているにもかかわらず壮大な無駄を敢えて行うことで、民主的な取引を確実に実施できると主張する仮想通貨サービスが登場してきた。発信者と受信者、及び時間情報、そして証書無しに取引情報を管理するだけで通貨の代替行為ができる、とされる。

2008 年に発表されたナカモトサトシなる人物の論文から始まった「Blockchain」及び「Bitcoin」は、これを

信奉する熱烈な信者によってあたかも民主的かつ安全であるとされてきたため、次世代の通貨を作り、また、様々な契約をこれによって記録する「スマート・コントラクト※1」までも実現できる、と大変な人気となっている。実験的論文としては大変面白く、それ以前のピア・トゥー・ピア型の電子マネーにおいて「信用のおける中央機関」なしに解決できなかった二重使用問題を時系列取引のコンピュータ的証明を作成する分散型タイムスタンプ・サーバーを用いた「プルーフ・オブ・ワーク」によって解決できる、という新しい提案を行っている。プルーフ・オブ・ワークとは、一種のゲームのようなもので、取引記録を保存するすべてのノード（他人の決済の承認を担う接続ポイント）が参加でき、その勝者一人だけが報酬を得て正しい記録を保存する権利を与えられ、そのほかのノードはすべてこの勝者に従って記録する、という合意形成を行う。書き込む権利者を民主的競争によって一人に絞り込むことで二重使用問題を回避できるとするものだ。そして、ナカモト氏も注記している通り、このシステムは良心的なノードが集合的に攻撃者グループのノードを上回る CPU パワーをコントロールしている限り安全である。つまり、巨大な数の取引記録記帳サーバーを用いその半数以上を書き換えることは困難であるという多数決論理を安全の拠り所にしている。これは確かに二重使用問題に対して一つの解を提示している。

ここで言う取引記録とは、図のように、誰かがマイニングしたコインを、現在所有していると考えられる所有者がいつどれだけ誰に譲渡したかというデータである。取引を安全に確定させるために、このシステムは、図のような取引記録を常に更新しながら持ち続けなければならない。ある取引を確定させる（例えば、誰が幾らのコインを現在所有しているかを確認する）ためには、関係する過去のデータを「すべて」検証する必要がある。このシステムでは、取引の度に過去のデータの検証がなされる。検証後取引が確定されれば、一定量の取引をまとめてブロックとする。このとき各ブロックのハッシュ値※2をとることで帳簿を締め、容易に書き換えが出来ないようにすることで過去のデータの正当性を担保する。この取引記録は、新たなブロックを過去の取引記録に次々に繋げていくので「ブロックチェーン」と呼ばれている。このようにこのシステムでは、取引の度に過去のデータを参照することにより、自らが行おうとする取引の正確性が担保されるのである。しかしながら、適切なハッシュ値を計算するには膨大な計算量が必要となるばかりか、膨大な過去のデータを保持し続けることも、その膨大な過去のデータを取引の度に検証することも不可避となる。実際、このシステムは検証を容易にする仕組みを備えているが、それでも上述の負担は大きい。

	Date XX	Date YY	Date ZZ	Date QQ
取引参加者A	+1,000BTC（マイニング）	To B: 100BTC（譲渡）	Fr D: 2,000BTC（譲受）	To D: 900BTC（譲渡）
取引参加者B		Fr A: 100BTC（譲受）	Fr C: 1,000BTC（譲受）	+1,000BTC（マイニング）
取引参加者C		+2,000BTC（マイニング）	To B: 1,000BTC（譲渡）	+1,000BTC（マイニング）
取引参加者D	+100BTC（マイニング）	To B: 100BTC（譲渡）	+1,000BTC（マイニング）	Fr A: 900BTC（譲受）
取引参加者E		+3,000BTC（マイニング）	To A: 2,000BTC（譲渡）	

つまりこのシステムでは、報酬をモチベーションとしてコンピューティングパワー次第のゲームに参加する多数の者がゲームを続け、ゲームに勝利したただ１人の者が報酬を得るとともに優先権をもって上述の如き過去のデータの書き換えを行い続けることで、新たに行われる取引の正当性と、膨大な過去の取引記録の正当性との双方を保証するものとなっている。取引、及び取引記録の正当性はゲームの勝者が常に良心的であるという前提によって保証されている。しかし、現在はほとんどの場合限られたグループだけが勝利し報酬を得る“弱肉強食”ともいえる事態となっている。これらの限られたグループが常に良心的であり続ける保証はどこにもない。実際ノードの 6 割以上が中国にあると言われており、どのような運営がなされているのか把握することさえ困難である。

＜ブロックチェーンの真実＞

Blockchain チャート※3（https://blockchain.info/ja/charts） によると、2017 年 1 月 1 日 9：00 時点でビットコインの総流通量は 16,077,350 である。そして、これらの仮想コインの取引のすべてがブロックチェーンにより記録されている。因みに、1 ブロック当たりの平均取引数は 1,157 件、これにかかる時間は約 10 分である。そして、このようなビットコインのためのブロックチェーンを記録するノードはすでに数百万台を超えたとされ、一説には 1 千万台ともいわれる。原則としてこの大量に存在するすべてのノードに、同一かつすべての取引記録が記録される。このような事を行うのは、同一の取引記録が記録された極めて多数のノードが存在すること自体が過去の取引記録のデータの正当性を保証するという仕組みをこのシステムが採用しているからである。このシステムでは、多数のノードでそれぞれ保存された取引記録に齟齬があった場合、それらのうちの過半数を取る取引記録を真正な取引記録とすることとしており、ノードの過半に対する大規模な取引記録の改竄は不可能であるということを根拠に取引記録の正当性を担保することとしているのである。

ノードに記録されている取引記録のサイズは、2017 年 1 月 1 日 9：00 時点で 96.345 ギガバイトである。つまり、約 1 千万台の CPU の全ての計算能力と 1 ヘクサバイトの記憶容量が取引の実行と取引記録の記録の為だけに使われていることになる。一般的に民主主義の維持のために多大な無駄も必要悪とされるが、実際にはほぼすべてのノードが約 10 のグループによって支配されており、決して民主的に運営されているとは言えない。ナカモト氏の論文は、小規模の二重使用問題の回避のためならば機能するが、すべてのノードが参加して同一の取引記録を保持しなければならないと規定する以上、大規模なものには向かないことが分かる。事実上、かなり前からすでに許容規模を大幅に超えていると推測される。

ところで、ナカモト氏は、独自のブロックチェーン方式によって二重使用問題を解決しようと試みているが、取引記録方式や取引記録を公開鍵暗号技術を用いてノードに伝達する方法など大部分の仕組みは 80 年代から 90 年代にかけて考案された数々の電子マネーの仕組みをほぼ踏襲している。その結果、このシステムは、筆者が 2016 年秋号、冬号で指摘した公開鍵方式の理論上の欠陥をそのまま内包しており、その処理速度は遅く、セキュリティ上の改善が必要である。ノードに対する占有攻撃やプロトコル遅延攻撃など様々な脅威が考えられるが、特に中間者攻撃（man-in-the-middle-attack）※4 に対しては全く無抵抗である。ビットコインの登場以来、大規模な攻撃に遭っておらずシステムの停止には至っていないと強弁する論者もいるが、日々起こるコインの盗難や取引所の破たんの例を挙げれば、その中に中間者攻撃が含まれていないと考えるには無理がある。それでも、約 1 千万のノード上に記された取引記録を過半数にあたる最低 5 百万ノードについて書き換えることは事実上不可能であるから記録が不正に書き換えられることはない、と主張する人がいるかもしれないが、中間者攻撃では、インターネットなどオープンなネットワークから分散台帳に新たな取引を書き込みに行く段階で、1 件 1 件の新たな取引そのものを書き換えることが可能で、その不正な記録がブロックチェーンとして書き加えられていくだけのことであり、ノードの数は関係ない。

最後に、同一の取引記録が大量のノードに記録されるので、災害時においても簡単に失くならず安全であるという人がいるが、もともと、ノード参加者はボランティアベースであり、過去から現在までの取引を完全に全部記録しなければならない義務はない。実際、一部の記録が抜けたノードは多い。とは言えゲームの勝者だけはブロックを書き加えなければならないし、1 千万台ものノードが 1 台も記録していないということは考えにくいのだが、究極の状況を考えると、1 人の勝者がまず記録を付け加えた瞬間など、万一その勝者 1 人しか記録していない状況で、その 1 台が事故で失われたら、大事な記録は完全に失われることになってしまう。可能性は極めて低いが、“仮想通貨”など重要な取引記録に使うのであれば、当然排除すべき可能性

である。

＜共同幻想としてのビットコイン＞

ナカモト氏の論文で述べられている通り、ブロックチェーンとは取引を確実に記録するだけのものであり、決して通貨を作り出すものではない。「取引記録によると間違いなくこの人はこれだけの額を持っているに違いない」と信じあっているだけの、空気のような実体のない共通認識をビットコインと呼んでいるだけである。「コイン」と言いながら、それが入っているはずの財布の中身は空っぽ、宅配便で例えれば荷物は空なのである。ナカモト氏が論文中で、ゲームの勝者への報酬の支払いを、実体とは似ても似つかないマイニングと例えたため、ビットコインをあたかも金や銀のような、実在するコインと誤解している人も多い。ナカモト氏の論文の本質は、実在のコインを発行すれば、これを管理する中央機関が全取引を監視し、コインを管理する必要が出てくるので、逆に実体のない空気のようなものをコインと呼ぶことによって、そもそも監視や管理の必要がないようにしたというレトリックにある。

ビットコインの価値とは何であろうか？「ビットコインをマイニングするのに使用された電気代」などと苦しい説明する人もいる。実際、現時点でマイニングマシーンをそろえて、マイナー（ノードを使用しゲームに勝利しビットコインを報酬として得る人）となり 1 コインを手にするのにかかるコストは約 10 万円と言われているが、2017 年 1 月 1 日 9：00 時点で 1 ビットコインは 998 ドル（117, 115 円）で取引されており、ほぼこれに等しくなっている。金貨の場合、その価値は、採掘と鋳造にかかるコストはそのほんの一部だけであり、装飾品などの金細工のための希少な材料としての価値が大部分を占めるが、ビットコインはマイニングコストのほかは何もないので、論理的に考えれば何の価値もないことが分かる。それでは、取引所で交換されている価格とは一体何だろうか？ビットコインはそれ自体実体のないもので、その価格はその実在性と同様、きっと価値があるに違いないとの共同幻想によって生じているだけの、まさに泡（バブル）のようなものであり投機以外の何物でもない。

ビットコインを、通貨の 3 つの基本機能である「決済手段」、「価値の保蔵手段」、「価値尺度」の各側面から考えてみると、前述のセキュリティの問題を無視すれば、また、冗長な取引記録を多数のノードで共有する必要があるということも無視すれば、取引記録から各ユーザが所有するビットコインの残高を計算することができ、取引記録を用いてあるユーザから別のユーザへとビットコインを譲渡することができることから、ビットコインは一応、「決済手段」と「価値の保蔵手段」としての機能を有する。他方、価値尺度としては、予め決められたルールによって発行量がコントロールされており所定のタイミングでの大幅な価値変動が避けられない（例えば、法定通貨に対する価値変動が激しいのは周知の事実であるが、それでは価値上昇時は良いが価値下落時には仕入れ値よりも廉価にサービス提供せざるを得なくなり商売にならない）ので、価値尺度としての機能は不十分であるといえる。また、政府が発行する一般的な法定通貨が政府が負う債務を信用の源泉として持つのに対して、ビットコインはその発行、及び譲渡の記録を民主的に行うことにしており、最終的にその価値についての責任を負う者がいないため上述の如き信用の源泉を持たない。この点を重視するのであれば、ビットコインは、価値尺度という点のみならず、決済手段、価値の保蔵手段という点から見てもその機能が不十分であるといえる。つまりビットコインは通貨として不完全である。

実は、多くの人が抱く中央管理を不要とする民主的なイメージについても、共有するブロックチェーンという取引記録によってビットコインが仮想的に存在するとした、①誰でもが参加でき、②合意形成プロセスを経て、③多くのノードが同一取引記録を共有するという過程の中で、フェアにビットコインが産出されるという設計自体に因る共同幻想である。本来の民主的システムとしての最低要件は、中央管理者がいなくとも

誰もが参加できる取引記録を常に間違いなく最新に保ち、改竄されないこと、いつでも誰でもチェックできることであるが、そのために決して大量のノードが同一の取引記録を保存する必要がある訳ではない。それればかりか、これら大量のノードは、前記の通り地理的に偏在するばかりか特定の勢力の影響下にあるとも思われ、現在稼働しているシステムは、およそ民主的なシステムとは言えないのである。

以上見てきたように、ビットコインは、通貨の要件である決済・保蔵メカニズムを担う「ブロックチェーン技術」自体が、ナカモト氏自らが述べているように、ノードが集合的攻撃者グループのノードを上回るＣＰＵパワーをコントロールしていなければ安全でない、大規模な二重使用問題の回避には機能しない、と云う欠陥を持つ。更に、公開鍵方式の理論上の欠陥を内包するため、中間者攻撃に対して全く無抵抗であり、そして何よりも問題なのは、通貨の要件の一つである価値尺度（信用）が確認出来ない。つまるところ、ビットコインは通貨と呼べるものかが大変疑わしいものだ、と言わざるを得ない。
それでは、通貨の３つの機能を有し、安全な「暗号通貨」というものは存在し得ないのか？
次回後編において、決済・保蔵メカニズムを担い価値尺度を持つ真の暗号通貨技術と具体的な応用例について詳述する。

※1. スマート・コントラクト

スマートコントラクトとは契約の自動化と訳される。事前に設定された条件に基づいてシステムがスマート（自律的）にコントラクト（条件に基づいたプログラム）を実行することからこのように呼ばれる。

（出典：仮想通貨通信　http://bit-economy.news/smartcontract/）

※2. ハッシュ値

元になるデータから一定の計算手順により求められた、規則性のない固定長の値。その性質から暗号や認証、データ構造などに応用されている。ハッシュ値を求めるための計算手順のことをハッシュ関数、要約関数、メッセージダイジェスト関数などという。

ハッシュ値は元のデータの長さによらず一定の長さとなっており、同じデータからは必ず同じハッシュ値が得られる一方、少しでも異なるデータからはまったく異なるハッシュ値が得られる。不可逆で情報量の欠損を含む計算過程を経るため、ハッシュ値から元のデータを復元することはできない。

（出典：e-Words　http://e-words.jp/w/ハッシュ値.html）

※3. Blockchain チャート

ビットコイン blockchain 上のデータをチャート化して提供するサイト。市場価格（USD）（主要ビットコイン取引所全体の平均 US ドルの市場価格）、時価総額（主要証券取引所全体の毎日の平均市場価格で計算すると、循環に供給をビットコインの総ドルの値）、Blockchain サイズ（すべてのブロックヘッダおよびトランザクションの合計サイズ）、ブロックあたりのトランザクション（ブロックあたりの平均トランザクション数）、取扱量（毎日確認されたビットコインのトランザクションの数）、Blockchain ウォレットユーザー（Blockchain 財布の総数）などを表示する。

※4. 中間者攻撃（ＭＩＴＭＡ、man-in-the-middle-attack）

攻撃者が犠牲者と独立した通信経路を確立し、犠牲者間のメッセージを中継し、実際には全ての会話が攻撃者によって制御されているときに、犠牲者にはプライベートな接続で直接対話していると思わせる。攻撃者は 2 人の犠牲者の間で交わされている全てのメッセージを横取りし、間に別のメッセージを差し挟む。これは多くの状況で容易なものである。

（出典：Wikipedia　https://ja.wikipedia.org/wiki/中間者攻撃）