一般社団法人フィンテック研究振興協会
ブロックチェーン関連情報　Vol.１
＜ブロックチェーン研究論文１：暗号通貨の考察＞

【暗号通貨の黎明】

暗号通貨の概念は、サトシ・ナカモト（Satoshi Nakamoto）が、２００８年初頭から metzdowd.com 内の暗号理論に関するメーリングリスト「電子通貨ビットコインに関する論文」を発表し始めたことから始まりました。

サトシ・ナカモトの論文の主旨は、「インターネット上の商取引は、例外なく電子取引を処理し信用できる第三者機関としての金融機関に頼っていることが現状である。金融機関は争いの仲裁を行うために、完全に非可逆的な取引は扱えない。仲裁コストが取引コストを引き上げるため少額取引の可能性は失われる。必要なのは、第三者機関を介さずに２者が直接取引を行うことです。その場合、信頼ではなく暗号技術に基づいた決裁システムがあれば良い。通貨を多重に使用されるような不正から守るために、P2P 分散タイムスタンプサーバーを利用する。善良なノードが、悪意あるノードよりも CPU が上回っていれば、このシステムはセキュリティ的に安全である」というものです。

この論文には、金融機関を通さずに直接２者間で、インターネット上において正常な取引を行えるシステムとして具体的なシステムデザインが示されています。
これが世にいうブロックチェーンと呼ばれている電子取引台帳です。

２００９年１月、サトシ・ナカモトの論文にあるブロックチェーン技術を使い、複数のコンピューター提供者との間で分散処理による取引方法を構築し、その上で売買される通貨として世界初の暗号通貨であるビットコインが誕生しました。

【ブロックチェーンとは】

ビットコインに見る、ブロックチェーンの特徴は大きく分けて３つあげられます。

１．分散システム（P2P ネットワーク）
２．暗号技術の活用（電子署名ハッシュ関数）
３．ビザンチン将軍問題への対策（コンセンサスアルゴリズム・PoW）

世に存在する仮想通貨の取引システムであるブロックチェーンは、これまで解かれてこなかった分散システム上の課題を解決しているのではないかと現在多くの機関が検証に乗り出しています。

暗号通貨の技術として導入されたブロックチェーンですが、暗号通貨はその技術

の利用分野のひとつに過ぎず、金融や証券のみならず医療現場やIoT（ネットワークで機械を遠隔操作する技術）にまで応用できる技術として注目されています。

しかし、このブロックチェーンの正当性を裏付けているものは、ビットコインのたった7年間の「未停止」という運用実績だけであり、理論的に第三者によって検証され、そのうえで確立されたものではありません。
今もなお、改善が繰り返されている進化中の技術なのです。

では、ビットコインにおけるブロックチェーンの特徴を見て行きましょう。

≪分散システム：P2Pネットワーク≫
P2P（Peer To Peer）とは複数の端末間で通信を行うもので、管理サーバーが存在しないネットワーク接続です。
通常の金融システムでは、高いセキュリティを施したクライアントサーバーが権限を持つことで運営されているため、多大なコストがかかるという問題があります。
ブロックチェーンは中央権限型ではなく、特定の端末に権限を集中させない非中央集権型のP2Pネットワークを構築することを前提にしています。
この、非中央集権型ネットワークは、コストがかからず、透明性を維持できるとされています。

しかし、なぜ金融システムや他のシステムでP2Pネットワークが構築されてこなかったのでしょうか？
それは、一つの解決できない大きな問題が存在していたためです。

その、大きな問題とは「ビザンチン将軍問題」といわれる、ネットワークにおいて故障または故意によって嘘の情報が伝達される可能性がある場合に、そのネットワーク内で正しい合意を形成できるかという問題です。
この問題に対してビットコインは、Proof of Work（PoW）というコンセンサスアルゴリズムによって解決を試みています。

このPoWとはP2Pネットワーク内で行われる取引の正当性を、マイニング（採掘）という他ノードの承認を取り入れることによって、正当性を示そうとするものです。
この承認には莫大なコンピューター処理能力を必要とする計算領域であり、この作業に時間的、経済的負荷をかけることによって、悪意ある攻撃を防ぐシステムを構築しているのです。
そしてその作業こそが、電子署名とハッシュ関数を使った暗号化技術によるものなのです。

≪暗号技術の活用：電子署名ハッシュ関数≫
ビットコインのブロックチェーンは、電子署名とハッシュ関数によって改ざんされることを防止しています。
例えば、あるブロックが形成されると、それまでの取引全てを要約したデータが

ハッシュ関数によって生成されます。
次に生成されるブロックは、要約データと取引データを含んだもので形成され、次のブロックではそれらの要約データが生成されます。
このように、一つのブロックにすべての取引データの要約データが入っているため、不正を行うためには、改ざんした取引以降のすべてのブロックを作り直さなければなりません。

加えて PoW により、より早く計算結果を出したものが、そのブロックの生成権利を獲得するため、これらの改ざんを通常の計算よりも早く行わなければならず、莫大な計算能力を有するコンピューターでもなければ改ざんすることは困難な仕組みとなっています。

≪ビザンチン将軍問題への対策：コンセンサスアルゴリズム・PoW≫
この PoW というコンセンサスアルゴリズムが、ビットコインのブロックチェーン技術の一つの特徴です。
前述したように、取引データを含むブロックを生成するためには、ハッシュ関数によるハッシュ値が必要ですが、これを生成するためには、前ブロックのハッシュ値からただ一つ導き出されるナンス（数値）を難解な計算により取得し、そのナンスを用いて次のブロックのハッシュ値を形成しなければなりません。

このナンスを一番早く見つけたマイナー（採掘者）だけが次のブロックを生成することが可能となり、ビットコインではこの計算が約 10 分で完結するように計算難易度を調整しています。
ビットコインでは、これらのブロックが長く続いているチェーンを採用する形を取っているため、改ざんしてブロックを生成することは、通常より遥かに多くの計算能力と時間を有することになり、現実的には困難であるとみなされています。
ただし、存在する良心的なマイナー以上に、悪意を持ったマイナー、または巨大な計算能力を持ったマイナーが存在すると、能力的に悪意のある者が上回ってしまうため、これらのシステムは簡単に崩壊してしまう危険があります。

このように悪意のある者がネットワーク内に存在する場合に、どのようにして正しい取引を承認するかという問題は「ビザンチン将軍問題」として、ビットコインのブロックチェーンに関わらず、分散システムを構築する上で長い間大きな課題とされてきました。

この「ビザンチン将軍問題」というのは、「敵国を囲む複数の将軍間で一斉攻撃の作戦の合意をとりたいが、将軍の中に裏切り者がいたり、伝令者が捕まったり、偽の情報を流されたりする可能性がある場合は、どのように正しい情報を判断し全員の合意を取るか」というものです。
インターネット上においてもハッカーに代表されるように、悪意のある者は必ず存在し、かつ通信環境も完全なものではなく不安定なものなのです。

例えば、インターネットで２者間の合意を得る、「２人の将軍問題」というのが

「ビサンチン将軍問題」とは別に存在しています。
　これは、現在ネットワークの世界標準通信プロトコルである、ＴＣＰ／ＩＰ（インターネット・プロトコル・スイート）が完全に解決しているとされています。

　しかし、世の中には完全なロジックやＩＴシステムは存在しないのです。
　このＴＣＰ／ＩＰにしても、２者のコンピューターが同時にハッキングされた場合には、これを検出できる方法は皆無で、何事も無かったかのように２者は不正な通信を正常な通信と何ら変わる事も無く継続してしまうのです。
　このような状況下で、他のノードが同じ正しい情報をもとに合意できるかという問題が、分散システムを構築する上では古くから課題となっていました。
　しかし、実際にビットコインが分散システムによって 7 年間維持されていることを見て、「ビットコインがビザンチン将軍問題を解決している」と言われるようになったのです。

　しかし、実態は解決しているのではなく、「悪意のある存在がいても、５０%以上の計算能力がなければ、支配されることはない」という推測理論によるものでしかありません。
　また、近年の研究では、４１%の計算能力でも１／２の確率でブロックを生成できることが示されています。

　結論としては、ビットコインをはじめ、世の中にある暗号通貨取引システムは、「ビサンチン将軍問題」を解決していない、むしろその問題を解決しなくてもよい方法を見つけ出し、「避けて通っている」というのが正解なのです。

　では、なぜビットコインはいままでシステムダウンすることなく、正常に運営し続けることができているのでしょうか？
　それは悪意を持つ者たちの根拠が経済的理由だった場合に、システムを乗っ取ったとしても「利を得ない」状況にしているためです。

　ビットコインは、ネットワークに参加するすべてのノードに対して、マイニングの報酬を与えています。
　マイニングの競争を勝ち抜くためには、他のノードよりも早い計算能力を持つコンピューターを用意する必要があり、さらにそれを運用する電気代などの設備やランニングコストといった経済的負担が伴うことになります。

　多くのマイナー達が、それぞれの計算能力を駆使してマイニングを行っているため、参加者の５０%を超える処理能力を持つコンピューターとその運用には、マイニングの報酬以上にコストがかかってしまうのです。
　その１０分という計算の難易度と、ビットコインの報酬のバランスなど、総合的に考えた場合に、悪意のある参加者にとって「利を得ない」結果を齎すことによって、安全を何とか確保しているという事に過ぎないのです。

　また、他の暗号通貨ではビットコインの PoW（マイニング）に代わり、PoI（proof

of importance）というコンセンサスアルゴリズムを用いて、取引高や貢献度を自動分析して報酬を支払うことにより、不正を働くよりも協力する方に利が有るという状況を作り出し、安全に運営しようとしています。

【暗号通貨の抱える課題】

ビットコインに限らず、世に存在するほとんどの暗号通貨に言えることですが、マイニングによる報酬や貢献度に応じた報酬は、不正をすることによって利を得たいという者たちにしか通用しないものなのです。

暗号通貨システムの混乱や破壊のみを目的とし、経済的価値も鑑みない悪意を持った者が存在する場合には、システムが故意に破壊もしくは支配される可能性を否定できません。
世界的に流通しているビットコインを始めとした暗号通貨の崩壊は、今や経済に多大な影響を与える結果を生んでしまうでしょう。

ビットコインのブロックチェーンは、すべての取引データが参加者全員に記録されていますが、５０%以上の計算能力をもつ悪意のある参加者によって、すべて書き換えられてしまう可能性も否定できません。
管理する権限を持つ者がいないがために、たとえ改ざんが発見されたとしても、それをリカバリーすることができないのが事実として存在しています。

また現在では、新たなるロジックを追加したブロックチェーンを構築し、それを活用した暗号通貨が数多く誕生していますが、ビットコインなどでノウハウを蓄積した参加者が、新しい暗号通貨のマイニングに参加した場合、圧倒的な計算能力で支配してしまうことも想定できてしまいます。
いわゆるマイニングを組織で行う、マイナープールの存在がその一つです。

このように、ビットコインを始めとした現在存在する暗号通貨は、「ビザンチン将軍問題」を解決しているとは言えず、たまたま上手く稼働させているに過ぎないシステムであり、いつシステムが崩壊や支配されてもおかしくない状態にあるということが、最大の課題となっています。

【非中央集権型の取引システムは本当に優れているのか？】

世の中には、ブロックチェーンに見る分散処理による非中央集権型取引システムを、疑問も持たずに支持する人で溢れかえっています。

かのアインシュタインは、「疑問を持たずに敬意を表するのは、事実に対する最大の冒涜である」という、けだし名言を残しています。
この名言が示すように、ＩＴ技術を熟知した人の多くは、非中央集権型の取引シ

ステムに多くの危険性を見出しています。

銀行や証券などの金融機関も近年では、ブロックチェーンによる取引を行おうとしていますが、全てが中央集権型のプライベート・ブロックチェーンを採用しようとしている事実を見ても一目瞭然です。
「人件費などのコストが少なく、透明性が有る」、この非中央集権型の優位点こそ最大の欠点でもあるのです。

非中央集権型の危惧する問題の一つには、確かにノードにおける台帳の安全性は確保されているかのように見えますが、例えばユーザーの端末が突然故障した場合、パスワードなどのアクセスキーをバックアップしていなければ、仮想通貨の取引台帳はノード間で保障されていても取引することはできなくなり、事実上保有通貨は失われることになります。
更にはハッキングされ盗用された場合も同じことです、この問題を現在多くの非中央集権型の仮想通貨取引システムでは全く解決の糸口さえ有りません。

もう一つは、スケーラビリティという、システムの規模の変化に対応できる柔軟性への対応です。
今や、ビットコインは世界中で利用されており、その利用量は日毎に増しています。
店舗での支払いや労働報酬の支払いなどにも利用され始めてきていますが、その取引速度の遅さが問題であり、決裁までに数時間を有する場合も発生しています。

この問題の対応策として、ビットコインの原論文(Satoshi Nakamoto, 2008)に記載されていながら、いまだ実装されていない Segwit（Segrageted witness）と呼ばれるる技術を開発者側が導入しようとしました。

これはブロックチェーンの容量を見かけ上増やすもので、電子署名部分をブロックから分離して管理するという、今までの仕様と互換性を保ちながら行うシステムの上位互換性のあるアップデートです。

対して、世界最大のマイニンググループである AntPool が支持したのは、ブロックチェーンの容量を完全に増やしてしまおうという解決策です。
現在のブロックチェーンのブロック自体は、約 3000 の取引記録が納められ、その容量が 1 MB と決められています。
この容量を 8MB にまで増加させようというものですが、今までの仕様で作られてきたブロック（取引台帳）は反映されず、事実上全く新しい暗号通貨ができることになってしまうのです。

前者の互換性を持ったままでアップデートを行うことを「ソフトフォーク」、後者の新しい仕様で、新しい仮想通貨を作ってしまうことを「ハードフォーク」といい、中央権限を持たない非中央集権型システムでは、しばしばこのソフトフォークとハードフォークの対立が起こることは否めません。

事実、ビットコインのような今回と同じ問題が、イーサリアムで過去起きており、イーサリアムではハードフォークにより２つのコインに分裂いたしました。

このように、技術的に避けて通れない課題、そして中央集権を持たないことで起きうる大きな保障問題、これら全てを熟知した人であれば、簡単に非中央集権型が優れているとは言えないのではないでしょうか？