エターナルコイン

ホワイトペーパー＜Vol .01＞

株式会社アトムソリューションズ

２０１７年8月２２日

１．イントロダクション

【仮想通貨の黎明】
仮想通貨の概念は、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いい。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システムです。
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、そのうえで売買される通貨として世界初の仮想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】
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。
仮想通貨の技術として導入されたブロックチェーンですが、仮想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「ノーダウン」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。

≪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集権型ではなく、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です。

≪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。

それに加えて 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。

≪Proof of Work（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るのです。

≪ビザンチン将軍問題≫
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かかわらず、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「ビザンチン将軍問題」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。
例えばネットワークの世界標準通信プロトコルである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、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。（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る）
結論としては、ビットコインをはじめ、世の中にある仮想通貨取引システムは､「ビザンチン将軍問題」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。

≪ビットコインが正常に動き続ける理由≫
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出来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、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、他の仮想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。

【仮想通貨の抱える課題】
ビットコインに限らず、世に存在するほとんどの仮想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。
仮想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仮想通貨の崩壊は、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、それを活用した仮想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、新しい仮想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。
所謂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仮想通貨は、「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るのです。

【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。この問題は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、事実上全く新しい仮想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？

エターナルコインを発行管理する、アトムソリューションズでは、これらの課題を解決し、世界に通用するフィアット通貨としての仮想通貨を目指そうとしています。

２．エターナルコインは世界一安全な仮想通貨

【何故、新幹線は世界一安全な乗り物で在り続けるのか？】
日本が世界に誇る新幹線は、１９６４年１０月１日に東京－大阪間で運行されて以来、過去５０年以上もの間、一度もシステムトラブルによる事故を起こしたことがありません。
その実績により、「世界一安全な乗り物」として、その存在感を世界に示してきました。

その安全性の中核システムが、新幹線 ATC（Automatic Train Control）というシステムなのです。
新幹線 ATC は車上システムと、地上システムの２つのシステムの連携により安全性を確保しています。
車上システムは、１６両編成の新幹線では、計４台の制御コンピューターが積まれています。
この車上システムは、４台の制御コンピューターを独自のプロトコルによって相互接続されており、それぞれの制御コンピューターは分散処理によって、１６両編成全ての制御を行う統合システムとして機能しています。

それぞれの車上システムは、それぞれに１６両編成全ての電子機器や計測機のセンシングを行い、４台全ての結果が揃わなければ、モーター駆動やブレーキなどの制御系に指示しないようになっています。

また、線路上には数百メートルおきに地上システム端末が置かれています。
地上システム端末は中央管理システムと常時繋がっており、それぞれの地上システム端末は無線によって通過する新幹線の４台の車上システムに位置情報や停止指示などを知らせています。
これらによって、新幹線は自動的にダイヤ通りに自動でしかも高速ながらも安全に運行できるようになっているのです。

ここで、仮に４台の車上システムの制御コンピューターが、同じ結果で無かった場合はどうするかというと、自動運行モードは瞬時に解除され、マニュアル運行モードに切り替わります。
マニュアル運行モードとは、運転手の操作によって速度制御やブレーキ操作を行う、普通の列車と同様の運転モードのことです。

また、自動運行モード中でも、運転手が急な病気や居眠りなどで操作レバーから手を離した瞬間、車上システムはアラートを上げ、時速２０ｋｍまで速度を落とし、次の駅に自動

的に停車するようになっています。
つまり、４台の分散処理されたコンピューターと、人間の判断とを連携させ、世界一安全な仕組みを作り上げているのです。
この４台の分散処理コンピューターと人間との連携こそ、これまで解決できなかった「ビザンチン将軍問題」の有効な解決策のヒントになると考えています。

平常時の自動運行モードと有事の際の手動運行モードの自動検出と自動切り替え、コンピューターと人間との相互連携、アトムソリューションズは仮想通貨の取引システムの安全なる運用方式に関して、この新幹線 ATC の安全確保方式に解決策を見出しました。

人間の命に関わる高速鉄道インフラの安全性の確保は、金融システムでの安全性確保とは次元が異なるほど確実で優れたものでなくてはなりません。
高速鉄道インフラの安全性確保技術を、仮想通貨取引に応用する仮想通貨は、世界にエターナルコイン以外に存在しません。

【取引は非中央集権型のブロックチェーン】
安全性が確保された上での、分散処理による非中央集権型取引システムは、エターナルコインを発行・運用するアトムソリューションズにおいても一定の評価を見出しています。
やはり、運用コストの低減化と取引の透明性は見逃すことはできません。

エターナルコインの平常時の取引においては、ブロックチェーンをコアとした分散処理取引システムを採用いたします。
また、安全性を確保する上でのロジックは、他の仮想通貨のように「ビザンチン将軍問題」を避けて通ろうとするPoWによるマイニングや、PoIといった報酬による解決策では無く、根本的に体制とロジックによる解決策を施します。

【監視サーバー】
ブロックチェーンによる分散処理により取引は非中央集権型で行うも、この監視サーバーの存在で安全性は飛躍的に向上します。

監視サーバーは、ブロックチェーンで生成される取引台帳を常時監視しながら、別の管理用台帳を生成していきます。
これによって、ブロックチェーンの取引台帳の改ざんや不正が行われた場合には、瞬時にそれを検出することが可能となります。

異常を検出した監視サーバーは、新幹線 ATC のように、アラートを上げ一時的に取引を停止する事も可能となり、また人間による判断や善後策を講じることが可能となります。
これにより、どのような事が起きても利用者の財産を守ることが可能となります。

この取引台帳とは別の管理台帳の存在は、例えば利用者のコンピューターが故障してアクセスキーを失った場合も、利用者の本人確認がされることで再発行を行う事も可能となります。

この監視サーバーの存在はエターナルコインの安全性への最大の特徴であり、他の仮想通貨には類を見ない方法です。

【管理サーバー】
利用者のウォレット開設や入金管理を行うサーバーであり、先述の監視サーバーがアラートを上げ取引を停止した場合や、利用者がアクセスキーを失った場合などに有益に機能するサーバーです。

新幹線でいう運転手に相当するサポート機能を有したサーバーとなります。

【責任者の所在の意義】
利用者保護の観点や、スケーラビリティ問題などへの対応など、責任母体が無い仮想通貨の諸問題は、エターナルコインでは起こりえません。
エターナルコインでは、発行・管理・運営するアトムソリューションズという責任母体が存在しているからに他なりません。

エターナルコインは、平常時には非中央集権型の透明性のある取引を行えるにもかかわらず、有事の際には管理・責任が問われる諸問題に関して、責任母体がそれを速やかに排除する体制を執っています。
つまり、非中央集権型と中央集権型の中間では無く、それぞれの良さを追求して、融合させたシステムと呼ぶのが相応しい仕組みを作り上げました。

コンピューターと人間による、それぞれに適した処理分担により世界一安全な仮想通貨取引の仕組み、それがエターナルコインなのです。

３．エターナルコインの特徴

【コンセプト】
世界には、ビットコインをはじめ数多くの仮想通貨が存在しておりますが、通貨としての存在を示し実際に支払いや決済に使われている例は極めて少ないという事実があります。
エターナルコインは、投資目的ではなく利用される通貨としての存在を目指しております。
そして、手軽に利用されるためには、取り扱いがシンプルである必要があります。
エターナルコインは、誰にでも手軽に取り組むことができ、便利なだけでなく利用するメリットがある仮想通貨です。

そして今以上に利便性を追求するためには、ウォレットや取引所の体制を含めた総合的な改善と協力体制が必要です。
エターナルコインは、これからも利用しやすいウォレットの改善やコンテンツの開発、そして各国の取引所と連携した活動によって、利用できる国や場所を拡大し続けていきます。

【多通貨取引可能ウォレット（マルチカレンシーウォレット)】
仮想通貨の特徴の一つは、国境が無いということです。
しかし、日本円を仮想通貨に変換して他の国の通貨に交換する場合には、交換したい通貨の国でウォレットを作成する必要があります。
ところが、エターナルコインを利用して、他の国の通貨に交換する場合には複数の取引所にウォレットを開設する必要はありません。
エターナルコインは、日本、香港、フィリピン、韓国に取引所があるので、一か国でウォレットを開設すればそのウォレット内で他の通貨への交換が可能となります。

この優れた特徴は、仮想通貨の売買だけを行う際には意識されませんが、海外へ行った際の両替やショッピング、そしてエターナルコインを利用した海外送金の際には、極めて優れた利便性を発揮いたします。
今以上に、エターナルコインの取引所が世界中に増えれば、更なる利便性を拡大していけます。
アトムソリューションズでは、今後も様々な国に取引所を増やし、エターナルコインがより便利な仮想通貨となることを目指しています。

【フィアット通貨（基軸通貨）での支払い】
仮想通貨で決済を行うということは、仮想通貨で支払いをする利用者、もしくは仮想通貨

で支払いを受ける店舗様、双方にとって仮想通貨を保有しておくことによる価格下落のリスクが発生いたします。
エターナルウォレットでは、価格下落のリスクを排除するために、その国の通貨での支払いが可能です。
日本人が日本国内での利用にエターナルウォレットの JPY を使用することはないと思いますが、海外へ行った際には、エターナルウォレットの JPY を現地の通貨に両替してショッピングや現地通貨の引き出しができるということは、仮想通貨を保有するために起こる仮想通貨の価格下落のリスクが無く、利用者と店舗様にとって大きなメリットとなると考えております。
このような使い方が出来るウォレットは、現時点ではエターナルウォレットだけです。
エターナルコインでは、これをマルチカレンシーウォレットと呼んでいます。

【ワンタッチ送信】
エターナルウォレットを利用して海外送金を行うには、取引を行う際に一度エターナルコインを購入して、その後売却する必要があります。

例）日本円（JPY）からフィリピンペソ（PHP）に交換して海外送金を行う場合
①JPY でエターナルコイン（XEC）を購入
②エターナルコイン（XEC）を売却して PHP に交換
③PHP を相手先ウォレットに送信

エターナルウォレットでは、上記の３つの取引をウォレット内でワンアクションで行うことができます。
したがって、海外送金を行う方や、海外旅行先でエターナルウォレットを利用したい方はエターナルコインを保有する必要がなく、格安で送金や両替を行うことができます。
このように、エターナルコインは両替や海外送金時のハブ通貨となり得るのです。

【エターナルコインを保有するメリット】
エターナルウォレットには、DoT という機能があります。
DoT 機能とは、トランザクションフィー（手数料）の分配を行う機能です。

エターナルウォレットを利用して、エターナルコインの売買や送信を行う際には、わずかな手数料が発生します。
この手数料をエターナルコインの保有者に対して、保有数に応じて自動的に毎週一度分配

するのが DoT 機能です。
この機能により、ハブ通貨としてのエターナルコインを保有しておくメリットが発生するため、エターナルコインがハブ通貨として使われ続ける限り、その価値が 0 となることはありません。

【有利なレート】
アトムソリューションズでは、利用者様に対して今後様々な API の発行を予定しております。

その API を利用することにより、BOT（人間に代わる機械）での自動売買取引を行うことも可能となっているために、各フィアット通貨とエターナルコインの価格が乖離した際にアービトラージ取引（裁定取引）を行うことが可能です。
アトムソリューションズでは、エターナルコインを利用したアービトラージ取引を行ってもらうことによりスプレッドが狭まることは、エターナルコインの価値が国によって乖離することがなくなるために非常に良いことだと考えております。
スプレッドが狭まることにより、従来の海外送金や両替所のレートよりも有利なレートを実現することが可能となるからです。

【現地両替所と比較した優位点】
海外に行った際には、通常現地通貨に両替をします。
この際に、エターナルコインを利用して両替を行えば、先述したようにスプレッドが他の業者よりも狭いために従来の両替所よりも現地通貨の受取額が多くなります。

【クレジットカードと比較した優位点】
海外に行った際に、クレジットカード決済をされる方は多いと思います。
日本人が海外でクレジットカードを利用する際には、クレジットカード会社のレートが適用されるため、支払い額が多くなってしまう傾向があります。
しかし、エターナルウォレットを利用して決済をする場合には、スプレッドが低いために支払額が少なくなります。

【電子マネーと比較した優位点】
一か国だけで利用するのであれば、エターナルウォレットより電子マネーの方が、利便性

が高いと思われます。
エターナルウォレットは自国での利用だけでなく、他の国でも利用できるのが特徴であり、優位でもあると考えております。
世界中での利用可能店舗の普及や両替所の普及が進むことにより、既存の電子マネーとの大きな差別化になると考えております。

【従来の海外送金と比較した優位点】
銀行による海外送金では、送金手数料、着金手数料、中継銀行手数料、スプレッド手数料等、多くの手数料が発生します。
エターナルウォレットを利用して送金すれば、お客様同士の P2P 取引となりますので、送金コストは、ほぼ無料で行うことが可能となります。

【分割機能】
仮想通貨の価格が上がると、小額決済ができなくなります。
エターナルコインは利用される仮想通貨を目指しているため、エターナルコインの価格が上がりすぎた場合には分割を行い、利用されやすい単位に調整されます。
エターナルコインを１０分割すると、エターナルコインの価格は１０分の１になりますが、保有するエターナルコインのコイン数は１０倍となります。

【公認取引所】
エターナルコインを取り扱う公認取引所は、一か国に対して一取引所としています。
また、公認取引所ではエターナルコイン以外の仮想通貨の取引は行えません。

この体制を敷く理由は二つあります。
一つ目の理由は、エターナルコインは世界に一つしかありませんが、一か国に取引所が 2 カ所以上あると、取引所ごとに発行するフィアット通貨（基軸通貨）が複数存在することになりますので、利用可能店での受付可能フィアット通貨が複数になることになります。
そうなると、利用可能店がどこの取引所で発行したフィアット通貨を受け入れてよいのかという問題や、出金申請を複数の取引所に対して行わなければならないという負担も増すことになります。
このように、利用可能店側にデメリットがあるために一か国に対して取引所は一つという体制をとっております。

二つめの理由は、エターナルコインは各国の取引所の普及活動により広がっています。
多数の仮想通貨を扱う取引所でエターナルコインの取り扱いがされても、その取引所ではエターナルコインが利用できる店舗の開拓は行っていただけないでしょうし、エターナルコイン専用のコンテンツの開発も行っていただけないでしょう。
しかし、エターナルコインだけを取り扱う取引所であれば、利用できる店舗の開拓や、エターナルコインの利用者を増やすための広報活動、またコンテンツの開発等も行っていただけます。
このような理由から、エターナルコインを世界中で使える仮想通貨とするために、取引所は一か国に一つとさせていただいております。

【今後追加される機能】
海外送金や外貨両替を世界一安い手数料で実現するために、現在以下のような仕組みを構築しております。

以下、本文では表記上、現金や銀行内にある通貨を、円・ペソと表記し、ウォレット内にある通貨を JPY・PHP と表記します。
また、エターナルコイン（XEC）を取り扱える取引所は日本、香港、フィリピン、韓国にありますが、説明を分かりやすくするために登場する国を日本とフィリピンの 2 か国とします。

≪ワンタッチ送信の問題点≫
現在のウォレットには、異通貨ワンタッチ送信機能があります。
異通貨ワンタッチ送信機能というのは、例えば日本からフィリピンに海外送金を行うときに、日本円を成り行き買いでエターナルコインを購入し、次に成り行き売りでエターナルコインを売って、フィリピンペソにした後に、フィリピンのウォレットにペソを送る機能です。
3 つの手順がワンアクションで完了する機能となっており、その利便性からエターナルコインを利用した海外送金に多くの人により利用されていますが、デメリットとしては、多額の送金を行う時には着金額が少なくなるという問題があります。
成り行き買いと成り行き売りを行うということは、エターナルコインの価格が市場の板の厚さに依存しているために、板が薄いと表示よりも高い価格で XEC を取得し、XEC を売却するときには表示よりも安い価格で売却するということになってしまいます。
このように現在の異通貨ワンタッチ送信機能では少額の送金には適していますが、多額の送金には適していません。

≪両替機能≫
この問題を解決するために、銀行の中値レートでの両替ができる仕組みを現在構築しております。
中値で両替ができるということは、すなわち世界一安いレートで両替ができるということになります。
海外送金を行いたい利用者は、ウォレット内で海外送金を行いたい国の通貨に両替した後に、送金先ウォレットに相手国の通貨を送ることによって、世界最安値で海外送金を行うことが可能となります。

≪両替の問題点≫
通常、両替を行うためには街の両替所や銀行といった中間業者が必要となります。
そして一般的に両替手数料が高い理由の一つは、この中間業者に支払う手数料が発生することに起因しています。

手数料を下げるためには、中間業者を介在させない相対での取引を行う必要があります。
いわゆるマッチング取引となりますが、マッチング取引の問題点はマッチングの相手が必要だということです。
マッチング取引を行って海外送金を行っているサービスは既に存在しますが、問題点があります。
例えば、日本とフィリピンという国を考えた時に、日本からフィリピンに海外送金を行う人とフィリピンから日本に海外送金を行う人（額）が同じくらいであれば問題はありません。
しかし、実際には日本に来ているフィリピン人が家族への仕送りに送金をしている額の方が多くなっております。
マッチングによる海外送金業社の中には、全ての取引をマッチングさせず、ネッティングでの取引を行っている業者もあります。
例えば、日本からフィリピンへの海外送金額が 1 億円、フィリピンから日本への海外送金額が 8000 万円だとしたら、差額の 2000 万円だけを、実際に銀行を利用して海外送金を行うことによって銀行送金手数料を低くすることができます。
しかし、上記のロジックでは実際に銀行を利用して海外送金を行う必要があるために、銀行送金による様々な手数料が発生します。
海外送金は必ず 2 国間で行われるために、互いの国の送金額がまったく同じとなるのは不可能です。
このように従来のマッチングを利用した海外送金サービスでは、送金額の違いがあることから銀行送金を行う必要があり、それがコストとなり利用者の手数料として反映されます

この問題を解決するためには、2 国間での両替額が限りなく同額に近づく必要があり、同額に近づくことによって、両替手数料が安価なサービスを実現することが可能となります。

≪プール≫
上記の問題は、エターナルウォレットを利用した両替にはプールという専用ウォレットを利用したロジックでの両替を行う事で解決します。
プールには、XEC、JPY、PHP などが入ります。
このプール内にてマッチング取引による両替を行います。
プールに入る XEC はユーザーから貸し出された XEC となり、JPY や PHP は両替を行うユーザーから入るということになります。

≪両替手数料≫
両替手数料は、両替額の 1%相当の XEC となります。(手数料は現時点では未定ですので仮として表記しています)
両替を行いたいユーザーは、自動で両替手数料分の XEC が両替時に引かれます。

≪プールに XEC が必要な理由≫
ユーザーが両替を行うときには、単純に JPY から PHP に両替するのではなく、JPY にて XEC を購入して、その後 XEC を売却して PHP を手に入れる必要があります。
その一連の取引はプール内で行われる事になり、ユーザーはワンタッチで両替が行われますが、両替を行った取引履歴には 2 つの取引が瞬時に行われているため、下記のように表示されます。

（例）1XEC が 100JPY。1XEC が 200PHP
10：01　　100000JPY で 1000XEC を購入
10：01　　1000XEC を売却して 200000PHP を取得

このような取引履歴となりますが、この XEC はユーザーから借りた XEC ですから、取引が終了した時点で貸し出されたユーザーのウォレットに自動で送信されます。
XEC を貸し出す人のメリットは、取引に利用された XEC 手数料の一部を利息として受け取れるというものです。(取引に必要な XEC は両替時の取引所のレートとなります。)

では、日本の取引所のユーザーばかりが XEC を貸し出すとどうなるかというと、貸し出す人が多いということは、市場で XEC を購入することになるので、単純に XEC／JPY の価格が他のペアよりも高くなります。
取引所が日本とフィリピンの 2 つだとすれば、フィリピンで XEC を購入した方が得という

ことになります。
そして、2 つの取引所にて相対的に XEC の価値が違うということは、アービトラージが行えるということになります。

例えば、日本のユーザーが JPY を PHP に両替し、その PHP にて XEC を購入して、XEC を JPY にすることで利益を得ることができます。
このようにアービトラージが発生すると、各国取引所間の XEC の価格差が小さくなるため、市場からは歓迎されることとなります。
以上が、XEC がプールに必要な理由の一つとなります。

しかし、上記の取引だけを見ると、誰も PHP を入金していないので、JPY から PHP に両替を行った人が出金できないということになります。

≪JPY や PHP の発行者について≫
JPY や PHP は各国の取引所が発行していますが、好きなだけ発行することはできません。
例えば、ユーザーA から１００円の入金があった場合、１００JPY がユーザーA のウォレットに反映されるので、JPY の発行は取引所が行っているということになります。

しかし、無限に発行しても意味がありません。例えば、自社で 1 億円分の JPY を発行して、それを現金で出金しようとしても、ユーザーからの入金が 1 億円分なかったら、取引所は 1 億円を出金する事ができないからです。
仮に 1 億円分の入金がユーザーからあったとしても、それを引き出すとユーザーから出金申請があった際に対応できなくなります。

したがって、ユーザーから入金があった金額分だけ、取引所は JPY を発行できる仕組みとなっており、逆にユーザーが出金を行った際には、ユーザーの JPY が取引所に戻って来る事になる為に出金額分の JPY が消滅します。

≪ユーザーの JPY や PHP もプール内に入る≫
例えば、JPY から PHP に両替を行うということは、プール内に JPY を入れて、XEC を購入して PHP として、PHP がユーザーのウォレットに入金されるということになります。
ですので、上記の取引を行うということは、プールに JPY が残り、PHP が無くなるということになります。

≪XEC の貸出金利の変動制≫
各国においての両替額の偏りを解決するために、本機能では変動金利を採用します。

例えば、日本円からフィリピンペソへ両替する人が多い場合は、反対の取引であるフィリピンペソから日本円へ両替する人を増やす必要があります。
しかし、そもそも両替を行いたくない人に両替を行ってもらうということは、現実的ではありません。
しかし、フィリピンの取引所で PHP から JPY に両替する人が増えれば、問題は解決します。

フィリピン取引所に入金をしていただけるお客さまを増やすために、フィリピンのウォレットからプールに貸し出された XEC は、日本のウォレットから貸し出された XEC よりも高い金利となるように設定されます。
設定値はプールにある PHP や JPY の残額から自動的に算出されます。
フィリピンウォレットから貸し出された XEC の利息が高いということは、PHP にて XEC を購入しようという人が多くなります。

≪不正防止≫
貸し出し金利が違うということは、貸出金利が高い国のウォレットから XEC を貸し出した方が利益を取れることになるので、中には不正をする人も出てくるでしょう。
不正とは、日本人がフィリピン人の知り合いにウォレットを作成してもらい、そのウォレットを利用して XEC を貸し出すというロジックです。
この対策として、PHP から購入した XEC しかプールに貸し出せないようにします。

この不正を行うためには JPY を PHP に両替をした後にフィリピンの知人のウォレットに PHP を送信し、PHP で XEC を購入して配当を受け取ったのち、XEC を JPY に戻すという方法が考えられますが、これは、貸出金利の割合が両替手数料の割合を上回ることがなければ回避することができます。

≪XEC の先着順制度≫
XEC を貸し出す人のメリットは、先述したように手数料が入るということです。
では、XEC を貸したらすぐに手数料が入るのかといえばそうではなく、貸し出した順番が早い人から順次消化されるということになります。

XEC は世界共通ですが、プール内には貸出金利別の部屋があり、国別の XEC を入れておく部屋を分けておく（パーテーションで区切る）ことによって貸出金利を管理します。

≪貸し出した XEC のポジション≫
ユーザーが貸し出している XEC には、ユーザーのウォレット内に入っていないことになる

ために、XEC の分配（DoT 機能）がありません。
しかし、XEC の貸し出しを中止したい時には、貸し出しを取り消すことができます。

≪プール内の PHP の取り扱いについて≫
2 国間で両替を行う人のバランスを取るために、貸出金利をご説明しましたが、これだけでは問題を解決できたことにはなりません。
貸出金利の高いフィリピンのユーザーが PHP を利用して XEC を購入した場合には、PHP がプールに入るわけではありません。
ユーザーが XEC を手に入れたということは、取引所を通じて別のユーザーが XEC を売却して PHP を手に入れたということになりますので、PHP は XEC を売却したユーザーのウォレットに入金されることになります。
つまり、プールには PHP が入っていないという事になります。

しかし PHP で購入した XEC は金利が高いため、PHP／XEC を購入するメリットが生じ、PHP／XEC のレートは JPY／XEC に比べて高くなります。
レートに差が出るという事はアービトラージが発生します。

アービトラージの仕方は、相対的に安い JPY で XEC を購入し、その後 XEC を売却して PHP にするということです。
そして、PHP を両替して JPY に戻します。
これでアービトラージが完了します。

この取引（成り行き注文の場合）が行われるということは、PHP／XEC の板に誰かが指値の買注文を入れておく必要があります。（指値注文の場合は成り行き注文でオーダーを出すユーザーを待つ必要があります）
アービトラージ取引が完了するためには、PHP を手に入れるユーザーが XEC を売却する取引を行うので、逆の取引となる XEC を買いたいユーザーがいることになります。
成り行きで売り注文を出すということは、誰かが PHP／XEC の板に買いの指値注文を出しているということです。
ということは、フィリピンのユーザーは PHP を取引所に入金はしているけれど、まだ XEC は持っていない状態となります。
ですので、この PHP は指値注文を出しているユーザーの物ですので、この時点では PHP がプールに移動することはありません。
しかし、上記のアービトラージを行うと最終的に PHP を JPY にする必要があるために、両替を行うので、指値注文を出していたユーザーの PHP は、アービトラージを行ったユーザーのウォレットへ移動し、その後両替を行う事によりプールへと移動することになりま

す。

アービトラージを行う方法は、もう一つあります。
フィリピンの PHP を JPY に両替した後、JPY で XEC を購入して、その XEC を PHP に戻すというやり方です。
このアービトラージ取引が行われることにより、PHP から JPY へ両替するユーザーが現れるということになります。
この取引においても同じように、プールに PHP が入るということになります。

このように、XEC の貸し出し金利が発生することによって、PHP／XEC の価格が高くなることになり、その結果、アービトラージが発生し、JPY から PHP の両替と PHP から JPY の両替の額は限りなく同じ額に近づく事になります。

以上で説明いたしました、プールと仮想通貨の貸出金利という世界で初めての概念により、エターナルコインでは今まで解決できなかった送金手数料の大幅な引き下げを可能にいたします。

４．エターナルコイン概要

エターナルコイン発行元	株式会社アトムソリューションズ
正式名称	XEC（エターナルコイン）
総発行数	2 億 XEC
送受信速度	0.5 秒～3 秒 （インターネットの環境により遅れる場合有）
送受信方法	エターナルウォレットを介した P2P 取引
エターナルコイン入手方法	弊社公認取引所での市場取引による入手及び利用者の相対取引
エターナルコイン取引手数料	1 取引に対して日本円約 5 円相当の XEC
トランザクションフィー分配率	全 XEC 取引手数料の 50%を XEC 保有率に応じて分配
トランザクションフィー分配日	毎週水曜日 12：00（日本時間）
最少取引数	0.00001 XEC
最少取引単位	1 円、1 フィリピンペソ、1 香港ドル、1 米ドル、 1 韓国ウォン
取引可能時間	24 時間 365 日
取引所	日本： Eternal Live フィリピン： Token Hub 香港： Eternal Hong Kong 韓国： Eternal Korea
取引可能通貨ペア	XEC/JPY 、 XEC/PHP 、 XEC/HKD 、 XEC/USD 、 XEC/KRW