http://mobile.nytimes.com/blogs/dealbook/2014/01/21/why-bitcoin-matters/?smid=tw-share

ビットコインに注目すべき理由

[](http://mobile.nytimes.com/images/100000002662257/blogs/dealbook/2014/01/21/why-bitcoin-matters/?from=dealbook)

マーク・アンドリーセンは、ベンチャー・キャピタルAndreessen Horowitzの共同創立者です。

KEITH BEDFORD / REUTERS

MARC ANDREESSEN著

2014年1月21日

*編集者注：マーク・アンドリーセンのベンチャーキャピタル、Andreessen Horowitzは、ほぼ5000万ドルに達する金額をビットコイン関連のスタートアップ企業に投資しました。同社は、さらに多くのビットコインに関連した投資機会を積極的に探っています。ただ、彼自身が保有しているビットコインの金額は、わずかです。*

得体の知れない新技術が、どこからともなく出現するように見えます。実際には20年間もの期間にわたって、無名の研究者が入念に開発と研究を繰り返した結果です。

政治的な理想主義者はその中に自由と革命のビジョンを見出し、既存のエリートは嫌悪と軽蔑を投げつけます。

一方で、技術関係者（つまり、オタク）は無性にひきつけられていきます。膨大な可能性を発見し、昼夜問わず没頭します。

[**ビデオ | ビットコイン信奉者** 規制当局がビットコインの良し悪しの議論に明け暮れている一方で、実際の社会における価値が上昇しています。その結果、次の疑問が浮かび上がってきました： お金をお金たらしめているのは、一体何でしょう？](http://mobile.nytimes.com/video/2013/11/24/business/100000002563247/david-gillen-bitcoin-believers.html?from=dealbook)

やがて、実社会において製品、企業、産業が生まれ、商業化が進み、影響が深く浸透し、後になって、どうしてもっと早くから可能性に気づかなかったのだろう、と多くの人が首をかしげるのです。

どの技術についての話かって？1975年のパソコン発明、1993年のインターネット発明、そして（私の考えでは）2014年のビットコインです。

ビットコインについては、語りつくされているように見えます。しかし、メディアや一般大衆が捉えているビットコインの姿と、大規模な数に増え続ける技術専門家が信じているビットコインの姿との間には、大きな違いが存在したままです。この記事では、ビットコインがシリコンバレーのプログラマーや起業家をなぜこれほど多く惹きつけているかについて説明し、そしてビットコインが持つ将来の可能性について私の考えを披露します。

まず、ビットコインはその根本において、コンピューター工学の革命であり、世界中の数千もの研究者による、20年に及ぶ暗号化通貨の開発と、40年に及ぶ暗号化の研究の成果です。

ビットコインは、ビザンチン将軍問題（B.G.P.）としてコンピューター工学で長い間存在してきた課題に初めて実用的な解を与えました。B.G.P.を定義した文書の一部です：「ビザンチン帝国の将軍達が、敵国の都市を包囲している状況を想像してみましょう。将軍達は、使者を通じたやりとりのみに頼って、とるべき戦術に合意しなければなりません。しかし、将軍達の中には裏切り者がいて、他の将軍達を混乱させようとたくらむ可能性もあります。課題は、国家に忠誠を誓う将軍達が必ず合意できるようなアルゴリズムを発見することです。」

より一般的に言えば、B.G.P.はインターネットのように信頼性が確立されていないネットワークにおいて、互いに無関係の他人同士が信頼を築くためにはどうすればよいか、という問題を提起しています。

ビットコインはこの問題に初めて実用的な解を与えます。インターネットにおいて、あるユーザーが特定のデジタル資産を別のユーザーに渡し、転送を安全でセキュアに行うだけでなく、転送が行われたことが誰の目にも明らかになり、転送の正当性に誰も疑問を挟めないようにできます。この革命が何をもたらすかについては、強調しすぎることはありません。

どのような類のデジタル資産が、この方法で転送できるのでしょう？デジタル署名、デジタル契約、デジタルロック（オンラインのロッカーや、物理的な鍵）、車や家屋といった実体のある資産のデジタル所有権、デジタル株式や債券、そしてデジタル通貨です。

これらは全て、信頼に基づいた分散型ネットワークを通じて交換され、銀行やブローカーのような仲介者を中心に置く必要はありません。資産の持ち主だけが送り、指定された受け手だけが受け取れ、資産は一度に一箇所にのみ存在でき、誰もがあらゆる取引や資産の所有権を検証できます。

どんな仕組みで機能するかって？

ビットコインはインターネット上に分散された台帳です。ユーザーは、現金を用いるか、ビットコインの商品やサービスを売って、上限が決められている台帳の欄のうち一つを購入します。自分のビットコインを、台帳の欄を購入したいほかのユーザーに売って、台帳から抜け出ることもできます。世界中の誰もが、好きなときに台帳に参加したり、離脱できます。許可を得る必要はなく、手数料も無料か非常に低く抑えられます。ビットコイン「コイン」自身は、台帳の記載内容にすぎません。株式取引所の会員権のようなものです。ただし、実社会での応用範囲はずっと広くなります。

ビットコイン台帳は、新しい決済システムです。世界中の誰でも、どんな金額であっても、台帳の所有権を移動するだけで、ビットコインを用いて他の誰かに支払を行えます。金額を入力し、送金すれば、受け手は金額を受け取れます。誰かから許可を得る必要はないし、ほとんどの場合手数料もかかりません。

2番目の点は非常に重要です。ビットコインは、取引が手数料ゼロまたは非常に低い値（数セント単位）で行える、初のインターネット決済システムです。既存の決済システムは2－3％の手数料を取り、先進国ですら、そうです。他の多くの場所では、現代的な決済システムは存在しないか、手数料が非常に高くつきます。この点は、後ほど振り返ってみましょう。

ビットコインはデジタルの持参人払式債券です。信用度が無くても、金額や資産を他人との間で取引できます。最も単純な方式では、メールやテキストメッセージを用いて、数列がやりとりされます。送り手は受け手を知る必要も、信頼する必要もありません。逆もまたしかりです。それに関連して、支払拒否も発生します。（この点は現金に似ていますね。）現金や資産を持っていれば、支払ができます。持っていなければ、できません。これは斬新な点であり、デジタル形式では、これまで存在していませんでした。

ビットコインはデジタル通貨であり、価値は次の2点から生まれています：現時点における決済システムの利用状況（台帳を通じて行われる取引の量と速度）と、決済システムの将来における利用状況の推測です。これが、混乱を生んでいます。ビットコイン通貨に始めから特定の価値があるため、人々が利用しているのではありません。人々がビットコインを用いて取引（どこにいても、詐欺の心配なく、無料または非常に低い手数料で）を行っているため、結果として価値が生じているのです。

現時点においては、ビットコイン通貨の価値の根拠となっているのは実際の取引量よりも投機的な思惑なのは事実でしょう。しかし、投機により通貨の価値が十分に上がり、支払が実用的に行えるようになったのもまた、事実です。ビットコインは、実社会で支払が行える取引量を得る以前に、何らかの価値を持つ必要がありました。これは新技術における典型的な「鶏が先か、卵が先か」の問題です。価値が与えられない限り、価値はありません。ビットコインが、半ば投機の力を借りて価値を得たということは、通常よりも早く実用的な段階に達したということを意味します。

ビットコインに批判的な人々は、一般の消費者や企業にとっての使い道が少ない、と言います。しかし、パソコンやインターネットに対してだって、初期段階では同じ批判が寄せられていたのです。毎日、より多くの消費者や企業が世界中でビットコインを購入、使用、売却しています。全体の数はまだ小さいままですが、急速に成長しています。また、ビットコインのツールや技術が向上するにつれ、参加者が誰でも気軽に扱えるようになっています。かつては、インターネットにアクセスするのですら難しかったことを思い出してください。今では、そうではありません。

ビットコインは変動性が高すぎて、企業には受け入れられない、という批判も的外れです。ビットコインはどんな時でも、決済システムとして使えます。業者はビットコインを保持していたり、ビットコインの変動性に晒される必要はありません。個人や企業を問わず、いつでもビットコインや他の通貨を売買できます。

ビットコインで支払う消費者の数がこれほど小さいのに、オンラインあるいはオフラインに関係なく、ビットコインを受け付けたい企業などいるのでしょうか？私のパートナーであるChris Dixonは、こんな例を披露しました：

「オンラインで電化製品を売っているとしよう。この商売における利益率は通常5%以下だ。つまり、一般的な2.5%の取引手数料を支払うと、利益の半分を持っていかれる。その金は、本来なら事業に再投資したり、消費者に還元したり、政府に税金として収めることが可能なはずだ。そうした可能性がある中で、インターネット上でビットを動かすだけで銀行に2.5%を渡すのは、最悪の選択肢となる。企業にとって、支払を受け付ける際のもう一つのリスクは、国境を越えた支払だ。どうして欲しい商品が自分の国では売っていないのかというと、通常は支払い方法が原因だ。」

さらに、ビットコインがクレジットカード詐欺のリスクを無くすのも、企業がビットコインに惹かれる理由です。この詐欺は犯罪者にたいそう好まれるため、パソコンの情報とクレジットカード情報を盗まれないように多大な努力が払われています。

ビットコインはデジタルの持参人払式債券です。支払の受け取り手が送り手に関して得られる情報を抑え、業者や業者を通じて犯罪者が、送り手から将来お金を騙し取れないようにできます。

クレジットカード詐欺は企業、クレジットカード業者、銀行にとって非常に重要な課題です。オンライン詐欺の検出システムは、本物の詐欺であるかどうかに関係なく、ほんの小さな疑いが発生しただけでも作動するように作られています。その結果として、多くのオンライン業者が注文の5～10%を拒否する事態が発生しています。顧客がビットコインを用いて支払を行っていれば、そうした注文も安心して受け付けることが可能になります。こうした注文は既に確定しているため、本質的に、業者にとっては利益に直結します。そうした注文を処理できるのであれば、多くの業者の利益率は大きく改善されるでしょう。

ビットコインの詐欺防止機能は、小売店やその客などの、オンライン外の世界にも適用できます。

「ターゲット」デパートチェーンにて、7000万以上もの消費者のクレジットカード情報が流出したような事件は、ビットコインを用いれば、起こりえなかったはずです。ビットコインを使えば、次のような仕組みが構築できます：

ショッピングカートに商品を詰め込み、レジへ向かいます。クレジットカードを指し出す代わりに、スマートフォンを取り出し、レジの画面に表示されるQRコードの写真を撮ります。QRコードには、ターゲットに送金する必要のあるビットコイン金額の情報が内蔵されています。スマートフォン上で「確認」をクリックすると、取引が成立します（ビットコインを所持していない場合、銀行口座内の現金がビットコインに変換されます）。

ビットコインは即座に現金と引き換えることもできるため、ターゲットは喜んでビットコインを受け付けます。取引手数料もほとんどかかりません。客側にしてみれば、個人情報が盗まれないので安心です。犯罪者にしてみれば、好ましくない事態ですが。（犯罪者にも利点はあるかもしれません：業者のコンピューターシステムのセキュリティが甘ければ、そこから盗もうとするでしょう。しかし、たとえそれがうまくいっても、消費者側は損失、詐欺、なりすましの被害に遭わずにすみます）。

最後に、犯罪者やテロリストが責任を問われずに匿名で送金できるため、ビットコインは犯罪行為の温床になっているという批判に答えようと思います。これは幻想です。メディアが大げさに書き立てたのと、ビットコイン技術についての理解があまり進んでいないのが、その原因です。Eメールを追跡することが可能であるのと同様に、ビットコインだって完全に匿名なわけではありません。むしろ、変名に近い形です。さらに、全ての取引はビットコインネットワークで追跡され、永久にブロックチェーンという高級記録内に保存され、誰でも閲覧できます。つまり、警察組織にとっては、現金や貴金属よりも、ビットコインのほうが追跡しやすくなっているのです。

ビットコインの将来はどうなるのでしょう？

ビットコインは典型的なネットワーク効果や正のフィードバックに基づいています。より多くの人がビットコインを利用するほど、ビットコインは誰にとっても価値が上がっていきます。そうすれば、ビットコインを試すのも簡単になっていきます。ビットコインのネットワーク効果は、電話、インターネット、eBayやフェースブックのようなオンラインサービスと似ています。

ビットコインのネットワーク効果は、4つの要素で構成されています。利己的な動機で、ビットコインの価値を高めようとする参加者が4種類存在するからです。（１）ビットコインを支払に利用する消費者、（２）ビットコインによる支払を受け付ける業者、（３）分散型信頼ネットワークを支え、全ての取引を処理して検証するために演算を行う「採掘者」、（４）ビットコイン上で新たに商品やサービスを構築する開発者や起業家です。

ネットワーク効果の4つの要素全てが、不可欠な役割を果たしてシステム拡大を担っていますが、4番目が特に重要です。

シリコンバレーや世界において、何千人というプログラマーが、以前では不可能だった新製品や新サービスを試す場としてビットコインを利用しているからです。私が関わるベンチャーキャピタル、Andreessen Horowitzにおいても、ビットコイン上で起業する素晴らしい起業家が続々と増えています。その中で少なからぬ会社が、金融業界にて実績を積んでいます。

この理由だけでも、ビットコインに対抗しようとする勢力は苦戦を強いられるのがわかるでしょう。現時点でビットコインの代替となるものがあるとすれば、ビットコインを大幅に強化し、かつそれを素早く実行に移す必要があります。さもなければ、ネットワーク効果により、ビットコインの優勢が確定するでしょう。

ビットコインを元にしたイノベーションの中でも、わかりやすく、かつ巨大な分野は、国際送金です。毎日、膨大な数の低所得者層が、労働で得たお金を本国の家族に送金しています。世界銀行によると、年間4000億ドルに達する見通しです。同様に毎日、銀行や送金業者は膨大な手数料を徴収しており、10%や時にはそれ以上のお金を送金時に徴収しています。

手数料がゼロまたはほとんどかからないビットコインに切り替えれば、こうした送金を通じて移民労働者やその家族の生活は大幅に改善されるでしょう。実際、世界の貧困地域において、多くの人に対して素早く好影響を与えることが可能なものは、他には考え付きません。

さらに、ビットコインを通じて、世界中の人々が、これまでよりもずっと大きな数で、現代の経済圏に参加できるようになります。世界中で、銀行制度や決済システムが完全に現代化されているのは、たった20カ国程度です。他の175カ国には、長い道のりが残されています。つまり、ほとんどの国にいる多くの人は、西洋社会で当たり前のように使えるサービスや商品とは縁が無いまま生活しているのです。完全に仮想化されたサービスであるNetflixですら、40カ国程度でしか利用できません。誰もがどこからでも、いつでも利用できる国際決済システムであるビットコインは、現代の経済システムを地球上の誰にでも利用できるように広める、強力な推進力なのです。

ここ米国においてすら、長い間課題とされてきた問題は、「銀行に拒否された人々」－伝統的な銀行口座を持たない人々ーが、基本的な金融サービスを受けるときでも支払う必要のある高額の手数料でした。ビットコインは既存の金融システムの外側にいる人々に対して、手数料が非常に安く済むサービスを提供しやすくして、この問題を直接解決できます。

ビットコインの第三の魅力的な使い道は、マイクロ決済（超小型決済）です。マイクロ決済は、20年間の努力にも関わらず、現実化していません。小額の決済を行うのが、既存のクレジットカード/銀行口座や金融制度では現実的ではないからです（1ドル未満、数セントあるいは1セント未満だと仮定してみてください）。こうしたシステムの手数料体系では、マイクロ決済は不可能です。

しかし、ビットコインを用いれば、あっという間にそれが簡単になります。ビットコインは、無限に分割できるという便利な特性を備えています。小数点以下8桁まで今は対応できますし、将来はもっとできるようになるでしょう。つまり、1セントの1000分の1というような小額を指定し、世界中の誰に対しても手数料無料（あるいはほぼ無料）で送金できます。

オンラインコンテンツを有料化する場合を考えてみましょう。新聞のようなメディア事業がコンテンツ課金できずにいる理由の一つは、全てに対して課金（コンテンツ全体の購読料）または全てを無料（ウェブのいたるところに醜悪なバナー広告が貼られることになります）、の2つの選択肢しかないためです。しかし、ビットコインを用いれば突然、記事単位やセクション単位、時間単位、ビデオ再生毎、アーカイブのアクセス毎、あるいはニュース速報毎に、小額課金を実用的に行える方法が得られます。

ビットコインのマイクロ課金は、スパム対策にも使えます。未来のメールシステムやソーシャルネットワークは、小額のビットコインが付属していないメッセージは拒否することができます。あまりに小額なので送信者にとっては気になりませんが、引責を気にせず何十億とメールを送るスパム業者にとっては高額になります。

最後に、第四の興味深い使い道は募金活動です。このアイデアは、2-3ヶ月前、あるニュース記事の中で見つけました。スポーツ試合のテレビ中継にて、とある観客がQRコードと「ビットコイン求む！」と記載されたプラカードを掲げていたのです。彼は24時間以内に25000ドル相当のビットコインを、赤の他人から集めることができました。テレビ番組や写真、あるいは直接手に持ってカードを掲げた人物に対して、スマートフォンで2回ほどクリックするだけで送金できた、史上初の例です。カード上のQRコードを写真に撮り、クリックすれば送金できたのです。

これが抗議行動でどうやって利用できるか、考えて見ましょう。今日、抗議活動を行う人々はテレビにて、活動の意義を訴えます。近い将来、彼らはテレビにて資金を集めるために、活動の意義に賛同する世界中の人々から瞬時に資金を得るために、カードを掲げることになるでしょう。ビットコインは、最も頑固な反資本主義活動家にとってすら、夢のような技術なのです。

今後数年間、この新技術を巡って非常に面白い運動や、出来事が起こるでしょう。

例えば、有名な経済学者の中にはビットコインに対して深く疑いの目を向けている人々もいます。ベン・バーナンキ前FRB議長は最近、ビットコインのようなデジタル通貨は「長期的な見込みがある。特に、決済をより素早く、安全に、効率よく行えるのであれば」と記述しました。1999年に、伝説的な経済学者であるミルトン・フリードマンはこう言っています：「現在存在しないが、将来必要になるのは信頼できる電子通貨だ。インターネットにおいて、AとBという2者が、互いを知らなくても資金を移動できる方法とも言える。私が20ドル札を手に取り、君が誰であるかを知らなくても、君に渡せるようなものだ。」

今日、ビットコインを批判する経済学者は正しい理屈を述べているのかもしれませんが、私個人はベン・バーナンキとミルトン・フリードマンを信じます。

さらに、規制関連で解決しなければならない課題が山積みです。ビットコインのような技術を予測して金融制度や決済システムを構築していた国家は存在していませんから。

ただ、ここではビットコインの巨大な可能性について少しでも理解していただけたら、と考えています。単なる自由主義者の夢やシリコンバレー発の話題ではなく、ビットコインは金融制度がインターネット時代にどう機能できるか、どう機能すべきかについて明確にできる可能性を秘めています。また、個人と企業の両方にとって、有利になるようにシステムを変革する力も秘めています。