**ビットコイン：初期評価**

FXと為替相場｜グローバル第5号、2013年12月

**David Woo** +1 646 855 5442 FXと為替相場担当ストラテジスト MLPF&S david.woo@baml.com

**Ian Gordon** +1 646 855 8749 FXストラテジスト MLPF&S ian.gordon@baml.com

**Vadim Iaralov** +1 646 855 8732 FXストラテジスト MLPF&S vadim.iaralov@baml.com

**防犯機能内蔵、供給量有限、分割可能**

私達は、ビットコインがe-コマースの主流決済方式となり、伝統的な送金業者にとって深刻な競合相手になる、と信じています。交換媒体として、ビットコインは明らかに大きな可能性と発展性を持つ、と私達は見ています。

**非合法市場のための貯蓄手段なのでしょうか？**

高額の税金を逃れ、資金を操作し、横領を行おうとする人々がビットコインの恩恵を得られる、と言われています。ビットコイン取引全体における人民元の割合と、ビットコイン価格が密接に関係しており、しかも上昇を続けています（グラフ1）。それを踏まえた上で、ビットコイン取引が全て公開されており、個々のビットコインには改変不可能な取引記録が残っているという事実は、最終的にブラックマーケットや犯罪市場における普及に歯止めをかけるでしょう。

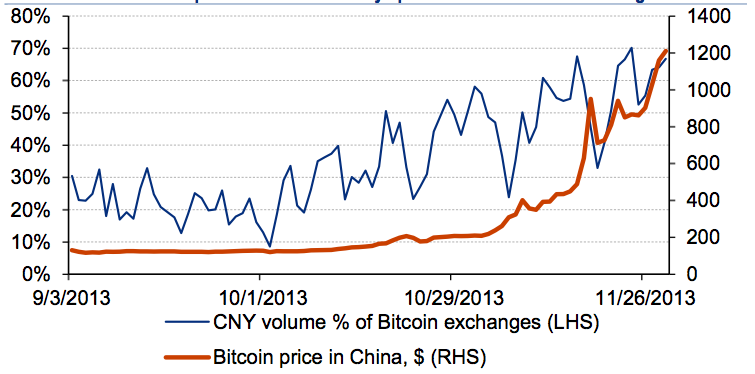
**変動性**

貯蓄手段としてのビットコインの役割は、交換媒体としての利用価値を減らす可能性があります。投機的な活動のおかげで変動性が高くなっており、ネット取引における支払方法としての普及があまり一般的には広まっていません。

**価格は適切なのでしょうか？**

ビットコインはバブルなのでしょうか？ビットコインが（1）eコマースや送金市場における主要な手段に成長し、（2）銀と同様に貯蓄手段として信頼されるまでに成長したと仮定します。その状態で、私達が分析するビットコインの公正価格は次の通りです：***ビットコインの最大時価総額＝150億ドル（1BTC＝1300米ドル）***この結果により、今年に入ってから100倍に膨れ上がったビットコイン価格は、経済の基本原理を逸脱しているリスクを孕んでいることが示唆されます。

**グラフ1：最近のビットコイン価格変動は中国市場の為替における投機が原因**



青：ビットコイン両替市場における人民元の割合(%)（LHS）

赤：中国におけるビットコイン価格（$）（RHS）

ソース：BofAメリルリンチ・グローバルリサーチ

**ビットコインとは何でしょう？**

Vadim Iaralov +1 646 855 8732

ビットコインはサトシ・ナカモト（匿名）によって2009年に設計されたデジタル通貨です。ビットコインを通じて、権力分散型のピアツーピアネットワーク経由で支払を行えます。決済を承認する中央官庁や、取引認証を行う金融機関を必要としないというユニークな特徴を持ちます。あるビットコイン口座／アドレスへ支払を行うためには、ビットコインソフトとインターネット接続が必要です。

ビットコインの最小単位は**サトシ**です。1ビットコインは1億サトシに相当します。設計時の制約により、ビットコインの供給量は2100万ビットコイン（2100兆サトシ）を超えることはできません。プログラムされた規定に従い、流通するビットコインの量は予測可能な速度で増えており、2140年まで続きます。現在の流通量は1200万ビットコイン、あるいは最終的な総量の57%です（グラフ2）。

**全ての取引記録が公開**されており、「採掘者」によって常に更新され、認証されています。採掘者は新規取引のまとまりをブロックに変換し、そうしたブロックを「ブロックチェーン」の最後に接続します。公開記録は取引の台帳となり、最初の持ち主から現在の持ち主にいたるまで、全てのサトシが追跡可能です。全ての記録が公開されていることで、買い手自身が使いたいビットコインを実際に所有していることが保証され、詐欺を防ぎます。

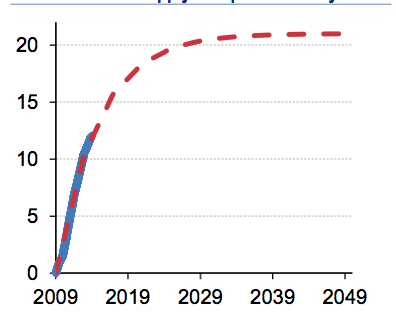
**ビットコインの供給量**は、公開記録（ブロックチェーンのことです）に新しい取引ブロックが追加される度に増えます。採掘者が新規取引を認証するのは比較的簡単に行え、一つのブロック内に多数の取引内容を手軽に圧縮して入力できます。しかし、全体の採掘速度に関係なく通貨供給の増加を一定に保つために、各ブロックにかかる演算処理には相当な困難が付きまといます。未処理の取引が一切存在しない場合でも、採掘者に支払を行うためだけの取引を1つ含んだブロックが生成されます。実際、最初の数百ものブロックは採掘者に支払を行うためだけに生成されており、他の取引は含まれていませんでした。（現在の各ブロックは数千もの取引記録を含んでいます。）この方法により、投機的なリスクを引き受ける覚悟のある採掘者達に、最初の種銭が配布されました。

大雑把な例えを用いるならば、ライバル関係にあるジャーナリスト達（**採掘者たち**）が、国立公文書館に所蔵される前提で国のニュースを毎日記録するよう依頼されているようなものです。各ジャーナリストは記事（**取引記録**）を本（**ブロック**）に記載するよう言われており、公文書館は毎日、そうした本のうち一冊を選択して報酬を払います。公文書館が本を選択して購入する際、追加要求があります。各ジャーナリストは、その日に生まれた人の指紋を10人分集めて、本に追記しなければなりません。そうした人たちは国のニュース（**取引**）とは関係ない人たちです。単に、毎日生成される本の数量を一定に保つために行われているだけです。ジャーナリストが協力しあうことで、同じ誕生日を持つ人をより多く探そうとすると、公文書館は必要な指紋の数を増やします。

**両替所**は現実世界の不換紙幣とビットコインの交換を行います（グラフ1）。両替を行う場合、消費者は与信リスクをとって、個人の口座から第三者の口座へビットコインを移す必要があります。実際の現金を預金機関へ預ける行為と似ています。しかし、銀行と異なってビットコインの第三者口座は規制を受けておらず、FDIC（連邦預金保険公社）保護の対象でもありません。個人口座は簡単に保護できますが、海外政府の管轄に入るスタートアップ企業が創始した両替所でオンラインのデジタル財布を扱うと、ハッカーの攻撃対象になることもしばしばあります。通貨の交換が完了する前に、両替所そのものがお金を持ち逃げするリスクもあります。取扱高の面で主要な両替所は以下の通りです。BTC China (CNY)、OkCoin (CNY)、Mt.Gox (USD, EUR, GBP, JPY, AUD)、FXBTC (CNY)、Bitstamp (USD)、Bter (CNY)、BTC-E (USD)、BTCTrade (CNY)、VirtEx (CAD)。

注1：中央当局が存在しないため、数式処理が所蔵庫の役割を果たします。

**グラフ2：ビットコインの供給量は2140年に2100万で頭打ちになります**

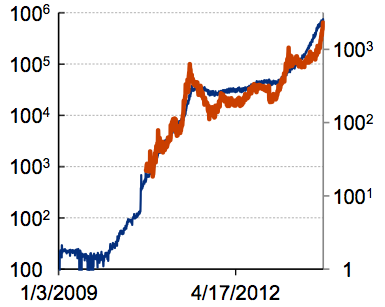


青：ビットコイン供給量（100万）

赤：予想されるBTC（100万）

ソース：BofAメリルリンチ・グローバルリサーチ

**グラフ3：採掘市場は爆発的に成長しています**



青：演算量、GHash/日（LHS）

赤：採掘による収入、$/日（RHS）

ソース：BofAメリルリンチ・グローバルリサーチ

**グラフ4：技術発展により演算がより楽になりつつあります**



青： $1を採掘するために必要な演算 (GHash)

ソース：BofAメリルリンチ・グローバルリサーチ

投機的取引とは別に、ビットコイン環境に関わった企業が初期に目をつけたのは、**ビットコインの交換媒体としての価値**でした。例えば、採掘者は特殊ICをビットコインを用いて購入できます。取引を円滑に進めるため、Bitpayのような支払業者は売り手に対して必要なソフトウェアを提供します。また、支払業者は為替レートと銀行への日常取引を保証して、為替変動リスクを吸収します。2013年4月以降、業者間の両替手段としてのビットコイン用法を開発、普及を行うスタートアップ企業に対して大規模な投資が行われています。（両替に対する投機的投資とは全く異なります。）例えば、CoinLabは採掘業者や両替業者などの他のビットコイン関連スタートアップを育成するための資金を手に入れました。ビットコインを取り入れている企業の中で最も有名なものは、中国のポータル大手であるBaiduでしょう。Baiduは2013年10月より、オンラインのセキュリティー・サービスについてビットコインの受付を開始しました。

BTC価格の急激な上昇（毎年292%）は、同様に**採掘収入**の大幅な伸びも誘発し、結果として**大規模な資本投資**を呼び起こしました。実際、演算処理量は毎年521%（グラフ3）で伸びており、高価で高機能なビットコイン採掘用ICが必要となっています。収入を得ようと競争が激化した結果、簡単に処理できる領域は取りつくされ、今では採掘は数百倍も「深く」行う必要があります（グラフ4）。採掘者がより多くのコンピューターを使用するため、電気代も増えています。付属の章にて、採掘市場と採掘者の課題について述べます。

**費用対効果の分析**

Ian Gordon +1 646 855 8749

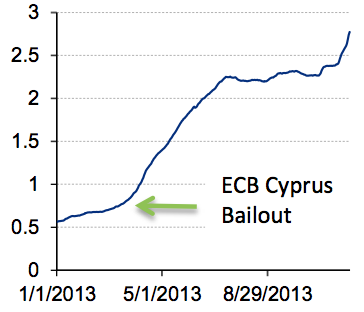
金銭／通貨は一般的に3つの大きな役割を持つと考えられています：取引単位、交換媒体、そして貯蓄手段です。ビットコインは、交換媒体としてユーザーに多くのメリットをもたらし、効率的に扱えます。それは、ビットコインが本質的な価値を持っており、普及が進むにつれてその価値はますます増えていく、ということでもあります。しかし、取引単位と貯蓄手段という役割に関しては多くの短所が見られ、それが原因で究極的には国際通貨の地位を得るには至らないだろう、と私達は考えています。この章では、ビットコインの長所と短所をより詳しく見ていきます。

**長所**

***ビットコインは取引手数料が少なく済むために、交換媒体として魅力的です。***それが可能なのは、ビットコインは決済を承認する中央官庁や、第三者として金融取引を行う金融機関を必要としないからです。分散型のピアツーピアネットワークを用いて、取引はネットワークユーザー（つまり、採掘者）同士で個別に認証されます。認証を行う採掘者に対しては新規発行されたビットコインが報酬として与えられます。加えて、クレジットカードや銀行カード、あるいはその他のeコマース手段を持たない人々も支払い方法が得られます。

***安全保護、取引の透明性、偽造防止についても、ビットコインは現金の代わりとして魅力を持っています。***ビットコインは所有者のコンピューター内に暗号化された状態で収まっており、ハッカーが電子的にアクセスして盗み取るのは、不可能とは言わないまでもかなり困難です。物理的にビットコインを盗むことも可能ですが、現金を得るため小口で行うより、大規模に仕掛けたほうが楽そうです。

**グラフ5：現在までに、ビットコインユーザー数は5倍に成長しています**



矢印：ECB（欧州中央銀行）によるキプロス救済

青：推定ビットコインユーザー数（100万単位）

ソース：BofAメリルリンチ・グローバルリサーチ

また、デジタル形式であるためにビットコインは現金よりもずっと持ち運びがしやすく、大規模な取引が現金で行われているような経済環境では特に大きな利点となるはずです。ビットコインは現金よりも追跡がやりやすい長所も持ち合わせています。各ビットコインには、発行以来の取引が全て電子的に記録されているからです。各ビットコインに取引が記録されているのみならず、全ての取引が公開台帳に記録されており、現金ではありえない透明性が確保されています。こうした透明性のおかげで、規制当局が非合法の疑いのある活動を追跡できます。最後に、自動認証を行えるデジタル形式を採用しているせいで、偽造は不可能です。

***ビットコインの供給量は有限です。***ビットコインは黄金の供給形態を模倣して設計されており、システム的に通貨供給が有限に設定されています。ビットコインの賛同者にとっては、無駄遣いの多い政府や中央銀行を逃れて、通貨の価格を維持する方法に映るでしょう。ビットコインの供給量は2100万に至るまで次第に増加するよう、システム的に設計されています。この計画を達成するために、新規発行されるビットコインの量は毎年50%ずつ、幾何学的に減っていきます。

***ビットコインは比較的匿名性を保つことができ、危険が多発する国家の市民にとって便利です。***

高額の税金を逃れ、資金を操作し、横領を行おうとする連中にビットコインが利用される、と考える人々がいることはわかっています。例えば3月16日に、欧州銀行の救済措置の一環としてキプロス当局が民間の貯金を一部押収しようとした際に、ビットコインへの関心が急激に高まりました。また、中国でもビットコイン活動が急速に広まっており、現在では通貨別に見ると取引の大多数を占めています。資本操作や没収の可能性を逃れようとする人々が、ビットコイン通貨の価値を高めている現実を反映しています（グラフ1）。

***「勝者が全てを手にする」市場では、ビットコインの普及と人気が高まるほど、成功を修める確率も高くなります。***ビットコインの人気が高まるにつれ、競合相手には進出する余地が少なくなり、ビットコインの市場シェアを奪う可能性が減っていきます。他にもビットコインに似た特徴を持つ数種のデジタル通貨が導入されましたが、あまり成功を収めてはいません。私達は、デジタル通貨市場は「一社独占」型の構造を持っていると考えています。ビットコインの普及がより広まり、使いやすくなれば、消費者は他の似たような通貨を代替として試してみる理由がますますなくなります。

***ビットコインは、金のようにリスクに影響されやすい資産との間に負の相関関係を持つため、（資産配分の観点から）大きな長所を有しています。***例えば、10月のFOMC会議にて出された宣言において、期待よりもやや不寛容な政策方針が示唆された結果、金は1%程度価格が下落しただけでしたが、ビットコインは3%でした。

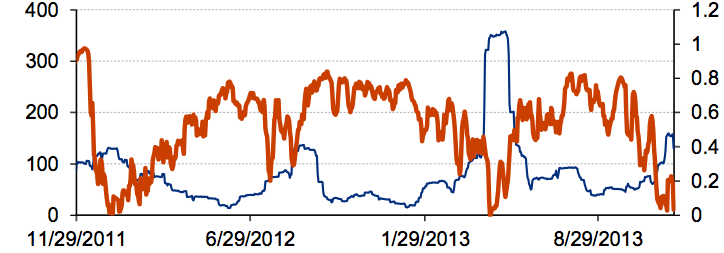
**短所**

***価格変動幅が大きすぎて、貯蓄手段としてのビットコインの役割には大きな疑問がつけられています。***創立以来、ビットコインの対ドル価格は毎日10%のレベルで変動しています。一日の中で価格が190%、上下に振れた日々もありました。こうした変動が意味するのは、より多くの人がビットコインに気づいたり、使い始めたりする中で、ビットコインの根本的価値に対する評価がぶれていることだ、と言えるでしょう。例えば、11月18日に上院で開かれた公聴会を受けて、ビットコインの対ドル価格は50%上がり、785ドルに達しました。

注2：ハッカー攻撃を試みる者がネットワークの過半数を制覇したら、不渡り小切手を流通させるのと同様な手法で二重使用を試みることはあり得ます。ただし、最初の受取人がそれを用いて支払を行えないため、通貨の供給量をごまかして増やすことはできません。採掘市場では大量のコンピューター処理が行われており、過半数を制するようなハッカー攻撃を行うよりは、正直に採掘を行ったほうが手っ取り早いのです。

2－3名の規制担当者がビットコインを代替の支払方法として用いることについて積極的な姿勢を見せたことが原因でした（注3）。これはヨーロッパの政府関係者がビットコインに対して示す態度と一致しています。しかし、より大きな原因は、市場の投機性が高いことでしょう。流通があまり広まっておらず、流動性が低い環境内で投資リターンが不安定であるため、投資家は非常に高いリターンを求めがちになります。変動幅が大きいことは、ビットコインの交換媒体としての役割を損なうことでもあります。価格がこれほど不安定な支払方法を、大規模な小売チェーンが受け入れる可能性は非常に低いでしょう（グラフ6）。現時点でビットコインを受け付けている店舗は、この価格変動コストをうまく内部処理して消費者に押し付けないようにしていますが、そうした割に合わないやり方が長く続くとは思えません。

**グラフ6：ビットコインの取引量の多さが交換媒体としての価値を損なっています**



青：ビットコインの実供給量（LHS）

赤：eコマース／総取引（RHS）

ソース：BofAメリルリンチ・グローバルリサーチ

***ビットコインが現金に比べて効率的で透明性が高いにも関わらず、規制当局が関与を加えるせいで取引手数料が増加する恐れがあります。***まず、「闇市場」における活動や脱税の手助けとなる、と見なされている新通貨を政府が後押しするとはあまり考えられません。結果として、規制当局はビットコインを広範な支払と税金の制度に組み入れ、規制の観点からどうすればうまくいくか、検討しています。結局、どんな規制が加わったとしてもビットコインの手数料は上がってしまうので、ビットコインの主要な長所が減るか、失われることになります。また、ビットコインが外国で簡単に使用できることから、規制面での国際的な協力体制がますます求められていきます。協力体制のおかげでビットコインを巡る規制環境が複雑化する恐れがある一方、いくつかの大きな国家／地域が厳しい規制を課すと、ビットコインの使用コストが大幅に上昇し、交換媒体としての有用さに制限がかかります。

***消費者がドルをビットコインに交換する（逆もあり）ビットコイン両替所の安全性には疑問符が付きます。***自身で採掘できないビットコインユーザーにとって、ビットコインを得る唯一の代替方法は両替所で現地通貨をビットコインと交換することです。こうした顧客が為替リスクを抱えるだけでなく、多くの両替所がこれまでにハッカー攻撃に遭い、顧客のビットコインが大量に盗まれています。報告されている例では、両替所であるBitcoinicaは、システムにハッカー攻撃を受けた後、18,547ビットコインを預金から奪われました。より最近の例では、BIPSと呼ばれるヨーロッパの両替所がセキュリティ侵害を受けて1295ビットコイン（あるいは9900万ドル）を失いました（注4）。ビットコインの見込みユーザーのほとんどは自身でビットコインを採掘できないため、現地通貨をビットコインに変換する上で、両替所が重要な鍵を握っています。預金保護（FDIC）や投資保護（SIPC）が存在しない以上、ビットコインユーザー／投資家は盗まれた資金を取り戻す手段をほとんど持ち合わせていません。つまり、投資リスクに加えて信用リスクも抱えていることになります。

注3：規制当局がビットコインの価値を認め、投資家があわてて同意(http://dealbook.nytimes.com/2013/11/18/regulators-see-value-in-bitcoin-and-investors-hasten-to-agree/?\_r=0)　注4： http://siliconangle.com/blog/2013/11/26/bips-bitcoin-exchange-cleaned-out-in-990k-virtual-heist/

***通貨発行益（注5）が、最高速のCPUを持つビットコイン「採掘者」に行き渡っています。***政府はビットコインの生成を管理できないので、時間が経つにつれて、政府の通貨発行益が失われていきます。つまり、政府にとってはビットコインが大きくならないうちに押さえ込みたい動機が存在します。

**支払の受領確認に50分間かかるため、広範囲の利用が進まなくなるでしょう。**二重使用を防ぐために、ブロックチェーンに十分な数のブロックを追加するのに50分間かかります。お互いを知っている二者間のやりとりならば、二重支払など起こらないとお互いを信頼できるので問題ないでしょう。しかし、匿名の相手の場合、回避不可能なリスクが大きくのしかかります。結果的に、ビットコインの取引を認証し、承認する中央当局の不在が非流動性要素となり、ビットコインは大規模な国際通貨に変貌できなくなるでしょう。

***法定通貨ではないため、国際通貨としてのビットコインの利用は限定されるでしょう。***不換紙幣と異なり、支払方法としてビットコインを受けつける義務は誰にもありません。それゆえ、ビットコインの価値はユーザーが価値を認めているか否か、に全て左右されます。後ろ盾となる買い手が不在なため、ビットコインには使い勝手がない、と思われ始めたら、ビットコインは急速に消え去る可能性があります。突発的な価格変動やさらなるハッカー攻撃が繰り返されれば、消費者や投資家の資金が危険に晒され、ビットコインに多くの長所があろうとも、そうした負の印象は拭えなくなります。ノンデリバラブル・フォワード（現物の受渡を伴わない先渡取引）がこの先出現する可能性は否定しませんが、それでもビットコインが備えているいくつかの特徴（権力分散型であり、取引の確認作業に時間がかかるなど）のせいで、店頭市場（OTC、ほとんどのFX取引が行われる）でその威力を発揮するかどうか、私達は疑わしいと感じています。

**ビットコインの正当な価格はどうやって評価できるのでしょうか？**

David Woo +1 646 855 5442

ビットコインの価格は過去1年に100倍以上膨れ上がり、バブルなのではないかとの疑問が上がっています。この疑問に答えるためには、ビットコインの本質的な価値を評価しなければなりません。私達はビットコインの未来予想を行うつもりはありません。以下に示すのは、どうやって価値を公正に判断できるか、についての初期的な考えです。ビットコインは交換媒体であり、貯蓄手段でもあります。私達は、公正な価格を判断する上では、この2つの特性を別々に分けたほうがやりやすい、と考えています。

**交換媒体としての価値**

既に述べてきたように、ビットコインは交換媒体として魅力的な特性をいくつか備えています。特に、eコマースについてそう言えるでしょう。B2C取引全体の10%を占めるような主流交換媒体にビットコインが成長した場合、公正な価格は何になるでしょうか？以下、試算を行ってみます：

* アメリカの家庭消費支出は2012年度に11兆ドルに達しました。
* 一般家庭の小切手用預金と現金の合計は2012年度に7000億ドルに達しています。
* 後者を前者で割ると、0.07という係数が得られます。（これ以降は、流通速度と呼びます）。
* 流通速度は2008年以来上昇しており、恐らくは一時的な溜め込み現象を反映しているものと思われます。過去10年の流通速度の平均をとって調整すると、0.04となります。つまり、米国の一般家庭では年間を通じて1ドル支出した場合、4セントを現金または現金に近い形で所持していることになります。  
  注5：通貨発行益とは政府が通貨を発行することで得る収入です。http://www.bankofcanada.ca/wp- content/uploads/2010/11/seigniorage.pdf
* 2012年度の米国内におけるB2Cのeコマースは総額で2240億ドルに達しました。
* オンライン販売の流通速度が米国内全ての家計支出の流通速度と同じだと仮定すると、一般家庭はオンラインショッピング用に100億ドルを割当てるでしょう。
* ビットコインがオンラインショッピング総額の10%を占めるまでに成長するという仮定を前提にすると、つまり米国の一般家庭はビットコイン用に10億ドル相当の残高を持つことになります。
* 世界全体ではどうでしょうか？アメリカのGDPは世界全体の20%程度です。世界全体においてeコマースが米国と同等に浸透し、米国外の一般家庭でも同じ流通速度が適用されるとすると、世界全体でオンラインショッピングに求められる現金／非現金残高の合計は、**50億ドル相当のビットコイン**になります。

上記は非常に大雑把な計算であり、たくさんの仮定を用いています。さらに、B2Cはeコマース全体の一部にしかすぎません。また、B2B取引においても、ビットコインが主要な交換媒体になる可能性は否定できません。それにも関わらず、この算出結果によると、ビットコインがただの交換媒体の役割に留まるとすれば、その価値には明確な上限があることになります。

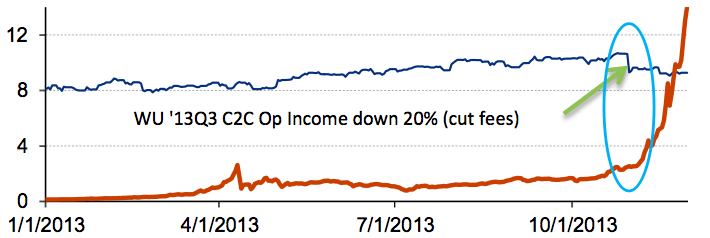
ビットコインは非合法な取引でよく用いられる支払い方法になるだろう、とも言われています。この点について、私達は見識を持ち合わせていません。しかし、ビットコイン取引が公開されており（つまり、理論的には警察組織による追跡が可能な状態であり）、全てのビットコインにはユニークな取引記録がある（つまり、犯罪者が追跡を逃れるのは困難である（注6））せいで、闇市場や犯罪市場での利用には歯止めがかかるでしょう。

オンライン取引の支払い方法としての役割に加えて、ビットコインは送金にも使えます（例：米国の移民労働者が本国に送金を行う場合）。これはとても安く、素早く行えます。（送金者が家族の一員であるなど、信用を得ている場合、オンラインの清算は10分以内で行われます。赤の他人同士の場合は、50分かかります。）ビットコインが持つこの役割に関しては、どうやって正当な評価を最大限行えるでしょうか？

ウェスタンユニオン、マネーグラム、ユーロネットは送金市場における三大企業です（市場全体の20%ほどを占めています）。ビットコインが市場における三大企業の一角に座る、と仮定しましょう。それは、ビットコインの評価にはどう関係してくるでしょう？ビットコインの供給量が固定である以上、ある個人がビットコインを購入すると、交換媒体を手に入れるだけでなく、ビットコインの企業価値に対して投資するということにもなります。この観点からすると、多少飛躍して言うならば、ビットコインの時価総額は、企業価値とみなすこともできます。ウェスタンユニオン、マネーグラム、ユーロネットの平均時価総額が約**45億ドル**であるので、私達はこの数字をビットコインの交換媒体としての役割が持つ時価総額として追加します。

注6：Reid と Harrigan (2011)は公開されている記録のパッシブ解析を行い、ユーザーの6割がウィキリークスの寄付アドレスに関連付けられていることを突き止めました。彼らはまた、盗難された疑いのある25,000ビットコインを追跡して、立証しました。資金を洗浄し、再編する試みが行われていましたが、それにも関わらず追跡に成功しています。警察組織は両替所における参加者のIPログを召喚でき、「マーク付きコイン」をばらまいて追跡することも可能なため、より簡単に上記の結果を得られるでしょう。

**グラフ7：BTCが時価総額にてウェスタンユニオンを超過**



青：時価総額 ウェスタンユニオン (10億ドル)

赤：時価総額 BTC (10億ドル)

|  |
| --- |
| 矢印：ウェスタンユニオンの2013年第三四半期、C2C収入は20%減 |



ソース：BofAメリルリンチ・グローバルリサーチ、ブルームバーグ

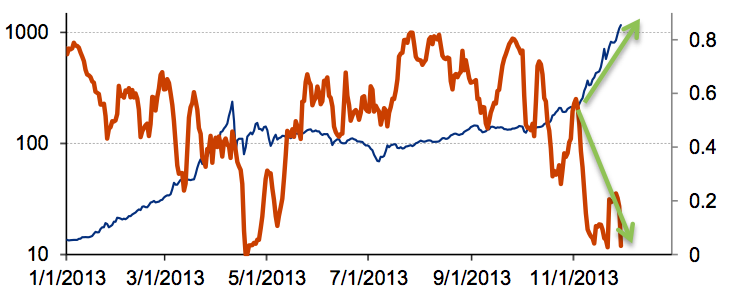
**総計：交換媒体としてのビットコインの最大時価総額＝50億ドル（B2C eコマース用）＋45億ドル（支払手段）＝95億ドル**

興味深いことに、95億ドルという仮定は、ビットコインが現時点で持つ実際の時価総額である130億ドルより低い金額です。これはつまり、ビットコインの現在の市場価格は次のいずれかを前提にしていることになります：ビットコインがeコマースの10%以上を占めているか、送金ビジネスの10%を占めているか（グラフ7）、あるいは貯蓄手段として非常に貴重であるか、です。

**貯蓄手段としてのビットコイン**

ビットコイン価格の最近の伸び率は、投機的な目的以外で行われる取引の成長率を上回っています（グラフ8）。この事実だけでも、ビットコインの評価額は、交換媒体としてよりも貯蓄手段や投資対象としての評価を元に行われていることを示唆しています。

**グラフ8：価格が上昇していても、両替所以外ではほとんど取引が行われていません**



青：ログ（ビットコイン価格）（LHS）

赤：eコマース／総取引（RHS）

ソース：BofAメリルリンチ・グローバルリサーチ

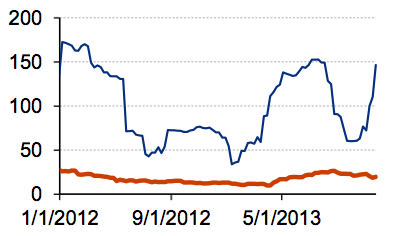
**表1：ビットコイン代替品の価格**

|  |  |  |
| --- | --- | --- |
| **ドル＋ユーロの高額紙幣価格** | **民間で所有される金の延べ棒／金貨／ETFの価値総額** | **スイス銀行における外国顧客の貯金総額** |
| $1.5兆 | $1.3兆 | $500億 |

 ソース：BofAメリルリンチ・グローバルリサーチ

貯蓄手段としてのビットコインの役割を、どうやって評価すればよいのでしょうか？これはとても難しい課題です。ビットコインには利息がなく、ビットコイン建ての投資用のツール（株式や債券）もありません。貯蓄手段するという点では、ビットコインの価値はそれほどなさそうです。この観点に立つと、貯蓄用としては、私達の意見では最も近い同類は貴金属や現金（表1）、となります。

**グラフ9：供給済のビットコイン量 vs. 金（52週単位）**



青：ビットコイン　赤：金

ソース：BofAメリルリンチ・グローバルリサーチ

ビットコインと金には、重要な共通点があります。どちらも利息が発生せず、どちらも供給量が有限であり、そしてどちらも他の金融資産と比べて追跡が困難です（現金を除けば）。現時点で、発行済みの金の延べ棒／金貨／ETF総額は1.3兆ドルです。ビットコインは金と同等な時価総額を得られるでしょうか？私達はそうは思いません。

まず、ビットコインは金よりもずっと変動が大きく、ビットコインは所有リスクが高い資産です。過去2年間において、ビットコインの変動幅は金より平均して5倍ありました（グラフ9）。他のすべての条件が等しいとすると、ビットコインは金に比べて5倍リスクを抱えていることになります。ビットコインの変動が大幅に抑えられたり、金の変動性が大幅に上昇しないかぎり、ビットコインの時価総額が3000億ドルを超えることは難しい、と考えるのが妥当でしょう。

さらに、過去10000年にもわたって、金は安全に価値を貯蔵できる唯一の存在として信頼を得続けています。ビットコインが同じ信頼を得るには、時間がかかるでしょう。金の信頼度を測定する方法は私達にもわかりませんが、金が銀に比べて60倍も価値が高い理由は多分、この評価でしょう。ビットコインがいずれ銀と同程度の評価を得るとすれば（それでも、とても高い目標ですが）、貯蓄手段としてのビットコインの時価総額は50億ドルに達するでしょう。

ところで、50億ドルという数字は現在までに鍛造されたアメリカの1ドル銀貨（1986年以来）の総額と同じ水準です。私達は、これが最もビットコインと適切に比較できると考えています。総額は80億ドル（12000トン）程度に達します。

**結論：価値を貯蔵する場所としてのビットコインの最大時価総額＝50億ドル**

ビットコインは金に対して、移動が楽に行えるという一点において優位に立っています。しかし、金のETF（価格連動型上場投資信託）が発展してきたことや、そうしたETFを口座ごとに移動できる事実を考えると、ビットコインの優位点はそれほど際立っているとは考えられません。この観点から、私達はビットコインには追加で価値を見出すことができません。

ビットコインの正当価格を市場がどう評価するかは、異常な金融政策がこの先どれだけ続くか、という点にも明らかに深く依存しています。既に予測されているように、連邦準備制度理事会の量的緩和が来年度に終了しなければ、安全避難的な資産（金やビットコイン）への需要が増し、価値は上昇するでしょう。私達は、連邦準備制度理事会は来年の第一四半期に量的緩和に介入を行い、米ドルは世界の準備通貨としての信用を取り戻し始めるだろう、と考えています。アメリカは財政赤字を解消し始め、来年度は恐らくGDPの4%以内に収まるはずです。私達の強気な2014年のUSD見通しが正しければ、貯蓄手段としてのビットコインの価値はあまり伸びないはずです。

**集計：**

交換媒体としてのビットコインの価値に加えて、貯蓄手段としての役割を考慮すると、私達が推定するビットコインの市場価値は約150億ドルという数字になります。（投機対象としての）ビットコインの価値がこれで頭打ち、というわけではありませんが、ビットコイン価格の最近の上昇ぶりが続くと、近いうちに経済の基本原理を逸脱するだろう、と私達は考えています。私達の考えは以下の通りです：

**ビットコインの最大時価総額＝150億ドル  
ビットコインの最大公正価格＝1300ドル**

**結論**

私達は、ビットコインがe-コマースの主流決済方式となり、伝統的な送金業者にとって深刻な競合相手になる、と信じています。交換媒体として、ビットコインは明らかに大きな可能性と発展性を持つ、と私達は見ています。

高額の税金を逃れ、資金を操作し、横領を行おうとする連中にビットコインが利用される、と考える人々は大勢います。ビットコイン取引全体における人民元の割合と、ビットコイン価格が上昇を続けているのも事実です。それを踏まえた上で、ビットコイン取引が全て公開されており、個々のビットコインには改変不可能な取引記録が残っているという事実は、最終的にブラックマーケットや犯罪市場における普及に歯止めをかけるでしょう。

貯蓄手段としてのビットコインの役割は、交換媒体としての利用価値を減らす可能性があります。投機的な活動のおかげで変動性が高くなっており、ネット取引における支払方法としての普及があまり一般的には広まっていません。

ビットコインはバブルなのでしょうか？ビットコインが（1）eコマースや送金市場における主要な手段に成長し、（2）銀と同様に信頼されている貯蓄手段に成長したと仮定します。その状態で、私達が分析するビットコインの公正価格は次の通りです：***ビットコインの最大時価総額＝150億ドル（1BTC＝1300米ドル）***この結果により、今年に入ってから100倍に膨れ上がったビットコイン価格は、経済の基本原理を逸脱しているリスクを孕んでいることが示唆されます。

**付属**

ビットコインは公開鍵暗号方式に基づいており、各取引は2種類の鍵を用いて参照されます：入金される支払を暗号化する公開鍵と、暗号化を解除する秘密鍵です。これらの鍵は長い数列で構成されており、単純な推測から暗号化が破られる事態を防いでいます。同一アカウント（公開鍵）を入金と受け取りの両方の取引に用いることは可能ですが、匿名を希望する人々は各取引に対して別々の公開鍵を用います。私達が銀行口座を利用する要領で、固定された単一アドレスを使いまわすのではなく、他の送金者から1回限りの支払を受け取って保存するために、個別にアドレスを生成します。さもなければ、各アドレスにどれだけの金額が納められており、所有者がどのようにそれを使っているか、類推ができるからです。金額の大きな支払を行う際は、資金元を数種類組み合わせます。例えば、0.7ビットコインを持つ公開鍵を10種類用意し、5ビットコインの支払を行った後に、残りの2ビットコインは別の新規作成したアドレスに残高として戻す、などです。

**採掘者**は公開台帳に新規取引を記録し、認証する作業を行う歴史学者のようなものです。台帳を更新する報酬として、採掘者は自身のブロックがブロックチェーンに関連付けられた際に一定額のビットコインを報酬として受け取ります。各ブロックは独立した課題として存在しています。最初に証明を行った採掘者には報酬が与えられ、残りの採掘者には何も与えられません。彼らは、新たなブロックを用いて一からやり直しです。各採掘者に与えられる課題は毎回異なります。なぜなら、課題はそれまでのブロック群、未処理の取引、彼ら自身への報酬という要素に左右されるからです。ゆえに、高速なコンピューターを使ったからといって成功が約束されるわけではありません。ただ、成功の確率を上げることはできます。実際は、採掘者は一人で作業を行って巨額な報酬を得る際の不確定さを減らすために、組合を結成して、個々の貢献度に応じて利益を得ています。

本体のブロックチェーンは最長の認証済みブロックを保持しており、取引の公開記録の合意を決定付けます。個々のブロックは「採掘証明」を得られた瞬間に認定されます。採掘証明は、「採掘者」が演算処理を行って生成する特殊コードです。個々の採掘者は暗号化ハッシュ関数として知られる機能を使用して新規取引をまとめます（注7）。新規取引の解説を簡潔な形でまとめたものであり、新規ブロックを構成します。採掘者はハッシュ値の計算を繰り返し、幸運にも「大当たり」に巡り合うまで続けます。大当たりとは、新規ブロックとそれに含まれる取引を要約したハッシュ値が小さな値に収まることです。最長のチェーン内にて各新規ブロックが直前のブロックを参照する形で、ブロックは互いに接続されます。この小さなハッシュ値を見つける目的は、採掘者が気が遠くなる回数の演算を既に繰り返しており（注8）、ブロックを得る資格を有していると証明することです。各ブロックを認証するために必要な演算処理は膨大であり、取引記録を全て書き直してハッカー攻撃を試みるやり方は割に合いません。

「軍拡競争」は、採掘者たちが年々高性能化する採掘設備を用いてお互いに出費を重ね、楽に採掘して利益を得ようとする競争を指します。実世界の採掘作業と異なり、自身のネットワークを広げたところで、ビットコイン採掘の結果は向上しません。各ブロックの認証仮定で、困難さが調整されるからです。困難さは、目標となるハッシュ値の小ささで測定されます。この値は、毎2016ブロック（毎2週間）ごとに変わります。処理能力が向上するにつれ、困難さも指数関数的に上昇しており、ブロックが毎10分ごとに生成されるように設計されています。実際には、時折5分や15分ごとに生成されるブロックも時折存在します。21万ブロック（4年）ごとに報酬は半減され、2139年に生成されるブロックは各自1サトシしか報酬を与えられません。2140年以降はゼロです。代わりに、取引の送り主が小額の取引手数料を報酬として最終的な採掘者へ送ることができるようにシステムが設計されています。そうなると、採掘者たちは報酬額の多さに応じて、どの取引を優先的にブロックに組み入れるかを決定することになります。

最近になって、資金提供を受けた専門の採掘者が採掘用の特殊ICを搭載したコンピューターを用いており、趣味的な採掘者を駆逐しています。1ドルを得るために必要な演算の量は毎年157%の勢いで伸びています。



注7：ハッシュ関数は、いかなる長さの入力をも固定長の出力に変換する単方向の暗号化機能です。例えば、「The quick brown fox jumps over the lazy dog」は37f332f68db77bd9d7edd4969571ad671cf9dd3bというハッシュ値に変換されます。「The quick brown fox jumps over the lazy **c**og」は 132072df690933835eb8b6ad0b77e7b6f14acad7となります。

注8：10億ハッシュはギガハッシュと呼ばれ、ネットワーク速度の標準測定値として用いられます。

