執筆者:
マット・クンケ
リサーチアナリスト

日付:2021年11月10日トピック:デジタル資産

GLOBAL X ETF リサーチ

ビットコイン の基本

2008年10月、暗号学研究者のメーリングリストに、突然ある怪文書がばらまかれました。それは「革命をもたらしかねない貨幣コンセプト」を喧伝するものでした。その9ページにまとめられた文書で、投稿者「サトシ・ナカモト」(個人または集団の偽名)は、世界初の非集中型ピア・ツー・ピア通貨システムを世に知らしめました。上記文書によると、この完全にオープンなシステム(インターネット接続があれば誰でもアクセスできる)に参加する者は、世界中でいつでも、信頼できる仲介者を通さずに価値の交換ができるというのです。

数か月後の2009年1月、ビットコイン・ソフトウェアの最初のバージョンが発表され、これによって正式に「ビットコイン・ネットワーク」が誕生することとなりました。このネットワークは、ブロックチェーン技術を採用した最初のアプリケーションで、完全なる透明性と共有性を持ち、恒常的に照合ができる分散型台帳(この台帳上で取引の記録や、資産の追跡が行われる)を備えたものでした。このネットワークの始まりと同時に、ビットコインも創設されることになりました。ビットコインは分配、交換が可能で、授受も容易に行えるデジタル通貨で、プログラム上で定義された方針によってその希少性が担保されたものです。

ビットコインの進化の歴史:「ニッチ」から「主流」へ

ビットコインの登場は、時宜を得たものでした。ビットコインが世に出たのは「世界経済危機」の真っ最中で、多くの個人が資産を預けていた大手銀行や、金融行政を行っていた政府に対する信頼を失っていた頃でした。ビットコインはいかなる中央組織からも管理・調整を受けない「ハードカレンシー」の新たな形を体現するものでした。ビットコインのこのような特質と希少性は、金融危機後に各国政府が大規模な量的緩和プログラムを実施し、不換通貨の供給を増やした中で、より多くの共感を得ることになりました。

金融危機後の数年間で、ビットコインは徐々に信用を得たものの、ボラティリティや疑念にさらされ、ニッチ資産の地位にとどまっていました。しかし、新型コロナウイルス感染拡大に伴い、大幅な財政支出が強いられる中、ビットコインの最も優れた特質が再び脚光を浴びることになりました。意欲の旺盛な投資家がこの機会を捉えてビットコイン市場や、さらに広範な暗号資産市場に参入してきたのです。依然として価格の振り幅も大きく、非難・中傷する人達も多かったのですが、ビットコインはかつてないほど、「主流」としての足場を固めていったのです。

今日、ビットコインの流通量は1,885万ビットコインで、その市場価値は1兆2,300億ドルと言われています。毎日約28万件のビットコイン取引がオンチェーンで行われています。平均取引額は約48億ドルに上ります。[1]

ビットコイン価格(対数スケール)
出典:Blockchain.com. 2021 年 10 月 21 日時点。

ビットコインについて知っておくべきこと―その構造と機能

ビットコインのステイタスが高まり、今後投資も増えると考えられることから、本稿ではまずビットコインとその機能について、基本的な質問にお答えします。

- **ビットコインとは何か?**: 金取引のデジタル版(但し授受はもっと簡単)です。
- **ビットコイン・ネットワークとは何か?**: 世界初の、真の意味でオープンで、許認可もいらず、信頼できる仲介者が最小限に抑えられた金融エコシステムです。
- **ノードとは何か?**:ビットコイン・ソフトウェアを操作するコンピューターで、ネットワークの安全性を守ります。
- **マイニングとは何か?**:特殊なノードが、数学的パズルを解き、チェーン上で次のブロックを創り出すことです。
- **なぜメイン・ブロックチェーンの定義づけが重要なのか?**:ネットワーク上の時差によって起こる問題を解決するためです。
- **本当の取引はいつ起こるのか?**: 取引によって十分な数のコンファメーションが発生したときです。

本稿では、経済環境におけるビットコインの位置づけについて議論するために、以下の3つの広範な問題も取り上げます。

- **ビットコインはどんな恩恵をもたらすのか?**: 独立した形で、「金融包摂」への信用とアクセスをもたらします。
- **ビットコインに対する規制環境は今後どうなるのか?**:今後の注目点です。
- **なぜ、今ビットコインなのか?**: 今日の経済状況にマッチした資産だからです。

ビットコイン:手軽に授受できる「金取引のデジタル版」

ビットコインはネットワーク上のユーザー間で通貨として取引される、供給量の限られた資産です。ユーザーはその価値について「お金の一形態である」と合意しており、単一のエンティティによって管理されたり変更されたりすることはありません。ビットコインはブロックチェーン技術を最初に応用したもので、ビットコイン・ブロックチェーン内の台帳上の資産残高として認識されます。政府によって保証されている伝統的な不換通貨とは異なり、ビットコインは物理的な紙幣や硬貨ではありません。

その代わり、ビットコインのユーザーはプライベートキーを持っています。これは口座パスワードのようなものと考えて結構です。ユーザーはパブリックキーとアドレスも持っています。これは暗号学的にプライベートキーから割り出されるもので、プライベートキーにリンクしています。重要なことは、プライベートキーの方がパブリックキーやアドレスから割り出されることはないということです。ユーザーのアドレスは、ビットコイン取引の行き先を特定するために使われる公共のユーザー名のようなものです。要約すれば、ビットコインを使用するには、ユーザーはプライベートキー(それにパブリックキーと、ビットコインが保管されるアドレスが関連づけられている)が必要になるということです。ユーザーがビットコインを受領するには、送り主に対して自身のアドレスを通知すればだけです。

パブリックキーとアドレスの割り出し方

出典：Global X ETFs,「Mastering Bitcoin: Programming the Open Blockchain.」

とはいえ、プライベートキーを公開することは問題があるのではないか、と思われるかもしれません。ビットコインはデジタル流通資産です。つまり、プライベートキーを持っている者であれば誰でも使えるものなのです。プライベートキーを呈示するよう要求されると、誰かが関連づけられたアドレスにあるビットコインを盗むことになると思われるかもしれません。ところが実際には、ビットコインを使用する際には、プライベートキーをネットワークで呈示する必要はありません。ビットコインを使用するには、デジタル署名を呈示することになります。デジタル署名によって、その署名者がプライベートキーを持っているということが、暗号学的に認証されるのです。

デジタル署名は、ユーザーのプライベートキーと、呈示された取引情報から割り出されます。パブリックキーとアドレスはプライベートキーから割り出されるものなので、デジタル署名を行ったプライベートキーと、パブリックキーに紐づいたプライベートキーが同一なのかどうかは、先進的な数学によって検証することができるのです。このような暗号学的な関係によって、デジタル署名はネットワーク上でビットコインの所有権を、独立した形で認証することができます。これによってビットコインのユーザーは、なりすましを行って他人のビットコインを使おうとする者に盗まれることなく、安心して自身のビットコインを使えるのです。

ビットコイン・ネットワーク: 世界初の、真の意味でオープンで、許認可もいらず、信頼できる仲介者が最小限に抑えられた金融エコシステム

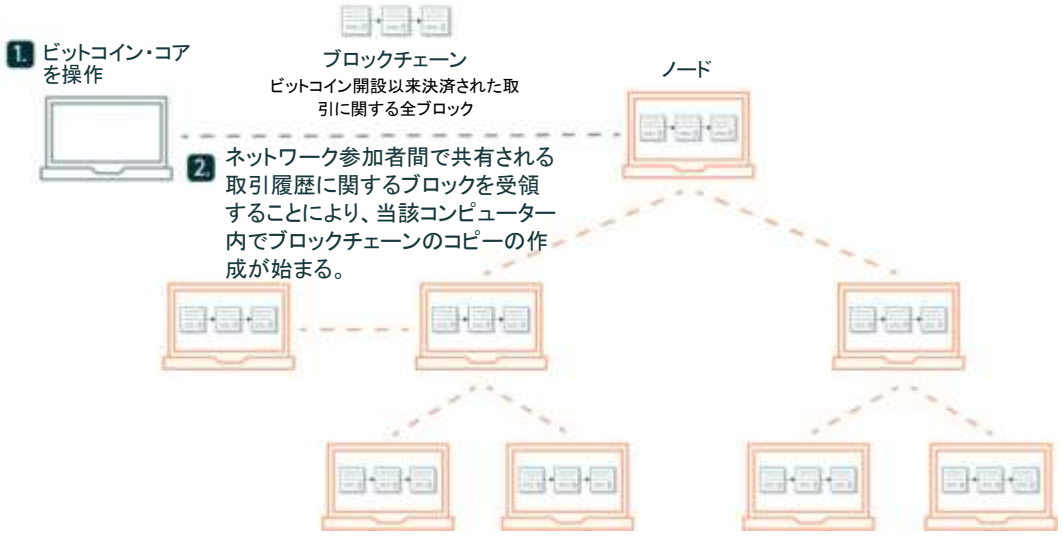
ビットコイン・ネットワークによってビットコインの授受が、金融機関のような仲介者を通すことなく、ピア・ツー・ピアで行われます。このネットワークは、取引の記録やビットコインの追跡を行うに当たって、完全に透明なブロックチェーン技術を利用しています。ネットワークの参加者は、プロトコル・ルールを遵守し、ルールに照らして取引やブロックを独自に検証することによって、ブロックチェーン内の分散型台帳を承認するという点について合意しています。

ネットワークはビットコイン・コアを使用しています。これは全てを網羅しているソフトウェア・パッケージで、これによってネットワーク参加についての完全な自律性が担保されています。コンピューターがこのソフトウェアを搭載していると、そのコンピューターはノードと呼ばれる他のコンピューターとネットワーク上でつながります。

するとそのコンピューターは、ネットワーク開設以降に発生した全ての取引に関するブロックを受領し始めます。次にそのコンピューターは、取引についての分散型データベースの完全なコピーを自身の中で作成します。これがビットコイン・ブロックチェーンです。ビットコイン・コアにはウォレット機能がビルトインされており、これによって参加者はソフトウェアを介して、ビットコインの取引が直接できるようになります。このウォレット機能は、パブリックキーとプライベートキーの組合せの管理、ビットコイン残高の追跡、ビットコインを使用する際のデジタル署名の作成許可などを行います。

ビットコイン・コアを搭載しているコンピューターのノードのネットワーク

出典：Global X ETFs.



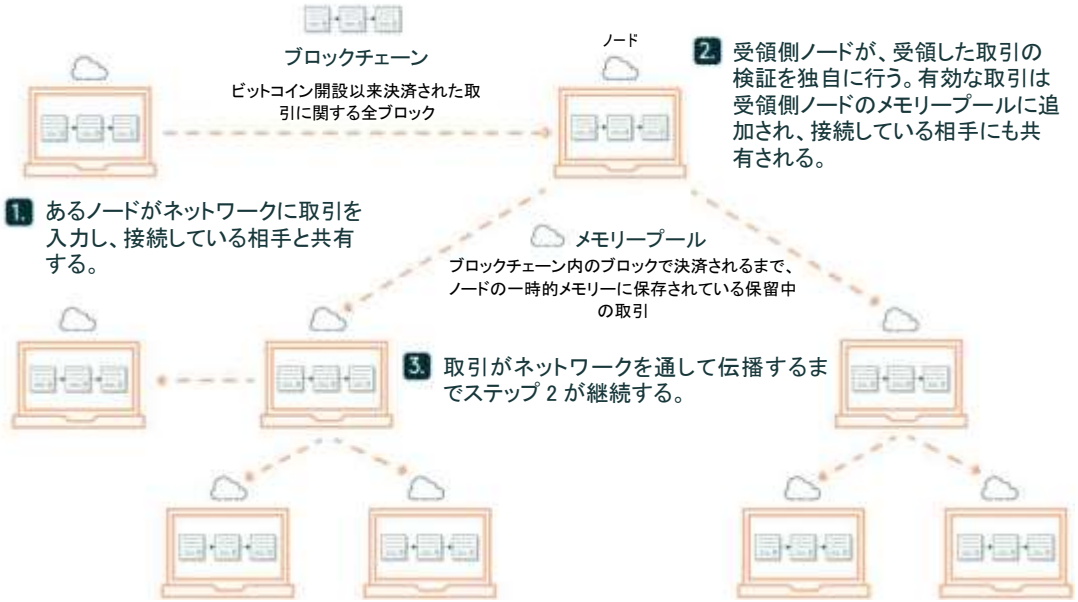
ノード: ビットコイン・ソフトウェアを操作するコンピューター。ネットワークの安全性を守る

各ノードは自身の中にブロックチェーンのコピーを作成した後、新たな取引や新たなブロックが発生する度に、リアルタイムで相互に連携しながら、自身内のチェーンコピーを更新していきます。各ノードは、全ての取引やブロックをプロトコル・ルールに照らして独自に検証し、有効な取引やブロックだけを接続しているピアに送信し合うことによって、ネットワークの安全性の維持に寄与します。各ノードは恒常的に、認証されたものの保留になっている取引のプール（メモリープール）のアップデートを行います。

あるノードが接続しているピアから新しい取引を受領した場合は、ソフトウェアが総合的な基準（デジタル署名の鑑定など）に照らしてこの取引の有効性について独自に検証します。当該取引が有効である場合は、この取引を受領したノードは自身の一時的メモリーの中に取引を保存し、接続している他のノードにもこの取引を送信します。それ以降も、このサイクルが繰り返されます。取引を受信した他のピアもこの取引を受領・検証し、接続している他のピアに送信します。このサイクルが、ネットワークを介したピア・ツー・ピアベースの情報の動きを表しています。

ビットコイン・ネットワークを通した取引の伝播

出典：Global X ETFs.



マイニング・ノード: 数学的パズルを解き、チェーン上で次のブロックを創り出す特殊なノード

全てのビットコイン・ノードは独自に取引の検証を行いますが、マイニング・ノードは特殊なタイプのもので、ブロック内に取引を集め、これらのブロックを取引成立のためにブロックチェーンに記録する役目を果たします。マイニング・ノードはチェーン内でブロックを作成するという点において、他とは区別されます。ブロックは、「各取引を成立させるレイヤー（層）」のようなものとも考えてもよいでしょう。取引は恒常的にノード間で送信され、一時的メモリー内に保存されます。この時点では、それらの取引は、マイニング・ノードがブロックに含めるまでは、事実上保留中の取引ということになります。

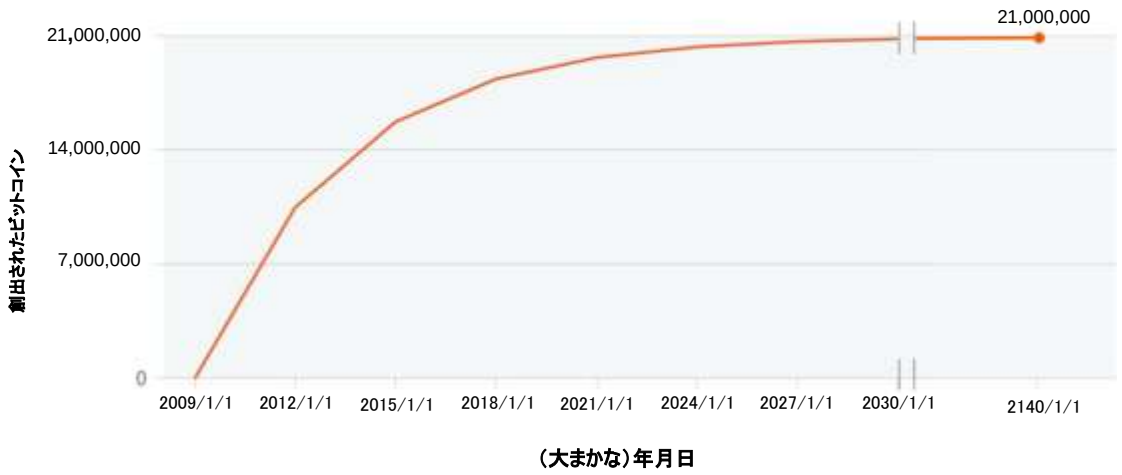
マイニング・ノードは、複雑な数学的パズルを最初に解く競争のために、多くの計算のためのリソースを必要とします。このパズルの解法は「プルーフ・オブ・ワーク」と呼ばれています。このパズルは激しい競争の末に解明されることになるのですが、マイニング・ノードはなかなか得られないアウトプット（ハッシュ値）を求めて、暗号学的ハッシュ関数を通して多くの異なるインプットを繰り返すことになります。プルーフ・オブ・ワークを見つけ出すのは難しいのですが、どのノードもわずかながら、マイニング・ノードがこの解明法を見つけ出そうと計算リソースを消費していることを検証することができます。デジタル署名がある場合のみ取引が有効であると考えられるのと同じ方法で、キャンディデート・ブロックが有効になるには、プルーフ・オブ・ワークが必要となります。

マイニング・ノードには、パズルの解法を一番に見つけ出すことに対して、金銭的な動機づけがあります。新たなブロックを、有効なプルーフ・オブ・ワークとともに最初に送信したマイニング・ノードは、そのブロック内のブロック報酬と全ての取引手数料を要求することができます。ブロック報酬は特殊な取引で、これによってマイニング・ノードは、新たに創出されたビットコインを自身に対して一定額送付することができます。この過程のことを「マイニング（採掘）」と呼びます。このブロック報酬は初めて産出されたビットコインとも呼ぶべきもので、地下から採掘された金のようなものだからです。

現在、ビットコインが新たに創出された場合に、ブロック報酬として6.25ビットコインが支払われます。これは現在約40万ドルに相当します。[2]しかし、ブロック報酬は21万ブロック毎（あるいは約4年ごと）に50%減少し、2140年頃には消滅することになります。このように半減期を経ることによって、ビットコインにはディスインフレ政策が適用されることになります。次回の半減期は2024年と見込まれており、この際にブロック報酬は1ブロック当たり3.125ビットコインに減額されることになります。

ビットコインの供給

出典：Global X（2021 年 9 月 30 日）

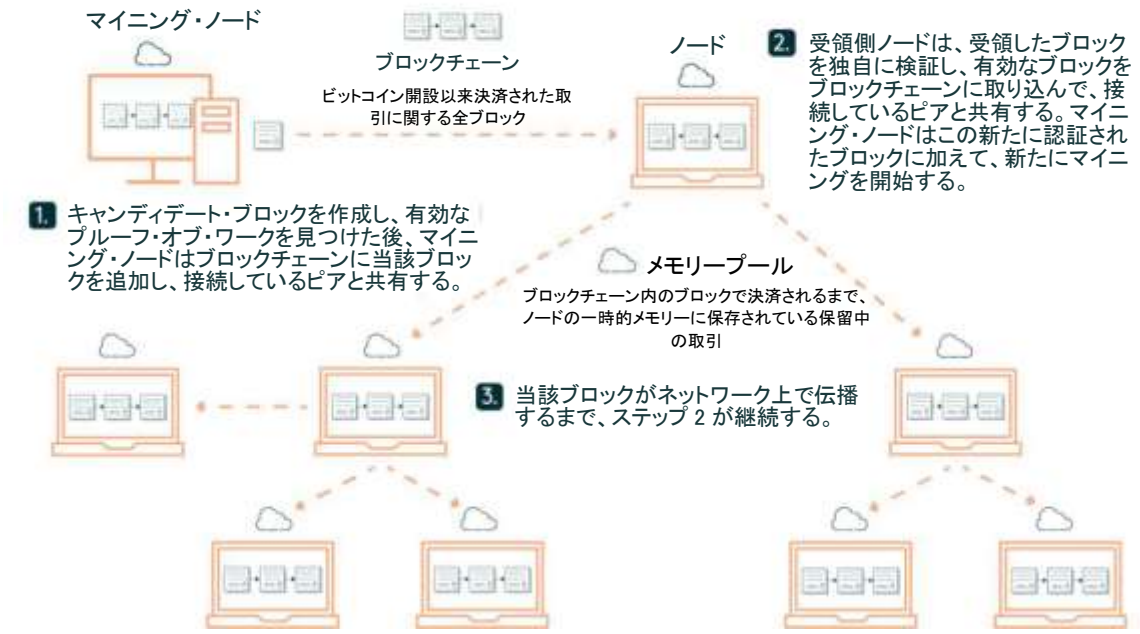


また、ユーザーはビットコイン・ネットワーク上で取引を行う際、通常、少額の取引手数料を支払います。これはマイニング・ノードがユーザーの取引のために、取引をブロックに追加するインセンティブを与えるためです。取引手数料はネットワーク上での需要が多い時期には大幅に値上がりすることがあります。その手数料は、ビットコイン使用者が彼らの取引を成立させるために行っている入札価格を反映しているからです。例えば、2021年9月時点での平均取引手数料はわずか2.50ドルでしたが、ビットコインの価格が初めて6万ドルを超え、ネットワークが渋滞に陥った2021年4月には、10日間で約20～65ドルの範囲で上下しました。[3]一般的には、ブロックは自身の中に1,500～2,500件の取引を保有しているので、通常、マイニング・ノードがブロックを解明するための総報酬額に取引手数料が占める割合は小さいと言えます。

マイニング・ノードがブロックを解明したら、それらのブロックはネットワークに送信されます。それぞれのノードは新たに受領したブロックの有効性を検証し、自身のブロックチェーン・コピーの中に取り込みます。新たに有効なブロックが取り込まれれば、ここでマイニング・ゲームは一旦終了です。全てのマイニング・ノードは新たなキャンディデート・ブロックを作成し、新たに受領したブロックに関連しているパズルを最初に解こうとします。

ビットコイン・ネットワークを通したブロックの伝播

出典：Global X ETFs.



ビットコイン・コア・ソフトウェアは、このマイニング・パズルが平均10分間に1回のペースで解明されることを前提に設計されています。このソフトは約2週間に1回、パズルを解く難易度を調整して、ペースを保つようにしています。つまり、難易度を上げる（下げる）ことによって、パズルを解く際のハッシュ率が上がる（下がる）ようにしているということです。そのため、貴金属を採掘する場合と違って、ビットコインをマイニングするペースを速めることはできません。言い換えれば、ビットコインの供給の増加は固定されており、ビットコインの需要とは無関係ということになります。ビットコインの発行率は一定であるため、マイニングの回転率を上げるために多くの投資を行ったとしても、パズルの解明がより計算能力を必要とするものになるだけです。

メイン・ブロックチェーン: ネットワーク上の時差によって起こる問題を解決する

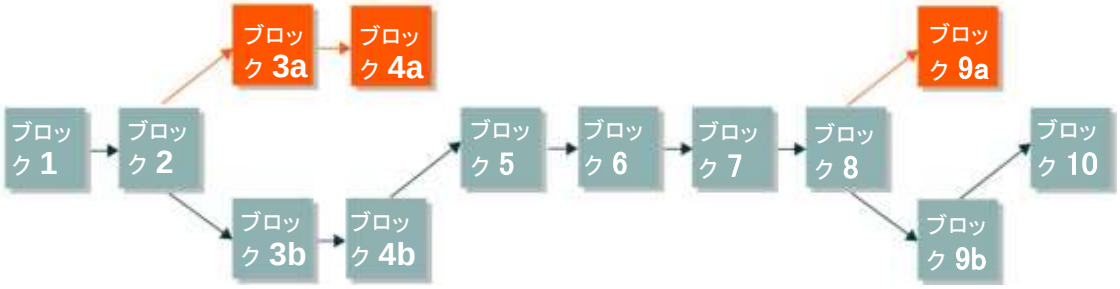
2つのマイニング・ノードが、ほぼ同時にプルーフ・オブ・ワークを解明し、有効なブロックを送信した場合に、1つの問題が起こります。ピア・ツー・ピアで情報が伝わる世界的ネットワークの性質上、ネットワーク内での時差の関係から、異なるノードがほんのわずかな時間の差で情報を受領するといった事態の発生は避けられません。プロトコル上のルールでは、各ノードが最も長い（より正確に言えば、最も多くの情報が累積されている）チェーンをメイン・ブロックチェーンとして特定することによって、この動態的な問題を解決することにしています。例えば、マイニング・ノードAとマイニング・ノードBがほぼ同時にブロックを認証し、マイニング・ノードCがAから、マイニング・ノードDがBから、それぞれ先にブロックを受領したとします。

この場合、ブロックチェーン内に「一時的分岐」と呼ばれるものが発生することになります。つまり、分岐した先の両方のブロックチェーンが一時的に有効になりますが、どちらがメインチェーンになるかは、その後ブロックがどちらに追加されるかで、後付けで特定されることになります。ですが、この状態は早い段階で解決します。マイニング・ノードがどちらのチェーンに後続のブロックをつなげるかを選択するからです。初期設定においては、マイニング・ノードは受領した最初の有効なブロックをチェーンにつなげることになります。従って、AとCは一方のチェーン、BとDはもう一方のチェーンにブロックをつなげることになります。

さらなるブロックが生成されるにつれて、分岐された両方のチェーンがプルーフ・オブ・ワークを同時に解明し続ける可能性は、早い段階でゼロに近づきます。一方のチェーンが次のブロックを、もう一方よりも早く見つけた時点で、こ

のブロックを生成した方のチェーンがメイン・ブロックチェーンと考えられるようになり、もう一方のチェーンはプロトコル・ルールに従って途絶することになります。このプロトコル・ルールによって、各ノードはブロックチェーンの状態や発生した取引についての合意・賛同を見出すことになります。下図において、オレンジ色のブロックは有効ですが、後付けでメインチェーンが青色に特定されますので、この部分はメインチェーンではなくなります。

ブロックチェーンの一時的分岐
出典：Global X ETFs.



本当の取引成立と不変性：取引によって十分な数のコンファメーションが発生したとき

取引は、ブロック内に取り込まれたときに成立すると、しばしば言及されます。しかし、ブロックチェーンが一時的に分岐したり、短時間のうちに組成しなおされたりする場合も考えられるので、本当の意味での取引成立と不変性を得るためには、いくつかの条件が満たされる必要があります。

十分な数のコンファメーションを受領して（具体的な取引を含むブロックの先に複数のブロックが追加されることによって）、はじめて本当の意味での取引成立と不変性が発生することになるのです。一般的には、1つのブロックに6つのコンファメーションがついた場合に、不変性が備わったものと考えられています。取引規模が小さい場合には、1つ～3つのコンファメーションでも安全であると見なされています。既存のブロックが、新たにマイニングされたブロック（その前のブロックのハッシュ関数を参照している）と相互に結びついていることを前提とすれば、そこに埋められているブロックの数が増えれば増えるほど、取引はより安全かつ不変のものになります。

例えば、ある悪意を持った者が、既に6つのコンファメーションを得ている取引を覆そうとするならば、その者は改竄しようとしている取引を含むブロックから6ブロック遡らなければなりません。その上で、その者は当該ブロックと、その分岐上に続く他の5つのブロックについて、それぞれ有効なプルーフ・オブ・ワークを探して再度マイニングし直さなければなりません。この間に、プロトコル・ルールを守る善意の者達が、それまでに定義されている通りにマイニングを行い、メイン・ブロックチェーンにつなげているのです。悪意を持った者がメインチェーンに対して6ブロックの不足分を埋め合わせるためには、ネットワーク上の総計算能力の50%超を、相当長い期間にわたってコントロールする必要があるでしょう。

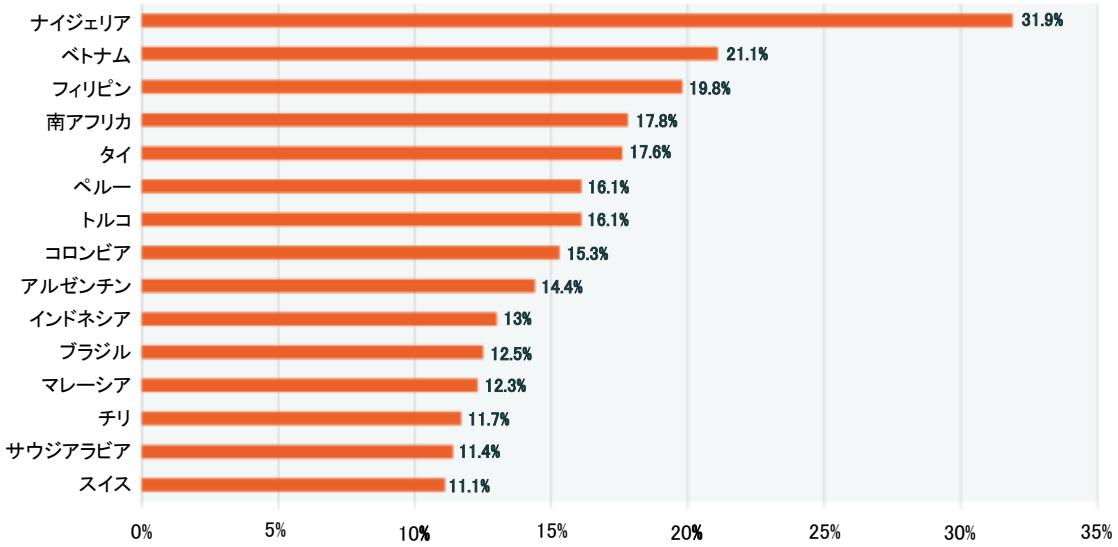
ビットコインがもたらす恩恵：「金融包摂」への独立したアクセスと信用

ビットコイン・ネットワークは、通貨の保証や通貨供給量の管理に関して政府を信用することなく参加できる金融エコシステムです。先進国においては、上記のような特質の重要性はおそらく理解しがたいものでしょう（最近の経済危機のために、多少は理解しやすくなったかもしれませんが）。信頼できる金融機関が、投資家保護のための強固な規制の枠組の中で営業を行うなどということは、世界中（特に新興国）で平等に与えられている特権ではありません。

ビットコイン・ネットワークは、銀行に口座を持てない人たち（特に、政治的不安定、汚職、過酷なインフレに苦しんでいる国々の人たち）を取り込む「金融包摂」を提供するメカニズムです。2021年2月に、市場・消費者データ会社「スタティスタ」が行った調査によると、人口対比で暗号資産使用率が高かった上位10か国は全て新興国でした。最上位はナイジェリアで、32%の回答者がビットコインやより広い範囲の暗号資産を使用していると回答しており、ベトナム（21%）、フィリピン（20%）がそれに次いでいました。[4]

国毎の暗号資産使用率

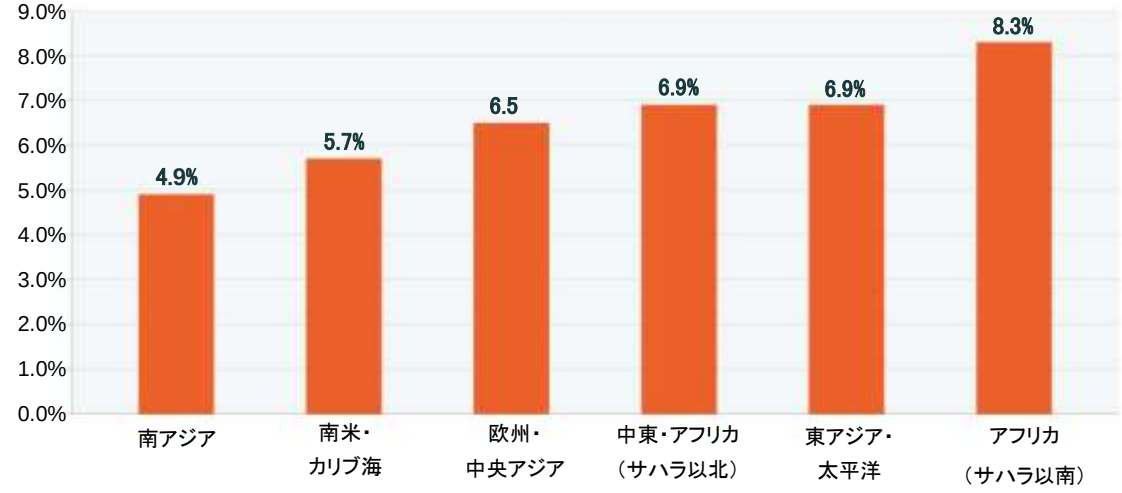
出典：Global Consumer Survey（2021 年 2 月 28 日）



送金市場も、ビットコインを使用する場の1つです。送金金額が当該国のGDPに占める割合は、先進国に比べて新興国では、はるかに高くなっています。世界銀行によると、世界中で行われた送金金額の平均6.4%が、取引手数料として差し引かれているとのことです。一部のコストのかかる経路をたどる送金では、手数料が占める割合は10%を超えることもあります。[5]

地域別送金コスト

出典：世界銀行、Remittance Prices Worldwide（入手元 http://remittanceprices.worldbank.org ：2021 年 3 月 31 日時点）



ビットコインを使って国際送金を行えば、一部の新興国においては大きなコスト削減につながる可能性があります。例えばエルサルバドルでは、人口の70%が海外からの送金を受領しています。同国政府は、世界で初めてビットコインを法定通貨にするとの決断を行いましたが、これはテストケースとして注目に値します。ビットコインを使用すれば、同国では送金手数料を1年に4億ドル削減できるという予測もあります。[6]

ビットコインに対する規制：今後の注目点

ビットコインは他のデジタル資産同様、まだ創設から日が浅いため、規制が不明確で継ぎ接ぎ状態のままで運営されており、規制環境も国によって、または同じ国の中でも法管轄区域によって、異なっています。例えば米国の場合、連邦政府レベルでは、暗号資産に対する規制は不十分なものですが、個別の州では独自の規制があり、中には厳しいものもあります。ニューヨーク州金融サービス局（NYDFS）は、米国内の多くの州に比較して、極めて厳しい規制を行っています。

世界中で規制、分類、税法上の扱いが異なる中で、ビットコインに対する規制が今後どうなるのかを占うのは困難です。現状、Global Xとしてはより明確な規制の枠組が現れると予測しています。そして、より明確な規制環境に伴うリスク低減によってビットコインは恩恵を受け、参加者の増加につながると考えられます。ビットコインの受容が進むに伴い、企業はビットコインをどう扱うべきかを決めつつあり、慎重に規制を導入しなかった場合には、その地域のイノベーションが遅れをとってしまう可能性があります。例えば、米国で最大の暗号資産の1つであるクラーケンは、ニューヨーク州が2015年にビットライセンスの枠組を実施した後、同州での運営を停止しました。[7]

過剰な規制のリスクは一考に値しますが、ビットコイン・ネットワークの非集中的かつ国際的な特質を勘案すれば、行き過ぎた規制を行った場合でも、その影響は抑制されると考えられます。中国政府による2021年9月の暗号資産全面禁止政策の後にも、価格はわずかしか下がらなかったことはその一例であるとGlobal Xでは見ています。[8]

なぜ、今ビットコインなのか？：現在の経済状況にマッチした資産

ビットコインへの注目度の高まりを理解する上で重要なことは、その形成期にあたる時期が偶然にも2つの歴史的な経済危機（そこに広範な政治的・社会的悪影響が伴った）と一致していた点です。これらの経済危機によって、伝統的な金融エコシステムにおける2つの大きな問題点が浮き彫りになりました。それは「信用不安」と「アクセスの難しさ」です。ところが、ビットコインの主たる理念は、この2つの問題を解決してくれます。

- ビットコインは非集中型ネットワークで、これによって参加者は、政府機関や金融機関といった信頼できる仲介者を通すことなく、世界中で価値の交換ができます。
- ブロックチェーン技術によってネットワーク参加者は、完全な透明性をもったプロトコル・ルールを遵守することによって、分散型台帳に対する同意を見出すことができます。
- デジタル通貨は、プログラム上で定義された通貨政策（これによって希少性が担保されている）に基づく、分配・交換・授受が容易な通貨です。
- 参加者になるためには、インターネット接続があれば十分です。

これらの特性に対しては、個人投資家や、さらには、金融サークルの主流派の間でも共感が広がってきています。投資銀行やヘッジファンドは、資金や人材をビットコインに割り当てるようになりました。企業はビットコインを、自社のバランスシート上の資産として保有し始めています。一部の大学さえも投資を行っています。また、規制下にあるビットコイン派生商品の発展が、ビットコインの信用度の向上につながっています。

2008年10月、最大のミステリーは「サトシ・ナカモトが何者か」ということではなく、ビットコインが、最終的に世界経済のどの領域で存在し得るか、ということでした。13年後、ナカモトの正体はいまだに不明ですが、ビットコインが人々に近い存在となるにつれ、その正当性も増してきています。結局のところ、世界中でユーザーのネットワークが拡大しつつある中で、その希少性が担保されている資産を保有できるとすれば、大抵の投資家の注目を集めることになるからです。

—

用語集

本稿内での記載順

暗号学: 敵対的な行為が存在する状況で、情報伝達の安全を確保するための技術を対象とした広範な研究。「パブリックキー暗号学」の項参照。

ビットコイン・ネットワーク: ビットコイン・コア・ソフトウェアを運営するコンピューターのピア・ツー・ピアのネットワーク。ビットコイン・ネットワークによって、信頼できる仲介者を通すことなく価値（ビットコイン）の移転が可能となる。

ブロックチェーン(チェーン): ピア・ツー・ピアを通して共有され、恒常的に残高照合が行われている分散型の台帳。これによって、取引の記録や資産の追跡が、信頼できる仲介者を通すことなく円滑に行われる。ノードと呼ばれる当ネットワーク参加者はネットワークのルールに従って、取引やブロックを他のノードに検証してもらうべく通信を行う。取引はブロック内に集められ、そこで取引の時間と順番が記録される。新たなブロックは、チェーンを形成する旧来のブロックに連結され、その後新たなブロックが追加されることによって直線的に広がっていく。平均して10分間に1つずつ新たなブロックが追加されている。

ビットコイン:ビットコイン・ブロックチェーン内の台帳残高上のみに存在するデジタル流通資産。ビットコイン・ネットワークに固有の暗号資産。

暗号資産: 信頼できる第三者ではなく、暗号学に依存した非集中型システムによって取引が検証され、その記録が維持・管理されているデジタル通貨。

オンチェーン: 実際のブロックチェーン内で取引が行われていること。例えば、集中取引所で他の暗号資産との交換取引を行う際、取引所の参加者は、ビットコインを全ての顧客のために管理している台帳上で動かすのみである。これらの取引は、当該資産がプラットフォームから引き出されない限り、ブロックチェーン内での実際の取引とはならない。

プライベートキー: デジタル流通資産であるビットコインの所有権を示すもの。口座パスワードと類似している。ビットコインの所有権を認証するためのデジタル署名を行う際に使用される。関連するプライベートキーを見つければ、誰でも当該アドレス内のビットコインを取得することができる。

パブリックキー: プライベートキーから数学的に割り出される。関連するビットコインを使うためには、パブリックキーを公開しなければならない。デジタル署名はパブリックキーを使用することで有効となり、ビットコインを使う者が関連づけられたプライベートキーを保有している場合に認証される。これとは別に、パブリックキーはアドレスを作成する際の暗号学ハッシュ関数への入力にも使用される。

アドレス: パブリックキーから数学的に割り出される。ビットコイン取引の行き先を認識するために使用される公開されたユーザー名と類似している。

デジタル署名: プライベートキーおよび取引のハッシュ関数から数学的に割り出される。デジタル署名は、プライベートキーおよび関連づけられたパブリックキーの所有権を、プライベートキーを他人に明かすことなく証明するもの。デジタル署名によって、ネットワーク上のビットコインに対する所有権が独立した形で認証され、これによってビットコイン所有者がビットコインを、当人になりすまして他人のビットコインを使おうとする悪意を持った者を排除した上で、自由に使うことができる。

ビットコイン・コア: オープンソース型のソフトウェアで、ビットコイン・プロトコルおよびビットコイン・ネットワークに関するあらゆる事項に対する実行を行う。

ノード: ブロックチェーンの独自コピーを管理するために、ビットコイン・コアを操作するコンピューター。ノードは、プロトコル・ルールに照らして全ての取引やブロックに対して独立して検証を行い、接続されているピアに対して有効な取引とブロックのみを送信することによって、ネットワークの安全に寄与している。

パブリックキー暗号学: 非対称暗号学とも呼ばれる。2つの明確に異なるが、数学的に関連づけられたキー（1方は暗号化用、もう1方は暗号解読用）を使用する。ビットコイン・ネットワークで利用されている特有の暗号学であり、パブリックキーがビットコインの受領、プライベートキーがビットコイン使用に関する取引署名に使われる。

ピア: ネットワーク上で相互に直接に接続されているノード。

メモリープール: メモプールとも呼ばれる。ブロック内で取引が成立する前に、ノードによってローカル・コンピューターのメモリー内に集積されている、有効ではあるがペンディングとなっている取引。

マイニング・ノード: 成立させるためにブロックチェーン上で記録された取引について、ブロック内で集積作業を行う特殊なノードの小集団。マイニング・ノードは暗号学的ハッシュ関数に基づいて、複雑な数学的パズルを最初に解こうと互いに競争する。マイニング・ノードは暗号学的ハッシュ関数によりできる限り速く、異なる入力による結果を全力で計算するために、大量の計算リソースを使用する。

プルーフ・オブ・ワーク: マイニング・ノードが競って解こうする、暗号学ハッシュ関数に基づいた複雑な数学的パズルの解法。暗号学的ハッシュ関数の特質のため、プルーフ・オブ・ワークは非常に見つけにくいが、マイニング・ノードがこの解法を見つけるために計算リソースを消費したことを、どのノードもわずかながら検証することができる。プルーフ・オブ・ワークによって、2つのブロックで同時にマイニングが行われている際の不整合を解決することができる。また、旧来のブロックの改竄を非常に難しく(コストがかかるものに)することによって、ネットワークを保護している。

暗号学的ハッシュ関数: 任意の長さのデータマッピングを、決定論的な固定の長さに変換するのに使用される一方向性関数。暗号学的ハッシュ関数には、以下の3つの性質がある。1) 繰り返されること:いかなる入力に対しても、その結果となる出力(ハッシュ値)は同じであるということ。2) 一方向的関数であり、与えられた出力から入力値を割り出すことが不可能であること。3) 入力値を微調整することで出力値が導き出すことが不可能なほど、関数がランダムであるように見えること。マイニングの過程は、何らかの出力値を得るために、暗号学的ハッシュ関数の結果を繰り返し、できるだけ速く算出することに依存している。これらの関数は、パブリックキーからアドレスを割り出すためにも使用される。

ハッシュ値: 暗号学的ハッシュ関数の出力値。

キャンディデート・ブロック: マイニング・ノードが有効なプルーフ・オブ・ワークを見つけ出すことによって、ブロックチェーンに追加しようとしている取引保留中のブロック。プルーフ・オブ・ワークが見つかった後に、キャンディデート・ブロックは有効なブロックとなり、チェーンに追加される。この時点で、マイニング・ノードは新たなキャンディデート・ブロックを作成し、新たに受領したブロックに関連づけられているパズルを最初に解き、次の有効なブロックをチェーンに追加しようとする。マイニング・ノードは、通常、メモリープール内の最も高い取引手数料の取引を選択することによってキャンディデート・ブロックの形成を行う。

ブロック報酬: マイニング・ノードが、ブロックの解明に対する金銭的なインセンティブとして、固定額の新たに創出されたビットコインを自身に向けて送金できる特殊な取引。現状、ブロック報酬は1ブロックにつき6.25ビットコイン。ブロック報酬は、新たなビットコインが創出される唯一の方法である。

取引手数料: 取引成立のためにブロックに自身の持つ取引を取り込むようマイニング・ノードを動機づけるために与えられる少額の取引手数料。取引手数料は、大抵の場合極めて少額だが、ネットワークが大変混雑している時期には大きな額になり得る。

半減期: ブロック報酬の額が50%にまで減少する時期。21万ブロック毎に、あるいは約4年ごとに半減期が訪れる。次回の半減期は2024年と見込まれており、この際にブロック報酬は1ブロック当たり3.125ビットコインに減額されることになる。

難易度: ビットコイン・ブロックのマイニングが、特定の時期にいかに困難かを示す計測値。ビットコイン・ネットワークは、ブロックが平均で10分間に1回のペースでマイニングされるように設計されている。難易度が高くなる(低くなる)と、ブロックが平均で10分間に1回確実にマイニングできるようにマイニング・ノードの計算能力が増加(減少)する。難易度は2,016ブロック毎、または約2週間毎に調整される。ソフトウェアは単純に、2,016ブロックをマニングするのに要すると予測される時間(20,160分)と、実際に直近の2,016ブロックをマイニングするのに要した時間の比率を採用しており、この比率によりこれまでの難易度を上昇または下落させている。

ハッシュ率: ある時点でのビットコイン・ネットワークが確保できる総計算能力の予測値。ネットワーク上の全てのマ

イニング・ノードが、1秒間に計算できるハッシュ値の総数で計測される。ビットコイン・ネットワークのハッシュ率は、2021年に毎秒約18垓（＝1京の18,000倍）ハッシュという最高値に到達した。

メイン・ブロックチェーン(メインチェーン): チェーン上にあるブロックの難易度に基づいて、累積的に最大のマイニング作業を行ったブロックチェーン。通常、メインチェーンが最も多くのブロックを有している。

分岐: 単一のチェーンから2つの異なるチェーンへと枝分かれしているブロックチェーン。これらのチェーンは同一の履歴を共有しているが、新たなブロックが同一性を失うポイントまで到達している。2つのマイニング・ノードが同時に1つのブロックをマイニングするときに、一時的な分岐が発生するが、プロトコル・ルールによりこの分岐は単一のメインチェーンに収束することになる。プロトコル・ルールに変化が起きる、またはプロトコル・ルールに関する意見の不一致が発生すると、より永続的な分岐が発生しやすくなり、ソフトウェア内で多重に分岐したバージョンが発生することになる。

不変性: これ以上変化できない状態。

コンファメーション: ブロックに特定の取引が含められた後に、ブロックチェーンに追加されたブロックの数。最初のコンファメーションは、取引がブロック内に含められたときに発生する。新たに有効なブロックがチェーン上でマイニングされる都度、追加のコンファメーションが発生する。

1. Blockchain.com（2021年10月21日）
2. Coinmarketcap.com（2021年10月21日）
3. Blockchain.com（2021年10月21日）
4. Statista Global Consumer Survey（2021年2月28日）
5. Remittance Prices Worldwide「Remittance Prices Worldwide Quarterly」（2021年3月31日）
6. CNBC.com「El Salvador's new bitcoin plan could cost money providers like Western Union and others $400 million a year, says President Bukele」（2021年9月9日）
7. Blog.kraken.com「Farewell, New York」（2015年8月9日）
8. Coinmarketcap.com（2021年10月21日）