http://www.coindesk.com/information/bitcoin-glossary/

CoinDeskで使われている用語は混乱しますか？ビットコインでよく使われる用語と、その意味をこの場で解説します。完全なビットコイン入門書として使え、デジタル通貨について理解しやすくなるでしょう。

51% attack（51%アタック）

暗号化ネットワークの処理能力のうち、過半数が一人の採掘者か、一つの採掘者グループによって支配されている状態です。理論的には、それだけの処理能力を擁していれば、ネットワークを掌握できます。つまり、ネットワーク上のクライアント全てが、そうした攻撃者（採掘者）が発行した取引ブロックのハッシュ値を鵜呑みにする、ということでもあります。例えば以下のように、ネットワーク上の権力を握られることになります：

* 他の誰かと衝突する形の取引を発行する。
* 特定のユーザーの取引が確認されるのを阻止する。
* 同じビットコインを複数回使用する。
* 他の採掘者が有効なブロックを採掘することを阻止する。

Address（アドレス）

ビットコインアドレスは[取引の受け取りや送信を](http://www.coindesk.com/information/how-do-bitcoin-transactions-work/)ビットコインネットワーク上で行うために用いられます。英数字の列にて構成されており、スキャン可能なQRコードとして表示することも可能です。デジタル的に取引に署名する際にビットコイン所持者が使用する鍵の組合せにおいて、ビットコインアドレスは公開鍵の役割を果たします（公開鍵の項目を参照してください）。

Altcoin（代替通貨）

ビットコインの[代替](http://www.coindesk.com/technology/altcoins/)として提供される暗号化通貨を総称したものです。Litecoin、Feathercoin、PPcoinは全て代替通貨です。

AML

AML（マネーロンダリング防止）技術は、非合法なやり方で入手した資金を、あたかも合法的に入手したかのように変換する行為を防ぐために用いられます。AMLの仕組みは、法的あるいは技術的な適合を前提にして作られています。規制当局はしばしば、AML技術をビットコイン交換所に対して行使します。

ASIC

ASIC（特定アプリケーション向け集積回路）は、指定されたタスクを実行する目的で設計されたICチップです。ビットコインの場合、新規ビットコインを採掘する際に、SHA-256ハッシュ演算を処理する目的で設計されています。

ASIC miner（ASIC採掘機）

ASICチップを内蔵する機器であり、[ビットコイン採掘用](http://www.coindesk.com/information/how-bitcoin-mining-works/)に構成されています。パソコンのマザーボードに接続する追加基板であったり、USB接続の機器であったり、単独のデバイスであったりします。ワイヤレスまたはLAN経由でネットワークに接続し、必要なソフトウェアを全て内蔵しています。

Bitcoin Investment Trust（ビットコイン投資信託）

この追加型個人信託は[ビットコインのみを投資対象としており、](http://www.coindesk.com/secondmarket-launches-bitcoin-investment-trust-invests-2-million/)最新型のプロトコルを用いて、株主に代わって安全にビットコインを保管します。

自身でビットコインを購入して保管しなくても、デジタル通貨へ投資する方法を提供してくれます。

Bitcoin Price Index（ビットコイン価格指数） (BPI)

CoinDeskが発表する[ビットコイン価格指数](http://www.coindesk.com/price/)は、BPIにて指定された基準を満たす世界の主要取引所の平均ビットコイン価格を表示します。開発者が取り扱えるように、[API](http://www.coindesk.com/api/)も用意してあります。

BitPay

ビットコインの決済処理サービスであり、[業者と](http://www.coindesk.com/companies/merchants/)連携して、業者がビットコインを支払用に受け取れるようにします。

BitStamp

ビットコインの取引所の一つであり、[人気上昇中です](http://www.coindesk.com/bitstamp-bitcoin-trading-volume-overtakes-mt-gox-for-first-time/)。最新の[Bitstampニュースを](http://www.coindesk.com/companies/exchanges/bitstamp/)参照してください。

Block chain（ブロックチェーン）

ビットコインの当初から、[採掘された](http://www.coindesk.com/information/how-bitcoin-mining-works/)ブロックを全て記したリストです。各ブロックがそれ以前のブロック全てのハッシュ結果を含むよう、設計されています。これにより、改ざんが防止されます。

Block reward（ブロック報酬）

[取引ブロック](http://www.coindesk.com/information/how-bitcoin-mining-works/)のハッシュ値を演算処理した採掘者へ与えられる、報酬です。該当の暗号化通貨に応じて、コインと取引手数料を組み合わせて支払われます。また、全てのビットコインが採掘され終わっているかどうかも、支払方法に影響します。現時点のビットコインでは、各ブロックの採掘ごとに25ビットコインが支払われます。一定のブロックが採掘されると、報酬も半減します。ビットコインの場合は、21万ブロックごとに半減が行われます。

BTC

ビットコインの略称です。

Buttonwood（スズカケノキ）

ビットコイン愛好家のJosh Rossiが設立したプロジェクトで、抗議行動の一環としてニューヨークのユニオン・スクエアにビットコイン交換所を設立しよう、というものです。ニューヨークの証券取引所の基礎を成した、1792年のスズカケノキ協定にちなんで名づけられました。

Client（クライアント）

デスクトップ、ノートパソコン、モバイル機器の上で実行されるソフトウェアプログラムを指します。ビットコインネットワークに接続し、取引を実施します。[ビットコイン財布](http://www.coindesk.com/companies/wallets/)（ノードの項を参照してください）を内蔵することもあります。

Confirmation（確認）

ビットコイン取引のハッシュ演算結果を取引ブロックに挿入し、検証を完了させる行為です。各確認作業は10分ほどかかります。これは、取引ブロックのハッシュ演算を行う平均時間でもあります。しかし、複雑な取引や大規模な取引には確認作業が複数回必要な場合もあります。より多くのブロックのハッシュ演算が必要になり、ブロックチェーンに追加する作業も増えます。ある取引ブロックの後に、ブロックチェーンにブロックを追加されると、そのたびにその取引は再確認されます。

Colored coins（カラーコイン）

ビットコインに[追加属性](http://www.coindesk.com/colored-coins-paint-sophisticated-future-for-bitcoin/)を与えるために提案されている、ビットコインのアドオン機能です。.属性はユーザーが自分で定義することが可能であり、ビットコインを株式や実体のある資産としてマーキングすることができます。これにより、ビットコインをトークンやその他の資産として取引できるようになります。

CPU

中央演算処理器：コンピューターの「頭脳」です。ビットコインの初期は、取引のハッシュ演算を行うために利用されましたが、今やCPUだけでは力不足になっています。代替通貨のために取引のハッシュ演算を行うことは、今でもCPUを用いて時折行われています。

Coinbase（コインベース）

ビットコイン生成時における取引に用いられる入力の別名です。ビットコインは、採掘者への報酬として採掘されます。他のユーザーから送られてくるわけではありません。それでも、報酬は取引の一種として記録されます。入力として用いられるのは任意に設定されたデータであり、他ユーザーのビットコインアドレスではありません。

[Coinbase](http://www.coindesk.com/companies/coinbase/)は、ビットコイン財布サービスの名前でもあります。業者に対して決済サービスを提供し、交換所からビットコインを購入する場合の仲介者として機能します。

Coin age（コイン年齢）

金額に所持期間を掛けて算出された、ビットコインの年齢です。

Cryptocurrency（暗号化通貨）

数式処理によってのみ成立している通貨です。印刷して生成される不換紙幣と異なり、暗号化通貨は暗号化に基づき数式処理を行うことで生成されます。

Cryptography（暗号化）

数式を用いてコードや暗号を作成し、情報を隠蔽する作業を指します。[ビットコイン取引](http://www.coindesk.com/information/how-do-bitcoin-transactions-work/)を検証し、保証する上での数式処理の根幹を成します。

DDoS

DDoS（分散型サービス妨害）は、攻撃者が大量のコンピューターを用いて攻撃対象の処理能力を消耗させる行為を指します。インターネットを通じて小規模のネットワーク操作が送信され、攻撃対象の帯域と処理能力を消費させることで、攻撃対象の顧客がサービスを受けられないようにします。ビットコイン交換所はしばしば、DDoS 攻撃の[対象とされてきました](http://www.coindesk.com/bitcoin-network-recovering-from-ddos-attack/)。

Deflation（デフレーション）

経済において、時間が経つにつれて価格が下がる現象を指します。モノやサービスの供給が通貨の供給を超える場合と、通貨供給量が有限でありかつ減少しつつある場合に発生します。通貨の一単位あたり、より多くのモノやサービスを購入できるため、購入に必要な通貨の量が減ります。ただし、マイナス効果もあります。価格が下がるだろう、と多くの人が期待すれば、人々は通貨の価値が上がり続けると考えるため、消費をやめてお金を貯め込みます。その結果、不景気が発生することもあります。

Difficulty（難易度）

難易度は、[新ブロックのハッシュ演算を行う](http://www.coindesk.com/information/how-bitcoin-mining-works/)難しさを表します。取引ブロックのハッシュにおける、ある数列内の最大許容値と関係があります。数値が低いほど、許容値に収まるハッシュ値を生成するのが難しくなります。ビットコインネットワーク上の採掘者が持つ処理能力の総量に応じて、難易度は変動します。多くの採掘者がネットワークを去れば、難易度は減ります。しかし、今のところ、ビットコインの人気が高まるにつれて、より多くの処理能力がネットワークに追加されており、難易度は上昇しています。

Double spending（二重使用）

同じビットコインを2回使用する行為を指します。ビットコインを用いて取引が行われ、その同じビットコインを用いてもう一度何かを購入しようとした際に、この問題が発生します。当事者はネットワークに対して、ブロック内のハッシュ演算を行い、2つの取引のうち1つだけを確認するよう促します。ビットコインネットワークの仕組みがうまくできているおかげで、二重使用は簡単に行えません。それでも、確認作業が完了していない取引をあえて[受け入れている人々](http://www.coindesk.com/domain-registrar-namecheap-now-accepts-bitcoin-with-zero-confirmations/)が抱えるリスクではあります。

Dust transaction（超小規模の取引）

とても小さな額のビットコイン取引を指します。金銭上の価値はほとんどない代わりに、ブロックチェーン上の場所はとられます。ビットコイン開発チームは、ネットワーク上で流通する最低取引金額を増やすことで、超小規模の取引を無くそうとしています。

ECDSA

楕円曲線デジタル署名アルゴリズムは、ビットコインプロトコル内の取引を署名するために用いられる、コンパクトな暗号化アルゴリズムです。

Escrow（エスクロー）

取引を全て一度に行えない場合に、資金や資産を一時的に保護するために、第三者の口座の中にそれらを保持しておく行為を指します。ボブがファイルの代金としてアリスに送金したくても、当事者同士で行えない場合、相手を信頼してお金とファイルを同時に受け渡すにはどうすればよいのでしょうか？代わりに、ボブはイブに送金することができます。イブは信頼できる第三者として、ボブがアリスからファイルを受け取ったと確認するまで、資金を保持しておいてくれます。確認後に、イブがアリスに送金します。

Exchange（交換所）

各種の通貨や他の資産を交換できる場所です。[ビットコイン交換所](http://www.coindesk.com/companies/exchanges/)は通常、ビットコインを他の通貨（通常は不換紙幣）と交換するために用いられます。

Faucet（水栓）

[代替通貨](http://www.coindesk.com/technology/altcoins/)を立ち上げる際に用いられるテクニックです。コインに興味を持ち、自ら採掘に加わる人の数を増やすために、一定量の通貨を先に採掘して無料で配る行為です。

Feathercoin

作業証明アルゴリズムのスクリプトを基にした[代替通貨](http://www.coindesk.com/technology/altcoins/)です。

Fiat currency（不換紙幣）

無から生み出される通貨であり、人々が価値を認めているというそれだけの理由で価値を持ちます。資金洗浄やテロ活動で好んで使用されるため、規制当局が常に監視を行う対象でもあります。[ビットコイン](http://www.coindesk.com/information/what-is-bitcoin/)とは違うので混同しないように。

FinCEN

米国財務省に所属する、金融犯罪執行ネットワークのことです。FinCENはこれまでに、ビットコイン交換に対して[規制を加えてきた](http://www.coindesk.com/fincen-boss-lays-out-bitcoin-rules/)主要な組織です。

Fork（フォーク）

複数のブロックチェーン[が同時進行で存在している](http://www.coindesk.com/bitcoin-activists-suggest-hard-fork-to-bitcoin-to-keep-it-anonymous-and-regulation-free/)状態を指します。ある採掘者のグループが、他とは別の取引ブロックのハッシュ演算を開始するのが主な原因です。採掘者のグループがネットワークで強大な権力を持つ場合（51%アタックの項を参照してください）など、悪意を持って行われる場合や、システム内のバグのせいで偶然起こる場合などがあります。中核の開発チームが新バージョンのクライアントに大幅な機能追加を行う場合など、意図的に行われる場合もあります。フォークの結果、ブロックチェーンが最長になれば、より困難度が高くなるので、結果としてうまくいったと言えます。

FPGA

フィールド・プログラマブル・ゲート・アレイは、製造後でも機能構成を変更できるICです。命令を書き込むことのできるシリコン性のホワイトボード、ととらえることができます。FPGAは大量生産した後に構成を変更できるので、メーカーは大規模生産のメリットを生かしてASICよりも安く製造できます。しかし、通常はASICよりもずっと速度は落ちます。

Freicoin

経済学者のSilvio Gessellが提唱したインフレ防止の原則に基づいて作成された暗号化通貨です。

Genesis block（起源ブロック）

ブロックチェーンの先頭に位置するブロックです。

Gigahashes/sec（ギガハッシュ/秒）

一秒間に行われるハッシュ演算の試行数で、10億回を単位にしています（メガハッシュを1000回）。

GPU

グラフィックス処理ユニットです。現代のゲーム画像処理用に、膨大な数のポリゴンをレンダリングするための高度な数式処理をこなすために、専用設計されたチップです。暗号化通貨の採掘に必要な暗号化処理にも、適しています。

Hash（ハッシュ）

様々な大きさのデータを入力し、固定長の短い出力を得る数式処理です。ハッシュ関数には2つの主要な特徴があります。まず、出力を見るだけでは、元の入力が何であったのかを数学的に特定するのは困難です。次に、入力をほんの少し変えただけでも、出力は大きく変わります。

Hash rate（ハッシュレート）

一秒間に[ビットコイン採掘者](http://www.coindesk.com/information/how-to-set-up-a-miner/)が処理できるハッシュ数を指します。

Inflation（インフレーション）

通貨の価値が時間が経つと共に下落すると、物価が上昇します。結果として、購買能力が下げられます。人々の間でお金を貯め込む動機がなくなり、物価が比較的低いうちに消費してしまおう、と考え始めます。

Input（入力）

ビットコイン取引のうち、ビットコインの出所を示す箇所を指します。通常は、ビットコインアドレスです。例外は、ビットコインの生成取引です。この場合、対象のビットコインが生成されたばかりであることを意味します（Coinbaseの項を参照してください）。

Kilohashes/sec（キロハッシュ/秒）

一秒間に行われるハッシュ演算の試行数で、1000回を単位にしています。

KYC（顧客熟知）

顧客熟知の規則により、金融機関は顧客を入念に調査して、合法的な取引が行われていることを確認する義務があります。

Leverage（レバレッジ）

外国通貨の取引において、レバレッジは自身の口座内にある資産を乗じる行為を指します。取引の結果、多大な利益を得ることが可能になります。しかし、トレーダーにレバレッジを依頼するということは、借りた額以上のお金を手数料として返すという前提で、トレーダーにお金を貸りるということでもあります。レバレッジは、マージン要求という名でも知られています。

Liberty Reserve

コスタリカに本拠地を置く、中央集権型の通貨決済業者です。資金洗浄の罪で有罪になった後、米国政府により[閉鎖](http://www.coindesk.com/liberty-reserve-exchange-shuts-down-founder-arrested/)されました。

Litecoin

作業証明のスクリプトを基にした[代替通貨](http://www.coindesk.com/technology/altcoins/)です。詳しくは[Litecoinニュース](http://www.coindesk.com/tag/litecoin/)を参照してください。

Liquidity（流動性）

取引の最中に価格を保ったまま、資産を簡単に売買できるかどうか、という指標です。流動性を保つには、売り手と買い手を多数確保することが重要になります。流動性が低い市場は価格変動が激しく、資産の価値を簡単に特定できません。

Margin call（マージンコール）

マージン要求を行う行為を指します。トレーダーが、レバレッジをかけた取引ポジションを負担できる額の資金を持っていない、と[交換所](http://www.coindesk.com/companies/exchanges/)が判断すると、交換所はマージンコールを発します。

Megahashes/sec（メガハッシュ/秒）

一秒間に行われるハッシュ演算の試行数で、100万回を単位にしています（キロハッシュを1000回）。

Market order（成り行き注文）

ある資産を市場価格で売買するよう、[交換所](http://www.coindesk.com/companies/exchanges/)に対して出される指示を指します。ビットコイン交換所においては、ビットコインを直ちに売買したいと希望する場合は成り行き注文を出します。指定した市場条件が満たされるまで待つことで、売買を通じて利益を得ようとする行為とは異なります。

mBTC

1ビットコインの1000分の1です（0.001BTC）。

Microtransaction（マイクロ取引）

主にオンライン上で、ある資産やサービスに対して[とても少ない額の支払](http://www.coindesk.com/coinbase-implements-zero-fee-microtransactions-off-the-block-chain/)を行う行為を指します。マイクロ取引は、伝統的な決済システムでは手数料がかかりすぎるため、実行が困難です。例えば、オンラインの記事を読むのにクレジットカードを用いて2セントを支払うのは、簡単ではありません。

Mining（採掘）

演算用ハードウェアを用いて[暗号化問題を解くことで](http://www.coindesk.com/information/how-bitcoin-mining-works/)新ビットコインを生成する行為を指します。

Mixing service（混合サービス）

自分のビットコインを他の誰かのビットコインと混ぜ合わせ、送金したビットコインの入出力を変更して送り返してくれるサービスを指します。[混合サービス](http://www.forbes.com/sites/jonmatonis/2013/06/05/the-politics-of-bitcoin-mixing-services/)（タンブラーとも呼ばれます）は、特定のビットコインを自分まで追跡できなくするため、プライバシー保護に利用できます。資金洗浄に利用される可能性もあります。

Mt. Gox

最初のビットコイン交換所の一つです。また、これまでで [最も人気のあった](http://www.coindesk.com/has-the-market-lost-confidence-in-mt-gox/)交換所でもあります。ただ、現在では[BitStamp](http://www.coindesk.com/bitstamp-bitcoin-trading-volume-overtakes-mt-gox-for-first-time/)などとの競争に晒されています。日本に拠点を置くMt. Goxは、Jed McCalebにより2010年に設立されました。

Namecoin

既存のドメイン名システムの代替を提供する目的で設計された[代替通貨](http://www.coindesk.com/technology/altcoins/)です。[Namecoin](http://www.coindesk.com/what-are-namecoins-and-bit-domains/)で支払を行えば、プロキシサーバー経由でアクセス可能な .bitドメインを登録できます。

Node（ノード）

他へ取引をリレー接続するクライアントを通じて、ビットコインネットワークに接続されているコンピューターを指します。

Nonce（使い捨てデータ）

[取引ブロックのハッシュ演算を行う際に](http://www.coindesk.com/information/how-bitcoin-mining-works/)入力として用いられる乱数データです。使い捨てデータは、ビットコインで設定された難易度に基づいて設定された数列パラメーターに合致する数列の要約を生成する目的で用いられます。各ハッシュ演算ごとに、異なる使い捨てデータが用いられます。つまり、各取引ブロックのハッシュ演算ごとに、何十億の使い捨てデータが生成されます。

Orphan block（孤児ブロック）

正式なブロックチェーンの一部ではなく、捨てられたフォークの一部を構成しているブロックを指します。

OTC exchange（OTC取引）

仲介を担当する中央取引所に頼ることなく、取引の当事者がお互いと直接やりとりを行う[取引所](http://www.coindesk.com/companies/exchanges/)を指します。

Output（出力）

[ビットコイン取引の](http://www.coindesk.com/information/how-do-bitcoin-transactions-work/)出力アドレスです。一つの取引に対して、複数の出力があり得ます。

P2P

ピアツーピアを指します。高度に相互接続されたネットワークにおいて、最低2箇所の間で発生する、分散型の通信です。全ての取引において、当事者が必ず中央の仲介ポイントを経由する「ハブアンドスポーク」方式に対する別の選択肢です。

Paper wallet（紙幣型ビットコイン財布）

一つまたは複数のビットコイン公開鍵と、対応する秘密鍵を記載した紙片です。破損の恐れがあるソフトウェア財布や、侵入や消失の恐れがあるオンライン財布の代わりに、安全に[ビットコインを保存する](http://www.coindesk.com/information/how-to-store-your-bitcoins/)ために使用されます。ビットコインを長期的に保管する便利な方法です。

Pool（プール）

共同でビットコイン取引ブロックを採掘し、報酬を分け合う採掘クライアントの集合を指します。採掘プールは、難易度が上がり続ける状況で取引ブロックを採掘できる可能性を上げるために、便利です。

PPCoin

[Peercoin](http://www.coindesk.com/technology/altcoins/peercoin/)またはP2Pコインとも呼ばれます。作業証明に加えて、権利証明を用いる[代替通貨](http://www.coindesk.com/technology/altcoins/)です。Sunny KingとScott Nadalが発表した白書に基づいています。

Pre-mining（プリ採掘）

暗号化通貨の創立者が、通貨の発表前に通貨を採掘し、採掘に加わりたい人々に情報を流す行為を指します。プリ採掘は詐欺目的の暗号化通貨ではよく用いられる手法です。ただし、全てのプリ採掘通貨が詐欺通貨であるわけではありません（詐欺通貨を参照してください。）

Primecoin

Sunny Kingが開発した[Primecoin](http://www.coindesk.com/new-currency-primecoin-searches-for-prime-numbers-as-proof-of-work/)は、作業証明システムを用いて素数演算を行います。

Private key（秘密鍵）

ユーザーのみが知りえる英数字列であり、公開鍵と組み合わせてハッシュ演算を行うことで、デジタル通信の署名を行うことができます。ビットコインの場合、秘密鍵と公開鍵がペアで用いられます。公開鍵はビットコインアドレスともなります（ビットコインアドレスの項を参照してください）。

PSP

決済サービス業者です。PSPはオンラインで支払を受け付けたい業者のために、決済サービスを提供します。

Pump and dump（価格操作）

大げさな宣伝や誤解を招きやすい解説を用いて、安く生成または購入した金融資産の価格を押し上げる手法です。宣伝活動を通じて他の人々にその金融資産を買わせ、価格を吊り上げます。価格が十分に上がった時点で、仕掛け人は資産を売り払い、現金を手に入れます。市場には資産が過剰供給され、価格が一気に下落します。

Process node（処理ノード）

トランジスタの大きさをナノメーター単位で測定したものです。チップの製造プロセス内で生成されます。処理ノードが小さいほど、性能が上がります。

Proof of stake（権利証明）

作業証明の代替として開発されたもので、ある通貨において既に保持している権利（金額）を用いて、採掘可能な通貨の量が決められます。

Proof of work（作業証明）

演算処理の量に応じて、採掘量を決めるシステムです。取引ブロックにて行う必要のある[ハッシュ演算](http://www.coindesk.com/information/how-bitcoin-mining-works/)は、それ自体では簡単な演算処理です。ただし、難易度を上げるために、別の要素が追加されています。ブロックのハッシュ演算は、終了までに時間がかかり、演算量もかさみます。よって、ハッシュ演算が完了したブロックは、それ自体が作業証明となります。

Public key（公開鍵）

公開されている英数字列であり、秘密鍵と共にハッシュ演算を施されて、デジタル通信を署名するために用いられます。ビットコインの場合は、公開鍵はビットコインアドレスとなります。

QR code（QRコード）

単色のパターンがデータ列を構成した、2次元の画像ブロックです。QRコードは携帯電話などのカメラを用いてスキャンするように設計されており、ビットコインアドレスをエンコードして埋め込むためによく利用されます。

Ripple（リップル）

あらゆる通貨（ユーザーが一時的に生み出した通貨を含みます）の取引に用いることが可能な、[決済ネットワーク](http://www.coindesk.com/10-things-you-need-to-know-about-ripple/)です。ネットワークは、中央当局が運営する支払ノードとゲートウェイにより構成されています。支払はIOU（借用証書）を用いて行われ、ネットワークは信頼関係に基づいています。

Satoshi（サトシ）

現在利用可能な、ビットコインの最小単位です（0.00000001 BTC）。

Satoshi Nakamoto（サトシ・ナカモト）

ビットコインの[発明者](http://www.coindesk.com/information/who-is-satoshi-nakamoto/)によって用いられている名前で、本人は2010年終わりにプロジェクトを離脱しました。

Scamcoin（詐欺通貨）

発行者が金儲けを行う目的でのみ発行される代替通貨です。詐欺通貨は、価格操作やプリ採掘と共によく利用されます。

Scrypt（スクリプト）

SHA-256演算における、新しい作業証明の方法です。ASICを用いた採掘者にはほとんど利点はありませんが、CPUとGPUを用いた採掘者にとっては大きな利点があるように設計されています。

Signature（署名）

秘密鍵と公開鍵をハッシュ演算して得られるデジタル形式の要約であり、[ビットコイン取引](http://www.coindesk.com/information/how-do-bitcoin-transactions-work/)が特定のアドレスにて生成されたことを証明します。

Silk Road（シルクロード）

ビットコインのような暗号化通貨をしばしば活用し、非合法の売買にて主に利用される[アンダーグラウンドのオンライン市場](http://www.coindesk.com/is-bitcoin-inherently-criminal-we-asked-a-criminal/)です。シルクロードは、オーナーの[Ross Ulbricht](http://www.coindesk.com/ross-ulbrichts-silk-road-head-smacking-rookie-errors/)が逮捕された後、2013年10月初頭にFBIによって[閉鎖されています](http://www.coindesk.com/silk-road-allegedly-shut-owner-ross-william-ulbricht-arrested/)。

SEPA

単一ユーロ決済圏を指します。ユーロ圏内にて、さまざまな銀行や国家の間で資金を移動しやすくする目的で、欧州連盟内にて取り決められた決済統合の方式です。

SHA-256

ビットコインの作業証明の基礎となる暗号化演算です。

SPV

簡易型支払証明です。ブロックチェーンを全てダウンロードしなくても、各ノードが支払を検証できるようにした、ビットコインプロトコル内の機能です。ブロックチェーン全体の代わりに、ブロックヘッダーをダウンロードするだけで済みます。

Stale（陳腐化）

あるビットコインブロックのハッシュ演算が終了すると、そのブロックに対するほかのハッシュ演算の試みは、「陳腐化」したため、終了します。他の誰かが既に行った作業を繰り返すだけで、何の見返りもないからです。この用語は、採掘プールにて既に終了したハッシュ演算作業の分け前を表現する場合にも用いられます。

Taint（痕跡）

2つのビットコインアドレスが両方とも同じビットコインを所持していたことがある際に、アドレス同士にどの程度関連性があるかを調べる作業です。痕跡解析を用いて、盗難ビットコイン用のアドレスとして知られるアドレスから現在のアドレスまで、特定のビットコインが何ステップで移動してきたかを追跡できます。

Terahashes/sec（テラハッシュ/秒）

一秒間に行われるハッシュ演算の試行数で、1兆回を単位にしています（ギガハッシュを1000回）。

Testnet

テスト目的のみに使用される、別のビットコインブロックチェーンです。

TOR

オンライン上の身元を隠したい場合に使用される、匿名のルーティング用プロトコルです。

Transaction block（取引ブロック）

ビットコインネットワーク上の取引の集合で、ハッシュ演算の後にブロックチェーンに組み込めるように、ブロック内に集められています。

Transaction fee（取引手数料）

ビットコインネットワーク上の取引に課せられる場合がある、手数料です。取引手数料は、対象の取引を含むブロックのハッシュ演算を行う採掘者に報酬として渡されます。

uBTC

マイクロビットコインです。 (0.000001 BTC)

Vanity address（バニティアドレス）

自分の名前など、好みのパターンで構成したビットコインアドレスを指します。

Virgin bitcoin（バージンビットコイン）

ブロック採掘の報酬として購入したビットコインです。こうしたビットコインは、それまでに使用されたことがありません。

Volatility（変動性）

取引対象の金融資産（ビットコインを含む）が、時間が経つにつれて価格が変化する様子です。

Wallet（財布）

ビットコインを[保管して](http://www.coindesk.com/information/how-to-store-your-bitcoins/)後に使えるようにするための手法です。財布内には、ビットコインアドレスとそれに連携した秘密鍵が収納されています。ブロックチェーンは、ビットコインアドレスとその金額を収めた記録です。

Wire transfer（振込み）

お金を電子的に誰かへ送金する仕組みです。ビットコイン交換所と不換紙幣の間で送金と受領を行う場合に用いられます。

Zerocoin

暗号化取引を真に匿名にする目的で設計されたプロトコルです。

Zero-confirmation transaction（確認作業不要な取引）

ビットコインの送金が採掘者によって確認され、ブロックチェーンに組み込まれることを確認する前に、製品やサービスを提供しても構わない、と業者が判断した場合の取引を指します。二重使用のリスクを孕んでいます。