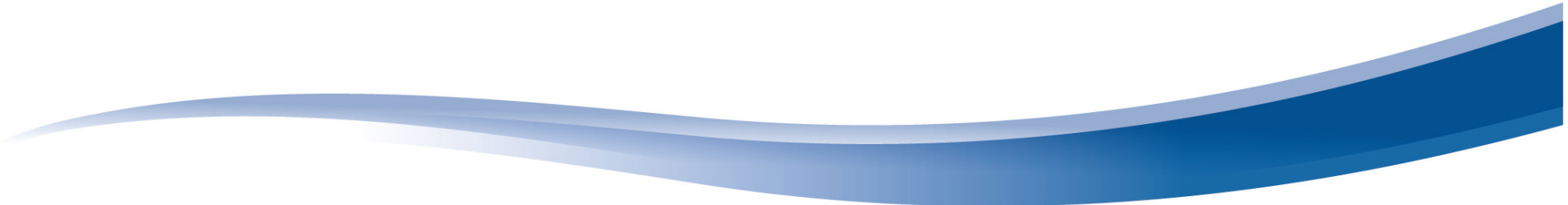




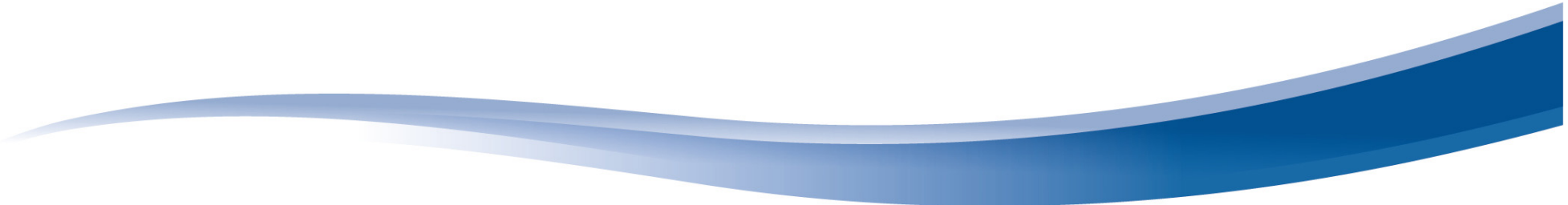
仮想通貨の全てが丸わかり！ 仮想通貨百科事典



仮想通貨(暗号)通貨とは？

仮想通貨はデジタルな通貨の一種です。インターネットを通じて、不特定多数の人や企業の間で物品やサービスの対価として使用でき、また専門の取引所を通じて円やドル、ユーロなどの法定通貨と交換することもできます。

仮想通貨は公開鍵暗号、ハッシュ関数などの暗号技術を利用して、安全性を確保しています。行われた取引はブロックという単位にまとめられ、ブロックの連鎖をブロックチェーンと呼びます。このブロックチェーン技術はほとんどの仮想通貨で用いられており、ブロックチェーン上に保存されているすべての取引データは公開・共有される仕組みとなっています。



仮想通貨の定義

日本の資金決済法では仮想通貨を次のように定義しています。

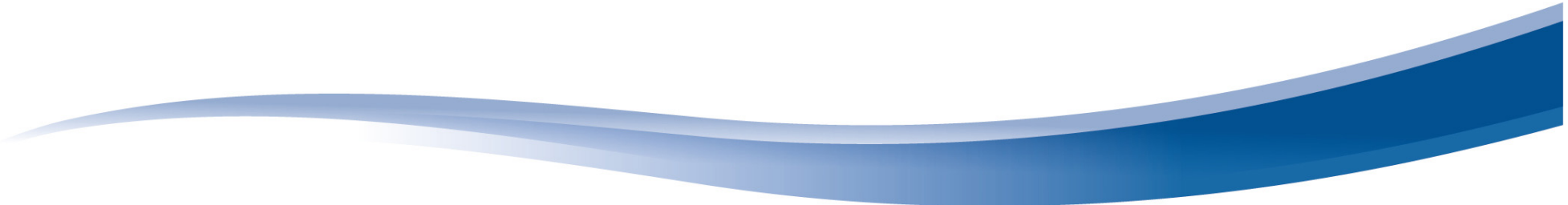
- 一 物品を購入し、若しくは借り受け、又は役務の提供を受ける場合に、これらの代価の弁済のために不特定の者に対して使用することができ、かつ、不特定の者を相手方として購入及び売却を行うことができる財産的価値(電子機器その他の物に電子的方法により記録されているものに限り、本邦通貨及び外国通貨並びに通貨建資産を除く。次号において同じ。)であって、電子情報処理組織を用いて移転することができるもの
- 二 不特定の者を相手方として前号に掲げるものと相互に交換を行うことができる財産的価値であって、電子情報処理組織を用いて移転することができるもの



仮想通貨と法定通貨・電子マネーの違い

法定通貨との違い

法定通貨は、公的な発行主体の信用に基づき発行・管理され、紙幣や硬貨といった形で実体があるのに対して、仮想通貨の多くはブロックチェーン技術を活用することで、公的な発行主体や管理者の裏付けなしに流通します。

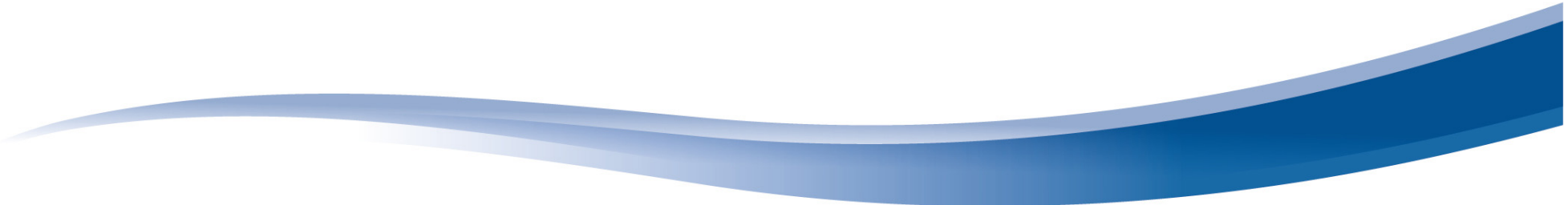


電子マネーとの違い

電子マネーは、第三者機関のインフラを介して電子的に決済を可能にする決済サービスの一つです。

一般的な電子マネーは、自国の法定通貨を利用して電子的に決済を行うために存在しています。

一方、仮想通貨は、紙幣や硬貨を利用せずに電子的な決済を可能にする点では電子マネーと共通しますが、仮想通貨にはブロックチェーン技術を用いることで第三者機関を経由せずに価値の移転を行うことができるという特長があります。



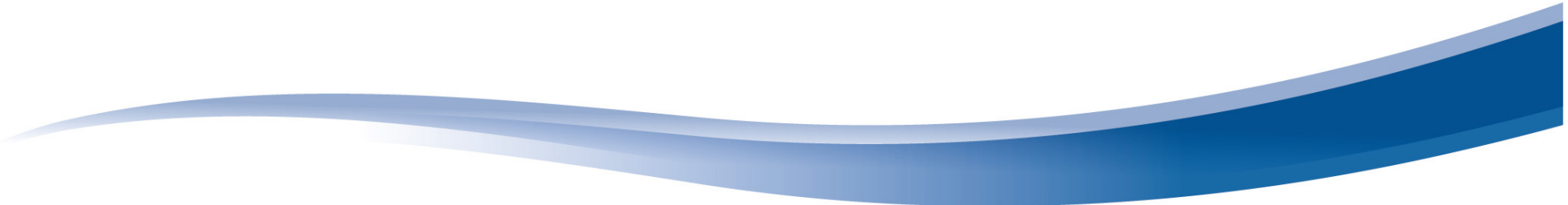
仮想通貨とは

ビットコインとは何か、ひとことで言えば「仮想通貨」です。

「仮想通貨」の「通貨」です。まず、「通貨」ということから、「コイン」ということから分かる通り、ビットコインはお金です。円やドルというように、「お金」であることには変わりありません。「お金」なので、円やドルのように通貨の単位が存在します。ビットコインの単位は、BTC(ビーティーシー)と表記されます。

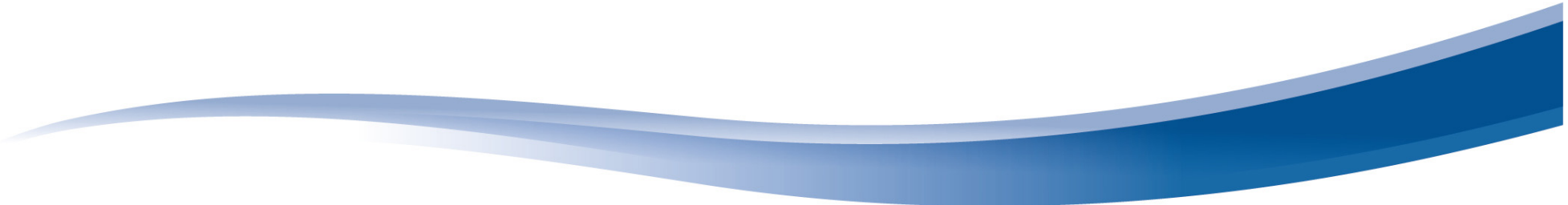
1円や1ドルのように、1BTC(1ビットコイン)と、数えることができます。しかし、「仮想通貨」ということから分かる通り、円やドルとは違って、手にとって目に見える姿形が存在しません。大きく「B」と書いてあるコインが存在するわけではないのです。

ビットコインは、「仮想通貨」の「通貨」です。



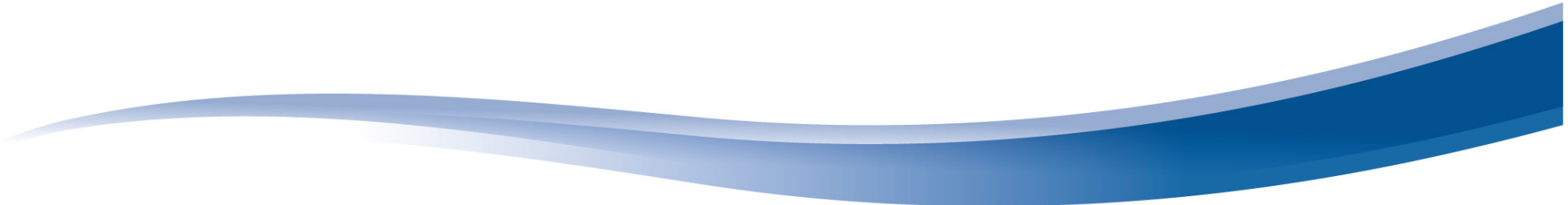
一般的な仮想通貨の例

仮想通貨としてイメージしやすいのは、オンラインゲーム内の通貨です。円やドルを支払って、ゲーム内で使われている通貨を手に入れば、そのゲーム内で使われている通貨が「使える」ゲーム内のお店で、アイテムを買うことができます。ゲーム内でのみ使える、仮想通貨の通貨です。他にも、特定の Web サイトでのみで使える仮想通貨も存在します。利用登録の際に1,000円で1,000ポイントを購入し、その1,000ポイントで有料サービスを購入するというしくみを利用している Web サイトが存在します。そのポイントが「使える」Web サイト内でのみ有効な、仮想通貨の通貨です。ビットコインも似ています。ビットコインを手に入れることができれば、ビットコインが「使える」所で物やサービスを買うことができます。

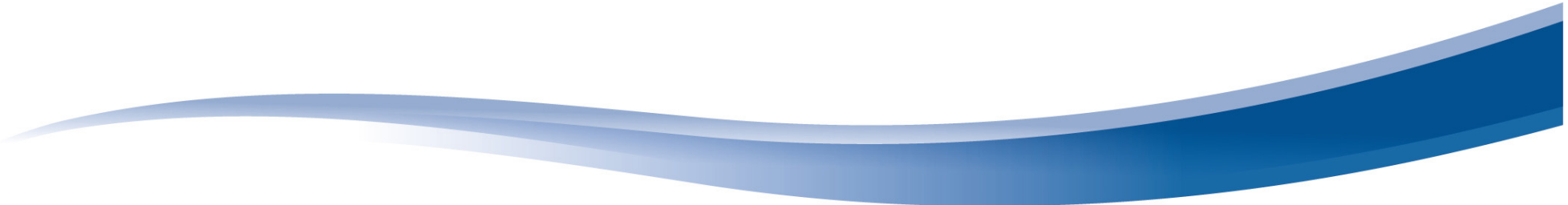


ビットコインは何が違うのか

**先の例で紹介したような仮想通貨とビットコインは、何が違うのか。
実は、存在している理由が全く違うのです。特定のゲームや Web サイト内でのみ使える仮想通貨は、企業単位で作られており、利用者を囲い込むことによって仮想通貨の運営主体(=ゲームや Web サイトの運営会社)が利益を上げること为目标としています。
一方のビットコインは、国家単位で運営されている円やドルと同じく、経済活動を円滑に進めるために作られた仮想通貨です。**



**ビットコインは、世界中で日常生活に「使える」ようにすることを
目指して作られています。仮想の通貨なので紙幣や硬貨は
存在しませんが、代わりにパソコンやスマートフォンを
お財布代わりにして、物の売買が実現できるようにつくられています。
まだまだ発展途上ではありますが、円やドル以上に利便性が高く、
安定し、世界中で利用できる次世代の通貨をめざして作られた
仮想通貨なのです。**



電子マネーとは

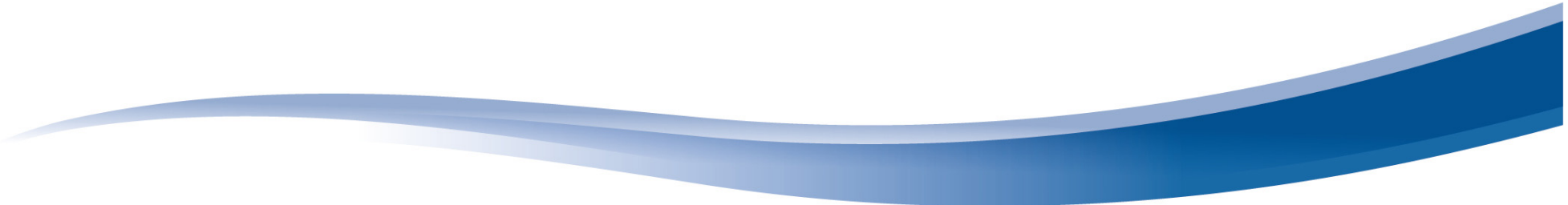
仮想通貨と似たような概念として、電子マネーというものが存在します。ビットコインを説明する上でよく登場する言葉です。

これらを混同していると理解の妨げになりますので、整理しておきます。

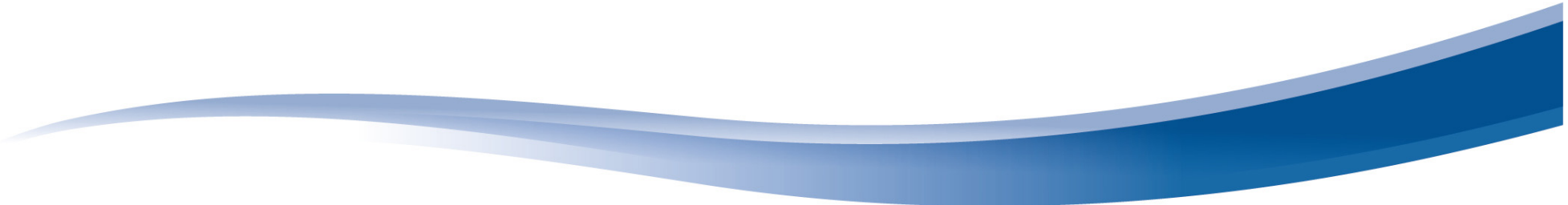
電子マネーとは、紙幣や硬貨を使わないで、
電子的に(＝データのやりとりで)決済を実現する手段の事です。

オンラインで決済を実行するタイプもあれば、最近主力になりつつある
非接触型の決済方法もあります。

電車に乗るときや、コンビニでの支払いに利用するものです。



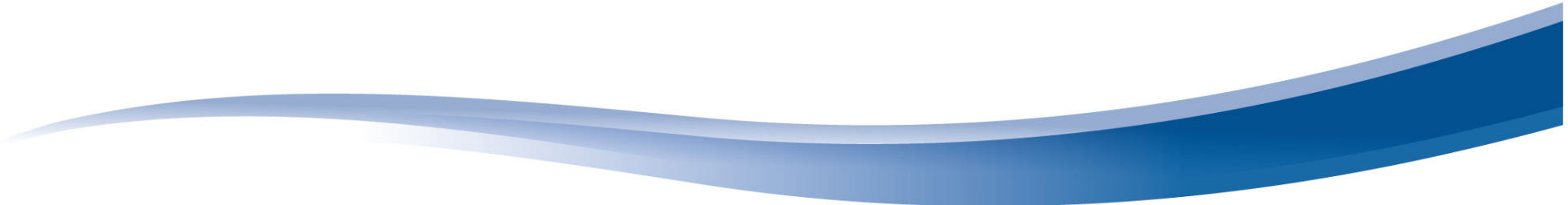
**すでに日常生活に浸透しつつあるしくみですので、
多くの方が実際に利用したことのあるものだと思います。
小銭を財布から出す手間もかからず、非常に便利です。
ビットコインも、電子マネーとして使える特徴を持っています。
そもそもビットコインは紙幣や硬貨が存在しない仮想通貨なので、
電子マネーとして使えるのは当然のことです。**



ではビットコインは電子マネーなのか

ビットコインを説明する際に、電子マネーであると説明するのは強引です。

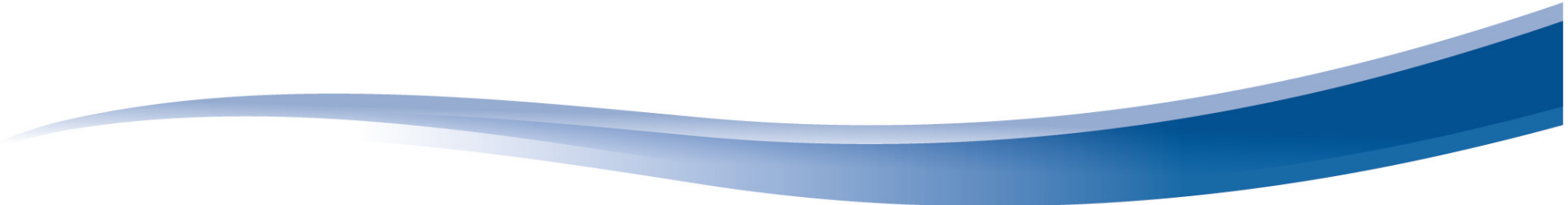
現在一般的に利用されている電子マネーは、基本的にはその地域で使われている通貨を使って電子的に決済を行うために存在しています。日本国内の例であれば、円での支払いをより便利にするために、円の紙幣や硬貨の代わりとして電子マネーが活躍します。そのため、利用者は所有する円を電子マネーの端末に入金したり、あるいは電子マネーでの支払いの際に利用される銀行口座にお金を入れておくことになります。



**紙幣や硬貨を利用せず、電子的に決済を実現していますが、
実態としては円という通貨をやりとりしていることには変わりありません。
ビットコインは、何らかの端末(カードなど)に円をチャージする
というものではありません。**

**ビットコインを利用して商品を購入する際には、まず手持ちの円
という通貨をビットコインという通貨に両替しなくてはなりません。
円をビットコインに両替してはじめて、ビットコインでの支払いが
実行できるのです。**

**両替をしたその後の支払いの流れは、一般的な電子マネーと同様です。
ビットコインでの支払いを受け付けているお店で、電子的にビットコイン
で決済を実行します。すると、自分の所有しているビットコインが減り、
お店の所有しているビットコインが増えます。**



ビットコインは、通貨です。

円やドルと違って仮想通貨ではありますが、通貨です。

**電子マネーとは、貨幣を使わないで決済できるようにする
しくみのことです。**

仮想通貨＝電子マネー、ではありません。

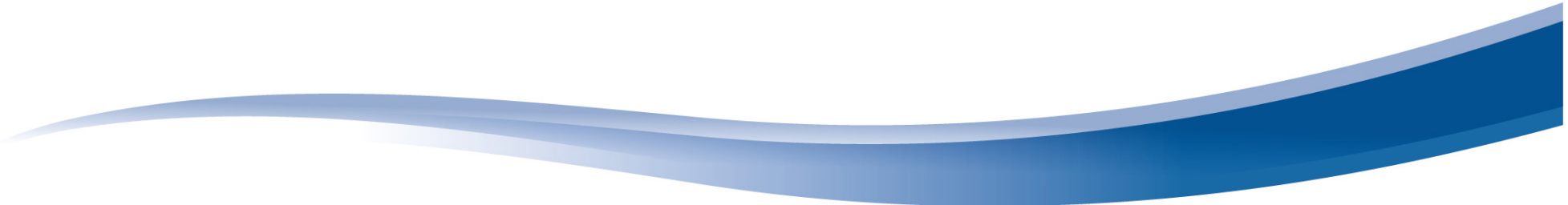


ビットコインを使うメリット

国家や企業が関与していないので、例えば個人間の送金において、次のようなメリットが存在します。

① 個人間で文字通り「直接」が送金できる

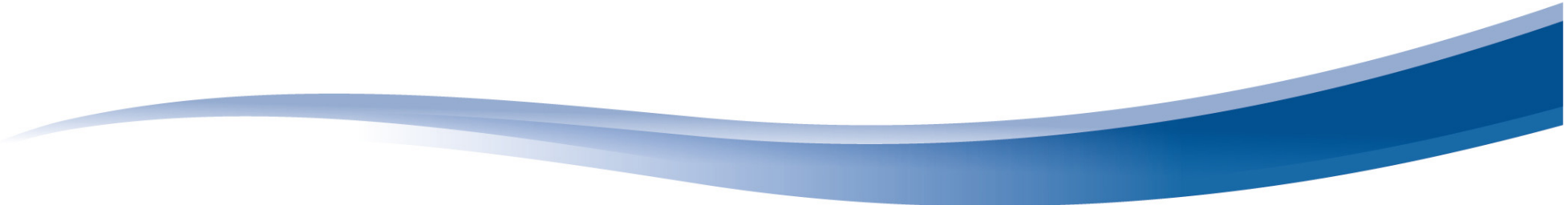
一般的な通貨で送金を行う際には、銀行などを仲介する必要があります。しかし、ビットコインの場合には、個人間が直接支払うことができます。ビットコインを使うメリットとして、直接会って財布からお金を出して支払うのと同じように、ビットコインを使えば直接相手にお金を支払うことができるのです。



② 手数料が無料もしくは、格安

仲介する組織が存在しないので、基本的には手数料を払う必要がありません。これは個人間の少額な支払いにおいては、非常に重要な特徴です。銀行送金でも、クレジットカード支払いでも、一定の手数料が存在します。そのため、少額の商品の売買が難しくなったり、ビジネスの利益率が下がったりします。

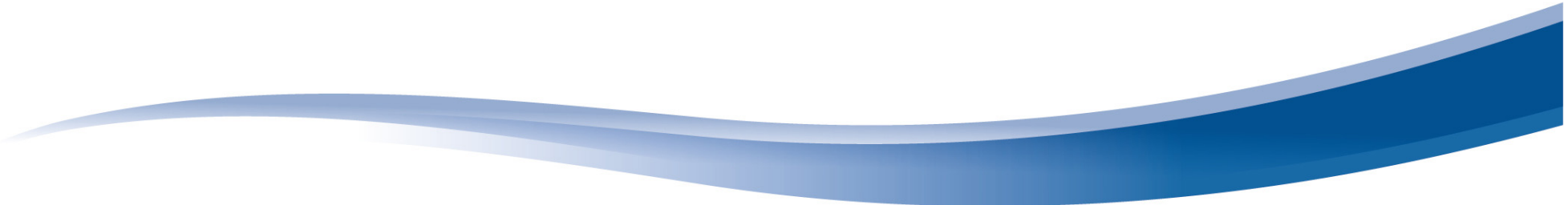
ビットコインは、その最大のメリットとも言える直接送金のしくみのおかげで、従来の手数料の概念を覆した決済を実現するのです。



③ 監視や制限などが存在しない

**ビットコインでの決済は銀行を経由した決済では無いので、
煩わしい手続きや制限が存在しません。
お金の流通が、より自由に行えるようになります。**

**また国によって通貨の単位が異なるといった特徴もありませんので、
ビットコインを使えば、世界中で同じ通貨が利用できるというメリットが
あります。そのためにはもっとビットコインが広まって、ビットコインでの
支払いを受け付けるお店が増える必要がありますが、いまでもすでに
ビットコインでの決済が可能なお店は世界中に存在します。**



どこにビットコインが保存されているか

ビットコインには、ウォレット(財布)という概念があります。これは、円やドルの例で言えば、銀行口座にあたるものです。

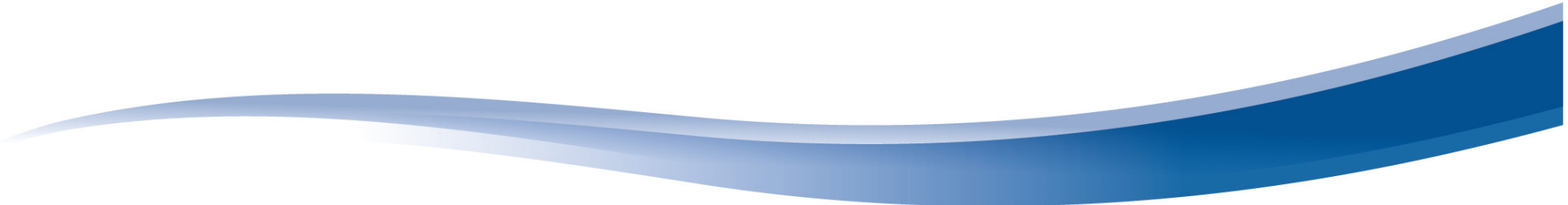
ビットコインを利用するすべての人はウォレットを持ち、そこにビットコインを保存し、決済に利用します。つまり、ビットコインを使いたい人は全員、ウォレットを作成する必要があります。

個人に割り振られるメールアドレスのようなものです。

実際には、長い文字列でウォレット ID が表現されます。

そのままでは覚えにくいいため、個人間送金が難しくなります。

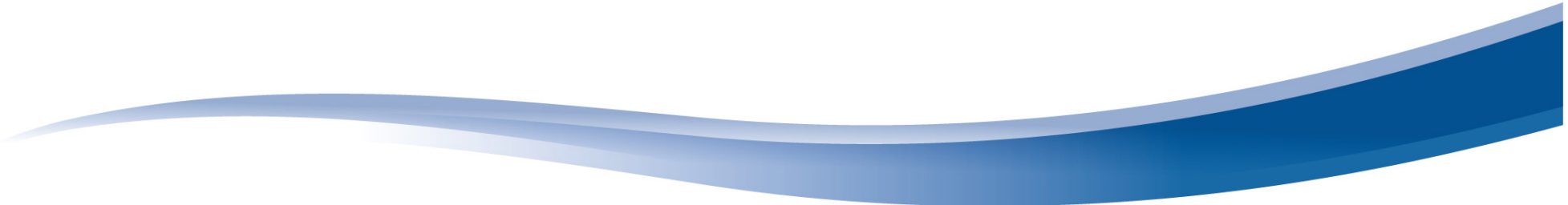
そこで、一般的には ID を短縮したコードを用いたり、スマートフォンで読み取れる QR コードに変換したりして、交換します。



ビットコインの課題

もちろん、円やドルでの決済がそうであるように、ビットコインでの決済でも、双方がビットコインによる支払いを受け付けている事が必須となります。ビットコインという通貨が「通じる」間柄でなければ、決済はできないのです。

円やドルと違ってまだまだ普及の初期段階にあるビットコインにおいて、これは非常に大きな課題です。



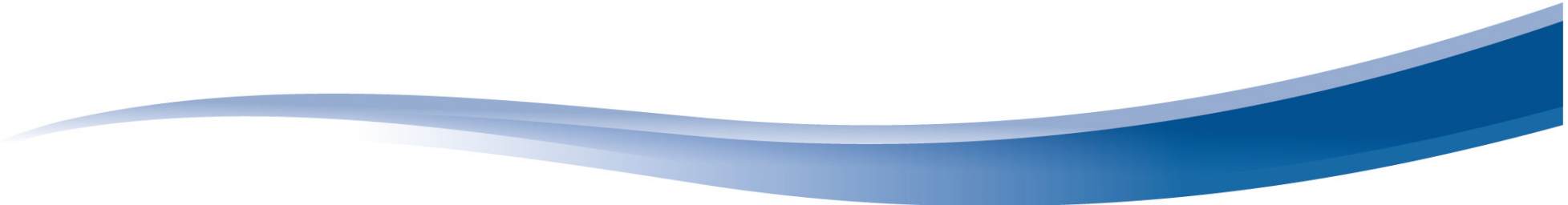
ビットコインで何ができるのか

ビットコインでできる事は、通常の通貨と同じです。

ビットコインを用いれば、個人間、企業間を問わず、物やサービスの対価として支払いを実行できます。つまり、ビットコインは仮想であるというだけで、通常の通貨と同じように使えるお金の一種だと言えます。

円やドルのような通貨と違う事としては、ビットコインでの支払いは電子的に行う必要があるという事です。現物の紙幣や硬貨がない仮想通貨なので、当然の事です。

ビットコインでは電子的に決済を行うため、インターネット経由で送金することが容易にできます。遠く離れた相手にでも、あるいは目の前にいる人にでも、短時間でビットコインを送金できるのです。

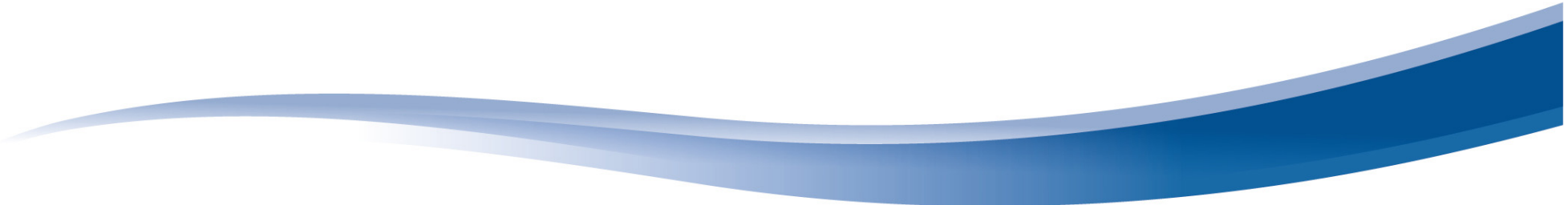


円やドルとの決定的な違い

円やドルと全く同じような通貨であれば、わざわざ新しい通貨を作る必要性はありません。ビットコインは、他の通貨と比較して何が決定的に違うのでしょうか。

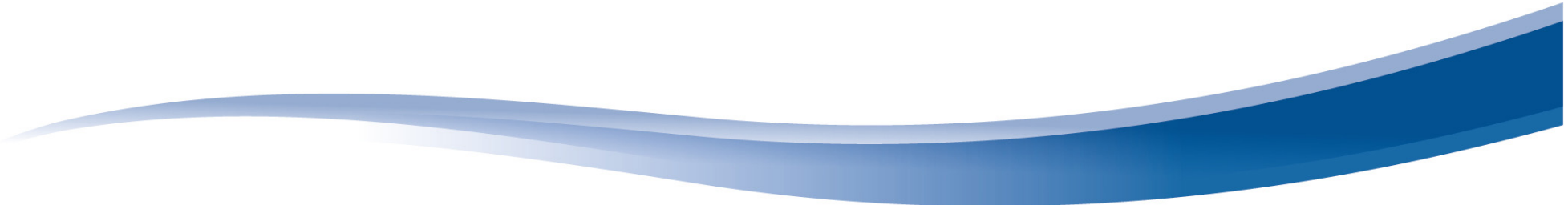
最大の違いは、通貨を管理する「中央銀行」が存在しない、ということです。ビットコインには、発行を司る組織や流通を管理する組織が存在しないのです。

ビットコインは、国家や企業が運営している仮想通貨ではありません。円やドルと同じような通貨なのに、どこの国も、企業も、ビットコインの発行・流通には関与していないのです。この非常識な概念が、ビットコインの最大の特徴です。



誰がビットコインを管理しているか

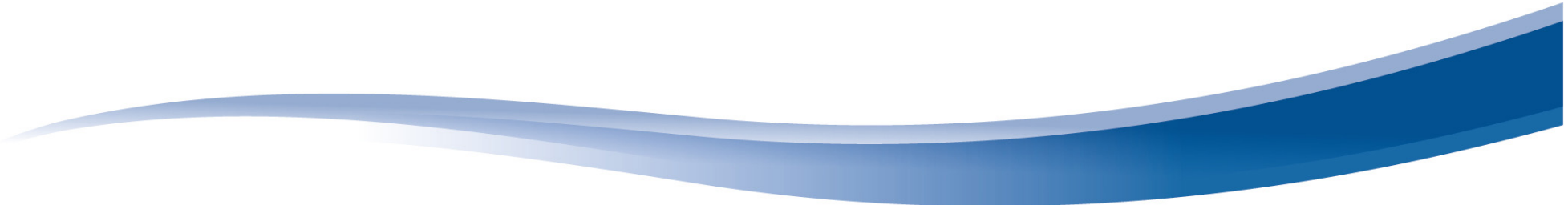
国家や企業が管理していない通貨と述べましたが、それでは一体誰がビットコインを発行し、流通を管理しているのでしょうか。常識的に考えれば、誰も管理していない通貨など、リスクの塊でしかありません。誰かが勝手に通貨を大量に発行してその通貨の大金持ちになることができてしまえば、通貨の信用は失われます。そんな不安定な通貨は流通しませんし、誰も価値を見出しません。ビットコインは、中央での管理を行わない代わりに、コンピューターのネットワークを利用して通貨を管理する仕組みとなっています。ビットコインにおける新しい通貨の発行や、取引の詳細情報は、そのすべてがコンピューターネットワーク上に分散されて保存されます。



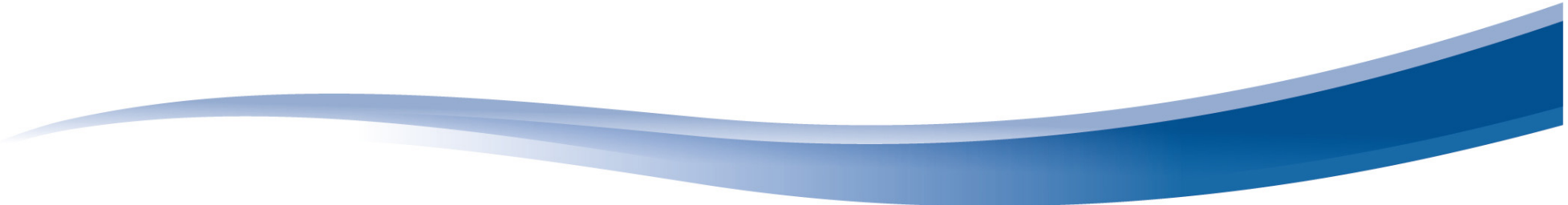
ビットコインで行われたすべての取引記録を記載した、1つの大きな取引台帳が存在しているとイメージしてください。

この可視化された記録のおかげで、通貨の偽造や二重払いなどを防止することができます。すべての記録は残りますが、その記録に個人情報を含みません。記録はあくまでも、ビットコインの流通の整合性を保証するために存在するのです。

1つの大きな取引台帳を特定の組織が管理していたら、これまでの通貨と同じです。ビットコインは、特定の組織の元ではなく、分散されたコンピューターのネットワーク上にその1つの大きな取引台帳を置くことで、中央管理を不要とする仕組みなのです。

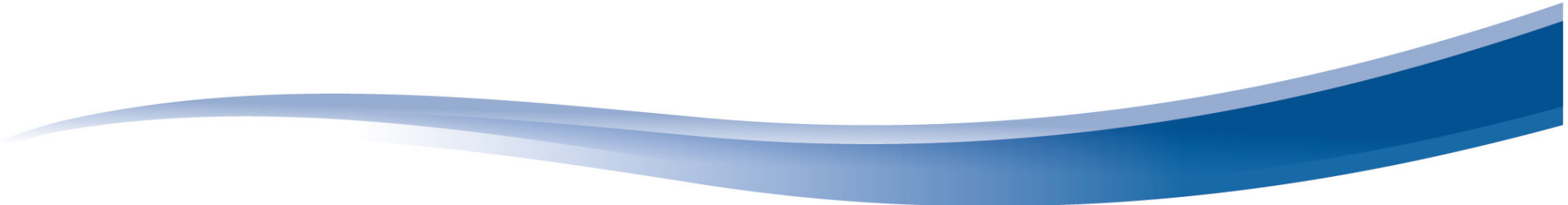


**取引の整合性を保証するための1つの大きな取引台帳なのに、
そのデータが分散されて保存されていたら、取引記録に
不整合が発生してしまいそうです。
しかし、ビットコインはこの解決策を生み出したために、
今日に至る広がりを見せています。**



ビットコインのマイニング(採掘)

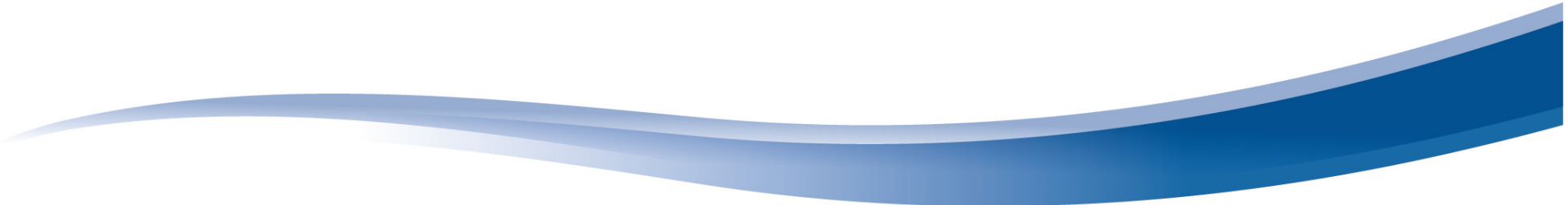
一定期間ごとに、すべての取引記録を取引台帳に追記します。その追記の処理には、ネットワーク上に分散されて保存されている取引台帳のデータと、追記の対象期間に発生したすべての取引のデータの整合性を取りながら正確に記録することが求められます。その整合性を取る作業はコンピューターによる計算で実現できるのですが、膨大な計算量が必要となります。分散されて保存されている1つの大きな取引台帳のデータも、追記対象の取引のデータも、すべてを正確に検証してから追記しなければならないのです。そこで、ビットコインでは、この追記作業に有志のコンピューターリソースを借りています。



余っているコンピューターの計算能力を借りることによって、膨大な計算を行い、みんなで共有する1つの大きな取引台帳に追記を行っているのです。

この追記作業の手伝いをしてくれた人、追記作業のために膨大な計算処理をし、結果として追記処理を成功させた人には、その見返りとしてビットコインが支払われます。つまり、追記作業を手伝ってビットコイン全体が健全に運用されるようにがんばってくれたことへの報酬として、ビットコインが支払われるのです。

この報酬は、新たに発行されたビットコインによって支払われます。つまり、通貨の新規発行がこの瞬間に起こるのです。



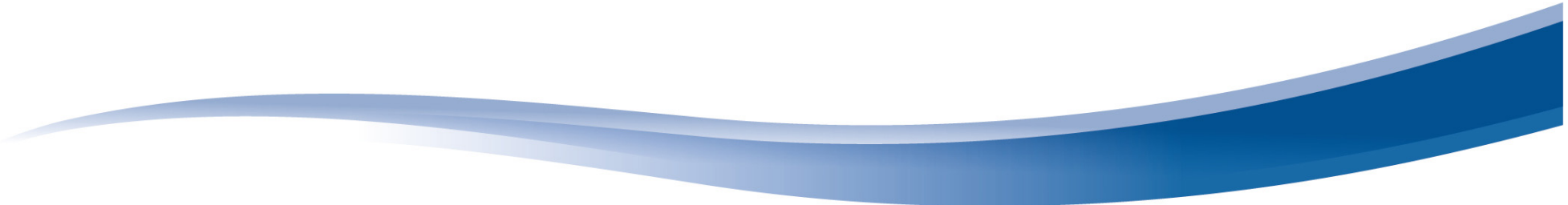
ゲームをしていてもいいし、ネットで遊んでいてもいいのに、わざわざ膨大な計算を行ってビットコイン全体の発展に貢献してくれた人へのささやかな感謝の形が、新規ビットコインの発行なのです。

この新規発行に至る行為は「採掘（マイニング）」と呼ばれています。

コンピューターの計算能力をお金に変えるビジネスと割りきって、日夜採掘（マイニング）に励んでいる人たちが世界中に存在します。

そのおかげで、今日もビットコインの安全性が保たれているのです。

通貨としてのビットコインの新規発行は、この採掘（マイニング）を通じてしか行われません。そのため、ビットコインの発展を信じる人達が、次々と採掘活動（＝1つの大きな取引台帳の更新作業）に力を注いでいるのです。



マイニング(採掘)は無限に新規発行が可能か

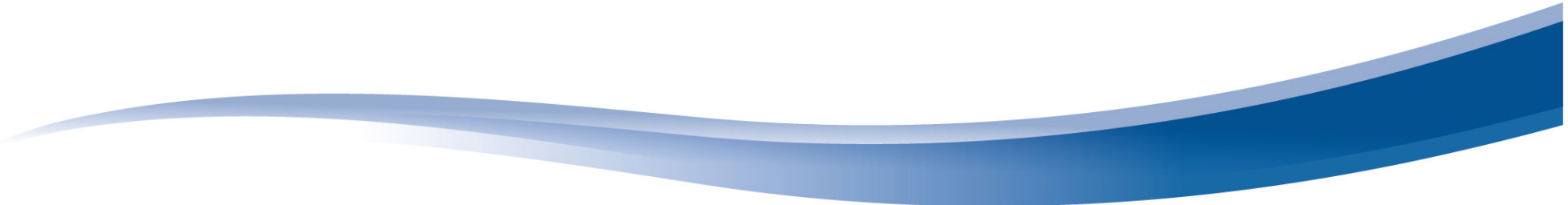
ビットコインの発行総量は、事前に決められています。

また、採掘(マイニング)によって発行される量も調整されています。

そのため、一瞬にして発行量が増えてインフレが起こったり、

混乱が生じることを避けた設計がなされています。

**ビットコインの発行総量は、2140年までに2,100万 Bitcoin と
されていて、それ以降は新規に発行されることがありません。**



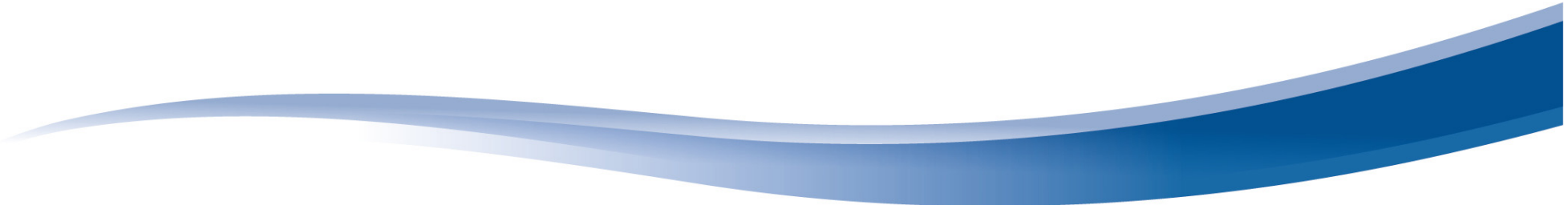
仮想通貨の種類

世界で流通している仮想通貨の種類は 1,500 以上とされています。

ビットコイン(BTC)

2008 年に「サトシ・ナカモト」と名乗る人物がインターネット上に公開した論文の中で構想が示され、それを受けて運用が開始された仮想通貨です。分散型台帳を作る技術であるブロックチェーンを利用することで、公的な発行主体や管理者の裏付けなしにネットワークを介して価値の保存や移転を行える特長があります。

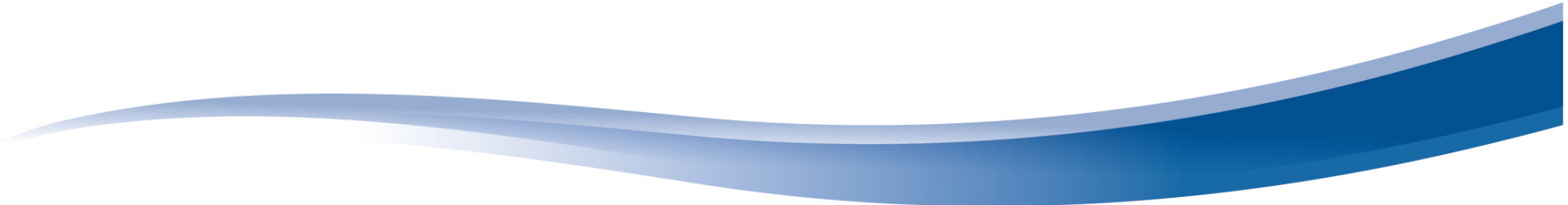
ビットコインは数ある仮想通貨の中で時価総額が最も大きいことから、仮想通貨の代表格と言っても過言ではありません。ビットコインから分裂や派生した通貨も多く、仮想通貨の基軸となっています。



ビットコインキャッシュ(BCH)

ビットコインキャッシュは、2017 年 8 月にビットコインからハードフォークして誕生した通貨で、ビットコインの課題であるスケーラビリティ問題をブロックサイズの拡大により克服しようとした仮想通貨です。

ビットコインと比べてブロックサイズが 32 倍になっており、手数料の減少にも繋がっています。



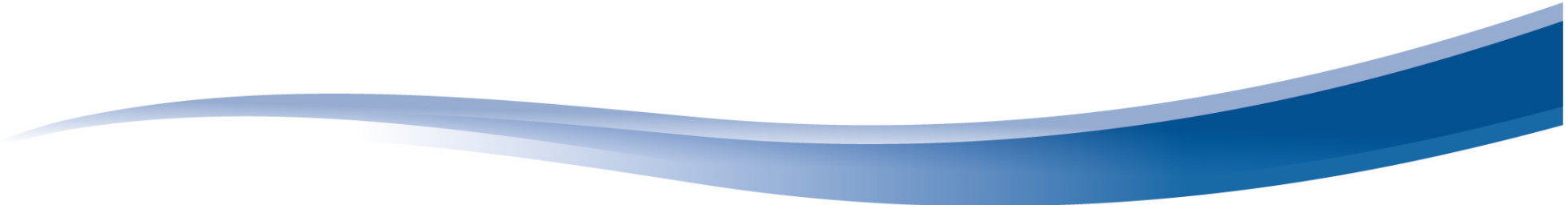
イーサリアム(ETH)

2015 年 7 月に登場したイーサリアムは、2018 年 6 月現在、ビットコインの次に時価総額が大きい仮想通貨です。

ビットコインがブロックチェーンを利用して取引記録を管理することに特化しているのに対して、イーサリアムは公的な発行主体や管理者なしにユーザーが独自に定義した契約を自動執行できる

「スマートコントラクト」を扱えるのが特長です。

スケーラビリティ問題に対しては、Plasma と呼ばれる新しい技術によって解決しようとしており、具体的な手法については日夜議論されています。

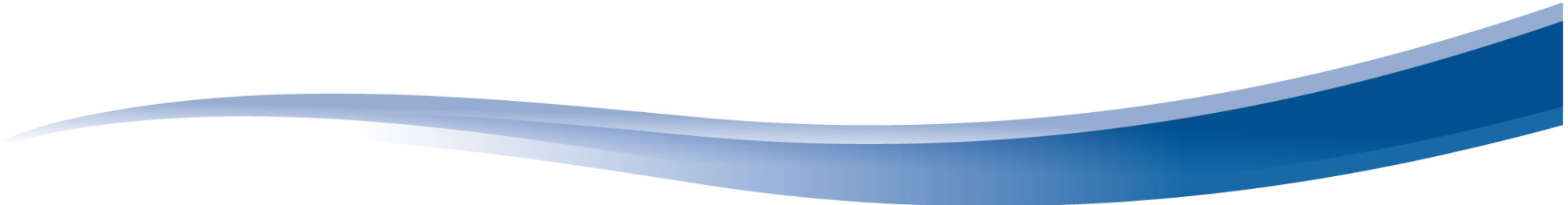


イーサリアムクラシック(ETC)

2016 年 7 月に登場したイーサリアムクラシックは、イーサリアムが分裂してできた仮想通貨です。

イーサリアムと同様に、スマートコントラクトによる利点も兼ね備えているのが特長です。

イーサリアムクラシックは、イーサリアム財団のハードフォーク反対派により立ち上げられ、ハードフォーク前のオリジナルのイーサリアムブロックチェーンを継承しています。



ライトコイン(LTC)

2011 年 10 月に登場したライトコインは、ビットコインのシステムを基盤として生まれた仮想通貨で、採掘(マイニング)にかかる時間が短くストレージの効率性に優れているという特長があります。
ライトコインの総発行量はビットコインの約 4 倍の 8,400 万枚です。
ライトコインの平均ブロック生成時間は 2.5 分であり、ビットコインの短所であった送金時間の問題を克服しようとしています。