# 01 ブロックチェーンとは何か

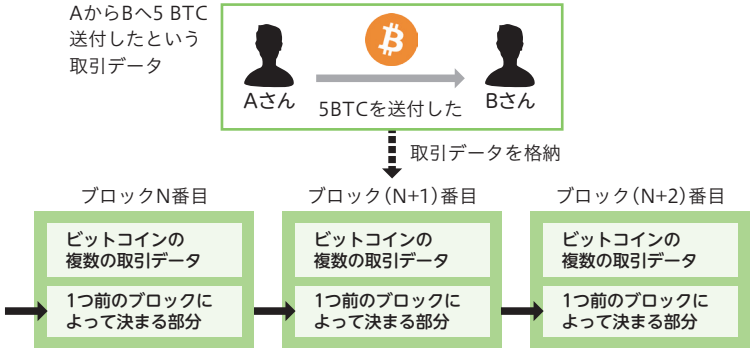
**「インターネット以来の革命」と称されることもあるブロックチェーン。今なぜ、これほどまでの注目を集めているのでしょうか。ブロックチェーン技術とは一体何なのか、どのような部分が革命的なのか、まずはその概要を理解しましょう。**

## ひとことでいうと「取引履歴をまとめた台帳」

ブロックチェーンとは「**複数の新しい取引（送金）データをブロックと呼ばれる塊にまとめて、1つ前のブロックにつなげていくことで1本の鎖（チェーン）のようになっている分散型のデータベース（台帳）**」のことです。

このデータベース（台帳）は、世界中の多数のコンピューターによって管理・検証されており、すべてのノード（コンピューター）が同じデータを共有しています。そのため、誰でもブロックチェーンの記録を参照することが可能です。また、ブロックチェーンの仕組みとして、各ブロックには前のブロックの情報が含まれており、順番に連結することでデータの整合性を保っています。仮に悪意ある第三者が、過去の取引データの一部を改変すると、次のブロックとの整合性がつかなくなってしまいます。つまり、すぐにデータの改ざんを検知することが可能です。加えて新しいブロックをつなげるには大きな計算能力が必要となるため、実質的にデータを改ざんすることが難しくなっています。

■ビットコインのブロックチェーンのイメージ




## ブロックチェーン≠ビットコイン

まず混同しないように注意したいのが、**ブロックチェーンとビットコインは同じものではない**ということです。ブロックチェーンとは、ビットコインなどの暗号資産を実現するための基盤技術のことです。ビットコインのブロックチェーンでは、新しい取引の記録がブロックとして約10分ごとに作成され、チェーンの先端に追加されていきます。過去の取引がすべてチェーン（鎖）としてつながっているため、1本のブロックチェーンを読み出すことで、どのアドレス（ウォレット）が、いくらのビットコインを所有しているか、確認することができるのです。

## 定義は一定ではなく、さまざまなブロックチェーンが存在する

2025年現在、世の中にはビットコインのブロックチェーン以外にもさまざまな種類のブロックチェーンが登場しています。そのため、ブロックチェーンとは何か？の厳密な定義は少々難しく、その言葉が指すものには幅があります。ここでは、一般にパブリックチェーンと呼ばれるものには、どのような特徴があるかを見ていきましょう。

■パブリックチェーンの特徴

| 特徴 | 説明 |
|---|---|
| トラストレス | 不特定多数の参加者がいるネットワーク上で、中央銀行のような信頼できる管理者がいなくても、データの合意（コンセンサス）を得られる。 |
| 高い改ざん耐性 | デジタル署名やハッシュ関数といった暗号技術により、取引データを改ざんするとすぐバレてしまうため、実質的に不正を行うことができない。 |
| 分散型ネットワーク | 特定のサーバーではなく、ネットワーク上に分散した多数のコンピューターが、同一の計算・検証をして、同一のデータ（台帳）を保持している。 |
| 高い障害耐性 | 分散化により、システム全体がダウンする可能性が極めて低く、かつデータの同一性が保証されている。 |

# 05 金融

**ブロックチェーン技術が金融分野での大きな可能性を切り開いており、従来の銀行システムに依存せず、迅速かつ低コストでの資産移転が可能になりました。ブロックチェーンを活用した金融分野の主要なユースケースについて紹介します。**

## DeFi（分散型金融）

DeFi（Decentralized Finance）は、ブロックチェーン技術を基盤とした金融サービスの総称で、**従来の金融機関とは違って中央管理者や仲介機関を必要としない金融システムを提供**します。ブロックチェーン上であらかじめ決められたルールを自動で実行するスマートコントラクトを活用することで、誰でもスマートフォンやパソコンから、貸し借り・取引・資産運用といった金融サービスにアクセスできるのが特徴です。

特に、2020年代以降にDEX（分散型取引所）、レンディング、ステーキングなどのサービスが急速に普及しました。

- **DEX（分散型取引所）**

中央管理者がいない取引プラットフォームであり、ユーザーは自分のウォレットを接続するだけで暗号資産を直接取引できます。これにより、取引手数料の削減や透明性の向上が図られています。

- **レンディング**

暗号資産を貸し出して利息収入を得たり、担保を差し入れて資金を借りたりすることができます。スマートコントラクトが貸し借りのプロセスを管理するため、安全で効率的な資産運用が可能です。

- **ステーキング**

特定のブロックチェーンネットワークに暗号資産を預けることで報酬を得る仕組みです。ネットワークのセキュリティ維持や取引承認に貢献する代わりに、預けた資産量や期間に応じた報酬が支払われます。

■ 従来型の金融とDeFiの比較

| | 従来型の金融 | DeFi |
|---|---|---|
| 管理者 | 銀行などの中央集権型 | スマートコントラクトによる分散型 |
| 透明性 | 一部のみ公開 | ブロックチェーン上で公開 |
| 手数料 | 通常手数料に加えて人件費や仲介コストなど | 仲介不要のため手数料が安価 |
| 金融商品 | 貯金・ローン・投資信託など | ステーキング・レンディング・ファーミングなど |
| アクセス | 管理者による審査が必要 | インターネット上で誰でもアクセス可能 |

## 暗号資産

暗号資産の代表であるビットコインは、ブロックチェーンを利用したデジタル通貨です。ビットコインは史上初めて中央銀行などの管理機関に頼らずに価値を持つ通貨として機能し、独自の経済圏を作り上げることに成功しました。銀行に頼ることなく送金ができ、手数料も低く抑えられているため誰でも世界中の相手に直接送金できるP2P送金や決済などの利用が期待されます。

暗号資産はスマートフォンなどネットワークに接続可能な端末さえあれば、銀行口座を持たない個人でも送金や預け入れといった金融サービスが利用できるため、既存の金融インフラが行き届いていない発展途上国の人たちの受け皿となる新たな金融インフラとして期待されています。

ここで「暗号資産」という言葉には、日本の法律上の定義と業界で広く使われる意味の2つがある点を整理しておく必要があります。

日本の法律（資金決済法）で定義される暗号資産は、簡単にまとめると「円やドルなどの法定通貨ではないが、**代金の支払いに使え、インターネット上で記録・送金でき、さらに円やドルと交換できるもの**」で、ビットコインやアルトコインを指します。

# 10 ビットコインの動作

**3章では、暗号資産の代表的存在であるビットコインを例に、ブロックチェーンの仕組みを詳しく解説していきます。その前に、まずはビットコインとはどのようなものであるかを押さえておきましょう。**

## ビットコインとは何か

ビットコインとは、サトシ・ナカモトによって2008年に発表され、2009年より運用が開始された**世界初の暗号資産**です。最大の特徴は、中央に管理者が存在せず、インターネットを介して世界中のコンピューター同士が直接つながるP2P（ピア・ツー・ピア）ネットワーク上で動作することです。

この仕組みにより、従来の銀行のような仲介機関を介さず、特定の国や企業、政府の許可や制限を受けることもなく、個人が直接お金をやり取りできるということです。そのため、政府が強制的に預金を凍結したり、送金を止めたりするような行為は、ビットコインの仕組み上では非常に難しくなっています。

ビットコインのネットワークは世界中の誰でも自由に参加することができ、誰の許可もなく自由に送金などの操作を行うことが可能です。すべてのやり取りはネットワークを介して行われるため、送金先が海外であっても、従来の国際送金のように何日もかかったり、高額な手数料が必要になったりすることはありません。ビットコインであれば、数十分～数時間以内に低コストで送金が完了します。また銀行の営業時間なども関係ないので、24時間365日いつでも利用できます。

またビットコインを利用するのに身分の証明手続きは不要です。銀行口座などを持っている必要もなく、最低限インターネットに接続できるスマートフォンなどの端末があれば利用を開始できます。この性質から、ビットコインは**プライバシーを重視する人、既存の金融インフラが未発達な国で銀行口座を持たない人**などに重宝されてきました。

## ビットコインの価値の源泉

ビットコインは米ドルや日本円などの法定通貨による裏づけがなく、国家や中央銀行の後ろ盾なしに独自の価値を持った通貨です。では、そもそもただの紙切れである「お金（紙幣）」自体に価値はないはずなのに、なぜ「お金（紙幣）」は価値を持っているのでしょうか。それは、「国家が保証しているから」という信用があるからです。つまり、通貨の価値とは、その背後にある信用に支えられているのです。

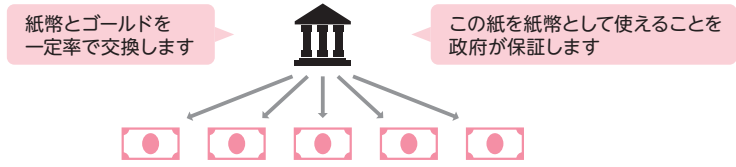
一方、ビットコインの場合は国家による価値（信用）の裏づけがありません。

- **国家や中央銀行に頼らず、また誰の干渉も受けず、瞬時にオンラインで価値を移転できるシステムであること**
- **それにより、ビットコインのシステムに高い利用価値があると信じている人が多数存在すること**

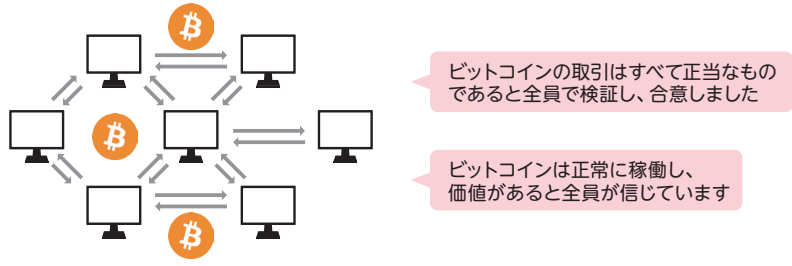
この2つの特徴がビットコインに価値をもたらしているのです。

■法定通貨とビットコインの価値の源泉

**法定通貨は政府や中央銀行の信頼、金との交換などで価値を担保する**




**ビットコインはネットワーク参加者の合意により、共同で価値を担保する**



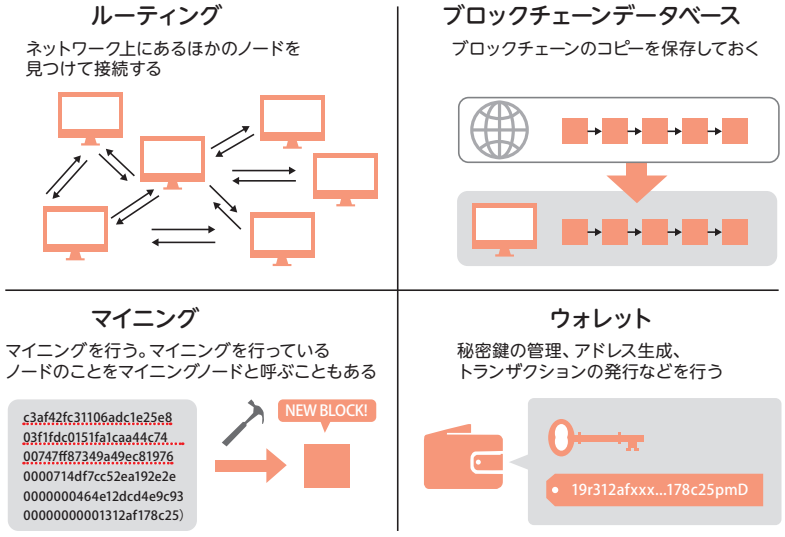
# 20 ビットコインネットワーク

**この節では、ビットコインネットワークを構成するノードの種類と役割、ノードがネットワークに参加するまでのプロセスを解説します。世界中に分散されているノードがどのように連携しながらネットワークを作り上げるのか、イメージを掴みましょう。**

## ネットワークを構成するノードの機能

ビットコインのネットワークは、3章で解説したP2P方式で運用されています。ノードは大きく分けて、下記の4つの機能を持っています。

■ ノードが持つ 4 種類の機能




- **ルーティング**：ビットコインのネットワーク上にあるほかのノードを見つけて接続する機能です。ネットワークに参加するために必須の機能なので、すべてのノードがこのルーティング機能を持っています。
- **ブロックチェーンデータベース**：ブロックチェーンのコピーを保存しておく機能です。チェーンの最初のブロック（ジェネシスブロックと呼ばれます）から最新のブロックに至るまで、すべてのブロックの完全な記録を保持しているフルブロックチェーンノードと、ブロックヘッダ部分の記録のみを保持している軽量ノード（SPVノード）があります。
- **マイニング**：その名の通り、マイニングを行う機能です。この役割を担うノードは「マイニングノード」と呼ばれ、取引データをブロックにまとめ、そのブロックをブロックチェーンに追加するための「PoW（Proof of Work）」に基づく計算競争を行います。
- **ウォレット**：秘密鍵を管理してビットコインアドレスを生成する機能、およびトランザクションに署名して送金指示を行う機能です。

## ビットコインネットワーク上のノードを見つける

ノードがビットコインネットワークに参加するには、まずすでにネットワークに参加しているノードを見つけて接続する必要があります。とはいえ、初めてビットコインネットワークに接続する際には、アクティブなノードのIPアドレスがわかりません。そのため、まずは**DNS Seeds**と呼ばれるサーバーに問い合わせて、接続可能なノードを教えてもらいます。

DNS SeedsはビットコインのDNSで、ネットワーク上のアクティブなフルノードのIPアドレスを収集し、提供しています。Bitcoin CoreやBitcoinJ等の主要なビットコインクライアントには、あらかじめこのDNS Seedsに問い合わせする機能が用意されています。

## ノード同士で接続する

ビットコインのネットワークでは、ノード同士が対等な立場で接続するP2P（ピア・ツー・ピア）構造を採用しています。P2Pネットワークでは、ノードが接続している（対等な関係にある）ほかのノードのことを**ピア（Peer）**、もしくは**ピアノード**と呼びます。

新規に参加するノードは、DNS Seedsの情報を元にネットワーク上のアクティブなノードを発見した際、そのノードに自身の接続情報を送信します。

# 30 ウォレットの種類と仕組み

**ウォレットという言葉から、暗号資産自体を保管しているように感じますが、実際は暗号資産の操作をするのに必要な秘密鍵を保管しています。ウォレットには、大きく分けて「ホットウォレット」と「コールドウォレット」の2種類があります。**

## ウォレットの定義

暗号資産におけるウォレット（Wallet）は「暗号資産のお財布」ともいわれますが、実は明確な定義があるわけではなく、使われる文脈によって意味が少しずつ異なります。主に、以下の3つの意味で使われることが多くなっています。

**1. 暗号資産の送金等の操作で使用する公開鍵と秘密鍵のペア、その実装**
**2. 秘密鍵を安全に管理・保管するもの**
**3. 暗号資産の送受信、残高管理、履歴確認などを行うためのアプリケーション**

ここでは主に、2の意味の、ウォレットが鍵の管理を行う仕組みを解説します。

## ウォレットの仕組み

ウォレットの定義からわかるように、**ウォレットは「鍵」を保管**しています。4章で学んだ通り、公開鍵は誰に知られても問題はありませんが、秘密鍵は第三者に知られてしまうと所有している暗号資産を不正に操作されたり奪われたりする可能性があります。ウォレットはこの秘密鍵を安全に保管するだけでなく、以下のような機能も持ちます。

- **アドレスの生成**
  秘密鍵から公開鍵、そしてそのハッシュ値から送受信に使うアドレスを自動的に作成

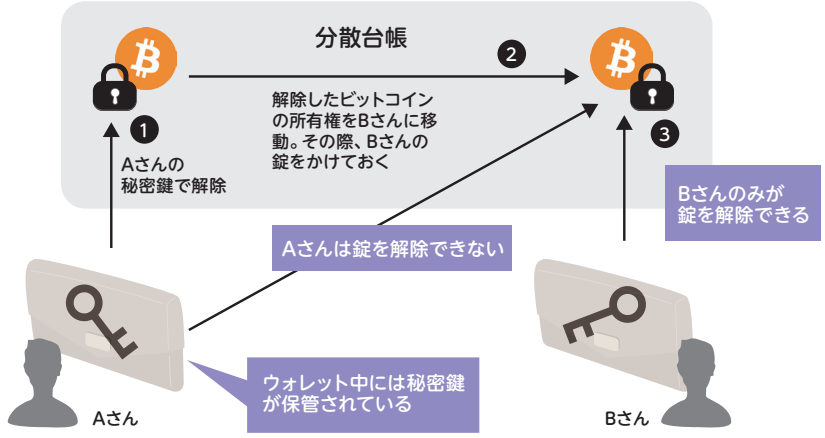


- **署名の生成**
  トランザクションを作成する際に、秘密鍵を使ってデジタル署名を生成

- **トランザクションの発行**
  ブロックチェーンネットワークに送金処理などのトランザクションを送信

次の図では、ウォレットを用いて暗号資産のやり取りをする際のイメージを示しています。

■ウォレットの秘密鍵を使ってビットコインの所有権を移動させる




**1. Aさん自身が所有している秘密鍵でトランザクションアウトプットのロックを解除します。**
**2. Aさんはコインをさんに移動させるトランザクションを発行します。このとき、Bさんの公開鍵を用いてトランザクションをロックします。**
**3. トランザクションの発行後は、Bさんの秘密鍵のみがロックを解除できるようになり、元の所有者であったAさんの鍵ではロックの解除はできなくなります。**

# 37 スマートコントラクトとは
## ～分散ネットワーク上での契約締結・自動執行

**スマートコントラクトとは、広義には「取引における契約・執行を自動で行う仕組み」全般を指します。また、ブロックチェーンの文脈では「イーサリアムなどのブロックチェーンに配置された自律的に動作するプログラム」のことを意味します。**

### スマートコントラクトの定義

スマートコントラクトに関しては専門家や著名人によってさまざまな解釈が存在し、明確な定義は定まっていません。もともとは、1990年代に法学者・暗号学者であるNick Szabo氏が「デジタルな方法により、あらゆる資産が動的に処理されるような契約（コントラクト）」をスマートコントラクトと呼んだことに端を発します。現在では、**広義では「取引における契約・執行を自動で行う仕組み」のことを指すもの**とされています。ただし、ブロックチェーンの文脈においては、スマートコントラクトは「ブロックチェーン上に配置された自律的に動作するプログラム」のことを指し、**日本語における法的な「契約」という意味合いは含まれていません**。本書でも、このブロックチェーンにおける定義で説明していきます。

イーサリアムの考案者であるヴィタリック・ブテリン氏は、2018年10月には「イーサリアムにおけるプログラムを”Smart Contract”と名づけたのを後悔している。より技術的な言葉として、例えば”Persistent Script”と名づけるべきだった」と発言しています。彼は”Persistent Script”という表現で、「ブロックチェーン上で永続的に動くプログラムである」という特徴を表したかったのでしょう。

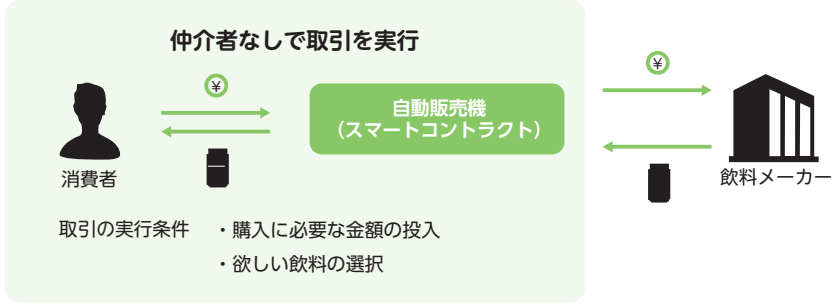
### スマートコントラクトの例

スマートコントラクトという概念の提唱者であるNick Szabo氏は、スマートコントラクトの例として自動販売機を挙げています。



自動販売機で飲料を購入するのに必要な条件は、「お金の投入」と「飲料の選択」であり、両方が行われない限り飲料は手に入りません。つまり、自動販売機は「あらかじめ設定されたルールに従って、自動的にお金と商品の交換を行うシステム」といえます。この仕組みでは、人を介さずに取引が成立しており、契約書も仲介者も必要ありません。まさに、スマートコントラクトの本質である「条件を満たしたときに、自動で取引を実行する仕組み」を体現した日常的な例です。

■自動販売機はスマートコントラクトの一例

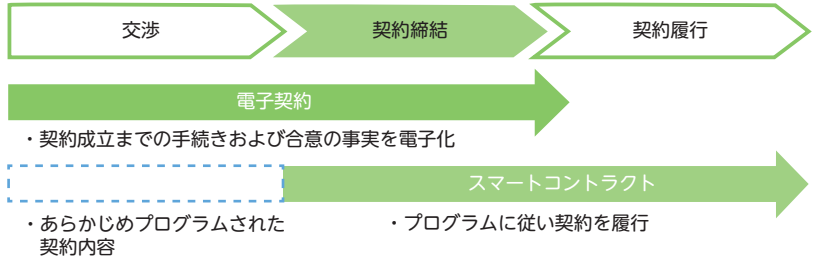



### スマートコントラクトと電子契約の違い

電子契約とは、契約成立までの手続きや、契約書の合意の事実を電子化することです。

一方、スマートコントラクトは、上記の自動販売機でも触れた通り、あらかじめ決められたプログラムに従い、契約の執行までを半ば強制的に行います。

■電子契約とスマートコントラクト



# 49 51%攻撃
## ～計算能力の過半を支配することによる弊害

**PoWは多数のマイナーの計算によって分散的に支えられています。しかし一部のマイナーがネットワークの過半数を超過するハッシュパワーを得てしまうと、そのマイナーはブロックチェーンを攻撃できてしまうため、ブロックチェーンのセキュリティが失われてしまいます。**

### 51%攻撃の概要

51%攻撃とは悪意のあるグループまたは個人が、ネットワーク全体のハッシュパワーの過半数より上か、それに準ずるような大きな割合を支配し、攻撃を行うことです。1つのグループが全体の計算能力の過半数超を支配すると、以下のようなことが可能になります。

- **トランザクションの恣意的（しいてき）な取り込み**
- **正当な取引の恣意的な拒否**
- **マイニングの独占**

51%のハッシュパワーを持つことで実現される攻撃の方法を、それぞれ見ていきましょう。

### トランザクションの恣意的な取り込み

事例を通じて、51%攻撃における**トランザクションの恣意的な取り込み**の仕組みを理解しましょう。以下は、ビットコインを送った後にそれを取り消し、商品を無料でもらう攻撃の例です。

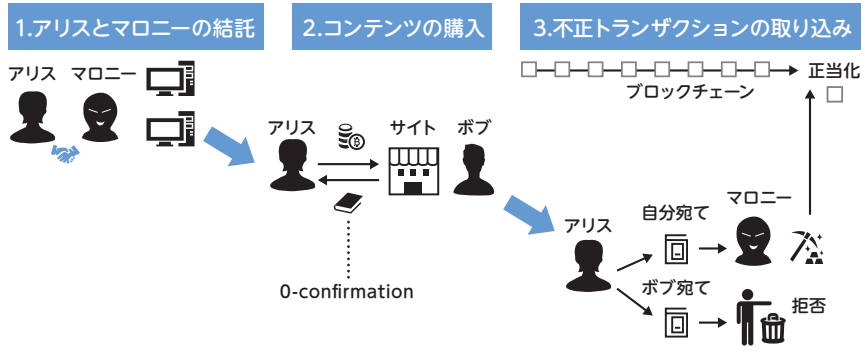
攻撃者のアリスと、過半数のマイニングパワーを持つ共犯者マロニーが協力し、オンラインショップ運営者ボブを騙すとします。アリスはまず、ボブのサイトでデジタルコンテンツを購入し、ボブ宛てのビットコイン送金をネットワークに送信します。



ボブは「0-confirmation（未確定の状態）」でもアクセスを許可する仕組みにしていたため、トランザクションがブロックに取り込まれる前に、アリスにコンテンツを提供してしまいます。その直後、アリスは同じビットコインを使って、今度は自分宛ての送金トランザクションを別途発行します。

マロニーはそのトランザクションだけをブロックに含め、ボブ宛ての送金は無視します。これにより、ボブは代金を受け取れないまま、アリスに商品を渡してしまった形となります。このように、トランザクションの取り込みを意図的に操作することで、支払いのキャンセルが成立してしまうのです。

■不正な取引の正当化




### 恣意的な正当な取引の拒否

マイナーは51%以上のハッシュパワーを持っていると、「正当な取引」を拒否することができます。通常トランザクションがネットワークに送信されると個々のノードによって伝播され、ネットワーク全体で共有されます。しかしネットワークの過半数超を握るマイナーは正当に作成したトランザクションを受け取っても、自分のトランザクションプールに取り込まず、ほかのノードにも伝播させないことで、そのトランザクションがブロックチェーン上に記録されることを意図的に妨ぐことが可能になります。これが仮に企業によるものだったら、**競合企業の取引だけを意図的に排除してネットワークを使わせないという妨害が可能**になります。

# 53 NFT（非代替性トークン）

**NFT（非代替性トークン）は、アート、ゲーム、音楽、さらにはアイデンティティ管理など、さまざまな分野で革新的な活用が進んでいます。本セクションでは、NFTの注目の技術や規格主を紹介し、NFT市場の新たな可能性についても考察します。**

## SBT (Soulbound Tokens)

SBT（Soulbound Tokens）は、譲渡不可能なNFTのことです。NFTは通常、誰でも売買や譲渡ができるのが特徴的ですが、**SBTは一度取得すると、そのトークンはウォレットに結びつけられ、別のウォレットに移動することができません**。

この特徴を活用することで、個人のアイデンティティ、評判などをブロックチェーン上で安全かつ不変的に管理することができるようになりました。例えば、学歴情報や職務経歴、資格情報やパスポートなど、個人のデータや信用履歴、実績を証明する手段としての活用に注目されています。また、過去の診療記録や医療記録をデータとして残すことで、医療分野で共通のデータを活用、応用されることも期待されています。

SBTの代表的な事例として、POAP（Proof of Attendance Protocol）があります。POAPはイベント参加証明として機能し、個人の活動履歴を示すデジタルバッジとして利用されています。

■ SBTとNFTの比較表

| | 正式名称 | 特徴 | 譲渡 | 非代替性 | ユースケース |
|---|---|---|---|---|---|
| SBT | SoulBound Token | 個人活動・履歴の証明 | × | ○ | 学歴・資格証明、イベント参加証明など |
| NFT | Non-Fungible Token | 所有権・希少性の証明 | ○ | ○ | アート、ゲームアイテム |

## NFTfi (NFT Finance)

NFTfi（NFT Finance）は、NFTを金融資産として活用する新しい分野です。これまでNFTはアートやデジタルコレクティブルとしての活用が中心でしたが、NFTfiは担保、融資、複数人で分割して所有するフラクショナル・オーナーシップなど、金融的なユースケースを提供することで市場に革新をもたらしました。NFTfiでは、**NFTを担保にして暗号資産を借りたり、NFTの収益を増やしたりする運用が可能**になります。

NFTfiの仕組みは、ユーザーがNFTを担保として預け、その担保価値に基づいてETHやDAIなどの暗号資産を借りるというものです。返済が滞った場合には、担保となったNFTが貸し手に移転されることでリスク管理が行われています。これにより、NFT所有者は売却することなく流動性を得られるようになります。

代表的なNFTfiプラットフォームには、NFTfi.comやBendDAOがあります。特に、CryptoPunksやBored Ape Yacht Club（BAYC）のような高額なNFTを担保にして融資を受けるケースがあります。また、貸し手側は短期間で高利回りを得られるため、投資の新たな選択肢としても注目されています。

## ERC-1155

ERC-1155は、FT（代替可能トークン）とNFT（代替不可能トークン）の両方を1つのスマートコントラクトで同時に管理・発行することができるイーサリアム上のトークン規格のことです。これまで紹介したTether(USDT)やUSD Coin(USDC)などのステーブルコイン、Uniswapが発行するUNIトークンなどは、ERC-20規格で発行されたFT（代替可能トークン）に該当します。CryptoKittiesやCryptoPunksに代表されるNFTもERC-721規格で発行されたNFT（代替不可能トークン）がよく使われています。これらの両方の特徴を兼ね備えたのがERC-1155規格になります。

# 56 ステーブルコイン

**価格の変動が激しい暗号資産は、日常生活における決済などの特定の用途には向かないとされています。そこで、価値を安定させたステーブルコインが開発されました。ステーブルコインの種類や仕組みについて解説します。**

## ステーブルコインとは

ステーブルコインとは、**価格が安定的な暗号資産**のことです。従来の暗号資産は価格の変動率（ボラティリティ）が円やドルといった法定通貨に比べて極めて大きく、利用用途が限られてしまうというデメリットがあります。例えば、ビットコインを日々の決済に利用した場合、買い手が時価で支払いを行ったとしても、売り手側で1日後に10%価値が下がってしまうのでは、決済通貨として機能しません。そこで価格が法定通貨などに連動（peg）するステーブルコインが開発されました。

## ステーブルコインの種類

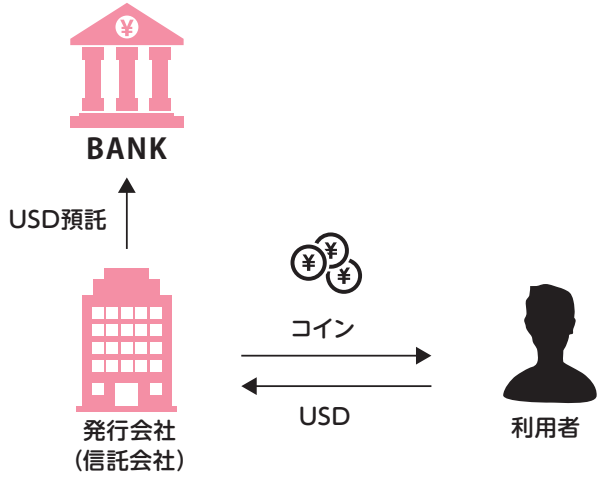
- **法定通貨担保型**

最も主要なステーブルコインが法定通貨担保型です。これは、銀行・信託会社に保管される法定通貨を担保として、ブロックチェーン上でステーブルコインを発行します。ユーザーは、発行したいステーブルコインと同額の法定通貨を発行会社に預けますが、これは準備金として銀行・信託会社に保管されます。ユーザーはコインを返却することで、いつでもその資金を引き出すことができます。供給するステーブルコインと同額の資金が保管されており、いつでも交換できることを発行企業が約束しているため、価格が安定します。この方法は、担保がブロックチェーンの外で保管されているため、**オフチェーン型**とも呼ばれます。



法定通貨担保型のステーブルコインを発行する会社は、定期的に監査法人の監査を受け、発行済みコイン以上の額の顧客預かり資産を持つことを証明する必要があります。また、多くの発行会社は、信託会社・信託銀行を利用して顧客預かり資産の分別管理を行うことで、資産管理の透明性を向上させています。

■法定通貨担保型のステーブルコイン




法定通貨担保型を採用する主要なステーブルコインとして、USDT（Tether）、USDC、BUSD（Binance USD）、TUSDなどがあります。

- **暗号資産（仮想通貨）担保型**

暗号資産（仮想通貨）担保型は、ブロックチェーン上にデポジット（預託）された暗号資産を担保としてステーブルコインを発行します。主にDAIという通貨が該当しますが、ユーザーはイーサリアム上のスマートコントラクトにEther（正確にはERC20に変換したPETH）を担保として預託し、DAIという1ドルに固定されたステーブルコインを受け取ります。このブロックチェーン上に預託されたEtherは、いつでも払い戻すことができます。また、預託する担保額は発行するステーブルコイン額の1.5倍以上を差し出すことになっています。これは、Etherの価格が急落した場合でも、担保額がステーブルコインの発行額を下回らないようにするためです。