

BTCC

新規口座開設限定

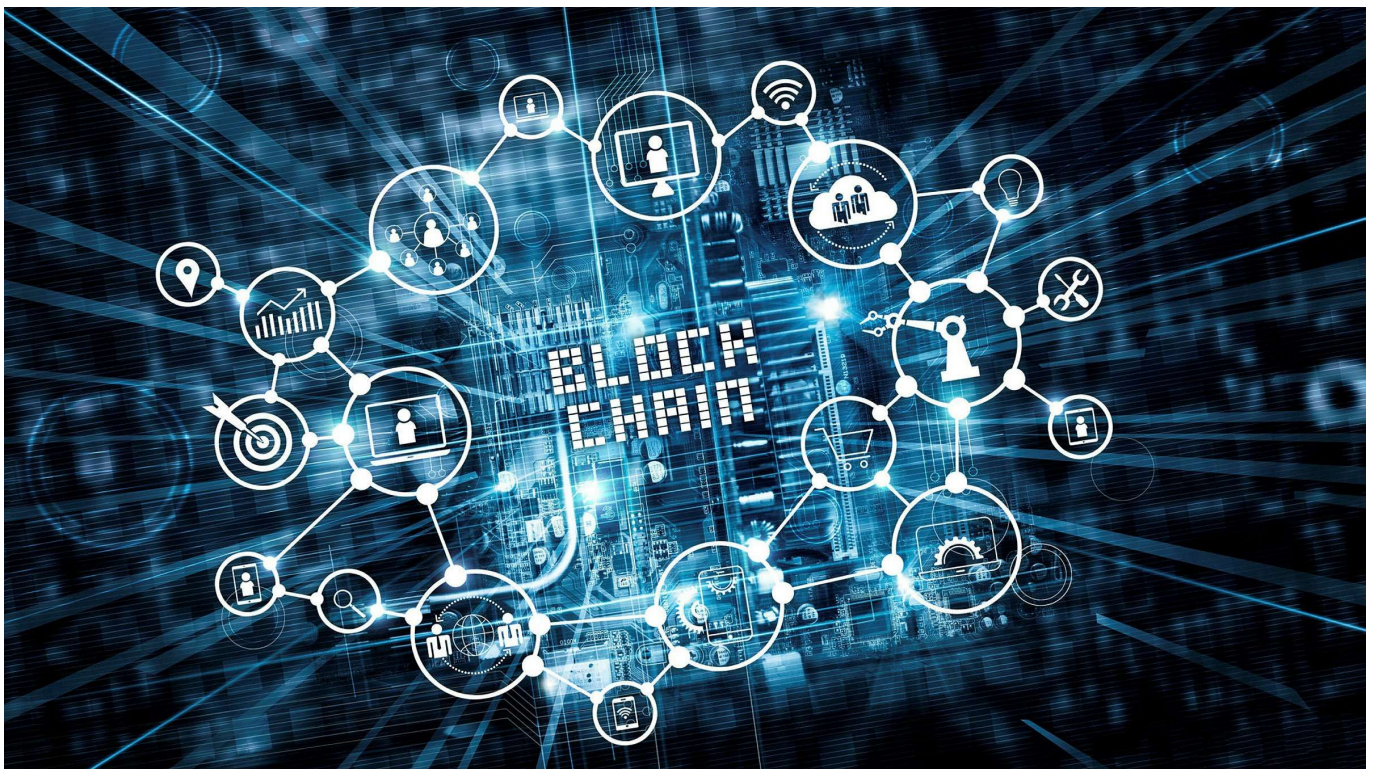
BTCC口座開設&入金で、最大**17500USDT**が獲得できる。
お友達を紹介するとさらにボーナスをプレゼント!

今すぐ口座開設/詳細はこちら

ブロックチェーンとは？ 技術の仕組みを分かりやすく解説

原文:

<https://www.btcc.com/ja-JP/academy/crypto-basics/blockchain>



ブロックチェーンとは、単一の管理者ではなく、地理的に分散した複数の**コンピューター**がデータを分散管理する新しいデータベースだ。公開鍵暗号技術で取引の安全性を保ち、一部のサーバーが攻撃を受けたとしても動き続け、さらに改ざんが不可能なシステムになっている。

ブロックチェーンの登場は**暗号資産（仮想通貨）ビットコイン（BTC）**とともに始まった。未だ正体不明の「サトシ・ナカモト」なる人物が2008年10月にメーリングリストで「Bitcoin: A Peer-to-Peer Electronic Cash System」という論文を発表し、P2P（Peer-to-Peer）による新しい電子通貨システムの仕組みを提案した。

関連: [BTCCでビットコイン（BTC）先物取引のやり方【初心者向け】](#)

ブロックチェーンの仕組み・技術

ポイント

- [1. P2Pの分散型取引システム](#)
- [2. 改ざんできない仕組み](#)
- [3. ブロックチェーンを支えるその他の技術](#)

1. P2Pの分散型取引システム

ブロックチェーンの肝は、P2Pの分散型の取引システムにある。従来の取引システムは、クライアント・サーバー型と呼ばれ、取引を行うクライアントと取引を管理するサーバーの役割は区分される。これに対し、P2P型では、ピア（Peer）と呼ばれるシステムの参加者はクライアントとサーバーの役割の両方を担う。取引の承認やシステムのアップデートも、中央により決められるのではなく、多数のピアの同意が必要になる。

2. 改ざんできない仕組み

ブロックチェーンを使ったネットワークでは、ピア同士でトランザクション（取引）が行われると、その取引履歴を含んだ一定量のデータの塊「ブロック」が、時系列で連なった既存のブロックに追加される。各ブロックには、「取引データ」「前のブロックのハッシュ値」「ナンス」が含まれる。このハッシュ値は、ブロックの内容をコンパクトに表した数値で、ハッシュ関数というアルゴリズムによって算出される。取引データの内容が変われば、このハッシュ値も変わる。もしある過去の時点の取引データを改ざんしようとするれば、そのブロックのハッシュ値に加え、後続のブロックに含まれる全てのハッシュ値も変えないと整合性を保てなくなるため、改ざんが不可能な仕組みとなっている。

3. ブロックチェーンを支えるその他の技術

新しいブロックを追加するには、システムの管理者全員（マイナー）がブロックの取引に間違いがないことを確認し、合意する必要がある。合意形成する方法（コンセンサスアルゴリズム）はブロックチェーンごとに異なるが、[ビットコイン](#)では「プルーフオブワーク（PoW）」が採用されている。PoWは仕事量による証明という意味で、マイナーはブロックに含めるナンスを膨大な計算によって求める必要がある。この他にもブロックチェーンでは、デジタル署名や公開鍵暗号などの技術を使い、システムの安全性を保っている。

【関連記事】

[DeFi（分散型金融）とは？ DeFiを徹底解説](#)

[イーサリアム\(ETH\)とは？ 基本事項や特徴をわかりやすく解説](#)

[ドージコイン（DOGE）とは？ 基本事項をわかりやすく解説](#)