ブロックチェーンとは

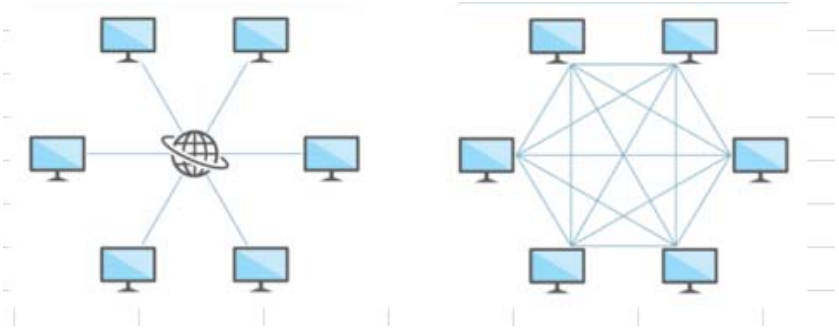
2024.01.24

ブロックチェーンとは、一言でいうとネットワーク上にある参加者の端末同士をダイレクトに接続し、暗号技術を用いて取引の記録を分散的に処理・記録する保存技術の一種です。
ブロックと呼ばれる単位でデータを記録し、それを鎖（チェーン）のように連結して、参加者全員でデータを管理する技術、仕組みを指します。今回は**インターネット以来の革新的技術**と言われているこの技術の仕組みを中心にレポートしてみたいと思います。

【センター型保存システムと分散型保存システム】

まず最初に、ブロックチェーンのデータ保存方法がこれまでのセンター型保存方法とシステム的にどう違うのか説明しておきます。
簡単に言うと、下図に示すようにデータがセンターに集中して保存されているか、それとも各端末に分散して保存されているかの違いです。
この違いによって、分散型には ①センターがなくても構築できる ②障害に対して耐性（＝ロバスト性）があるなどのメリットがあり、ブロックチェーンはこの分散型のメリットを生かしたシステムと言うことができます。

センター型保存型システム　　**分散型保存システム**



https://yuyu-life.blog/investment-money/kasoutuka/blockchain/
【5分で解説】仮想通貨に使われているブロックチェーンの仕組みやメリット（yuyu-life.blog）

ブロックチェーンの応用

このような分散してデータ管理・保存する仕組みはどんなことに使われるのでしょうか。
先ほど述べたように、センター設備が不要であることから、システムが簡易になると言うメリットがあります。また、ネットワーク内のすべての端末に同じデータが保存されているために、サイバー攻撃やシステム障害に対する耐性（ロバスト性）が高いこともメリットになります。
中央の処理装置がないために、複雑な処理が必要となるシステムや大量のデータを保存しなければならないシステムには不向きですが、単にデータを正確に管理するシステムなどには向いています。この種の開発が必要となるDXの時代には、幅広い業務に使われることが想定され、特にオープンデータの管理が必要となる業務では積極的に検討すべき技術といえるでしょう。
例えば、銀行・金融サービス、不動産分野、ヘルスケア、教育、小売業、政府と公文書、政治など、あらゆる分野での応用が既に考えられており、プライスウォーターハウスクーパースなどは、ブロックチェーン技術が世界中で広く採用された場合、2030年までに世界のGDP（国内総生産）に1.76兆ドル（約186兆円）の経済効果をもたらすと予測しています。

ブロックチェーンを理解するための3つのキーワード

まず、この技術を理解するためのキーワードを列挙します。

① **記録データ**＝取引情報（トランザクションデータ）
② ハッシュ関数、**ハッシュ（値）**＝ハッシュ関数から得られる戻り値
③ 採掘難易度　ハッシュ（値）に課す条件（ex.先頭の6桁が0など）
④ **ナンス（値）**（Number Used Once）データに追加しハッシュ値を調整する数字
⑤ タイムスタンプ　新しいブロックが作られた時間

このキーワードのうち、**ブロックチェーン技術のコア**になるものは、**記録データ、ハッシュ（値）、ナンス（値）**の3つです。
このキーワードを使って、仕組みを説明していきますが、説明の範囲を広げると煩雑になり、見通しが悪くなるため、基本となるメインストリームの話に限り、合意形成のプロセス、例外処理の説明などは省きます。

ブロックチェーンの構造

https://thinkit.co.jp/article/21858
ブロックチェーン(2)ブロックチェーンの構造と仕組み(マイニング・PoW)｜Think IT（シンクイット）

次にブロックチェーンの基本となるブロックの構成を調べてみます。この構成は次図の説明図を見ると分かる通り

① **ブロックデータはヘッダ+取引情報**で構成される。
② ヘッダは**前のブロックのヘッダのハッシュ値+タイムスタンプ+採掘難易度+ナンス+今回の取引の情報のハッシュ値**で構成される。
③ ブロックチェーンはこのブロックをつなぐことで構成される。

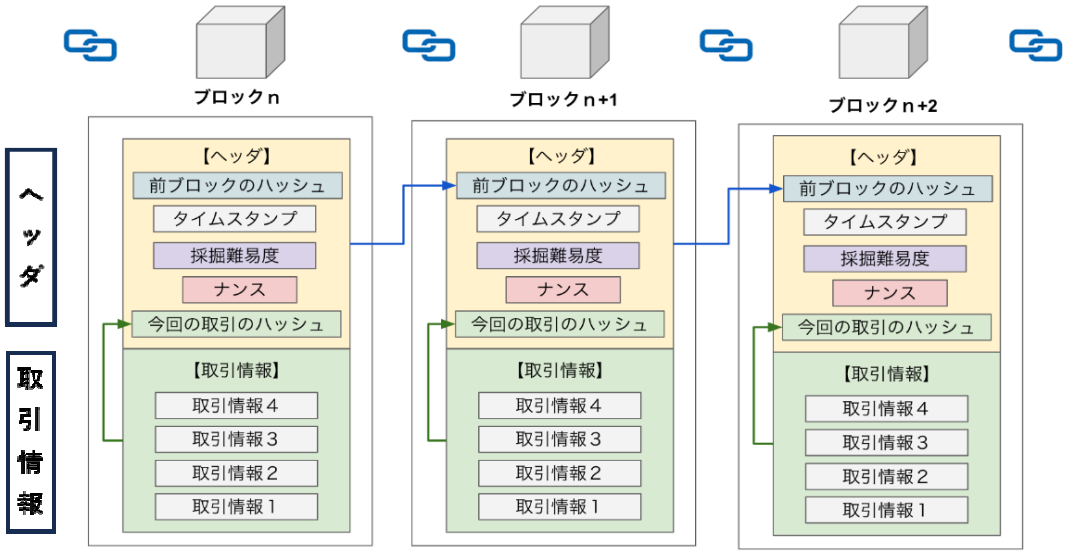
となっています。ここで説明では取引情報となってますが、単にデータと考えれば結構です。
ブロックの構成が分かったところで、次に個々の言葉の意味を説明しながら解説します。

【ハッシュ関数とは】
ハッシュ関数とは、任意のデータから規則性のない固定長のビット列を生成する関数です。
その特徴は以下の4つです。この特徴がブロックチェーン技術のキーとなります。

① １ビットでもデータが異なると全く異なるハッシュ値を生成する⇒**改竄が分かる。**
② 入力するデータの大きさにかかわらず一定の長さのハッシュ値を生成する⇒**比較が簡単。**
③ 狙ったハッシュ値を生成することは非常に困難⇒**データの改竄は事実上不可能。**
④ ハッシュ値から元のデータを推測することは非常に困難⇒**データの改竄は事実上不可能。**

非常に困難と言う表現はあいまいですが、原理的に不可能ではないものの、実行には膨大な時間が必要となるため事実上できないと言う意味だと考えればよいと思います。

【ブロックチェーン説明図】



ブロックを生成し、つないでいくルール

次にブロックを生成し、これをつなぐルールですが、上の図に沿って説明を加えると以下のようになります。ただし、この手順はどのシステムでも同じと言う訳ではなく、システム毎に異なります。ただし、コアとなる部分は同じなのでこの流れを理解すればルールについては十分です。

① **前のブロックのヘッダ**（その前のブロックのハッシュ～前回の取引のハッシュまで）**のハッシュ値を得る。⇒前のデータの正統性を引き継ぎ、改竄を防ぐ。**
この時のハッシュ（値）は採掘難易度の条件(ex.先頭の6桁が0など)を満たす必要がある。
⇒**新たなブロックの追加が簡単にできないための条件。**
② 新たに追加する取引情報をまとめて【取引情報】＝追加データを作成する。
③ その取引データのハッシュ（値）を計算する。
④ 得られたそれらのデータをまとめて、**今回のブロックのヘッダを作成する。**
⑤ **ヘッダに追加した取引情報を加え、今回追加するブロックとする。**
⑥ **このブロックが正しいと承認されると、新たなブロックをすべての端末が追加する。**

採掘難易度とは、例えばハッシュ値の最初6桁が0であるというような条件のことを言います。狙ったハッシュ値を生成することは非常に難しいため、ナンス値を変えながら、虱潰しの計算（ハッシュ関数の引数）を条件に合うまで繰り返し続けることになります。
新たなブロックの追加でも手間がかかるわけですから、途中のブロックのデータを悪意を持って改竄しようとしても、前後のブロック全てを修正しなければならず、実際にはに不可能ということになり、データのセキュリティが守られます。
なお、ここではデータ承認のプロセスについては説明を省きました。

【ブロックチェーンについて識者に質問をしました。以下がその回答です。】

① 誰がどのタイミングでブロックを追加するのか不明？？ ⇒**基本的に新しいデータを追加する時る人が先着順で追加する。**
② データの暗号キーは誰が管理するのか？⇒**管理する人はいない。ブロックを作成する人が公開鍵で暗号化し、秘密鍵で電子署名する。**
③ ブロックの発行の順序はコントロールされるのか？⇒**コントロールはしない。⇒早い者勝**

ち。発行されたデータが正しいと皆が認めれば承認される。

今までの議論とは趣が変わるが、取引所の様な所が介在し、デジタル通貨を購入するような場合には、様子が変わる。一般の人はこれまでのブロックチェーンを作る作業には関与しない。単に取引所にデジタル通貨の購入・販売を依頼するだけである。

ブロックチェーンのセキュリティ確保の仕組み

ブロックチェーンのセキュリティがどう確保されるのか、ここまでの説明をまとめてみます。

① ブロックチェーンのデータは分散されて記録されるので、システム障害に強い。

② ブロックチェーンのデータはハッシュ値も保存されているので、改竄ができない。

また分散型データベースの特徴として、管理者不要の仕組みとなり、参加者の公平性が担保されるという特徴もあります。これは**DAO**（分散型自律組織）と言われ、新しいネットワーク上の組織形態として注目されていますが、これは同時に技術面だけでなく、社会的な組織形態としても盛んに議論されています。

ブロックチェーン作成を疑似体験してみる。

これまでの説明でブロックチェーンの仕組みはお分かり頂けたと思いますが、こんな簡単な仕組みで本当にセキュリティは大丈夫かと思われるのではないでしょうか。

そこで、実際にブロックデータを作成し、新たなブロックを作る事さえ大変だと言うことを体験してみましょう。

実際のブロックチェーンで使われている桁数の大きいハッシュ関数を使うと面倒な取扱になるので、最も簡単なハッシュ関数を使い、雰囲気だけでも感じていただきます。ハッシュ関数は以下のサイトにあるものを使用します。

https://coding.tools/jp/md5　　**：オンラインハッシュ関数**

直前のハッシュ値＝0577273FF885C3F84DADB8578BB41399

とし、今回付け加えるトランザクションデータを**6789**とします。ここで上記のハッシュ関数を使って、ハッシュ値の**先頭が0に成る様なナンス値を探します。**

ハッシュ値を計算するデータ　0577273FF885C3F84DADB8578BB41399+**6789**+**ナンス値？**

虱潰しの試行錯誤の結果、68回目にナンス値＝69で先頭が0になりました。(たまたまです。)

0577273FF885C3F84DADB8578BB41399(+)6789(+)69　これをハッシュ関数に入力します。

返ってきた戻り値は（ハッシュ値）＝　**0**9B0974B044E897B158CE5F2BCA3EF0C　です。

ハッシュ値の先頭が0 、 1桁の場合でも結構な回数試行をしますので、実際のブロックチェーンのように、0が6桁程度並ぶという規則になるとナンス値の探索は更に困難になります。虱潰しの演算が必要で時間もかかり、だれでも簡単にブロックを追加できると言う訳にはいきません。

【まとめ】

ともあれ、このように比較的簡単な仕組みでブロックチェーンは作られており、従ってそのシステムの簡便さ、サイバー上の脅威や障害に対するロバスト性とあいまって、今後広く利用される事が期待されています。今後ともDXを進める上で中心になる技術である事は間違いないでしょう。

以上