

## 日税メールステーション 特別号

### 税理士が知っておくべき IT 知識～基本の"き"～

#### 第 21 回 ブロックチェーン

メールマガジンをお読みの皆様こんにちは、株式会社コアブリッジの柳です。

暗号資産(仮想通貨)やフィンテック(Finance Technology)等の話とともに『ブロックチェーン(Blockchain)』という言葉をよく聞くようになりました。

今回はこのブロックチェーンを取り上げます。

#### ■概要：ブロックチェーンとは何物？

「インターネット以来の発明・技術革新」との呼び声も高いブロックチェーンは、『情報の塊をつないだもの』という意味合いで、『分散型台帳(技術)』と書き表されることもあります。仮想通貨ビットコインを実現するために「サトシ・ナカモト(Satoshi Nakamoto)」と名乗る人物(正体不明)が 2008 年に発明したとされます。

情報の塊を数珠繋ぎにして保持し、それらが常に正しいものであること(改ざんされていないこと)を運営者全員で確認していく、という仕組みです。

偽造防止や真正性証明に有効なため、ビットコイン以外にも著作権管理などにも使われ、サプライチェーンの製品管理にも応用されています。

もう少しイメージしやすいように例示してみます。

#### ■ブロックチェーンのイメージ

銀行の入出金処理をブロックチェーンで管理しているとしましょう。

- 1) 入出金を記録する用紙(1枚に50件分記録できるとする)がある
- 2) 「AさんがBさんに1万円振り込んだ」「Bさんが口座から5千円引き出した」「C社がD社に100万円振り込んだ」「E社が銀行から1千万円融資を受けた」・・・という取引を記録用紙に書き込んでいく
- 3) 取引を50件分書き込んだら、その記録用紙を提出して入出金処理を申請する
- 4) 台帳ファイル(記録用紙を束ねたもの)の所持者は、特殊なクリップを作成して、提出された記録用紙を台帳ファイルの最後に綴じ込む

- 5) その際に台帳ファイル関係者に誤りや不備がないか確認してもらう (OK が出たら綴り込み完了)
- 6) 登録用紙に書かれている 50 件分の入出金処理がまとめて実行される
- 7) 紛失や不正な書き換えに備えて、常に複数人 (5 の台帳ファイル関係者) で同じ台帳ファイルを複製して保管しておく

という感じです。

3 の 50 件分書き込まれた記録用紙がブロックで、5 で 1 枚追加されたことでチェーンが伸びていきます。ブロックチェーンでは、記録用紙 (ブロック) が一本の鎖でつながれていて枝分かれすることはなく、順番や内容は一切変更できません。

4 の「特殊なクリップ(※1)」というところや、7 の「台帳は複数人で同じものを保管しておく」というところがブロックチェーンの特徴です。

※1：特殊なクリップは「ハッシュ(Hash)」という技術を使って作られます。詳細説明は割愛しますが、ハッシュを使うと改ざんがあっても容易に判別できます。

## ■管理者がない！

ブロックチェーンの特徴の一つは、中央で管理する人がおらず、運営者全員で確認をしているということです。

IT によるサービスは、多くの場合に「サーバー(Server)」と呼ばれるコンピュータが中央集権的に処理を行なっています。日常的に使っているメールも Web ページも、メールサーバーや Web サーバーがサービスを提供してくれています。

しかしブロックチェーンの場合には、ブロックチェーンを処理するコンピューターが世界中に存在して対等につながっており(P2P: Peer-to-Peer といいます)、しかも「早い者勝ち」で処理を競っています (※2)。

上のイメージ解説のところでは煩雑になるので書きませんでした。4 で記録用紙の提出を受けると、台帳ファイルを持っている人たちは「我先に」と大急ぎで特殊なクリップを作り始めます (※2 のように作成に時間がかかります)。世界中で最初にクリップを作り上げた人だけが記録用紙を台帳ファイルに綴じる権限をもらえ、二番手以降の人は、5 番の確認作業にまわり、綴り込みが完了した後に更新された台帳ファイルのコピーをもらいます。

※2：早い者勝ち以外の方法もあるのですが、暗号資産(仮想通貨)のビットコインの場合を例にとると、競争しているのは、上述の例の 4 番の「特殊なクリップを作成」という処理です。ものすごい回数 of 試行錯誤が必要な処理で、マシンパワーを要する代わりに、一番の人には賞金(ビッ

トコインで支給される)が与えられます。これがいわゆる『マイニング(mining)』です。

7で「常に複数人で同じ台帳ファイルを複製して保管しておく」というのは、世界中のブロックチェーン処理コンピューターが同じ台帳ファイルをコピーして持っていることを意味します。中央管理者がいないため、複数人が同じものを持ち合わせ、他者と確認することで真正性を担保しています。誰かが持っている台帳ファイルの過去の取引が改ざんされても、他の人が持っている台帳ファイルと照らし合わせれば改ざんがすぐに判明します。

管理者がいない→全員が同じものを持っておく→誰かが改ざん→他の人と異なるのでバレるという図式で、これが「分散型台帳」と呼ばれる所以です。

「管理者がいなくても全員で同じものを所持してお互いに照らし合わせていけば不正はできない」というのはコロブスの卵のような発想ですね。

今号は以上です。

では、また次回お会いしましょう。

※本文中の情報、状況、数値等は執筆時点のものです

#### 執筆者

柳 恵太 (やなぎ けいた)

株式会社コアブリッジ代表取締役。

ソフトウェア開発会社、メーカー、教育ベンダーを経て、2014年に株式会社コアブリッジを設立。これまでの、システム開発の上流から下流、受託側から発注側、エンジニアからプロジェクトマネージャー、ユーザーと開発者、企画・営業・開発・提供、日本と海外、社員から経営者といった、組織における幅広い役割を活かし、主にIT企業向けの人材育成やコンサルティング等のサービスを提供している。

情報提供元：



株式会社コアブリッジ

<https://www.corebridge.co.jp/>

※本コラムは、<https://www.corebridge.co.jp/column/>でもご覧になれます。