ブロックチェイン技術の仕組みと可能性

山崎 重一郎 ●近畿大学

世界のメガバンクがR3 CEVコンソーシアムを設立。カラードコインによりビットコイン上で債券を実現。サイドチェインの生態系に期待。

■はじめに

インターネットの黎明期に「インターネットってどこの会社が運営しているの？」と尋ねられて困惑したことがある。ブロックチェイン技術は、このころのことをいろいろと思い出させる。

ブロックチェインはP2P型の分散型データベースであり、ビットコイン型仮想通貨システムの中核である。仮想通貨のソフトウェアを自分のパソコンにインストールして実行すると自動的にP2P型ネットワークに接続され、ブロックチェインのデータベースの同期が始まる。この同期が完了すると自分自身がブロックチェインのノードの一つになる。ブロックチェインとは「あちら側」にあるものではなく、コードを稼働させている自分自身がその一部なのである。

ブロックチェインは一種のタイムスタンプサービスであり、そこに登録された記録は誰にも改ざんや削除ができない非可逆的な記録になる。また、ブロックチェインを構成するP2P型の各ノードはスクリプト言語の処理系を備えており、一種の分散型計算システムとしての側面も持つ。ブロックチェインへの登録候補となるデータは、スクリプト型のプログラムになっており、各ノードはこのスクリプト言語処理系を使ってそれぞれ独立にそのデータの検証を行う。

ブロックチェイン技術は、「信頼できる記録」を構成するための技術の歴史的発明である。

現在、世界中の金融機関や金融ネットワークは、「信頼できる記録」の維持に莫大なコストを費やしている。ブロックチェイン技術はそのコストや統治の構造に大きな変革を迫る可能性がある。そのインパクトは、かつてインターネットが通信ネットワークのコストや統治の構造に与えたものに似ている。

2015年の後半、20行を超える世界のトップクラスのメガバンクがR3 CEVというブロックチェイン技術の相互利用のためのコンソーシアムを設立した。R3 CEVに加盟するメガバンクは現在も増え続けている。

このコンソーシアムの主な目的は、既存の中央集権的な統治構造を持つ高コストの国際金融ネットワークに代わって、ブロックチェインというより低コストで民主的な銀行間取引の「信頼できる記録」の再構築であろう。

■ビットコイン型仮想通貨技術

●ビットコインにはコインは存在しない

「ビットコイン」という名称から、ビットコインは「ビットでできたコイン」だと想像する人が多いだろう。しかし、実際にはビットコインにはコインにあたるものは存在しない。ではビットコインとは何かというと、「できごと」の非可逆的

な記録である。

電子マネーの課題の一つは、一度決済に使用した貨幣的価値を二重に使用できてしまうという二重使用の問題である。ビットコインでは、送金という「できごと」の記録を参加者全員が検証することによって二重使用の問題を解決している。そして、この「できごと」の非可逆的な記録を実現するのがブロックチェインである。

●ブロックチェインとは

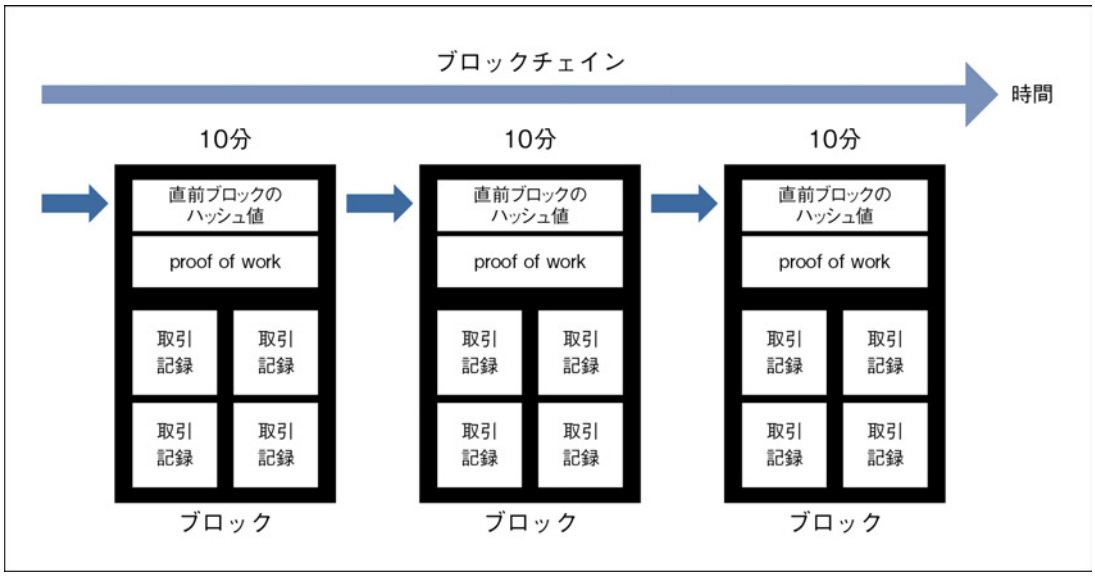
ブロックチェインとは、ブロックというデータ構造を時系列で鎖のように接続したものである（資料4-3-6）。ブロックは一定時間ごとに新たなものが生成され、ブロックチェインに接続される。ビットコインでは平均10分でこれが繰り返されている。また各ブロックには、それが生成されるまでの一定時間に発生した取引記録という「できごと」が内包されている。

ブロックチェインは、基本的に時間を意味している。新しいブロックが生成されブロックチェインに接続されることは、時間が推移したことを意味する。「できごと」の記録がブロックの中に取り込まれることは、その取引記録にタイムスタンプを付与したことに相当する。

ブロックの中には、それぞれ「プルーフ・オブ・ワーク」と呼ばれる値が含まれている。これはその名のとおり「莫大な計算をした証拠」であり、この値は実際に消費電力が問題になるほどの莫大な計算をしなければ決して得ることができない。

また各ブロックは、それぞれ直前のブロックから一定の計算で算出された値である「ハッシュ値」を含んでいる。このハッシュ値とは、計算の元になるデータが1ビットでも変更されると、計算の結果は全く異なる値になるというものである。

資料4-3-6　ブロックチェイン



出典：著者作成

もしブロックチェインの中の過去のブロックを改変すると、それに後続するすべてのブロックのハッシュ値も連鎖的に変わってしまうため、後続するブロックのすべてのプルーフ・オブ・ワークも再計算しなければならなくなる。

●マイニングのインセンティブ

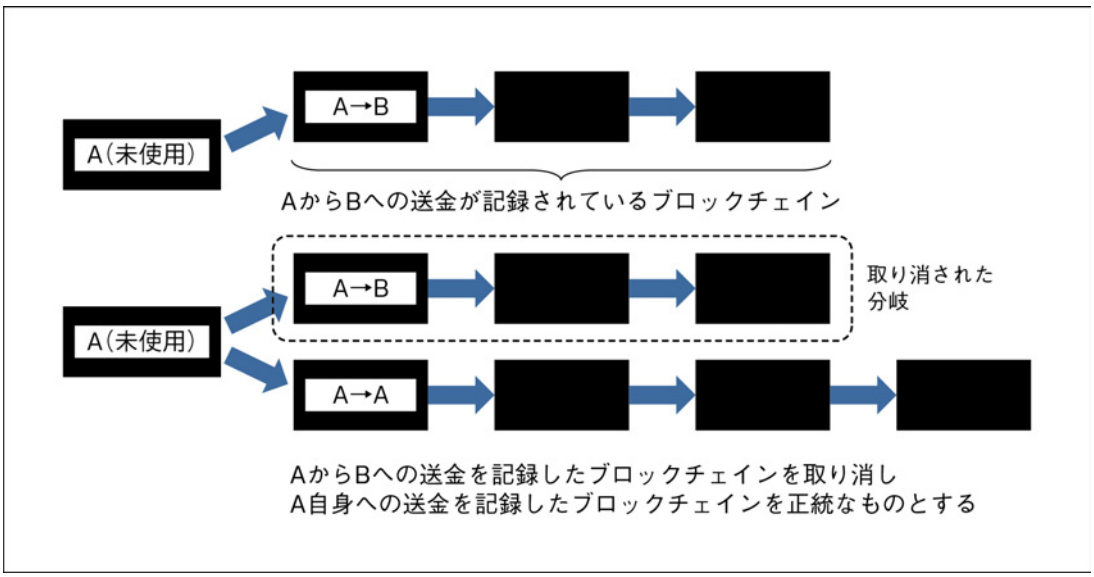
「信頼できる記録」を作る一般的な方法は、銀行や政府のような「信頼できる第三者」を利用する方法だが、ビットコインの発明者であるサトシ・ナカモトは、その論文の中で、ビットコインの目的は「信頼できる第三者」が不要な決済システムを提案することであると述べている。

ビットコインのプルーフ・オブ・ワークは、それを最初に発見した者に通貨発行益を与えるというインセンティブにより、ゴールドラッシュにも似た計算競争状態を人工的に作り出している。この計算競争は、金の採掘になぞらえて「採掘（マイニング）」と呼ばれ、計算競争への参加者は「採掘者（マイナー）」と呼ばれている。

「採掘」による計算競争の勝利者は、新しいブロックを作成して既存のブロックチェインに接続する権利を得る。そしてこの新しいブロックの中に自分宛ての送金となる「コインベース」と呼ばれる取引記録を含めることが許される。採掘者の目的はこれであり、計算競争のインセンティブである。

もし、プルーフ・オブ・ワークが誰でも簡単に発見でき、過去のブロックを容易に取り消すことができ、「新しい時系列の歴史」を作ることができるという前提の下で、P2P型分散データベースの一貫性を維持しようとすると、たちまち難しい問題に直面する。

資料4-3-7 「新しい時系列の歴史」を作成した例



出典：著者作成

たとえば、巧妙に結託している複数のノードたちが、ある標的ノードに対して、過去の取引記録をブロックごと取り消して、すでに使用済の貨幣的価値を二重に使用する不正な取引記録を含む一連のブロック群を送りつけたとする。その標的ノードは、正しいブロック群も受け取っていたとしても、いずれの取引記録の検証も成功するので、どちらの時系列が正しいものなのか判断することができない（資料4-3-7）。

また、通信する相手によって巧妙に送信する内容を変えることによって、本当は正しいノードを不正なノードに仕立てあげることも可能なので、誰が本当に不正なノードなのかということもわからなくできる。このような「巧妙な裏切り者」が存在する分散システム上での合意形成の方法は、「ビザンティン将軍問題」と呼ばれる難問として知られている。

●アイデンティティと電子署名

ビットコインは、公開鍵暗号による電子署名を利用した転々流通型の電子送金システムである。

電子署名を正しく検証するためには、単に各当事者が自分の公開鍵と秘密鍵を持っているだけでは不足であり、公開鍵と署名者のアイデンティティ（＝識別名）を確実に結びつける方法が必須である。

ビットコインでは、ビットコインアドレスをアイデンティティとして用いている。ビットコインアドレスは、本人の公開鍵から作られる一見ランダムな文字列である。公開鍵とビットコインアドレスは計算式によって1対1に結びついているため、公開鍵を使えば、ビットコインアドレスと電子署名が秘密鍵を持っている送金者本人のものであることを確かめることができる。

■仮想通貨の原理

●時制式三式簿記構造

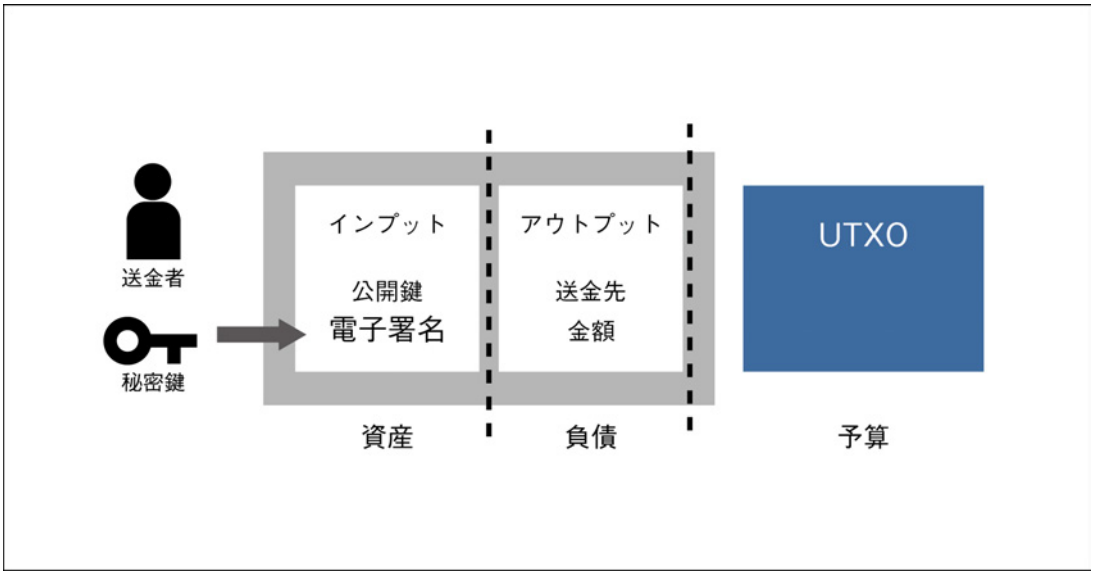
仮想通貨の取引記録は、インプットとアウトプットの2つの要素で構成されている。これにUTXO（unused transaction output）を加えた3要素を、それぞれ資産、負債、予算とみなすことができる。この3要素のそれぞれの合計は基本的に一致する。われわれはこれを時制式三式簿記と呼んでいる（資料4-3-8）。

送金者が送金を行うときには、取引記録のインプット部分に自分の公開鍵と自分の電子署名を埋め込む。アウトプット部分には送金先の公開鍵のハッシュ値と金額が記載される。ただしコインベースにはインプットが存在しない。

取引記録には、複数のインプットを持つものや複数のアウトプットを持つものもある。その場合でも、インプットに含まれる金額の総量とアウトプットの金額の総量は一致しており、アウトプットの総量とUTXOの総量も一致する。

議論の単純化のためにここでは説明しないが、正確には「取引手数料」という採掘者への報酬のための会計要素が存在するため、インプットの総額とアウトプットの総額は完全には一致しない。

資料4-3-8　時制式三式簿記



出典：著者作成

●分散型計算システムとしてのブロックチェイン

ブロックチェインの各ノードには、スクリプト言語処理系が備わっており、これを使って各ノードで取引記録の検証処理を行っている。つまり、ブロックチェインは一つの分散型計算システムとしての側面を持っている。

Ethereumは、ブロックチェインの分散型計算システムとしての機能を強化し、電子契約などのプラットフォームとなることに主眼をおいた仮想通貨システムである。

●採掘者は通貨発行者ではない

ビットコインの採掘者は通貨発行権を持つと言われることがあるが、正確にはそうではない。採掘者はそのコインベースのUTXOを受領する権利を持っているだけである。コインベースにはインプットが存在せず、送金者やその電子署名も存在しない。

つまりビットコインには「債務者」が存在しないことに注意が必要である。ビットコイン自体は債券ではない。解釈によって債券として扱おうとしても、送金者の電子署名の責務はそれ以前の所有者に連鎖的に還元されて、最終的に「無」に至る。そのため、債権債務関係を構成することができないのである。

●カラードコインによる債券の構成

カラードコインは、ビットコインのブロックチェイン上に様々なアセット（流動資産）を構成可能にする技術である。オープン・アセット・プロトコルは、カラードコインを実現する技術の代表である。

2015年5月にNASDAQは、非上場の株式市場にオープン・アセット・プロトコルを採用すると発表した。

オープン・アセット・プロトコルの重要な点は、アセットに発行者が存在することである。これによって債権債務関係を構成することが可能になる。さらにアセット発行者は、そのアセットに関する約款などのメタ情報を定義することがで

きる。

■サイドチェインとプライベートチェイン

ビットコインが市場価値を持ち始めた時期に、「オルトコイン」と呼ばれるビットコインの亜種が次々に誕生した。その主な目的は、オルトコインの市場価格の上昇による「創業者利益」を得ることだった。しかし、ほとんどのオルトコインは、そのような夢を実現することができなかった。また、類似した技術をそれぞれ独自に開発するという、技術開発の非効率性も無視できないものとなった。

●パブリックチェインとプライベートチェイン

現時点で事実上、ブロックチェインと呼べるものはビットコインのブロックチェインだけである。したがって、これを「ザ・ブロックチェイン」と呼ぶことにする。

ビットコインは参入が自由でソフトウェアを自分のパソコンやスマートフォンなどにインストールするだけで利用できるようになる。その反対に、参入に制限をかけて許可型にしているものもある。自由に参加ができるブロックチェインを「パブリックチェイン」と、許可型のものを「プライベートチェイン」と呼ぶことにする。メガバンクの国際コンソーシアムであるR3 CEVは、銀行間のセトルメント専用のプライベートチェインを指向している。

●サイドチェイン

サイドチェインとは、ザ・ブロックチェインから分岐したブロックチェインである。サイドチェインでは独自仕様による実装が可能である。たとえば、ブロックの生成と確認のサイクルを10分ではなく5秒にすることや、プルーフ・オブ・ワーク法以外の採掘方法を採用することもできる。またサイドチェインの中で行われた取引記録をパブリックにしなくてもよいし、サイドチェインで流通するものもビットコインとは別のアセットでもよい。

●1ウェイペグ型サイドチェイン

サイドチェインの利点は、ザ・ブロックチェインと連携できることである。その方法の一つがペグ付きサイドチェインである。

ペグ付きサイドチェインの代表は「カウンターパーティ」である。カウンターパーティは、ビットコイン2.0と呼ばれるものの一つであり、ザ・ブロックチェインのUTXOに対して、それを「消滅させた証拠」をもとにサイドチェイン側にコインベースを登場させるという方法である。「消滅させた証拠」のことをProof of burnと呼ぶ。

このサイドチェイン側のコインベースにはインプットが存在するため、オープン・アセット・プロトコルと同様に発行者や約款などのメタ情報を付与することも可能である。

●2ウェイペグ型サイドチェイン

サイドチェインに移転したザ・ブロックチェインのUTXOを、一定のロック期間を経た後に再びザ・ブロックチェインに復帰させる技術が、2ウェイペグ型サイドチェインである。このような技術が実現できれば、サイドチェインは、本当の意味でザ・ブロックチェインの拡張になる。また、ザ・ブロックチェインに復帰するときにサイドチェインでの取引記録が検証されるため、サイドチェインの内容も「信頼できる記録」になる。

ビットコインのザ・ブロックチェインの経済規模はまだ数千億円でしかないが、現時点では唯一と言ってよいパブリックチェインである。R3 CEVが実現すれば、その経済規模はビットコイ

ン経済よりも遥かに巨大になるだろうが、プライベートチェインであるという限界を持つ。

２ウェイペグ型サイドチェイン技術は、ザ・ブロックチェインと様々な機能や特性を備えたサイドチェインやプライベートチェインとの相互接続を可能にする。そしてこういったブロックチェインの相互接続が、さらに生態系として発展することも期待できる。

■まとめ

ブロックチェイン技術は「信頼できる記録」という社会基盤のための歴史を画する発明である。これまで中央集権的体制の中に埋め込まれ、支配されていた高コストの「信頼できる記録」を、従来とは異なるコストや統治の構造で浮上させる可能性を持つ技術だと言ってよいだろう。

一方でブロックチェインはまだ未熟な技術である。金融、契約、投票、行政記録など、ブロックチェインの利用が期待されている領域は広がりを見せている。適用領域ごとに必要となる要件を整理し、本質を違えない姿で洗練させていくことが必要であろう。

R3 CEVのような「プライベートなブロックチェイン」という概念の登場によって「ブロックチェインとは何か」という定義に混乱が見られる。インターネットがTCP/IPという通信方式を指すのではないのと同様に、ブロックチェインもP2P型の分散データベースや分散型計算システムやタイムスタンプサービスなどの機能面のみで定義しようとすると本質を見誤る。ブロックチェインの正確な定義のためにはさらに、今後のブロックチェインの生態系や関連技術の発展を見ながら議論を深める必要があるだろう。

インターネット白書 ARCHIVES

1996,1997,1998,1999,2000....

［インターネット白書ARCHIVES］ご利用上の注意

このファイルは、株式会社インプレスR&Dが1996年～2016年までに発行したインターネットの年鑑『インターネット白書』の誌面をPDF化し、「インターネット白書ARCHIVES」として以下のウェブサイトで公開しているものです。

http://IWParchives.jp/

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、データ、URL、名称など）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真・図の作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は掲載されていない場合があります。
- このファイルの内容を改変したり、商用目的として再利用したりすることはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用される際は、出典として媒体名および年号、該当ページ番号、発行元（株式会社インプレスR&D）などの情報をご明記ください。
- オリジナルの発行時点では、株式会社インプレスR&D（初期は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

お問い合わせ先　株式会社インプレスR&D　✉ iwp-info@impress.co.jp