ご存知ですか？

このコーナーでは、NTTグループ会社の新技術、新サービスや最近の話題及び新社会用語などを説明しています。最近話題の仮想通貨で多額の通貨流出などが発生し社会問題となっています。今回は、どうも良く分からない仮想通貨とブロックチェーンを分かり易く解説します。

「仮想通貨」とそれを実現する技術「ブロックチェーン」

NTTサービスエボリューション研究所
主任研究員（博士）中平　篤
株式会社情報通信総合研究所
主任研究員　滝田　辰夫

仮想通貨の衝撃

2018年1月、仮想通貨の一種である「NEM」の不正流出の疑いがあるとして、仮想通貨取引所コインチェックが金融庁に報告したと報道されました。コインチェックはTVCM等広告も相当数打っており、仮想通貨取引所[a]の中では大手とみなされていました。その後の報道で、対象の仮想通貨の流出規模は5億NEM以上、時価総額は日本円にして約580億円に上ることが判明しました。

同年2月になると、やはり仮想通貨取引所のZaif（ザイフ）において、仮想通貨ビットコインがゼロ円で取引可能な状態となり、20億ビットコイン（約2,200兆円相当）の取引が仮想通貨取引所のシステムに反映されてしまったことも報道されました。

これらの報道により、仮想通貨は一気に耳目を集めることになりました。しかし、仮想通貨というものは、なんだかわかったような、わからないような気がします。そもそも仮想通貨とは何なのでしょうか？

仮想通貨とは

日本においては、「資金決済に関する法律（資金決済法）」の第2条5項に仮想通貨が2種類定義されています。一つ目（一号通貨）は、有名なビットコインのように、不特定多数の人（誰でも）が、モノやサービスの売買に使用可能で、電子的に移転可能なもの、というように規定されています。法定通貨とそれが電子化されたものは含まない、ともされています。二つ目（二号通貨）は、（直接モノやサービスの売買に使用できなくても）不特定多数の人が一号通貨と交換でき、電子的に移転可能なもの、となっています。

同じように電子的に移転できるものとして、電子マネーというものがあります。電子マネーも名前の通り、誰でもモノやサービスの対価として使用できますし、電子的に移転ができます。違いとしては、現在の電子マネーは、国が発行する法定通貨である「円」を電子化したものとなります。つまり「円」が（たまたま）電子化して使いやすくなったもの、ということができます。一方、仮想通貨は「円」自体ではありませんし、そもそも発行主体が国ではありません。極論すれば誰でもが発行可能なものになりますが、法定通貨の裏付けはありません。この点が大きく異なるところです。

仮想通貨も、円やドルとの交換が可能となる仕組みがあります。その一つが先の報道にも出てきた「仮想通貨取引所」ということになります。バーチャルな仮想通貨と、円やドルといったリアルな法定通貨の交換所、ということになります。ただし、1円が1ビットコインといった、一対一の関係ではなく、時価での交換ということになります。こうしてみると、仮想通貨の利用者からは、仮想通貨の売買は、外貨の売買と似ているように見えるかもしれません。

こうした仮想通貨は、ビットコインやNEMの他にも多

a 一般的に「仮想通貨取引所」と呼ばれていますが、取引を媒介するだけではなく、仮想通貨を販売している業者も多く、資金決済法上はいずれも「仮想通貨交換業者」とされています

数存在しています。多くの仮想通貨の時価総額をとりまとめるサイト、「Cryptocurrency Market Capitalizations」では、1,500以上の仮想通貨が取り上げられています。

ICO（Initial Coin Offering）とは

仮想通貨が使われるようになるにつれ、この仮想通貨を活用して資金調達をしようとする動きが出てきました。IPO（Initial Public Offering：新規株式公開）をもじってICO（Initial Coin Offering）と呼ばれます。先にお話しましたように、仮想通貨は国家でなくても発行できます。そこで、資金が必要なある企業がみずから仮想通貨を発行し、それを投資家が購入することで、当該企業が資金を得るという形です。

ICOはこのところ流行ってきていますが、ICOを行う企業側には情報公開義務や法定のプロセスが現時点ではありませんので、投資家にとっては非常にリスクの高いものとなります。詐欺的な被害も出ているとの報道もあります。ICOは海外だけではなく、日本でも既に実施されており、ICOを通じて100億円以上を集めた事例も存在しています。

各国政府における仮想通貨の取扱い

仮想通貨は新しいもので、かつ急速に利用されるようになってきたため、政府の制度・規制整備はこれからという状況にあります。主要国の中でも、日本は仮想通貨に対して先進的とみられている状況です。主要各国における仮想通貨の取扱い状況を以下の表にまとめました。

国名	仮想通貨の取扱い
日本	・2016年の資金決済法改正により、仮想通貨の定義、及び仮想通貨取引所に対する登録等の義務を定めるなど、先進的取り組みを進めています。 ・ICOについては、仮想通貨取引所としての登録が必要になる場合があるとの見解を金融庁が示しています。
米国	・州毎に仮想通貨の取扱いは異なっています。例えばニューヨーク州では仮想通貨取引業者にライセンスを求めるなど規定しています。仮想通貨全般については寛容的と評されていますが、ICOについてはSEC等が規制・介入を強めています。
中国	・2017年９月にICO全面禁止。 ・2017年10月には仮想通貨取引所を閉鎖するなど、強力に規制。
韓国	・2017年９月にICOを禁止。その後も取引アカウントの実名登録を求める、外国人による取引を禁止するなど規制を強めています。
EU	・仮想通貨全般については比較的寛容的ですが、ICOについては、規制すべきとの意見をESMA（欧州証券市場監督局）が述べています。

主要国の中では、日本、米国、EUは全般的に寛容的で、中国、韓国は厳しい立場を採っていると言えます。それでもICOに関しては、各国とも懸念を持っていると言え、今後規制の厳格化が予想されます。

仮想通貨を支える仕組み：ブロックチェーン

さて、こうしてみてくると問題が多そうに見える仮想通貨ですが、それでも仮想通貨がこれだけ利用されたり話題になったりするのには理由があります。一つには、仮想通貨が今までになかった機能や便益を実現できるからなのです。

仮想通貨の歴史には諸説ありますが、現在の仮想通貨隆盛のきっかけとなったのは、仮想通貨ビットコインであることは間違いないでしょう。ビットコインは、サトシ・ナカモトという人物の考えに基づき、2009年から運用が始まった仮想通貨です。ビットコインが目指すのは、インターネット上で、銀行等の中央管理機関を必要とせず、少額であっても手数料がほとんどかからない形でグローバルに価値のやりとりができる、ということです。

政府や銀行等の中央管理機関が不在なまま、価値移転の信頼性を担保するために、ビットコインにはブロックチェーンという仕組み・技術が導入されています。価値移転の取引がある場合、その取引を記録する「台帳」というものが必要となります。例えば、「2018年４月XX日にAさんからBさんに10ビットコインが渡されました」、という取引を記録しておかないと、その後の取引を行うことができない、ということはご理解いただけると思います。ブロックチェーンの場合、その取引記録である「台帳」は、取引データ等の集合体である「ブロック」として格納されます。各ブロックに、前のブロックを一定の方式で変換した値（変換値）を入れ込むことで、そのブロック同士が数珠つながり（鎖/チェーン状）のようになっているため、ブロック+チェーン＝ブロックチェーンと言われています。ブロック同士が一連となって参照しあっているため、実質的に改ざんが極めて困難であると言われています。

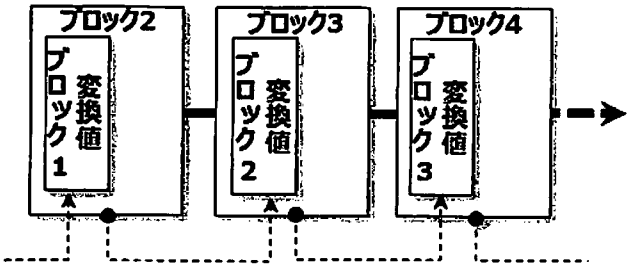

図1　ブロックチェーンのイメージ

更にそのブロックチェーンは各端末に送信され、保存されます。それぞれの端末は同じブロックチェーンを所有しており、対等な関係にある端末間で相互に接続されるピアツーピアと呼ばれるネットワークを構成しています。そのため、どこか一つのブロックチェーンがなくなったとしても、複製が多数ありますので、バックアップとしての信頼性が担保されます。加えてブロックチェーンは(より正確にはビットコインは)システムとして、分散・自律的に運用できるように設計されていますので、中央管理機関による高品質・大規模なシステム構築・維持が不要で、低コストかつ安定的な運用が実現されます。このブロックチェーンという仕組みがあるため、ビットコインをはじめとした仮想通貨は、中央管理機関が不在なまま「通貨的な」機能を実現することができるのです。

冒頭にあったような仮想通貨に関わる騒動では、「仮想通貨取引所」の運営システムに起因する問題から発生しています。例えばコインチェックの例では、報道に基づくと、仮想通貨の保管方法に関するセキュリティ対策が不十分であったとされています。仮想通貨の仕組みによって、不正アクセスを行ったアカウントも特定できていますし、その流出先もトレースされています。Zaifの例では、取引所の仮想通貨売買に関する価格計算システムに異常があったため、と発表されています。これらの例をみてもわかる通り、仮想通貨自体や、その根底にあるブロックチェーン自体に問題があった訳ではありません。

仮想通貨以外に広がるブロックチェーン

ブロックチェーンは、もともと仮想通貨ビットコインを運用するために開発されたものですが、ブロックチェーンの特徴的機能を活かして、仮想通貨以外にもブロックチェーンを利用しようとする考え方が出てきました。価値あるものの取引を低コストで記録し、改ざんできないようにする、という機能は、世の中の様々な営みに応用し得る、と考えたのです。

この新たな利用形態では、ビットコインのブロックチェーンに相乗りするやり方を取るものが出てきました。既にシステムとして安定的に運用されているビットコインのブロックチェーン実績を活かし、仮想通貨以外の用途に利用しようという訳です。この例としては、貸付、証券、保険、医療等の記録を格納する、というFactom（ファクトム)という企業や、デジタル著作物の著作権管理を行おうとするAscribeなどといった企業があります。しかし、ビットコインのブロックチェーンは、当然ではありますが、仮想通貨の取引に最適化されているため、その他の用途では限界がありました。例えば、条件付き契約自動執行、つまり「○○をやってくれたらBさんからCさんに100ビットコイン渡す」、というようなものは仕組み上できなかったのです。これを実現するには、契約内容をプログラム化できる、新たなブロックチェーンの開発が必要であったのです。

プログラマブルブロックチェーン

プログラムを登録しその実行結果も保証するブロックチェーンとして、2014年にEthereum（イーサリアム)が登場しました。Ethereumではプログラムを登録して支払に条件を設定することができます。例えば、先に述べたような、Aさんの承認が得られたらBさんからCさんへの支払を実行する、或いは、DさんEさんFさんの中から一番良い条件を示した人にGさんからの支払いを実行する、などです。プログラムの登録やそのプログラムへの入力値と実行結果をEthereumに参加するノード間で相互に検証し、確定します。このようなプログラムは、ある条件で実行を約束する契約という見方ができると考えられ、スマートコントラクトと呼ばれています。また、プログラム実行可能なブロックチェーンはプログラマブルブロックチェーンとも呼ばれ、Ethereum以外にも複数の実装が提案されています。

スマートコントラクトは支払実行の条件にとどまらず、多様なプログラムの実装ができます。それを活用した例として、ファンドの運営が考えられています。出資者の投票によって投資を決定し、得られた収益は出資比率に応じた配分を行います。これをスマートコントラクトとして登録、実行することによって、管理者の無い自律的なファンド運営が可能になります。また、先に述べたICOの多くは、Ethereum上のスマートコントラクトで新たな仮想通貨(トークンとも呼ばれます)を発行、管理できることを利用しています。このトークンをビットコイン等の仮想通貨と交換する

形での資金調達が実際に行われています。

プログラマブルブロックチェーンの登場により、ブロックチェーンの活用の幅が格段に広がると考えられています。仮想通貨の送金という応用のみならず、様々な分野への活用に期待が寄せられ、ブロックチェーンは一気に注目を集めることになったのです。仮想通貨ビットコインのコア技術として誕生したブロックチェーンですが、ここ最近は、ブロックチェーンのひとつのアプリケーションが仮想通貨である、という考え方になってきています。

中央管理機関が無いシステム

スマートコントラクトを工夫することで、取引記録だけでなく、多様なデータをブロックチェーンで管理することが考えられます。すなわち中央管理機関の無いデータ管理システムを構築することができると考えられます。このようなシステムに対し、あらゆるビジネス領域での活用が期待され、検討が始まっているといえる状況です。例えば、サプライチェーン管理やシェアリングサービス、さらには、IoTデータ管理やメディアコンテンツ流通、電力エネルギー管理などがその一端です。

ここであらためて、中央管理機関が無い、というのはどういうことなのでしょうか？仮想通貨の場合は、中央銀行のような価値を保証する機関が無い状況でも、取引記録をユーザ間で検証、確定することで価値の移動を可能としています。改ざんできない取引データを信頼の源泉として、仮想通貨としての価値を認めていると考えられます。

データ管理についても、ブロックチェーンで管理されるデータが信頼の源泉と考えられます。中央管理機関がデータを管理する場合、管理者以外はデータへのアクセスが制限されていて、データが正しいかどうかユーザは確認しようがありません。データを管理している中央管理機関を信頼するしかないのです。仮に中央管理機関の管理者が不正にデータを書き換えても、それを見抜くことは非常に困難です。これに対して、ブロックチェーンにおいては、ユーザが相互にデータを検証し、確認済みのデータを持ち合います。あるユーザが勝手にデータを変更しようとしても、他のユーザが待っているデータと不整合が起きてしまい、データの変更が認められません。

このようにユーザが相互にデータを検証し、確定するため、いったん登録したデータを取り消すことはできません。データを変更する場合には変更の記録が残ることになります。データ改ざんの難しさに加え、ユーザがデータをトレース可能なことも特徴です。また、全ユーザから見られているということが、心理的にも不正を起こしにくい状況である、と言えるかもしれません。

さらに中央管理機関があるということは、その管理機関がルールを定め、それに従うことが必須になります。例えば、動画配信サービスを利用する場合、必然的にそのサービスの規約に従うことになります。その規約に同意できない場合は、そのサービスは使えないことになります。従来システムを前提とすれば当たり前なのですが、中央管理機関の無い配信システムができれば、権利者自身が動画の利用ルールを決めることも可能になります。自分が持っている権利を自由に行使できるということになります。

このように、中央管理機関が無いデータ管理システムでは、データの相互監視、トレースが可能なため、改ざんが難しい、その結果、証拠性が担保できる、という特徴があります。この特徴を利用することで、権利を所有しているユーザが柔軟に利用条件を設定してデータ流通させることができると考えられます。ただ、一方で、応用に際しては、従来にないビジネスモデルの構築やシステム運用での工夫も必要になってくると考えられます。

NTTでの研究開発の取組み

ＮＴＴサービスエボリューション研究所でもブロックチェーン技術の可能性に着目し、コンテンツ流通での活用について、室蘭工業大学岸上順一教授との共同研究を2014年に開始しました。コンテンツの権利を所有している制作者自身がエンドユーザに対する利用許諾を柔軟に管理できる仕組みをコンセプトとして提案しました。中央管理機関を持たず、ブロックチェーンでコンテンツの権利を管理するシステムです(図２)。

この提案では、動画等のコンテンツを制作と共にブロックチェーンに登録します。映像コンテンツはファイルサイズが大きいためブロックチェーンの外で流通させ、コンテンツの管理情報をブロックチェーンで管理する方式です。管理情報には、コンテンツ自体の情報と権利(使用許諾条件等)の情報があります。ユーザからの使用許諾要求に対して、権利者が許諾する場合、ブロックチェーン経由でコンテンツへのアクセス情報をユーザに伝えます。アクセス情報は他のユーザには開示したくない情報ですので、これを暗号化してブロックチェーンに登録します。これにより権利者が

ユーザに情報を伝えたという証拠がブロックチェーンに記録されます。情報の暗号化には公開鍵暗号方式を利用します。ここでは公開鍵暗号方式の詳しい解説は省略しますが、暗号化する時と暗号を解く時とで別の鍵を用いる方式です。ブロックチェーンに登録されるのはユーザの公開鍵で暗号化されたアクセス情報のため、他のユーザは暗号を解くことができません。使用許諾を得たユーザだけが暗号を解読できて、アクセス情報を入手することができるのです。この方式を研究所で開発しました。

この、特定のユーザにだけ情報を開示する方式は他の応用でも活用が期待されます。ブロックチェーンのビジネス活用において、当事者でないユーザに情報が丸見えになることが大きな課題になっています。研究所では、この方式を発展させ、ブロックチェーンで適切に情報管理できる、一部秘匿化モジュール、権限管理モジュールを開発しました。ブロックチェーンに登録するデータに暗号技術を活用することで、ブロックチェーンの応用範囲を広げられると考えています。

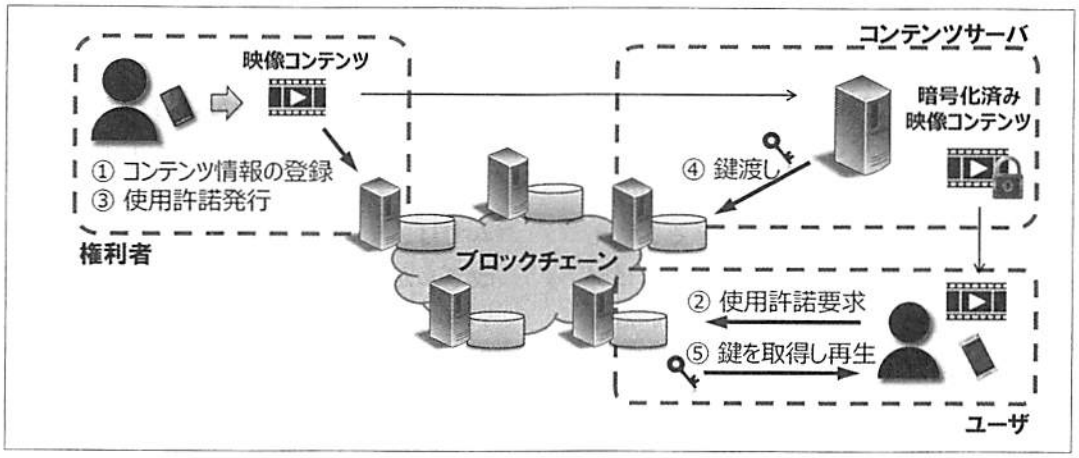

図２　コンテンツ流通におけるブロックチェーン活用

ビジネス化に向けた取り組み

事業化という面においてはＮＴＴデータが様々な注目すべき取組みを進めています。ビジネス化に向けたブロックチェーン活用例として貿易業務があります。具体的には、貿易業務での情報連携にブロックチェーンを活用することを目指していて、実証実験を実施するなど国際的にも先駆的な取組みを進めています(図３)。貿易業務においては、さまざまの業種の様々な企業・組織が協力して業務を進めていきます。その業務をブロックチェーンで管理していくシステムの中で、外航貨物海上保険に関連するデータ管理について、実証実験が実施されました。適切なアクセス性能、業務効率性、セキュリティ性能等の効果について検証が行われ、ブロックチェーン技術適用の有用性が確認されました。この中では、研究所で開発した一部秘匿化機能やユーザ権限管理機能が使われています。

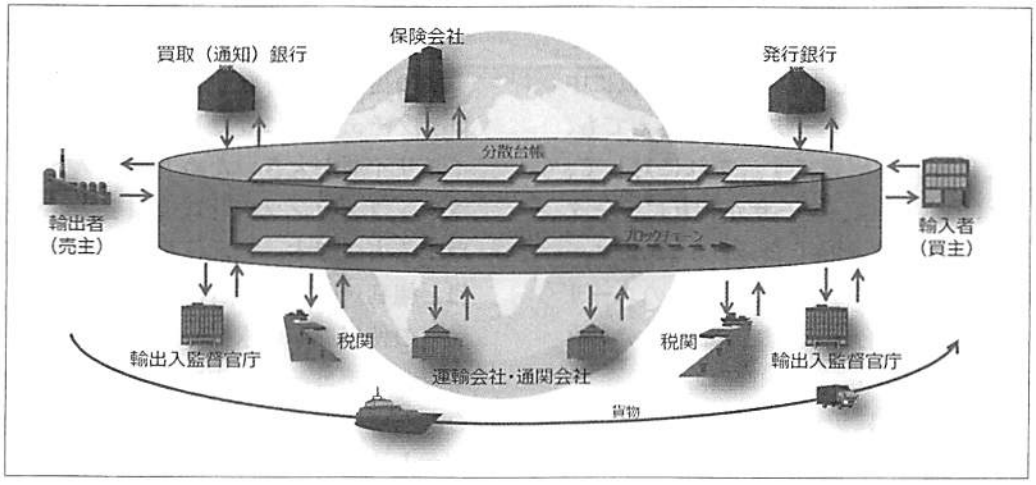

図３　貿易業務におけるブロックチェーン活用例

ブロックチェーンの実用に向けては仲間づくりも重要です。貿易業務については、NTTデータ主導のもと、「ブロックチェーン技術を活用した貿易情報連携基盤実現に向けたコンソーシアム」を2017年８月に発足させ、貿易情報連携基盤の実用化に向けた課題への対応が進められています。

おわりに

ブロックチェーンの活用が期待される分野は多岐にわたり、将来の情報通信分野でも大きな役割を担うと期待されています。事業会社での事業に資することに加え、社会的にもインパクトのある成果を目指し、研究所でのブロックチェーン技術の要素技術開発を進めて参ります。

【参考文献等】

・Cryptocurrency Market Capitalizations
https://coinmarketcap.com/all/views/all/
・Factom
https://www.factom.com/
・ascribe
https://www.ascribe.io/
・Ethereum
https://www.ethereum.org/
・書籍「ブロックチェーン技術入門」 森北出版, 2017年８月.
・NTT技術ジャーナル 2015.5.「競技の感動を世界中で共有できるサービスに向けた技術開発」
・NTT Technical Review, Vol. 15, No. 12, Dec. 2017, "Initiatives Concerning Development of Applications Utilizing Blockchains."
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201712ra1.html
・NTTデータ ニュースリリース2017.4.24「保険証券へのブロックチェーン技術適用に関する実証実験の完了」
http://www.nttdata.com/jp/ja/news/release/2017/042401.html
・ＮＴＴデータ　サービスインフォメーション2017.8.15「ブロックチェーン技術を活用した貿易情報連携基盤の実現に向け、13社でコンソーシアムを発足」
http://www.nttdata.com/jp/ja/news/services_info/2017/2017081501.html

「日比谷同友会会報」第221号

平成30年４月１日　発行
編集兼発行人　田村　俊毅
発行所　電友会本社地方本部　日比谷同友会
〒100-8019　東京都千代田区内幸町１-１-６
NTT日比谷ビル内
電話（03）3509-3020　FAX（03）3509-8490
E-mail douyukai@hibiya-ob.jp
URL　http://hibiya-ob.jp
印刷所　船舶印刷株式会社　電話（03）3831-4181（代）