2018年5月31日号 ご参考資料

NikkoAM Newsletter

日興ＡＭニュースレター

ブロックチェーンの将来像
～インターネット同様、身近なインフラとなる可能性

nikko am fund academy

解　題

- ブロックチェーンは、信頼できない人々が参加していても「信頼できる」仕組みを備えた手法
- 当初は単純な通信手法であったインターネットは、サービスの拡がりでインフラとなった
- 現在、仮想通貨で利用されるブロックチェーンも身近なインフラと成り得るか

■まず始めに、「ブロックチェーン」とは何なのか？

ブロックチェーンは、一般に、取引情報に暗号を加えて作成した「ブロック」を複数の参加者で共有し、そのブロックを次々につなぐ（＝「チェーン」）仕組みを指します。ブロックチェーンは、共有された取引データの正確性を多数決で判定することで、中央で一括管理するシステムに比べ処理速度は遅いものの改竄に強く、安価で、且つ、多重性に富んだ分散システムとなっており、将来性が期待されています。

従来の中央で一括管理するシステムは、信頼性を高める手法を駆使して運営されていますが、ブロックチェーンは参加者が信頼できないことを前提に考えられた仕組みです。これは信頼できない者同士の共同作業で裏切られない手法（一般に「ビザンチン将軍問題」と呼ばれる課題）を基にした技術が用いられています。つまり、ブロックチェーンは性善説ではなく、悪意を持った参加者が利益を狙って取引情報を改竄した場合、改竄で期待される利益よりも改竄に必要なコストが多くなることが事前に分かり、「悪事が採算に合わない」ことで改竄を行なわせない（＝安心できる）仕組みなのです。

少し詳しく

ブロックチェーンは、取引情報に暗号を加えてブロックを構築しますが、暗号の作り方が改竄防止のポイントとなります。
ブロック構築では、一つ前のブロックに保存された暗号と今回の取引内容をもとに、膨大な計算（量、時間）をして次のブロックで使う暗号を新たに作成し、これらをブロックに埋め込みます。

データを改竄した場合、取引内容が正規のものと異なるため、次のブロック用の新たな暗号が必要となります。ブロックチェーンでは複数のブロックが現れた（分岐した）場合、長い方を正規と見なす規則があるため、参加者全員の計算能力を上回る能力で独自に次のブロックを作成し、自ら作成したブロックのチェーンを正規のチェーンと差し替えさせる必要があります。

極めて参加者が少ないブロックチェーンでは改竄の成功例がありますが、参加者が少ないために得られる利益は少なく、価値ある（？）改竄は事実上、不可能と言えます。

公開鍵と秘密鍵

仮想通貨の取引では、個人認証が暗号を使用して行なわれています。個人認証で使われる暗号方式（公開鍵と秘密鍵方式）は仮想通貨に限らず、インターネットなどでも幅広く使われています。

個人認証は、ネットワーク内での改竄や盗難、なりすましを防ぐために、公開鍵と秘密鍵の2種類を用いる方法で行なわれています。個人認証により電子商取引などの信頼性が高まり、インターネットの利便性が高まりました。

二種類の鍵を使う個人認証は、受け取る情報を事前に配った錠前（公開鍵）で施錠（暗号化）した上で送信してもらうことで、輸送中の改竄などを防ぎ、受け取った情報を、自分だけが保有するカギ（秘密鍵）で開錠（解読）する仕組みとなっています。

■ブロックチェーンと似た仕組みを持つインターネット

ブロックチェーンは仮想通貨などで幅広く使われている技術ですが、足元で少しずつ利用シーンが拡がりつつあります。この先、ブロックチェーンの利用シーンが拡がって行くかどうかについて、同じ分散方式で普及したインターネットの歴史から、ある程度推測できると考えられます。

少し詳しく

インターネットは、東西冷戦下の1960年代に米国で研究が始められたARPANETに起源を持つとされています。それまでの中央局（サーバー、ホスト）にデータを集約してやり取りする「センター方式」の弱点であった、一部ネットワークの故障による不通（届かない）を克服する方式として開発されました。

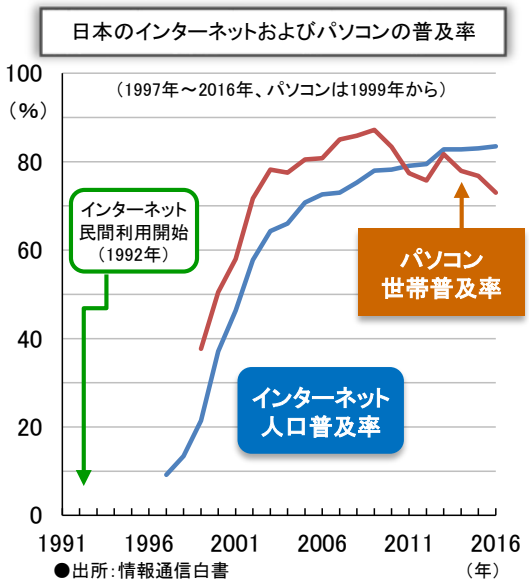
ARPANETは、複数の中継局を配置し、中継局同士を結ぶことで、障害区間を迂回して最終目的地にデータを届ける分散型のネットワークであり、情報を「パケット」と呼ぶ通信単位に小分けし、それぞれのパケットに配送先のアドレス（場所情報）などを記載した荷札を付け、届いた先で到着したパケットを復元（繋ぎ合わせる）する通信手法をとっています。

	センター（中央局）方式	分散（中継局）方式
イメージ図		
交換方式（イメージ）	回線交換方式（専用トラックでの輸送）	パケット方式（宅配便のような混在輸送）
通信速度 通信品位	常に一定速度が保証され、確実に届けられる	ベストエフォート（最高能力）は示されるものの、混雑状況によって変化し、遅延や紛失もある
利用先	固定電話、銀行ATM、取引所など	インターネット（ブロックチェーン）

分散方式は、通信速度や正確性でセンター方式に劣るものの、運営コストやネットワークの拡がりやすさの面で、圧倒的に優位にありました。

その後、通信技術の進歩により、通信速度や容量が拡大する中で、正確性やセキュリティを高めた通信規格も整備され、日常生活での利用に耐えうるネットワークとなりました。

■身近なサービスの登場により普及が進んだインターネット



当初は通信速度の遅さや、学術的な利用が多かったことから、扱われるデータは文章が中心であり、インターネットは専門的な道具として扱われていました。

ブラウザーが進化し通信速度が向上した1990年代後半、Yahoo！JAPANがサービスを開始し、パソコンの普及率の高まりと共に、生活に欠かせない道具へと変化しました。

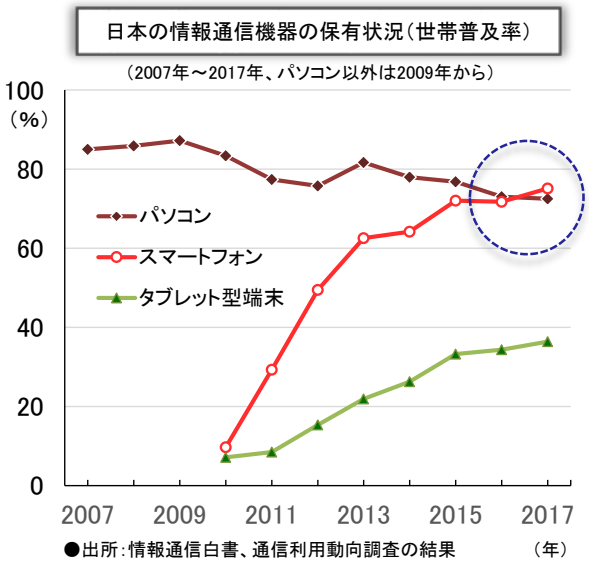
また、暗号技術の進歩やブラウザーの高度化により、情報収集の手段であったインターネットは、各種予約や通信販売を取り込み、日常生活に入り込み始めました。その後、携帯電話などの移動体通信技術の進化により、インターネットは携帯端末による個人利用が中心となる中で、SNSなどのサービスも登場し、無かった時代が想像できない日常の一部となりました。

■ブロックチェーンは、携帯端末を介したサービスでの活用が見込まれる

情報通信端末の機器別の保有状況を見ると、足元でパソコンとスマートフォンの普及率が逆転しています。インターネットはサービスと既に一体と捉えられており、利用していることが意識されないレベルであることから、携帯できる情報端末が優位に立ったと考えられます。

この流れは、そう簡単に変わるとは考えられないことから、この先、ブロックチェーン技術の活用が見込まれるサービスは携帯端末を介したものと考えられます。

また、ブロックチェーン技術は、迅速な処理や大量のデータの蓄積などには向いていない一方で、コストを抑えて利用することが可能な技術ですので、コスト面の問題でデジタル化が進んでいない分野での活用が見込まれます。



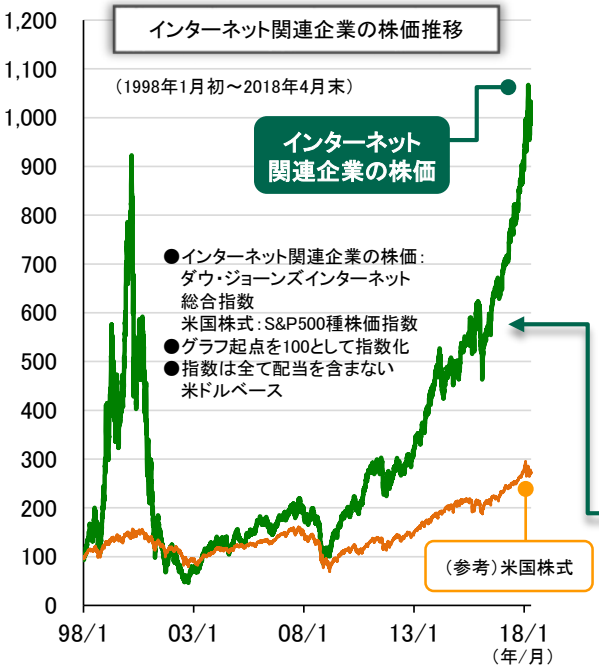
●出所：情報通信白書、通信利用動向調査の結果

今後、ブロックチェーン技術の利用が見込まれるサービス

■ 著作権や所有権に絡むサービス

インターネットで音楽や映像などを適切（少額）な課金で気軽に楽しんだり、提供したりするサービスはまだ少なく、こうした「コンテンツビジネス」は、ブロックチェーンを導入することで拡大すると見込まれます。

また、今後、普及の本格化が見込まれる「シェアリングビジネス」においても、収益の配分のために所有権や所有割合の明確化が欠かせません。こうした管理にもブロックチェーンが活用できると考えられます。



●信頼できると判断した情報をもとに日興アセットマネジメントが作成
●上記は過去のものであり将来を約束するものではありません

■ 個人承認を必要とする行政サービス

正確さと信頼性が求められるためにデジタル化が進んでいない、選挙や登記などの公的な事業に対し、効率化などをめざしてブロックチェーンが導入される可能性があります。

また、デジタル化により地域を越えて利用が可能となれば、医療データ（電子カルテ、服薬情報など）、社会保障（年金や支援など）、税金といったサービスの充実が期待されます。

インターネットが生活の一部となる中で、関連企業の株価（左グラフ参照）は大きく上昇しており、ブロックチェーンにおいても、今後、身近なインフラとなる中で、関連企業への注目は高まるものと考えられます。