仮想通貨シリーズ（1）

仮想通貨とは

Fin Tech監査推進チーム

最初の仮想通貨であるビットコインは2008年にSatoshi Nakamotoと名乗る人物によって発表され2009年に実際に誕生した。それと同時にビットコインを支える主要な技術としてブロックチェーンが誕生した。

昨今、ビットコインを初めとする仮想通貨の普及が日本を中心として急速に広がりを見せており、仮想通貨及びブロックチェーンについて金融領域のみならずサプライチェーン、デジタルアイデンティティ、C2C市場など様々な分野への応用可能性が議論され、世界中で検討・検証が進んでいる。

本稿では、仮想通貨及びそれを支える主要な技術であるブロックチェーンの基礎について解説を行う。

【目次】

Ⅰ 仮想通貨・ブロックチェーンの作る未来

1．仮想通貨のインパクト（Unbanked、マイクロペイメント）

仮想通貨は2009年に誕生し、しばらくの間はマニアの間でのみ取引がされていた。現在アメリカではでビットコインによる決済を利用するサービス等が増えており、日本においても利用できる店舗・オンラインストアが急速に増えている。しかし、日本においてはビットコインで決済をするメリットは今のところほとんどなく、ビットコインは現在も価値変動が激しいことや取引の承認に10分ほどの時間がかかることから必ずしも決済には向いていない。

そのような中で仮想通貨をなぜ使うのかわからないとの声を多く耳にするが、新しい価値であるため何に使えるかわからないのは至極当然であって、むしろ何に使うとメリットがあるかを自ら考え世の中に発信していける機会が今到来している。

仮想通貨の本質的な価値はインターネット上で誰でも価値の移転を行えること、改ざんできない共有台帳であることにあり、そのインパクトはUnbanked（銀行口座を持たない人々）、マイクロペイメントの分野にあると筆者は考えている。以下2点について説明する。

（1） Unbanked（アンバンクト）

Unbankedとは銀行口座を持たない人々のことをいう。Unbankedの人口は日本においては370万人ほど（人口の3.3%）であるが、東南アジア（シンガポール、インドネシア、タイ、ベトナム、フィリピン、マレーシア）では2.3億人ほど（人口の57%）であり、東南アジ

アの複数の国で60%を超えている（2016年時点の統計による）。Unbankedの人々は既存の金融サービスにアクセスする手段を持たない。しかし近年スマホの普及が進んでおり、銀行口座は持っていないが、スマホをでインターネットに接続できるUnbankedの人々が急増している。

仮想通貨での送金は24時間365日可能であり、送金手数料も数十円から数百円程度で世界中の誰にでも送ることができる。このことから、スマホ・インターネットのみで完結する仮想通貨が爆発的に利用されるポテンシャルがある。

また、今まで寄付でしか生活が成り立たなかった人々の生活も一変する可能性を秘めている。従前は例えばアフリカの現地調査をする際などに現地の人々に日本から依頼して仕事を実施してもらい報酬を支払うということが一度限りの依頼では実行しにくかった。これは相手の報酬の振込先がないことと支払いに対して送金手数料が多額であるためである。仮想通貨を利用することで、相手は仮想通貨の受取アドレスさえ持っていれば報酬の支払いを受け取ることができ、送金手数料の安さから数十円・数百円から仕事を請け負うことができる。寄付ではなく仕事と報酬で生活することができる可能性がある。

決済や銀行が便利な日本、とりわけ、東京にいると仮想通貨のメリットが見えてこないが、金融サービスを知らない・利用できない人々にとってはライフスタイルすら変えてしまうインパクトがある大きなパラダイムシフトなのである。

(2) マイクロペイメント

マイクロペイメントとは数銭から数十円といった非常に少額の支払いのことをいう。仮想通貨の送金（支払い含む）は上述の通り、安価な手数料で実施することができる。このことにより、今まで送金手数料が理由で元が取れないことから実施されていなかった経済行動が行われる可能性がある。例えば、雑誌社や新聞社が紙面や雑誌というまとまった単位で販売していた記事等を仮想通貨を利用することで一記事単位で海外の消費者に販売することができる。これは実際に既に行われており、海外では、仮想通貨の決済サービスを利用して一記事、一時間、一日という単位で0.1ドルから1ドルにてインターネット上で記事を読む権利を販売している実例がある。

また、仮想通貨による決済は将来的にはマシーン対マシーン（M2M）の決済に利用される可能性が高いと筆者は考えている。昨今のIoTの盛り上がりによって、将来的に様々なデバイス（マシーン）にセンサーや通信端末が搭載されていくことになることが予想されている。そうすると、IoTデバイスは今まで計測できなかった単位、場所、時間等で様々な変化・行動・挙動を計測することができるようになる。一方で仮想通貨による支払いは将来的にはライトニングネットワークという技術革新等により数銭、1/1000円のような単位で支払いが可能になる可能性がある。

つまり、将来的にはIoTにより今まで測定できなかった単位で物事が測定され、仮想通貨により今まで支払うことができなかった単位で支払いが可能になるため、極少額での従量課金やデータ販売が可能になる。このことにより、例えばジェットエンジンを販売するのではなくジェットエンジン1回転あたり数千円のような従量課金のビジネスモデルが可能になり、また、クラウドサーバーの使用料についても一ヶ月数万円ではなく、1分当たり使用量ごとに数百円のような課金も可能になる。

そうなると、マシーンが勝手に情報を収集し、データの販売等により支払いを要求し、買い手側のマシーンが予め決定した方針に従って当該データ等を購入して仮想通貨で支払いを都度行うといったM2Mの売買と決済が自動で行われることになる可能性がある。

このように今まで計測できないことや手数料の問題で不可能だった極少額の支払い、マイクロペイメントが可能になり、様々な産業・サービスのビジネスモデルを変革する可能性を秘めている。

2. 仮想通貨・ブロックチェーンによってモノではなくモノを買う・使う権利を売買するようになる？

仮想通貨は発行者の信頼ではなく、ブロックチェーンという技術への信頼、つまり、改ざんできないデータベースへの信頼によって誰が今いくら所有しているというデジタルなデータを保持することで成立している。（正確には「誰が」ではなく、「どの仮想通貨のアドレスが」である。）

つまり、誰がいくらその仮想通貨を所有しているが常に把握でき、その仮想通貨を発行者の信頼ではなくブロックチェーン技術への信頼を利用して誰でも発行することが可能である。これを利用することにより、企業はモノを製造・開発して販売するのではなく、モノの所有権を付与した独自の仮想通貨を発行して販売することができ、製造・開発前に権利を売却してから製造を開始できるようになる。また、購入者は商品を将来受け取るだけではなく、他の消費者にその所有権を販売したり、所有権を分割して複数人で所有することもできる。

例えば、将来的に自動車メーカーが新たな自動車を製造販売する際に、将来新車を購入することができる権利を自社独自の仮想通貨新車コインとして発行・販売する。新車を購入したい人は対価の支払いをして新車コインを購入する。これにより自動車メーカーは製造開始前に資金を集めることができ、集めた資金で製造を開始できる。新車コインの所有者は商品を受け取るまでの間にその新車コインを他の消費者に売却することも可能であり、また、新車コインを10分割して10人で所有権を分割して保有しカーシェアすることもできる。

つまり、仮想通貨・ブロックチェーンにより管理された改ざんできないデジタルデータとしての買う・使う権利が発行され、その権利がインターネット上で自由に売

買される将来が来るかもしれない。

実際に自動車メーカーの研究機関で、複数のブロックチェーンベンチャーと提携し、自動運転車とブロックチェーン、カーシェアやライドシェアとブロックチェーンの研究等を始めている事例がある。また、Nasdaqはモノの所有権ではなく企業の所有権である株式に上記のようにブロックチェーン技術を応用しており、既にブロックチェーン技術を利用して未公開株式の売買市場を形成・運営している。

II　仮想通貨・ブロックチェーンの基本事項

1．仮想通貨の定義、ブロックチェーンの定義

(1)　仮想通貨の定義

仮想通貨の世界共通の定義は存在しないが、筆者は下記のように考えている。

仮想通貨とは、ブロックチェーン技術を利用して発行した電子的な価値であり、インターネットを通じて不特定多数の間で物品やサービスの対価に使用することや送付し合うことができるもので、単独・特定の管理者が存在しないものをいう。仮想通貨の種類は600種類以上あるといわれている。

また、日本においては「資金決済に関する法律」（以下、「資金決済法」という）にて仮想通貨が定義されている。

「この法律において「仮想通貨」とは、次に掲げるものをいう。

一　物品を購入し、若しくは借り受け、又は役務の提供を受ける場合に、これらの代価の弁済のために不特定の者に対して使用することができ、かつ、不特定の者を相手方として購入及び売却を行うことができる財産的価値（電子機器その他の物に電子的方法により記録されているものに限り、本邦通貨及び外国通貨並びに通貨建資産を除く。次号において同じ。）であって、電子情報処理組織を用いて移転することができるもの

二　不特定の者を相手方として前号に掲げるものと相互に交換を行うことができる財産的価値であって、電子情報処理組織を用いて移転することができるもの」

（資金決済に関する法律　第二条　5より転記）

つまり、不特定多数の間で支払い・交換できるため、Suicaや商品券などの前払式支払手段とは異なり、特定の管理主体がいない点で法定通貨や銀行口座の残高とは異なる。上記のように特定の会社が発行したとしても、仮想通貨は発行者の管理が及ばないところで転々流通することができるため、特定の発行主体が存在することと特定の管理者がいることはイコールではない。

法律により国として仮想通貨を定義したのは2017年9月時点で日本のみである。

(2)　ブロックチェーンの定義

ブロックチェーンについても世界共通の定義は存在しないが、筆者はブロックチェーンを広義に捉えて以下のように定義している。

ブロックチェーンとは、下記3つの特徴を有するデータベース及び仕組みを含む実装をいう。

① peer-to-peerのネットワークによって完全分散したデータをそれぞれのピアが保持し処理・参照することができる
② 分散処理した結果・合意を一意に保つ分散合意形成プロトコルを持つ
③ 電子署名及びハッシュポインタを使用した改ざん困難なデータ構造を持つ

日本ブロックチェーン協会によるブロックチェーンの定義は以下の通りである。

「1）「ビザンチン障害を含む不特定多数のノードを用い、時間の経過とともにその時点の合意が覆る確率が0へ収束するプロトコル、又はその実装をブロックチェーンと呼ぶ。」

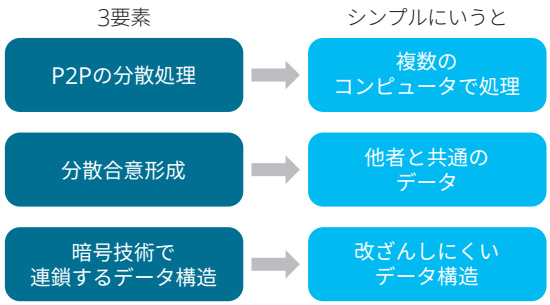
2）「電子署名とハッシュポインタを使用し改ざん検出が容易なデータ構造を持ち、且つ、当該データをネットワーク上に分散する多数のノードに保持させることで、高可用性及びデータ同一性等を実現する技術を広義のブロックチェーンと呼ぶ。」

（日本ブロックチェーン協会ホームページより転載）

上記の筆者のブロックチェーン定義を噛み砕くと、以下のようになる。

① 複数のコンピュータがそれぞれ全く同じの全てのデータを保持・処理・参照している
② ①にて処理した結果を重複や矛盾の無い一意のデータとして保持するための合意形成ルールがある
③ 数学的な暗号技術により改ざん困難なデータ構造を持っている

【図表1　ブロックチェーンの定義3要素とシンプルにしたイメージ】



つまり、銀行の口座残高であれば、銀行のみが管理・処理をすることで誰がいくらの残高を保有しているという一意なデータベースを保っている。これに対して、ブロックチェーンは複数のコンピュータで誰がいくら払ったという取引の承認などを処理しており、複数のコンピュータで処理した結果、誰がいくら持っているというデ

ータがそれぞれのコンピュータで異ならず同じ取引記録になるようにするルールが決まっていて、その承認された過去の取引は暗号技術によって後から書き換えができないデータとして保持されることになっている。

これは、例えると、世界中のビットコインの送金履歴が世界共通の通帳に全て記載されていき、その通帳のコピーを全員が持っている。そして誰でも一定のルールに従って送金の承認・確認に参加することができて、過去の送金記録は暗号とともに記録されて改ざんできなくなるイメージである。そしてこの暗号は誰でも正しい暗号であるか及び過去の取引記録が正しいかを検証することが簡単にできるため、改ざんされたとしてすぐに発見されてしまう構造になっている。

2．仮想通貨・ブロックチェーンの種類・類型

仮想通貨・ブロックチェーンと一口に言ってもその種類は多岐にわたり、世界中で新たな仮想通貨・ブロックチェーンの研究開発が行われている。

(1) ブロックチェーンの種類

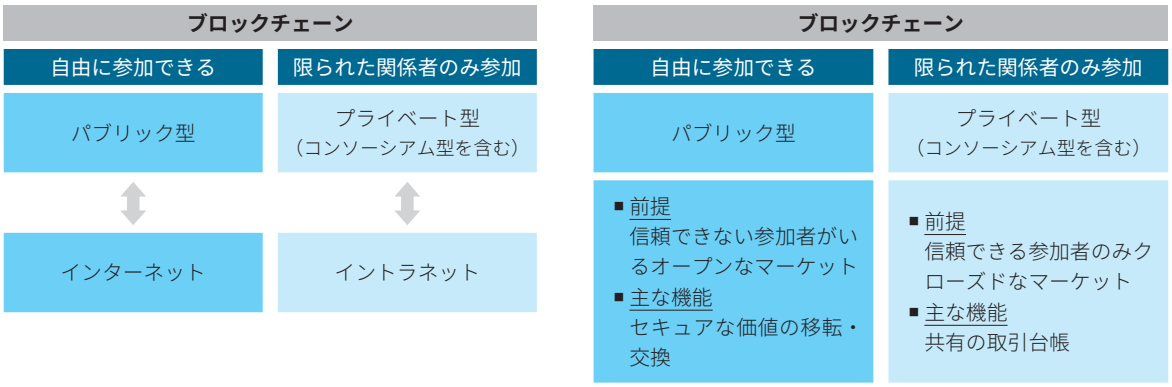
まず、ブロックチェーンについては大分してパブリックブロックチェーンとプライベートブロックチェーンという2種類に分けることができる。簡単なイメージとしては、パブリックブロックチェーンはインターネット、プライベートブロックチェーンはイントラネットのような違いがある。

パブリックブロックチェーンとは、特定の管理者がおらず、不特定多数の者が誰でも当該ブロックチェーンのネットワークに参加して取引の承認・参照をすることができる。よって、信用できない参加者がブロックチェーンのネットワーク上に存在し、意図的に改ざんや不正取引を行おうとする可能性がある。

これに対して、プライベートブロックチェーンとは、特定の管理者が存在し、特定の者のみが当該ブロックチェーンのネットワークに参加して取引の承認・参照をすることができ、特に複数の者によって管理されるものをコンソーシアムブロックチェーンと呼ぶことがある。そのため、信頼できる者のみがブロックチェーンのネットワーク上に存在し、ハッキングやコンピュータの故障等に起因して正しくない振る舞いをする可能性はあるが、基本的には参加者に不正や改ざんの意図はない。

仮想通貨は基本的には上記のうちパブリックブロックチェーン上に乗っている電子的な価値であり、ブロックチェーンの性質から不特定多数の者の間で流通することができ、その記録の改ざんが困難であることから、通貨のようにふるまうことが可能になっている。

【図表2　ブロックチェーンの大分類とそれぞれの前提条件・主な機能】



(2) ブロックチェーンの種類ごとの特徴

パブリックブロックチェーンは、特定の管理者が存在せず、誰でも自由に参加できるため、不正を防ぐ厳格な分散合意形成の仕組み（コンセンサスアルゴリズム）が必要になる。このコンセンサスアルゴリズムにはプルーフオブワーク（PoW）、プルーフオブステイク（PoS）などがある。その他下記の表にあるような違いがあり、パブリック型は仮想通貨を実装しており、不正や改ざんに強いことから価値の移転に利用しやすく、プライベート型（コンソーシアム型含む）は比較的多量の取引データを速く処理できることから改ざん耐性のある共有台帳として使うことが想定される。また、企業間取引などでは情報の秘匿性が必要なケースが多く、プライベート型の利用が想定される。

【図表3　ブロックチェーンの種類ごとの特徴】

管理者	無し	複数企業	単一企業
分類名	パブリック型	コンソーシアム型	プライベート型
参加者	自由	許可制	
トークン（通貨）	必要	任意	
分散合意形成ルールの必要性	厳格なルールが必要	厳格なルールが不要	
取引量	多量の取引を処理できない	比較的多量の取引を処理できる	
改ざん耐性	不正や改ざんに対して強固	通常単独の会社や担当者で改変はできない	
実用例	Bitcoin、Ethereum	Mijin、Miyabi、Broof、Hyperledger fabric	

3．メリットと課題

（1） 仮想通貨を利用するメリット

仮想通貨を利用するメリットとしては利用するコストが安価であること、今までの決済では困難だった極少額（数銭～数十円）の決済から利用できること、国境をまたいですぐに送金できることが挙げられる。仮想通貨決済を受け付ける店舗からすると、既存の決済手段（電子マネー、クレジットカード）は十数万円する決済端末を導入し、決済手数料としてもクレジットカードによる売上の数%を要するが、仮想通貨決済の場合はスマホ又はタブレットがあればすぐに導入でき、決済手数料も1～2%程で済むことが多い。

この価格の差は主に既存の決済手段には複雑に仲介者が介入していることや重厚長大なシステムを利用しているのに対して、仮想通貨の場合は仲介者がいない、又は1社程度しかいないこと及びブロックチェーンシステムのみで支えられていることに起因する。

【図表4　仮想通貨と銀行振込・海外送金、電子マネーの比較】

	仮想通貨	振込・海外送金	電子マネー
利用者のコスト	低	高	無
運営コスト	低	高	高
管理者に起因するリスク	無	有	有
改ざん等の不正	非常に困難	管理者のセキュリティ次第	管理者のセキュリティ次第
価格のボラティリティ	高	低～中	無
取引金額の幅	極小額～高額まで可	小額～高額まで可	小額

（2） 仮想通貨の課題

仮想通貨の課題としては、仕様変更の困難さ、手数料増大のリスク、取引の処理速度の遅さが現状は挙げられる。

①　仕様変更の困難さ

ビットコイン等の仮想通貨は特定の管理者が存在しないため、誰かの一存で仕様変更することはできない。例えば、ビットコインの場合は誰でもビットコインのブロックチェーンについて仕様変更・改善の提案をすることができるものの、マイナー（取引の承認を実施している者）の殆どがこれに賛成し、かつ、仮想通貨を実際に売買する取引所が仕様変更に応じないと新しいバージョンにできないという問題をはらんでいる。

実際ビットコインは仕様変更を巡って数年間も議論をし続け昨今遂に変更が実行された。また、上記のコミュニティの中で意見が大きく割れると、Ethereumのように2つの仮想通貨に分裂してしまう可能性もある。管理者がおらず民主的に決定する仮想通貨のガバナンスにも問題があるようだ。

② 手数料増大のリスク

手数料について上記においては既存の決済手段と比較して安価な手数料で済むと記載したが、取引が増加するにつれてビットコインでの送金手数料が増加傾向にある。1、2年前まで数百円～数千万円送金するのに5円～10円ほどの手数料で済んでいたが、最近は数十円～数百円かかり高くなってきている。この問題に関しては技術革新により解消される可能性があるが、現状解決には至っていない。

③ 取引の処理速度の遅さ

ビットコインの場合、取引が承認されるまで10分程、Ethereumの場合は15秒程時間を要する。このため対面での決済には現状使いにくい。大手量販店などでのビットコイン決済は、基本的には決済システムのベンダーとなっている業者（仮想通貨取引所）が自社にて消費者へ提供しているビットコインウォレットアプリから支払いを受け付けることで、同じ仮想通貨取引所のシステム内で残高をつけかえるようにしているため、この点が問題になっていない。

実際、2017年4月5月頃はビットコインの取引量が急増したためビットコインのブロックチェーンの処理性能が追い付かず、場合によっては送金手続き後1日経っても承認されていないこともあった。2017年9月には技術的な改善により取引の混雑は解消されたものの、根本的な解消には至っておらず、取引量が今後増大していくことで同様のリスクをはらんでいる。

この点についての根本的な技術革新は研究開発中であり、実用化のスケジュールはまだ不明である。

4．日本の法整備

2017年9月時点では、日本は世界で国として唯一仮想通貨を法律上で定義し、仮想通貨の交換業つまり仮想通貨取引所を規制している、仮想通貨先進国である。

具体的には2016年4月に情報通信技術の進展等の環境変化に対応するための銀行法等の一部を改正する法律案が成立し、その中の「資金決済法」に「第三章の二 仮想通貨」が追加された。これがいわゆる「仮想通貨法」と呼ばれている。2017年4月から同法律及び政令等が施行されている。これによって、仮想通貨交換業、つまり、仮想通貨の上記Ⅱ1.(1)に記載した仮想通貨の法律上の定義が定められた仮想通貨の売買や他の仮想通貨との交換又はこれらの媒介、取次、代理をするものは仮想通貨交換業者の登録をしなければならなくなった。

また、同法律の要請により、仮想通貨交換業者は顧客からの預かり資産について、自己の資産と分別管理する必要があり、その他利用者保護の施策を講ずることや、犯罪収益移転防止法の定めに従った本人確認等の手続きを実施しなければならない。

特に自己資産と顧客資産の分別管理については監査法人又は公認会計士による監査を受ける必要があり、さらに事業報告及び貸借対照表・損益計算書（関連する注記を含む）についても監査報告書が必要になる。この点から公認会計士にとっても仮想通貨交換業は既に無縁ではなくなっている。

以　上