2019 年 5 月 1 日

MIGA コラム「新・世界診断」

仮想通貨とブロックチェーン技術

浜口　友一

武蔵野大学国際総合研究所フェロー

1967 年京都大学工学部卒、
同年日本電信電話公社入社、同社にてコンピュータ・システムの開発に従事、その後同部門の分社にともない㈱NTT データに転籍
同社代表取締役社長（2003～2007）
一般社団法人・情報サービス産業協会会長等を経て現在に至る
現在同協会顧問の他、JR 東日本等数社の社外取締役を勤める

IT の世界はドッグイヤーと呼ばれており、通常より 7 倍速く変化が起きると言われている。仮想通貨も投機バブルの崩壊等により一時人気が低下したが、最近は世界の証券取引所が関心を示す等、また関心が高まってきている。仮想通貨は暗号通貨とも呼ばれその安全性は暗号技術を使ったブロックチェーン技術によって支えられている。そしてこれには公的機関による信用保証に代わり参加者全員による保証システムであるコンセンサス・アルゴリズムと呼ばれる仕組みが含まれ、今後様々な分野への適用が期待されるものである。

以降、仮想通貨の状況とそれによってもたらされたブロックチェーン技術について述べる。

「仮想通貨について」

Q:仮想通貨は日本人の書いた論文に基づいているとの説があるが本当か、また論文の内容は

仮想通貨の構想は 2008 年 11 月に Satoshi Nakamoto という人物（正体不明）が暗号技術のメーリングリストに発表した論文から始まった。

論文の書き出しは次のように始まっている。

「A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution.」

すなわちピア・トウ・ピア（注 1）による電子貨幣（仮想通貨）は金融機関の介在無しに流通可能ということであり、この構想は公的機関の介在無しにワールドワイドにダイレクトに取引者間で決済を可能とすることにその目的があった。（現在は投機目的が強くなっているのは残念）。

また論文には安全性を支えるブロックチェーン技術についても書かれている。

仮想通貨に使われている技術は既知の技術であったが、これらを実際に適用したことに意義があった。

2009 年 1 月には最初のブロックがネット上に生成され、ビットコイン（ＢＴＣ）が誕生した。10 月には法定通貨（ドル）に換金された。

Q:金に似ていると言われるが金は実態がある、仮想通貨はどういう形で存在するのか

仮想通貨と言われるように物理的な実態は無い。強いて言うならばコンピュータ・ネットワーク上に書き込まれた仮想通貨発行・取引記録（トランザクション）が仮想通貨と言える。取引記録は一定量が蓄積されるとブロックにまとめられる。ブロックは最初のブロックから現在まで、すべての取引記録が記録されブロックチェーンとして延々とつながっている。

Q:マイナー（採掘者）と言われる人たちが仮想通貨を採掘すると言われているがどういう仕組みか。

取引が一定量に達すると次のブロックを作る取り決めになっている、ブロックを作ることがマイニング（採掘）である。ブロックを作るためにはある計算（高性能コンピュータで 10 分程度に設定されている）が必要で、一番早くその計算を成し遂げた者がそのブロックを形成し前のブロックにつなぐ権利を獲得できる。

そしてその者に報酬として新たに仮想通貨が発行される。これが金の採掘に似ているのでマイナーと呼ばれる。

報酬で与えられる仮想通貨の価値が採掘に要するコンピュータ費用よりかなり高いのでマイナーは一万程度が存在する。

Q：法廷通貨との交換はどのように行われるのか

マイナーとは別に交換業者がネットワーク上に存在する。仮想通貨を売買したい者は交換業者を通じて仮想通貨を売買する。勿論これら取引記録はネット上に記録されることにより正しいことの証明に使われる。

価格は変動し通常のＦＸ取引と同じである。

また最近は物品の購入時に仮想通貨そのものを使える店も増えてきている。

Q:かなりの数の仮想通貨があるがどうしてなのか

現在２千近くの仮想通貨があるが、元祖のＢＴＣから分かれたほぼ類似の機能のコインや、最初のブロックを独自に作り名前をつけて始める者もある、これをＩＣＯ（注３）という。
ブロックチェーン技術を理解しそのプログラミングが出来れば誰でもブロックを作ることが出来る。ただ中にはセキュアな技術を使わず、見せかけだけの詐欺まがいのものもある。

Q:安全性は問題ないのか

ブロックチェーン技術を使いＰ２Ｐのコンセンサス・アルゴリズムによっているコインは現時点では安全と言ってよい。
しかし仮想通貨交換業者の運営やシステムなどは仮想通貨の安全技術とは異なるものであり、その仕組みやセキュリティ対策によって安全度が異なる。
これまで起きた仮想通貨のセキュリティ問題は総て交換業者の問題によるものである。

Q:各国の制度・規制は

２０１８年３月のＧ２０にて仮想通貨は暗号資産と呼称変更され、法定通貨と明確に分離すること、並びに規制を検討する表明がなされた。

・日本　世界に先駆けて「仮想通貨法」を施行。取り組みは早く比較的寛容。金融庁がＧ２０に合わせて暗号資産と呼称変更したことに加え｛仮想通貨交換業等に関する研究会｝においてＩＣＯについて金融商品取引法を含めた規制強化の方向性を示唆している。
・米国　好意的、証券取引委員会（ＳＥＣ）中心に議論、交換業者の登録を
義務化。
ほぼ総てのＩＣＯトークン（電子的有価証券の呼称）は有価証券であるとの見解を表明しており既存のＩＣＯも規制する方針。
・中国　仮想通貨取引所閉鎖、マイニングを禁止。しかしブロックチェーン
プロジェクトの２５％は中国発であるため中国サイバースペース管理局は特定企業への許可を出している。
・韓国　ＩＣＯを全面禁止していたが２０１９年に入って見直しを検討している。
・ロシア　好意的、中国からのマイナーが流れ込みマイニング大国、規制議論中
・インド　扱いについて混乱、今後規制が強まる可能性。
・中東　エジプト：イスラム教で禁止している賭博に当たるとして取引禁止の宗教令
・ＥＵ　比較的寛容だが２０１９年１月に欧州銀行監督機構と欧州証券市場監督局が仮想通貨の規制の必要性を表明

・イギリス　中央銀行（ＢＯＥ）が日銀と実機検証を行うなどブロックチェーン全般に好意的。

「ブロックチェーン技術について」

・ブロックチェーン

ブロックチェーンは過去の取引等が時系列でつながっているため改ざんが困難である。ブロックは取引等の記録と前のブロックの情報を暗号化した乱数（ハッシュ値）等で構成される。あるブロックの取引記録を変更するとそのブロックのハッシュ値が変わり次のブロックにある前のブロックのハッシュ値を変えなければならない。この作業（計算）を延々と続けなければならず、処理量から改ざんは困難である。この技術はデータの安全を担保出来る技術であり、応用範囲は広い。

・分散型台帳とコンセンサス・アルゴリズム

注１で述べたＰ２Ｐでは加盟する総てのマイナーに同じブロックチェーンが
持たれている。（分散型台帳）、これらを総て改ざんするのはさらに困難で実質不可能である。これはコンセンサス・アルゴリズムと呼ばれている。

「まとめ」

ブロックチェーン技術は「データが正しいことを管理者無しで証明する技術」である。現在多くの証明作業が公的機関や資格保持者により行われているが、
ブロックチェーンでは参加者全員のコンセンサス・アルゴリズムにより証明を行うこととなる。
当初の発想は金融機関の介在無しに送金が出来るセキュアなシステムであったが、今その応用範囲は大きく広がりつつある。
最近のＩＴのバズワードにフィンテック（金融とＩＴの融合）とかXテック
（Ｘ分野とＩＴの融合）があるが、いずれもブロックチェーン技術が一つの役割を担っている。
金融取引、貿易手続き、不動産取引、車の売買、バイオ情報の管理等々多くの分野での事例も出つつある。
ブロックチェーン技術は適用分野によってはコンピュータの処理能力による制限やコスト等解決すべき課題もあるが、間違いなくＩＴの重要な技術の一つとなるであろう。

以上

注１　ピア・トウ・ピア（Ｐ２Ｐ）

コンピュータ・ネットワークには集中型と分散型がある、Ｐ２Ｐは分散型ネットワークの呼称である。

・集中型　中央に処理を行うコンピュータがあり、総ての端末は中央につながり端末では処理は殆ど行わない。中央集権型

・分散型　端末同士がネットワークで相互につながり、端末それぞれが処理を行なう。中央の処理コンピュータは無い。地方分権型

集中型は取引記録等の台帳を中央にのみ持つが、分散型は端末それぞれが
同じ台帳を持つ（分散型台帳）。これによりコンセンサス・アルゴリズムが
可能。

注２　ハッシュ値

大量のデータをハッシュ関数により変換した乱数、ハッシュ関数は不可逆的で乱数からデータを復元することは出来ない。

注３　ＩＣＯ

イニシャル・コイン・オファリングの略。仮想通貨を新たに独自で発行し資金を調達すること、但しこの通貨の価値が上がりそうも無ければ誰も買ってくれない。