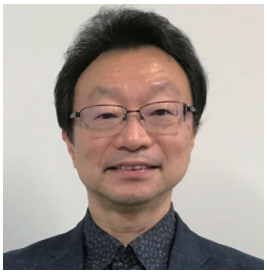
デジタル通貨とスマートコントラクト
：ゲーム理論家の視点から

松島 斉｜東京大学大学院経済学研究科 教授



松島 斉

東京大学大学院経済学研究科教授
1983 年東京大学経済学部卒、同大学大学院経済学研究科博士課程修了（経済学博士）、同助教授を経て 2002 年より現職。

要約

デジタル通貨を下支えする秀逸な技術として注目されるブロックチェーンは、まだ日の目を見ない利用の可能性を大いに秘めている。理想的に社会実装されるようになれば未来社会に多大な影響をもたらすだろう。未知の利用方法を開拓していく主役となるのがスマートコントラクトだ。しかしスマートコントラクトが悪用される可能性を未然に防ぐ制度的措置もあわせて開発していかなければならない。この開発を社会が怠った場合には逆に甚大な社会的費用がもたらされることになるので要注意だ。

はじめに：トークン型とアカウント型

貨幣には２つの形態がある。１つはコインやキャッシュといった「トークン型」で、もう１つは銀行口座に代表される「アカウント型」だ。この２つには正当な支払いかどうかの確認方法に大きな違いがある。トークン型ではトークン自体が本物か否かで確認されるが、アカウント型では支払主が本人かどうかで確認される。アカウント型では個人情報や取引データが必要になるがトークン型では必要ない。

アナログのコインやキャッシュでは偽造防止のコストや交換手段としてのリスクが高いため、アカウント型が主流になっていった。銀行に対する信認こそがアカウント型を支持する所以だ。しかしデジタル通貨が可能になるとトークン型の欠点は削減される。よって今後はアカウント型からトークン型にシフトしていく可能性が考えられる。

民間団体はデジタルトークンを SDGs のミッション達成に利用できる。バンクーバー発祥の ETS のような地域通貨をデジタル化してコミュニティを活性化できる。独自のミッションを持つ発行主体には独自の価値尺度が必要だ。利用内容や利用者の制限も必要だ。デジタルトークンはこれらを後押しする。

重要なことはデジタル通貨自体に価値が宿ることだ。その源は「他の人が貰ってくれる」というバブル的価値である。しかしこれだけでは通貨価値は長持ちしない。 ビットコインは政情不安国で送金手段に用いられたり日々の買い物に使われたりしている。こうしたことで付加価値が付くと長く使われるようになる。トークンを持っていても（良し悪しは別にして）何某かの使い道がなければ利用者は減っ

てしまう。 発行主体は営利的なネットワーク創りも併せて開発することになる。

デジタル通貨が様々に開発され成功すれば差別化競争の様相を呈するようになる。競争の主役はプラットホームプロバイダーだ。プラットホームプロバイダーは自前のデジタル通貨を作り、貨幣の機能とデータ仲介機能を組み合わせて独自のサービスを創発することで独自の取引データを占有できる。占有できるとなるとクロスボーダーでプラットホーム間の差別化競争が起こり、さまざまなセグメンテーションができる。 こんな状況はデータ占有ができないアカウント型では生まれない。

上に記したことは数年前なら絵空事だったがもはや現在進行形だ。デジタル通貨が未来の社会におよぼす影響は計り知れない。

ゲーム理論家の視点

このエッセーのテーマは、将来的なデジタル通貨の可能性を、ゲーム理論家としての私の独自の視点から考察することだ。特に「ブロックチェーン」が今後積極的に活用される場合、社会がこの影響にどのように対応していくかについて検討したい。ブロックチェーンはデジタル通貨を下支えする根幹に位置する。注目したいのは、ブロックチェーンを使って契約を自動化してくれる「スマートコントラクト」という技術だ。スマートコントラクトは、積極的に活用されるようになれば、実社会にとりわけ大きな影響を及ぼすと考えられる。それはビジネスにおける信用の役割にも深くかかわる。

一般にビジネスの成功には信用が不可欠とされる。ビジネスを続ければレントが得られる。ズルをするとレントを失う。だからまじめに働いて信用を失わないようにする。しかしレント稼ぎがもたらす弊害も大きい。ブロックチェーンとスマートコントラクトは弊害のあるレントを引き下げ信用のあるべき姿を変容させる。

ブロックチェーン

ブロックチェーンは「オンライン分散型取引台帳技術（DLT）」で、デジタル通貨のウォレット間の移動を時系列的に 1 本のチェーンとして記録する技術のことだ。ブロックチェーンにより不正や改ざんがほぼ不可能になる。大事なことは、交換手段としての価値が法定通貨の裏付けがなくても発生しうることだ。そのため通貨としての独立性を保ち固有の価値尺度で決済や送金ができる。ドル建てや円建てではなく、デジタル通貨だけで取引と決済が完了する。ここにブロックチェーンの強みがある。

例えば多くの人々が、ブロックチェーンに支えられたある架空の通貨「HIT（ヒットコイン）」に対して「1HIT ＝ 1 万円」の価値があると思っている状況を考えよう。私は 300 万円の中古車を購入しようとしている。その代金として私は 300 万円ではなく、300HIT をディーラーに支払うことにした。両替所で 300 万円を 300HIT と交換し、それをディーラーに送金するのである。まずこの送金のことが書かれた取引を作成する。次に私とディーラーの署名をつけて、この取引をネット上に公開する。するとこの取引は見ず知らずの誰かによってピックアップさ

れ、300HIT の移動が妥当な取引かどうかについて何らかのチェックがなされる。ブロックチェーンに記載されている過去のデータが遡及追跡される。問題なければこの取引は承認されブロックチェーンに追記される。こうして晴れて 300HIT は送金され、取引は無事完了する。

クレジットカードの場合、最終的にはプラットホームの外でのアカウント決済になる。 口座の本人確認などが新たに必要となり、余計な情報が外に流れる。ところがブロックチェーンの場合にはブロックチェーンに記載されている情報の範囲で完了できるため、このような情報漏洩は生じない。またウォレットの保有者ではない人が暗号キーを盗んで送金をした場合の責任問題は、ブロックチェーンの外の問題として切り離される。こうして個人情報を必要としない仕組みが出来上がる。取引手段として自立している点がデジタル通貨の本質だ。クレジットカードはアカウント型なので別物だ。

ブロックチェーンのガバナンス

ブロックチェーンは複数の利用者にダウンロードされて分散型の管理がなされる。管理に携わる人は、取引をまとめてブロックを組成しチェーンの先に追加していく。この際に過去の記録と矛盾していないかチェックされる。取引の内容は複雑な計算によって数字の羅列に変換されるなどして暗号化して、プライバシーが守られる。このような計算は迅速を求められるとコストのかかる作業になる一方、改竄防止の役目をなす。この作業をだれが担うかによってブロックチェーンのガバナンスの仕組みは様々に設計されうる。

ひとつは、特定の個人、組織、あるいは国家が代表してブロックチェーンを管理するやり方で「プライベート型」と呼ばれる。管理者がまともならスムースに組成承認の処理がすすむが、強い独占力を発揮する弊害も生まれる。ブロックチェーンに託している夢とは逆方向だ。ならば共同体（コンソーシアム）を設置し、管理者の行動をチェックするのはどうか。これを「コンソーシアム型」と呼ぶ。この良し悪しは、管理者が一人に固定されるのか、コンソーシアムのメンバーが交代でおこなうのか、誰がどんな基準でメンバーに選ばれるかなど、細かな規定の仕方に左右される。

コンソーシアムのメンバーは、ブロックチェーンの利用者全体の利益を必ずしも代表しない。ならばいっそのこと組成承認の作業を不特定多数にゆだねてみてはどうか。例えばブロックチェーンをよく使う人、あるいは通貨をたくさん所有している人にこの作業をお願いしてみてはどうだろうか。この考え方は、「POS（Proof-of-Stake)」と称される。このような人たちは、作業を怠ると通貨価値に傷がつき、自身の利益を損ねると考える。だからまじめに作業するインセンティブをもつはずだ。こんな POS の考え方は発展途上にある。

現実にビットコインなどで使われてきた仕組みはどのようなものか。それは「POW（Proof-of-Work)」と呼ばれ、不特定のだれもが組成承認の作業に参加できる。数字の羅列をもとめる難しい計算問題を速く解いた人だけが、自身が用意したブロックをチェーンにつなぐことができる。このブロックに続けてさらに

チェーンが伸びていけば、ブロックがみんなに承認されたとみなされ、ご褒美としてコインを受け取ることができる。ご褒美目当てに計算作業（マイニング）を我先におこなうインセンティブが芽生える。

このようなブロックチェーンは特定の人や団体によって中央集権的に管理されていない。ブロックチェーンをみんなが使うようになれば得てしてその管理者は独占権を行使し、利用料を法外に取ったり、営利のために利用を制限したりしがちになる。そうならないように、ブロックチェーンの台帳はネット上に公開され、誰でも閲覧できるようにされている。ブロックチェーンはコモンズ（共有資産）になっている。

新しい取引をブロックチェーンに追記していく作業には誰もが参加できる。この人たちは必ずしも信用できる人たちとは限らない。しかしこの大事な作業を積極的にまじめに遂行するインセンティブが、信用できない人々にも適切に提供されるように、ブロックチェーンの仕組みがデザインされている。

ブロックチェーンの課題

ブロックチェーンはまだ課題を抱えている。まずこれは「早い者勝ちレース」の様相を呈する。専用のパソコンをたくさん用意して計算速度を高めよう。電気代がかかるから、電気代の安いところに引っ越そう。きっとライバルも同じことを考えるだろう。こうしてマイナーたちは消耗戦を戦うはめになり、結果的にご褒美のほとんどが電気の浪費につぎ込まれてしまう。

こんな環境負荷の高いブロックチェーンをどう改良すればいいか。これは昨今のゲーム理論の研究領域にもなっていて、POS や POW を良くするための理論的な糸口が模索されている。しかし、改善案も出てきているのに改善はすすんでいない。コモンズの悲劇が起きているからだ。改善案の社会実装には、環境負荷の高いシステムを段階的に排除していく国際合意形成が不可欠だろう。

ブロックチェーンはスケーラビリティーにも難がある。利用者が増えても、容易には処理スピードをアップしたり、ブロックの容量を増やしたりできない。また、匿名性が担保されるとはいえ、ブロックチェーンをつかって契約を秘密裏に結びたいと思っても、支払いの行方や金額、契約の内容までもが他者に漏れてしまう恐れが心配される。ブロックチェーンのガバナンスには承認プロセスに関与するマイナーの存在が必要だが、かれらに中身が筒抜けになる。

しかしこれらの課題については、今後よい方向に改善されていくものと楽観視しよう。特に秘匿性を備えた近未来のブロックチェーンは、情報を持っているが無力な個人の権利を守るための決定打になるかもしれない。

スマートコントラクト

さて、このエッセーが着目する、ブロックチェーンにおける重要な革新はイーサリアムに実装されている。それが「スマートコントラクト」だ。 スマートコントラクトは「Programmable Money」という、貨幣をプログラム化する技術だ。

スマートコントラクトによって、様々な「条件付き支払いルール」をプログラムとして付与し、ブロックチェーン上に設置することができる。 そうすることによって、プログラムの内容が自動的に実行できるようになる。 ブロックチェーンを使うことによって、プログラムの内容を改ざんできないため、スマートコントラクトは事実上「Credible Commitment（拘束力のある約束）」として機能することになる。現実の契約は、単なる口約束に過ぎず実行される見込みがないと判断されれば、日の目をみない。しかし、いかなる状況における契約もスマートコントラクトを使えば拘束力ある約束に近づけることができる。

たとえば特定のプログラムをスマートコントラクトとしてブロックチェーンに設置することを考えよう。つまり「入力 A であれば、ウォレット X から Y に 1 コイン（1 ＨＩＴ）を移動する」とする。 しかし「A 以外、たとえば入力 B であれば、X から Y に 0 コイン、つまり移動しない」とする。このプログラムをスマートコントラクトとしてブロックチェーンに設置するのだ。その後、オフチェーン（現実社会）からデジタル入力 A あるいは B を実施する。すると、スマートコントラクトに従って自動的にコインが移動することになる。このようにして 1 コインか 0 コインのどちらかが移動することに正しくコミットできる。

この方法を使って、オフライン（現実社会）で X さんは Y さんからパソコンを 1 コインで購入する約束をするケースを考えてみよう。パソコンが X さんに送られた場合には、入力 A を実施し 1 コインが移動する。パソコンが送られなかった場合は、入力 B を実施してコインは移動されないという使い方をする。

注意するべきは、デジタル通貨の条件付き移転しかコミットできない点にある。円の移転もドルの移転も、モノやサービスの移転もコミットできない。パソコンを移動するようなことは当然できない。その意味では、コミットメントの範囲はかなり限定される。しかしスマートコントラクトは、その使い方を工夫すれば、こんな範囲の限定をものともせずに経済活動促進の万能薬になりうる。

オラクル問題

スマートコントラクトの利用に際して、当事者が解決しておかなければならない問題がある。それはオフチェーン（実社会）とオンチェーン（ブロックチェーンの中）の連結をどうするか、オフチェーンから正しい情報を正直に入力させるにはどうしたらいいか、という問題だ。 入力の段階で嘘をつかれてしまっては、スマートコントラクトの技術は絵に描いた餅になってしまう。これは「オラクル問題」と呼ばれている。

「私はあるディーラーから上質の中古車を 300 万円で買うことにした。約束通り 300 万円振り込んだが送られてきたのはボロ車だ。文句を言いたいが『その電話番号は使われておりません』という返事しか返ってこない。騙された。」

この逸話のような事態はどんな取引にも起こりうるが、実際に起きているわけでなく「信用」によってうまく解決されている。ディーラーは、ボロ車を送り付けようものなら、後で信用を失ってビジネスを続けられなくなる。これを避けたいので

約束通りの中古車を送るのである。

ディーラーが信用できる人物でない場合でも解決の余地はある。それは「信用できる仲介人」を雇うことだ。仲介人に、私は 310 万円を、ディーラーは 10 万円を預ける。次にディーラーは約束通りの中古車を私に送ったか否かを、私は約束通りの中古車をディーラーから受け取ったか否かを、各々イエス・ノーで仲介人に告げる。2 人ともにイエスならば、仲介人からディーラーに 310 万円、私に 10 万円が支払われる。2 人ともにノーならば、ディーラーに 10 万円、私に 310 万円が支払われる。2 人の意見が一致しないならば、ディーラーにも私にも何も支払われず、預けられた 320 万円は凍結される。私とディーラーは、このように周到にしつらえた契約を仲介人と取り交し、「どのような事態になろうとも、イエスノーだけは正直に仲介人に伝えようね」と固く誓う。

こんな契約を取り交わすことができれば、信用できないディーラー相手でも気持ちよく売買できるようになる。ディーラーは、嘘を伝えれば私と意見が一致しなくなるので、代金 300 万円を受け取れないどころか罰金 10 万円をもとられる羽目になるからだ。しかし、肝心の仲介人が信用できない人物だったら、元も子もない。

これに対してスマートコントラクトは、信用できる人が一人も介在しない状況でも契約を成立させる技術になる。

オラクル問題の解決（1）：ナッシュ均衡

このことを理解するため、中古車を 300 万円で購入する状況を再度検討しよう。私とディーラーは、第三者を雇う代わりに、エスクロー取引をスマートコントラクトとして作成し、ブロックチェーンに承認してもらう。私は 310HIT、ディーラーは 10HIT をブロックチェーン内のエスクローに閉じ込める。後日、閉じ込められた 320HIT をどう分配するかについて、改めて二人の署名入りの取引を作成し、ブロックチェーンに承認してもらう。それは「エスクローから私に X（HIT）、エスクローからディーラーに 320 − X（HIT）を送金する」という取引である。大事な点は、二人の署名付きの取引がブロックチェーンに承認されない限り 320HIT はエスクローに閉じ込められたままになることだ。

私とディーラーは以下のコンセンサスを形成しておく。約束通りの中古車が送られた場合には「エスクローからディーラーに 310、私に 10 を送金する」という取引（X = 310）がディーラーから私に署名付きで送られる。私の署名をつけ、それをブロックチェーンに承認してもらう。10HIT 未満しか私が受け取れない別の取引（X > 310）が送られてきても私は署名しない。逆に、約束通りの中古車が送られなかった場合には、「エスクローからディーラーに 10、私に 310 を送金する」という別の取引（X = 10）が署名付きで送られる。私の署名をつけ、それをブロックチェーンに承認してもらう。310HIT 未満しか私が受け取れない取引（X > 10）が送られてきても署名しない。

このようなコンセンサスが形成されると、私とディーラーにはこのコンセンサス

を守ろうとするインセンティブが芽生える。私はディーラーから条件の悪い取引が送られてきても署名しない。なぜなら、いずれディーラーがコンセンサス通りの取引を送ってくると予想しているからだ。私自身が条件のいい取引を先回りしてディーラーに送ったとしても、ディーラーは署名しない。なぜなら、自身がコンセンサス通りの取引を送りさえすれば、私はかならず署名すると予想しているからだ。

こうして、約束通りの中古車が送られた場合には「ディーラーは 320、私は 10」という取引（X = 310）が、誰かに強制されることなく「自己充足的に」作成され承認されることになる。送られなかった場合には「ディーラーは 10、私は 310」という別の取引（X = 10）が、やはり自己充足的に作成され承認される。つまり、どのような事態になろうとも常に事実に正直に入力することが「ナッシュ均衡」になるように、スマートコントラクトを設計することができる。

オラクル問題の解決（2）：一意性

このままではまだオラクル問題の十分な解決に至っていない。なぜなら不都合な結果をもたらす別のナッシュ均衡も同時に存在するからだ。

正直に入力するインセンティブが発生する根拠は「相手が正直に入力する」という予想をたてるからに他ならない。もし「相手が不正直に入力する」と予想するならば、逆に不正直に入力するインセンティブが発生してしまう。二人の意見がことなると閉じ込められたコインが戻ってこなくなるため、意見を合わせることが動機付けの根拠になる。そのため二人が同じ嘘をつくケースも別のナッシュ均衡として成立してしまう。

こうして、正直入力のナッシュ均衡の方が成立しやすいことを裏付けるきちんとした説明が、別途必要になってくる。これは「メカニズムデザイン」というゲーム理論の研究分野で考察されてきた「一意性問題（Implementation Theory）」に対応する。私自身長くこの分野に学術貢献をしてきた（たとえば文献 3）。スマートコントラクトにおける複数ナッシュ均衡の是正を説明するためには、この分野における比較的新しい学術的発見が必要になる。

スマートコントラクトでは支払いルールしかコミットできない。 スマートコントラクトは財やサービスについてはコミットできない。こんな制約下で、コインのもつ金銭的便益にのみ関心のある利己的な経済人だけを考えてみよう。この場合、どのように制度の設計を工夫してみても、不正直入力のナッシュ均衡を排除できないことが理論的にわかっている。そのため、利己的動機以外の動機も考慮してナッシュ均衡の一意性を再検討することが不可欠になる。

利用者のコミュニティには、利己的動機以外に、正直でありたい選好、あるいはむしろ敵対的でありたい（嘘をわざとつく）選好など、さまざまな動機が不確実な形で共存している。しかも正直でありたいという倫理的選好をもつ人はごく少数で稀だ。しかし一連の実験実証研究（文献 1）と筆者による理論研究（文献 4, 5, 7, 8, 9）によって、非常に一般的な環境においても正直入力のナッシュ均衡が実

質的に一意になることが経済学的に裏付けられるようになった。スマートコントラクトにおけるオラクル問題は原理的には解決されているといえる。

デジタル法廷

オラクル問題を克服したスマートコントラクトの使い方の提案として「デジタル法廷」がある。 裁判所の役割の一部を自前のスマートコントラクトに代行させる案だ。 これによって司法コストをゼロに近づけることができる。デジタル法廷は野田俊也氏と私によって 2020 年に発表され、プレスリリースもされた（文献 2，10，11）。

司法コストが高いためオフライン（実社会）の契約は口約束になりがちだ。 そこで、オフラインの契約とは別に、「オフラインの契約の違反者に罰金を科すための罰金ルール」をスマートコントラクトとして書く。 これをブロックチェーンに設置しておけば、スマートコントラクトが裁判所の代わりを務めることができ、裁判を自動化できる。

スマートコントラクトの悪用

スマートコントラクトはどんな契約も実行可能にする。ならばスマートコントラクトを不正な取引に悪用する輩が出てくるだろう。入力内容が抽象的であるため、スマートコントラクトの中身からは不正な目的か否かを判別できない。 このことが事態を深刻にする。ドラッグやマネーロンダリングの取引、サボタージュやカルテルのための取引であっても、スマートコントラクトの中身を見ただけではわからない。

仲介人を使うケースとブロックチェーンを使うケースとでは、違法契約の対処に違いがある。常識的な仲介人ならば「取引が何の用途でなされるのか」に注意を払うはずだ。中古車売買という用途であれば仲介を引き受けるが、非合法ドラッグ売買であれば引き受けまい。一方、常識的でない仲介人は不正目的の代行を引き受けてしまうかもしれない。しかし、何らかのトラブルが発生し裁判沙汰になったとしても、裁判所はそもそも不正目的の契約自体を認めない。そのため不正目的にはマフィアの掟のような闇の慣行が使われる。

しかしスマートコントラクトが使えるとなると、たとえ堅気であっても不正目的の誘惑に駆られてしまう。ブロックチェーンではデジタル通貨の流れと実社会の出来事とが分離される。そのため、実社会で実際にどのような品物の移動が起きていたかを調べ上げる他に手だてはなくなる。さらに気がかりなことが、物の受け渡しをともなわないケースにおいて起こる（文献 6）。

例を使って説明しよう。ある会社が従業員を二人雇う。景気に左右されずきちんと働いてほしい。しかし成果は景気に左右される。そのため相対評価によって報酬を支払うことにした。成果の高いほうに 1000 万円、低いほうに 600 万円の報酬を払うとした。ならば二人は景気に関係なく競い合って働くに相違ない。しかし従業員同士がブロックチェーンを使って「成果の高い従業員は低い従業員に 200HIT 支払う」というスマートコントラクトを結べば、一所懸命働くか否かに

関係なく定額 800 万円を受け取ることができる。こうして結局二人はまじめに働いてくれなくなる。

まとめ：信用できる仲介人の新たなイメージ

デジタル法廷は実社会の裁判に求められる社会的役割の一部のみを肩代わりする。それは契約が正しく履行されたかどうかのチェックだ。しかし契約がそもそも社会的に正当なものかどうかのチェックも求められる。これはデジタル法廷あるいはスマートコントラクトには搭載できない機能だ。この機能はブロックチェーンの外部に別途設置しておく必要がある。

「信用できる仲介人」にこの機能を担うことを期待するべきだ。仲介人が正当だと判断した案件だけにスマートコントラクトの利用を認めるのである。違法性を事後的に問う裁判所とは異なり、仲介人は事前審査によって不正目的を排除する。仲介人には継続性があるので、稀ではあっても万が一不正目的を許したことが発覚した場合、信用失墜という大きなデメリットが生じる。それを恐れて事前審査を真摯にこなすインセンティブをもつことになる。しかし言うまでもなくこれは困難な作業だ。ブロックチェーンが未来においてそのポテンシャルを最大限に発揮できるかどうかは、不正目的の排除がどれほどの社会的費用を伴うかに係っている。

参考文献

- 1. J. Abeler, D. Nosenzo, and C. Raymond: “Preference for Truth-Telling,” *Econometrica* 87. 2019.
- 2. AlphaGalileo: “A Digital Court for a Digital Age,” Press Release. April 6, 2020.
- 3. D. Abreu and H. Matsushima: “Virtual Implementation in Iteratively Undominated Strategies: Complete Information,” *Econometrica* 60.1992.
- 4. H. Matsushima: “Role of Honesty in Full Implementation,” *Journal of Economic Theory* 139. 2008
- 5. ――― : “Behavioral Aspects of Implementation Theory,” *Economics Letters* 100. 2008.
- 6. ――― : “Blockchain Disables Real-World Governance,” CARF-F-459, University of Tokyo. 2019.
- 7. ――― : “Epistemological Implementation of Social Choice Functions,” *Games and Economic Behavior* 136. 2022.
- 8. ――― : “Social Interaction and Epistemology in Information Elicitation,” CARF-F-549. University of Tokyo. 2022.
- 9. ――― : “Honesty and Epistemological Implementation of Social Choice Functions with Asymmetric Information,” CARF-F-548. University of Tokyo. 2022.
- 10.H. Matsushima and S. Noda: “Mechanism Design with Blockchain Enforcement,” CARF-F-474. University of Tokyo. 2020.
- 11.UTokyo FOCUS: “A Digital Court for a Digital Age,” Press Release. April 6, 2020.