ブロックチェーンへの期待と，普及へ向けた課題

楠 正憲（くすのき・まさのり）

ヤフー株式会社 CISO-Board ／国際大学 GLOCOM 客員研究員

なぜブロックチェーンに関心が集まっているのか

このところ連日のように，金融機関によるブロックチェーンや DLT（Distributed Ledger Technology：分散台帳技術）を使った実証実験やサービスの発表が相次いでいる．日本取引所グループに続いて 3 大メガバンクや地銀などが次々とブロックチェーンを利用した実証やサービスを発表した．世界を見回してもオランダ，カナダ，イギリス，中国，ロシアなどの中央銀行が，中央銀行発行のデジタル通貨について検討している．日本のソラミツ株式会社もカンボジア中央銀行の開発する電子通貨の開発にブロックチェーン技術を提供する．トヨタの研究機関である Toyota Research Institute も，プローブ情報の共有やカーシェアリングにブロックチェーンを利用する研究を進めていることを明らかにした．なぜこれほど金融当局や金融機関をはじめとした企業のブロックチェーンに対する関心が高まっているのだろうか．

無視できないビットコインの成功

もともとブロックチェーンは，ビットコインのデータ管理技術として開発された．ビットコインは運営者がいなくても機能する電子マネーシステムとして設計されており，各利用者が自由に作成したキーペアを使って取引に署名を行い，取引を束ねたブロックを P2P（Peer to Peer）で共有しながら，任意の計算ノードが参加できる計算パズルを解くプルーフ・オブ・ワーク（Proof of Work）によっ

楠 正憲
ヤフー株式会社 CISO-Board／国際大学 GLOCOM 客員研究員．インターネット総合研究所，マイクロソフトを経て 2012 年ヤフー入社．現在 CISO-Board としてセキュリティ対策，CDO-Board としてデータ戦略の立案推進に従事．内閣官房 番号制度推進管理補佐官，政府 CIO 補佐官，内閣府 CIO 補佐官として番号制度を支える情報システムの構築に携わる．一般社団法人 OpenID ファウンデーション・ジャパン代表理事，ISO/TC307 国内委員会委員長．

て取引を確定していく．

ビットコインをはじめとした仮想通貨の価値が上がるにつれて，不正によって取引記録を改ざんすることで得られる利益が増えて，様々な不正の手口が試みられるようになった．ビットコインの安全性といったときには二つの側面があり，一つは利用者から見て不正が行われているかという視点で，もう一つは決済手段としてのビットコインそのものの信頼を揺るがす，たとえば設計を超えた貨幣発行量の増加や，通貨の二重使用といった問題を引き起こさないかという視点である．

前者に関してはその時々で様々なトラブルが起こっているが，後者の通貨供給量の管理や二重使用の防止はおおむね実現されてきたことから，ビットコインの価値は維持されてきた．ここでビットコインが安全といっているのは，必ずしも利用者にとってではなく，通貨システムとしての信頼を守ってきたという意味においてである．通貨に例えれば，泥棒や詐欺を防ぐことはできないけれども，偽造されないようにはできているということだ．プルーフ・オブ・ワークが実現しているのも，最終的にビットコインの中で正しい取引の連なりを確定することであって，すべての取引を確実に実行できているわけではない．たとえば悪意ある者が二重利用を試みた取引のように，全体の一貫性を維持するために切り捨てられる取引もある．結果として善意の第三者による取引が切り捨てられることも少なくない．

ビットコインと現実の情報システムとの要件の違い

ビットコインがデータの一貫性のために割り切って取引を切り捨てることがで

きるのは，ビットコインの上位概念としての守らなければならないルールや，そのルールを執行する主体が存在せず，ビットコイン・ブロックチェーン上のデータを原本として扱うことができるからだ．銀行の勘定系オンラインをはじめとした現実のシステムにおいては，システム上の記録は現実の債権債務関係を正確に反映している必要があり，システムの都合で勝手に取引を切り捨てたり，裁判所の令状に基づく差し押さえなどに応じないことは認められない．システム上のデータは，あるべき現実に合わせなければならないところがビットコインとは決定的に要件が異なる．

たとえば破産手続きで銀行口座を凍結することは一般に行われるが，ビットコインのアカウントを凍結することは極めて難しい．ビットコインで送金を行うには，アカウントに対応したキーペアを必要とするが，そのキーペアが適切に保全されているか，後から検証することは困難である．したがってビットコインアカウントを凍結する場合，まずキーペアを保全したうえで，新たに別のキーペアを作成し，新たなキーペアのアカウント宛に送金する必要がある．そうしないと以前の鍵を保全した段階ではアカウントに残高が残っていたとしても，保全したはずのキーペアの秘密鍵が漏洩していた場合には，後から別のアドレス宛に送金できてしまう．

また不当に盗まれた仮想通貨を取り戻すことも一筋縄ではいかない．銀行口座であれば誤った送金を組み戻したり，詐欺などの犯罪を通じて得られた資金を，後から被害者に移し替えることは技術的に難しくない．しかしながらブロックチェーンは後から修正することができないため，こうした対応が非常に難しい．スマート・コントラクトの脆弱性を利用して暗号通貨を詐取した The DAO 事件の事例では，脆弱性を突いた不正送金を無効にするために，イーサリアム・ブロックチェーンのハードフォークを実施した．この際ハードフォークに反対するグループはイーサリアム・クラシック（Ethereum Classic）に分裂して，今なお両方が併存している．ブロックチェーンの特徴の一つは運営者がいなくても機能する点にあるが，合議によってハードフォークを行えるのであれば，運営者がいると考えることもできるのではないか．また，ハードフォークを認めてしまうと，改ざん不可能や発行残高があらかじめ決められているといった設計上の特徴が，軒並み後から変更可能となってしまう．

将来的には口座凍結や不正な取引の無効化，誤った書き込みの修正といった定

型的な異常系処理をスマート・コントラクトとしてライブラリー化することで，ブロックチェーンの上に現実の事務を載せることができるようになるかもしれないが，現時点では分散台帳の書き換えにはハードフォークという多数の関係者からのサポートが必要かつ，ブロックチェーンの前提を覆す副作用の大きな作業を経る必要があることは認識しておく必要がある．

ブロックチェーンは廉価でも高速でもない

ビットコインを支えるブロックチェーンは廉価で高性能な分散データベースと捉えられがちで，それ故に情報システムへの応用が期待されているが，現実的には結構なコストがかかっており，処理性能も限定的である．ビットコインは執筆時点で 10 分おきに約 10MB のブロックを生成しているが，そこに組み込まれている取引数を均すと平均 4 取引／秒となる．これは消費者向け決済を処理する容量としては極めて不十分と言わざるを得ない．そのため実際に取引がなかなか処理されず，優先度を上げるために手数料を上乗せするといったことが行われている．

また，ブロックあたり 12.5BTC が採掘者への報酬として支払われており，これを取引ごとで均すと千数百円／取引（2017 年 5 月末時点）となる．とてもマイクロペイメントには使えないし，ちょっとした銀行振込やクレジットカード手数料よりも高額だ．採掘報酬にはビットコインの通貨発行益が充てられており，実際にユーザーが負担しているわけではないが，これはビットコインのスキーム特有の仕組みであって，他のブロックチェーンを運営する場合には，運営者なり利用者がその費用を負担する必要がある．ブロックあたりの採掘報酬が一定だと仮定した場合，トランザクション単価が高いことは，処理容量が低いことの裏返しでもある．

処理容量を拡張する方法としてはブロックサイズの拡張に加えて，署名などの証跡をブロックサイズに含めない SegWit（Segregated Witness）と呼ばれる技術が提案されており，これが実現すると 20 取引／秒弱まで取引を詰め込める可能性があるが，まだ採用されていない．ビットコインの仕様を変更するために必要なハードフォークは，取り決め上 8 割の採掘者が同意する必要があるが，その同意の取り付けが遅々として進まなかったからだ．

ブロックサイズの拡張やSegWitの導入が進まない背景には，いくつかの理由がある．採掘者の多くがネット環境の貧弱な中国で採掘を行っているが，ブロックサイズが拡大すると採掘者はこれまでよりも多くのネットワーク帯域を必要とするようになる．SegWitはスケーラビリティの改善だけでなく，ブロックチェーンの外側でビットコインのやりとりを行うライトニングネットワークなどのオフチェーン取引を実現する布石でもある．オフチェーン取引が増えることでビットコインの流通速度は速まるが，採掘者に分配される送金手数料が減ることも考えられる．

ビットコインの利害関係者は採掘者だけでなく，コアの開発者や取引所をはじめとした取扱事業者，エンドユーザーと多岐にわたるものの，現時点では取引を処理する採掘者の合意なしには仕様を変更できず，採掘者はビットコイン全体のためではなく，しばしば自らの利益のために合理的な判断を行う．ビットコインがなまじエコシステムに参加する多様な主体の損得をうまくバランスさせているだけに，その仕組みをいじるためには，それぞれの協力が必要となる面もある．ブロックチェーンによってはこうしたビットコインのような利害調整を要さずに仕様を変更できるものもあるが，現実には今のところ世界で最も大きなブロックチェーンを使って実稼働しているシステムはビットコインなのである．

それでもブロックチェーンは世の中を変えるのか

これまでブロックチェーンに対する世間の過大評価を中心に論じてきた．一方で仮想通貨の価格は暴騰し，取引は活発化して，金融機関はブロックチェーンに関心を持っている．ブロックチェーンへの取り組みが，結局のところ情報システムや社会に対して何をもたらすのだろうか．計算機導入の歴史が古く，資金が豊富で情報システム部門よりも事務部門が強い伝統的な金融機関において，まず連綿と続けてきた業務があって，それを支える仕組みとして情報システムが設計されてきたのではないだろうか．

しかしながらビットコインやブロックチェーンは非常に制約が強く，その上にシステムや業務を載せようとすると，これまでと逆の順番でシステムを設計することになる．ブロックチェーンに載るデータ構造，それをハンドリングできるシステムで回せる業務という順番で設計すると，これまでとかなり違った，技術的

には効率的でバグが出にくく，外部と繋げやすいシステムを構築できる可能性がないだろうか．

システム間連携も同様で，これまでは各組織で個別の異なる情報システムがあって，それらを繋げる共通のプロトコルを設計した．そうすると各システムの内部データ構造は分断され，内部データ構造とプロトコルとを結ぶ取引処理のためのプログラムは，それぞれ別々に保守することとなる．業務をブロックチェーンに載せるということは，異なる組織間でデータ構造を共有し，複数組織にまたがる業務処理をそのブロックチェーン上で動くスマート・コントラクトとして実装し，それらと個別組織の業務を繋げる部分だけを個別に開発する構造となる．結果として組織をまたいでデータの一貫性を保持しやすく，最小限の工数で柔軟に拡張できる，ロバストな分散システムを構築できるかもしれない．

これまで情報システムのセキュリティは信頼できる相手としか接続しないことによって担保してきたが，ビットコインは不正を企む者も含む多様な参加者を受け入れつつデータの一貫性を維持できている．ネットワークの規模が拡大するほど，内と外を分けて内側のみを信頼する境界セキュリティが機能しなくなるが，ブロックチェーンであれば，これまでアクセスコントロールが難しく，割に合わなかった組織をまたいだ情報システムの構築が容易になる．

これらはかなりブロックチェーンの特徴をポジティブに表現しており，裏を返せば従来の情報システムと比べてブロックチェーンが苦手なものも少なくない．業務に合わせてシステムやデータフローを設計すること，個別システムの違いを吸収すること，データに対してアクセス管理を行うことなどをブロックチェーンは苦手としている．また参加する全ノードがミドルウェアやデータ構造を一斉に更新する必要がある．クライアント・サーバ型であれば，決められたプロトコルさえサポートしていれば情報システムを塩漬けにできるところ，ブロックチェーンを使っていると他ノードとミドルウェアのバージョンやデータ構造を合わせることを強いられるともいえる．これは従来の保守的なシステム開発にとっては，かなりのストレスになるだろう．

それでもブロックチェーンは社会を変える

ブロックチェーンのようなデータの前後関係や不変性を保障する技術はこれま

でにもあった．たとえばタイムスタンプ署名やヒステリシス署名といった技術である．P2P ファイル共有やスカイプ（Skype）などで使われているマークルツリーハッシュや分散ハッシュテーブルが，ビットコイン・ブロックチェーンの管理にも使われている．だからといってブロックチェーンが全く新しくないかというと，そうとも言い切れない．たとえばセキュリティに対する考え方や割り切りが，これまでの情報システムとは異なっており，想像力を刺激するのである．

たとえば同じ電子署名を使った技術として PKI（Public Key Infrastructure）があるが，現実社会の階層構造をサイバー空間にマッピングするために設計されており，運営者が管理する前提となっている．ビットコインでは自由にキーペアを作ることができ，プルーフ・オブ・ワークという別の仕組みで，データの真正性を保障することで，運営者を置かなくても二重払いなどの不正を防げるように設計されている．異なる制約条件に基づいて技術の取捨選択を行ったところが，ビットコイン・ブロックチェーンの設計の独自性に繋がっている．

たとえば文書の実在性を保障するだけであれば，ブロックチェーンを使わなくともタイムスタンプ署名などの技術で実現できる．しかしながら，たとえば特定の事業者が運営するサービスに依存した仕組みでは，その製品やサービスが提供されなくなったところで使えなくなってしまう．ブロックチェーンであれば自分でノードを動かし続けることで，製品やサービスの終了に振り回されずに使える可能性がある．実際にはアルゴリズムの危殆化や脆弱性対応が必要となるので，P2P だからといっていつまでも同じように使えるとは限らないが，個別の事業者やサーバに依存した仕組みよりは自前でリスクを管理できる．

実際に海外でブロックチェーン上に契約を記述するスマート・コントラクトの利用が増えた場合，ブロックチェーンの利用者に限らず電子データの法的有効性に影響を与えることも考えられる．今のところ電子署名法によって認定認証局・特定認証局の発行した証明書で署名したデータに限って，電子署名法によって文書の真正な成立が推定されるが，本来の民法の考え方では，口約束であっても当事者間の合意があれば契約として成立しているのであって，その証跡が保存されていたならば，登録された認証局の発行した証明書で署名されているか否かに関わらず裁判で証拠となり得る．

役所の委嘱状や民間の見積書，請求書をはじめとして，判子が必要なために紙が残っていて電子化できていない事務が数多くあるが，こうした事務のうち自

治体に登録された実印（登録印）での取引はごく一部で，たいがいの文書では三文判なり角印が使われている．紙の事務では民間が生産し，簡単に複製できて，役所に登録されてもいない印章が使われているのに，電子データになった途端に PKI を使わなければならない，決まった事業者の発行した証明書で署名しなければならないという誤った先入観が植え付けられてきたことによって，我が国の事務の電子化は阻害されてしまった．ビットコイン取引所マウントゴックス（MTGOX）の破綻や，The DAO 事件のように，海外で運営されているブロックチェーン上での金銭取引やスマート・コントラクトでの契約が増えたならば，本来の民法の考え方である当事者間の合意と証跡の証拠力に基づく紛争解決が求められる．結果としてブロックチェーンだけでなく，迷惑メール対策として電子署名技術に取り組んできた電子メールなど，様々な電子データの法的証拠能力を再検討する契機となるかもしれない．

しかしながらブロックチェーン上での取引やスマート・コントラクトの法的有効性を問うことは，ブロックチェーンにとって諸刃の剣にもなり得る．前述したように現行のブロックチェーンは，法律が求める差し押さえや，民法上の不法行為や錯誤があって契約が無効になった場合の取り扱いをハンドリングする仕組みを持たない．ビットコインも含めて法執行当局が取り扱いに苦慮するなかで，コードそのものによって契約を自動執行することによって，法執行がない状態でも私的自治で契約を執行する仕組みを築き上げてきた．国境を越えた取引や違法ドラッグなどの違法な取引においては，裁判による紛争解決が難しいことから，こうした私的自治が選択され，それなりに機能してきた．しかしながら運営者が法的責任を負う情報システムにおいては，こうした私的自治だけでなく，法に基づく対応を行う必要が生じる．ブロックチェーンにおける改ざんの難しさは，こうした例外処理への対応の難しさともなり得る．

このようにブロックチェーンの実社会での活用は始まったばかりだが，ユースケースが広がっていくほど，実社会での多様なニーズや法的要請に直面することになるだろう．こうした課題を乗り越えるためにデータの証拠力や取引・同意の有効性について考え直すことは，ブロックチェーンの利活用促進だけでなく，社会全体のデジタル・トランスフォーメーションに資するのではないだろうか．