



⑥ ブロックチェーン、分散レジャー 技術と社会の未来

—空中約束固定装置のある暮らし—

齊藤賢爾（慶應義塾大学／（株）ブロックチェーンハブ）

ブロックチェーンとは何か

まずはじめに、ブロックチェーンとは何か、改めて振り返るとともに、本稿がブロックチェーンという用語で指し示す範囲を明確にしたい。

● 分散タイムスタンプサービス

ブロックチェーンは、2008年、匿名の開発者サトシ・ナカモトにより、デジタル通貨システム「ビットコイン」を実現するための分散タイムスタンプサービスとして提案された。

ビットコインは、管理者のいない環境下で電子的に表現されたコインの制御権^{☆1}の移転、すなわち送金を実現することを目標に設計されている。送金の取引は入金（入力）と出金（出力）の間の関係を記述するが、ビットコインでは、未使用の取引出力がコインであるとするいわゆる UTXO（Unspent TX^{☆2} Output）構造（図-1）を用いて電子コインのデジタルデータ形式を定義している。

この構造は、適切な秘密鍵を用いて取引にデジタル署名できる主体だけが送金できることを保証するが、署名の検証に必要な情報（公開鍵）をデータ構造の中に埋め込み、公開鍵のメッセージダイジェスト（ハッシュ値）をコインの送金の宛先とすることで、まったく関係のない第三者でも公開鍵の正当性を確認でき、取引の形式的な正しさを検証可能にした点で画期的である。

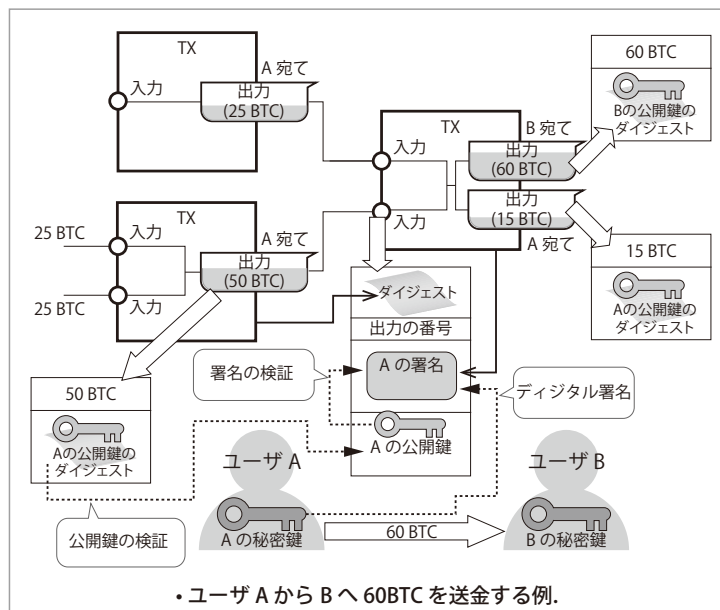


図-1 ビットコインのいわゆる UTXO データ構造

ところが、デジタル署名だけでは同じコインが二度使われるような不正があっても検出できない。「二重消費（double spending）」と呼ばれるこの問題を解決するための方法は色々あるが、一度使われたコインを使用済みとして記録するべく、全取引を時間軸で一覧になるように固定し、その順序関係が参加する全員にとって一致するようなタイムスタンプサービスを使うという単純な発想も可能である。この発想がビットコインと同時に発明されたブロックチェーンの基本である（図-2）。

この言わば第1世代のブロックチェーンでは、取引群を格納する各ブロックのヘッダ部に、直前のブロックのダイジェストを置くことにより前後の関係を明確にする^{☆3}が、前のブロックから受け継がれるターゲット値^{☆4}以下のダイジェストが得られる

☆1 一般に貨幣は公共財であり、私的に所有されないが、持ち主は次にそれをいつ誰に渡すかを制御できる。

☆2 TXはトランザクション（transaction）の略。

☆3 この構造をハッシュチェーンと呼ぶ。

☆4 ビットコインでは、ブロック間の間隔が平均して10分間になるように2016ブロックごとにターゲット値を調整している。

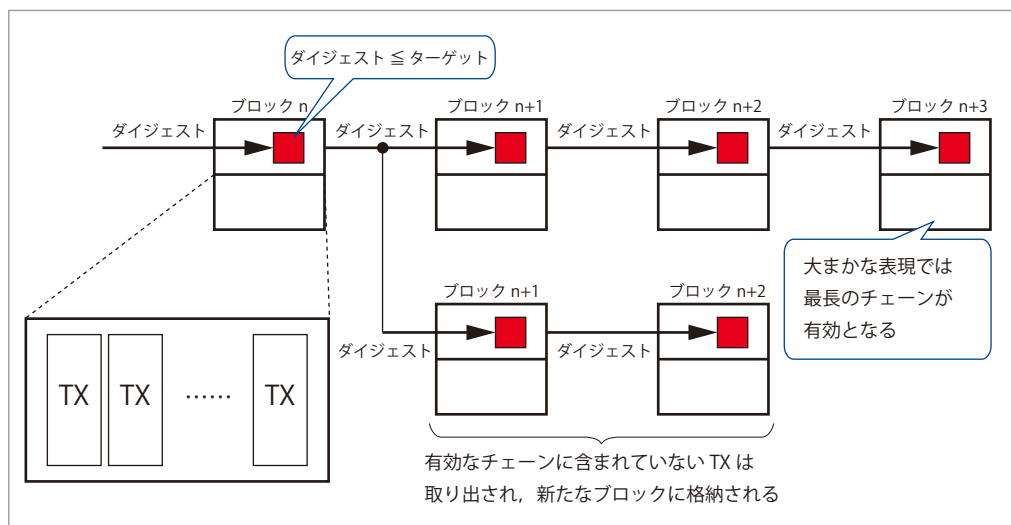


図-2
第1世代のブロックチェーン

ようにブロックのデータを構成しなければならないという、作業証明（proof of work）の仕組みによって改ざんを抑止している。

ネットワークに対するブロックの提案は自律分散的に行われるため、条件を満たす別々のブロックが複数の参加者から同時に提案され、参加者がそれぞれ独自の判断でそれらに続くブロックを繋げていき、結果としてチェーンが分岐していくことがある。順序が一意に定まらなければ二重消費の問題を解決することにならないので、ビットコインでは、作業証明のコストがより多く支払われてきたチェーン（大まかには、より長く延びているチェーン）を全員が採用するというコンセンサス機構（ナカモト・コンセンサス）を備えている。

本稿における「ブロックチェーン」は、こうした第1世代のブロックチェーンの特徴を踏襲しているものを指す。

ブロックチェーンを理解する

技術は、問い（要求）に対する答えであるので、ある技術を理解するためには、まずその問いを理解する必要がある。ビットコインの問いは、「自分が持っているお金をいつでも自分の好きに送金することを誰にも止めさせないためには？」というものであり、そのほかのブロックチェーンや、より一般化した概念であり後述する分散レジャー（distributed

一般モデル	ビットコイン (◎で囲んだ部分は筆者による評価)
アプリケーションロジック スマートコントラクト	⇒ BTC（ビットコインの単位）の量の 移転のためのロジック（ビットコインでは固定）
コンセンサス機構 トランザクションとしての確定に向けて	⇒ ナカモト・コンセンサス （よりコストが投入された履歴が有効） 《後追いでしか有効性を判断できず実時間で動かない》
分散タイムスタンプ 相対時刻を定義する、証明の基盤	⇒ 作業証明を課したハッシュチェーン 《計算コストを大規模に投入すれば誰でも覆せるため 想定されていたほど強固ではない》
レジャー構造 誰もが制御を持って、自己充足構造で検証可能	⇒ いわゆる UTXO 構造 《有益だが秘匿性を持たない》

図-3 ブロックチェーン／分散レジャーの階層構造

ledger：分散台帳）技術にも適用可能なように汎用化すると、「アセット（資産）の制御の権限を中央ではなくエンド（端点）が持つには？」となる。

図-3は、そうした問いに答える技術としてのブロックチェーンや分散レジャーを理解するために、その機能を階層構造として整理したものである。

こうした構造を持つことで、ブロックチェーンは、言わば「空中に約束を固定する装置」として機能する。ビットコインで言えば、約束とはコインの宛先だけがそのコインを送金できるというものである。約束がどの主体にも属さず、空中で維持されていることにより、エンドが権限を持つことを保証でき、かつ、常時ネットワークに接続しているわけではなく間欠的にシステムに参加するような主体にも対応できる。

以降、ブロックチェーンや分散レジャーのこの性質に言及する際は、「空中約束固定装置」という用

語を用いる。

ブロックチェーンへの期待と課題

ここで、ブロックチェーンの期待される応用について述べ、ブロックチェーンが抱える技術とガバナンスの諸問題を明らかにした上で、そうした問題の解決・解消に向けたヒントを紹介したい。

● 期待されている応用

後述するハイパーレジャープロジェクトでの整理の仕方に倣って、ブロックチェーンについて期待されている応用を列挙する。

金融アセット管理

仲介を不要とする直接アクセス、合意された実時間内の決済、ビジネスルールの記述・埋め込み、秘匿性の制御等が期待されている。このうち、実時間性や秘匿性については第1世代のブロックチェーンでは対応できない。

企業行動（特に財務上の意思決定）の自動化

株式分割、減資・併合、株式移転・交換、合併、第三者割当増資等の実時間での実行と秘匿性の制御が期待されている。同様に、実時間性や秘匿性については第1世代のブロックチェーンでは対応できない。

サプライチェーン管理

材料のトレースバックや、生産・貯蔵から販売までの記録と検索機能の提供が期待されている。

マスターデータ管理

権限を持つ者のみが更新でき、指定された検証者がそれを承認する仕組みが期待されている。

シェアリングエコノミーとIoT (Internet of Things)

信用が必ずしも確立していない状況下でのスマートシティ、交通、ヘルスケア、リテール、建築、教育等への応用が期待されている。暗に実時間性や秘匿性についての期待があるが、第1世代のブロックチェーンでは対応できない。

● スケーラビリティの課題

実時間性や秘匿性の欠如に次ぐ技術的な課題の代

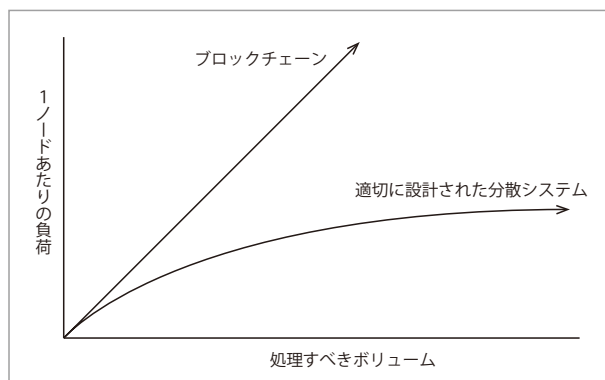


図-4 スケーラビリティの課題

表例として、システムがスケールアウトしない、すなわち、ノードを追加することでは性能上の問題を解決できないという課題がある。

ブロックチェーンでは、全機能を有するノードの各々がブロックチェーンのデータ全体を処理するため、取引の増加に伴い、データ構造を維持するためのコストが直線的に上昇する（図-4）。

ただし、ブロックチェーンを実装するためには、ハッシュ値をキーとするブロックや取引の検索機構を備える必要があるため、それを KVS (Key-Value Store) だと捉えれば、既存の分散 KVS の手法を用いた改良の余地があると考えられる。

● ワンネスの罫

ブロックチェーンは、大規模災害や政変などによりネットワークが分断されると、チェーンが安定的に分岐することになり、唯一の正しい歴史が保たれるという大前提が崩れ、正しく動作しない。「世界が1つ」でなければ動作しないというこの性質を、以降は「ワンネス (oneness)」と呼称する。

「分散」の考え方と真っ向から対立するかたちとなるワンネスがもたらす重要な帰結は、技術を進化させるガバナンスが利きにくいということである。ブロックチェーンでは、インターネットのその他のアプリケーションでは普通に行われている、「一部で違うことを試して、うまくいったら全体で採用する」ということができない。一部が異なる仕様で動くとチェーンが分岐してしまうからである。すると、現実への適用性を実地で評価しながら技術を

進化させていくことが困難になる。めまぐるしく変化する技術的・社会的状況の中で、実際に使われていく技術を維持していくためには、この困難性は致命的となる。

● 課題の解決・解消に向けたヒント

ブロックチェーンのスケールアウトの困難性とワンネスがもたらす問題には共通の要因がある。それは、分権できない構造による欠点だということである。逆に、分権できるかたちで同様の技術を実現することには、大きな期待と可能性がある。

分散レジャー技術の動向

ここで、ブロックチェーンを分散レジャーの一種として捉え直し、現在開発途上にある一連の技術について動向を見ていきたい。

● 問いの立て直し

前述のように、技術は問いに対する答えであるので、問いを立て直すことにより、それを解くための技術を改めて考えることができる。分散レジャーを「空中約束固定装置」として捉えるならば、その技術への問いは以下である。

Q1：空中とはどんな範囲か。

Q2：その空中にどうやって約束を固定するか。

分散レジャーの設計では、これらを各々のアプリケーションの文脈の中で問うことになる。

● さまざまな分散レジャー技術

ハイパーレジャー (Hyperledger)

ハイパーレジャーはリナックスファウンデーションにおけるプロジェクトであり、多くの企業による貢献で成り立ち、複数の汎用の分散レジャーをオープンソースで開発している。

その中の1つである「ファブリック (Fabric)」は、コンセンサス機構について、既存の耐ビザンチン障害^{☆5} プロトコル (BFT: Byzantine Fault Tolerance) の応用を基調に置いている。

BFTではノードの総数 n が既知である必要がある。その意味で「空中」を完全なるパブリックかつオープンな空間にはできない。しかし、ビジネス応用の多くにおいては、それはむしろ望ましい性質と言えるかもしれない。

コーダ (Corda)

コーダは金融系の分散レジャーとしてR3 Consortiumにより開発されている。コーダの問いは、金融上の契約に関し、「私が見ているものはあなたが見ているものと一致しており、我々はどちらもそのことを知っていて、かつ監査にも同じものが見えていると知っているという状態をいかに作り出すか」というものである。その意味で「空中」とは契約の当事者たちおよび監督者がかかわる範囲であり、コーダでは全体のコンセンサスという概念を捨てていると考えられる。

タングル (tangle)

タングルはIoTへの適用を見据えた分散レジャーであり、ブロックという概念を捨て、取引が個別に過去のいくつかの取引を承認する有向非巡回グラフの形態を採る。すなわち、ブロックチェーンが取引の全順序を形成・維持しようとするのに対し、タングルでは半順序を形成することになる。「空中」は単一の空間ではなく、枝分かれし、分権のための構造をもち得る。

来たるべき社会変容

ここで、ブロックチェーンや分散レジャー技術が社会にどんなインパクトをもたらしつつあるか、そして未来においてどう発展するかを考えたい。

● 人類史における転機

「約束」は人間社会の基礎であり、「空中約束固定装置」により、人が約束を結びそれを実行に移していくやり方が変わっていくとするならば、そうした、社会を下支える基盤の変化による影響を受けるの

^{☆5} ビザンチン障害は、プロトコルからの任意の逸脱であり、共謀なども含み障害の種類について前提を置かない。

は、何も金融機関だけに限らない。一般化するならば、人々が共同で何かをしたり業を起こす（起業する）方法が変わっていくことになる。

現在、起業と言えば会社づくりであるが、人類史に残る会社の代表格は「東インド会社」だろう。これは初の株式会社と言われる。すなわち今、人類史に残っているのは、現在の会社の仕組みの起点となる会社なのである。とすれば、次に人類史に残る会社は、近代的な株式会社を終焉させる形態を採ることになるだろう。

そのような会社のかたちとして有力だと筆者が考えるのが「自律分散組織（DAO：Distributed Autonomous Organization）」、すなわち、経営が自動化された組織である。実は、たとえばビットコインはDAOの具体例だと言われる。ユーザを株主、コインを株式、ブロックチェーンを維持する参加者であるいわゆるマイナー（採掘者）たちを従業員と考えれば、ビットコインのプロトコルは、株式の移転を業とするその組織の経営の仕方を記述していると思えることもできるからである。

DAOのような考え方を一般化すると、「法」を技術の提供者が定義するということになる。ただし、Lawrence Lessig（サイバー法学者）がかねてから指摘している通り、コンピュータソフトウェアには元々そういう力があると考えられる。

● 地球規模 OS

筆者は、2007 年頃、仲間らとともに「地球規模オペレーティングシステム（OS）」の概念を提唱した（図-5）。これは、地球上の資源と人間との関係をコンピュータとユーザとの関係になぞらえ、現在はOSに当たる金融・貨幣経済システムを時代遅れにし、人類が真っ当に資源の共有・共用を行うための基盤である。地球規模OSは、人々がアプリケーションとして新たな業を起こすための基盤として、何らかの決済システムを内包し、かつ、プログラミング言語・プログラミング環境を内包することになる。そして、人的資源を含む地球上の資源の会計システムを提供し、人々はその上で新たな「法」を

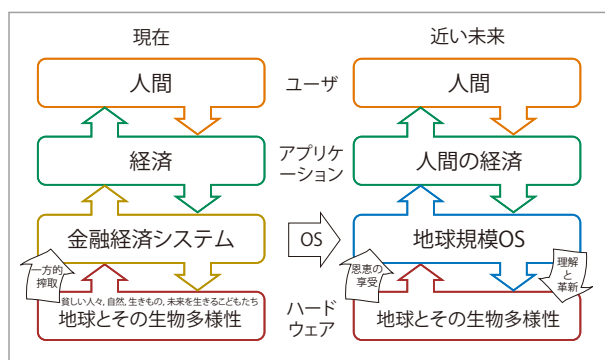


図-5 地球規模 OS

定義できることになる。

こうした基盤づくりへの道は、地球規模OSという言葉で呼ばれるかは別として、すでに始まっているようにも思える。

現在はまだ、社会を変えたい、と考えたときに人々が起こす行動として、「選挙に立候補するなどして政治を志す」「公務員になって行政に参加する」「起業する」あるいは「非営利活動を立ち上げる」といった方法がばらばらに存在している。すなわち、政府、営利企業、非政府／非営利（NGO/NPO）というセクタが独立している。ところが、各種のハッカソンに代表されるように、これらの方法やセクタを統合するかのように、「アプリをデザインして社会に投入すると、そのエージェントとして人々が働くことで社会の課題が解決される」という道筋ができ始めている。

この道筋は、ブロックチェーンの動向とも無縁ではなく、オープンソースで開発が進められている「イーサリアム（Ethereum）」は、第1世代のブロックチェーンの課題に対しある程度の取り組みを見せると同時に、そこにプログラミング言語を載せ、分散アプリケーション、特に履行が自動化された契約としてのスマートコントラクトを開発・実行するためのオープンな基盤として作られている。

● サイバーフィジカル社会

本当に社会のインフラとしてスマートコントラクトが使われていくためには、物理的な世界との接続はどうしても必要である。たとえば、遺言を自動的

に実行するためには、システムが「人の死」という契機を正しく捉えることが必須となる。カーシェアリングで用いられるためには、運転免許証や乗用車のキーとシステムが接続される必要がある。

これは、スマートコントラクトの実用化には、「サイバーフィジカル (cyberphysical)」な環境が前提になるということを意味する。サイバーフィジカルとは、広く捉えれば、さまざまなセンサ (検知器) / アクチュエータ (駆動装置) や、スマートフォンなどの携帯デバイスや、あるいは法制度などによって、人間の生活環境を支える社会インフラとコンピュータネットワークとが互いに密接に繋がっていることを指す。

そして、一人ひとりがスマートフォン等を持ち歩き、情報環境と常に密接に繋がりながら生きている現在、我々は、すでにサイバーフィジカル時代への入口に立っていると言えるのである。

スマートコントラクトは、生活空間におけるプロセッサの数ほどもあるかもしれない。エアコンや電子レンジといった世の中に存在するすべての家電や、乗用車、時計、ロボット、電車、航空機、あるいはエレベータなど、コンピュータを内蔵するありとあらゆるものが、将来的にはスマートコントラクトに基づいて挙動を決めるかもしれない。

「空中約束固定装置」としてのプラットフォームは、そうしたサイバーフィジカルな世界を前提にすると同時に、サイバーフィジカルな世界のための基盤になり得るのである。

分散レジャー技術と社会の未来

まとめとして、今後我々が課題とどのように向き合い、どのような社会の変化を目撃することになるのか考えたい。

● 露見したガバナンスの課題

2016年6月17日、イーサリアム上に作られた自律分散投資ファンド The DAO のコードの脆弱性が突かれ、360万 ETH (50～60億円相当) という

デジタルコインが盗難に遭った。イーサリアムの開発・運用コミュニティがこの事件に対処するための選択肢としては、チェーンの互換性を維持して窃盗犯のアドレスのみを凍結する (ただし盗難された資金は戻らない) といった手段もあったが、結果として「盗難がなかったことにする歴史の書き換え」が選択され、7月20日に実行された。これは強権発動とも言え、それを支持しないユーザたちが書き換え以前のチェーンの継続使用を固持する分裂騒ぎが起きるなど、ブロックチェーンにおけるガバナンスの課題を浮き彫りにする結果となった。

● 自動化される未来へ

そのように、技術が実際に社会で使われていく中で、課題を明らかにするさまざまな事件が起きていく一方で、約束は本来的に空中に置かれる必要があるし、ブロックチェーンが可能にするとされる世界には、やはりインパクトがある。

自動化は、今後発展する人工知能の助けを得て、社会のあらゆる場面に浸透していくと思うが、知力の面で人間を凌駕し得る人工知能は、いつどのようになり人間の社会が定めたプロトコルを逸脱するかも分からず、社会という分散システムにおける潜在的なビザンチン障害ノードであるとも言える。そうした相手との約束をどう結んでいくかということも、今後は考えていかなければならないだろう。

ブロックチェーンや分散レジャー技術とそのガバナンスには課題が山積しており、現在のかたちからの変化は免れない。しかし、空中に約束を固定するための何らかのプラットフォームが、未来社会における自動化の基盤として大きな役割を果たしているだろうことには間違いなさそうである。

(2016年9月7日受付)

齊藤賢爾 ks91@sfc.wide.ad.jp

1993年、コーネル大学より工学修士 (計算機科学)。2006年、慶應義塾大学より博士 (政策・メディア)。現在、同大学 SFC 研究所上席所員および (株) ブロックチェーンハブ CSO (Chief Science Officer) としてインターネットと社会の研究に従事。