BCG

THE BOSTON CONSULTING GROUP

ブロックチェーンの経営戦略

THINKING OUTSIDE THE

BLOCKS

ボストン コンサルティング グループ（BCG）

BCGは、世界をリードする経営コンサルティングファームとして、政府・民間企業・非営利団体など、さまざまな業種・マーケットにおいて、カスタムメードのアプローチ、企業・市場に対する深い洞察、クライアントとの緊密な協働により、クライアントが持続的競争優位を築き、組織能力（ケイパビリティ）を高め、継続的に優れた業績をあげられるよう支援を行っています。

1963年米国ボストンに創設、1966年に世界第2の拠点として東京に、2003年には名古屋に中部・関西オフィスを設立しました。現在世界48カ国に85拠点を展開しています。

http://www.bcg.com/

BCG

THE BOSTON CONSULTING GROUP

ブロックチェーンの経営戦略

Philip Evans

with

Lionel Aré

Patrick Forth

Nicolas Harlé

Massimo Portincaso

《日本の読者の皆さまへ》

本稿は、ブロックチェーンという破壊的技術が企業経営全般にどのような影響を与えるか、経営者は今後の事業戦略を考える上で何に留意するべきかについて示した論考です。英語版が発表されたのは2016年の12月ですが、年末までの1カ月でBCGグローバルの出版物サイト「bcg.perspectives」における年間最多ダウンロードを記録しました。この分野への各国経営リーダーの関心の高さをうかがい知ることができます。

我が国でも、デジタル技術を活用した新たな金融モデル/サービスを立ち上げようとする、「フィンテック」の動きは大きな注目を集めており、金融業界内外でフィンテックをいち早くビジネスに取り入れようという動きが活発です。ブロックチェーンはこのフィンテックのなかでも、中長期的に突出した変革力を持つ技術だと言われています。筆者らは、ブロックチェーンの変革力の本質は何かという問題意識から出発し、金融実務者、ベンチャー企業、アカデミック等との具体的なプロジェクトや対話を通じてその戦略的意味合いを導出することを試みました。

ブロックチェーン技術はもはや未来ではなく現実です。その破壊的な革新性は、仮想通貨や金融サービスの枠をはるかに超えています。筆者らは、本質的な問いは、ビットコインが通貨として成功するかどうかではなく、そのベースとなるブロックチェーンに関する基盤技術が仮想通貨「以外の」分野にどう応用されるのか、であると言います。

本稿が、金融業界にとどまらず、日本のさまざまな業界の経営のリーダーの皆さまに対し、「既存の型を越えた(Out of the block)」、未来を踏まえた現実の経営戦略を構築していく上での新しい見方を提示できればと願っています。

ボストン コンサルティング グループ
パートナー&マネージング・ディレクター　佐々木 靖
パートナー&マネージング・ディレクター　山井 康浩

目　次

はじめに

ビットコインという言葉がビジネス一般の世界で認識され、たびたび会議の場に登場するようになったのはつい最近のことだ。それは、ブロックチェーンという技術的な枠組みのなかで広く認知されるようになった。テクノロジーの未来についてのベストセラーで知られるドン・タプスコットは、「(ブロックチェーン技術ほど)人類にとって大きなポテンシャルを持つ技術は見たことがない」と語る。グローバル企業でも、ブロックチェーンが潜在的に持つ破壊的なパワーが経営レベルでの検討事項となり、各事業分野でブロックチェーンがもたらす変革についての調査が始まっている。だが、ブロックチェーンをめぐる動きは非常に複雑で、ビジネスにおける本質的な役割について理解するのは困難である。

ビットコインやブロックチェーンの本質を理解するカギは、これらの技術がビジネスに与える影響について戦略的に分析することにある。

過去数十年間における最も破壊的なイノベーションであるパソコンとインターネットには、いくつかの共通点がある。両者とも、新たに生まれた安価なリソース——前者は演算能力、後者は帯域幅——を惜しみなく使うことで、まったく新しい価値を実現したという点である。そして今、デジタルトークンとブロックチェーンという相互補完的な技術は、安価なストレージ(補助的記憶装置)を大量に消費することにより、データに現実世界の資産と同様の「連続性」を実現させた。

ビットコインは、ブロックチェーンがもたらすイノベーションの端緒となるアプリケーションに過ぎない。ブロックチェーンに関わる技術はまだ完成には程遠いが、将来的には、現実世界の多くの取引——商取引、医療、IoT(モノのインターネット)など——に、長期的かつ破壊的な影響を与える可能性がある。また、これらの技術は、現実世界

のさまざまな分野で取引を仲介してきたプレーヤーの担う役割に、大きな影響を与える可能性を秘めている。

本稿では、ブロックチェーンとデジタルトークン、そしてそれらが基盤とするスタック構造が、「取引コスト」と「信用」をめぐる経済原理をどのように変化させるかを概説する。本稿の狙いは、企業のリーダーが実行すべきことを事細かに説明することではなく（すべてのビジネスは唯一無二であり、悪魔は細部に宿るものだ）、企業の経営者の方々が以下のような問いに答えるための戦略的視点を提供することにある。

- 自社のビジネスのなかで、ブロックチェーンによって顧客から見た価値が失われる可能性があるものはどの領域か。また、それが発生する可能性はどの程度か。

- 発生する可能性が高い場合、他者に先んじて既存ビジネスを再検討・再構築するには、どうすればよいか。

- 新たなプロダクトやビジネスモデルを構築するに当たり、ブロックチェーンが実現するデジタル世界における連続性の利点をどのように活用できるか。

- ブロックチェーンベースのソリューションに優位性がある場合、自社だけで取り組むべきか、それともスケールを重視し他社と協働すべきか。

まず、そもそもの始まりであるビットコインから議論を始める。

1. 基盤技術としてのブロックチェーン

2014年冬、ウクライナは革命の瀬戸際にあった。キエフの反体制派は、テレビカメラに向かってサインボードを掲げて資金援助を求めた（図表1）。ボードにはQRコードが表示され、支援者がそこから反体制派にビットコインを寄付できるようになっていた。世界中の何千もの人々が自分の携帯電話のカメラをテレビに向けて、文字通り3クリックで寄付をした。操作は20秒以内に完了し、寄付した金額の1%にも満たないわずかな手数料で10分以内に承認された。寄付者は匿名の人々で、政府が監視することはできず、寄付を受けた人が感謝すべき相手を知ることもなかった。

図表1

ビットコインによる支払いは、直接的、匿名で、取り消し不能である。これは、ウクライナの反体制派にとっては極めて理想的なものである

資料提供：OLGA BONDARCHUK.（掲載許諾済）

銀行経由で寄付をすることもできたが、その場合は送金先の銀行口座(持っていればの話だが)の情報を、自らの身を危険にさらしながら開示する必要がある。手数料は10%かそれ以上かかる場合もあり、手続きの完了までに3~4日を要する。もちろんペイパルを使えばより早く低コストだが、ウクライナ政府はこれを禁止していた。ビットコインでの支払いは直接的で匿名性があり、取り消しができないものだ。それはまさに、キエフの独立広場を通りかかった人が、運動に共感してプラスチックのコップに2グリブナを投げ入れるようなものである。

これは単なるたとえ話ではない。ビットコインはデジタルな無記名証券であり、所持人と管理人が一致している。ビットコイン「口座」を作る必要はなく、ちょうどポケットにお金を入れておくように、単純にビットコインを保有することができる。紙幣や硬貨と同じで、失くしたり盗まれたりすることもあり、取引は取り消し不可能である。ビットコインは従来の支払い方法の10倍も効率的な交換手段になりうるが、既存の通貨(不換通貨)と交換する際のコストを含めると、必ずしも安価とは限らない。むしろ、ビットコインの革命的利点は、効率性やコストではなく匿名性である。

自由主義者のなかには、ビットコインを「デジタル・ゴールド」、つまり、中央銀行や金融機関の都合によって発行されたり価値が低下したりする既存の通貨に最終的に取って代わる、公正でグローバルな通貨だととらえる者がいる。しかし、JPモルガン・チェースCEOのジェイミー・ダイモンが繰り返し指摘するように、もしビットコインが既存の通貨に取って代わる存在に近づけば、中央銀行がその阻止のために介入することはほぼ間違いないだろう[1]。従って、通貨としてのビットコインは、決済システムの小さな隙間を埋める存在とならざるを得ない。卓越した発明ではあるが、活用範囲は極めて限定的だ。

経営戦略的視点でビットコインをとらえると、通貨としての重要性よりも、それを支える2つの基盤技術、すなわち、デジタルトークン(この場合はビットコイン)とブロックチェーンを初めて実用化した事例

としての重要性のほうが大きい。デジタルトークンは仮想通貨である必要はない。あらゆるデジタル資産や、あらゆる有形資産をデジタル情報で表現したものがトークンになりうる[2]。そして、ブロックチェーンは、あらゆる種類の取引において、安全で信用できる改ざん不可能な「分散型台帳」の役割を果たすことができる。

そのため、本質的な問いは、「ビットコインが通貨として成功するかどうか」ではない。デジタルトークンとブロックチェーンという2つの基盤技術が、どのような形で仮想通貨「以外の」分野に応用されるのか、である。

ブロックチェーンの可能性は、金融サービスの枠をはるかに超える。サプライチェーンの管理、土地登記、医療記録、少額取引、そして世界中の何十億台ものスマート・デバイスを活用したスマートコントラクト(契約の自動化)なども視野に入ってくる。

ベンチャーファンドや企業は、これらの技術で産業全体に破壊的変化を起こすこと、あるいは、そのような変化を阻止したい既存の企業に自社のサービスを売り込むことを目指し、これまでに10億ドル以上の資金を投じてきた。

このように、決済のみならずあらゆる産業に破壊的影響を与えうるブロックチェーンは、どのような原則を基盤としているのだろうか。

ビットコインとブロックチェーンの仕組み

ビットコインとブロックチェーンは、2つの暗号化手法、すなわち「ハッシュ」と「公開鍵/秘密鍵」暗号を基盤としている。これらは、個人情報の安全な送受信やオンラインストアで既に活用されている技術である。

ブロックチェーンの基盤技術：ハッシュ関数と、公開鍵/秘密鍵暗号による電子署名

- 「ハッシュ」は関数の1つで、任意の長さのデータを入力すると、特定の決まった長さの数値を出力するものである。ハッシュ関数は一方向性の関数であり、データからハッシュ値への変換は簡単だが、ハッシュ値から逆算して元のデータに戻すことは不可能である。ハッシュは文字列を要約する効率的な方法として用いられている。また、この関数は非常に精緻に設計されており、入力値が少しでも変更されると、まったく異なるハッシュ値が出力されるという性質を持っている。

- 「公開鍵/秘密鍵」は暗号化手法の一つであり、公開鍵でデータを暗号化し、公開鍵と対になる秘密鍵で復号するというものである。暗号化に必要な公開鍵は、信用できる方法で全世界に公開されるが、もう一方の秘密鍵は非公開だ。データの送信者が受信者の公開鍵でメッセージを暗号化すると、受信者だけが自分の秘密鍵でそれを復号できるため、安全にメッセージを送信できる。

また、公開鍵/秘密鍵暗号は、電子署名の基盤技術としても活用されている。送信者が、ドキュメント（より正確にはドキュメントのハッシュ値）を自身の秘密鍵で暗号化し、元の文章に添

付して送付する。受信者は、送信者の公開鍵を使って暗号化されたドキュメントを復号し、元の文章(のハッシュ値)と比較する。両者が同一であれば、対になる秘密鍵の持ち主がそのドキュメントを送ったことが確認できる。このように、公開鍵と秘密鍵のペアを使用することにより、ドキュメントの送信者が本人である(秘密鍵を所有している)ことを確認するのが、電子署名のメカニズムである。

電子署名の連鎖(チェーン)による、過去の取引履歴の保証

ビットコインは電子署名の単純なシークエンス(連鎖)である。すなわち、1つ1つの電子署名が、ある保有者から次の保有者への送金を認証する。具体的には、送金者は自分の秘密鍵を用いて、送金記録に署名する。受け手は、送金者の公開鍵を用いて受信した送金記録を検証し、送金情報が有効であることを確認するのである。

上述のビットコインの送金(取引)の記録には、直前の取引のサマリーをハッシュ化したものが含まれる。従って、ある取引の記録がハッシュ化されて次の取引記録に正しく組み込まれているかどうかを誰でも確認できるため、送金記録をそのコインの出現時までさかのぼって追跡することが可能だ。このように、ビットコインそのものに含まれる過去の取引情報が、その「祖先」を保証するのである。

ブロックの作成と「プルーフ・オブ・ワーク(PoW)」による取引の認証

しかし、ビットコインの過去の取引履歴が保証されたとしても、有効なビットコインが二重に支払われることは阻止できない。何らかの方法で、二重払いが行われていないことをチェックす

る必要がある。

ここで活用されているのは以下の仕組みである。まず、発生した取引は、有効な取引の記録のまとまりである「ブロック」の作成を目指して競争する「ノード（ネットワークの結節点の意）」たちのオープンネットワークに向けて配信される。すると、各ノードが、ソフトウェアを通じてビットコインの履歴をチェックして、送金者がまだそのビットコインを使用していないことを確認するのである。新規のブロックは10分に1つのペースで生成され、通常200の取引の記録を含む。次のブロックには前のブロックのハッシュ値が含まれるため、ブロックは連続的な「ブロックチェーン」を形成する。このようにしてブロックチェーンは「子孫」を保証するのである。

ブロックは、生成後まもなく変更不可能になる。なぜなら、すべての後続ブロックのハッシュがそれに依存して生成されるためだ。取引の記録を書き換えようとすれば、すべての後続ブロックを――ネットワークの他の部分で新たなブロックが生まれる前に――再計算しなければならない。

ノードマシンの保有者は、ビットコインの「マイナー（採掘者）」と呼ばれ、新たなブロックを作り出す「競争」を動機として取引を認証する役割を担う。競争の勝者は、新たに発行された12.5ビットコインを獲得する。約5,700のノードが同時に稼動しているため、不正や同期の遅れによって矛盾が生じる可能性があるが、これに対処するために、ノードは必ず「長い方のブロックチェーンを優先する」という、単純な規則に従う。これはいわゆるコンセンサスメカニズムである。各ノードの相互の信用関係は不要である。各ノードは、ブロックが孤児化する（チェーンの長さにおいて少数派となること）と、報酬が自動的にキャンセ

ルされると認識している。そして、他のすべてのノードもそれを知っていると認識している。そのため、彼らにとって、コンセンサスに従うことには合理性がある。外部機関の指示や法的義務、利他的な動機に頼るのではなく、ブロックチェーンのプログラムそのものが、ポジティブ・サム・ゲームを定義する。

ビットコインの採掘、すなわち取引の認証のため、採掘者は膨大な演算を総当たりで実行することが求められる。その際、1ブロックにつき平均1万テラハッシュを計算する必要がある。ポイントはこの非効率性だ。この仕事量、いわゆる「プルーフ・オブ・ワーク」が、システムを不正に操るコストを引き上げているのだ。ブロックの書き換えやサービス妨害を目論んで攻撃を行おうとすれば、ネットワークの51%に当たる膨大な計算能力を支配する必要がある（前述のとおり、ブロックチェーンは多数決原理に依拠しているため、不正なチェーンが採用されるためには、ビットコインの採掘に使用されている全世界の計算能力の過半数を支配する必要がある）。そのような不正を画策するよりは、取引を認証してビットコインを採掘するほうがビジネスとして合理的なのである。

1. “Jamie Dimon: You’re Wasting Your Time with Bitcoin,” Fortune, November 4, 2015を参照。動画はhttp://fortune.com/video/2015/11/04/jamie-dimon-youre-wasting-your-time-with-bitcoin/。
2. 決済と無関係のブロックチェーンでも、有効性の確認作業をしたノードへの報酬として、デジタル通貨を必要とすることがある。

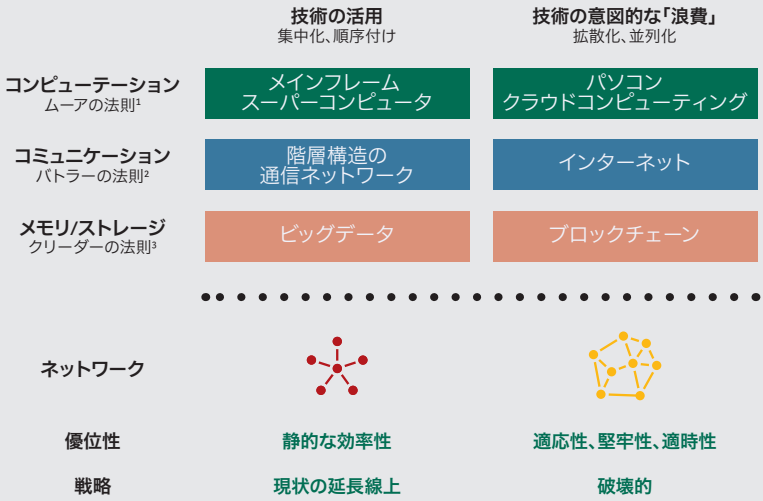
2. ブロックチェーンは、ストレージの大胆な「浪費」が実現したイノベーションである

ブロックチェーンとデジタルトークンは、安価なストレージを意図的に浪費することによって、破壊的イノベーションをもたらしている。これは、これまでの情報革命の歴史の「第3章」に位置づけられるものである。

過去50年間の情報革命は、演算性能、通信性能、メモリ（主記憶装置）/ストレージという3つの要素における、コスト低下、スピード向上、キャパシティ増加の指数関数的な進行が後押ししてきた[3]。企業は、これらの情報技術の急激な発展を2つの方法で活用してきた。第一は、より多くのデータを計算、通信、保存することによって、事業の効率化や、高品質で安価な商品の開発、既存のビジネスモデルの拡大を実現することだ。しかし、演算やストレージなどのリソースが安く大量に得られるようになると、第二の方法、すなわち、リソースを惜しみなくつぎ込んで、まったく新しいものを生み出すことに経済的な意味が生まれる段階がやってくる。

パソコンはメインフレーム・コンピュータよりも性能の面で劣るが、エンドユーザーの自由度が飛躍的に向上した結果、メインフレーム・コンピュータの市場を完全に破壊してしまった。また、インターネットは、階層的な構造の通信ネットワークよりも効率面ではるかに劣るが、変化への適応性、堅牢性の高さにより、イノベーションの場を中央からネットワークの末端へと移動させた。インターネットはあらゆるものに破壊的な影響をもたらした。

図表2｜指数関数的速度で発展するリソースを意図的に浪費することでイノベーションが生まれた



技術革新がある段階まで達すると、計算能力などのリソースが極めて安く豊富になるため、それらのリソースを浪費することで新しいものを生み出すことに経済合理性が出てくる

1 半導体の集積密度（性能）は、約2年間で2倍になるという経験則
2 光ファイバーの通信量は約9カ月で2倍になるという経験則
3 ストレージの容量も、ムーアの法則と同様に指数関数的に向上するという経験則
出所：BCG分析

メモリとストレージも同様の軌跡をたどっている。テラバイト当たりのメモリのコストの急落を受け、より多くのデータを蓄積することが可能になった結果、ビッグデータの活用というアイデアが生まれた。同様に、ストレージをいくらでも浪費できるとしたら、何が生み出せるだろうか。

ビットコインはその答えの1つである。ビットコインのブロックチェーンは、各取引を5,700回も重複して保存することによって、改ざん不可能な記録を維持するのである。つまり、ブロックチェーンは演算分野におけるパソコン、通信分野におけるインターネットと同様に、ストレージを活用して破壊的イノベーションをもたらす技術である。飛躍

的な技術進歩のパワーが生んだ最も新しい技術の一つが、このブロックチェーンなのである（図表2）[4]。

では、ストレージの大胆な「浪費」によって実現したブロックチェーンによって、どのようなことが可能になるのだろうか。

3. The Singularity Is Near: When Humans Transcend Biology, Viking Press, 2005（邦題『ポスト・ヒューマン誕生　コンピュータが人類の知性を超えるとき』（NHK出版））　第1、2章のレイ・カーツワイルによる指数関数的な技術進化の説明が秀逸。

4. ビットコインの皮肉な点（実際には矛盾点）の1つは、ネットワークの安全性を守るために、そのネットワーク内で電力という別の資源を途方もなく浪費していることだ。二酸化炭素排出量の多さが拡張性を妨げている。この点は後述する。

3. ブロックチェーンによって、仮想世界に現実世界と同様の「連続性」が生み出される

ビットコインなどのデジタルトークンは、ストレージを大量に使用してブロックチェーンを何千回も複製し、ヴァーチャルな「連続性」を生み出している。これは画期的なブレイクスルーだ。

連続性は（量子力学は別として）物理世界の普遍的な特性である。もし私が背中の後ろに手を回して何かをやり取りしたら、正面からそれを見ていた人は、私の左手に現れたものと右手から消えたものは同じものだと合理的に確信できる。連続性によって、ヒトやモノの同一性を確認することができるのだ。また、連続性によって財産権の存在も認めることができる。これは、連続的に識別可能なモノは、連続的に識別可能なヒトが保有できるためである。このように、連続性によって、取引、すなわち財産の移転を認めることができる。また、「信用」という概念、ひいては契約そのものも連続性をよりどころとしている[5]。契約の前提となっているのはアイデンティティ、財産、取引、そして往々にして信用である。

つまり、資本主義システムの構成要素全体が、連続性を前提としているのである。もちろん連続性だけで財産や契約を扱うことはできないが（法律も必要だ）、連続性は必須要素なのである。これはあまりにも当たり前のことで、経済学の教科書では触れられることさえない。署名、パスポート、公証人、印影、印鑑、写真付きIDなどは、いずれも現実世界の連続性を拡大・拡張するものである。

しかし、インターネットのようなヴァーチャルな世界には、現実世界のような連続性が存在しない。仮想世界では、ある一連のデータがコピーではなくオリジナルであるという保証はなく、ヒトもモノもアイデンティティを持たない(古いジョークに「インターネットではあなたが犬だということを誰も知らない」というものがある)。もちろん、このことが歓迎されるべき状況は多い。しかし、仮想世界において連続性がないということは、アイデンティティや所有権、取引、信用、契約が有効なものであると当事者間で相互に確認するための土台が存在しないということである。

もちろん、仮想世界における取引の当事者間に、事前に現実世界での接点があれば、仮想世界でも暗号を使って直接的に関係を築くことができる。そうでない場合も、仲介者を立てて仮想世界の連続性の欠如に対処できる。たとえば、私は現実世界で銀行との接点を持っている。あなたも現実世界で銀行との接点を持っている。銀行同士も現実世界で接点を持っている。そして全体として、銀行という仲介者が、私とあなたの仮想世界におけるアイデンティティを保証し、私たちの取引を仲介してくれるのだ。このように、銀行などの現実世界の仲介者を介在させることによって仮想世界での連続性を実現するのが、これまでのやり方である。

ただし、ここには2つの大きな問題がある。第一に、もし仲介者が1人しかいない場合、その仲介者は独占者になってしまう。利益を最大化する余地があれば投資を絞り、価格をつり上げ、付加価値の大半を独り占めにするだろう。第二に、競争が激しい市場であっても、仲介者自身が仲介を必要とするという問題が生じることがある。たとえば、キエフに送金するには国際送金システム上で複数の取引を行う必要があり、遅れや重複作業、エラーが発生する。

このような、仮想世界における「連続性」の問題を解決するポテンシャルを秘めるのが、ビットコインをはじめとする、デジタルトークンとブロックチェーンの技術である。

ビットコインを例に説明しよう。ビットコインは単なる情報のやりとりだが、ブロックチェーンによって、採掘時までさかのぼって祖先を追跡することができる。すなわち、そのコインの過去にわたる連続性の証明が可能となる。同様に、ブロックチェーンによって、同じコインを2度使うことが不可能となるため、将来にわたる連続性も保証される。このように、ビットコイン技術では、ストレージをふんだんに使ってこの2つの性質を実現し、仮想世界での連続性を生み出している。これが、仮想世界においても仲介者を通さずに、過去に接点のない当事者同士の間で、アイデンティティ、所有権、取引、信用――そして、契約や市場――を成り立たせる土台となる。

この技術には、仮想世界のあらゆる仲介者に破壊的な影響を与えるポテンシャルがある。現行の仲介システムのコスト、複雑性、重複度が高ければ高いほど、その破壊力は大きくなる。

ヴァーチャルな連続性は、最終的に、ある対称性に行き着く。最近の技術の波、とりわけIoT(モノのインターネット)、スマート・デバイスの普及、AR(拡張現実)は、物理的なモノに対して、直接的に情報や知性を付与するものだ。つまり、「現実を仮想化する」ものと言える。これに対し、デジタルトークンやブロックチェーンの技術は、データに連続性を付与することにより、「仮想を現実化する」。現実と仮想が収斂する――それはちょうど、物理的な世界そのものと、世界地図の区別がつかなくなるようなイメージだ[6]。

5. 信用に関する技術のインパクトについてはPhilip EvansによるBCGレポート "*From Reciprocity to Reputation*," (2006年4月)を参照。

6. 広範囲に及ぶ現実と仮想の収斂は、相互に増幅性のある4種の最新技術――IoT、ビッグデータ、人工知能、モバイル機器――によって促進される。Philip Evans とPatrick ForthによるBCGレポート "*Borges' Map: Navigating the World of Digital Disruption*" (2015年4月)を参照。

4. ブロックチェーンの重層的なスタック構造が、革新的なアプリケーションを生む土台となる

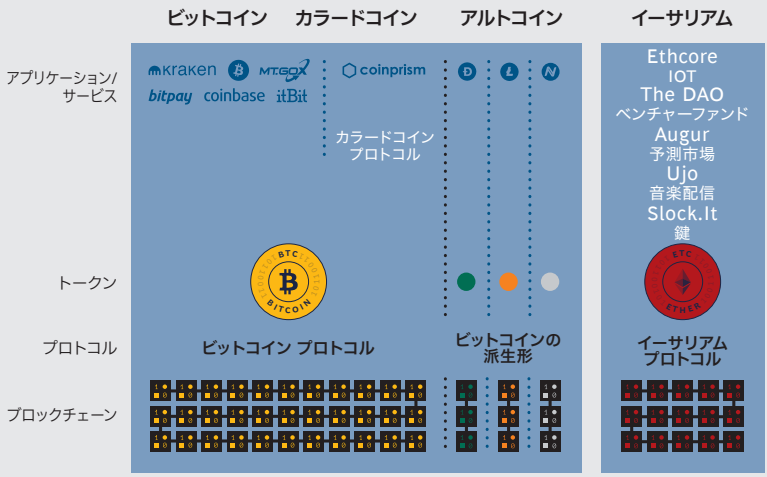
ビットコインは、他のあらゆるトークンやブロックチェーンのモデル、ないしはテンプレートとなりうる「スタック構造」を持つ（図表3）。「スタック」とは、相互運用可能なモジュールが階層化した構造であり、上層の機能は下層の機能をベースに設計される。規模や信頼性が求められる汎用的機能は、スタックの最下層（インフラストラクチャ）に位置する。一方、最上層に位置するのは、よりユーザーに近く、カスタマイズや実験、イノベーションにより常に進化している機能である[7]。各層間の相互運用性によって、下層における効率性と上層における順応性を兼ね備えたシステムになる。インターネットも、スタック構造を持つシステムの一つである。

ビットコインのスタック構造を構成する各層は、それぞれ以下の通り異なる役割を持つ。

ブロックチェーン

スタックの最下層はビットコインのブロックチェーン、すなわち「ブロック」の形にグループ化されて何千もの「ノード」により複製された、全取引のデータベースである。ブロックチェーンは規模に依存する性質があり、ノードの数（現在は5,700）とブロックの数（現在は43万）が増え続けるとともに信用度と堅牢性を増していく。物理的には、これらのノードはいわゆるマイニングプール（複数の採掘者によって構成される効率的採掘を目的とした集団）が所有するデータセンターで稼動する専用のコンピュータ群であり、その所在地は主に中国に集中している。

図表3 | ブロックチェーンのスタック構造



ブロックチェーンとデジタルトークンは、4階層のスタック構造のなかで最も重要な要素である

出所：BCG分析

プロトコル

ビットコインの「プロトコル」はブロックチェーンのすぐ上に位置する層だ。これはいわゆるオペレーティングシステム（OS）に相当するもので、ビットコイン・コアチームが保守する無料のオープンソースソフトウェアである。オープンソースOSとして有名なリナックスと同じように、参加者全員による徹底的なコードテスト、改善サイクルの早さ、（特定の保有者が存在しない）共同開発のプロダクトに対する信用といった、オープンソースモデルとしての強みを最大限に発揮し運用されている。一方で、コンセンサスに基づく戦略的判断が難しいという、この種のモデルに典型的な弱みも抱えている。

トークン

トークンは、プロトコルのすぐ上に位置する。たとえばビットコインは、システム内で交換され、取引の有効性を確認することの報酬と

して採掘者に付与されるトークンだ。他のあらゆる交換手段と同様に、トークンの価値を他者も認めているということが周知されて初めて、トークンは価値を持つ。ビットコインによる購入例が確認されたのは、2010年にラズロ・ハニエッツというプログラマーが採掘したての1万ビットコインでピザを買ったのが最初だと言われる。現在のレートで換算すると、その価値は600万ドル以上になる。

アプリケーションとサービス

アプリケーションとサービスは最上層に位置し、「ウォレット」(スマートフォンやコンピュータでビットコインを保持・管理するためのソフトウェア)、ビットコインと既存通貨間の両替サービス、情報サービスで構成される。この種のプロダクトやサービスは何百も存在し、主にスタートアップ企業が開発に取り組んでいる。

スタックの最下層に位置するビットコインのブロックチェーンは極めて堅牢だ。総価値が約100億ドルにもなるビットコインは世界中の有能なハッカーの標的になってきたが、ブロックチェーンへの攻撃が成功したことは1度もない。しかしスタックの最上層では様相はまったく異なる。広く知られたマウントゴックスやシルクロードの事件[8]などをめぐって、その脆弱性や犯罪との関連性が取りざたされている。しかしスタック構造の長所は、上層に倫理的・経済的な脆弱性があっても、下層の革新的な堅牢性は損なわれないという点である。

このように、スタック構造によって提供された組み替え可能なフレームワークにより、スタックの上層・下層それぞれにおいて、以下のような新しい通貨、新しいサービス、新しいコンセプトが開発されてきた。

カラードコイン

カラードコインはスタックの最上層のイノベーションで、ビットコインの空きスペースに、実物資産の情報などのデータを記録するものである。ビットコインに新たな情報を付与することは、コインに

「色」をつけるようなものであるため、カラードコインと呼ばれている。たとえばイギリスを拠点とするエバーレッジャーは、ビットコインを使って、ブロックチェーン上に宝石の情報を登録した。個々のダイヤモンドに関する40種類の識別情報を記録し、原産地や所有者を証明できるようにしたのである。ここでは、ビットコインはダイヤモンドの売買ではなく、鑑定済みの個別の宝石に関する改ざん不能な記録を作るために利用されている。このアプローチは、複雑な取引履歴をともなうあらゆる貴重な資産の追跡に利用できるだろう[9]。

アルトコイン

アルトコインは、ビットコインのプロトコルの大部分あるいは全部を活用して、独自のスタックを持つ別個のトークンを生み出したものであり、「BaconBits」「CoinKimdotcoin」「Zombiecoin」などが有名である。アルトコインは玉石混交であり、何かのジョークのような名前がつけられたものもあれば、ポンジ・スキーム（投資詐欺）に近いものさえある。しかしなかには、ビットコインのプロトコルを大きく改善することをめざして調整を加えたアルトコインも存在する。たとえば「Litecoin」は、ビットコインよりも少ない計算量で、速いペースでブロックを生成する設計になっている。また、「Monero」は仮名での支払いの追跡さえも回避できる、既存のコインよりも匿名性の高い仕組みを持つ。

イーサリアム

イーサリアムは、ビットコインとは異なるまったく新しいスタックであり、ビットコイン2.0と呼ばれることも多い。立ち上げからわずか1年後の2015年7月には時価総額が10億ドル近くに達した。イーサリアムは独自のブロックチェーンとトークン（イーサ）を持ち、決済だけでなく「スマートコントラクト」、すなわち、法律ではなくプログラムによって自動的に執行される契約を実行可能である[10]。イーサリアムの生みの親であるヴィタリック・ブテリンは、イーサリアムを「ワールドコンピュータ」と表現する。イーサリアムのアプリケーション

は急速に拡大してきたが、その成否はまちまちである。なかでも注目すべきはイーサリアムのスマートコントラクトによって自律的に動く組織であるDAO（分散型自動化組織：Decentralized Autonomous Organization、具体的にはベンチャーファンド）の構築を目指した試み、「The DAO」である。2016年6月、The DAOはイーサで1億3,000万ドル相当の資金調達に成功したが、その後、不正攻撃を受けて崩壊した。しかし、この脆弱性はThe DAOのプログラミングに起因するものであり、イーサリアムそのものの脆弱性によるものではないことに留意する必要がある。決済以外の領域でのアプリケーションを構築しようとしているオープンソースの開発者らは、優れたプラットフォームとして、引き続きイーサリアムを重視している。

パーミッションド・ブロックチェーン

パーミッションド・ブロックチェーンは、ブロックチェーンへのアクセスや権限を、特定のメンバー（典型的には金融機関）だけに制限するものである。そのため、ビットコインなどのオープンな枠組みとはかなり異なる。ブロックチェーンの詳しい調査、取引への参加、ノードとしてブロックチェーンを運営することをメンバーだけに許可するのである。パーミッションド・ブロックチェーンでは、取引を法律用語とコンピュータコードの両方で書き記すことができる。また、規制当局による審査も可能になる。現在はまだ実証研究の段階だが、銀行業界のコンソーシアム（R3 CEVが主導する「R3」など）や多くのフィンテック企業が、特に証券や外国為替におけるクリアリングやセトルメントの分野で、パーミッションド・ブロックチェーンの実現に力を入れている。

ブロックチェーンとデジタルトークンの有望な応用分野7選

トークンとブロックチェーンの破壊的なポテンシャルは、まず決済分野で表面化した。これは、両技術を応用したビットコインが人々の議論と関心を呼んだためだ。しかし、この2つの技術の応用範囲は決済分野にとどまらない。本文で解説しているように、ブロックチェーンとデジタルトークンは、デジタルな「連続性」を構築する。デジタルな連続性によって、互いを信用する根拠を持たない多数の当事者を結びつけることが可能となるが、これはさまざまな分野で応用可能である。また、取引記録の重複やエラーを減らしたり、デジタルアイデンティティの確保のために活用したりすることもできる。セキュリティ、機能性、規模のトレードオフのハードルが5年以内にほぼ解消すると仮定すると(これは大前提であるが)、さまざまな分野でブロックチェーンの画期的な応用法が実現するだろう。以下に挙げる7つの分野は、ブロックチェーンとデジタルトークンのキラーアプリケーション(圧倒的な影響力を持つ応用法)の候補である。

1. IoTにおける取引

現在、IoT活用例では同じ所有者の機器同士を接続することが多いため、各機器は情報や指示を交換するだけでよい。しかし機器の所有者が異なる場合は、何らかの取引が必要になる。現状では、機器の所有者の間に共通の仲介者が存在せず、扱われる金額の総額も少ないため、取引を行うことに経済的な価値はない。しかしブロックチェーン、特にスマートコントラクトを実現するようなブロックチェーンを使えば、機器同士が直接取引できるようになる。たとえば、車載のトランスポンダー(送受信機)と、ネットワークに接続された埋め込み式センサーを

交信させれば、駐車スペースに車を停めるだけで駐車券を購入できる(シリコンバレーのベンチャー企業Streetlineは、すでにこの種のトランスポンダーを実用化している)。ドイツ企業のSlock.itは、家庭用のスマート・デバイスとイーサリアム・ブロックチェーンを仲介する安価なコンピュータのプロトタイプを開発した。この技術の活用法の1つとして、このコンピュータがスマートコントラクトの形で部屋の賃貸希望者と交渉し、借り手が到着したら玄関のドアを開けるようにスマートロックに指示を出すことが考えられている。ブロックチェーンは手付金をエスクロー(第三者預託機関)に保持し、契約が履行されたらそれを放出する。こうすれば、ペイパルや銀行システムだけでなく、Airbnbも含めた仲介者を省くことが可能だ。

2. デジタルコンテンツをめぐるビジネスモデルの根本的変化

現在、インターネットのコンテンツは、購読料や広告料の形で集めた資金で作成されている。しかしブロックチェーンベースの低コストの仕組みを使えば、コンテンツの消費をページや時間(分)ごとに計測できるようになるだろう。プライバシーに関する消費者の懸念が高まっていくようなら、ブロックチェーンはオンラインメディア業界の収益モデルの根本的な変化を後押しする可能性もある。

このアイデアをさらに進めたのが、ブロックチェーンを使った知的財産の登録と保護である。2015年10月、イギリスのシンガーソングライターのイモージェン・ヒープは、イーサリアム・ブロックチェーンを使って、スマートコントラクトの形で『Tiny Human』という楽曲をリリースした。これにより、ファンはこの曲をダウンロード、ストリーミング、リミックス、同期する権利を獲得するとともに、制作者側にロイヤリティを直接支払う

ことができた。複雑でコストのかかる音楽業界の仲介構造をすべて回避することに成功したのである。

3. サプライチェーンのコスト抑制と透明性の向上

40兆ドルに達すると言われるグローバル・サプライチェーンも、非効率な取引ネットワークの1つだ。当事者相互の信用が不十分で、取引実行のプロセスに時間がかかり、エラーが発生しがちである。一部の銀行は、すでに信用状(L/C)をブロックチェーンに登録し、輸出入業者や関係する他の銀行との間で同じデータを共有して、遅れやエラーを防いで資金を拠出できるようにしている。これをさらに進めれば、データそのものに(ビットコインのように)連続的な識別子を保持させ、運送会社や関税当局、荷主、卸売業者、小売業者、信用できる独立認証機関等がデジタル署名を付加してブロックチェーンに追加したデータにアクセスできるようにすることが可能だ。これは船荷証券(B/L)の代わりになるだけでなく、ある品物がフィレンツェで手作りされたこと、フェアトレード協会加盟者の製品であること、遺伝子組み換え作物を使っていないことなどを認証することも可能だ。また、Provenance.orgは、先行者であるエバーレッジャーと同様に、企業が自社、自社製品、さらには特定の製造ロットに関する情報を登録できるイーサリアム上のプラットフォームを提供している。書類業務が撤廃され、信用の根拠が仲介者から情報の発信者へと移るのである。

4. 土地登記の改革

先進国であっても、土地登記には書類の不備がついて回る。手作業で確認したり保険をかけたりして、エラーの発生から身を守らなければならない。一方、多くの新興国では、登記簿が根本的に未熟だったり不正が横行したりして、貧しい人々の基本

的な財産権が奪われている。ホンジュラスでは土地の約60％が未登記で、役人が不動産を自己の名義に勝手に書き換えているケースもある。ここで、登記内容をブロックチェーンに格納することにより、改ざん不可能な登記情報の公開データベースを構築することが可能になる。ホンジュラスとグルジアでは既にこのような取り組みが始まっている。今のところ成果はまちまちだが、長期的には巨大なポテンシャルがある。ペルーの経済学者エルナンド・デ・ソト氏が主張するとおり、土地の所有権を明確にすることで、貧しい人々が土地を担保にした借入を利用できるようになり、投資意欲が生まれるのだ。

5. デジタルアイデンティティの保証

各国政府（あるいはサービスプロバイダの大規模な連合）は、ブロックチェーンを通じて市民にデジタルアイデンティティ（ID）を与え、すべての個人間取引における信用を強化することができる。デジタルIDはビットコインと同様に、承認され、誰もが検証可能なデータになるだろう。ただし、このようなデータを全てブロックチェーンで保管する必要はないかもしれない。市民は公開鍵/秘密鍵のペアを作って、選択した自分の個人情報のみを特定の受領者に送ることができるからだ。こうすれば、たとえば若者がアルコールを購入する際に、運転免許証に記載されているような余分な情報を開示しなくても、規定年齢に達していることを証明できる。将来的には、これを基盤として、法的拘束力のあるデジタル署名、パスポート、免許証、セキュリティパス、カードキー、証明書、ログイン情報、所有者ドキュメント、有権者登録など多岐にわたるデジタルIDを構築できるだろう。

この分野における最も大規模な取り組みが、これまでに10億人以上の国民にデジタルIDを付与してきたインドの国民ID制

度「アドハー（AADHAAR）」である。この基盤の上に構築された「インド・スタック」が発展し、銀行口座を持たない人々の支払い手段が実現する可能性があると考える専門家もいる。

6. ヘルスケアの効率化と、医学研究の手法における革命

医療現場では治療記録の重複、矛盾、不一致がつきものだ。一方、患者データには厳重なセキュリティとプライバシーの保護が求められており、まさにパーミッションド・ブロックチェーンの利用がふさわしい。しかし、先見者たちが視野に入れているのは単純なデータ共有にとどまらない「プレシジョン・メディシン」、つまり電子カルテ、データ分析、疾病のデータベースに基づいて学習し続ける医療システムである。この新しいシステムには、患者のデータ（最終的には完全なゲノム地図）、症状、治療履歴、そして治療の結果が記録されるようになるだろう。

このようなシステムを設計する際の重要な課題は、患者のプライバシーと、粒度の細かい普遍的なデータセットを求める研究者のニーズの折り合いをつけることである。単純な匿名化では役に立たない。ブロックチェーンの場合、個人の記録を暗号化して複数のノードに分散させ、データベースのクエリを帳簿全体に分散させることができる。アクセス権はスマートコントラクトとデジタルIDによって管理されるだろう。アメリカでは組織の縦割りによって、電子医療記録といった比較的分かりやすいイノベーションでさえも、実行が極めて難しいことが知られている。この分野を切り拓くのは、アメリカではなく北欧諸国だろう。

7. デジタル通貨の発行

少なくとも6つの中央銀行が、このアプローチを検討中だ。イ

ングランド銀行は中央銀行が発行するデジタル通貨についての研究を発表している。ビットコインとは異なり、このデジタル通貨（CBDC：Central Bank issued Digital Currencies）は固定価値で、政府の十分な信頼と信用によって裏付けられる。今後、中央銀行はブロックチェーンを用いて、国債をCBDCで買い入れるかもしれない。また、民間銀行がCBDCによって銀行間債務のネッティングを行えるようになれば、2008年に金融システムを崩壊の瀬戸際に追い込んだカウンターパーティ・リスクを大幅に抑制するだろう。ゆくゆくは、CBDCへのアクセスが拡大し、最終的には全国民に広がるかもしれない。そうすれば、CBDCは、物理的な現金や、民間銀行の従来型の決済機能の大部分に取って代わる存在になるだろう。

CBDCは普遍的に流通可能なゼロリスクの通貨であり、ビットコインにも破壊的な影響を与えるだろう。また、金融システム全体で、監督・規制やコンプライアンスのコストが大幅に減ると考えられる。イングランド銀行は、最近の研究で、CBDCによりマクロ経済政策が執行しやすくなる（たとえばCBDCではマイナス金利を支払うことができる）と指摘している。同様に、このような仕組みによって、実質金利の低下、不要な税制の撤廃、取引コストの低減の結果、GDPが恒久的に3％上昇するという予測まで示している。

7. これはジェリー・サルツァー、デビッド・リード、デビッド・クラークが“End-to-End Arguments in System Design,” ACM Transactions on Computer Systems, November 1984で初めて提案した「エンド・トゥー・エンド」原則の大まかな要約である。

8. 2014年、東京にあった当時最大のビットコイン取引所「マウントゴックス」の顧客資産が消失する事件が発生。また、2013年にはビットコインを使ってアメリカで薬物などを不正販売するサイト「シルクロード」がFBIに摘発された。

9. エバーレッジャーはその後、ビットコインからハイパーレッジャーのプラットフォームに移動。これによりカラードコインではなくなった。

10. 「スマートコントラクト」は法的な契約ではない。典型的なスマートコントラクトは、開始時にイーサをエスクロー（第三者預託機関）に登録し、定義した条件が達成されると開放する。このようにしてコンピュータコードを法律的文言の代わりにすることができる。理論的には、このようなコントラクトで損害を受けた当事者は訴訟を起こすことができる。しかし現実的には、適用されるべき法律を特定することや、場合によっては損害賠償を提起する相手を特定することさえ困難かもしれない。

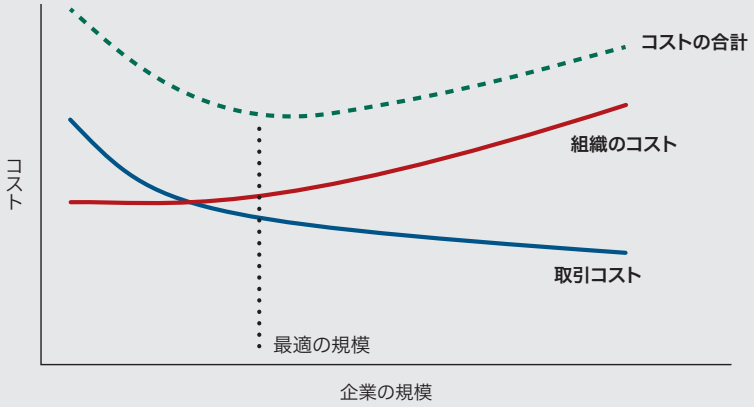
5. ブロックチェーンは、経済取引の基礎となる「信用」のあり方を大きく変える

ブロックチェーンに代表される分散型台帳システムは、しばしば「Trustless（相互の信用が不要）」なシステムだと説明されるが、これは正しいとは言えない。より正確に言うと、信用の根拠がネットワークの末端に分散されたシステムである。

4章で触れたエバーレッジャーがダイヤモンドを認証する際、あなたが実際に把握できるのは、「エバーレッジャーの秘密鍵を持つ人物が、ある日時にあるデータを投稿したということが、ブロックチェーンレベルで確実だ」ということである。その上で、あなたはエバーレッジャーに追加されたデータの内容が正しいということを、何らかの根拠によって信用する必要がある。そこでエバーレッジャーは、ダイヤモンドの鑑定において、業界で定評のある認証機関のグローバルなネットワークを活用している[11]。エバーレッジャーは、ダイヤモンドの画像や関連情報とともに、認証機関による認証情報をブロックチェーンに登録するのだ。また、イーサリアムのスマートコントラクトを使った農作物保険の場合は、すべての参加者が、気象データをブロックチェーンに登録する主体を信用しなければならない。ブロックチェーン内部で生み出される資産を表すトークン（つまり、ビットコインなどのデジタル通貨）を除けば、トークンの信用度は、そのトークンが表す現実世界のデータ（を最初に登録する者）がどれだけ信用できるかによって決まる。

これを突き詰めると、いわば、コースの提唱した経済理論のブロックチェーン版に行き着く。1991年にノーベル経済学賞を受賞したロ

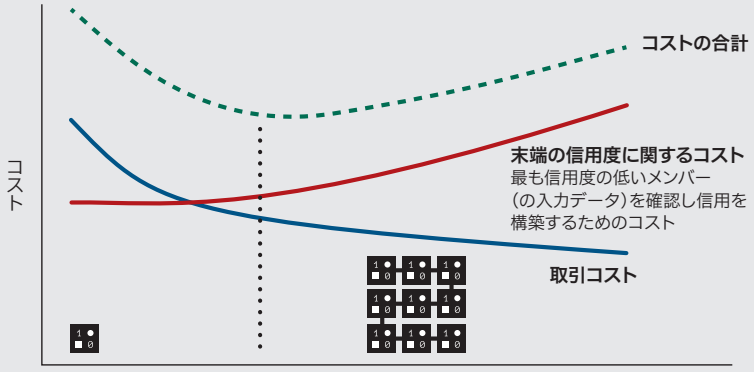
図表4 | コースの企業組織に関する経済理論



企業の最適規模は、取引コスト（規模の拡大により改善）と組織コスト（規模の拡大により悪化）のトレードオフによって決定される

出所：BCG分析

図表5 | ブロックチェーンの取引費用に関する理論



ブロックチェーンの最適規模は、取引コスト（規模の拡大により改善）と、末端の信用に係るコスト（規模の拡大により悪化）のトレードオフによって決定される

出所：BCG分析

ナルド・コースによると、企業組織は市場における「取引コスト（相手や条件を調べるコスト、交渉コスト、契約を順守させるためのコスト等）」を削減するために存在する。しかし、企業が一定以上の規模に達すると、企業組織の複雑性がもたらすコストが取引コストの削減効果を上回るようになる。つまり、取引コストの削減効果と組織の複雑性によるコスト増がつりあう状態が、最適な企業規模である（図表4）。

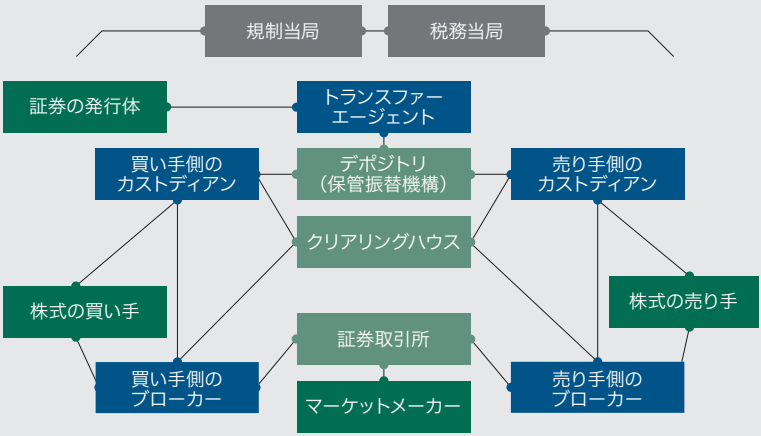
ブロックチェーンも同じように、取引コストの削減のために存在する。ブロックチェーンは共通データベースを障害や攻撃から守り、記録管理の重複とそれにともなう遅れやエラーを取り除き、ネットワーク全体に信用を行き渡らせる。しかしブロックチェーンがより大きく、あるいは網羅的になればなるほど、最も信用度の低いメンバーが登録するデータの信用度は低くなる。従って、ブロックチェーンの最適な規模は、取引コスト（規模が大きくなると改善する）と末端の信用度（規模が大きくなると低下する）のトレードオフに基づいて決まる（図表5）。

これは、単なる経済理論にとどまる話ではない。ブロックチェーンの用途のなかでも最も研究が進んでいる分野の1つが、証券取引のクリアリング・セトルメント業務である。これは、現時点では、ブローカー、カストディアン、トランスファー・エージェント、規制当局、受託者がからむ複雑なプロセスになっている。送金処理1回につき10回以上の仲介取引が必要なこともあり、一般的な所要期間は3日である。処理の20％でエラーが発生し、それらは手作業で修正しなければならない。ブロックチェーンを使えば、取引の両当事者が、信用度が高くエラーのない共通データベースを参照できる。取引は法律用語とコンピュータコードの両方で書き記すことができるため、データの交換それ自体がセトルメントの執行になる。さらに、規制当局は取引を確認できるが、他者の目に触れることはない。このような、ブロックチェーンを用いた金融取引の仕組みの構築をめざしているのが、R3 CEVが主導するコンソーシアムが開発中のパーミッションド・ブロックチェーンのプロトコル「Corda」である。このプロトコルによって、当事者間のエラーがなくなるほか、既存の決済プラットフォームを最新式にするよりも

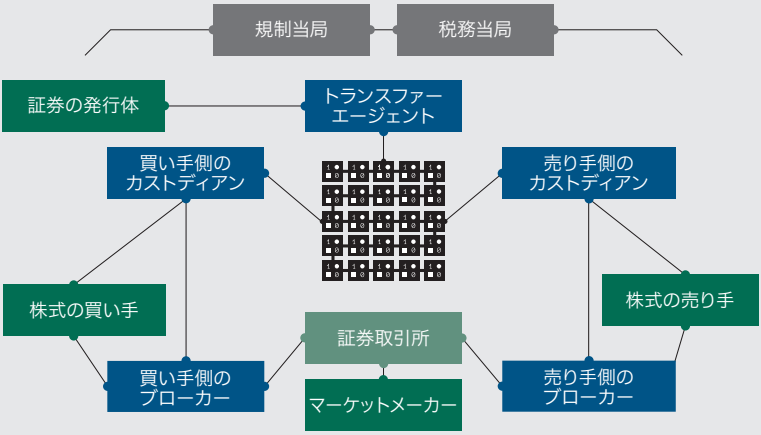
図表6 | 証券クリアリングシステムにおけるブロックチェーンの利用

プリンシパル（本人）　エージェント（代理人）　取引プラットフォーム

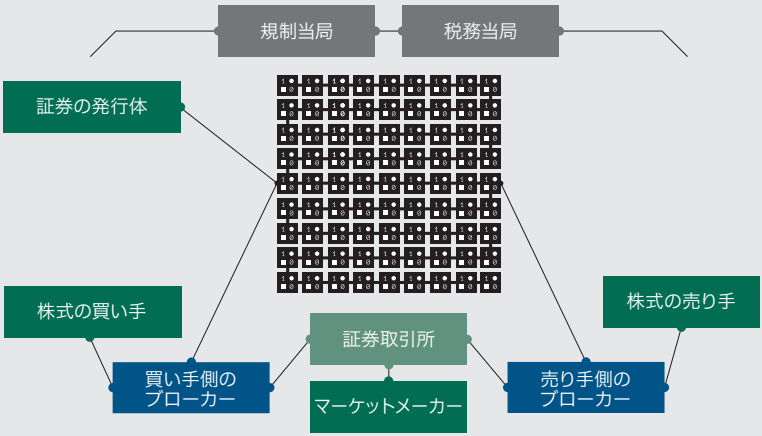
現在の証券クリアリングシステム



シナリオ1：カストディアンとトランスファーエージェント間にパーミッションドブロックチェーンが導入された場合



シナリオ2：発行体とブローカーの間にパーミッションドブロックチェーンが導入された場合



ブロックチェーンとデジタルトークンは、証券のクリアリングなど、多数のプレーヤーを複数の仲介者が繋いでいる全ての産業において、大きなインパクトを有する

出所：BCG分析

安く済む可能性がある。ここでの焦点は既存のシステムの効率化であり、既存のシステムを捨てることではない。

さらに発展的なソリューションも考えられる。ブローカー（買い手と売り手の仲介者）は、カストディアンの仲介を省くためにより大きなブロックチェーンを用いて取引を行えば、全体の取引コストをさらに減らせる可能性がある。企業や自治体などの証券発行体は、ブロックチェーンに直接証券を発行することで、トランスファーエージェントの仲介を省くことができるだろう（図表6）。

ただし、これらの発展的なソリューションの実現可能性は、ネットワークの末端がどれだけ信用できるかに左右される。各国当局に規制される約50のグローバル銀行ネットワークの間では、他行の公平性や取引執行能力に関する信用が醸成されている。しかし、何百ものブロー

カーや何千もの証券発行体が信用を獲得するのははるかに難しい。そのため、取引コストと、ネットワークの末端の信用度はトレードオフの関係にある。

最初は小規模のブロックチェーンから始め、参加する主体の信用度を確認する手法の開発にあわせて、しだいに大規模かつ低コストなものに発展させていくというやり方もあるだろう。しかしより先進的なアイデアもある。現在、「証券」が実現している重要な機能を、ブロックチェーン上のトークンの形で表現される、新たなスマートコントラクトで実現できるかもしれないということである。トークン自体が証券の役割を果たせば、ネットワークの末端の信用度は制約にならない。このようなブロックチェーンは、仲介者を壊滅させ、契約の当事者らを直接的に結びつける。「証券取引」はビットコインでの支払いと同じくらいに早く、安く、安全なものになるだろう。そうなれば、既存の金融サービスの大部分が消滅するかもしれない。

11. たとえば、米国宝石学会など。

6. ブロックチェーンが真価を発揮するためには、拡張性の問題を解決する必要がある

前述のとおり、ブロックチェーンには規模が大きくなればなるほど、取引コストが抑えられる一方、ネットワークの末端の参加者の信用度が低くなる、というトレードオフが存在する。

ブロックチェーンの規模に関しては、他にも以下のような論点がある。

- ノードの数が増えれば増えるほど、またブロックチェーンが長くなればなるほど、記録される取引の安全性が増す。これにより、実績のあるブロックチェーン(特にビットコインやイーサリアムで使われているもの)は、小規模で新しい代替物よりも優位に立つ。これは決済だけでなく、ブロックチェーンを土台にして構築されるあらゆるアプリケーションに当てはまる。

- 流通するデジタル通貨のドル換算金額が増えれば増えるほど、その通貨の流動性が増し、その結果為替レートが安定するだろう。この場合も、実績のある通貨(ビットコインやイーサなど)のほうが新興通貨よりも有利である。しかし、さらに重要なのは、特定のデジタル通貨がクリティカルマスに達すると、その通貨が交換の仲介手段として、また経済全体のなかでの価値の蓄積として認められるようになり、関連する取引コスト——すなわち、そのデジタル通貨とドル通貨の両替コスト——が大きく軽減されるということである。

- 極めて有力なキラーアプリケーションが1つあれば、関連するイノベーションのエコシステム全体のパフォーマンスが向上し、スタックの上層と下層の両方でネットワーク効果が生まれる。しかし、ブロックチェーンにおいて、そのようなキラーアプリケーションは未だ出現していない。通貨としてのビットコインは、いわゆる「イノベーションのS字カーブ」の上の平坦な部分に達しつつあるようだ（過去1年間の、一日当たり取引量の伸びはわずか1/3である）。また、多くの人々がイーサリアムのキラーアプリケーションだと考えていたThe DAOは、攻撃によって崩壊してしまった。

- ブロックチェーンが大きくなり、参加者の属性が多様になるにつれて、ブロックチェーンの方向性に関する意思決定は複雑になる。パーミッションド・ブロックチェーンでは、多数の競合企業のマネジメントが非常に重要だ（特に銀行業界では、協業をめぐり業界が混乱したことがある）。他方、パーミッション制ではない（オープンな）ブロックチェーンの課題は、オープンソースコード開発者、採掘者、アプリケーションの開発者たちの優先事項が対立しあうなかで、技術的なロードマップを策定・実行することである。デジタル通貨の場合、一部の者が保有する通貨の価値が着々と増えるにつれて、対立がエスカレートしている。また、自由に参入できるということは、撤退も自由にできる。オープンソースコードは独占所有ができないため、「もっと優れたものができる」と不満を持つコード開発者は、既存のものを改良した派生的なコードを生み出し、成長と世間の注目を奪い取ることができる。

また、規模の問題に加えて、技術的拡張性の面でも大きな課題がある。

現在、ビットコインは毎秒3～5件の取引を処理することができる。イーサリアムの処理速度は毎秒15～25件であるが、現行の決済ネットワークと比べスピードの面で劣る（たとえば、visaの決済システムは毎秒2,500件を処理している）。従って、ブロックチェーンが将来本格的に実用化されるためには、現在の技術的な拡張性のハードルを克服する必要がある。

ビットコインの場合、ブロック発生速度とブロックの最大サイズが固定されていることによって、キャパシティの上限が決まっている。他方、ブロックの発生速度を速めると、不正なブロックチェーンの増殖にネットワーク全体のコンセンサスメカニズムによる否認処理が追いつかず、有効性の確認プロセスが不安定化する恐れがある。また、ブロックの最大サイズを大きくすると、採掘作業のスケールメリットが強まるため、取引を認証する仕組みが談合の影響を受けやすくなる(すでに中国の4つのマイニングプールが、ハッシュパワー(採掘を行う能力)の58%を保持している[12])。

さらに、ビットコインやイーサリアムに意図的に組み込まれた非効率性が、ゆくゆくは実用面での制約になるだろう。ブロックを作成する(コインを採掘する)ためには、採掘者は「プルーフ・オブ・ワーク」と呼ばれる、莫大な計算処理(1ブロック当たり1万テラハッシュ)を実行しなければならない。この非効率性によって、ブロックチェーンの改ざんコストが大いに高まり、ネットワークの安全性が保たれているのだ。しかし、このような計算処理(ビットコインの採掘)に要する電力は、すでに米国の28万人都市の消費電力に匹敵するまでになっている。ある推計によると、2020年にはデンマークの消費電力に並ぶ見通しだ[13]。現在43万のブロックチェーンの数が数百万、数千万……と増えていけば、コストと二酸化炭素排出量の負担によって経済的にも環境的にも持続できなくなるだろう。

このような拡張性の問題については、いずれも実現には至っていないものの、以下のような幅広い解決策が検討されている。

プルーフ・オブ・ステーク

このプロトコルでは、プルーフ・オブ・ワークを課す代わりに、ブロックを有効化する際に、そのブロックを作成したノードが、そのトークンで表現される資産を十分に保有していることを証明する必要がある。たとえばビットコインであれば、新たなブロックを作成した採掘者が、

一定量のビットコインを保有していることを求めるのである。これによって、各ノードには、その資産の価値を落とさないようにする（改ざんに手を貸さない）という強い動機が働く。プルーフ・オブ・ステークは、膨大な計算を必要としないため計算コストや取引コストが劇的に低減することになる。そのため、（現在はコスト面で対応が難しい）はるかに小さい規模の取引にも対応できるようになるだろう。

ペイメントチャネル

もう1つの案が、ブロックチェーンのスタックとは別のペイメントチャネルと呼ぶレイヤーを活用するものである。たとえば、少額の決済を何度も行うようなとき、直接の取引はペイメントチャネルを通じて行い、最初と最後の取引のデータのみをメインのブロックチェーンに記録する。そうすることで、メインのブロックチェーンへの負荷を回避しつつ、ブロックチェーンの安全性を維持しながら取引数を拡大することができる。このアイデアは、ビットコインのブロックチェーンについて提案されているライトニング・ネットワークなど、多くのバリエーションがある。

サイドチェーン

サイドチェーンは、メインのブロックチェーンから派生するチェーンである。サイドチェーンでは、取引の「ミラー」として内部で独自のトークンを生成することができるため、ユーザーはトークンをメインチェーンからサイドチェーンへ移したり、再び戻したりすることができる。また、サイドチェーン上では、メインチェーンでは実装が難しい改変（たとえば、小規模取引向けの安全レベルの緩和、迅速なブロック作成、スマートコントラクト）を柔軟に実現できる。さらに、サイドチェーンそれ自体が、一個の閉じたパーミッションド・ブロックチェーンにもなりうる。

シャーディング

シャーディングは、1つのグローバルなブロックチェーンを維持しつつ、現状のように、すべてのノードがすべての取引の有効性を確認する方法ではなく、取引記録をいくつかのシャード（破片）に分割し、個々のシャードを別個のノードのグループが確認するものである。ある意味、セキュリティ面で妥協することによって拡張性を実現するアプローチである。

これらの4つの解決策は、ブロックチェーン研究・実験の最先端である。ビットコイン・コアチームは、安全性の高い優れたブロックチェーンをめざして、これらのアイデアを慎重に検討している。一方、イーサリアムの開発者コミュニティはより積極的であり、2017年にリリースする次期バージョン2.0（コードネーム「セレニティ」）は、4つの設計原則のすべてを明確に踏まえて開発されている。しかし、守るもののないスタートアップ企業は、これらの原則を適切に組み合わせて、実績のあるブロックチェーンを打ち負かそうとしている。既存のビットコインやイーサリアムのコードや通貨を土台にする場合もあれば、一から始める場合もあるだろう。すでに大方のピースはそろっているが、世界は決定的な組み合わせ、つまりキラーアプリケーションの登場を待ち望んでいる。

12. ウェブサイト「Blockchain Info」（https://blockchain.info/pools）を参照。

13. “Bitcoin Could Consume as Much Electricity as Denmark by 2020”, Motherboard, March 29, 2016

7. ブロックチェーンを経営戦略で活用する上での5つの原則

ブロックチェーンに関する戦略を検討する際は、以下の5つの原則を踏まえる必要がある。

1. 競争よりも協力を重視する

デジタルトークンやブロックチェーンが真価を発揮するのは、現状において、多数の主体が、不完全な信用関係の下で高コストな取引をしている場合である。従って、ブロックチェーンの導入によるメリットは、特定の参加者ではなく取引ネットワーク全体が享受することになる。そのため、先進的なグローバルテクノロジー企業は、医療や国際貿易などプレーヤー間が寸断された業界において取引のプラットフォームを構築することを目指し、顧客とのアライアンス構築に力を入れている。シリコンバレーの何百ものスタートアップ企業も同様だ。これらの取り組みは、10年がかりのプロジェクトになるだろう。こうした業界に属する企業は、ブロックチェーンの導入による成長や効率化のメリットと、ブロックチェーンという新たな独占的取引プラットフォームにより自社のビジネスがコモディティ化するリスクを冷静に比較する必要がある。もし、ブロックチェーン導入によるリスクがメリットを上回る場合は、業界全体の自律性を守るため、協調的な行動（銀行が試みているような）を検討する必要があるだろう。

2. 技術と同様、組織力が必要

向こう数年は、既存の仲介者の連合体が主導するパーミッションド・ブロックチェーンと、より先進的なオープンなブロックチェーンのせめぎあいが起こるだろう。いわば、少数企業による寡占と民主主義の

対立である。金融サービスをはじめ、仲介により成り立っている多くの業界では、既存企業がパーミッションド・ブロックチェーンなどの形で、自らの業界内に新たな技術を取り入れるという理性的な反応を示している。しかし、それで十分かどうかは分からない。

オープンなブロックチェーンは、ブロックやノードの数、正確な有効性確認など、規模のメリットを享受できる。これに対し、パーミッションド・ブロックチェーンは拡張性の面でメリットを享受できる。必要な参加者が比較的少なくて済み、プルーフ・オブ・ワークなど拡張の支障となる機能を省くこともできるからである。ここで重要になってくるのは、技術進化の側面よりもむしろどちらが速いペースで推進できるかであろう。カギとなるのは意思決定のあり方だ。パーミッションド・ブロックチェーンを活用しようとする業界のコンソーシアムは、市場では激しく競争しているメンバー同士をまとめる必要がある。他方、オープンコミュニティーの場合は、コミットメントの度合いがばらばらであり、ともすれば新たな仕組みを立ち上げようとする多様な参加者がいるなかで、一つの筋書きにそって進めなければならない。戦略策定者は、オープンとパーミッションド・ブロックチェーンの双方のメリットとデメリットを熟知し、どちらに勝機があるかを冷静に判断する必要がある。

3. 規制（政府）のあり方を所与としない

ブロックチェーンに対する現在の規制環境は非常に好ましいものである。大半の国・地域の法制度においてビットコインは合法であり、金融商品としてではなくコモディティとして規制されている。規制対象は主にスタックの最上層（特に取引所）であり、下層（ブロックチェーン）ではない。むしろ、ブロックチェーンは政府による取引の規制・監督を後押しするものであるとも言える。なぜなら、ブロックチェーンはカウンターパーティ・リスクを抑制し、顧客確認（KYC）やマネーロンダリングに関する規則の適用を促進し、規制当局が取引をチェックするための「バックドア」を提供するからだ。しかし、当然のことなが

ら、規制環境は――セキュリティ面の脆弱性が判明すれば特に――突然変化する可能性がある。

他方、政府自体が、個人識別、医療、デジタル通貨の分野でブロックチェーンの革新的なアプリケーションを推進する可能性もある。政府にはそれを推進するだけの十分なインセンティブがあり、普及に必要なクリティカルマスを確保している。この種の技術を、より広範な景気刺激、雇用創出、自国の競争優位の源泉と見なしている政策決定者も多い。一部の国は、その他の国に先んじて技術を取り入れるだろう。

4. 中長期の目線で取り組む

経営層からは、これらの技術のROIが期待ほど高くないという不満も聞こえてくる。既存企業は、ブロックチェーンを自社のビジネスに活用することを華々しく打ち出しているものの、平等な競争の場を作ること(つまり、業界の価格水準を下げるだけのこと)に積極的に協力したり投資したりするケースはほとんどないのが現状である。企業の幹部は、イノベーションによって新規市場が開拓できる、あるいは、真に破壊的な脅威への対応としてイノベーションは不可欠だ、という信念を持たなければならない。さもなければ、業界内のプレーヤーの大半が技術導入を先送りした結果、現状維持されている企業の大連立が崩壊することは想像に難くない。

先見の明あるCEOは、目先の損得勘定を度外視するものだ。将来、新たな技術を活用して業界秩序を破壊した企業が成功した場合は、ビジネススクールのケース・スタディで成功事例として紹介されるだろう。逆に、技術革新を無視した結果市場の変化に乗り遅れれば、誤った経営判断の事例として取り上げられることとなる。

5. 抜本的変化があることを前提とする

ブロックチェーンによる経済のエコシステムが、今後どのように発展していくかは誰にも分からない。もし、広く支持を得る強力なアプ

リケーション(キラーアプリケーション)が1つでもあれば、広範に導入が進み、補完的なインフラ、商品、サービスも急速に発展するだろう(なお、この点について現時点で確実なのは、キラーアプリケーションは通貨としてのビットコインではないということだ)。逆に、ハッカーによりセキュリティ面の重大な欠陥が一つでも露呈すれば、規制当局を動揺させることになる。あるいは、前述の拡張性の問題が解決不可能なものであることが明らかになるかもしれない。

または、その中間のシナリオも考えられる。まったく異なる複数のアプリケーションがいずれもまずまずの成功を収めた結果、パソコンやインターネットのような1つの大きな流れに収束しないという状況になるかもしれない。革新的なアイデアが、十分な勢いを得られないまま、実を結ばずに終わることもある。シリコンバレーの企業がもう一度盛り上がりを見せるかもしれないが、このまま次の新しいテーマに移る可能性もある。確実なのは、将来のことは誰にも分からないということである。

8. 経営者が備えるべき3つのポイント

革新的な技術に関する戦略を立てる際には、財務予測もビジョンも絶対の基準にならない。このような不確実な環境下での戦略策定においては、学習する姿勢、戦略オプション、実験という3つの要素を重視しなければならない。

持続的に学習する姿勢を保つ

企業組織は、周りの環境――技術、競争動向、連携企業間の駆け引き、常識破りの新興企業、政策の変更――を十分に理解する必要がある。あらゆる点で、状況の非連続性に注意すべきである。たとえば、オープンなブロックチェーンプロトコルが、業界のコンソーシアムによるクローズドな取り組みの魅力を奪うかもしれない。一方、遠く離れた国の政府が支援するイニシアティブが、キラーアプリケーションの触媒になるかもしれない。もしくは、暗号技術のブレイクスルーが、セキュリティや拡張性に変革をもたらすかもしれない。パソコンやインターネットの登場によって、全ての産業が丸ごとそれらのアプリケーションになったのと同じように、他の業界における進歩が自社の業界に押し寄せてくるかもしれない。ブロックチェーンがビジネスにどのような影響を与えるのかについては議論が定まっていないため、部下に判断をゆだねるのではなく、自らの鋭敏な嗅覚に基づいて決断を下すべきである。そのためには、経営層が自ら、先端技術について持続的に学習する姿勢を保つ必要がある。

戦略的なオプションを考える

ファイナンスの世界と同様に、経営戦略では不確実性が高まれば高まるほどオプションの価値が高まる。オプションとは、結果に関わら

ず投資する価値のあるものである。成果がはっきりするまで努力を怠ったり遅らせたりするのは経済合理性に欠ける行動だ。投資の重複や、矛盾/競合する複数のイニシアティブを進めるリスクがあったとしても、さまざまなオプションに幅広く投資するのが望ましい。代替技術のポートフォリオを受け入れよう。業界のアライアンスやコンソーシアムに参加しよう。参加メンバーになることで、有望な取り組みにいち早く参加したり、先進的取り組みについて学ぶチャンスを得たり、グループの優先事項を決定する側に回る機会を得たりすることができる。

実験と割り切って試行錯誤で進める

トークンやブロックチェーンのアプリケーションの開発には「アジリティ(迅速性)」の原則を取り入れよう。実験は、戦略の方向性を示すと同時に、実験そのものがオペレーション上の能力や信用性を向上させるため、重要な意味を持つ。インターネット・プロトコル開発を主導したマサチューセッツ工科大学(MIT)のデビッド・クラークが、初期のインターネットコミュニティのスローガンとして「ラフ・コンセンサス&ランニング・コード(システムの仕様を開発初期に確定させることはせず、ゆるやかな合意(ラフ・コンセンサス)に基づき開発を進め、実際の運用を通じてコードを改善していくという考え方)」を掲げたことは有名である[14]。

• • •

ブロックチェーン技術の開発者、起業家、政策決定者らと近い関係を保ち、持続的に学び続けること。オプションを確保しておくこと。実験すること。これらが、型(ブロック)にとらわれずに柔軟な戦略決定を行うための合言葉だ。

14. D.D. Clark, "A Cloudy Crystal Ball: Visions of the Future," plenary presentation, 24th meeting of the Internet Engineering Task Force, Cambridge, MA, July 1992.

Philip Evans
BCG ボストン・オフィス シニア・アドバイザー、BCGフェロー

Lionel Aré
BCGパリ・オフィス シニア・パートナー&マネージング・ディレクター、
BCGフィナンシャル・インスティテューション・プラクティスのグローバルリーダー

Patrick Forth
BCG シドニー・オフィス シニア・パートナー&マネージング・ディレクター、
BCGテクノロジー・メディア&テレコミュニケーション・プラクティスの
グローバルリーダー

Nicolas Harlé
BCGパリ・オフィス パートナー&マネージング・ディレクター、
ブロックチェーンに関するBCGグローバルのトピックリーダー

Massimo Portincaso
BCGベルリン・オフィス パートナー&マネージング・ディレクター

原題：*“Thinking Outside the Blocks”*（2016年12月）

本冊子に収録した論考の原典、および文中でご紹介した論考はbcg.perspectives
サイトでご覧いただけます。
https://www.bcgperspectives.com/

弊グループでは、企業経営に関するさまざまなテーマについてコンサルティング
サービスを提供しております。
ご関心をお持ちの方は、bcgjapan@bcg.comまでお問合せください。

2017年4月発行

ボストン コンサルティング グループ

東京オフィス

東京都千代田区紀尾井町4-1 ニューオータニガーデンコート〒102-0094
Tel.03-5211-0300　Fax.03-5211-0333

中部・関西オフィス

愛知県名古屋市中村区名駅1-1-4 JRセントラルタワーズ〒450-6036
Tel.052-533-3466　Fax.052-533-3468

ミックス
責任ある木質資源を使用した紙
FSC® C012064
FSC www.fsc.org


BCG
The Boston Consulting Group