© Crown copyright 2016

この出版物は別に記載されていない限り Open Government Licence v3.0 の定める条件により使用許諾されています。この使用許諾は以下で閲覧できます。
nationalarchives.gov.uk/doc/open-government-licence/version/3
または下記にご請求ください。
Information Policy Team, The National Archives, Kew, London TW9 4DU
電子メール送信先：psi@nationalarchives.gsi.gov.uk

第三者の著作権情報を表示している場合は、その著作権者からの許可を必要とします。

本出版物は以下で入手できます。www.gov.uk/go-science

本出版物についてのご質問、または別形式のもののご請求は以下にお願いします。

Government Office for Science
1 Victoria Street
London SW1H 0ET
電話：020 7215 5000
電子メール：go-science@go-science.gsi.gov.uk

GS/16/1

デザインおよび制作 WordLink

日本語版監修　公益財団法人 NIRA 総合研究開発機構

分散型元帳技術：ブロックチェーンを超えた応用の可能性

英国政府科学局

Government
Office for Science

分散型元帳技術：ブロックチェーンを超えた応用の可能性

UK Government Chief Scientific Adviser（英国政府チーフ科学顧問）報告書

謝辞

本検討報告を支援してくださった多くの方に感謝します。 -- Sir Mark Walport (Government Chief Scientific Adviser)

指導および根拠論文起草のための専門家パネル：

Robleh Ali	Bank of England
Richard Brown	R3
Patrick Curry	British Business Federation Authority
Richard Copland	CGI Group
Dr Phil Godsiff	University of Surrey
Mike Halsall	Singularity University/ Almanis
Derwen Hinds	CESG
Matthew Johnson	Guardtime
Dominic Hobson	COOConnect
Dr Vili Lehdonvirta	Oxford University
Jonathan Levin	Chainalysis
Dr Catherine Mulligan	Imperial College London / Future Cities Catapult
Professor M. Angela Sasse	University College London
Dr Chris Sier	FiNexus
Daniel Shiu	GCHQ
Simon Taylor	Barclays

その他の貢献者および助言者

Hadley Beeman	GDS
Dr John Baird	EPSRC
Alastair Brockbank	British Embassy Tallinn, Estonia
Dr George Danezis	University College London
Shaul David	UKTI
Nick Davies	DWP
Igor Nai Fovino	Joint Research Centre, European Commission
Leanne Kemp	Everledger
Dr Sarah Meiklejohn	University College London
Jean-Pierre Nordvik	Joint Research Centre, European Commission
Tom Price	BIS
Thomas Wilkinson	Home Office
Naomi Wright	HMRC

根拠論文作成の支援および編さん

Dr Claire Craig	GO-Science
Martin Glasspool	GO-Science
Emma Griffiths	GO-Science
Elizabeth Surkovic	GO-Science

編集者

Dr Mark Peplow

目次

序文 4
要旨および勧告 5
定義 17
第 1 章 : ビジョン 21
第 2 章：技術 33
事例：研究およびホライズン・スキャニング 37
第 3 章：ガバナンスおよび規則 41
第 4 章：セキュリティおよびプライバシー 47
第 5 章：破壊的な可能性 53
事例：ダイヤモンド 56
事例：コーポレートアクション 58
事例：SETL による取引 60
第 6 章：政府での応用 65
第 7 章：グローバルな視点 73
事例：欧州エネルギー小売市場 76
事例：エストニアにおけるブロックチェーン導入による支払、取引、契約形態の変貌 80
参考文献 84
謝辞 87

本報告書の補足資料として短篇ビデオを作成しました。
https://youtu.be/4sm5LNqL5j0 をご覧ください

（注）本報告書の日本語訳については、公益財団法人NIRA総合研究開発機構が監修を行いました。

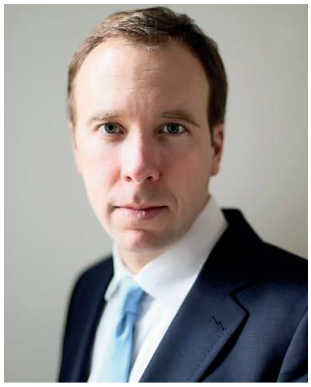
序文

人類は、新しい技術の出現と、それらによってさらに発展した人間の知恵をもとに進歩してきました

分散型元帳技術には、飛躍的なイノベーションにつながる爆発的な創造をもたらす潜在的な力があると言ってもよいかもしれません。この技術は、さまざまなサービスにおいて新しい信用形態を生み出す可能性があります。オープンデータによって国民と国との関係が抜本的に変化したように、このような技術の出現により、金融市場、サプライチェーン、消費者サービスや B2B（企業間取引）サービス、公開企業に大変革が訪れることが期待されます。

分散型元帳が発達し、データに対する私たちの考え方や保管方法が劇的に変化するにつれ、さまざまな課題が生まれることが予想されます。英国はこのような課題を探索し、公的サービスや経済にそのメリットが最大限に生かされるように支援しているという点で、世界の先駆者的な位置にいます。英国はすでに世界有数のデジタル能力を有し、革新的な金融サービスや優れた研究コミュニティーを擁しています。また、民間部門の専門知識も蓄積されつつあります。わが国で推進役となっているアラン・チューリング・データ・サイエンス研究所（Alan Turing Institute）、オープンデータ研究所（Open Data Institute）、デジタル・カタパルト・センター（Digital Catapult）などの機関が、民間部門および国外の協力機関と連携し、この技術が持つ潜在的な可能性を最大限に引き出すことが非常に大切です。

このたび、私たち両省は共同でこの分野を牽引していく運びとなったことを喜ばしく思い、今後、他の省庁とも連携して、この機会を活かし、英国国民と英国経済にとってメリットとなる応用のあり方について理解を深めていけることと期待しています。



マシュー・ハンコック
（THE RT HON MATTHEW HANCOCK MP）
内閣府担当大臣・財務省主計長官
（Minister for the Cabinet Office and Paymaster General）

エド・バイゼイ
（THE RT HON ED VAIZEY MP）
文化・デジタル経済担当大臣
（Minister of State for Culture and The Digital Economy）

要旨および勧告

はじめに

分散型元帳の作成を可能にするアルゴリズムは、強力で破壊的なイノベーションであり、公共および民間サービスの提供方法を大きく変え、さまざまな分野に応用することによって生産性の向上をもたらすことが期待されます。

元帳は古代から商取引の中核をなすものであり、多くの事物、一般的には金銭や資産などの財産を記録するために使われてきました。記録形態は粘土板からパピルス、羊皮紙、そして紙へと進化してきましたが、この長い歴史において主要なイノベーションといえば、コンピューター化されたということのみであり、コンピューター化といっても単に紙からビットに移行しただけにすぎません。アルゴリズムによって今初めて、従来の紙ベースの元帳をはるかに超える特性と能力を備えた、デジタル分散型元帳の共同作成が可能になったのです。

分散型元帳とは、本質的に複数のサイト、地域または組織間のネットワーク全体で共有可能な資産データベースです。ネットワーク内の参加者は全員、各自で元帳の同一コピーを保持することができます。元帳の変更内容はすべてのコピーに数分以内、場合によっては数秒以内に反映されます。資産は金融上の資産や、その他法律上のものであり、物理的または電子的な形態をとります。元帳内に記録される資産の安全性と正確性は、どの当事者がどのような操作を実行できるかを統制する「キー」と署名の暗号化によって維持されます。また、記録はネットワーク内で合意された規則に従い、単独または複数の参加者、あるいは全員で更新することができます。

この技術の根幹となっているのは、2008 年にビットコインという、ピアツーピア（P2P）の仮想通貨に用いるために発明された「ブロックチェーン」という技術です。ブロックチェーンのアルゴリズムでは、暗号化された署名を使ってビットコイン取引が「ブロック」で集計され、既存の一連のブロック、すなわち「ブロックチェーン」に追加されます。ビットコイン元帳は、分散型で「許可を必要としない」形式で作られているため、新しい取引ブロックを追加するための新しい暗号パズルを解読できれば、誰でも取引ブロックを追加することができます。これを推進するため、現在、「ブロック」のパズルを解いた者に報酬として 25 ビットコイン（当時）が与えられています。インターネットおよびコンピューターにアクセスして、暗号パズルを解くことができれば、誰でも元帳への追加が可能であり、このような人たちは「ビットコインマイナー（採掘者）」と呼ばれます。マイニング（採掘）にたとえられるのは、ビットコインの収集プロセスには、膨大な計算能力といった大量の労力（エネルギー）が必要であるためです。ビットコインを運営するのに必要なエネルギー量は、1 ギガワット（GW）を超えると見積もられており、これはおよそアイルランド国内の電力使用量に相当します。

ビットコインとは、オンライン上で取引される仮想通貨のことです。現金の真偽は、その外見と物理的特性により判別され、銀行券の判別の場合は、記番号および他のセキュリティデバイスによって行われます。しかし、現金自体には取引を記録する元帳が存在せず、硬貨・紙幣のいずれについても偽造の問題があります。ビットコインの場合は、取引元帳によってその真偽を確認できます。貨幣、ビットコインのいずれであっても、財布または仮想財布（ウォレット）にしっかりと保管する必要があり、それを怠ると、貨幣もビットコインも盗難に遭うことになりかねません。従来の通貨とビットコインとの根本的な相違は、前者は中央銀行が発行するのに対し、後者は世界的な「協調」の上、合意

に達した金額で発行される点です。交換・交易手段としての通貨は、何千年も前から使われてきました。タカラガイから秤量貨幣へ、そして今、このビットコインへと、一筋につながっているといえるでしょう。

しかし、本報告書はビットコインに関するものではありません。本報告書は、ビットコインを実現させたアルゴリズム技術と、元帳の概念を変えるその力に関するものです。それは、元帳は、非常に広範囲な取引の成立、記録およびセキュリティの確保を可能にするための手段となるものです。そして、基本的なブロックチェーン手法に変更を加え、規則、スマートコントラクト、デジタル署名、およびその他各種の新しいツールを取り入れることが可能であるという点について、明らかにします。

分散型元帳技術には、政府による税金徴収、給付金・サービスの提供、パスポート発行、土地登記、資材調達におけるサプライチェーンの確保に役立ち、また、全般的に政府の記録およびサービスの健全性を保証する可能性を持っています。たとえば、国民保健サービス（NHS：National Health Service）の場合、この技術により、提供するサービスの質の向上と認証化、および厳格な規則に従って記録を安全に共有することができるようになり、健康・医療を向上させることが期待されます。また、これらのサービスの利用者はこの技術により、状況に応じて各自で個人記録へのアクセスを制御し、その記録に誰がアクセスしたかを知ることができるようになる可能性もあります。

従来のデータ管理、特に個人データの管理では、通常、単一組織内にある大規模な古いIT システム（いわゆるレガシーシステム）が使用されています。これに、他の組織との通信用に各種ネットワークおよびメッセージ通信システムが付加されますが、それによってコストが増大し、システムが複雑なものになっています。高度に集中化されたシステムでは、一か所の故障がすべてに影響することになりかねず、その場合には多大なコストが発生します。また、このようなシステムは、サイバー攻撃に対し脆弱である可能性があり、さらにデータの同期が取れていない、古い、または単に正確でない、という状況が頻繁に発生します。

これに対し、分散型元帳への攻撃は本質的難しくなっています。それは単一のデータベースではなく、同じデータベースが複数存在するため、サイバー攻撃を成功させるにはすべての元帳を同時に攻撃しなければならないからです。この技術では、元帳の一部に変更があればそれをネットワーク参加者がすぐに発見するため、勝手な変更や悪意を持った改ざんに対しても抵抗力があります。これに加え、情報の保護や更新方法についても、参加者がデータを共有し、常にすべての元帳が相互に一致することが保証されるようになっています。

しかし、だからといって分散型元帳は、サイバー攻撃に対し脆弱性がないということにはなりません。原則として、誰でも元帳の1つのコピーを「正当に」修正する方法を見つけたら、その元帳のすべてのコピーを修正できるからです。したがって分散型元帳のセキュリティの確保は、現代社会が依存するデジタルインフラストラクチャーのセキュリティ確保という大きな課題の一角をなす、重要な任務です。

各国政府は、分散型元帳技術を業務に採用し始めています。エストニア政府は、同国のGuardtime という企業が開発したキーレス署名インフラストラクチャー（KSI：Keyless Signature Infrastructure）という一種の分散型元帳技術を用いて、何年にもわたり分散型元帳技術の応用を図ってきました。

KSI により、国民は、政府のデータベースに収録されている自らの記録に間違いがない

か検証できます。また、この技術は政府ネットワーク内で権限を持つ内部の者による違法行為ができないように意図されています。このように、国民が自らのデータを安全かつ正確に維持できることを保証する技術を利用して、エストニアでは、e-Business Register や e-Tax のようなデジタルサービスが提供されており、こうしたサービスにより、国にとっても国民にとっても管理負担が軽減されています。エストニアは英国、イスラエル、ニュージーランド、韓国とともに「Digital 5」（D5：5 大デジタル先進国）の 1 つに数えられています。英国にとっては、ブロックチェーンおよび関連技術の応用について、これらの国々や同じ考えを持った他国の政府と協力し、そこから学ぶ良い機会であるといえます。

ビジネスではこのような可能性が早くも評価されてきており、分散型元帳は、商品や知的財産の所有権や出所を保証するための新しい方法であると考えられています。たとえば Everledger は、ダイヤモンドの同一性を採掘、研磨から販売、その保険契約までを記録する分散型元帳です。Everledger は、書類偽造が比較的多い市場において、出所の確認を効率的に行い、詐欺行為を減らし、ブラッドダイヤモンドの市場流入を防止することが期待されています。

この一連の新技術における重要課題は政策立案者および市民に対しその重要性を伝えることであり、それが本報告書の重要な目的の 1 つです。

普及を難しくしている第 1 の理由は、ブロックチェーン技術がビットコインと密接に関連付けられている点です。ビットコインとは暗号通貨、つまり暗号化された仮想通貨の一種です。このように呼ばれる理由は、同通貨の供給と追跡の根幹として、暗号化技術が利用されているためです。ビットコインは、犯罪取引や今は使われていない「シルクロード」などの「闇ウェブ」の取引サイトと関連していることから、市民や政府の政策立案者から疑念の目で見られています。しかし仮想・暗号通貨に対しては、世界各国の中央銀行や財務関連の省庁が強い関心を抱いて研究をしています。これは、仮想通貨を電子的に流通させることで、効率が向上する可能性があるうえに、現金とは異なり取引元帳が付随するからです。

普及を難しくしている第 2 の理由は、紛らわしい用語が多数使用されている点です。これらの用語については、サイモン・テイラー（Simon Taylor）がまとめた定義を、本要約の末尾に記載しています。特に混乱を招きかねないのは「分散」という用語で、何かが分散されると、全体を統制する当局や所有者が存在しなくなるという誤解につながる点です。分散型元帳の場合は、これが該当する場合もあれば該当しない場合もあり、それは元帳の設計次第です。実際には分散型元帳モデルは多種多様で、さまざまな業務のニーズに合わせ、集中管理の度合いが異なる、多様なアクセス制御形態があります。これには、誰でもデータを元帳に記入できるが、元帳を所有することはできない「許可不要型」元帳と、1 人または複数の所有者が存在し、彼らだけが元帳への記録の追加やその内容の確認ができる「許可型」元帳があります。

ここで重要なことは、政府も民間部門も、技術を十分に理解することで、特定の目的に最も適合する設計を選択する際に、セキュリティおよび集中管理という要素と、各種組織と個人間におけるデータ共有の利便性や機会という要素の、バランスを取ることができるということです。

新しい技術がどれもそうであるように、将来どのような利用や乱用があるかを完全に予測することはできません。そして、いかなる新しい技術も、その技術が「それ自体」良

いものか悪いものかという点は問題ではありません。問題となるのは、その技術が何に応用され、どのような目的を有し、どのような形で応用されるか、そしてどのような保護手段があるか、なのです。

これらの問題に答えるため、政府科学局（Government Office for Science）では産・学・官の専門家による上級顧問グループを設置して、政府および民間部門における分散型元帳利用の可能性を検討し、分散型元帳技術の有効利用と、起こりうる弊害の回避のために必要な政府や他の機関の実施策を決めることとしました。同グループの目的は、この技術に使われている用語を政策に関わる人々にわかりやすく解説すること、そして、対策が必要な分野とその対策の実施方法を政策立案者が決定するのに、役立つビジョンと根拠を彼らに提供することにありました。

要するに、分散型元帳技術は、政府が不正行為や汚職、過誤を減らし、また、紙を大量消費する処理形態に要するコストを削減するための枠組みを提供するものです。この技術はデータの共有、透明性および信頼性に関して、政府と国民の関係を再定義する可能性を秘めています。また民間部門でも同様の可能性が期待できます。

本要旨では、我々の検討会議で得た主要 8 項目の勧告を提示しています。これらの勧告は、ビジョン、技術、ガバナンス、プライバシーおよびセキュリティ、破壊的な可能性、応用、ならびにグローバルな視点に関する重要ポイントに基づいており、続く 7 つの章でそれぞれ詳しく説明します。これらの章は、分散型元帳技術の専門家によって専門家以外にも理解できるように執筆されています。これら専門家の方々のご指導、ご配慮ならびにご貢献に対して心より感謝いたします。

マーク・ウォルポート卿（Sir Mark Walport）
英国政府チーフ科学顧問（Chief Scientific Adviser to HM Government）
2015 年 12 月

ビジョン

分散型元帳は、政府やその他の公共部門および民間部門のさまざまな組織において、数多くの恩恵をもたらします。その名前が示唆するように、分散型元帳は正確に管理された形式で非常に広い範囲に分散させることができます。元帳の変更の際に必要な許可を得て行なわれた、参加者による変更はすべての元帳に即座に反映されるため、非常に効率的です。また元帳は不正な変更を受け付けないように堅牢に作られており、元帳を破損させるのはきわめて困難です。しかし分散型元帳それ自体を、目的であるとみなしてはなりません。元帳にスマートコントラクトなど他の応用技術が加わったときに、はじめてその潜在的な力が完全に発揮されるのです。

分散型元帳の発展を支援するにあたり政府が最初に担う役割は、この技術によって政府の業務のやり方や国民に対するサービスの提供方法が、どのように改善するかについて明確なビジョンを定めることです。次に、政府は適切な分野に分散型元帳ソリューションを導入し、専門知識を持った顧客として、この技術を実際に利用する必要があります。そうすることで政府は、新規事業者、成長過程の企業、および既存の大企業を含め、この分野の経済活動の進展を支援し、影響を及ぼすことができます。

これは、政府が将来的に、よりいっそう個人に合った直接的で効率的なサービスを行えるようになる良い機会です。また、必要に応じてスマートコントラクトに参加することで、国民は各自の好みとニーズを伝える機会を持てるようになります。分散型元帳にスマートコントラクトを埋め込んだ形式で応用することにより、コンプライアンス、費用対効果、説明責任の面で大きな向上が期待できます。

政府デジタルサービス（Government Digital Service）は、政府によるサービス提供のためのデジタルプラットフォームを開発中ですが、分散型元帳はその核心部分となる可能性があります。

第 1 の勧告：政府がすべきこと：

- **政府内での分散型元帳技術採用に関して、政府が確実にビジョン、リーダーシップ、プラットフォームを提供できるように、閣僚レベルでのリーダーシップを発揮する。特に、政府デジタルサービスが分散型元帳のユーザーとして政府内での導入事業を先導し、DCMS デジタル経済ユニット（DCMS Digital Economy Unit）が、分散型元帳の推進役として政府における導入事業を先導する（ビジネス・イノベーション・技能省（Department of Business, Innovation and Skills）および Innovate UK と共同して行う）。**
- **政府デジタルサービスおよび DCMS デジタル経済ユニットは、本報告書の作業ならびに各部局ですでに始動している初期段階の活動に基づき、大まかなロードマップとその実施を支える計画の概略を策定し、これを遅滞なく実行する。さらに本報告書の他の勧告の実施状況を監督し、迅速な対応を続ける。この導入事業を実施する際は、政府の他の部局および産・学と密接に連携し、支援を目的とした期間限定の専門家による諮問グループの設置も検討する。**

技術

分散型元帳技術はまだ開発の初期段階にありますが、ブロックチェーン技術の開発は、破壊的ともいえる元帳技術の一大革命に向けた非常に重要な最初のステップで、官・民とも、組織の活動を大きく変える可能性を含んでいます。この技術は原則として、全員（「許可不要型」元帳の場合）または承認を受けた少数もしくは１人の個人によって（「許可型」元帳の場合）元帳を「正当に」変更できるようにします。政府での応用としては、「許可型」元帳の方がビットコインの「許可不要型」のものより、採用される可能性が高いと考えられます。これは、１人または複数のデータ所有者が、システムの利用を許可する者と許可しない者を一定の規則で指定できるからです。さらに分散型元帳では、複雑なセキュリティ管理の多くは裏で処理されるため、システムが安価で利用しやすくなるという利点もあります。

この技術および関連技術の潜在的な能力を完全に引き出すためには、プライバシー、セキュリティ、パフォーマンス、拡張性の問題など、多くの未解決の問題に取り組む必要があります。一方、スマートコントラクトや署名機能などのアプリケーションをサポートすることにより、元帳をさらに洗練させるアルゴリズムを開発する機会も、非常に多くあります。これらによって、元帳利用の価値がさらに高まり、その利用範囲がいっそう広がることでしょう。この分野は急速に進化しており、これらの問題の多くについてはすでに調査がなされ、解決したものもあります。政府が「完璧な」解決法が生まれるのをただ待つだけでは、公共部門に最大の恩恵をもたらすことが期待される、この技術を応用する計画・導入する機会を逸し、その結果、国全体で経済的な恩恵を得る機会をも失う可能性があります。

さまざまな利用が考えられる中、分散型元帳技術の堅牢性と拡張可能性を確保するとともに、その倫理的および社会的な意味、および採用したときのコストとメリットについても理解する必要が生じます。研究開発に関して英国は好位置にいますが、世界各国が分散型元帳技術の開発に関心を寄せており、互いに競っているため、現在の地位に安住すべきではありません。

工学物理科学研究会議（EPSRC：Engineering and Physical Sciences Research Council）および経済社会研究会議（ESRC：Economic and Social Research Council）が主導する各種研究会議は、諸大学機関ならびに新たに創設されたアラン・チューリング・データ・サイエンス研究所の研究を支援するという重要な役割を務めています。ビジネスにも、研究開発への投資という重要な役割があり、またセキュリティ、プライバシー、基準の制定といった、いずれも競争ではなく協力することで恩恵を得られる一般的な問題に取り組むためには、官・民共同でこの重要な機会に対して投資を行う必要があります。

政府および民間部門がすでに実施しているデジタル分野への投資としては、デジタル・カタパルト・センター、未来都市創造センター（Future Cities Catapult）、オープンデータ研究所などがあります。これに加えてホワイトチャペル・シンクタンク（Whitechapel Think Tank）のような研究グループでは、議論とアイデアの共有が行われていますが、これは英国が分散型元帳に関する研究および試験能力を構築するという点で好位置にいることを意味します。しかし、このように一貫性のない活動からは、十分な価値が得られないおそれがあります。さらに官・民両方の研究開発コミュニティーが、必要に応じて協力を奨励し、最も創造的な研究を刺激する部分では競争を奨励するという、「自律的な組織」として機能することも求められます。

次の 2 つの勧告は、研究をさらに奨励し、英国がさまざまな分散型元帳ソリューションの試行と実験を行う能力を確立することを目指すものです。

第 2 の勧告：英国の研究コミュニティーは、必要な研究に投資し、分散型元帳が拡張可能で安全であり、内容の正確性を証明できることを保証できるようにする。この技術が採用されている分野にふさわしい高パフォーマンスで遅延の少ない稼働が提供されるようにする。また、エネルギー効率の良さも求められる。新設のアラン・チューリング・データ・サイエンス研究所は、ホワイトチャペル・シンクタンクなどの研究グループと協力して、この技術および関連技術に関心を持つ官・民の研究開発部門間の調整をして、それらの「自律的組織化」において重要な役割を果たすべきである。民間部門においては、最終的に新しく堅牢で安全な商業的応用を実現する研究を、アラン・チューリング・データ・サイエンス研究所が、各社間で競争が始まる前に支援できるようにするため、同研究所への投資を検討する必要がある。この研究には暗号化およびサイバーセキュリティのような関連性が明らかな分野における作業だけではなく、新しい種類のアルゴリズム開発も含まれる。

第 3 の勧告：政府は、地方自治体に対し、この技術とその応用試験のために必要な要素を網羅した、分散型元帳シミュレーターの設置を支援する。都市レベルのシミュレーターを設置することにより、分散型元帳技術の試行と実施の重要な機会を提供できる。たとえば、Innovate UK が「シティディール（都市協定）」の開発でいくつかの市と共同作業をした内容を活用して、市レベルのシミュレーターを開発することが考えられる。

ガバナンス

分散型元帳の実施を成功させる鍵となるのは、効果的なガバナンスと規制です。ガバナンスは、元帳の所有者と参加者が、彼らの個人的利益を守るために定める規則からなります。これには、広く公益を保護するため外部の当局が定めた規則の枠組みからなる、規則や立法による補完が必要になります。政府は法律を作り、単独でまたは地方自治体とパートナーとなり、規則の枠組みを作成し、通常は業務を行うために政府に報告する監督者を創設または指名します。

デジタル世界の場合、デジタル技術の運用を制御するための規則または規定は 2 組あります。1 組目は、法的枠組み、法令および規制により指定される旧来の意味での規則で、2 組目はソフトウェアにより符号化されたアルゴリズムの動作を決定する技術的な規則です。これは技術的な規則体系、いわゆるコードで、法規の遵守と同様、技術的コードの厳格な定めが確実に実行されることに重点を置く必要があります。

分散型元帳が効果的に運用されるには、参加者や利害関係者を保護するガバナンスと、システムの耐性を保証するための規則とを組み合わせる必要があります。それにより、システムや市場全体に波及しかねない、いわゆるシステマティックリスクや犯罪活動を防ぐことができます。同時に、システム参加者の利益および社会の広範な利益を保護するという目的と、過度に厳格な体制でイノベーションを抑制しないようにするという目的の間でバランスをとることが課題です。

また、法規と技術的コードが相互に作用する可能性があり、その活用も期待できます。たとえば現在のように完全に法規のみによるのではなく、法規と技術的コードとの組み合わせにより公的規制の影響力がより発揮されるるようにできます。つまり、技術的コードを、法規の遵守を確実に行うために利用し、これにより法規の遵守に必要なコストを削減できます。このような規制強化への技術応用事例として RegTech が挙げられますが、

これについては政府科学局によるFinTech報告書に主要な勧告の1つとして記載されています[1]。

ガバナンスと規則間の最適なバランス、および法規と技術的コード間の最適なバランスを見つけ、第3章に示すような主要な問題を解決するためには、法律家、数学者、コンピューターの専門家など異種の技能を組み合わせる必要があります。

第4の勧告：政府は、分散型元帳技術に関する規制の枠組みの導入方法を検討する。この技術が新たに実施・応用されていくのと並行して、規制も進化していかなければならない。政府が規制について検討する際には、法規とともに技術的コードを用いながら、いかにして規制の目的を達成するかについても検討する必要がある。この勧告についてはDCMSデジタル経済ユニットが管掌することとなろう。

セキュリティおよびプライバシー

犯罪者は金庫破りや銀行強盗にはもはや関心がありません。通貨は今やデジタル化・仮想化しつつありますが、このような仮想通貨は、デジタル世界のコードを解読するハッカーやクラッカーに対しては脆弱です。デジタル世界の暗号化されたコードを解読することは非常に困難ですが、どれほど困難であるとしてもそれがバイパスされてしまえば脆弱です。バイパスのメカニズムには、人間が誤って、または意図的にキーを他人に渡すことから、ソフトウェアコードに欠陥があるため「バックドア」（裏口）が存在することまで、さまざまです。これに加え、分散型元帳のホストとして使用されるハードウェアも脆弱性をもたらす可能性があり、ハードウェアシステムの耐性とセキュリティにも同等の注意を払う必要があります。

ビットコインの場合、通貨を保管する「ウォレット」には盗難の危険性があることが判明していますが、元帳自体の耐性が損なわれることはありません。原則としてコンピューターのビットコイン元帳処理能力の50%超が悪意を有する個人または組織に掌握されると脆弱になることが予想されますが、実際のところ、分散型元帳の大きな強みは攻撃に対する耐性の高さです。

しかし重要なのは元帳の整合性だけではありません。プライバシーと機密性保持も重要な問題です。元帳の性質により、金銭的なものから、家族や健康に至るまでさまざまな個人の秘密情報が保存されます。分散型元帳の技術によって、現在のデータベースと比較してこれらのデータに対するセキュリティは高まりますが、何もしなくてもそれが実現するわけではありません。この分野もこの技術を開発するうえでさらに研究開発が必要となります。

セキュリティとプライバシーは政府が重要な役割を担う分野です。次の勧告は以下の通りとなります。

第5の勧告：政府は産・学と共同して分散型元帳とその内容の整合性、セキュリティ、プライバシーに関する基準を定め、このような基準を法規とソフトウェアコードの両方に反映させる。

本技術を個々に利用していく際、政府や民間部門の利用者は、必要に応じ、関連する脅威を明らかにするための特別なリスク評価を実施する必要があります。国家インフラストラクチャー防護センター（CPNI：Centre for the Protection of National Infrastructure）および通信機器セキュリティグループ（CESG：Communications-Electronics Security Group）は、分散型元帳技術に関する情報を絶えず収集し、分

散型元帳の整合性、セキュリティ、プライバシー確保に関する専門的な助言を行ううえで、政府の内外で中心的役割を果たさなければなりません。第 2 の勧告にあるとおり、新設のアラン・チューリング・データ・サイエンス研究所は、ホワイトチャペル・シンクタンクなどの研究グループと協力して、CESG とともに、官･民の研究開発部門の調整と「自律的組織化」において重要な役割を果たすことができます。

今よりも優れた技術が生まれ、悪意を持つ者が「新しい犯罪テクニック」を身に付けていくのと同時に、ソフトウェアおよびハードウェアのシステムが時間の経過とともに劣化することを見過ごしてはなりません。そこで、長期間の使用が想定されるシステムでは、その寿命が来るまで、ハードウェアおよびソフトウェアのコンポーネントを容易に更新できるように、当初から設計しておく必要があります。さらにこの技術を新たに導入する場合、システムとユーザーの両レベルでの侵入テストを試用評価に含めることが重要です。

信頼性および相互運用性

グローバルな視点に関する第 7 章で述べるように、信頼とは複数の個人、組織、国家間におけるリスク判断です。サイバースペースでは、信頼性は本人であることの証明（認証）と、求めている行動を行うために必要な許可を得ていることの証明（承認）という 2 つの主要要件に基づいています。それに対して相手は、サービスまたは製品を安全で効率的かつ信頼できる方法で提供することで、自らの信頼性を証明します。

認証と身元確認は相互に関連していますが、同一ではありません。認証では認証者が相手方のアイデンティティを知っている必要はありません。しかしその相手方が認証者に対し、自らのアイデンティティと密接不可分な証拠、たとえばクレジットカードやデビットカードの暗証番号、または生体認証といった文書に関連付けられている指紋などを提出する必要があります。同様に、相手も認証の証拠を提供する際は、正しい人物または組織に対して提供している、つまり提供を受ける者が名乗ったとおりの者であるという確証が必要になります。そのため、組織が個人、他の組織、政府のいずれであっても、ユーザーに認証を提供できるようにすることが等しく重要です。

デジタル環境では、より強力で堅牢なアイデンティティ管理ツールを作成・利用することで、プライバシーを保護しつつも認証を提供することができるようになります。そのようなシステムの 1 つに、X.509 という暗号化基準に基づいた公開鍵インフラストラクチャー（PKI）があります。PKI を利用する組織では、認証連携（フェデレーション）により、サービスや製品の安全な配送を提供し、共有、さらに簡素化することができます。このほかに、法的組織登録（ROLO：Register of Legal Organisations）として知られる、組織の身元確認のための重要な国際基準が開発されているところですが、これが個人のかわりに組織を認証するための基盤となる可能性があります。

このほか、個人ユーザーによる安全な認証処理を実現する重要な技術として、「デファクト」（事実上）で信頼されているユーザーデバイスとしてのスマートフォンの利用があります。最新型のスマートフォンには、認証、暗号化、署名用のデジタル証明および暗号化キーを保護する「Trusted Platform Module（TPM）」や、「マルウェア」の干渉を防ぐ「Trusted Execution Environment(TEE)」および「Trusted User Interface(TUI)」のような、重要なセキュリティ機能が組み込まれています。

認証に関するこのような議論から、分散型元帳の力を最大限に発揮させるには、分散型元帳が他の元帳と相互運用の可能性を持つ必要があることがわかります。しかし相互運用の可能性を最大限に発揮させるには、認証の相互運用だけではなく、データの相互運

用、ポリシーの相互運用、国際基準の効果的な実施について合意が必要となります。

第 6 の勧告：（この勧告は第 5 の勧告と関連します。）政府は産・学と協力して、個人と組織の双方に関し、最も効果的で利用可能な身元確認および認証のプロトコルを実施することに努める。ただし、この作業は国際基準の策定および実施と協調して進めていく必要がある。

破壊的な可能性：政府業務における応用事例

分散型元帳には破壊的ともいえる潜在能力があります。その処理はリアルタイムで、改ざんはほぼ不可能、低コストであり、金融サービス、不動産、健康・医療、アイデンティティの管理など、さまざまな産業・サービスへの応用が期待できます。スマートコントラクトやモノのインターネット（IoT）といった、他のソフトウェアおよびハードウェア・ベースのイノベーションの基礎にもなります。さらに分散型の合意（コンセンサス）、オープンソース、透明性、およびコミュニティーという、分散型元帳の根幹をなす哲学により、このような分野の多くで破壊的な影響が与えられることが考えられます。

急進的イノベーションの例にもれず、分散型元帳は機会を提供する一方で、対応に失敗したり対応できない人々にとっては脅威となります。特に、分散型の合意という性質により、この技術は、銀行や政府機関のように従来、階層的な組織で管理的地位にあり、信頼できる仲介者という役割を務めてきた者にとっては、その役割に対する脅威として見られることもありえます。

政府はその利害関係者、サービス、役割が多岐にわたり、さまざまな業務を行っています。中には価値を創造するのではなく分配する部局もあれば、効果的な規制体制を作り、維持する部局もあります。分散型元帳によるイノベーションによって、このような活動の多くでさらに強化・拡大されるものもあれば、変化が強いられるものも出てくることでしょう。

最終的には、技術を発展させる最善の方法は、それを実際に利用することです。この報告書の作成を支援した専門家グループは、英国政府による応用の可能性が考えられる以下の具体例について検討しました。この 5 つの応用事例については第 6 章で詳述します。

- サイバー攻撃に対する重要インフラストラクチャーの防御
- 福祉支援の運用コストの削減と受給資格の追跡、ならびに利用可能な金融機関の種類の拡大
- 援助金使途に関する透明性および追跡可能性の確保
- 経済成長の機会創出、中小企業の支援および雇用拡大
- 脱税の減少

これらの事例ではそれぞれ、提案する分散型元帳の概要、それによってもたらされる可能性があるメリット、応用実施に必要な技術の成熟度の評価について説明しています。

この報告書で明らかにしているのは、応用可能性のうちのごく一部ですが、これらの事例が、政府の部局でこの技術の導入を試行する際の出発点となることを期待しています。そこで最後の勧告として、分散型元帳技術の試験的な実施と政府の能力開発を目標とすることを挙げます。

第 7 の勧告：分散型元帳の真の潜在能力を理解するためには、この技術を研究するだ

けではなく実際に応用して利用してみなければならない。政府は公的部門での技術の有用性を評価するため、分散型元帳の試験を行う必要がある。

この試用は、健全性を確保し、できる限り厳密なプロセスを確立できるようにするため、治験の実施、報告、評価と同様の方法で行うよう勧告します。また、試用の結果とそこで得られる教訓は、第 1 の勧告で提案されているロードマップに反映されるようにします。

応用が考えられる分野としては、国のインフラストラクチャーの保護、中小企業の市場摩擦削減、労働年金省（DWP: Department for Work and Pensions）やその他政府省庁からの資金分配などがあります。本報告書をまとめる中で、職員の一部は、政府による分散型元帳技術の応用可能性について、すでに深く考えていることが明らかになりました。このような職員を強力に支援し、政府省庁と政府デジタルサービス（GDS）間の連携を推進するよう奨励することを勧告します。

第 8 の勧告：トップダウンのリーダーシップとともに、政府内で能力と技能を養成する。関係省庁から分析および政策の専門家を集め、共同研究コミュニティーを創設し、将来「応用事例」となりうるものを開発し、行政サービスの知識と専門技術体系を築くよう勧告する。この共同研究コミュニティーの招集は、GDS ならびにデータサイエンス・パートナーシップ（Data Science Partnership）が中心となって行う。データサイエンス・パートナーシップは、GDS、国家統計局（Office for National Statistics）、内閣府（Cabinet Office）および政府科学局の連携である。また、これは、政府自身が分散型元帳アプリケーションを購買する顧客となり、民間企業に刺激を与える重要な機会となる。

結論：グローバルな視点を持つ

分散型元帳技術の重要性を認識しているのは英国に限りません。大小問わず、他の国々はすでに分散型元帳の採用にすばやく取り組み始めています。エストニアの事例でわかるように、たとえ小国でもデジタル化を理解している効果的なリーダーシップがあれば急速に発展できるのです。しかし、英国がこの先頭グループに入るにはまだ間に合います。むしろ英国経済に対する金融およびサービス部門の重要性を考えると、そうすることが必要不可欠なのです。

第 7 章で、パトリック・カレー（Patrick Curry）、クリストファー・シアー（Christopher Sier）、マイク・ホルソール（Mike Halsall）がデジタル先進国の特徴について考察し、次のような点を挙げています。

- 指導者層がデジタル化についてよく理解している。
- 国のデジタル化について権限を与えられ、国際的視野を持ち、あらゆる産業部門と密接に協力する政府の専門部局が存在する。
- 産業が主導し、政府が投資する実現可能で協調的な国家計画策定が行われている。
- どの政府組織にも技術に明るく、資格と経験を有し政策に携わる上級幹部が配置されている。
- 政治家とともにエンジニアおよびデジタルビジネスのリーダーが存在する。

情報技術によって推進されている、このすばらしいポスト産業革命は、まだ始まったばかりです。これは新しい重要なメリットとリスクをもたらす革命なのです。この革命では、分散型元帳技術の到来により、既存のビジネスのやり方に大きな変革が訪れ始めている

ことは明らかです。

最も古い人間の会計記録は、はるか 5,000 年も前のバビロン、アッシリア、シュメールに遡ります。記録、集計、通貨の進歩における初期の技術革命を示すものとして多くの粘土板が残っています。デジタル記録が粘土板ほどの長い寿命を持つかどうかは定かではありません。しかし、それを別にしても英国にとって、国民および経済に恩恵をもたらすために、分散型元帳技術を進歩させ利用する大きな機会があることは明らかです。情報技術の画期的な発展に伴い、その恩恵を最大限に得つつ、弊害を最小限に抑えるための課題に取り組む、一連の「グランド・チャレンジ」が行われています。本報告書では、専門家の根拠に基づき、政府に対して重要な勧告をいくつか提示しています。これらの勧告で最も重要な点は、英国内の官・民で、また英国と諸外国との間で、密接なパートナーシップが必要であるという点です。

定義

この新しい分野の用語は進化の途上にあり、多くの人がブロックチェーン、分散型元帳、共有元帳などの用語をほぼ同じ意味で使っています。すべての人を満足させるような正式の定義になるとは限りませんが、本報告書では主な用語を次のように定義します。

- **ブロックチェーン**はデータベースの一種で、多数の記録を（1 枚の紙に並べるのではなく）ブロックに保存するものです。そして、これらの各ブロックは暗号化された署名により後続のブロックに「チェーン」でつながれます。これによりブロックチェーンを**元帳**のように利用し、その元帳は適切な許可を得ていれば誰でも共有し、補強することができるようになります。

  元帳の正確性を補強するには多くの方法がありますが、そのような方法は一般的に合意**（コンセンサス）**といわれています（「マイニング（採掘）」という用語は、暗号通貨であるビットコインで、このプロセスの変形に対して使用されています）。以下を参照。

  このプロセスへの参加者が事前に選択されている場合、この元帳は**許可型**です。誰でもこのプロセスに参加できる場合、元帳は**許可不要型**です。以下を参照。

  ブロックチェーン技術が真に画期的である点は、それが単なるデータベースを超え、取引自体と結び付けられた取引規則（ビジネスロジック）も定めることができるという点です。これが従来のデータベースとは異なる点です。従来のデータベースでは、通常、規則はデータベース全体またはアプリケーションレベルで定められ、取引レベルでは定められていません。

- **許可不要型元帳**（ビットコインなど）には単一の所有者は存在しません。というより、元帳を所有することはできないのです。許可不要型元帳の目的は、誰もが元帳にデータを加えることができ、元帳を保有する人は全員、同一の元帳のコピーを所有できるようにすることです。これにより検閲耐性 (censorship resistence) が生まれます。つまり取引が元帳に追加されることを、どんな人や組織、あるいは外部システム（アクター）も妨げることができなくなるのです。参加者は元帳の現状について合意することにより、その整合性を維持します。

  許可不要型元帳は、編集不可能な全般的な記録（たとえば遺言および証言、または不動産の所有権譲渡）として利用できます。しかしこのような元帳は、組織の権力構造や既存の産業に対する挑戦ともなりえ、政策的対応が必要になる可能性があります。

- **許可型元帳**には 1 人または複数の所有者が存在します。新しい記録が追加されると、元帳の整合性が限定的な合意プロセスによって確認されます。これは信頼できるアクター（たとえば政府部局または銀行）によって実施され、許可不要型元帳で行われる合意形成プロセスよりも、共有されている記録の維持がはるかに簡単になります。許可型のブロックチェーンでは、合意形成プロセスでデジタル署名が作成され、それをすべての当事者が見ることができるため、データセットを高い精度で確認することができます。記録の検証に多数の政府部局の参加が必要になれば、たとえば部局間で紙ベースでデータを共有しなければならないことが多い現状に比べ、記録のセキュリティ面での信頼度が高まります。許可型元帳は通常、許可不要型元帳よりも速く処理されます。

- **分散型元帳**は複数のサイト、国、組織間で分散し、通常は公開されているデータベー

スの一種です。記録はブロックにまとめられるのではなく、連続する元帳内に順番に保存されますが、記録が追加されるのは参加者が定足数（クォーラム）に達したときに限ります。

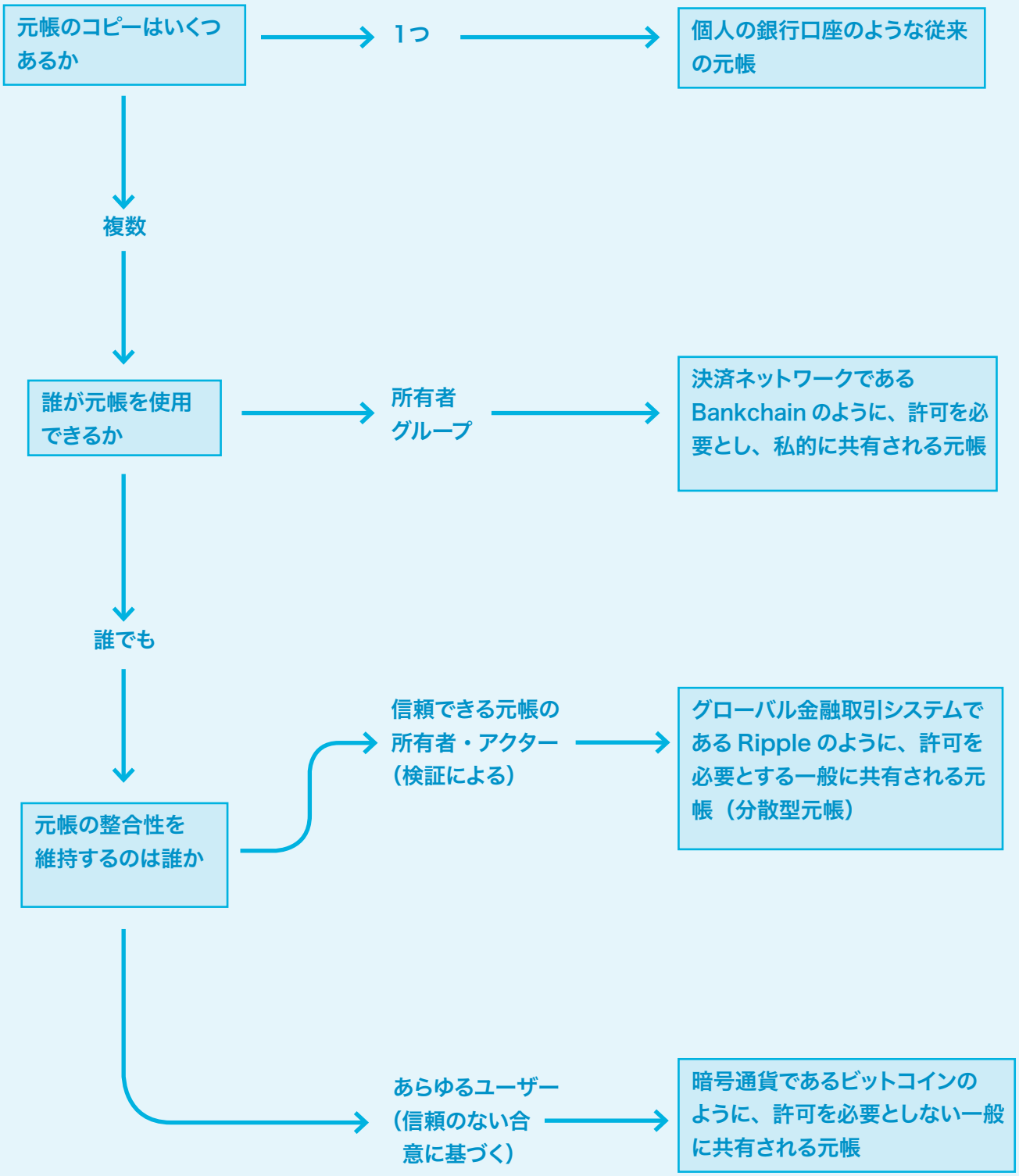
分散型元帳では元帳の検証者または運用者への信頼が求められます。たとえばグローバル金融取引システムの Ripple では、取引に参加しているアクターに対する詐取行為に加担しないとして信頼される、最大 200 人の既知、未知、または部分的に既知の検証者を選び、固有ノード検証者のリストが作成されています。このプロセスのデジタル署名は、ビットコインと比べて検閲耐性は弱いのですが、はるかに処理が速いと考えられています。

- **共有型元帳**は、かつて IBM に勤務し、現在は Distributed Ledger Group の最高技術責任者（CTO）であるリチャード・ブラウン（Richard Brown）が生み出した用語で、通常は産業界または民間コンソーシアムで共有されている、または一般に公開されているデータベースおよびアプリケーションを意味します。これはこの種の技術を最も包括的に表す用語です。

  共有元帳には、その根幹となるデータベースとして分散型元帳またはブロックチェーンが利用されますが、多くの場合、ユーザータイプ別に許可レベルが設定されます。それゆえ「共有元帳」は、一定のレベルで許可を与えることが可能な一連の元帳またはデータベース設計を意味します。たとえばある業界の共有元帳で、一定の限られた数の検証者に対し、この元帳の維持を行う者としての信頼を与えることができれば、大きなメリットを提供できることになります。

- **スマートコントラクト**は、その条件を法的な言語ではなくコンピューター言語で記録する契約です。スマートコントラクトの履行は、適切な分散型元帳システムのようなコンピューティングシステムで、自動的に行うことができます。スマートコントラクトの潜在的なメリットとしては、契約締結、その執行、およびコンプライアンスにかかるコストが安く、その結果、無数の少額取引について契約を締結しても経済的に引き合うという点などが挙げられます。しかし契約の履行をコンピューティングシステムに依存するといった潜在的なリスクがあります。今の段階ではスマートコントラクトの技術はまだ初期のもので、広く普及するまでには時間がかかるため、これらのリスクやメリットは主に理論上のものです。

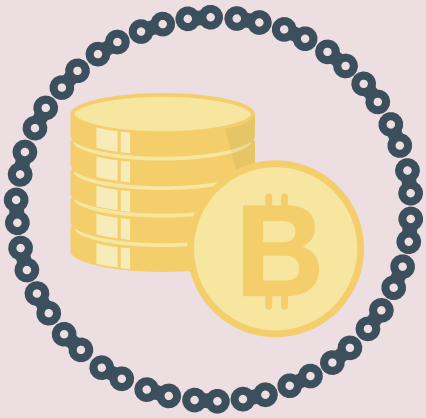
分散型元帳の分類



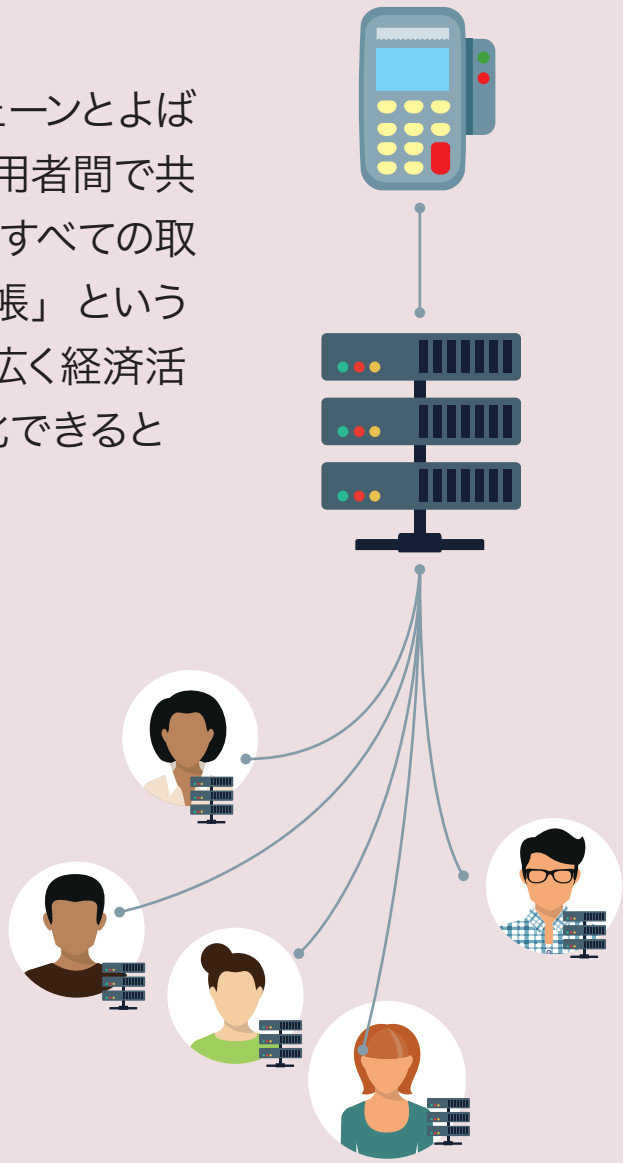
図提供：デイブ・バーチ（Dave Birch）、Consult Hyperion

第1章

ビジョン



ビットコインなどの仮想通貨は、ブロックチェーンとよばれる技術が根幹となっています。これは、利用者間で共有される分散型元帳の複数の同一コピーに、すべての取引を記録するという技術です。この「共有元帳」というアプローチを利用することによって、政府や広く経済活動で取引される多種大量のサービスを効率化できるという可能性が期待されています。



著者
サイモン・テイラー（Simon Taylor）
バークレイズ ブロックチェーン研究開発担当副社長
（VP、Blockchain R+D、Barclays）

第１章：ビジョン

はじめに

ビットコインなどの仮想通貨では、従来型の取引に先駆けて、金融取引を追跡するための新しいアプローチが採用されています。その根幹となっている技術は一般的にブロックチェーンとよばれていますが、これは、通貨の利用者間で共有される分散型元帳の複数の同一コピーに、すべての取引を記録するという技術です。

金融機関、規制当局、中央銀行および政府では、現在、この「共有元帳」というアプローチを利用することによって政府や広く経済活動で取引される多種大量のサービスの効率化が図られています。

これらの応用可能性の多くは中期的な予想ですが、政府および民間部門での開発サイクルが長期にわたることや、著しい効率性の向上があると早くからいわれていることを考えると、政府閣僚や公務員は、この技術によって、自分たちにどのような利益がもたらされるかについて、今から考えていく必要があります。この章では、これらの可能性についてまとめています。

共有元帳とは

共有元帳とは本質的に、ダイヤモンド、通貨、あるいは輸送コンテナの中身などの金融資産、実体資産、あるいは電子資産の所有者を追跡するデータベースです。重要な点は、参加者全員がブロックチェーンのコピーを保持することができ、各コピーは新しい取引が行われるたびに自動的に更新される点です。情報のセキュリティと正確性は、元帳のすべてのコピーが互いに一致するよう、数学、特に暗号化によって維持されています。今日、紙形式の元帳に存在するほぼすべてのものを、共有元帳に存在させることができます（共有元帳技術についての詳しい説明は第２章を参照）。

ビットコインは、2008 年の誕生以来、ブロックチェーン技術を基盤としています。仮想通貨、およびその基盤となっている原理については、多くの固定観念や誤解が生じており、シルクロードとよばれるデジタル闇市場と関連づけて、ビットコインは本質的に資金洗浄やテロリストとつながっているとの印象が、一部の人の中に植えつけられています。そのような誤解が人々のブロックチェーン技術に対する考え方に影響を与え続けています。

しかし実際には、共通の元帳およびデータベースというシステムは、ブロックチェーン技術の４つの重要な特性によって、政府や金融サービスに大きな利益をいくつかもたらす可能性があります。

1) **暗号化による照合：**現在、民間ビジネスや政府機関では、取引の詳細についてメッセージを送信することで、相互に伝達しています。メッセージを受信すると、各機関は自分の元帳を更新します。しかし、これらの元帳が一致することを保証するための簡単な方法はありません。ブロックチェーンでは、基盤となる同一データを単に共有したり、データ認証用の「プルーフポイント」を提供したりするなど、いくつかの方法によって、この問題を解決できます。この方法は政府機関の各種データにも適用できます。各種合意形成アルゴリズム（たとえば、プルーフ・オブ・ワーク、プルーフ・オブ・ステーク、実用的ビザンチン・フォールト・トレラントス）によって、元帳を共有利用するさまざまな当事者（ユーザー）が、取引の基盤となるデータの状態について合意できるようになります。

2) **多数機関での同一コピーの複製：**多くの当事者が、データの一部あるいは全部のコピーを保持することができるため、システム全体に障害をきたすような、単一障害点が存在する可能性が減少します。複製は現在のデータベース技術において大きな問題となっており、産業や政府の IT プロジェクトでコストの増加や複雑化などの問題が生じています。この技術のもう 1 つのメリットは、1 つの元帳が攻撃にさらされた場合でも、残りの元帳に影響が及ばない点です。また多くの当事者が、各自、照合計算を行うことにより、これらの記録が追加されたことを確認することもできます。

3) **詳細なアクセス制御:**分散型元帳では、どの当事者がどのような操作を実行できるかについて、共有される元帳内で、「キー」と署名を使用して制御されます。これらのキーには、一定の条件のときに限り特定の権限を割り当てることが可能です。たとえば、規制当局に対してある機関のすべての取引を閲覧することが可能な「ビューキー」を与えるが、それは裁判所が所有している別のキーでそのような閲覧が許可されている場合にのみ限定される、というように設定できます。

4) **高い透明性とプライバシー：**多くの当事者が（1）元帳のコピーを保持し、（2）すべての記録を確認できるため、共有元帳では高い透明性が確保されます。これによって規制当局あるいは司法当局などの独立機関は確信を持って、データベースの内容が不正に編集あるいは変更されていないか、検証できるようになります。また適正な条件であれば、これらの独立機関は、当事者以外は閲覧不可能な個人情報のロックを解除できるようにもなります。これは銀行などの民間企業が、規制当局へ報告をしたり不正を防止したりするうえでも有用で、さらには市民が政府の説明責任を追及するうえで武器にもなります（詳しくは第 5 章を参照）。記録は、暗号化された固有の署名を伴って追加されますが、この署名は正しい参加者が正しい規則に従って正しい記録を追加したことの証明となります。

これらの特性を組み合わせると、従来は非常に高コストまたは困難であった課題が解決する可能性があります。

スマートコントラクトとは

ブロックチェーンがデータベースであるとすると、スマートコントラクトは、ブロックチェーン技術で約束される大部分を現実化する、アプリケーション階層に該当します。概して、従来の契約は、その契約を実行するコンピューターコードとの直接の関係はありませんでした（第 3 章参照）。多くの場合、契約は紙媒体で保管され、その契約の条件を近似的

図 1：
従来の契約ではその契約を実行するコンピュータコード（アプリケーション）との直接の関係はない。

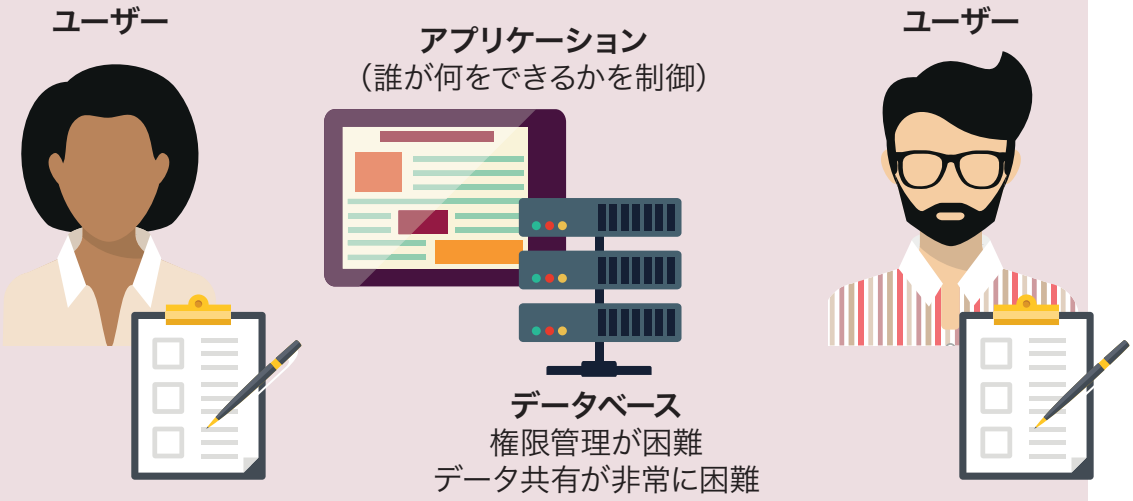


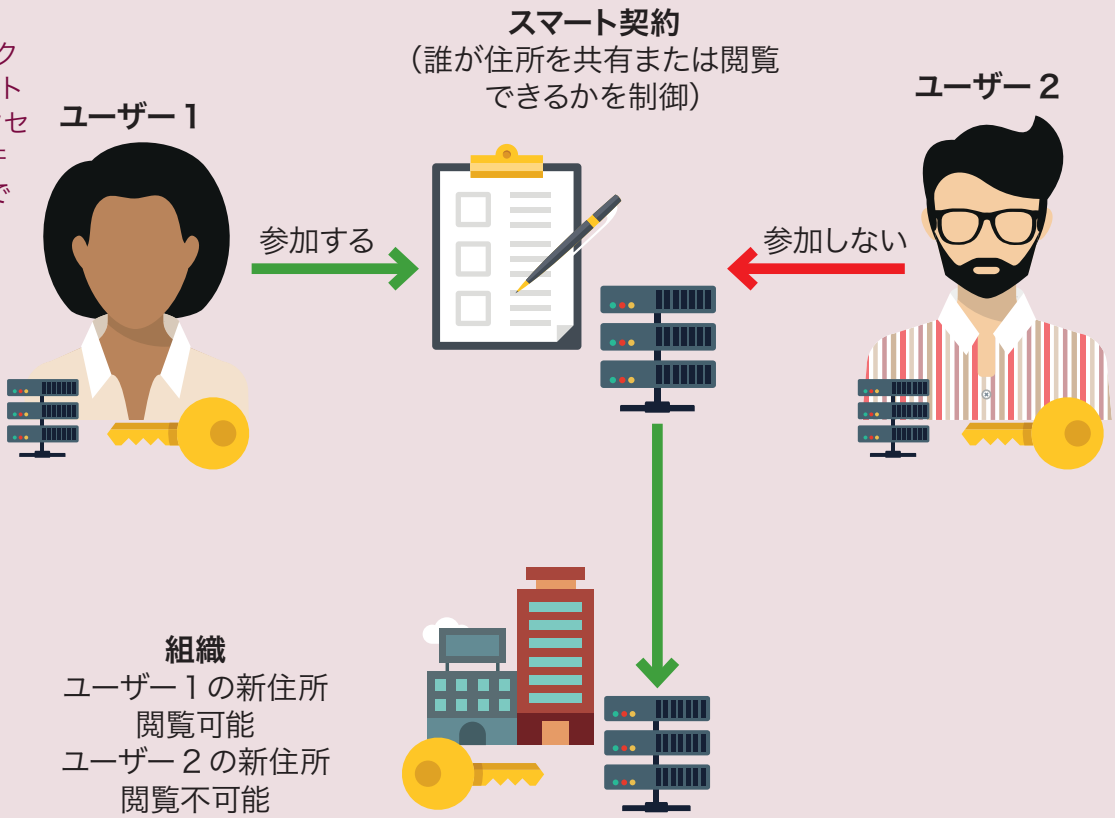
図 2：
スマートコントラクトには契約を実行するコンピューターコードが含まれている。

にコンピューターコード化したものをソフトウェアが実行します（図 1 を参照）。

これは、ビデオオンデマンドといった単一サービスの利用に登録する場合には著しく効果的ですが、複数の政府機関のデータベースで住所を更新する場合など、単一ユーザーに対して複数の複雑なサービスを提供する場合には、非常に難しい課題が生じます。この結果、個人の機密・プライバシー管理を確実に行うために、より複雑なデータ保護法・データプライバシー法が必要になりました。さらに広く経済活動においては、データ共有あるいは契約締結等の活動は、自動化されず紙媒体の形式のまま残っています。

共有元帳の主な特性（暗号化による照合、多数機関での同一コピーの複製、詳細なアク

図 3：
スマートコントラクトではプライベートなデータへのアクセスをどの機関に許可するかを制御できる。



セス制御および高い透明性とプライバシー）をスマートコントラクトと組み合わせ、一定の条件でデータの複製・共有を認めることにより、これらの課題に対処する機会が生まれます。2 人のユーザーがスマートコントラクトに署名すると、その契約には、共有される元帳内のすべてのデータに適用される論理が含まれることになります（図 2 を参照）。これにより、政府や民間部門の諸組織における自動化の促進や手作業の削減をすることができ、生産性向上と成長に役立つ可能性があります。レガシーデータベースの管理や処理といった他の課題があるものの、この複数システム間での「許可」という概念こそ、スマートコントラクトの本領が発揮される点です。

別のシナリオ（図 3）では、ユーザー 1 が、ブルーキーを保持する機関と共有元帳で住所を共有する、スマートコントラクトに参加します（別の多種多様なキーを保持する他の機関が多数存在する可能性あり）。しかし、ユーザー 2 は住所の共有に参加しないため、その機関が受け取る最新の住所のコピーは、ユーザー 1 からのもののみとなります。これは、たとえば個人が地元の自治体を介して住所を変更した場合、その変更がパスポート、運転免許証、その他主要部門のデータベースに反映されるため便利です。現在 Onename.io などのサービスがこの概念をソーシャルネットワークで利用していますが、いずれすべての機関に広がることが予想されます。

スマートコントラクトは、以下の部門で特に企業コンプライアンス、商品の追跡やサービス管理、さらに偽造品や詐欺対策などにおける幅広い利用が検討されています。

- 食品
- 金融サービス
- エネルギー
- 医薬品
- 医療・健康
- 航空宇宙産業
- 航空機産業
- 通信事業
- IT および通信
- 運輸
- 公共サービス
- 農業
- 石油ガス

これら利用例の一部については、本章および第 6 章と第 7 章で紹介します。

要約すると、スマートコントラクトは機械、企業あるいは人間がデジタル契約を作成する際に有用であり、暗号化によって、契約に参加するすべての当事者の元帳、データベースあるいは勘定において契約内容が履行されることを保証します。

将来へのビジョン

民主的な政府の大きな役割は、資源を個人および企業両方に適切に配分することです。これには金銭的資源の配分にとどまらず、法治社会維持の条件としての保安や民主主義、経済条件としての自由市場の振興や低インフレの維持と安定、個人財産権の保護、契約の保証などの社会的無形資産も含まれます。そしてこの配分は、規則の定め方に関する国民と政府間の合意（公約と投票による）に基づきます。

このような民主主義モデルが発達するにつれ、政府機構（この配分が行われるメカニズム）が拡大および中央集権化し、結果、個々の国民との距離がますます広がっているとも言われています。

さまざまな種類の課税による（金銭的）資源の徴収は非常に複雑化し、費用もかかるようになり、また、同じことが福祉支援、助成金、年金による配分についても起きています。このように複雑化した理由の１つは、その中央集権的な性質であると言ってよいかもしれません。

民間部門では、このような中央集中型モデルでは顧客サービスが十分にできず、もはや経済採算性が悪く、電子商取引とデジタルによる利便性も十分に享受できていないことに気づき始めています。政府も国民の期待に民間部門と同じような方法で応えねばならない、つまりリアルタイムで、その個人に合わせたデジタルサービスをすべての政府サービスで提供しなければならないと認識され始めています。共有元帳およびスマートコントラクトを応用することで、この分野で政府が優位に立つ機会が生まれ、金銭的に余裕のある人だけでなく、最も必要とする人にも、技術の恩恵が享受されることを保証できるようになります。

この傾向は、あまり明確な形式をとらない「シェアリングエコノミー」の成長や、特にソーシャルメディアが牽引役となって活性化したアラブの春やオキュパイ（占拠）運動のような現象に見て取れます。これは、社会におけるコミュニケーションや組織化の方法が変わってきていることを示すものです。しかし、引き続き自由市場を拡大しながら契約を保証しつつ、このような動きを安全な方法で実現するやり方は今日までのところ未だありません。私たちが民主主義をオンラインに移行しない理由は、非常に費用がかかり、また、誰が何に票を投じたかを確認する方法が、非自由主義的で中央集権的な身元確認システム以外にないからであると、言われてきました。これを望ましくないとするならば、ブロックチェーン技術の特性（暗号を使った照合、多数組織間における同一コピーの複製、きめ細かなアクセス制御、透明性、プライバシー）を国民のメリットとなるように応用する可能性について考えていくべきでしょう。

さらに、政府がブロックチェーン技術の開発と展開に早期に関与することで、政府が簡素化され、コストを削減する機会が生まれます。これは、今よりも個人に合った即時的で、かつ、より民主的にもなりうるガバナンスの基盤の構築につながり、その結果、コンプライアンス、コスト効率、説明責任の面で大きな向上が期待できます。

ブロックチェーン技術の受容に向けてのステップ

共有元帳技術は、米国、中国、シンガポール、ラテンアメリカなどの世界の主要経済圏で積極的に推奨され、開発が行われています。英国にとっては、この新しい分野を理解し、成長を支援することにより、この競争に参加する良い機会であるといえます。

政府による分散型元帳技術への関与の可能性は、次の 3 つの観点から見ることができます。

- 国民へのサービス機関としての政府
- 立法者としての政府
- 経済に対する奉仕者としての政府

国民へのサービス機関としての政府

国民へのサービスの中にはこの技術の影響を受ける重要なものがいくつもあり、特に、モバイル技術のプライバシー、データのポータビリティー、知覚･認識機能という重要な点に関する有用な応用事例がいくつかあります（これらの事例の詳細は第 6 章を参照）。

立法者としての政府

分散型元帳の技術はまだ成熟しておらず、さらに発展サイクルが何回か繰り返されると考えられます。そのため、この技術の発展プロセスにおける政府の対応では、次の 3 つの目標を目指すことになるでしょう。

第 1 の目標：新たに出現したエコシステムの支援
ビットコインのエコシステムにも、またその他の共有元帳システムにも、すでに仮想通貨の両替システム、「ウォレット」プロバイダー、およびその他のサービスプロバイダーが多数存在します。この技術とビジネスがさらに成熟していくことを考えると、第 1 の目標のために行う活動には次のようなものが考えられます。

- 顧客の身元を確認するためのやり取りの要求（「顧客を知る（KYC）」の規制）。
- このスペースにおける次のような企業形態の違いを示す、融部門向け指針の発行：(i) ブロックチェーンシステムを介して価値を移転する者、(ii) ブロックチェーンを利用する業界にソフトウェアを提供する者、(iii) 従来のビジネス上の問題を解決するためのブロックチェーン・ベースのソフトウェアを提供する者。
- ウォレットプロバイダー向けのセキュリティ基準の策定。
- ブロックチェーンのエコシステムに固有の、次のようなギャップを検討することを目的とした、学会およびスタートアップエコシステムに課する課題の設定：(i) 適切な技術アーキテクチャーの確立、(ii) 技術を利用した顧客のアイデンティティ確認の精度向上、資金洗浄対策、犯罪防止の方法の確立、(iii) 政府・国民の新しいユーザー体験を作り、政府によって所有される自己に関わるデータを、国民がより確実に管理および監査できるようにするための、マルチシグネチャ・ウォレットの利用法の確立。
- 政府と産業界間の協調と対話を維持するためのパートナーシップの活用。

第 2 の目標：早期の試用およびパイロットプロジェクトの実施
政府は機に乗じて、早期に事例の実地試用を行うと良いでしょう。その際、政府が特に検討すべき課題には次のものが考えられます。

- 共有元帳またはデータベース技術で恩恵を受ける主な公益事業には、どのようなものがあるか。
- この試用では、政策のどの部分が支援される可能性があるか（年金改革、福祉改革など）。
- この試用から最も多くが得られると期待されるのはどの分野か。

第 3 の目標：グローバル競争で英国をリーダーの地位に就かせる
今日まで、ベンチャーキャピタルによる分散型元帳技術への投資の多くは、ビットコインと米国西海岸に集中してきました。しかしこの技術の新たな機会は他の応用分野にあります。

- 英国はこの意味合いを認識し、規制体を通じてそのような効果がもたらされるようにするための指針を作成する（ガバナンスおよび規則については第 3 章を参照）。
- 英国は、このような技術の中核的研究拠点を設け、これをグローバル FinTech または英国貿易投資総省（UK Trade and Investment）の検討課題に追加する。

経済に対する奉仕者としての政府

政府がいかにして、この技術がもたらす恩恵を最大限に奨励し、実現させることができるかについて理解するには、金融サービスと、保険およびその他の産業という、2 つの異なる分野における応用事例を見てみるとよいでしょう。

金融サービス
金融部門におけるこの技術の応用としては次のようなものがあります。

- 資本市場での効率向上
- 詐欺行為の防止および貿易金融の効率向上

1. 資本市場での効率向上

資本市場では、取引の相手方との照合を紙の記録に依存しています。これまで集中管理機構は作られてきましたが、今日、取引の相手方の合意を確認するには、信頼が必要であるため、取引を照合し（「決済」）、これを行う能力があることが重要です。銀行の科料や固定費の多くは、信頼という概念に基づき算出されています。本質的に銀行は他の銀行の処理を信頼するしかなく、その銀行の行動を確認する方法はありません。しかし、規制者も確認できる方法で取引のチェーンを開示し（暗号を用いた照合）、関与しているアクターも明らかにするブロックチェーン技術によって、これを解決できる可能性が出てきたのです。さらにこのデータの監査にはコストがかかるうえに、それが行われるのは取引実行後です。大手銀行では効率向上のため、現在この技術を基にした適切な連携手段が検討されています。

2. 詐欺行為の防止および貿易金融の効率向上

貿易金融は数千年間ほぼ同じやり方で行われてきました。通常、ある品物の売買に少なくとも 5、6 人の当事者（たとえば買い手、買い手の銀行、船会社、運送会社、売り手、

売り手の銀行）が関与します。貿易金融の標準化と集中機構創設の試みはこれまでにもありましたが、共有元帳には固有のメリットがいくつかあります。

- 「部分許可型」システムによって、紙の書類（たとえばコンテナ内の製品の名前、数量、色などを記載している船荷証券）の安全な署名が可能になります。その後、この書類は（署名可能な形式、かつデジタル形式で）各当事者により署名されます。（主な特性：**高い透明性、暗号を用いた照合**）
- 共有元帳システムでは、今日行われているように単に書類が保存されるだけでなく、このような書類の状態の証明が記録されることになります。これが普及すれば、書類を印刷して署名するのではなく、共有元帳を使って配布することが可能になるでしょう。（主な特性：**高い拡張性と容易な複製**）

産業界および諸機関

1. 資産の追跡および出所の保証

美術品や電化製品など多くの品物には、物理的なデジタルマーカーが付けられています。しかしこれらの品物を追跡し、どの資産が管理されているかについて、誰が確認できるかを決める許可制御能力を持つグローバルな機構は存在しません。多くの組織では原産地の証明を紙の書類に頼っています。しかし流通経路を示す書類が偽造された場合は、原産地を確認する手段がありません。そのサプライチェーンの一部に共有元帳が使用され、デジタルで「署名」されるなら、その書類がいかなる方法でも修正または偽造されていないことが、全当事者にとって明らかとなります。

たとえば Provenance.org は、ブロックチェーン技術を使い、小売業者に衣料品の出所と持続可能性についての信頼性を提供するスタートアップの組織です。現在、小売業者は衣料品の出所を確認するのに、紙の書類に依存していますが、その書類を、正当な人物が正しい時間に作成したかを確認する方法はありません。ブロックチェーン技術を利用すると、適切な人物がプライベートキーを使い契約にデジタルで署名することができ、正当な権限を持つ人物が正確な日付と時間に書類に署名したということについて、高い信頼性が得られます。さらに、ブロックチェーン技術の性質によって、適切な権限を持つ小売業者全員がこれを確認することができます。

2. 限定ユーザーによる機密データの使用

データの正確性と機密データの共有は、組織にとって重要な課題です。保険会社では、信頼できる者（政府または銀行など）によって正確であると検証された追加のデータを入手できれば、より正確な商品を作り、適正な価格、保険料を設定することができます。難しい点は、これを安全に行うのと同時に、確実に国民が自らのデータを管理し続けるようにするという点です。

ブロックチェーンでは、Guardtime のようなソリューションを使うなどして、すべてのデータにどのようにアクセスされたかに関する証拠が提供されます。たとえば ARM 社の TrustZone チップなどの携帯電話用の信頼された実行環境（TEE）を用いることで、政府保管データへのアクセス要求はすべてブロックチェーンに記録されることになります。国民が保険会社に許可を与えない限り、このデータは動かせません。そのデータに変更を加えたり、アクセスしようとしたりすると、その国民または所管する当局に速やかに通知されます。

共有元帳技術に単純な携帯電話ユーザーインタフェースを組み合わせることで、多くの複雑なセキュリティ管理が背後で処理されるようになる可能性があります。この方法の採用を検討している組織は一般社会の信頼を獲得する必要があり、そのためには早期試用の実施が役立つことでしょう。

3. 産業機器（「IoT」に接続）

運輸、公共事業、農業などのさまざまな部門で、産業機器に関する正確なデータをリアルタイムで集めるのは困難です。モノのインターネット（IoT）が出現して、いくつかの課題は、低価格になったハードウェアを用いることで解消されてきていますが、これは攻撃に対して脆弱である可能性があります。IBM Institute for Business Value の最近の報告[2]では次のように述べられています。

> 「結果：何千億もの低価格・高性能デバイスが急増し、低価格にもかかわらず複雑な統合システムの一部として運用できるようになりました。」
>
> 「IoT スケールのネットワークでは信頼を構築するのは非常に難しく、保証するのは不可能ではないとしても高価になります。IoT はますます拡大し、利用されることが多くなっていますが、ユーザーが自らプライバシーを制御できるようにするという形態で、プライバシーおよび匿名性が設計の中に組み込まれていなければなりません。クローズドソース・アプローチに基づいた現在のセキュリティモデル（「隠蔽によるセキュリティ」と呼ばれることが多い）は、透明性によるセキュリティという新しいアプローチで置き換えられる必要があるのです。」
>
> 「私たちが持つ分権型 IoT のビジョンでは、ブロックチェーンは、取引の処理と、相互作用するデバイス間の調整を可能にする枠組みです。それぞれが自分の役割と行動を管理し、それにより「分権的かつ自主的なモノのインターネット」、すなわちデジタル世界の民主化が実現するのです。」

各デバイスが自律エージェントとしても、全体の一部としても機能するようになれば、単一障害点は存在しなくなります。この応用事例では、組織は IoT デバイスを応用することにより、政府科学局の IoT に関する最近の報告書に概要が記載されているように、リアルタイムデータと接続性に関連したさまざまなメリットを得ることができます[3]。共有元帳とブロックチェーン技術によって、セキュリティの高い IoT を備えた新しいビジネスおよび技術のモデルが実現されます。

例 1：自律ユニットとして稼動するトラクターで、一定地域の農家からのアクセスを許可できるようになり、これによって従量制課金リースモデルが可能になります。また、このトラクターには気候データの収集および支払機能が備わっており、メンテナンスおよび修理のため製造元と連絡をとることもできます。

例 2：純正で許可されている産業機器であれば、その機器の新しい部品を発注することができます。また、機器の性能あるいは効率性に基づいた、新しいローン方法や新しい市場の誕生にもつながる可能性があります。

結論

この技術により、国民に対する説明責任がより重視される、ある種の「ガラス張りの政府」が将来実現すると思い描くことができます。数多くの応用事例がすでにあり、技術が発展するにつれ、さらに多くの応用が出てくることはほぼ確実であり、これは政策目的の達成に役立つことが期待されます。政府の閣僚および官庁の重要項目として次の点が挙げられます。

この技術はまだ初期の段階にありますが、大きな可能性を秘めています。ブロックチェーン技術の可能性を引き出すためには、以下の特性を組み合わせて利用することで、さまざまなことが実現されるということを理解する必要があります。

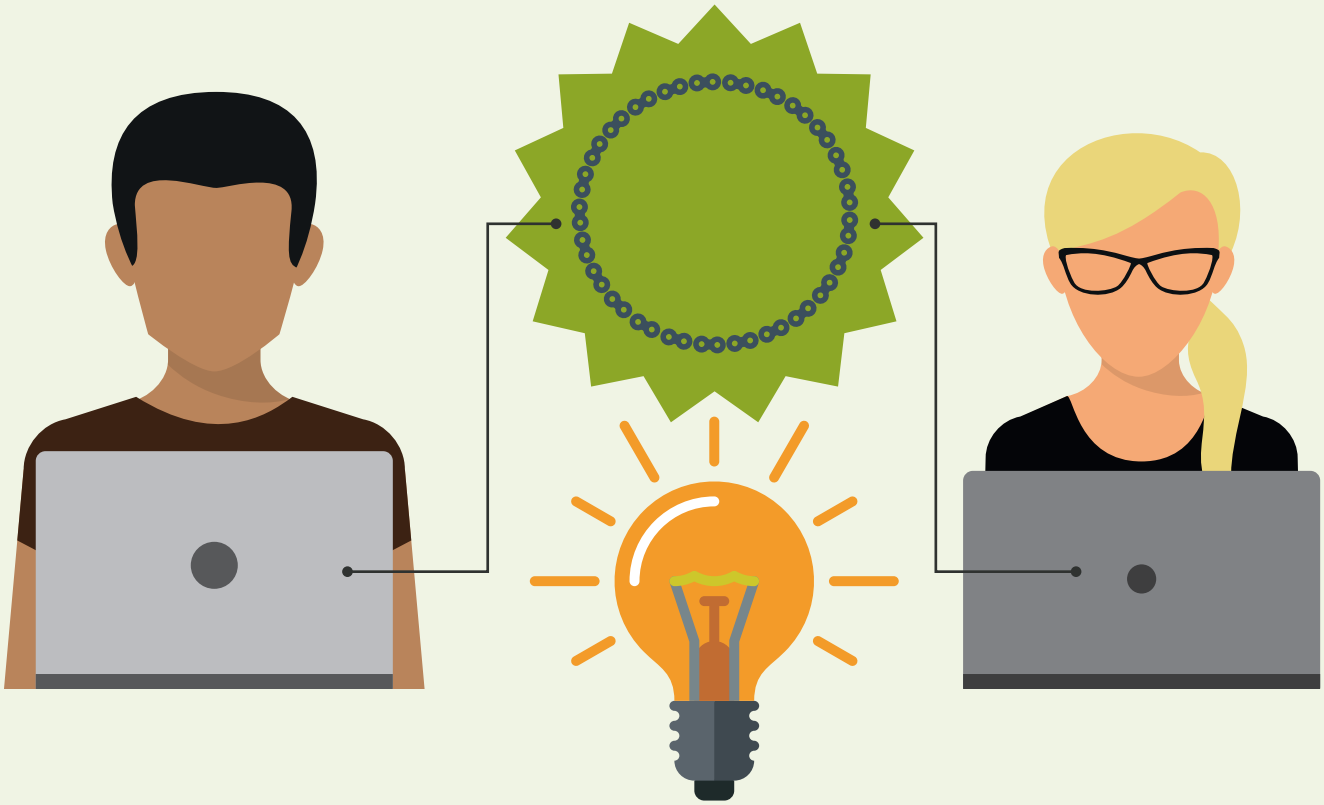
- 暗号を用いた照合
- 大規模かつ安全なデータの複製
- 証明可能な透明性

これらによって次の 3 つが実現する可能性があります。

- 新たに出現したエコシステムの支援
- 早期の試用およびパイロットプロジェクトの実施
- 英国をグローバルリーダーにする

第2章

技術



現金は、その他の通貨形態とは異なります。現金は 2 人の当事者の間で、銀行や政府など非当事者の関与や許可なしに移転することができます。ビットコインとブロックチェーンでは、これを電子的に行う方法が示されました。しかしこのデジタル技術による影響とそれが提供する機会にはより幅広いものがあります。

著者
リチャード・G・ブラウン（Richard G Brown）
最高技術責任者（CTO：Chief Technology Officer）、R3

第 2 章：技術

はじめに

ビットコインは新しい形の**仮想通貨**です。その発行は、イングランド銀行（Bank of England ）のような中央銀行が行うのではなく、コンピューターの**非集中型**ネットワークにより制御されています。このネットワークでは暗号化、およびその他の手法に依存して、ビットコインの供給の規制ならびに所有者の追跡が行われます。その結果、ビットコインは**暗号通貨**として知られるようになりました。

銀行では、顧客残高の追跡は**元帳**で行われます。ビットコインでも元帳が利用されますが、元帳はコンピューターの分散型ネットワークにより共同管理され、**分散型元帳**として知られています。

新しい項目がいくつか分散型元帳に追加される際、前回の入力内容を参照できるようになっているため、参加者は全員、元帳に記載された内容すべてについて真の出所を自ら確認することが可能です。このような項目のまとまりは**ブロック**と呼ばれ、これが全体としてつながったものが**ブロックチェーン**です。

本章ではこのような概念、それが重要となる理由と、それがいかにしてさまざまな分野で応用される基礎となるのかについて説明します。

通貨とは何か。

20 ポンド紙幣はすばらしいものです。単にこの紙幣を誰かに渡すだけで、取引を第三者が確認しなくとも、すぐさま 20 ポンドの価値がその人に移転されるのです。2 人の他に誰もいなければ、全世界で移転が行われたことを知る必要は誰にもなく、その移転を誰も止めることはできません。

しかし、この P2P（ピアツーピア）の移転は近距離でしか成立しません。20 ポンドの価値を、別の町や別の国の誰かに移転するには、現金の入った封筒を扱う郵便局の職員や、電子送金を行う銀行といった他者を信頼し、支配権の一部をその他者に引き渡す必要があります。実際に銀行は資金が違法行為に関連しているとみなした場合、その電子取引を阻止したり、電子資金を差し押さえたりできます。

世界における資金供給のための支払システム、銀行間の取引関係、SWIFT（国際銀行間通信協会、Society for Worldwide Interbank Financial Telecommunication）のような電子取引ネットワーク（ECN）は、現金はその他の形態の通貨と根本的に異なるという事実から直接生まれたものです。唯一、現金だけが無記名証券であり、しかも他人の許可なしに移転できます。つまり検閲耐性があるのです。

ビットコイン誕生が発表された 2008 年後半まで、私たちはこのように考えていました。考案者は、ビットコインは「純粋に P2P 型の電子現金」を実現するシステムであり、保有者が完全に管理し、銀行の許可や没収のリスクを冒すことを必要とせずに、誰にでも送ることができると主張していました。

ビットコインシステムの完全参加者は各自、システム開始からのすべての取引を「ブロック」化したコピーを保有します。各ブロックは直前のブロックに暗号化を用いて関連付けられ、ブロックチェーンとなり、そこに取引の全履歴が保存され、これによって分散型元帳の機能を果たすことになります。ユーザーは、Coinbase や Blockchain（根底となっている技術概念と混同しないように注意）などのさまざまなアプリケーションを使用して

元帳にアクセスできます。元帳のコピーはすべて、それぞれ元帳の状態について「合意」に達するように設定されたアルゴリズムで同期されます。

ビットコインは 2008 年に突然生まれたわけではありません。仮想通貨システムに関する研究は数十年前から行われ、システムの各構成要素はすでに存在していました。ビットコインを大きく前進させたブレイクスルーは、既存の技術を革新的な方法で組み合せることでしたが、それが可能となった背景には、インターネット上でのオープンソース開発という考えが成熟していたことと、人々の間で代替通貨システムという考えが受け入れられるようになってきたということがありました。

システムは、古いブロックほどその書き換えが難しく、実質的には不可能になるように設計されています。いったん取引が十分に確認されると、元に戻すことはできなくなり、これにより検閲耐性が生まれます。つまりこれは真に仮想通貨なのです。

よくある質問（FAQ）

「ブロックチェーン」とは何ですか。

ブロックとは単なる支払リストのことです。ブロックチェーンはブロックのリストで、各ブロックはその直前のブロックを参照します。しかし、一般にはブロックチェーン」は、ビットコインシステムの根幹となっている技術や手法の集合体を示す用語として使われる傾向があります。それが金融やその他の分野でビットコインとは無関係の問題も解決するケースが出てきたため、これから発想を得て他のプロジェクトでも使われるようになったのです。

これゆえ、世界の政府や規制当局がこの発明には用心が必要であるとみなしているのも不思議ではありません。検閲耐性を備えた仮想無記名資産は、犯罪ネットワークでは理想的な通貨と見られ、実際ビットコインは、今はなきデジタル闇市場のシルクロードの主要通貨単位になりました。

しかし、英国の複数の機関を含めほとんどの規制当局はビットコインの使用を禁止しておらず、また、多数の合法的な企業がこの技術形態に多額の投資をしています。それはなぜなのでしょう。

機会ととるか、脅威ととるか。

まず、これは人々が想像するような統制不能、あるいは「許可が不要」なシステムではありません。一般の見方とは反対に、根幹をなすアーキテクチャーにより、取引の追跡およびシステム誤用者の身元の判明が比較的簡単にできます。さらに、規制当局側でも、価値がシステムに流入･流出する「オンランプ」および「オフランプ」をどのように制御するかについても解明されてきています。

ビットコインのようなプラットフォームは、はじめは警戒すべきものに聞こえるかもしれませんが、ユーザーの匿名性は保証されず、また、ビットコインをポンド、ドルあるいはユーロに両替したい場合は、両替システム側で身元確認、資金洗浄、テロリストの資金調達に関する規制に従うよう求められます。さらに、このすぐあとで説明するとおり、この技術の最も興味深い応用の多くが、システムの利用を許可される者と許可されない者の指定に関する規則が強制されるようになっています。

その後、ビットコインの根幹となっている技術には価値があり、安全な使い方が可能で、大きな将来のイノベーションを実現させるかもしれないという見方が出てきました。しかし、ビットコインに検閲耐性があるということは、法執行機関および規制の観点からは問題であり、したがって大企業や銀行がビットコインやそれに関する技術に関わることは短期的、中期的にはほぼないでしょう。

しかしながら、暗号通貨の背景にある分散型元帳の技術には汎用性があり、非常に有用

となる可能性があります。1つの企業に支配されず、しかも活発な開発者コミュニティーを持つオープンプラットフォームがイノベーションを推進してきたことは、これまでに何度もありました。このようなプラットフォームは、これまで取り残されてきたユーザーに対し、開発企業以外の者や新規参入者が新しい製品・サービスを提供することを可能にしました（この技術の破壊的な可能性については第5章を参照）。

分散型元帳技術は、仮想通貨という1つの目標を達成するために発明されましたが、現在、企業やその他の組織は、これ以外のさまざまな差し迫った課題にどのように応用できるかについて積極的に探っています。たとえばビジネスでは、「許可型」ブロックチェーンの方がビットコインの許可不要型モデルよりもずっと有用であるとみなされることがよくあります。これは、特定の当事者だけに、取引の確認を行う権限が与えられるためです。これによりビジネスでは、相互に信頼する企業や個人のみが参加できる安全でプライベートなネットワークを構築することが可能になります(許可型および許可不要型システムに関する詳しい説明は第3章を参照)。

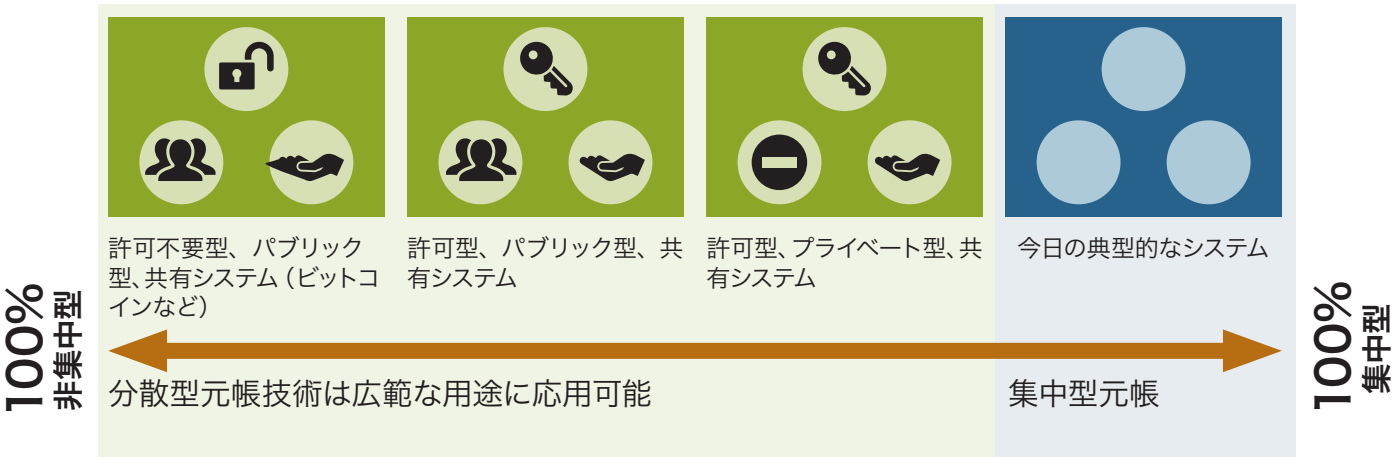
FAQ

FAQ：ビットコインと従来の通貨との根本的な違いは何ですか。

ビットコインは銀行や政府の許可なく誰でも所有できます。ビットコインは「ビットコイン・ウォレット」の操作方法を知っている世界中の誰に対しても送金できます。この「検閲耐性」の原則こそが、ビットコインが本質的に画期的である点である一方、立法者や規制当局が当初懸念していた点でもあります。

概して、この分野では複数の技術が存在し、それらが連続的につながっていることは明らかであり、これらの技術はいかに「非集中的」であるか（分権化されているか、つまり真の意味でどの範囲まで許可を必要としないか）を基準にして分類できます（図1参照）。しかし集中型かどうかという点は、この分野を分析する際の1つの側面にすぎません。この他、さかんに研究されている点には、資金使途に関する規定の程度（たとえば保護者の連署がある場合に限り、子供が使ってもよいとされる資金）や、金銭以外の資産を表す可能性（たとえば有価証券やさらには財産の所有権）などがあります。

図1：「集中度」別の元帳技術の分類



応用の可能性

分散型元帳の技術は、コスト、複製、照合に分類可能なビジネス上の問題を解決する可能性を含んでいます。

銀行業務を例にしましょう。どの銀行でも、金融取引のライフサイクルを追跡および管理するためのシステムを、少なくとも１つ（通常は複数）構築または購入しています。これらのシステムはどれも構築するのに費用がかかり、その管理にはさらに多くの費用がかかります。システムは相互に接続され、通常、照合といわれるプロセスを経て同期させなければなりません。これには双方の銀行から何人かの者がともに、すべて一致することを確認し、合わない場合は問題に対処するという、確認作業が必要になります。

一般的な解決策としては、単一の集中型元帳を作り、全参加者で共有するという方法があります。英国ではこのアプローチに基づいた成功事例が多数あり、特に Faster Payments Service はその好例です。しかし集中管理機構はデータと処理を集中管理し、また、各参加者のシステムと統合されなければならないことも多いため、コストがかかることがよくあります。そのかわり、多くの分権（非集中）型データベースをネットワーク末端に配置し、メッセージをデータベース間で移動させることもできます（図２を参照）。

図２：
分散型ネットワークでは、集中型データベースおよび分権（非集中）型データベースで行われている、時間のかかる照合プロセスを省くことができます。

ティム・スウィンソン
（Tim Swinson）

これに対してビットコインでは、インターネットを介して、分散ネットワーク内にある数千のコンピューターを同期させます。自分のコンピューターが、自分がビットコインを所有していると考えると、ネットワーク内の他のコンピューターも同じように考えるのです。同様の手法を銀行業務で採用すれば、すべての銀行システムが互いに、常に歩調が合った状態となり、照合や問題解決のために多くの人手をかける必要がなくなります。重要なことは、これを達成するためにビットコインは必要ないという点です。解決策を生み出す可能性があるのは、その根底となっている分散型元帳の技術なのです。

これは金融サービスが抱える最大の問題の１つである、紙の消費コストという問題の解決に役立つ可能性があります。近年、経済活動から紙の書類をなくそうという意図で、多くのさまざまな試みが行われてきました。しかし、新しい技術でも、単に古いプロセスを新たな方法で繰り返すだけのものだったり、プロセスの別の段階で依然として紙に頼っていたりするという状態は少なくありません。たとえば輸出業者への融資はいまだに大変な手作業です。輸入業者の銀行が信用状を出し、それに対して輸出業者の銀行が資金を提供します。このプロセスは普通電子的に行われますが、その後の確認には数多くの紙の書類が必要であり、それは世界中どこでも手作業で処理されています。これに対し、共有元帳の技術を利用することで、紙ベースの銀行業務の一部を、より迅速にペーパー

事例

研究およびホライズン・スキャニング

ジョン・G・ベアード（John G Baird）
RCUK デジタル経済テーマ主幹（RCUK Digital Economy Theme）、EPSRC

工学物理科学研究会議（EPSRC：Engineering and Physical Sciences Research Council）は、英国研究会議（RCUK：Research Councils UK）のためにデジタル経済（DE）テーマ（Digital Economy (DE) Theme）の研究を主導しています。この DE テーマは、2008 年から 1 億 7000 万ポンド超を投資し、特に、経済のデジタル化に関する社会的課題と、それが社会的包摂や地域経済、個人データ、セキュリティ、アイデンティティ、信頼性、プライバシーに及ぼす影響についての学際的応用研究を進めてきました。DE テーマは、2015 年 3 月に発表された予算のとおり、仮想通貨および IoT（モノのインターネット）の両方の推進を主導していくことに努めています。分散型元帳技術の分野では今日までに次の活動に投資をしてきました。

1. デジタルトランスフォーメーションにおける暗号通貨の影響(CREDIT:Cryptocurrency Effects in Digital Transformations）[1] は、18 か月に及ぶ 40 万ポンドの研究プロジェクトで、暗号通貨の現象とそれに関連する根幹技術であるブロックチェーンについて、デジタルトランスフォーメーション、プライバシー、コミュニティー、組織の 4 つの主要テーマに分けて調査します。研究の成果として期待される主な項目は次のとおりです。

- スタートアップ企業および既存企業が、自社の製品・サービスにブロックチェーン技術を採用する際に検討すべき問題を理解するのに役立つ段階別の指針
- 企業との共同による、暗号通貨の影響に関する多数の小規模パイロット研究
- この新しい研究分野をさらに発展させられる、学術研究者と専門家からなるコミュニティー

2. CREDIT は、「暗号通貨の破壊的役割（The disruptive role of crypto-currencies）」[2] および「ICT と金融サービスの将来（ICT and the Future of Financial Services）」[3] という、私たちがこれまでに支援してきた 2 つのスコーピング・レビューに基づいています。この 2 つではいずれも、暗号通貨についての現在の理解を見直し、社会、倫理、法、規制面における暗号通貨の影響についての理解との間にギャップがあることを明らかにしました。その結果として私たちは「デジタル経済における信頼、アイデンティティ、プライバシー、セキュリティ（Trust, Identity, Privacy and Security in the Digital Economy）」[4] についての研究を提案し、1000 万ポンドを求めることにしました。この中で「分散型元帳技術の広範な応用」は 6 つの重点分野の 1 つとして位置付けられています。この重点分野では、個人、コミュニティー、組織、国家が分散型元帳システムを信頼し、利用するために必要な社会、倫理、法およびビジネス上の枠組みを理解したうえで、そのようなシステムにおける技術の進歩と一体化し、バランスの取れた研究を支援することを目標としています。最終的にはこの研究により、個人および組織間の金銭的価値ならびに非金銭的価値、そして将来的には「スマート」オブジェクトのさまざまな交換形態を支援する「スマート」経済へ通じる道が開かれることを願っています。

3. 最後になりますが、私たちは「第三者による資本の脱物質化および再物質化（3DaRoC：3rd Party Dematerialisation and Rematerialisation of Capital）」[5] という 26 万ポンドの研究プロジェクトにも資金を提供しています。これは、P2P の貸金業者の Zopa Limited と、コミュニティー通貨である Bristol Pound という 2 つの小売金融サービス組織の事例を基に、効果的なデジタル小売業向け金融サービスを構築する方法を探るものです。このプロジェクトでは、デジタル金融商品の設計・使用に影響する重要な問題に関心があるユーザーおよびビジネスを支援するためのオンラインツールキットを作成しました[6]。

レスで行うプロセスによって置き換えることができるという可能性があります。工学物理科学研究会議（EPSRC：Engineering and Physical Sciences Research Council）では、そのような金融分野への応用に関する初期段階の研究をすでに支援をしています（研究およびホライズン・スキャニングに関する上記の事例を参照）。

しかし、適用の範囲は金融業務に限られません。検討されている応用には、健康・医療（患者記録）、政府（土地登記、給付金・サービスの給付。第 6 章を参照）、電子機器（「モノのインターネット」を含む。第 1 章を参照）などがあり、さらに芸術や宝飾品の世界（ダイヤモンドの出所追跡。第 5 章を参照）でも考えられます。

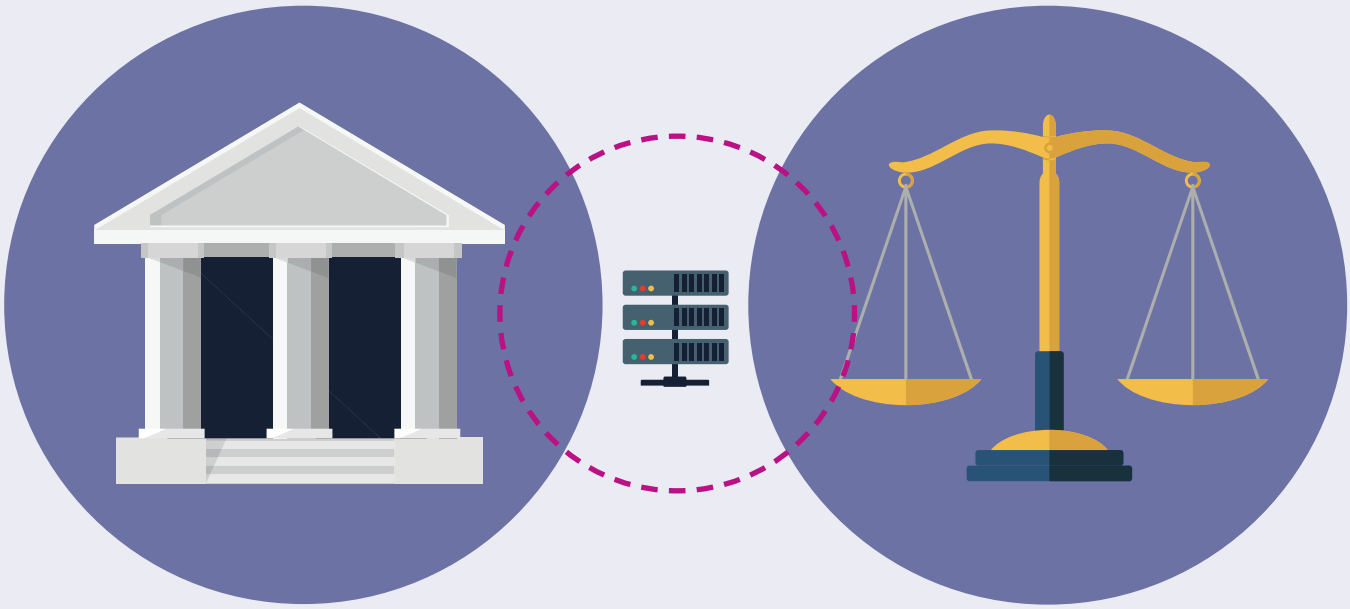
なお、このような技術は開発の非常に初期の段階にあり、プライバシー、パフォーマンス、拡張性の問題などこれらの応用を実現する前に取り組むべき未解決の問題が数多くあることを強調しておく必要があります。この技術は、銀行が信頼するのに十分なだけの仕事を実際にこなせるでしょうか。プラットフォームが共有および共同化される場合、もしも簡単に料金を課すことができなかったら、誰がこれらのプラットフォームを作るのでしょうか。

しかし、この分野は急速に発展しており、多くの問題はすでに解決されています。今では、技術のこれらの側面のうち、長い間にわたって変化することが予想されるものと、本来の特性であり、今後おそらく変化することがないと思われるものとを、区別することが可能になりつつあります。分散型元帳技術を使うことにより、企業や政府はコストのかかる照合や複製を行わず、もっと効率的に運営できることを、私たちはすでに予測できます。またこれにより、安全に共有されるデータへのオープンアクセスに基づいて新しい製品・サービスを消費者に提供できるという点で、既存企業も新規参入企業も同一条件で競うことができます。

これは検閲耐性を実現した仮想通貨という以上に、世界を変える一大革命を導き出す可能性があるのです。

第3章

ガバナンスおよび規則



法の世界でもデジタルの世界でも規則によって統制されていますが、これらの規則の性質は異なります。デジタル環境では法（法規）およびソフトウェア・ハードウェア（技術的コード）の両方によって活動が規制されます。分散型元帳システムに関する規則を定める際には、この両方の影響を考慮する必要があります。

著者
ヴィリ・レードンヴィルタ（Vili Lehdonvirta）、オックスフォード大学、オックスフォード・インターネット研究所（Oxford Internet Institute, University of Oxford）；
ロブレ・アリ（Robleh Ali）、イングランド銀行仮想通貨担当マネージャー（Manager – Digital Currencies、Bank of England）

第 3 章：ガバナンスおよび規則

はじめに

本章では分散型元帳システムにおける規則と規則の制定について論じます。ここでは**法規**（法的義務からなる規則）と**技術的コード**（ソフトウェアおよびプロトコル）とを区別します。また**ガバナンス**（システムの所有者または参加者による、彼らの私的利益保護を目的とする規則の制定）と**規制**（公益を代表する外部当局により制定される規則）についても区別します。

法規と技術的コード：2 種類の規則

金融システムとは、組織間の一連の法的義務と、これらの義務に関する一連のデジタル記録のことです。法の世界でもデジタルの世界でも、規則によって統制されていますが、これらの規則の性質は異なります。これについてはハーバード大学（Harvard University）のローレンス・レッシグ（Lawrence Lessig）が論文で[1]、このような法的規則とデジタルの規則が活動の統制においてどのように相互に作用するかについて述べています。レッシグは、デジタル環境の活動は法（法規）とソフトウェア・ハードウェア（コンピューターコード）の両方によって規制されるため、規則について理論を構築するときには両方の影響を考慮する必要があると、主張しています。本章では「コンピューターコード」ではなく「技術的コード」の用語を使用します。分散型元帳が機能するにはソフトウェアとプロトコルの両方に依存するため、この用語の定義にはこれら両方が含まれます。

法規と技術的コードの根本的な違いの 1 つは、それぞれが活動に影響するときのメカニズムの違いです。法規は「外因的」、つまり規則は破られる可能性がありますが、その違反にはしかるべき結果を伴うため、それによってコンプライアンスが遵守されます。これに対し、技術的コードは「内因的」で、規則が守られないとエラーとなり、いかなる活動も行われません。したがってコード自体の動きを通してコンプライアンスが遵守されるのです。さらにソフトウェアの特性として、規則の遵守によって予想外または望ましくない結果が生じたとしても、マシンはその規則に厳格に従うという点があります。これによって分散型元帳システムの運用では、現在の金融システムと比較したときに大きな違いがいくつか出てきます。

1. 現在の金融システム：法規による統制

現代の金融システムはすでにその多くがデジタル化されており、技術的コードに大きく依存しています。この技術的コードによって、組織間の法的義務のデジタル記録の作成･改定が統制されます。金融規制が対象とするのは、銀行に十分な資本または流動性があるかどうかといった、このような法的義務によってもたらされる影響です。金融システムはすでにこのような技術的コードと法規の組み合わせによって統制されていますが、金融ガバナンスおよび規制では伝統的に後者に重きが置かれています。

法規の公的要素の施行は、システムの参加者によるコンプライアンスの遵守について、責任を有する金融監督官庁の専門グループの役割です。参加者は、自分がシステムの規則を遵守していることを、監督官庁側で確認するために必要な情報を、提供する必要があります。ある組織にコンプライアンス違反があれば、監督官庁はその組織に対する是正措置をとることができます。これは、技術的コードが既存の規制プロセスに何の影響も及ぼしていないということではありません。監督官庁に提出される情報はすべてデジタル形式であり、技術的コードの産物です。ただ、ガバナンスと規制の目的は、技術的コードの変更によってではなく、法規を作ることで達成されるということなのです。

2. 分散型元帳システム：技術的コードによる統制

ビットコインのような分散型元帳システムでは、それが法的規則なしに機能することが示されました。かわりに、各参加者が従わなければならない規則は技術的コードによってのみ定義され、そして施行されるのです。ネットワークの各参加者は、許可される取引の種類を定義する、同一または互換性のあるソフトウェアを使用します。たとえばビットコインのソフトウェアでは、参加者の残高のうち使用できるのは、暗号キーを用いて所持していると証明できる金額までに限られています。またビットコインソフトウェアでは、新規に通貨を発行する方法を規制し、マネープールの絶対限度額を定めることもできます。分散型元帳システムには、これらの規則を定める内規や他の法的書類は存在せず、またそれを施行する人間もおらず、純粋にそれ自体の技術的コードによって統制されます。

参加者がコードのコピーを変更して、規則に反する取引が発行されないように防止するため、各取引は元帳に記帳される前に検証されなければなりません。ビットコインのような「許可不要型」の分散型元帳システムでは、検証者（マイナー（採掘者）と呼ばれる）は抽選で選ばれます。これらのシステムでは、経済的インセンティブの体系を通じて、ソフトウェアで統制されるプロセス内でその整合性が保証されます。「許可型」の分散型元帳システムでは検証者はシステム所有者によって任命され、整合性は法的な契約などの伝統的な手段で保証されます。

つまり、分散型元帳システムは法規ではなく技術的コードで規制されるという点で伝統的な金融システムとは異なっています。この利点の１つはコンプライアンスコストが低いことです。参加者は取引を発行する際、準拠したソフトウェアパッケージを使うだけでよいからです。施行コストも低いように思えるかもしれませんが、これは必ずしもそうではありません。普及している分散型元帳システムのほぼすべてで使用されている取引確認用のマイニングシステムでは、非常に多くの計算資源が消費されるからです。そのコストは最終的にはシステムユーザーが負担しなければなりません。

ガバナンスと規制：2 種類の制定方法

現在の金融システムおよび分散型元帳は、基本的に異なる種類の規則で統制されています。すると、誰によってこれらの規則が制定されるのかという点が重要になります。

1. 現在の金融システムにおける規則制定：民間ベースと公的ベースの混合

現在の金融システムでは、法規はさまざまなところで制定されていますが、これらは大きく民間ベースの規則制定（ガバナンス）と公的ベースの規則制定（規制）の２つに区分されます。民間ベースの規則制定の例には、金融サービス会社の Visa Inc. が公表している Visa Core Rules がありますが、これは Visa システムの全参加者の行為を統制するものです。そのような民間ベースの規則は、Visa のような私的な金融ネットワークの所有者によって制定されるものと、私的な金融機関の団体によって、相互の利益のために活動を調整する目的で制定されるものとがあります。公的ベースの規則制定の例には、イングランド銀行による Visa Europe の支払システムの法的監督があります。

現在の金融システム内で公的な法規に何を盛り込むかを決めるのは、政策立案者の仕事であり、その際、金融システム内のさまざまな機関に対する規制の効果（「マイクロプルーデンス」アプローチ）と、システム全体への影響（「マクロプルーデンス」アプローチ）が考慮されなければなりません。金融システムは世界的なものであるため、バーゼル銀行監督委員会（Basel Committee）のような国際組織で世界各国の政策立案者が招集され、自主的合意に達したあと、合意内容が各国・地域で立法化されます。

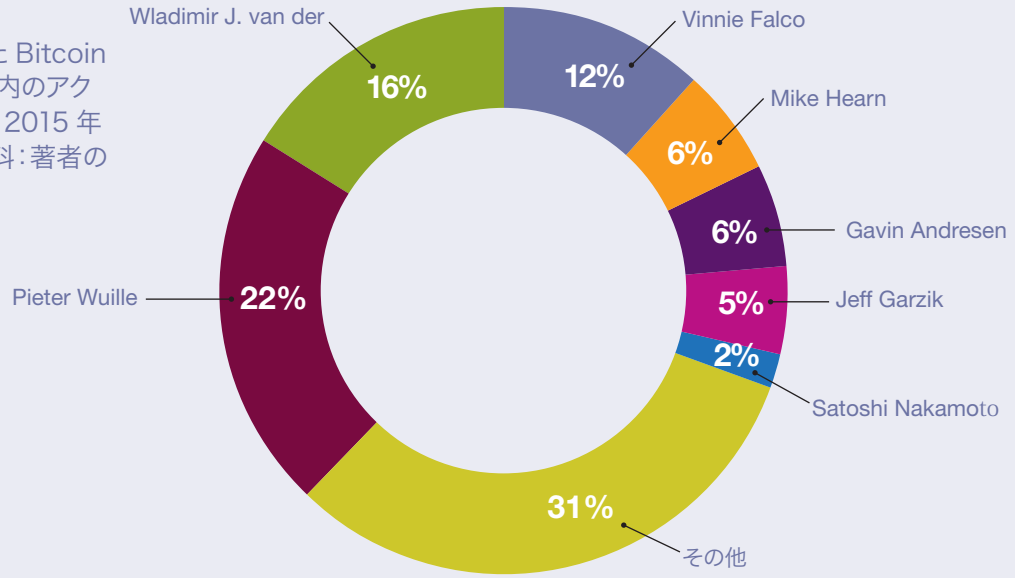
2. 分散型元帳システムにおける規則制定：特定の目的のための私的な規則

許可不要型の分散型元帳システムは、人間による規則の制定とは無関係に、数学的アルゴリズムだけによって統制されるものと考えられることがあります。しかしこれは誤解です。法規と同様、技術的コードでも人間が規則を定め、それを具体化するコードを作成し、管理する必要があります。ビットコインを例にすれば、このソフトウェアの最初のバージョンはナカモトサトシ（仮名）により発表されました。2010 年にナカモトはプロジェクトの主導権をオーストラリア生まれで米国在住のプログラマーであるガビン・アンダーセン（Gavin Andresen）に譲りました。他のソフトウェアと同様に、ビットコインもバグ、セキュリティの問題、オペレーティング環境の変化に対応するため、定期的に更新する必要があります。原理上、そのような更新があるごとに、会計や所有に関する規則など、ソフトウェアのどの部分についても変更が可能です。したがって誰がソフトウェアを記述するか、また、そのプロセスをどのように統制するかは、分散型元帳システムのすべての参加者にとって非常に重要です。

ビットコインの場合、ソフトウェアは少数の非公式団体と支配権を持っている者によって目的に応じて行われる、いわゆる「アドホックなプロセス」で統制されています。図 1 は、現在のビットコインのコードの大部分が誰によって記述されているかを示すものです。ソフトウェアはオープンソースであり、誰でも変更を提案できますが、公式バージョンへの変更を許可する技術的な権限は、アンダーセンが任命した 5 人の中心開発者チームが保有しています。そして、中心開発者の権限は非公式の自己規制憲章により制約されています。そこには、規則に重大な変更を加える場合は、コミュニティーの広い合意を必要とすると定められています。さらに、ソフトウェアへの変更内容はいずれも、マイナー（採掘者）の多数（貢献するコンピューター処理能力で測定）によってインストールされなければ有効にはなりません。したがって、このような方法で、マイナー（採掘者）がソフトウェアの更新を批准するか否かを決定するという点で、いわゆる「マイニングプール」を管理する一握りの個人が大きな影響力を持っているといえます。

このガバナンスプロセスは、コードの変更が議論の余地のないバグの修正であればうまく機能しますが、最近では機能停止の兆候が見えています。決定の中には、どの利害関係者の利害を他の利害関係者の利害よりも優先させるかについて、判断しなければならないものがあるからです。アンダーセンおよびその他の者は、プロセスをもっと公式的なものにする必要があると述べています。コミュニティーではそのような公式のガバナン

図 1
開発者別に見た Bitcoin Core のコード内のアクティブ行の数、2015 年 5 月 14 日（資料：著者の分析）



スシステムがどのようなものになるかについて議論していますが、もともとビットコインは反制度主義の精神で作られたという経緯からするとこれは複雑な問題です。このことは、法規の存在意義を証明し、技術的コードだけでは最適の結果を得ることができないことを示すもので、興味深い難問です。

許可型の分散型元帳システムでは、通常はコードに対し、明確な法的および技術的な権限を持つ所有者が存在するため、ソフトウェアのガバナンスがより簡単になります。コードをどのように変更するか決定するのは所有者次第であり、ソフトウェアに対する権限を行使する所有者がいても構わないかを決めるのはユーザー（多くはサービスの顧客）次第です。責任を定めそれを遵守させるようにするには、サービスレベル契約や他の従来の手段を利用することができます。この点では、許可型の分散型元帳システムは、Visa や SaaS（サービス型ソフトウェア）システムのような従来のプライベート型金融ネットワークと大差はありません。

分散型元帳システムをどのように規制したらよいか。

これまで説明した分散型元帳システムのガバナンスは、システムの利害関係者の利害に関わるものでしたが、分散型元帳がどのように機能すべきであるかについては、もっと広い社会的な利害関係が関与することも考えられます。たとえば規制当局としては、徴税、犯罪訴追を行うことで、犯罪目的での分散型元帳の利用を制限したいと考えるかもしれません。また、あるシステムについて、社会の一か所で何かが起こると、他の場所にも連鎖反応が起きる可能性があるほど広く普及すれば、規制当局としては、そのシステムがシステミックリスクや市場の失敗に対する耐性を持つようにしたいとも考えるでしょう。このような規制は、法規または技術的コードを通じて適用することができます。

1. 法規による分散型元帳の規制

許可型の分散型元帳システムの規制の制定は、単に所有者に法的義務を課すかどうかのみです。これに対し、ビットコインのような許可不要型システムを法規で規制することは、システムを統制する法的主体が 1 つもないため、より複雑になります。人々が自分のコンピューターにインストールできるソフトウェアを規制するのは困難です。そのかわりに法規によるビットコイン規制の試みでは、両替業やウォレットプロバイダーなど、ビットコインの取引をするビジネスの規制に焦点を合わせています。このようなビジネスはそれ自体で（ウォレットプロバイダーによる顧客資金持ち逃げの防止など）、または間接的に元帳の用途を規制することによって（資金洗浄防止規制によるコンプライアンスの遵守など）規制が可能です。

法規によるビットコインの規制としてよく知られている例は、ニューヨーク州の金融サービス局（New York State Department of Financial Services）が、ニューヨーク州在住者に仮想通貨サービスを提供する事業者向けに発行した BitLicense です [2]。事業者がこの免許を取得する期限は 2015 年 8 月 8 日で、免許のないサービスプロバイダーには罰則が課されます。

2. 技術的による分散型元帳の規制

ビットコインのような分散型元帳システムの技術的コードは現在、一部の人々によって目的に応じて行われる「アドホックなプロセス」で作られています。けれどもソフトウェアとプロトコルからなる技術的コードが公的部門から出現することもありえます。たとえば、TCP/IP やその他のインターネットプロトコルは政府助成の研究プロジェクトの結果、生まれたもので、現在は地理的な場所と特定の関心に基づくオープンメンバーシップ構造をとる国際的非営利組織のインターネット協会（Internet Society）の後援を受けて管理されていま

す。インターネットのインフラストラクチャーの他の部分は、多数の利害関係者が関与する国際的なプロセスで管理されていますが、一部はまだ米国の公的規制の監督下にあります。

このようなつぎはぎの状態では、完璧な解決とみなすにはほど遠いのですが、これは、技術的コードの作成における公的部門の関与と民主的な決定プロセスが可能であることを示すもので、法規ではなく技術的コードを介した公的規則といえます。

表 1
公的部門と民間部門が作成した法規およびコンピューターコードの例

	法規	プロトコル
民間部門により作成	Visa Core Rules Faster Payment Service Rules	Financial Information eXchange(FIX)プロトコル ビットコイン
公的部門により作成	European Market Infrastructure Regulation BitLicense	インターネット(TCP/IP) World Wide Web(HTTP)

分散型元帳システムへの応用には、技術的コードを維持するための正式な複数利害関係者のプロセスの確立から、コードに関する公的基準の開発まで、あらゆるものが含まれます。この応用によりコンピューターコードに組み込まれる規則に影響が及び、政府や一般大衆が正当な規制の目指すものを直接に達成できるようになれば、これらのシステムを規制する一連の新しい法規はさほど必要ではなくなるでしょう。

あるいは、公的部門が許可型システムを開発し、現在のように完全に法規のみによるのではなく、法規と技術的コードを組み合わせることで、公的規制が影響力を持つことも考えられます。このように、中核的なインターネット技術では、政府が触媒となって、民間部門の活動の基盤となる技術的コードを作ることが可能なのです。

結論

Visa のような従来の民間金融ネットワークと対比すると、ビットコインのような許可不要型の分散型元帳システムには、システムに対して公式に責任を負う中央の法的主体がありません。そのかわりにシステムは、通常、目的に応じて行われる「アドホックなプロセス」に統制されており、それはシステムのソフトウェアコードを作成する一握りのソフトウェア開発者に集中しがちです。このようなシステムの価値が高まり影響力が大きくなれば、より堅牢な内部ガバナンスのプロセスを作る必要が出てきます。また中央に法的主体が存在しないことも、公的な規制当局が分散型元帳システムを法規によって規制することを難しくしています。したがって政府は、その規則を定義する技術的コードに影響を及ぼすことで、分散型元帳システムを規制する方法についても、検討する必要があります。政府が技術的コードと法規の適切な均衡点を見つけるには、両者が相互に作用し合うことに留意し、そのように設計される必要があることを認識しつつ、両者の強みと弱みを考慮する必要があります。

またビットコインと分散型元帳システムの出現は、現在の金融システムにおける技術的コードの問題も浮き彫りにしました。分散型元帳は、金融システムが技術的コードと法規によって統制・規制できることを示しています。政策立案者には、金融システムに対する技術的コードの影響力を認識し、そのような影響力を規制体系の一部として取り込みつつ、コンプライアンスコストの削減などのメリットを享受する方法を検討することが求められます。

第4章

セキュリティおよびプライバシー

分散型元帳システムには数多くの種類があり、セキュリティやプライバシーに関して、それぞれにさまざまな機会と脅威があります。大切なのは、どのタイプの元帳を利用するかを決定する前に、提案された実施案のビジネスとセキュリティ上の要件を分析することです。

著者

M・アンジェラ・サッス（M. Angela Sasse）、ユニバーシティ・カレッジ・ロンドン（University College London）
協力者：ジョージ・ダネジス（George Danezis）およびサラ・メイクルジョン（Sarah Meiklejohn）、ユニバーシティ・カレッジ・ロンドン；ダニエル・シウ（Daniel Shiu）、政府通信本部（Government Communications Headquarters）；フィル・ゴッドシフ（Phil Godsiff）、サリー大学（University of Surrey）

第 4 章：セキュリティおよびプライバシー

はじめに

セキュリティは単純に、「発生すべきことは行い、発生してはならないことは行わないということ」と定義できます。どのような分散型元帳とブロックチェーン技術の実施においても、望ましい結果･望ましくない結果が生じるリスクがあり、その制御は技術をどのように設計、応用、統制するかにかかっています。利害関係者ごとに異なるリスクがあります。

システムに対しては、外部からの攻撃だけではなく、内部の利害関係者の行為やソフトウェアなど構成要素の不具合も脅威となります。システムを実装し結果を得るには、事前に詳細な脅威モデルを開発しておく必要があり、また、個別のセキュリティ要件を明らかにしておく必要もあります。

効果的なセキュリティ対策は、個人および組織の利害関係者のプライバシー確保に欠かせませんが、しかしそれだけでは十分ではありません。実装で開示される情報と、個人やグループの身元を明らかにする、あるいはその活動を認識するために他から得られる情報がどのように組み合わされるのかについても考慮しなければなりません。

イノベーションの利点

セキュリティの観点から見たビットコインやその他の暗号通貨の特徴の 1 つとして、ネットワーク上での統制が中央に集中していないことが挙げられます。システムは、合意に基づいて動作する、グローバルにつながっているピア（対等な装置）により統制されるため（17 ページの定義を参照）、信頼や不具合が一か所に集中しません。これは、悪意を持ってシステムを攻撃するには、相当の労力が必要であることを意味します。個人ユーザーに対しては、システムによって高度なセキュリティが保証されます。攻撃者がウォレット内のビットコインを動かそうとしても、パブリックキー（実際にビットコインが保存されている場所）に関連付けられているプライベートキーを知らなければ動かせません。そのため、誰かのビットコインを盗むには、攻撃者は、すでに確立されている暗号基準である楕円曲線デジタル署名アルゴリズム（ECDSA：Elliptic Curve Digital Signature Algorithm）などのセキュリティを破壊する必要があるのです。

ビットコインおよび関連する「アルトコイン」（代替コイン）には、より広範なコンピューターセキュリティのインフラストラクチャー―つまり分散型元帳―が利用されています。そのため、高い健全性と一貫性のある内容表示（ビュー）をが可能なのです。そのような元帳では、暗号技術を利用することで、重要な情報を元帳内に持つすべての人が、特定の記録が元帳内に存在するかどうか、確認できるようになっています。同時に、合意のための複雑なプロトコルを使い、システム内の誰もが確実に、元帳の同一ビューを得られるようになっています。これは、ビットコインの二重使用防止能力の面で重要な点ですが、分散型元帳を契約証書の記録などの他の用途で利用する場合でも、同様に重要となるでしょう。このことから、分散型元帳は、公証やタイムスタンプ機能、信頼性の高い文書保存など、高度なサービスに応用でき、さらに、自動化の促進、サービスプロバイダーの切り替えプロセスの簡素化、ピア取引を通じてこのような活動のコストを削減できることが期待されます。

安全なオンライン通信に関して主な問題の 1 つは、パブリックキーが、ユーザーがアクセスを希望するサービス側に保有される点です。1990 年代から一般に使われているメカニズムは、公開鍵インフラストラクチャー（PKI）と呼ばれ、基本的にはキーとサービス間のリンクを認証する証明書を提供する、一連の信頼された第三者機関です。しかし、

これらの認証局も完璧ではないことが明らかになっています。もしセキュリティが破られると、知らない間に無効な証明書が発行される可能性があります。

証明書の透明性（CT：Certificate Transparency）[1] というシステム（近年 Google により提唱され、現在はワーキンググループの監督下）では、この問題を軽減するために分散型元帳技術が使われています。すべての証明書は分散型元帳に追加され、すべてのユーザーやサービスは、使用しようとする証明書がその元帳に含まれているものであるかどうかを確認できます。その結果、不正な証明書は簡単に検出されるので、PKI システムに侵入し乱用しようとする攻撃者に対する大きな抑止力となります。

また、ユーザーが私的な通信を保護する際、信頼できる結び付き（バインド）をキーと通信主体の間に確立させることについても、問題があります。現在のソリューション（中央集中型ソリューションである PGP Web of Trust など）では、利用できるようなセキュリティ特性がないか、またはあっても脆弱です。この代替手段として有望なものに、CONIKS[2] があります。これは、電子メールの暗号化や署名に使用可能なユーザーのパブリックキーの保管および検索のために、特別に作成される分散型元帳に依存するものです。分散型元帳を維持および監査するのに第三者のネットワークに依存する CT とは異なり、CONIKS では通信プロバイダーと彼らがすでに持っているユーザーのデータベースを利用して、整合性の高い元帳が構築されています。

セキュリティ上の課題

これまでに説明した非集中型システムのセキュリティ上の利点、特に耐性と堅牢性が完全に当てはまるのは、グローバルな信頼性の理論に従っている許可不要型元帳だけです。許可型元帳や他の集中化機能を有する例では、耐性や堅牢性は劣るものの、信頼性・機能の集中管理を保証する能力は優れています。

事実、完全非集中型システム（ビットコインなど）と完全許可型のシステム（専用プライベートネットワーク）との間にはさまざまな選択肢があります（第 2 章を参照）。これら両方の長所を活用した中間的なソリューションの例に、ユニバーシティ・カレッジ・ロンドン（University College London）のジョージ・ダネジス（George Danezis）とサラ・メイクルジョン（Sarah Meiklejohn）が提案している、中央銀行のための暗号通貨 [3] があります。これは取引を収集する分散型の「mintettes」ネットワークを利用しつつ、中央で統制されるサーバーを基盤にしたブロックチェーンを確立するというものです。

このようにさまざまなソリューションがあることから、どの種類の元帳を利用するかを決める前に、採用の際に必要になるであろう、ビジネスおよびセキュリティ上の要件について分析することが重要です。

たとえば、労働年金省の福祉手当の支払管理システムの重要な優先事項として、サービスの確実な提供と、ネットワーク障害に対する耐性の確保が挙げられます（第 6 章を参照）。最大の脅威は、おそらく、金銭目的で個人ユーザーを狙った、機会便乗型のサイバー犯罪者によって引き起こされる攻撃でしょう。したがって、次の点を考慮する必要があります。

- システムは、個人ユーザーにとって、最低限の知識と努力で済むように設計される必要があります。つまり選択肢と設定の数を限定し、その結果が明確な形態で得られるようにしなければなりません。
- スマートフォンのような汎用デバイスが使われるときには、本人証明やキーへの安全なアクセスを保証し、他のアプリケーションからはアクセスされないようにします。
- 元帳自体は広範なサーバーネットワークで管理することにし、ネットワーク障害に対す

る耐性を確保する必要があります。

- 普及のためには、支払承認サービスを専用ハードウェアで集中管理し、攻撃に対する防御を強化する必要があります。

また、対外援助の分配の為のシステムでは、（資金が他の目的に使われるのを防止するために）取引の整合性を確保することや、災害復旧時にシステムの稼動維持を確保するということが必要となります。脅威としては、取引を混乱させることで地政学的優位性を得ようとする国家からのもの、または支援の受け入れ国の中で不正行為を行う仲介人からのものが考えられます。したがって、次の点を考慮する必要があります。

- システムは、小規模で強い防御力を持つ専用のサーバーネットワーク上で稼働し、政府が元帳のコピーを、オフラインのバックアップとともに保有できるようにしなければなりません。
- 顧客に対しては、元帳について独自の元帳ネットワークを構築することを奨励し、政府のサーバーから定期的な更新・修正を受けられる安全な設計についての助言を与えます。
- システムは、深刻なネットワーク攻撃が疑われる場合、オフライン化できるようにする必要があります。

しかし、どの政府支援のシステムについても最大の脅威は陳腐化であるといえるかもしれません。利用しにくい、または必要な機能を欠いていると採用されません。

さらに、最近浮上してきた脅威として、異種のソフトウェアの導入によって既存のシステム内で「分裂」を生じさせることによる、システムのハイジャックもあります。暗号分析を研究している UCL のニコラス・クルトゥワ（Nicolas Courtois）は、ビットコインを詳しく研究し、2015 年 8 月に次のように報告しています。

「新しいバージョン番号と新しい規則を用いたブロックのマイニング（採掘）が可能になると考えられる。これはブロックの大型化、1 秒当たりの取引量の拡大、コスト削減、普及拡大につながり、ビットコインがより民主的になることを意味する。現在のビットコインは、最近数か月の間に能力の限界に達したが（1 秒間に 4 件以上の取引が困難）、ビットコインの開発者コミュニティーはこの問題をまったく解決できていない」。

これは、政府支援による導入におけるガバナンスには、将来的な技術開発の動向と、（敵対的か否かを問わず）他の主体による奪取を防ぐ方法を、あらかじめ十分検討する必要があることを示しています。

セキュリティに関する勧告

この技術を各自の目的に導入するにあたり、政府は、それぞれに関連する脅威を注意して特定する必要があります。どの国家主体も、ビットコインを破壊することには関心はありませんが、英国政府の仮想通貨を攻撃しようとすることには関心を持つかもしれません。また、不正な元帳入力で金融上の利益があるとすれば、セキュリティに関する認識が低いユーザーが、組織犯罪の標的とされる可能性もあります。

このような脅威が明らかになったところで、政府は、脅威をもたらす者に対する適切なセキュリティレベルを定め、また、提案された利用法の有効期限も決める必要があります。サイバー攻撃が予想されるのであれば、システムは最初から安全な利用を念頭に置いて設計されていなければなりません。たとえば許可不要型の元帳ネットワークでは、アクターが独自のサーバーを追加する、あるいは正当なサーバーに DoS 攻撃を仕掛け、ネッ

トワークの健全性に脅威を与えることができてしまいます。これに対処するには、国家の利害に関わり長期的に管理される元帳については、量子耐性を持つ署名スキームが必要となることが予想されます。

新しい安全なアプリケーションには、既存のインフラストラクチャーを適合させるよりも、新しい安全なインフラストラクチャーを構築する方が簡単です。そこで既存のインターネットサーバーの再利用よりも、一連の新しい専用許可型サーバーの方が設定や認証が楽に行えるということになります。安全なシステムの構築については、英国政府通信本部（GCHQ：Government Communications Headquarters）や業界で定評のあるプロバイダーから助言を求める必要があります。

長期の使用が予想されるシステムについては、その寿命期間中にコンポーネントを簡単に更新することが可能となるように、当初から設計しておかねばなりません（ネットワークのノード機器を最新のハードウェアと交換できるようにする、もはや安全に使用できなくなった暗号化アルゴリズムをアップグレードできるようにするなど）。

また、どの技術の場合でも試用については、システムとユーザーの両方のレベルで侵入テストを実施できるように助成することも重要です。現実世界の攻撃者は小規模な試作には興味を示さなくても、もしそれが大規模に実用化された場合には関心を示し、脅威となる可能性があるのです。

プライバシー上の課題

ビットコインという暗号通貨は、当初から一種の偽名性を提供するもの[5]として設計されています（考案者のナカモトサトシはこの特性を「匿名」と表現しているが、これは不適切な表現）。

ユーザーはビットコインを保持するウォレットをいくつでも作ることができ、保有可能なウォレット数には制限がないばかりか、ウォレット開設時の身元確認も要件とされていません。コインは１つのウォレットから別のウォレットに移されますが、ウォレットと現実世界の人物との関係が曖昧になることで、ある程度のプライバシーが生じてきます。

偽名を許し、ウォレットをいかなる現実世界の身元確認手段と関連付けないとしたことは、ビットコインにとっては実用的な判断であり、それが普及に役立ちました。多くの国や地域では、現実世界の身元とオンライン取引とを関連付ける強力な方法が存在しておらず、したがって、そのようなメカニズムの存在に依存するという点が、初期から現在に至るまでビットコインの普及の妨げとなってきました。さらにビットコインのネットワークは国際的な性質を持つため、身元情報を証明する際、どの国や地域の法規に準拠するのか、また、どの法的管轄区域が特定のユーザーの身元を確認する権限を有しているかについて定める方法は明確になっていません。

最後に、ウォレット開設の際に身元確認が必要とされることになれば、通貨としてのビットコインの代替可能性に影響する可能性があります。つまり、取引の認証に認証プロバイダーが関与すれば、一部のユーザーにビットコインとして保管されている価値を選択的に否認することで、そのプロバイダーは取引をブロックすることが可能となるのです。他の当事者は、将来ビットコインに保存されている価値を無条件に引き出すことができるかどうかについて、確証を得られなくなります。このように、ビットコインはその偽名性ゆえに、（まだ存在しないか、あるいは断片的である身元確認インフラストラクチャーに依存しないようにすることで）急速な普及が可能になり、また、通貨としてのビットコインの重要な側面（つまり価値の無条件保管というステータス）も維持しているのです。

しかし、このユーザーとウォレット間の偽名性による関係は、完全・完璧な匿名性にはなっていません。ウォレットからの出し入れやウォレットからウォレットへの一連の取引は、全員が見ることができ、公での追跡が可能です。UCL のサラ・メイケルジョンとその同僚は、ビットコインの盗難事件を、両替によりビットコインを引き出そうという特定の試みと関連付けることによって、ビットコインのブロックチェーンを通じた一連の取引を追跡できることを示しました[6]。このようなアプローチは顧客の身元確認の規則を施行するために利用できます。あるウォレットのアドレスを特定でき、実際の人物との関連性がわかれば、取引内容をすべて明らかにすることが可能になるからです。

このように偽名性が完全ではないことと、ビットコインのブロックチェーンを使った取引の透明性とが結びつくと、実際にはプライバシーの問題が生じます。取引の当事者と金融機関しか見ることができない従来のオンライン決済とは異なり、ビットコインでの決済は使われているウォレット、取引のおよその時間、取引金額を含め、公開のブロックチェーン内に記録されます。誰もがブロックチェーンを処理し、たとえばオンライン業者の売上高、特定ユーザーの購入パターン、さらに一般の個人間の送金までも推測できます。このようなことは、これまでは金融機関と法執行機関しかできませんでした。

プライバシーに関する勧告

ブロックチェーンは完全にガラス張りであるというプライバシーの問題を緩和するため、さまざまな技法および代替の暗号通貨が提案されてきました。

1番目の技法はシステムの「混合」で、この技法では、多数のユーザーからコインを取り出し、そのコインを元のユーザーに関連付けられていない別のアドレスに出力します。支払人のウォレットと受取人のウォレット間の関連性を切断することによって、何らかの匿名化処理を提供します。しかしそのようなシステムを設計するには、大きな課題が 2 つあります。第 1 に、これによって実現される匿名性は完全なものではありません。あるコインを追跡し、数あるアドレスの 1 つと関連していることが付きとめられるとしても、ビットコイン内で該当しそうなほぼすべてのウォレットの中に、完全に隠れてしまっているわけではありません。このように部分的な情報の漏れがあることで、いわゆる「統計的開示攻撃」により反復取引の当事者の名前が開示されるというような、統計的攻撃が可能になります[7]。ただし、このような攻撃にどれほどの効果があるかはまだ明らかではありません。第 2 に、混合システムで不正な要素がある場合、コインが受領されても支払は行われず、結果として盗むことができるという可能性があります。多数ある混合型のビットコイン（Mixcoin[8] など）では、プライバシーを犠牲にせず、処理の整合性を保証するのに十分なだけ混合型の処理の一部を透明にすることによって、この問題を緩和しようという試みがなされています。

2 番目は、ビットコインの支払方法とブロックチェーンの記録内容を大きく変え、より厳重なプライバシー保護を達成するというシステムです。たとえば Zerocoin[9]、Zerocash[10]、Pinocchio Coin[11]、または特定の Sigma プロトコル[12] では、暗号通貨取引の設定にグループ署名アルゴリズムが採用されています。支払人は、どれかを明かさずに、リストに記載されているコインを所有しているという、ゼロ知識証明を提供し、同時に二重支払を防止するのに十分なだけの情報も開示します。これにより支払人は、以前の取引とは完全に関連付けられることなく、コインを支払うことが可能になります。システムの混合と同様、このような技法では、全員ではなく、ユーザーである可能性がある者のみが含まれる、限定的なユーザーリストの中に受取人が隠されるのみにすぎず、複数の取引の匿名性が奪われる可能性があります。しかしこれらは整合性の点において堅牢で、性能や信頼性を得る際の障害となりかねない、第三者機関による操作の混合が不要です。

第5章

破壊的な潜在力

分散型元帳技術（DLT）は既存のビジネスモデルおよびガバナンスモデルに対する大きな挑戦といえます。分散型元帳技術のような技術的なイノベーションは、ビジネス構造の革命的な変化を可能にし、最終的には経済および社会組織自体の統治のあり方を大きく変貌させることが期待されます。このような変化は、製品、サービス、オペレーティングシステムの分野における通常のイノベーションよりはるかに大きな影響があります。

著者
フィル・ゴッドシフ（Phil Godsiff）
サリーデジタル経済センター上席研究員（Senior Research Fellow, Surrey Centre for the Digital Economy）、サリー大学、サリービジネススクール（Surrey Business School, University of Surrey）

第 5 章：破壊的な潜在力

はじめに

イノベーションはビジネス・経営に非常に大きな影響を及ぼすことがあります。新技術は、ビジネスにおける新製品やサービス、また新しい収益源を生み出します。さらに、低コスト運営や、組織構造の簡素化をも可能にします。既存のビジネスの側が、導入で後れをとったり参入障壁を作ろうとしたりすれば、イノベーションを利用した新規参入者によって取って替わられることになります。

イノベーションは、ビジネスモデルや産業界だけではなく、最終的には経済および社会組織自体のあり方と統治の方法をも革命的に変える可能性があります。たとえば蒸気機関の発明は、鉄道の発展につながり、人口の都市部への移動を可能にしました。

分散型元帳技術（DLT）は、既存産業の枠組みでいうところの製品やサービス、収益源、オペレーティングシステムのイノベーションを超える破壊的な潜在力を秘めています。これらの技術には経済全体および社会を混乱させる潜在力があります。これを理解することは、分散型元帳技術によって与えられる機会と脅威、ならびに政府の役割と政府によって提供されるサービスにおいてどのように変化がもたらされるかについての、枠組みをとらえる手助けとなります。

イノベーションの役割

競争力を向上させるため、常に組織は変革し続けています。製造業は製品のイノベーションに注力し、サービス産業ではプロセスのイノベーションを通じて発展します。私たちはイノベーションを新しい製品やプロセスに関するものとして考える傾向がありますが、わずかな変化でも産業構造に大きく影響することがあります。たとえばコンピューターのディスクドライブの製造元の多くは、小型軽量ドライブの登場に適応できませんでした[1]。またイノベーションはビジネスモデルでも生まれ、「協力的競争（cooptetion)」という新たな関係、つまり業界内で企業が協力しつつ競争するという関係を作り出すこともよくあります[2]。

デジタル革命により、イノベーションがビジネスモデルのレベルでも発生しうること[3]、そして産業全体というレベルでも発生しうることが次第にわかってきています。たとえば Uber アプリにより顧客は近くにいる運転手を雇うことができるようになったことで、どれほどタクシー業界に混乱をきたしているかを考えてみてください。たとえばオープンソースソフトウェアを使うことで、誰もが修正および利用可能なプラットフォームを作成できるというように、組織が短期的利益から長期的な富の創出へと観点を変えることで将来の活動やものの見方を革命的に変えることにつながります[4]。

アプリのような技術イノベーションにより、今では顧客はサプライヤーからソリューションを「プッシュ」（押し出す）されるのではなく、リソースインテグレーターとして「プル」（引き出

よくある質問（FAQ）

分散型元帳技術の破壊的な潜在力とは何ですか。

分散型元帳技術には破壊的ともいえる潜在的な力、可能性があります。こう称される理由としては、この技術が発展に役に立った分野(暗号技術、ソフトウェアエンジニアリングなど)、この技術によってイノベーションがもたらされると考えられる業界およびサービス（金融サービス、不動産、医療・健康、身元管理など)、その処理能力（低コスト、リアルタイム、不変性など）が挙げられますが、その破壊的な可能性は、分散型のコンセンサス、オープンソース、透明性、コミュニティーといった、その根幹をなす原理にも関連しています。

す）することが可能となりました。これは、たとえば「プロサンプション(prosumption)」（ライドシェアリングサービスのBlaBlaCarや宿泊レンタルサービスのAirbnbで使われている、同じ当事者が生産と消費の両方に関与するモデル）、ソーシャルレンディング、クラウドソーシングなどを通じ、価値の創造に対する今の考え方を覆すこともありえます。このような形のイノベーションは、産業構造に影響を与え、新しい産業を作り出す潜在力がある、すなわちこれは「誰が何をするか」と「誰が何を得るか」を変えるものなのです[4]。

新規参入者によって導入されたモバイル決済システムの普及により新しい顧客基盤が生まれています（小規模商店でモバイル端末を銀行・クレジットカードリーダーとして利用できるなど）。また、これまで利用されていなかったデータが新しい利害関係者に提供され、新しい収益源となって価値が生み出されています。さらに銀行を使わずデジタルウォレットや携帯電話プロバイダー（M-Pesaなど）のような、これまでと違うオペレーティングシステムを使った価値の移転が増えています。しかしこれらの多くでは、基盤をなす取引は依然として既存のレガシーシステム（決済銀行、VisaやMastercardといったクレジットカードネットワークなど）を使って処理されています。M-Pesaは、交換取引のための価値の移転は銀行を介して行わなければならないという考え方に挑戦し、発展段階をいくつも一気に飛び越しました。しかしこのようなイノベーションも、技術があり信頼される仲介者を使うという既存の階層構造にまだ依存しています。この変化により顧客の利便性が向上し、ユーザーおよび顧客側のコストは著しく削減されますが、これは進化であって革命ではありません。

技術革命

一般的に、イノベーションは徐々に進んでいきますが、時折、急激な進歩があり、それを経済学者のヨーゼフ・シュンペーターは「創造的破壊」といい、カルロタ・ペレスは「技術革命」と呼んでいます[5]。このようなイノベーションは技術、経済、社会の間での複雑な動きの中に存在するもので、ときにはイノベーションにより特定の社会や経済の成り立ち方が抜本的に変わることがあります。

過去数世紀の間に、第一次産業革命、鉄道革命、石油革命といったいくつかの技術革命がありました。それぞれの革命により産業構造が変わり、新しい形のエネルギーがもたらされ、社会の成り立ち方に影響がありました（表1を参照）。今、私たちは膨大な情報、接続性、専門性、グローバル化に象徴される情報･電気通信革命の真っただ中にいるのです。

通常、これらの革命には、大幅なコスト削減、新しいコミュニケーション手段、そしてインフラストラクチャーおよび流通の変化という3つの柱があります。普及にかかるコストを軽減することで市場に緊張が生じ、しばしば金融バブルとその崩壊が起こり、最終的には既存の制度の詳細な見直しが必要になります。ペレスによると、革命的なイノベーションは「相互に関連する一連の革命的で飛躍的な進歩で、相互に依存する技術の集合体を形作るもの」で、かつ「その技術を用い、かつ市場において利用されている各種システムが強く結びつき、それ以外の経済を（そして最終的には社会を）抜本的に変革する能力がある」ものとして特徴付けられます[5]。

	説明	年 (おおよそ)	新技術と産業	新しいインフラ	コモンセンスとされる原則
第1次	産業革命	**1770**	機械化産業	運河、水力	**工場生産、生産性、地域の住民同士のつながり**
第2次	蒸気、鉄道	**1830**	蒸気機関、鉄製機械器具	鉄道、電信、港湾	**集積の経済、部品の標準化、都市化**
第3次	鉄鋼、電気、重工業	**1875**	鉄鋼の大量生産、重化学	電気ネットワーク、グローバルな海運	**規模の経済と垂直統合、生産力としての科学、効率性**
第4次	石油、自動車、大量生産	**1910**	自動車、安価な石油、石油化学、家庭用品	道路網、電気の普及	**大量生産、水平統合、製品標準化、エネルギー強度、郊外化**
第5次	情報および電気通信	**1970**	マイクロエレクトロニクスの大量生産、コンピューター、携帯電話の低価格化	世界的なデジタルコミュニケーション	**情報集積、ネットワーク分散化、資本としての知識、専門化による経済、グローバル化**

表 1: 5 つの技術革命（ペレスの論文を基に作成 [5]）

各技術革命において異なる「コモンセンスとされる原則」が生まれ、それらの原則によってビジネスと社会の運営のあり方が変化してきました。このような変化は工場の機械化に始まり、規模の経済と垂直統合、大量生産、標準化を経て、職能分化、ヒエラルキー（ピラミッド型の階層組織）と官僚制に至ります。そして今日の高度情報化と非集中型ネットワークの時代は「異質性、多様性、適応性、協力」として表されます [5]。これらの革命は、最終的には新しい " テクノエコノミックス・パラダイム " に通じ、そこではコスト構造やイノベーションの機会、そして組織も明らかに異なるという原則の上に構築されます。各パラダイムにおいて、組織は破壊的イノベーションから、その利用と乱用（そして抵抗）へ、さらに成熟と最終的な置換へという、S カーブに沿って進歩します [5]。これら既存の考え方を変え、新しいものに置き換えていくには、新しい技能、能力、知識を必要とする変革的な転換がなければなりませんが、それがビジネスのやり方を根本的に変えるのです。

これまでの技術革命では、組織およびガバナンスのピラミッド型の階層的システムにはほとんど影響がありませんでした。しかし私たちが経験している新しいテクノロジーの時代には「協働型コモンズ」が生まれる可能性があり、そこでの社会の動機付けは個人的利益ではなく共同の利益になる、と示唆する人もいます [6]。これは階層的に組織された仲介者（銀行や政府など）に依存しない、分散型で合意に基づくコミュニティー構造となる可能性があります。分散型元帳技術はまさにこのような挑戦を意味しているのです。

分散型元帳技術

分散型元帳技術は、仮想通貨、分散型のオープンで透明性のある記録保存、非階層的ネットワークシステム、暗号技術、ソフトウェアエンジニアリングなど、多くの関連分野で革命的イノベーションとなりえるものに関与しています。分散型元帳技術は革命的な変化をもたらすイノベーションです。それはこの技術が、新製品・サービスからオペレーティングシステムや組織構造のみならず、多様な産業構造や、これまでのビジネスモデルに影響を及ぼす潜在的な力があるからです。そのためこの技術は相互につながり合い、関連するブレークスルーの１つとして、技術革命を引き起こすことが期待されます。

分散型元帳技術はコスト面で多大なメリットがあります。この技術は本来が低コストであるだけではなく、業界レベルで運用できる共通でオープンな元帳を実現することで、統制および調整の際にも重複や非効率性を回避できます。また、各自で保有されている元帳やデータベース間の照合のような処理にかかる組織全体のコストが削減されます。ダ

事例 1

ダイヤモンド

レアンヌ・ケンプ（Leanne Kemp）Everledger 創業者兼 CEO

ダイヤモンド産業は犯罪活動に巻き込まれる可能性が高い産業です。宝石は小型で密かに持ち運ぶことが簡単で、その取引は秘密裏に行われる傾向があり、ダイヤモンドはその価値を長年維持してきました。そのようなことからダイヤモンドは、世界的な規模で資金洗浄やテロ資金の調達に使われています。

このような非合法活動を取り締まるため、鑑定書によるダイヤモンドの追跡などの努力がなされています。しかし書類の改ざんは後を絶たず、違法取引を隠すために書類が偽造されることもあります。また、ダイヤモンド取引の主要国の中には、このような犯罪防止のための法律制定が十分でない国もいくつかあります。

これに対処するためダイヤモンド産業ではブロックチェーン技術を基盤にしたEverledgerというシステムの導入を始めていますが、これは各ダイヤモンドのデジタル「パスポート」を確立するものです。これはダイヤモンドの出所、移転、取引を固有の暗号化された符号とともに記録するものです。

このシステムには３つの段階があります。

- 各ダイヤモンドに e-ID（電子的アイデンティティ）を付け、その属性をデジタル化し、信頼できるブロックチェーン元帳にシリアル番号をレーザーで刻印します。
- ダイヤモンドにデジタルパスポートを割り当てその移動、取引履歴、出所を記録します。
- 違法行為や不正な行動を検出し防御します。

このデータの保存に変更不可能なブロックチェーンを使うことで、元帳はすべてのダイヤモンドについて、原産地、所有者の変遷、（実施されたと推測される）処理を明らかにし、透明性を付与することができます。この元帳は業界、各国政府、消費者市場、国境警備および法執行機関がダイヤモンドについての真実を検証できる、唯一の資料として使用可能です。

またこのシステムでは、ダイヤモンドの販売・輸送の条件を自動的に作成できるスマートコントラクトを利用することも可能です。分散型元帳の作成にブロックチェーンを利用することにより、スマートコントラクトを追跡し、ビジネス関係や合意内容を確認するために使用できます。ブロックチェーンの透明性により、ダイヤモンドの所有権、ダイヤモンドの購入資金の調達、保険証書、登記された権利・所有権の移転を信頼して、契約を施行する方法が得られます。さらに、取引の認証は真正性の証明書とともに、政府および法執行機関にとって重要な証跡になります。

イヤモンドから米俵までほぼあらゆる資産に関する情報をデジタル化して安全に保管できるということから、組織では所有者や場所を確認および追跡することが可能になります（56 ページのダイヤモンドの認証に関する事例を参照）。また、分散型元帳技術によるスマートコントラクトを利用して、義務および価値の移転を記録する新しい方法が開発されています。たとえば Ethereum は、「スマートコントラクト」のための非集中型プラットフォームです（第 1 章を参照）。その破壊的な潜在力は大きく、これまで信頼され、またあるいは必要とされ、階層構造で独占的に運営してきた仲介者に対しても、大きな影響を及ぼします。よりオープンでフラットなコミュニティーをベースにした合意型の構造が加わる、もしくは代替されてしまうという、新たな状況が生まれる可能性があります（58 ページのコーポレートアクションに関する事例を参照）。

また、分散型元帳技術および関連技術の開発により、リアルタイムでの取引の記録やアクセスの可能性も生まれ、取引は迅速かつ安価になります（60 ページの SETL の事例を参照）。たとえば自動車保険は車とその運転者の両方の状態に基づいており、保険の条件は行動、価格、リスク選好の程度に応じて、保険を提供する保険会社間で変わります。これにより、スマートコントラクトを利用し、人の介入をほとんど必要としない非集中型のネットワークとエージェントに依存し、さまざまな製品・サービスを提供する自律分散的な組織として運営する「プログラマブル（プログラム可能）経済」が実現する可能性があります。

分散型元帳技術の運用の最たる例は暗号通貨のビットコインで、この新しい通貨によってイノベーションがもたらされることが最も明らかである分野は金融サービスです。さらに、分散型元帳技術によって既存の構造およびガバナンスの枠内でも運用コストが削減されますが、システム全体のコストを減らし簡素化する機会も生まれます。これは個別に存在する多くの独自システムにおける重複を排除およびコストを削減し、そのようなシステムの「集中型」構造を変えることにより実現されます。たとえば通貨の発行はもはや中央政府だけの責任または特権ではなくなります。それに代わり新しい形態の通貨が生まれ、そこでは人々のアイデンティティとつながりがコミュニティー内での取引を保証し、引き受ける手段となります [7]。

さらに技術の進歩により可能になったのが、基本となるビットコインに個別の属性情報（物理的資産や契約など）が加わった「カラードコイン」です。これにより単なる価値以上のものを持つ通貨が可能になりました。この通貨には、必要な目的、有効期限、使用できる場所などの属性を付すことができるのです。たとえば通貨で購入・利用できる商品・サービスに制限を付ける（第 6 章を参照）、あるいは Airbnb でアパートを借りる人に対し賃借料の支払遅延や契約期間満了のときに電子アクセスキーを取り消すということが可能になります。

よくある質問（FAQ）

分散型元帳技術から生じる脅威にはどのようなものがありますか。

他の急速なイノベーションと同様に分散型元帳技術も既存組織に対してチャンスとなることもありますが、対応できない、または対応に失敗する者にとっては脅威にもなります。また、その分散と合意という性質により、この技術は階層の上位にあり、信頼されている仲介者の役割を脅かすものにもなります。ビットコインのような新しい通貨を生み出したブロックチェーンは、国内外の経済および通貨システムを管理している政府が持つ現在の優位性に対する挑戦といえます。

政府が考慮すべきこと

政府はその利害関係者、サービス、役割が多岐にわたり、多数のさまざまな業務を行っているのは明らかです。政府の中には価値を生み出すのではなく分配をするものもあれば、効果的な規制の仕組みを作りそれを管理しているものもあります。これらの活動の多くは分散型元帳技術がもたらすイノベーションにより向上しますが、中には変化を強いられる活動もあるでしょう。しかし、変化は製品・サービスのレベルだけでなく、運用レベルや組織レベルでも可能なのです。

事例 2

コーポレートアクション

ドミニク・ホブソン（Dominic Hobson）COOConnect 創業者

上場企業は年次決算を決められた形式で公表しなければなりませんが、投資家に判断を求める企業側からの発表（コーポレートアクションと呼ばれる）については、通常、文書は定型化されておらず、また PDF 形式で公表されています。何らかの行動を取るのに文書内の情報に頼らなければならない場合、それに記載されているデータを機械ではなく自分の目で読んで解釈しなければなりません。

コーポレートアクションの 90% 超はデータベンダーから配信され、証券保管機関やファンドマネージャーなどの代理人が投資家のために処理します。情報は原本から手作業で抽出、解釈され、ベンダーにより再入力されます。自動化のレベルは低く、誤りが頻繁に起こり、処理はきわめて非効率です。コーポレートアクションの処理に要するコストは、世界全体で年間最大 100 億ドルになるという見積もりがあります[1]。証券保管機関では顧客の指示を実行しなかったり、誤って実行したりした場合にその顧客に対して返金しなければならないことも少なくありません。

ブロックチェーン技術ではこの処理をもっと効率化できます。コーポレートアクションは契約に関する情報と価値を表すものですが、原データが当事者にとって信頼できるものであり、当事者が受領した情報に基づいて行動するのに必要な経験を有していれば、原則的には仲介者を必要とせず支払人と受取人との間で直接授受できます。

ブロックチェーンを、定形化されたコーポレートアクションの公告を読み込み、保管するアプリケーションと組み合わせて利用することで、そのデータが確認済みの情報源からのものであり、また、記載されている日時が実際の公告日であることを確認できるようになります。逆にこれは指示の実行にも利用できるでしょう。さらに、そのようなブロックチェーンに基づいた分散型元帳を利用して、処理に関わるすべての当事者に対して、当事者の情報が正確で最新のもので、かつ公表後に変更されていないことを保証できます。理論的にはこれにより発行者とファンドマネージャー間に存在する仲介者がすべて不要になり、情報が正確でタイムリーであるという信頼性を確立できます。

ここで重要な問題は、完全に分散した形態でこれを実現できるかどうかです。コーポレートアクションでは、投資家や株主が自らの代理人として専門知識を有する仲介者を利用する必要がよくあるため、その情報は資金の売買といった単純な契約情報とは異なっています。

このような仲介者にはデータを仲介する前にそれを修正・補強する能力が求められることがあり、また元のコーポレートアクション自体もその後の補足公告で変更されることがあります。このように変更されたデータは、データベンダーが顧客と共有したり、他のデータと統合したりする過程で、すぐにその出所が不明になりやすいため、処理の自動化を困難にさせています。

現在のところ、ブロックチェーン技術はそれ自体では処理能力が遅すぎるため、常に変化する統合化されたデータの処理への対応ができていません。ビットコインのブロックチェーンは 1 時間に約 2 万件の取引を処理でき、取引の信頼性が確認されるまでの待ち時間は最大 1 時間です。しかし、これはファンドマネージャーが最終期限までの時間をできるだけ長く確保したいコーポレートアクションの処理には非常に不都合です。

たとえば福祉手当を正しい受給者に対し正しい時期に確実に支給するためのプロセスは、さまざまな方法で改善することができます（第 6 章を参照）。受給資格者の身元と権利を記録しリアルタイムで更新される単一の元帳は、革命的なイノベーションとなり、効率を向上させ運用と開発面のコストを削減することが期待できます。それぞれの支給に属性を付加すれば、金額だけではなく給付の目的とその予定や履歴を指定したり、追跡したりすることが可能になります。これにはもちろん利害関係者と十分に話し合いをする必要があり、このような形態の通貨と法定通貨との等価性を確保するためには何らかの管理が求められることになります。

英国のモンマスに本社がありコーポレートアクションのデータを処理している Codel は、ブロックチェーンシステムと自社のデジタル公証ソフトウェアとを組み合わせて、これらの制限を克服しています。このシステムでは、真正であることを示すためにチェーンに連なる当事者がそれぞれ参照できる、変更不可能な監査証跡を残すことができ、データの出所に関する貴重な信頼性が得られます。

同システムは、Codel 社と同業他社数社との新たな協力的事業です。コーポレートアクション情報の検索可能な中央登録システムである、Instant Actions と連動しています。登録データは、金融情報をコンピューターで読み取り可能な形式で抽出するときの指針を示す ISO 15022 および ISO 20022 の形式で保存され、コーポレートアクション情報が修正または置き換えられると登録データが更新されます。これによって情報の整合性と正確性が保証され、SWIFT の安全なネットワークを介してその情報をコーポレートアクションのチェーンに参加している全当事者が利用できるようになります。このようにすることで、ブロックチェーンのみを利用した場合の認証の遅れという問題が克服され、情報（分散型元帳として効率よく共有される）をリアルタイムで更新、配信、修正することが可能になり、情報が正確で最新であることが保証されます。

政府は、規制を変更し、企業に分散型元帳のアプローチを利用してコーポレートアクション情報を公告させることで、そのようなシステムの普及を支援することができます。

階層型の組織を、分散型システムで置き換えることは、より大きな可能性を秘めています。政府およびその機関には内部的にも、また各システムにおいても、さまざまなレベルの権限が存在する傾向があります。たとえば人々は、地方、国、超国家的な組織で、それぞれ選挙で代表を選出します。金融に関しては決済銀行、手形交換所、中央銀行、政府が関与します。民主主義は、大部分が紙の記録に基づく定期的に行われる投票に頼るのではなく、選挙民にデジタルウォレット（仮想通貨ウォレット）と「投票コイン」を与え、投票ブロックチェーンを用いるというような形態が実現できるようになるかもしれません。これには、（各投票者は自らの一票が正しく集計されているかを確認できるため）不正投票を減らすのみでなく、いかなる問題についても投票を行うという、「リアルタイムの民主主義」を導入できる可能性もあります。これによって社会的責任と参加意思に関し大きな疑問が生まれてきますが、より分散型の民主主義が作られる可能性もあります。

脅威

分散型元帳技術によって実現されるイノベーションは魅力的ですが、その技術には通貨の性質、および管理者の役割や信頼に関わるものなど、重大な脅威がないわけではありません。

事例 3

SETL による取引

ドミニク・ホブソン（Dominic Hobson）COOConnect 創業者

有価証券の発行、取引、保有に伴う清算、決済、保管、登録といったサービスにかかるコストは、累積すると非常に大きなものになります。投資家の間で有価証券および現金を移動するときには、さまざまなエージェントや取引相手が関わってきます。このようなサービスにはそれ自体のコストがかかるほかに、ビジネスプロセスの運用に必要なシステムに関わる付随的なコストもかかります。金融業界は世界全体で合計すると年間で 650 億ドルから 800 億ドルの取引処理コストを支払っています。

ブロックチェーン技術は、このような取引処理サービスを簡素化しコストを大きく削減する手段を提供します。これにより参加者はノードとして機能する多数のサーバー内に保存されている共有元帳を運用することが可能になります。取引の実行権限は暗号化されたパブリックキーとプライベートキーにより与えられます。

取引はブロックにあるデータベースに追加され、各ブロックはノードにより見直されます。ブロックは、そのブロックには有効な取引しか存在しないことがノード間で合意されたときにのみ、データベースに追加されます。このブロックチェーンのネットワークは、ノードの設定と管理以外は完全に自律的で、統制または規制を行う主体を必要としません。

SETL ソリューション

ベンチャー企業の SETL は、専門家によるブロックチェーンの開発･運用を目指しています。これは金融市場の参加者が P2P ベースの有価証券取引を決済し、有価証券および現金の残高を記録する包括的な " 黄金”の分散型元帳を管理できるようにするものです。特に SETL は中央銀行の通貨をブロックチェーンで使えるようにすることを目指しています。このブロックチェーンは自律的に機能し、現在の金融市場支払、交換のインフラストラクチャーと一体化します。

SETLでは各取引の証券と現金の両方を取り扱うことができ、単純な支払、特別な契約、コーポレートアクション、配当、利払などに伴う有価証券と現金の一方向の移転も可能です。

SETL は、コストがかかり、リスクのある清算・決済の処理を当事者間でリアルタイムに決済できるように設計されています。さらに所有権に関する黄金元帳を作ることで、SETL は有価証券の登録と保管にかかる諸経費を大きく削減します。

SETL のブロックチェーンには次のような特性があります。

- SETL ブロックチェーンで使用されるパブリックキーは、ブロックチェーンのユーザーに対し各キーを誰が証明したかについて明らかにするため、認証局の署名が必要です。認証局ではパブリックキーのユーザーについてその現実の身元情報を保存し、資金洗浄および顧客の身元確認を行います。SETLでは、法的に求められた場合は認証局がその情報を開示することを想定しています。
- 金融市場の通常の取引量に匹敵する毎秒当たり数千件の取引を処理するのに十分な能力があります。
- 現金およびあらゆるタイプの有価証券などさまざまな資産を取り扱うことができます。
- 複数の署名を必要とするマルチシグネチャ取引を処理でき、特定のユーザーグループに承認を限定できます。
- 「アトミックトランザクション」（原子取引、つまりすべての取引が発生するか、あるいはまったく発生しないか）処理が可能で、すべての段階の情報が提出され適切な認証が行われたときにのみ取引が処理されます。
- 特に参加者が流動性の管理がしやすくなるようにする機能を備えています。
- 規制で定められている記録保存、取引報告、監査を

分散型元帳技術は、中心業務として貨幣と価値の移転を行う従来の金融サービスを混乱させる可能性があります。しかし通貨自体、すでに政府の後ろ盾なしに作られた通貨であるビットコインのような暗号通貨や、通貨ユニットに異なる種類の価値を持たせた「カラードコイン」によって、その形態や利用法について混乱をきたしています。通貨の管理とそれを通じた経済の管理は政府の重要な役割であると考えられており、代替通貨システムはその役割に対する脅威となりうるものです。

分散型元帳技術は、トップダウン型の統制の代わりに合意を用い、信頼される仲介者、または必要な仲介者なしに、分散型ネットワークを使って接続し運用できる能力を持つことから、あらゆるヒエラルキー構造いかなる管理層にとって脅威となります。ヒエラルキー構造は重複、コスト高、権力乱用、財務管理の失敗の可能性など、非常に非効率な問題を生みます。しかし中立的な仲介者が必要なとき、そしてたとえば代表制民主主義においては、ヒエラルキー構造が有利なこともあります。

代表制民主主義は民政に安定をもたらしていますが、今後、分散型元帳技術の普及によって脅威にさらされる可能性があります。国民国家はすでにグローバル化と国家の流動化の進展により脅威に直面していますが、ビットコインの創設メンバーの開発者とその支持者の一部は極端ともいえる反政府主義的な見解を抱いています。課題は、支援基盤として整備されたインフラストラクチャーの中で、分散型元帳技術とそれに関連するイノベーションを、インフラストラクチャーが整備されネットワークでつながった生産的な社会のために確実に生かしていくことでしょう。

簡素化するため、取引および残高の完全な記録を保存します。

その他のメリット

現在、現金および他の資産は特定のシステムに保存される傾向があり、特定の目的のためにのみ利用できるもので、いいかえると「そのシステムに特定」のものです。これに対してブロックチェーンに保存される現金および資産は、どのような目的でも使えます。これにより銀行では、必要な流動性準備金の量を削減するとともに、その管理も簡素化されます。

SETLでは、既存のイングランド銀行のリアルタイムグロス決済（RTGS：Real Time Gross Settlement）システムを利用できないときの安全で実行可能な選択肢として、RTGSと同時に運用できるソリューションを提供できると期待されています。SETLはいつでも利用できるため、現在RTGSが稼動していない夜間や週末に存在する銀行間のリスクを低減します。

SETLの支払･決済システムは、単純かつ統一的で、即時に実行されます。英国がこのようなシステムを最初に採用すれば、ロンドンが金融サービスの拠点として、英ポンドがその際の通貨として、それぞれ選ばれるように促進できます。ロンドンで定着すればこのシステムはもっと広く採用され、国際金融におけるグローバルリーダーとしてのロンドンの地位をさらに固められる可能性があります。

結論

創造性と技術とが結びつくと、既存のビジネスモデルやそれを支える組織構造を大きく変える可能性があります。分散型元帳技術は、現在のところ既存の構造に対する挑戦であり、疑問を投げかけている状態です。それに対する一連の回答や実用的な可能性を提示している訳ではありません。しかし少なくともそうなるための性質は備えており、流れに適っており、革命的な変化を生む可能性を持っていると思われます。

分散型元帳技術は、既存の権威と今既にベストプラクティスとされているものに対する大きな挑戦であり、取引の記録や元帳にとどまるものではありません。革命的となる可能性がある新しい組織構造とその実装は、実務的、法的、政策的な影響を探るため、恐らく技術的と非技術的な実証プロジェクトの形で実験して試す必要があります。

ビジネスモデルにおける急進的なイノベーションは、特に構造と運用システムにおいては、緩やかでありつつ効率的な規制環境での実験を通じて実現します。政府は、低コストの運用モデルと組織構造を検討し、自由に新規参入できる環境を奨励し、その恩恵を受けられるような規制体制を樹立する方法を考慮する必要があります。

分散型元帳技術を採用する際の金融コストとそのメリットについては、システム全体のレベルでもっと研究される必要があります。これにより政府は、既存のフリクショナルコストのどれを回避できるか、他にどこでコスト削減をし、どこに新たな機会があるかを認識できるようになります。

第6章

政府内での応用

分散型元帳技術は、民間企業においてはデータ管理の方法や顧客やサプライヤーとのやり取りですでに大きな影響を与えています。これが政府内で採用されれば、コスト削減、透明性の向上、金融包摂の拡大、イノベーションと経済成長の促進などが実現される可能性があります。本章ではこのようなメリットを示す５つの事例を検討します。

著者
キャサリン・マリガン（Catherine Mulligan）、インペリアル・カレッジ・ロンドン研究員兼フューチャー・シティーズ・カタパルト デジタル戦略責任者(Research Fellow、Imperial College London and Head of Digital Strategy and Economics、Future Cities Catapult)
協力者:サイモン・テイラー（Simon Taylor）、バークレイズ ブロックチェーン研究開発担当副社長（VP、Blockchain R+D、Barclays）；マイク・ハルソール（Mike Halsall）、カリフォルニア NASA リサーチパーク、シンギュラリティ・ユニバーシティ グローバル・グランド・チャレンジーズ（Global Grand Challenges、Singularity University、NASA Research Park、California）

第 6 章：政府内での応用

はじめに

分散型元帳技術（DLT）は、ビットコインのような仮想通貨の管理以上に非常に多くのことを可能にします。分散型元帳とそれに使われるブロックチェーンのために開発された概念と構造は、ポータビリティがきわめて高く、他の分野の経済および社会活動にも拡大することができます。そのようなことから、この技術には政府の業務において非常に重要な意味を持つ大きな応用可能性があります。実際、最終的に分散型元帳技術によって英国社会にもたらされる影響は、マグナカルタの制定のような社会の根底に影響する重大な出来事であるといえます[1]。

分散型元帳は、プライバシー、セキュリティ、身元、信用の問題が十分に考慮されたうえで適切に適用されれば（第 4 章を参照）、政府や地方自治体にとって次のような真の機会を生み出します。

- 支払における不正や過誤の減少など、業務コストの削減
- 政府機関と国民間で行われる取引の透明性の向上
- 現在は金融システムにあまり関与できていない人々の金融包摂の拡大
- 国民のデータの保護にかかるコストを削減する一方で、異なる主体間でデータを共有できるようにし、情報交換市場を創出
- 橋やトンネルなどの重要インフラストラクチャー（インフラ）の防御
- 市場摩擦を減らし、中小企業と国および地方公共団体との相互交流を促進
- 中小企業によるイノベーションと経済成長の可能性を支援

このように多種多様なメリットは、分散型元帳技術を 3 つの異なる方法で応用することで得られます。

- 通貨への応用
- 契約管理および新しい契約形態の創出
- 新しいサードパーティー・アプリケーション開発の奨励、さらに効率的な活動の整理および遂行方法の提供

本章では、これらの各機会と、さまざまな技術的応用について、5 つの事例を通じて見て行きます。

- 重要インフラのサイバー攻撃からの防御
- 福祉支援の運用コストの削減と受給資格の追跡、ならびに金融包摂の拡大
- 援助金使途に関する透明性および追跡可能性の確保
- 経済成長の機会創出、中小企業の支援および雇用拡大
- 脱税の減少

事例 1：重要インフラの防御

概要
分散型元帳技術によって、英国とその政府機関は重要な公共インフラをサイバー攻撃からより強力に保護できるようになります。

背景
デジタル技術は、国の重要なインフラにいっそう組み込まれるようになり、また、これらのシステムの多くもインターネットでつながるようになってきました。これにより、これらのシステムは、既存のサイバーセキュリティの防御では検知不可能なハッカーや他国からの攻撃の脅威にさらされています。たとえば重要なルーターの制御を乗っ取り、そのルーターを監視および操作することで、あらゆる企業および政府組織のデータをルーターの背後から取り込むという攻撃が考えられます。さらにその他の各種組み込み技術が橋、鉄道、トンネル、防潮堤、エネルギー設備などの公共インフラに採用されるようになるにつれ、そのような攻撃によって財産および人命に危害がもたらされる可能性も出てきました。

分散型元帳技術の応用に関する提案
分散型元帳技術は、重要インフラで使用されているオペレーティングシステムおよびファームウェアの改ざん防止に応用することが可能です。分散型元帳では、不正な変更がないかどうかを検出するため、ソフトウェアの状態と整合性が監視でき、モノのインターネット（IoT）技術が採用されているシステムから送られるデータが改ざんされていないことを確認できます。

成果
- 大規模インフラの効率と効果の向上と、より強力な人命保護の保証
- 重要インフラとの通信におけるデータの整合性の確保

成熟度
すぐに利用可能

事例 2：労働年金省（Department for Work and Pensions：DWP）

概要
新しい支払モデルは、財務省（HMT：HM Treasury）と労働年金省（DWP）による福祉手当支給業務の効率向上と公共政策実施の改善を可能にします。政府の補助金および給付金に関する登録および支払処理に分散型元帳技術を採用することで、労働年金省（DWP）には次のようなメリットがもたらされます。

- 不正や過誤による資金損失防止
- 完全な金融包摂の実現から得られる恩恵を提供することにより社会的弱者を支援
- 政府の広範な政策目標、特に持続可能な方法による貧困層の救済を支援
- 価格相応以上の価値の提供、および持続可能な公的資金の支出

背景

労働年金省(DWP)は税金から年間約1,660億ポンドを福祉支援に支出しています。そのうち不正行為(12億ポンド)、誤請求(15億ポンド)、職員の過誤(7億ポンド)により約35億ポンドが過払いになっており[2]、回収されたのは9億3000万ポンドです。現在の税額控除制度(新しいユニバーサル・クレジット(Universal Credit)制度の一環として今後数年間をかけてDWPに移管予定)での不正や過誤に加え、毎年総額50億ポンドを超える過払いがあります。

受給資格のない者への給付金の過払いという直接費用を別にしても、納税者は給付後の介入費用(債権回収、調査、訴追、受給者からの問い合わせの対応、紛争解決)も負担することになります。

さらに、金額は把握されていませんが、福祉支援の支出の中で何らかの形で政策目的に沿っていないものがあります。たとえば福祉手当の支給の偏りに起因して生じる受給者の支出、つまりはノンバンクへの借金返済やいわゆる「貧困プレミアム」の支払いへと、事実上資金を供給している可能性があります[3]。

分散型元帳技術の応用

福祉手当の受給者の多くは銀行を利用できないか、または利用が制限されており[4]、信用確認、伝統的な金融製品の利用、不正取引によって生じる費用の負担といった金融サービス利用の全般で障壁に直面している状況です。分散型元帳技術は、あまり費用をかけずにこのような受給者を給付制度に取り込み、支援する手段を提供します。

デジタルアイデンティティは、安全に暗号化されたデバイス上で稼働する分散型元帳、あるいはさらに進んでモバイルデバイス上のソフトウェアを介して、確認でき、エンドユーザーは銀行や地元公共団体に多くの取引手数料を支払わずに直接に給付金を受けられるようになります。これにより受給者は、銀行口座よりも信頼できる安全な受給場所を得ることができ、より多くの金融サービスを受けられるようになる可能性もあります。そのようなソリューションは、身元の偽装がさらに困難であるため、他のシステムとも関連付けて給付の際の不正や職員の過誤を減らすこともできます。

そのような活動は、貧困のサイクルと国への依存状態から人々を救い上げるという労働年金省(DWP)の主要な政策目標を達成するのに役立つ可能性もあります。そのような技術を革新的に応用することで、対象となる受給者との合意のもとに、福祉関連取引の受給者側と業者側の両方で規則を定めることができるようになります。さらにこれは政府にとっても、給付金の利用に関する規則を合意または制定することで、福祉手当の支給による政策実現効果を高めるための政策手段を検討する機会となるでしょう。

成果

- 不正および職員の過誤による損失を削減できる。
- 政府は、公的資金が真に必要なものに対してより効率的に使われていることを納税者に保証できるようになる。

成熟度

- 受給者への十分な教育が必要。
- 法定通貨と給付用の分散型元帳とのある程度の統合が必要。
- 「給付コイン」と揶揄されるような、ミニ経済圏が生まれる可能性がある。

事例 3：国際援助システムの強化

概要

分散型元帳技術により、政府は対外援助金の分配をより効率的に管理し、意図した人々の元に資金が届けられるようにすることができます。これは政府にとっても、透明性を向上させ、効果的な財務管理を奨励するのにも役立ちます。したがって分散型元帳技術を利用することは、英国が「グローバル目標（Global Goals）」を達成するという国際社会に対する約束を実践するのにも役立つのです。

背景

世界的な義務を履行するために、各国は透明性、説明責任、健全性を確保するための手段を備えた「グローバル目標」の行動計画を支援しなければなりません[5]。国際援助国および機関は、透明性の高い堅牢な支援システムの開発を手助けすることに重点を置いています。不正、窃盗、資金横領の防止措置にはコストがかかります。このような防止措置の強化に役立つ技術の進展は、広く支援制度全般にとって有益です。

不正や汚職があると貧困撲滅の機会が減り、その国への投資が少なくなるだけではなく、教育達成度が低い大きな要因ともなります。したがって分散型元帳技術は、国際援助において資金の透明性と追跡可能性を保証するために応用できることが大きく期待されます。資金が有効利用されていることを証明できれば、各国からの拠出金・出資金は増加し、すべての資金提供者はより重要な案件に集中できるようにもなります。

分散型元帳技術応用の提案

この提案で大切なのは、分散型元帳技術の 3 つの大きな特徴を活用することでしょう。第 1 に、国際的な資金提供者は、従来の銀行業務にある官僚的な多くの障壁にぶつかることなく、法定通貨の価値を持つ貨幣の発行を許されなければなりません。分散型元帳は地理的な境界がないためにこれを実現することができます。元帳は世界のどの国や地域でも同じように運用できるのです。したがって国際援助にかかる外国為替手数料を標準の取引コストよりもはるかに削減できるかもしれません。さらにスマートコントラクトを使い、「見知らぬ人たちの間で自主規制の契約を作成し、国内の司法や行政とは独立して市民に取引の枠組みを提供する」[6] ことも可能です。

第 2 に国際的な資金提供者は分散型元帳技術の力を活用し、取り消しや変更が不可能な信用できるデジタル財（この場合は支援資金）の移転ができるようになります。さらにデジタル元帳は二重払いの問題も解決します。仮想通貨ではエンドユーザーが同一の通貨ユニットを繰り返し使用することができてしまうかもしれませんが、デジタル元帳では各「コイン」が固有であるため、それを防止できます。これにより支払において仲介が不要となります[6]。援助がエンドユーザーに対する直接支援である場合、通貨および金融サービスに限界・制限がある国では、資金を P2P で移転することでそれをバイパスすることができます。

第 3 に、法定通貨に関連付けられた固有の通貨を使うことで、国際援助の観点からは不適切と思われるものへの使用を防止することができます。たとえば貧困削減のために送られたインフラ整備資金をその他の目的に充当すべきではありません。分散型元帳技術ではその通貨がどこで誰によって使われたかを追跡できるため、これを防止できます。

成果

- 特に「グローバル目標」を目的とする国際援助での資金提供の透明性を高め、汚職を減らし本来の開発目的を達成できる。

成熟度

- 資金提供者の要求するものが予想できず、不正や汚職よりも大きな問題となる可能性があるため、効果を確実なものにするためにはプロジェクトの結果と整合性を取るように注意しなければならない。
- 国際的援助ではどのような場合でも、資金提供者が受け入れ側政府と関係を維持していく必要がある。受け入れ側政府の省庁職員が汚職に関わっている、あるいは組織が汚職体質であるという場合、この種のシステムを採用することについて、受け入れ側の国から同意を得ることが重要になる。
- 分散型元帳をこのような目的・形態で利用できるサービスにするためには、それを補完するさまざまな性能を備えておく必要がある。

事例 4：市場摩擦の削減とイノベーションの実現

概要

分散型元帳技術の潜在的なメリットとして最大なものは、市場の障壁・摩擦をなくし新しい形態の情報市場を作る力があることです[7]。第 1 章で見たように、分散型元帳を使い、経済主体間で情報を共有することにより、新しい形のイノベーションが生まれる可能性があります。これにより、政府は技術イノベーションを有効に利用して中小企業の経済成長の支援に関わるさまざまな政策を実現できます。

背景

中小企業が国や地方自治体と取引をするときに取引コストを減らすことができれば、市場でもっと自由に動くことができ、全体の経営コストを引き下げられます。また、中小企業がこれまでの従来の特許出願のかわりに分散型元帳を使って知的財産（IP）を登録できれば、契約に関わる訴訟の数が全体的に減少するかもしれません。英国では、全訴訟のうち契約に関わるものが 57% を占め、他のいかなる分野の訴訟よりも多くなっています。

分散型元帳技術応用の提案

分散型元帳技術は広くさまざまな分野に応用できますが、特にスマートコントラクトと資産登記に応用できます。資産を分散型元帳で登記することで、あらゆる財産が実際には「スマート資産」となり、現在中小企業にとって時間とコストの面で負担となっているさまざまなサービスの記録について堅牢で信頼できる証明が得られます。例としては IP および特許、遺言、公証サービス、国民保健サービス（NHS）の健康に関するデータ、年金または自己投資型個人年金の登録などがあります。分散型元帳により、この種のサービスを完全デジタル化し、大規模かつ効率的に連携させる新しい方法が生まれます。

分散型元帳では現在のウェブでは実現できていない少額の支払、非集中型取引、トークンの獲得・使用、移転を扱えます[8]。これにより分散型元帳技術によって、次のような地方官庁およびビジネスの運営コストを見直す可能性が出てきます[9]。

- 事業の許可
- 登録
- 保険
- 地方公共団体や規制当局の税務管理
- 年金データ

分散型元帳技術は、企業がその技術を使うことで単に自社業務についてだけではなくその資産についても登録できるために、非効率な一部門を完全になくすことも可能となります。さらに重要なのは、これまでは政府によって保有されていた個人データ（健康に関するデータなど）を国民自身がもっと管理できるようになることです。これにより国民は、自分自身のデータが適切な方法で適切な理由のためにアクセスされ、利用されているかどうかを確認できるようになります。

さらに分散型元帳を利用することで新しい形態の情報市場（さらにはデータ公益事業）を通じてデータを共有できるようになり、年金データの共有が可能になります。

成果

- 中小企業の取引コストおよび国や地方公共団体の運用コストを削減できます。さらに知的財産のようなデジタル資産の所有権を信頼できる形で証明できれば、訴訟を減らし、英国社会全体のメリットとなります。

成熟度

- 国と地方公共団体が分散型元帳技術を採用することが必要。

事例 5：欧州の VAT

概要

経済はさまざまな分類が可能で、（i）納税義務が遵守されている経済、（ii）納税義務が部分的に遵守されている経済、（iii）納税義務がまったく遵守されていない経済（つまり「ブラックマーケット」）という分類もできます。付加価値税（VAT）の徴収不足はこの 3 つの分野のいずれでも発生し、その理由としては、倒産や、国際法を都合よく解釈した納税義務回避のための会社組織化、より直接的な「書類を残さない現金のみの取引」などがあります。EU における付加価値税の徴収不足は、年間で 1,510 億ユーロから 1,930 億ユーロであると見積もられています [10]。

分散型元帳技術は大きな成長性があるとともに、取引を透明化するという潜在的な力も秘めています。英国は、EU の VAT 徴収不足を解消するための分散型元帳技術の開発、処理プロトコル、およびソリューションの実施を支援するうえで、中心的な役割を果たせる可能性があります。

背景

ムーアの法則は、デジタル計算処理能力の指数的成長を数十年前に的確に予測したものでした。事実、情報技術は 1800 年代後半から指数的に成長し続けており、このような成長は 21 世紀を通じて続くと現在予想されています。

情報技術は未知なる自然を科学的に解明しながら進むようにできていて、自生的です。さらにこれがより高速で効率の良い技術の開発につながり、その結果として他の自然の節理が明らかにされ、最終的にはこれが統合されて大きな技術力に到達します。

VAT の徴収不足を大きく改善するのに役立つ情報技術には、機械学習、スーパーコンピューター、量子コンピューター、そして分散型元帳技術など数多くあります。各国政府の大きな課題は、これらの技術を組織犯罪グループが装備する前に実装して活用することです。

分散型元帳技術応用の提案

EU 全域にわたる一連の VAT 基準とプロトコルを定めることにより、請求書から銀行の受取までの VAT 会計すべての取引を統一し、分散型元帳技術を欧州全体で採用することが可能になります。システムには、納税義務が部分的にしか遵守されていない経済にも対応できるようにスマートコントラクトを含めることができます。これはさらに EU 加盟国間で VAT を適用する際に国ごとで課税範囲が異なるという問題の解決にも役立つでしょう。

機械学習デバイスで EU の VAT 取引をリアルタイムに読み取ることができれば、違法な取引（いわゆる「回転木馬詐欺」を含む）を見つけ出す可能性は、現在の監査手法よりもはるかに高くなります。決済事業者、銀行、その他の金融機関などで追跡可能性と透明性が向上すれば、ブラックマーケット経済が隠れて存在するのが困難になるでしょう。

成果

- VAT の徴収・支払のために会社やその他の組織に課されている事務的負担を削減。
- 経済全体でのリアルタイム取引の透明性を増大。
- 与信リスクの正確な測定機会の増加と、倒産によって生じる徴収漏れを削減。
- 中小企業への与信者（ファクタリング会社を含む）に対するデータを提供。
- 国庫と商業間のスマートコントラクトを実現。

成熟度

- 技術面での準備は完了。
- 支払決済に関する可視性確保には支払組織からのデータ提供も必要になるため、これら組織の議論への早期参加が重要。
- 政府機関には租税用の分散型元帳技術の取扱能力が必要。
- エンドユーザーと小規模事業者には、税金の効率的管理のための分散型元帳技術活用法についての理解が必要。

結論

政府にとって分散型元帳は、不正や過誤を減らし、貧困層ユーザーへのサービス提供コストを削減する新たな業務運営法を提供するもので、有用なものであることは間違いありません。また、このような技術は英国の中小企業にとり、取引コストを削減できる新しい形のイノベーションとなりえます。本章では可能性のある一部の事例を採り上げただけですが、分散型元帳がさらに普及すれば、新しい政府サービスの運営形態が出現することでしょう。

第7章

グローバルな視点

サイバースペースでデジタルビジネスを行う組織は、相手を信頼し、同時に相手から信頼されなければなりません。また世界中に広がる他の組織の大きく、かつ成長中のコミュニティーとも相互運用ができなければなりません。ブロックチェーンはこの両方に貢献する可能性を持っています。

著者
パトリック・カリー（Patrick Curry）、英国ビジネス連合機構、ディレクター（Director of the British Business Federation Authority）；クリストファー・シアー（Christopher Sier）ディレクター（Director）、FiNexus；マイク・ハルソール（Mike Halsall）、カリフォルニア NASA リサーチパーク、シンギュラリティ・ユニバーシティ、グローバル・グランド・チャレンジーズ（Global Grand Challenges、Singularity University、NASA Research Park、California）

第 7 章：グローバルな視点

はじめに

世界が変化するスピードは、インターネットによってもたらされたグローバリゼーション、社会の期待、資源競争の激化により、良くも悪くもますます加速しています。発展途上の世界とは異なり、先進国とその国民は消費者の立場に立ち、プライバシーを当然のものと考えていますが、これは伝統的で根強い共同体の価値や個人の行動規範と対立することがあります。そのため困窮者の支援については共同体ではなく国家に任されています。消費者の期待と、際限のない社会福祉への要求は増大する一方ですが、政府はこれを満たそうと苦慮しています。米国元大統領ジョン・F・ケネディの「国が自分のために何をしてくれるかと問うのではなく、自分は国のために何ができるかを問うてみよ」という言葉は、今日の状況を語るにますますふさわしいものとなっています。国民の大部分は自国のために役立ちたいと考えているのですが、そのための手段をデジタル時代に持っていないのです。人々は、弱いはぐれ者であるよりも、群れに属したいと望むものです。

共同体が一致団結していない場合、結果として態度が両極化し、異なる見方が生じるとともに、複雑な変化を白か黒かという一連の細かな問題に単純化しすぎる傾向も顕著になります。世界の現実は、物理的、バーチャル、法律、歴史、地理、社会、行動、経済、情報、技術といった要素が絡み合う複雑なマトリクスになっています。さらに、変化の早さに、新しい破壊的な技術が導入されるスピードが加わり、より複雑さを増しています。そのため規模、速度、複雑さを同時に考える必要がありますが、これにより産業界のリーダーや各国政府が、このマトリクスを理解し、協力を前提としない伝統的な組織構造を用いて便益の提供を計画、実施、実現するのは次第に困難となってきています。この分野では、金融市場や組織犯罪のように、より機敏な者が先手を打ちます。また、ケニアやルワンダのような発展途上国が、古いものに囚われることなく新しい技術に飛び込んでいる例もますます増えてきています。先進国に関しては、特に欧州の国々で、小さく、同質的な傾向が強い国々が国境を越えて国際的な便益を提供しているという点で大きく先に進んでいます（76 ページの欧州のエネルギー市場に関する事例、および 80 ページのエストニアの事例を参照）。

デジタル先進国の特徴には次のようなものがあります。

- 指導者がデジタル化についてよく理解している。
- 国のデジタル化について、権限を与えられ、国際的視野を持ち、あらゆる産業部門と密接に協力する政府の専門部局が存在する。
- 産業が主導し、政府が投資する実現可能で協調的な国家計画策定が行われている。
- どの政府組織にも技術に明るく、資格と経験を有し政策に携わる上級幹部が配置されている。
- 政治家とともにエンジニアおよびデジタルビジネスのリーダーが存在する。

英国がデジタル先進国となるには、これらの分野においてやるべきこと数多くのことにと取り組む必要があります。しかし世界はますますデジタル経済に依存してきています。このため、コンピューター技術を既存の経済モデルに適用するにとどまらず、今後デジタル経済がどうなっていくのか、そこでのアクターとその活動内容についての理解を再評価する必要があります。これは現金ベース会計から資産ベース会計への移行と似ています。つまりどの組織もサプライチェーン、サービスおよび市場からなる複雑さについてより広

く理解する必要があり、協調的なリスク管理、意思決定、利益の共有ならびに責任の共有について異なるアプローチを考える必要があります。サイバースペースでデジタルビジネスを行うには、組織は相手を信頼し、自らも信頼されねばなりません。また他の組織の大きく、かつ成長中のコミュニティーとも相互運用ができなければなりません。信頼と相互運用性はサイバースペースの基盤であり、それは物理的な世界以上に重要であるといえます。ブロックチェーンはその両方に貢献できる可能性がありますが、それを実現させるのは技術ではなく、私たちが国としていかにそれを活用するかによるのです。

信頼性および相互運用性

信頼とは複数の個人、組織、国家間におけるリスク判断です。サイバースペースでは、信頼性は次の 2 つの要件に基づいています。

- 相手が本人であることの証明（**認証**）
- 行動指示するために、相手が必要な許可を得ていることの証明（**承認**）

回答が満足できるものでなくとも先に進むのを許可できますが、それはリスクが伴います。しかし相手もこちらを信頼しなければ関係は成立しません。この意味で、信頼性があるということは信用力があるということと似ているといえます。

相互運用性にはいくつかの要素があります。

- データの相互運用性。一緒に仕事をするためには相互に理解する必要があり、互いのデータが構文上も意味上も同じ基盤を持っていなければならない。
- ポリシーの相互運用性。こちらの情報をこちらが意図したとおりに相手が取り扱うであろう（また、その逆も同様）ということに対して自信を持てるように、互いのポリシーが整合している、つまり合意した共通のポリシーに基づいている必要がある。
- 有効でかつ協調に基づいた国際標準規格を利用する必要がある。

情報の保護とはアクセスを制御することであり、そのためには認証および承認などが必要とされます。認証には一定の国際的な保証レベル（LoA:Level of assurance）に準拠した、関与するすべての主体（通常は個人、組織、デバイス、ソフトウェア）のアイデンティティ(身元)管理が必要です。また、複数の官公庁や組織で形成されるコミュニティーでの認証には、連合アイデンティティ管理（FIM:Federated identity manegement）が必要です。

国際的な規模では、そのような FIM は現在のところ国際標準で「保証度:低」（LoA 1）に指定されるレベルのものしか存在していません[1]。主にこれは複数の国・地域間にまたがることが重大な問題とならないソーシャルネットワーキングに適用されます。Google、GakuNin（日本の大学・研究機関ネットワーク）、Microsoft、Ping Identity、日本経済新聞、東急電鉄、mixi、Yahoo! Japan およびソフトバンクでも FIM システムが採用されています。さらにこの他に Deutsche Telekom、AOL、Salesforce.com などの組織ではもう少し高度なシステムの導入が進められています。

「保証度：中」（LoA 2）では、顧客の身元確認（「顧客を知る（KYC）」）の要件が課されていて、登録の際にアイデンティティ（身元）を示す証拠が必要とされます。これは金融機関が金融取引を行う消費者およびビジネスに対して求めている要件です。主に銀行システムにおいて、LoA 2 レベルの連合が一部採用されています。

業界によっては X.509 という暗号標準に準拠した公開鍵インフラストラクチャー（PKI）連合（フェデレーション）に基づくセキュリティシステムが利用されています。このような

システムでは従業員の認証に「保証度：高」（LoA 3）および「保証度：最高」（LoA 4）という非常に高い保証レベルが使用されており、特に航空、製薬、防衛、金融の業界で採用され、さらに e- ヘルスでも採用が増えています。国際標準 PKI 連合は米国および中国で最も多く採用されており、それに韓国がすぐ続き（全企業による準拠を義務付け）、その後にエストニア、オランダなど多くの国が続きます。LoA 3+ ではユーザーのアイデンティティを、法的に正当性が確実に保証されるデジタル署名、アイデンティティに関連付けられた暗号、建物内の物理的なアクセスの制御のような他の信頼できる機能に関連付けることも可能です。大規模なサプライチェーンの連携や機密情報の共有について高度の保証が必要なときには、PKI 連合だけが選択肢というわけではありませんが、今日ではこれが事実上の標準となっています。ブロックチェーンはこれを代替するものとして期待されますが、PKI 連合とブロックチェーン連合を組み合わせ、それに新しい技術を採り入れることで、ビジネスプロセスにおけるデジタル形式での説明責任、保証、信頼を活用できるより多くの魅力的な機会が見つかる可能性があります。

英国では、国際標準に準拠する形で大規模に PKI 連合を採用しているのは、警察のサービスだけであり、これもまだ基本的段階です。これは、最も効率のよい共同ガバナンスを併用して、緊急サービスなど英国政府による各種サービスの支援、さらに今日同様の PKI 連合に加わっている他の組織と協力して、貿易、入国管理や移民・難民の分野における国際協力にも拡大できます。しかし、政府の公共サービスネットワーク（Public Services Network）において職員の認証に PKI 連合を利用するという戦略はまだ実施されていないため、政府のさまざまな組織を通じて、信頼性の高い職員のアイデンティティ管理や国際標準に基づく共同的な信頼性確認システムは存在しません。このようなものがあれば産業界のパートナーや米国やフランス、オランダと国際的な連合を組むことができるでしょう。

PKI 連合はブロックチェーンと組み合わせることで、プライバシーに配慮しながらアイデンティティ・データが取り扱えるようにしたり、また支払の追跡可能性を向上させたりというようにサービスを拡大できます。

国民保健サービス（NHS）には非常に大きな PKI がありますが、国際標準を満たしておらず、（まだ）連合を組むことができません。国防省（MOD）は、米国中心の防衛サプライチェーンとの PKI を整備するという国際的な義務があり、また、NATO サイバー防衛行動計画（NATO Cyber Defence Action Plan）にも同様の義務がありますが、公表されている実施計画はありません。産業界ではこの他に PKI 連合を活用できる分野がないか、たとえば 2014 年のエリオット報告（Elliott Review）にあるような食品偽装に対処するため食品供給ネットワークの健全性を確保し保証できるか、可能性を探っています。さらに、英国企業がサムスン、起亜、現代、大宇（現在世界最大のコンテナ船メーカー）など韓国ビジネスのサプライチェーンで利用できる PKI 資格証明を取得できるように、韓国政府機関との覚書も準備しています。

国連の国際海事機関では海事に関するサイバーセキュリティの国際的ガイドラインを策定中ですが、それに英韓の PKI 連合イニシアチブが活用される可能性があります。他の分野でもさらに多くの例がありますが、いずれも協調的な討論の場を利用してこのような議論が活発に行われています。

EU 議会は 2014 年 9 月に電子識別認証信頼性確認サービスに関する規則（eIDAS：Electronic Identification, Authentication and Trust Services Regulation）を承認し、各国に 3 年以内に準拠することを定めました。eIDAS ではある加盟国が電子公開の目的で自国民の e-ID スキームを「通知」すると、他の加盟国はいずれもその e-ID

を法的に受理する必要があると規定しています。まだ多くのことが完全には整備されていませんが、eIDAS が目指しているのは、政府および産業界が社会的便益および商業的便益のために FIM をどのように活用するかについて全体計画を検討することです。英国では政府が、GOV.UK Verify という連合型で標準ベースのアイデンティティ保証のアプローチを導入しています。GOV.UK Verify は市場での最新の開発に対応するものとして創設され、アイデンティティサービスを提供するプロバイダー同士の競争を認め、ユーザーが選択できるようにしています。Verify を拡張しブロックチェーンおよび PKI 連合と関連付けることで、Verify 自体にもメリットが生じ、また、Verify の入力ではプライバシーが配慮されており、ブロックチェーンと保証性が高い PKI 連合ソリューションにとってメリットとなります。これらはともに、それぞれ別の形で英国のデジタル経済、入国管理、サイバー犯罪対策に大きく役立つことが期待されます。

サイバースペースでは、すべての主体と取引は、ある 1 つの組織と結びつく、または関連

事例 1

欧州のエネルギー小売市場

イゴール・ナイ・フォビノ（Igor Nai Fovino）およびジャン・ピエール・ノルドヴィック（Jean-Pierre Nordvik）
欧州委員会共同研究センター（Joint Research Centre、European Commission）

欧州委員会(European Commission) はエネルギー同盟枠組み戦略(Energy Union Framework Strategy) [1] で、「市民がエネルギー転換の主導権を握り、新技術を利用して光熱費を削減でき、エネルギー市場に積極的に参加し、そして立場の弱い消費者が保護される」、市民中心型の「エネルギー同盟」というビジョンを打ち出しました。しかし、エネルギーのスマートグリッドは着実に進歩しているものの、エネルギーの小売市場はまだ近代化されていません。同委員会の政策イニシアチブである「新エネルギー市場の設計（New Energy Market Design）」は、次のようないくつかの重要な点に対処する必要があるでしょう。

- 完全に統合された欧州大陸のエネルギー市場で、消費者が新しい機会を見出せるよう、コストと消費量に関する適切な情報をいかに彼らに伝えるか。
- いかにして積極的な参加に報い、契約の切り替えがしやすくなるようにし、変動する価格に応じたデマンドレスポンスを管理するか。
- いかにして家庭向けエネルギーサービス市場における相互運用性を確保し、消費者の選択肢を増やし、自家発電、自家消費および地域マイクロ発電からのメリットを得られるようにするか。

この面で、分散型元帳がエネルギー小売市場の統合と発展を高めるための新しい推進役の役割を果たすことが期待できます。欧州委員会の共同研究センター（Joint Research Centre）[2] では現在、次の事例に示すような実践的な応用について調査しています。

1. マイクロ発電エネルギー市場：マイクロ発電は消費者が自家または地域の共同体でエネルギーを生産するものです。「市場」という言葉から、消費者や「生産消費者」がマイクロ発電されたエネルギーを取引する可能性があることが示唆されます。しかし、従来このような市場は生産消費者と小売エネルギーの供給者との事前に取り決められた双務契約で取り仕切られていました。今日まで、発電を行う生産消費者はエネルギー市場に本当の意味ではアクセスがなく、このような市場はそこで活動する特権を持つ既成のエネルギー供給者だけのものとなっています。これが原因で、マイクロ発電のエンドユーザー、つまり消費者がその経済的なメリットを享受することは大きく妨げられていました。そこで、分散型元帳をスマートメーターシステムや次世代バッテリー（エネルギーを地域で蓄積するために使用）と組み合わせることにより、生産消費者によって生産されたエネルギーを市場に提供できる可能性が出てきました。スマートメーターを使用してマイクロ発電エネルギーを測定し、分散型元帳に記録する（「エネルギー貨幣」システムのようなものになる）という利用法が考えられます。

自家発電の電力は普通、自家で消費されるか、あとで使用するときのため次世代バッテリーに蓄積されるか、または単にグリッドに戻されます。その代わりとして、元帳の分散および浸透するという性質を利用して、産出され

付けられています。ある組織が望ましい保証レベル（LoA）の正当な組織であることを確認でき、さらに、その組織に関する情報をリアルタイムまたはそれに近いタイミングで検証できるということは、デジタル時代の基本要件です。

ブロックチェーンが次第に普及するにつれ、チェーン内の記録の改ざんを防止するためのこのような要件はいっそう厳しくなると予想されます。

組織のデジタル識別については、合法的組織登録（ROLO：Register of Legal Organisations）と呼ばれる新しい国際標準が作成されている途中です。米国を含め、いくつかの国ではすでに、そのニーズを満たすため ROLO 仕様の採用が検討されています。今日グローバル化が進展しているにもかかわらず、デジタル世界に適したビジネスの登録手段がありません。特に EU 諸国など、ある国で活発に金融活動が行われている組織の大部分が、その国あるいはどの国でもまったく登録されていない、しかもその違いを判別することが不可能である、という状況が生まれています。英国の産業界、ならびに法執行機関およびサイバーセキュリティ組織などの政府組織は、信頼できるデジタル登録を行うために、その拠り所となる英国版 ROLO である ROLO UK を至急整備する必要があります。産業界は ROLO UK の設立準備を始めていますが、政府側でユーザーとなる組織からもより積極的な参加があればメリットとなるでしょう。

たエネルギーを他の場所で、たとえば海外で電気自動車を充電するときに使う、あるいは証券取引所のような仕組みに従い元帳を通じて最高の買い手に売却する、などができます。

2. エネルギー契約元帳:消費者がエネルギー供給者を他に切り替えたいと考える場合、現在のところは現行の供給者との契約を終了させ、次に新しい供給者と新たな契約を締結し、さらに第三者によって提供されているすべての補完的なエネルギーサービスの契約条件を再検討する必要があります。

このような切り替えに伴う複雑な事務手続の管理が、競争が盛んなエネルギー小売市場が発展するうえで大きな障壁となっており、また、エネルギー供給および販売を行う者にとってはコスト要因となっています。分散型元帳を使いオンラインでエネルギー契約を記録できれば、このような手続が大きく簡素化されます。これにより消費者は、ある供給者から別の供給者への切り替えを、コンピューターやモバイルデバイスで 2、3 回クリックするだけで終えることができます。同様にエネルギーの供給者や関連サービスの供給者にとっては、このような事務的手続にかかる資源を節約できます。

このような応用に関しては、その拡張性、セキュリティ、安定性の面でまだ疑問が残ります。しかし大きなメリットが期待されるため、さらに調査する価値は間違いなくあります。

デジタル経済

デジタル経済では、スピード、普及度、効率性の向上が求められています。「信用の連合」が実現できれば、信頼が得られ、リスクを削減できます。相互運用が可能になれば、さまざまな能力の効率向上や再利用が可能になります。成熟したサプライチェーンでは、企業が新しいプログラムや部門で競争をするときに、前の技術を再利用すれば対応が機敏になり競争力が増します。この考えは航空宇宙や防衛産業で一般的であり、Airbus、Boeing、BAE Systems、Lockheed Martin、Northrop Grumman、Raytheon[2] など各社によって

公に提唱されています。

2014 年 2 月、当時、欧州委員会（European Commission）の副委員長（Vice-President）でデジタル問題コミッショナーであったニーリー・クロエス（Neelie Kroes）は、「民主主義は技術と対話しなければならない」[3] と発言しました。彼女は、私たちはデータ主導の世界に移行しており、そこでは信頼が重要であり、「セキュリティなしではプライバシーもない」と主張しています。彼女は、欧州の単一デジタル市場にとってサイバーセキュリティは重要で、EU のサイバーセキュリティ戦略はその根幹としての役割を適切に果たすものであると指摘し、そのようなイニシアチブなしでは、民主主義は「技術を管理できない」と結論付けています。

これらの問題に関する EU、米国および東南アジア諸国（ASEAN）が参加している話し合いでは、次第に銀行業務、エレクトロニクス、製薬、食品、海事、航空宇宙、サイバースペース、法執行機関の分野に議論が集中してきています。発展途上国がグローバルなデジタル経済に組み込まれていく過程で、先進国が発展途上国を支援すべきであるという声が国連および欧州評議会（Council of Europe）のような組織を通して次第に高まっています。しかし、デジタルガバナンスの欠如が発展途上国の足かせとなり、最終標的を先進国にするサイバー犯罪およびテロリズムの温床となっています。イギリス連邦はこの状況に対処するうえで大きな役割を果たすことができます。協力・協調が重要な鍵です。

分散化元帳およびブロックチェーンの持つ潜在的な力

経済において、金融市場が信頼されるようにするには、協力・協調的なガバナンスが必要であり、全員が合意した規則に従わなければなりません。デジタル経済も同様です。ブロックチェーンがサイバー犯罪に関連付けられる主な理由は、合意された規則を制定し、そのコンプライアンスを確保するための戦略的ガバナンスが欠如していることです。そのようなガバナンス（およびポリシー、手続、制度）が確立され、執行機関が整備されれば、社会におけるブロックチェーンの真のメリットが享受されるようになります。政府の立場からすると暗号通貨とそれを使った交換取引の不安定性と脆弱性に対する懸念があるため、各国政府はブロックチェーンの利用に慎重になっており、一般的に産業界が主導して状況の改善を進めることを望んでいます。

今日、開発の対象となっている主な分野は次のとおりです。

- 管理者のいないブロックチェーンは規則のない犯罪活動に使われ、特に当事者が匿名でいることや責任義務を負わないことを望む場合に使われています。
- スタートアップ企業が大手銀行と共同し、信頼できる暗号通貨およびブロックチェーン（「信頼できるビットコイン」など）を開発しています。これは消費者向け商品の大手オンライン販売会社にとって大きなメリットとなります。
- プライベート型のブロックチェーンは、アクセスが一部の者に限定された商業的なコミュニティーで当事者独自の規則のもとで機能する、デジタル形式の信頼メカニズムを支えるために使われています。このようなブロックチェーンには相互運用性がなく、規模を拡大してサプライチェーンを支援することはできません。

ブロックチェーンの戦略的な可能性を探るために政府が産業界と協力するようになったのは、ごく最近のことです。しかし実用化は次の 4 つの要素における発展により加速していくことが予想されます。

- 暗号化された信頼性の基盤が PKI と同様の方法で提供されるようにします。これは

ブロックチェーンが互いに連合し、また既存の PKI 連合ともつながるということを意味します。ブロックチェーン側では PKI の導入規模とガバナンスを活用でき、PKI 側でもブロックチェーンの持つ支払および元帳の機能を活用できます。このような相乗効果によりスマートで協力・協調的なガバナンスがいっそう進むという新たな機会が開けてきます。

- 許可型元帳のデータフィールドのサイズには制限がありません。契約、認可、著作権などの取引に関する情報を含めることで、信頼をさらに強固なものにすることができます。これにより、効率的で否認不可の「スマートコントラクト」（つまり、取引に契約の拘束力を付加すること。詳しくは第 1 章を参照）が可能になります。
- 生産者と運送業者、顧客、製品、支払、銀行、そしてスマートコントラクトとも関連付ける新しい統一経済移転プロトコル（UETP：Uniform Economic Transfer Protocol）のような新しいプロトコルを活用します。オランダは英国の産業界の協力とおそらく警察による参加もあり、この分野で他国よりも進んでいます。米国も参入し始めており、すべてのサプライチェーンにサイバー保証を求める規制が浮上してきていることから、この動きが加速すると予想されます。韓国や日本などその他の国も間もなく参加してくると予想されます。
- スマートフォンは事実上信頼されるユーザーデバイスとなりつつあります。最新のスマートフォンには、認証、暗号化、署名に用いるデジタル証明と暗号化キーを安全なものにする Trusted Platform Module、マルウェアに対し脆弱な可能性があるオペレーティングシステムを使用せずに安全な処理を実行する Trusted Execution Environment、ユーザーとデバイス間へのマルウェア攻撃を防ぐ Trusted User Interface といった新しい重要なセキュリティ機能が含まれています。近接距離無線通信（NSC）を利用することで、スマートフォンが一部の国民電子 ID カードや電子パスポートと安全に通信できるようになり、ユーザーはオンラインで入国管理や警察などの当局と安全に通信できるようになります。利用者および従業員は今初めて安全で信頼できるデバイスを手にすることができ、これを用いて取引に署名する（たとえばブロックチェーンを使用）、支払をする（たとえば「信頼できるビットコイン」を利用）ことが可能になったのです。Samsung、HTC、LG ではそのような高度なセキュリティ対応のスマートフォンをすでに数千万台も販売しています。この機能を備えたソフトウェアは 2016 年初めから半ばにかけて展開予定です。Apple およびその他もこれに続くことが予測されています。

ただし、このような能力の乱用・誤用がないよう、協力・協調に基づいた広範で強力なガバナンスが必要です。これらの 4 つの要素によりブロックチェーンと分散型元帳は、金融、あるいはサプライチェーン全体や政府において増え続けるさまざまなデジタル、データ中心型の利用目的により広範に利用されています。そのようなシステムが成熟し能力が拡張されるにつれ、これら 4 つの要素が社会的およびグローバルな数々の困難な課題を解決するのに役立ちます。この事例には次のようなものがあります。

- **透明性のある誠実な政府。**発展途上国では、安定し、説明責任を備えた法治国家体制を持つ国々よりも国民の国に対する信頼度が低く、より良い共同体の確立と社会的な行動の妨げとなっています。戦争で破壊された地域や独裁体制下で生活してきた人々が、政府を信頼し、汚職が減るようにするには長い時間がかかります。ブロックチェーン、FIM、その関連機能を利用して説明責任と保証のメカニズムをビジネスプロセスに組み込むことは、法、ポリシー、組織構造を有効に実施・執行するのに欠かすことができません。

- **脱税および資金洗浄。**一国の富の分布曲線が極端に急勾配になると、資金や資産を持つ者はその富を海外に隠そうとするため、国内の金融資産の流動性が減り、富の分布曲線の下部にある低所得層の経済機会が奪われることになります。その結果として資本枯渇による経済の衰退が始まり、若年層の大量失業があとに続き、失われた世代にはリーダーシップに対する不信感が傷となって長く残ります。これが民主主義を弱体化させ、社会の崩壊、国家の機能不全、テロリズム、悲惨な状態の人々が生まれる条件を整えることになります。この場合でも、これらの問題に取り組むためには説明責任と保証が必要になります。
- **違法取引および環境破壊。**海洋生物のおよそ 50% が過去 30 年間に死滅し、その状況は陸上でも同様です。「絶滅のおそれのある野生動植物の種の国際取引に関する条約（CITES:Convention on International Trade in Endangered Species of Wild Fauna and Flora）」（ワシントン条約）による国際的な努力にもかかわらず、地球は第 6 次の大量絶滅時代に向かっているという証拠があります。このグローバルな状況を救おうと望むのであれば、資産の発見・追跡のためのより強力なメカニズムを実施し、同様に十分な説明責任と保証を求めなければなりません。

事例 2

エストニアにおけるブロックチェーン導入による支払、取引、署名形態の変貌

アラステア・ブロックバンク（Alastair Brockbank）、在タリン英国大使館（British Embassy Tallinn）

エストニアにとってブロックチェーン技術の実験は当然のステップでした。分散型の変更不可能な情報元帳を提供することで、同国は理想的な質の高いパブリックキーの保管・管理を実現することができました。これは専門の機関から提供される暗号化キーの形態をとったもので、プライベートキーと組み合わせて、効果的にメッセージを暗号化しデジタル署名を認証するものです。現在エストニアは、世界で最も頻繁に利用されている公開鍵インフラストラクチャー（PKI）を有しています。

さらにブロックチェーンは非集中型のソリューションであるため、本質的にポータビリティが高く、規模の拡大が可能です。毎秒膨大な量のデータを計算し、境界を越えてシームレスに運用することもできます。このため、人口わずか 130 万の国に所在する企業にとっては、ブロックチェーンによって国内ソリューションを容易にグローバルソリューションに発展させる可能性が提供されます。その大きな計算能力も処理を高速化するのに役立ち、場合によってはこの技術は既存の仲介者を不要にするだけの破壊力を持っているといえます。

銀行、スタートアップ企業、サイバーセキュリティのプロバイダーを採り上げた以下の 3 つの事例は、ブロックチェーンのさまざまな取引を変貌させる影響力を示すものです。3 つの例はいずれも、ブロックチェーンはユーザーにとり使いやすいように作られる必要があるということを強調するものです。顧客は、自分がカラードコインで取引をしていることや、あるいは ID カードのログインでハッシュ関数の暗号化が使用されていることなど知る必要はありません。この意味では、ブロックチェーンは、モバイル決済アプリ、オンラインのクラウドファンディングおよび取引用のプラットフォーム、ログインポータルなど、よく知られているソリューションの背後で静かに効率よく動いているといえます。

英国と同じように、エストニアの政府当局にとって規則の必要性とその適用範囲は重要な問題です。エストニアの政府当局は、厳格さはもちろんのこと、躊躇や優柔不断さが、イノベーションにとり有害であるということを理解しています。規制の緩やかな新しい分野に参入するイノベーターにとり、リスク、特に商業機会を活用できずに収益を失うリスク、および犯罪行為となる可能性があるリスクがあることは明らかです。

- **食品偽装とサプライチェーンの混乱。**英国はこれまで以上に輸入食品に依存しており、1917年や1942年よりも全国的な食品危機に対して脆弱になっています。食品のサプライチェーンを追跡するのは、たとえば2013年の混入肉の問題（「馬肉スキャンダル」として広く報道）に見られるように困難なことであり、偽装の機会は多数あります。国際的にも英国国内でも食品のサプライチェーンで説明責任ときめ細かな追跡可能性を確保するためには、他の分野で最高水準のサプライチェーンの保証を選択するしかありません。
- **サプライチェーンへの脅威。**サイバー犯罪と国際的な知的財産窃盗が増加する中（世界的には7兆ドル超）、サプライチェーンに対して説明責任および連合的なアイデンティティ管理を含め、協力・協調的なリスク管理を基にしてより確実な保証が行われるよう、規制、市場ならびに社会的な圧力が高まっています。

説明責任と保証を提供・実施されるようにするため、英国は他の先進国や国際的な専門家とともに、欧州評議会、世界銀行、G20、国連に対して、強力な認証ができるブロックチェーンを採用するよう働きかけることができます。しかし、これは英国政府だけでは実現できません。産業界は、政府が産業界と協力し国の能力を高め先行者としての優位性を保ち、英国がグローバルリーダーの1国としての地位を確保できるよう、この活発な国家的な努力の一翼を政府が担うことを求めています。

先進的な銀行による暗号通貨建て有価証券の発行

今年初め、エストニア最大の独立銀行であるLHV Pankは、暗号で保護された10万ユーロの預金証書を発行し、世界で初めてプログラム可能通貨の実験をした銀行となりました。この実験は、ビットコインをベースにしたデジタル有価証券に特化したLHVの新子会社であるCuber Technologyの設立に続いて行われたものです。Cuberの業務にはCUBERの有価証券とCuber Walletの2つがあります。

Cryptographic Universal Blockchain Entered Receivable(CUBER) 有価証券は単にビットコインのブロックチェーンに記録される銀行の預金証書にすぎません。証券はユーロ建てで、利子を付すことができ、価値の保管、交換手段、信託およびエスクローサービス、さらにモノのインターネット(IoT) への応用の可能性を開くマシンツーマシン取引などさまざまな目的に適しています。LHVでは、CUBERの有価証券を将来の金融イノベーションの布石のようなものと見ています。

Cuber WalletはCUBERの利便性を初めて示しました。これはモバイルフォン用のソフトウェアで、CUBER有価証券を担保にして、即時無料のP2Pユーロ取引、および商店や消費者による低コスト即時支払を可能にするものです。

ユーザーは自分のプライベートキーを自分のスマートフォンに保管することで、より高いセキュリティとモビリティが得られます。サーバーのセキュリティを守るため、Cuber Walletでは信頼をサーバーから分散させ、ユーザー自身をビットコインのクライアントにします。アプリでは一種の「シンクライアント」セキュリティであるSimplified Payment Verification（SPV）が利用されており、これによってユーザーがチェーンの各ブロックの完全なコピーを持つことは決してありません。そのかわりにユーザーは「ブロックヘッダー」という、取引をチェーン内のある特定の場所と関連付ける少量のデータをダウンロードします。これによりユーザーはネットワークのノードで取引が受け付けられたことを確認でき、さらにその後に付加されたブロックにより、ネットワークでその取引が受け付けられたことを確認できます。

ウォレットでは、ビットコインをデータの搬送体として使い、ビットコインは固有マーカーを付加することにより「ペイント」します。これはその後、データベースへの入力によって伝統的な銀行制度で請求権があることが示されるように、LHV銀行に対する不換紙幣による請求権があることを意味します。不換紙幣を使用することにより、ウォレットは個人の資金移転だけでなく小売支払にも利用することができ、商店では、クレジットカードを承認しなければならないのと同じように、この支払を承認する必要があります。LHVでは現在これを実際に何か所かの店舗で試験していますが、オンラインビジネス、特に少額支払でもっと広く利用されることを想定しています。

不換紙幣の使用によりこのアプリがユーザーにとり使いやすいものになっていることは間違いありません。しか

事例 2（続）

し、LHV では銀行の関心は根幹となっている技術であることを強調しています。Cuber でビットコインが使用されていることをユーザーおよび売り手は見たり知ることはないし、その必要もないのです。

Cuber のオープンソースコードとアプリケーションのプログラムインターフェースはサードパーティーがオンラインで入手でき、他の暗号通貨との交換を勧誘し、開発者にこの技術に触れるよう奨励するものです。LHV とその開発パートナーである ChromaWay は、大銀行とではなく、小規模なソフトウェア開発企業やスタートアップ企業と共同して、役立つイノベーションを推進することを望んでいます。

LHV の挑戦に対する姿勢は明確で、不確実な規制が行われれば、Cuber に大きな制約が課され、変革力が削がれるリスクがあると考えています。規制当局がブロックチェーン技術を恐れて逃げるのではなく、それを受け入れて採用するようにと同行は主張しています。

見たところ、銀行の支援を受け、従来の銀行口座からデジタルウォレットへの資金移転は（そして再び戻すのも）簡素化されているため、Cuber には大きな優位性があります。CUBER は、非集中型の記録保管機能があるとはいえ、技術的には依然として（銀行取引の基盤である）証券の一種です。しかし現実には銀行であるということが規制の面で障害となります。一般に、銀行は他のイノベーターたちと比べ、より法的規制の対象となるからです。同様に銀行口座開設時に面談を必要とする EU の顧客の身元確認（「顧客を知る（KYC）」）の規則は、TransferWise や Holvi のような他のオンライン決済サービスで必要なのは簡単なオンライン登録のみであることと比べると、Cuber にとって不利です。銀行がこの市場で効果的に競っていくにはこれ以上障害となる規則を銀行に課す必要はなく、新しいユーザーを獲得するためにその機動性を弱める必要もありません。

確かに LHV は「イノベーション・フレンドリー」を自ら実行しているユニークな銀行といえますが、現在のところその進歩は規制の不確実性によって制約を受けています。前向きな動きがなければ、Cuber は LHV の事業許可と銀行と関連していることによるメリットを放棄するか、欧州以外の国・地域への移動を検討しなければならないでしょう。

暗号を基にした銀行業務と伝統的な銀行業務との間をつなぐ、単純で安全、しかも法規を遵守した橋を築くことは、すべての参加者にとって今後も大きな挑戦であり続けることでしょう。しかしその中では LHV が最も目標に近い位置にいるといえるのです。

スタートアップ投資流動化のためのアフターマーケット

スタートアップ投資の非流動性はエンジェル投資家および創業者に共通する悩みです。後援者は一般に最低 10,000 ユーロの投資が必要で、エクジットには 5 年以上待たねばならないことがしばしばです。

投資家向けビジネス情報収集のプラットフォームである Funderbeam は、この問題を解決しているといえるかもしれません。これはブロックチェーンをベースにして、スタートアップシンジケートへ投資したカラードコインの売買を行う投資市場です。

投資家は間もなく、Funderbeam のオンラインプラットフォームを利用して 1 社または複数のスタートアップ企業への投資シンジケートを組成できるようになります。投資ではどのような設定も可能で、協調融資（シンジケーション）の規模に制限はありません。10 万ポンドの投資は、1 人のリード投資家とその他 99 人が 1,000 ポンドずつ投資する場合もあれば、リード投資家が 75,000 ポンドを投資し 5 人が 5,000 ポンドずつ投資する場合もあり、さらにその他どのような組み合わせもありえます。これにより、クラウドファンディング同様、スタートアップ企業への投資における制限が解消されます。

Funderbeam とクラウドファンディングとの違いは、シンジケートメンバーの投資であることを表す「カラードコイン」の発行にあり、これはすぐに売買したり他の投資家と取引したりすることが可能です。これにより投資ポートフォリオの管理がもっと流動的になり、スタートアップ企業の資金調達が促進されます。ビットコインのブロックチェーンがアフターマーケットの基盤となり、迅速で効果的で透明性の高い資産の所有権の追跡を可能にします。

各シンジケートはマイクロファンドと対にされます。シンジケーションが完了し、スタートアップ企業の資金調達ができると、Funderbeam のアフターマーケットではカラードコインを使用して、シンジケートの全メンバーにマ

イクロファンドでの出資分に相当するコインが付与され、それは速やかに取引可能となります。出資者はこれにより、一定収益の確保後、または損切りのため、持ち分のすべてまたは一部を売却できます。

ブロックチェーンというソリューションが提供するメリットは、投資家の柔軟性だけではありません。Funderbeam の CEO であるカイディ・ルーサレップ（Kaidi Ruusalepp）は、分散型元帳では官僚主義を回避して得られる効率性も指摘しています。「取引の整合性を確認するのにビジネス登録や預託金、その他の権限は必要ありません」、そう彼は語ります。「ブロックチェーンによりすべての投資、あらゆる所有権の変更には安全で分散型の監査証跡が付されるのです」。

Skype の共同創業者で Funderbeam に投資しているヤーン・タリン（Jaan Tallinn）は、オンライン取引に関するセキュリティおよび検証機能が強化されている点を称賛しています。非集中型で変更不可能であることから、ブロックチェーンは誰のプライバシーを侵害することもなく株式市場により多くの透明性を与えることができます。

Funderbeam が提供する柔軟性、スピード、セキュリティ、透明性は、21 世紀で中小企業が成長するための資金調達において、分散型元帳がいかにしてこれまでと違い、しかも完全に実現可能な選択肢となりうるかを示すものです。

次世代のパブリックキーインフラストラクチャー

2013 年からエストニア政府の登録では、国民およびビジネスに関する情報の保管を含め、そのデータベースに収録されるデータの認証に Guardtime を利用しています。同国のキーレス署名インフラストラクチャー(KSI) は「ハッシュ関数」による暗号化（以下を参照）を分散型元帳と組み合わせたもので、これによりエストニア政府はネットワークおよびデータストア内の全コンポーネントの状態に関する記録について保証することができます。

これは小規模な試みではありません。エストニアには世界で最も頻繁に利用されている国家レベルの PKI があります。国民は ID カードを使い、処方薬注文、投票、オンラインバンキング、子供の学校の成績の確認、国からの給付金申請、税金の申告、建築許可申請、遺言のアップロード、兵役応募、その他およそ 3,000 の機能を実行できます。企業はこの ID カードを使い、年次報告書提出、株主への書類の発行、認可申請などができます。政府職員は ID カードを使い、安全な通信のための書類の暗号化、許可、契約、申請の確認と承認、法執行機関への要求された情報の提供を行います。閣僚も ID カードを使用して、閣議の準備、閣議への参加、議案見の確認、態度表明、反対意見の提出、議事録の確認を行います。

このようにデジタル認証は、政策立案、立法から財務公表、財産や相続した権利の登記まで、政府、ビジネス、公的サービスにおいて等しく重要となっています。これまでに 2 億件を超えるデジタル署名が ID カードを使用して行われ、これは 1 人当たり年間 39 件になり、今も利用は増加しています。したがって政府にとっては、その記録が正しいもので、内部、またはサイバー攻撃により変更されていないことを確認することが必須です。

ではブロックチェーンはどのように役立つのでしょうか。これが役に立つのは、データのどのような部分の変更もすべて記録されるからです。時間、アイデンティティ、真偽性についての証明を示すことで、KSI 署名はデータの整合性、遡及的保護、データが改ざんされていないことに関する検証可能な保証を提供します。さらに、ブロックチェーンには透明性がありユーザーにもメリットがあります。国民はデータを閲覧した者、その理由、時刻を見ることができ、個人データへの変更は承認されねばならないのです。さらにほとんどの PKI で使用されている非対称型暗号技術ではなく、ハッシュ関数が使用されているため、KSI は量子アルゴリズムによっても破られません。またこれは簡単に拡張が可能で、毎秒 1 エクサバイトのデータに署名することができます。しかも計算とネットワークの負荷は無視できるほどです。これにより認証局が不要となり、署名データは国や地域の境を越えて検証可能となり、顧客データを取り込まないのでプライバシーの侵害もありません。このシステムが PKI における大きな進歩であることは明らかです。

エストニアの ID カードは絶対に侵害されないわけではありませんが（これまでにその例はない）、エストニア政府は最終的に KSI ブロックチェーンによって公開データの不正な改ざんは 100% 探知可能となることを確信しています。

参考文献

要旨

1 Government Office for Science ‘FinTech Futures: The UK as a World Leader in Financial Technologies’ 2015. 参照：https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/413095/gs-15-3-fintech-futures.pdf

第 1 章

1 Government Office for Science ‘FinTech Futures: The UK as a World Leader in Financial Technologies’ 2015. 参照：https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/413095/gs-15-3-fintech-futures.pdf

2 IBM Institute for Business Value ‘Device democracy: Saving the future of the Internet of Things’ 2015. 参照：http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=XB&infotype=PM&appname=GBSE_GB_TI_USEN&htmlfid=GBE03620USEN&attachment=GBE03620USEN.PDF

3 Government Office for Science ‘The Internet of Things: making the most of the Second Digital Revolution’ 2014. 参照：https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/409774/14-1230-internet-of-things-review.pdf

第 2 章 事例：研究およびホライズン・スキャニング

1 ‘CREDIT: Cryptocurrency Effects in Digital Transformations’ EPSRC reference EP/N015525/1 (2015). 参照：http://gow.epsrc.ac.uk/NGBOViewGrant.aspx?GrantRef=EP/N015525/1

2 ‘2015 ITaaU Community Conference’. 参照：http://www.itutility.ac.uk/event/2015-itaau-community-conference/

3 Networked Society Lab, Ericsson ‘ICT and the Future of Financial Services’ (2014). 参照：http://www.slideshare.net/Ericsson/horizon-scan-ict-and-the-future-of-financial-services

4 EPSRC ‘Trust, Identity, Privacy and Security in the Digital Economy’ (2015). 参照：https://www.epsrc.ac.uk/funding/calls/trustidentityprivacysecurity/

5 Perry M and others ‘The currency of digital money’ (2015). 参照：https://www.youtube.com/watch?v=PCa3pTCegE8

6 3DaRoC ‘Digital Intermediary Exchange Toolkit’ (2015). 参照：https://digitalintermediaries.wordpress.com/toolkit/

第 3 章

1 Lessig L ‘Code and other laws of cyberspace, Version 2.0’, New York: Basic Books 2006.

2 New York Department of Financial Services ‘BitLicense Regulatory Framework’. 参照：http://www.dfs.ny.gov/legal/regulations/rev_bitlicense_reg_framework.htm

第 4 章

1 Internet Engineering Task Force ‘Certificate Transparency’ 2013. 参照：https://tools.ietf.org/html/rfc6962. または http://www.certificate-transparency.org/

2 Melara MS and others ‘CONIKS: Bringing Key Transparency to End Users’ Cryptology ePrint Archive: Report 2014/1004. 参照：http://eprint.iacr.org/2014/1004.pdf

3 Danezis G and Meiklejohn S ‘Centrally banked cryptocurrencies’ Cryptology ePrint Archive: Report 2015/502. 参照：https://eprint.iacr.org/2015/502.pdf

4 Courtois N ‘Is Bitcoin Going to Split in Two?’ 2015. 参照：http://blog.bettercrypto.com/?p=1811

5 Nakamoto S ‘Bitcoin P2P e-cash paper’ 2008. 参照：http://satoshi.nakamotoinstitute.org/emails/cryptography/1/

6 Meiklejohn S and others ‘A fistful of bitcoins: characterizing payments among men with no names’ Internet Measurement Conference 2013 pp. 127-140

7 Danezis G and others ‘Statistical Disclosure or Intersection Attacks on Anonymity Systems’ Information Hiding 2004 pp. 293-308

8 Bonneau J and others ‘Mixcoin: Anonymity for Bitcoin with Accountable Mixes’ Financial Cryptography 2014 pp. 486-504

9 Garman C and others ‘Rational Zero: Economic Security for Zerocoin with Everlasting Anonymity’ Financial Cryptography Workshops 2014 pp. 140-155

10 Miers I and others ‘Zerocoin: Anonymous Distributed E-Cash from Bitcoin’ IEEE Symposium on Security and Privacy 2013 pp. 397-411

11 Danezis G and others ‘Pinocchio coin: building zerocoin from a succinct pairing-based proof system’ PETShop@CCS 2013 pp. 27-30

12 Groth J and Kohlweiss M ‘One-Out-of-Many Proofs: Or How to Leak a Secret and Spend a Coin’ EUROCRYPT 2015 pp. 253-280

第 5 章

1 Christensen CM and others ‘Strategies for Survival in Fast-Changing Industries’ Management Science 1998: volume 44, pp. S207-S220

2 Jacobides MG and others ‘Benefiting from innovation: Value creation, value appropriation and the role of industry architectures’ Research Policy 2006: volume 35, pp. 1200-1221

3 Baden-Fuller C and others ‘Business Models & Technological Innovation’ Long Range Planning 2013: volume 46, pp. 419-426

4 Jacobides MG and others ‘Who does what and who gets what: capturing the value from innovation’ Advanced Institute of Management Research Briefing 2006. 参照：http://faculty.london.edu/mjacobides/assets/documents/whodoeswhat.pdf

5 Perez C ‘Technological Revolutions and techno-economic paradigms’ Working Papers in Technology Governance and Economic Dynamics 2009: Tallinn University of Technology, Tallinn, Norway

6 Rifkin J ‘The Zero Marginal Cost Society: The Internet of Things, the Collaborative Commons, and the Eclipse of Capitalism’ 2014. New York, Palgrave Macmillan

7 Birch D ‘Identity is the New Money’ 2014. London Publishing Partnership

第 5 章 事例：コーポレートアクション

1 Oxera. ‘Corporate action processing: what are the risks?’ May 2004. http://www.oxera.com/Oxera/media/Oxera/downloads/reports/Corporate-action-processing.pdf?ext=.pdf

第 6 章

1 Swan M ‘Blockchain: Blueprint for a New Economy’ O’Reilly Media Inc 2015

2 Department for Work and Pensions ‘Fraud and Error in the Benefit System 2013/14’ 2014. 参照：https://www.gov.uk/government/collections/fraud-and-error-in-the-benefit-system

3 Financial Inclusion Commission ‘Financial Inclusion: Improving the financial health of the nation’ 2015. 参照：http://www.financialinclusioncommission.org.uk/report

4 Rowlingson K and McKay S ‘Financial Inclusion: Annual Monitoring Report 2014’. 参照：http://www.birmingham.ac.uk/Documents/college-social-sciences/social-policy/CHASM/annual-reports/chasm-annual-monitoring-report-2014.pdf

5 United Nations ‘The Millennium Development Goals Report’ 2010. 参照：http://www.un.org/millenniumgoals/pdf/MDG%20Report%202010%20En%20r15%20-low%20res%2020100615%20-.pdf

6 Ammous S ‘Economics beyond Financial Intermediation; Digital Currencies’ possibility for growth, poverty alleviation and international development’ Columbia University Working Paper No. 82 November 2013

7 Mulligan CEA ‘The Communications Industries in the Era of Convergence’ Routledge 2011

8 Swan M ‘Blockchain: Blueprint for a New Economy” O’Reilly Media Inc 2015

9 詳細なリストは以下を参照：‘Bitcoin Series 24: The Mega-Master Blockchain List’. 参照：http://ledracapital.com/blog/2014/3/11/bitcoin-series-24-the-mega-master-blockchain-list（2013年8月13日現在）

10 EU Taxation Commissioner Algirdas Semeta, quoted in 2013 at http://www.eureporter.co/economy/2013/09/20/fight-against-fraud-study-confirms-billions-lost-in-vat-gap/（2015年9月18日現在）

第 7 章

1 ISO/IEC 29115 – Entity Authentication Assurance Framework

2 Including Boeing, Northrop Grumman and Raytheon joint video.

3 EU Cybersecurity Strategy High Level Review – 28 Feb 14.

第 7 章 事例：欧州のエネルギー小売市場

1 European Commission ‘A Framework Strategy for a Resilient Energy Union with a Forward-Looking Climate Change Policy’ 25 February 2015: COM(2015) 80 final. 参照：http://eur-lex.europa.eu/resource.html?uri=cellar:1bd46c90-bdd4-11e4-bbe1-01aa75ed71a1.0001.03/DOC_1&format=PDF

2 Joint Research Centre. 参照：https://ec.europa.eu/jrc/