

東京大学 公共政策大学院

ワーキング・ペーパーシリーズ

GraSPP Working Paper Series

The University of Tokyo

GraSPP-P-17-001

ブロックチェーン技術のテクノロジーアセスメント

グレッグ海 嶋吉慧 白石桃子 三重野航 宮本寛之

2017 年 10 月

GraSPP
THE UNIVERSITY OF TOKYO

GraSPP Policy Research Paper 17-001

GRADUATE SCHOOL OF PUBLIC POLICY
THE UNIVERSITY OF TOKYO
HONGO, BUNKYO-KU, JAPAN

GraSPP
THE UNIVERSITY OF TOKYO

GraSPP-P-17-001

ブロックチェーン技術のテクノロジーアセスメント

東京大学 公共政策大学院 事例研究(テクノロジー・アセスメント)2017年度

東京大学大学院公共政策学教育部公共政策学専攻(経済政策コース)専門職学位課程1年 グレググ海
東京大学教養学部学際科学科(科学技術論コース)学部4年 嶋吉慧
東京大学大学院公共政策学教育部公共政策学専攻(経済政策コース)専門職学位課程1年 白石桃子
東京大学大学院公共政策学教育部公共政策学専攻(経済政策コース)専門職学位課程1年 三重野航
東京大学大学院工学系研究科システム創成学専攻修士1年 宮本寛之

GraSPP ポリシーリサーチ・ペーパーシリーズの多くは

以下のサイトから無料で入手可能です。

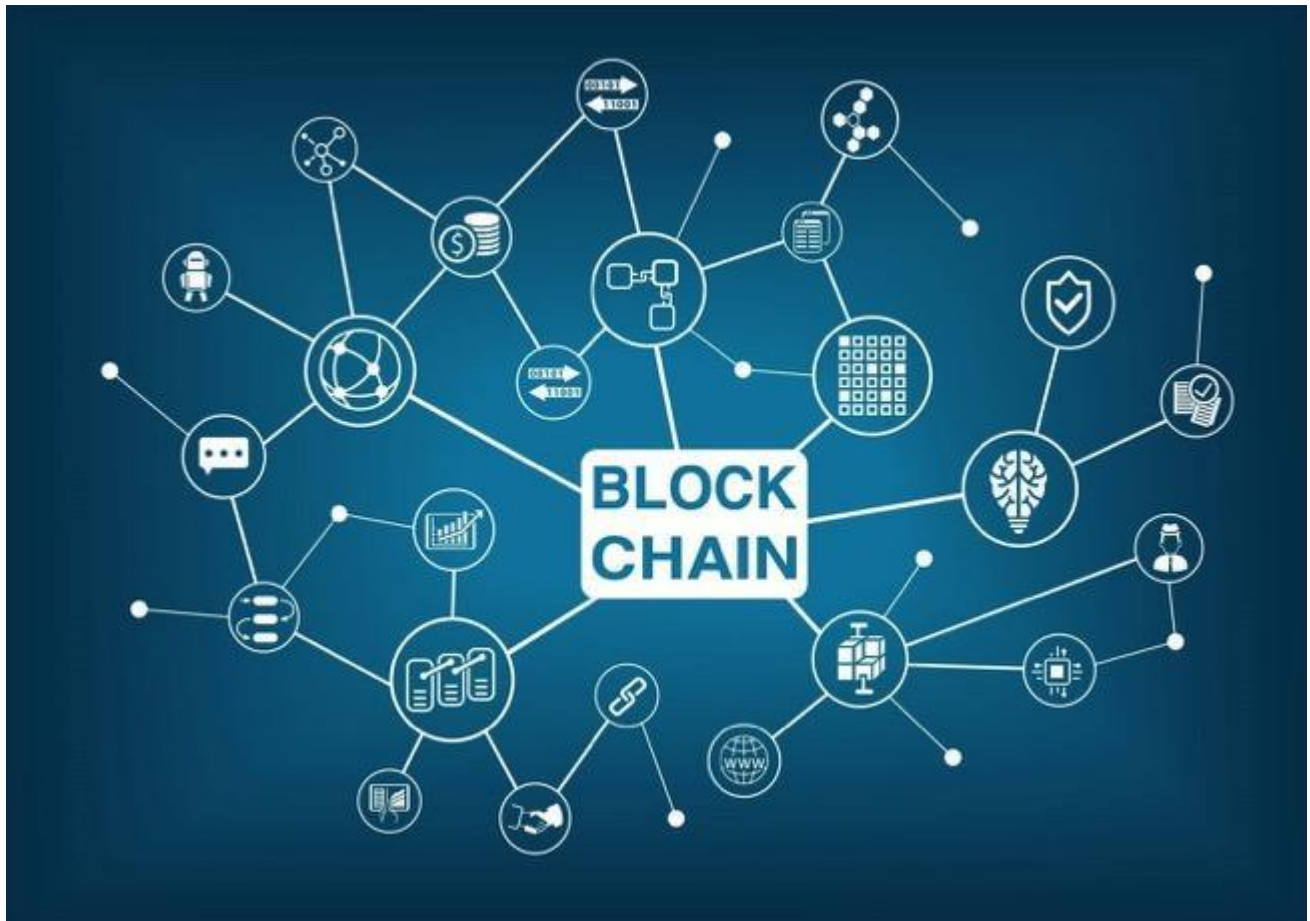
<http://www.pp.u-tokyo.ac.jp/research/wp/index.htm>

このポリシーリサーチ・ペーパーシリーズは、内部での討論に資するための未定稿の段階にある

論文草稿である。著者の承諾なしに引用・配布することは差し控えられたい。

東京大学 公共政策大学院 代表 TEL 03-5841-1349

ブロックチェーン技術のテクノロジーアセスメント



グレッグ海
嶋吉慧
白石桃子
三重野航
宮本寛之

東京大学公共政策大学院 経済政策コース修士1年
東京大学教養学部学際科学科科学技術論コース学部4年
東京大学公共政策大学院 経済政策コース修士1年
東京大学公共政策大学院 経済政策コース修士1年
東京大学大学院 工学系研究科システム創成学専攻修士1年

目次

1. はじめに	- p2 ~ p3
1.1. 背景と問題意識及び TA の目的	
1.2. 想定クライアント	
1.3. 報告書の構成	
1.4. 基本用語	
2. ブロックチェーン技術について	
2.1. 本章の目的	- p4
2.2. ブロックチェーン技術の概観	- p4
2.3. 要素技術	- p5 ~ p12
2.3.1. P2P ネットワーク＝台帳分散化技術	
2.3.2. 狭義ブロックチェーン技術	
2.3.3. コンセンサスアルゴリズム	
2.3.4. 公開鍵暗号方式	
2.4. インフラとしての新概念	- p13 ~ p15
2.4.1. 管理形態	
2.4.2. トークン・マイニング	
2.4.3. スマートプロパティ	
2.4.4. スマートコントラクト	
2.5. 技術・原理から導かれる特徴	- p16 ~ p17
3. 活用事例の紹介と未来予測	
3.1. 分析の共通フロー	- p18
3.2. カネ分野	
3.2.1. 仮想通貨	- p18 ~ p21
3.2.2. 中央銀行発行デジタル通貨	- p21 ~ p22
3.2.3. 資金調達	- p23 ~ p24
3.2.4. 徴税	- p25
3.3. モノ分野	
3.3.1. サプライチェーンマネジメント	- p26 ~ p27
3.3.2. 信用情報の管理（スマートプロパティ）	- p27 ~ p28
3.3.3. 広告の運営管理	- p28 ~ p29
3.3.4. 所有権管理・知財管理	- p30
3.4. ヒト分野	
3.4.1. デジタル ID	- p31 ~ p32
3.4.2. 投票	- p32 ~ p33
4. 総論	- p34 ~ p36
5. おわりに	- p37

謝辞

付録

参考文献

1. はじめに

1.1 背景と問題意識及びTAの目的

ブロックチェーン、仮想通貨、ビットコイン…これらの言葉は日々、新聞紙面やニュースを賑わす。ブロックチェーンという言葉を知っていても、ブロックチェーンが世の中に与える影響やそのポテンシャルを十分に理解している人は多くはないのではないだろうか。

ブロックチェーンとは、ビットコインや仮想通貨技術を支える「分散型台帳技術」である。「分散型台帳技術」の定義する範囲は第2章で論じるが、一言でいうならば、従来、政府や企業のような一組織が情報の管理を行っていたところを、皆で情報を共有し管理することである。遡ってみれば、Satoshi Nakamoto を名乗る人物による論文でビットコインの構想が初めて登場したのが2008年、ビットコインが現実に運用開始されたのが2009年のことである。Nakamoto 論文から10年足らずの間に、仮想通貨の種類は1000種類以上、時価総額は990億ドルを超える（2017年8月2日現在¹）ほどの拡がりを見せている。また、世界経済フォーラム（ダボス会議）が2016年8月に発表した「世界に大きな影響を及ぼす可能性が高い10大新興技術²」にもブロックチェーン技術が選ばれるなど、ブロックチェーン技術への注目度は高まり続けている。

一方で、仮想通貨利用の可能性に関心が集まり、スマートコントラクトなど仮想通貨以外の目的でのブロックチェーン技術の活用や、中央集権的な情報管理システムからの脱却という、ブロックチェーン技術がもたらしうる、より破壊的な変化が生じているにもかかわらず、それに対して理解がされていない。このことへの危機感こそが、本レポート執筆の動機である。ブロックチェーン技術という発展途上の未熟な技術に対して、現状の利用局面の紹介にとどまらず、ボトルネックや今後の展開可能性、普及による社会的インパクトなどの未来視点での影響を、できる限り多角的・体系的に分析した。本レポートを読んだ読者の方々が、ブロックチェーン技術について本質的な理解を深め、不確実な未来に備えるための一助として本レポートが活用されることを願ってやまない。

1.2 想定クライアント

本レポートの主なクライアントとしては、大学生を想定した。クライアント選定理由として、ブロックチェーン自体が市民の中から生まれた技術であり、組織の存在自体を否定しかねない非中央集権的な技術特性を考慮すると、政府、国家の主導によらず草の根的に一般市民の間で広がっていくことが予想される。そのため、政策立案者ではなく、技術の使い手である市民に対して働きかけるレポートとした。また、市民の中でもこれからの時代を背負いブロックチェーンの普及する社会から最も強く影響される世代である大学生を読み手として特に想定し、教科書として本レポートが使用されることを期待した。技術への基本的な理解にとどまらず、ブロックチェーンが活用される理想の社会像やその負の側面についても本レポートの内容に留まらない発展的な議論を期待したい。

尚、大学一般教養レベルの教科書として利用できるように、できる限り難解な説明を避け、図表を用いて視覚的な理解を伴うように工夫を凝らした。

1.3 報告書の構成

第2章において、ブロックチェーン技術の仕組みと特徴について説明する。細かい技術的特性に拘りすぎることなく全体像をとらえ、ブロックチェーン技術のどこに革新性があるのかを意識しながら読んでほしい。第3章ではブロックチェーンの応用可能性を、現時点で実現されていないものも含めて事例として紹介する。特に、ブロックチェーンの活用により、どのような社会的影響があるかに重きを置いて執筆した。第4章では、第3章での各事例の分析を受けて、普及の課題と将来予測の包括的な考察を行った。そして、最終章では読者に向けた提言を行う。

技術の深い理解よりも、実生活に馴染みのある文脈でブロックチェーン技術を理解したい読者には第2章の指示に従いつつ読み飛ばし、第3章に進むことを勧める。

¹ 日本経済新聞 8月2日朝刊 「1000種類 11兆円、ビットコインだけじゃない仮想通貨」

http://www.nikkei.com/article/DGXLASDZ02H6L_S7A800C1000000

² http://www3.weforum.org/docs/GAC16_Top10_Emerging_Technologies_2016_report.pdf

1.4 基本用語

本レポートを読み進めるにあたって、前提となる基本的な用語を以下にまとめた。理解の一助となれば幸いだ。より専門的な用語は2章以降で適宜説明していく。

- ブロックチェーン
本レポートの評価対象となる、分散型台帳技術。その定義については2章で詳しく述べる。
- トランザクション
ブロックチェーンを用いたシステム上で行われる各取引を指す。
- ブロック
ブロックチェーンの構成要素であり、一定時間ごとの全トランザクション情報が入っている。
- ノード
オンラインネットワークに参加している各端末及びユーザーを指す。
- ビットコイン
仮想通貨の一種。ここでいう仮想通貨とは、国家が発行する通貨の信用に基づき各企業が独自に運営しているような通貨ではなく、国家の通貨発行の信用性とは独立して P2P ネットワーク（参加しているノードが対等、特定の管理者が不在なネットワーク。詳細は2章を参照）上で管理運営される通貨を指す。
- スケーラビリティ
利用者の増加、サービスの普及に対するシステムの耐久性、またその普及可能性を指す。
- ゼロダウンタイム
システム・サーバなどが停止（ダウン）せず、常時稼働し続けること。
- コンセンサス
中央集権的な管理者を持たないブロックチェーン上で、全員が情報の共有の合意を行うこと。

2. ブロックチェーン技術について

2.1. 本章の目的

本章では、ブロックチェーンが社会にもたらすインパクトを論じる前に、「ブロックチェーンはどうしてそのようなインパクトをもたらすことができるのか？」という技術の本質に迫る。

「ブロックチェーン=ビットコイン」ではないということには特に注意して欲しい。ビットコインはブロックチェーンを用いるアプリケーションの一つに過ぎない。本レポートでは、ビットコインにとどまらない「ブロックチェーンの様々な応用可能性」を議論するべく、まずはこの第2章で、共通基盤である技術面を整理する。

2.2. ブロックチェーン技術の概観

1章でも触れたように、ブロックチェーンとは、情報や取引記録を、非中央集権的に皆で管理してしまう「分散型台帳技術」である。そのブロックチェーンという仕組み全体を構造化したものが図1である。

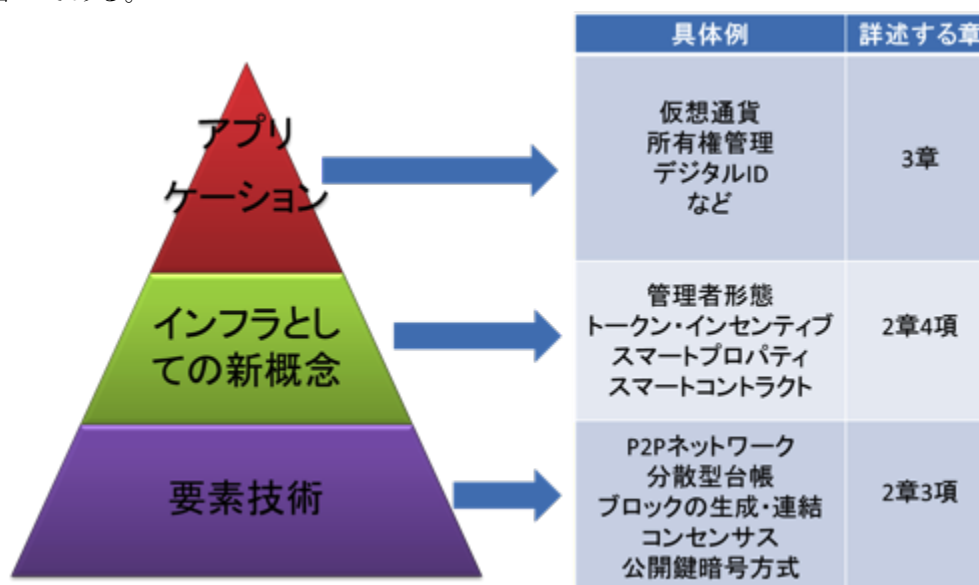


図1. ブロックチェーン技術の構造化

各要素技術によって広義ブロックチェーン(分散型台帳技術)が形成され、実際にインフラとして運営するにあたって既存システムにない新概念が生じ、そしてそれらを応用した各分野へのアプリケーションが実社会で普及している、という構造である。本章ではこのうち、「要素技術」と「新概念」について整理する。「各分野へのアプリケーション(活用事例)」については3章にて詳述する。

このような「ブロックチェーン技術の階層化・構造化」を行う目的として、「ブロックチェーンという基盤技術はそのどこに技術的課題があるのか」を明確にすることが挙げられる。一般に、世間からの認知度が低い段階にある新興技術は、わずかなトラブルがあるだけで信頼性を損ない社会受容性を大きく低下させる傾向にあるが、これはリテラシーの向上によって解決される問題である。例えば、イーサリアム(ブロックチェーンを基盤技術とした仮想通貨)を用いた自律分散組織 DAO³が2016年6月に不正攻撃を受けて崩壊(The DAO Attack)し、ブロックチェーンの信頼性は大きく揺らいだ。しかし、この脆弱性はブロックチェーン技術にあるものではなく、それを利用するにあたってのDAOのプログラミングシステムにあり、ブロックチェーンという基盤技術はそれ以降も問題なく運用されている。こうした事件・課題の本質を見極めるリテラシー向上のために、本章のようなブロックチェーン技術の構造化が必要である。

³ decentralized autonomous organization の略。投資ファンドを非中央集権的に行うプロジェクトのこと。

2.3. 要素技術

本レポートでは、情報の台帳である「ブロックチェーン(以下、狭義ブロックチェーン)」と、分散型ネットワーク「P2P ネットワーク」によって成立する全体のシステムを広義ブロックチェーン(分散型台帳技術：Distributed Ledger Technology)と定義する。以降の章で単にブロックチェーンと言及した場合は広義ブロックチェーンのことを指す。これらの関係は要約すると、

広義ブロックチェーン(分散型台帳技術)

=P2Pネットワーク(分散型)×狭義ブロックチェーン(台帳)

と表現することができる。

狭義ブロックチェーンとは、一定時間ごとに新しいブロック(その時間内の全トランザクション情報を格納したもの)を既存のブロックに連結していく仕組みの情報台帳のことを指す。このブロックの連結は、P2P ネットワークでのコンセンサスによって承認され、最新のブロックチェーンとして P2P ネットワーク上の各ノードに共有される。

また、P2P ネットワーク上の各ノードは、公開鍵暗号方式というセキュリティの下で自由にトランザクション(取引)を行う。

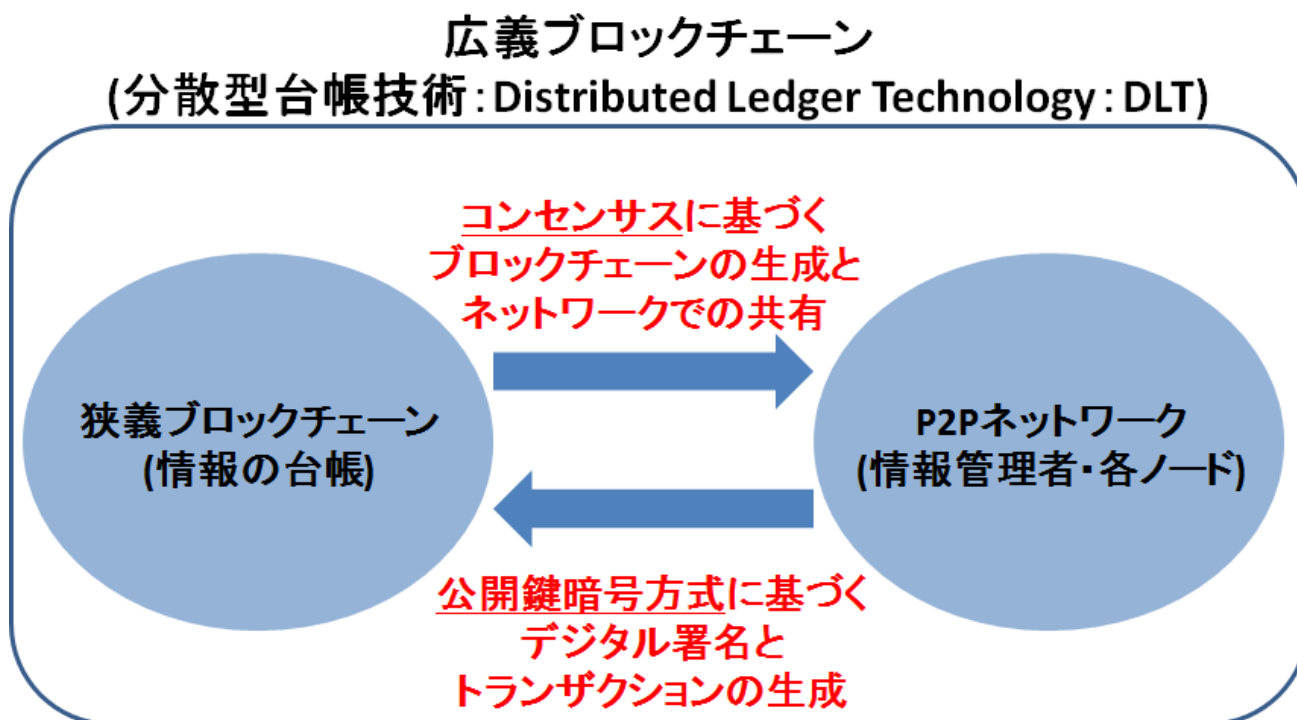


図 2. 広義ブロックチェーンの概要

2.3.1. P2P ネットワーク＝台帳分散化技術

ブロックチェーンにおいて、情報はクライアント/サーバ型システムのように特定の一ヶ所に集積されることはなく、そのシステムに参加する人(ノード)が各自情報を所持・管理する P2P システムによって管理されている(図 3)。

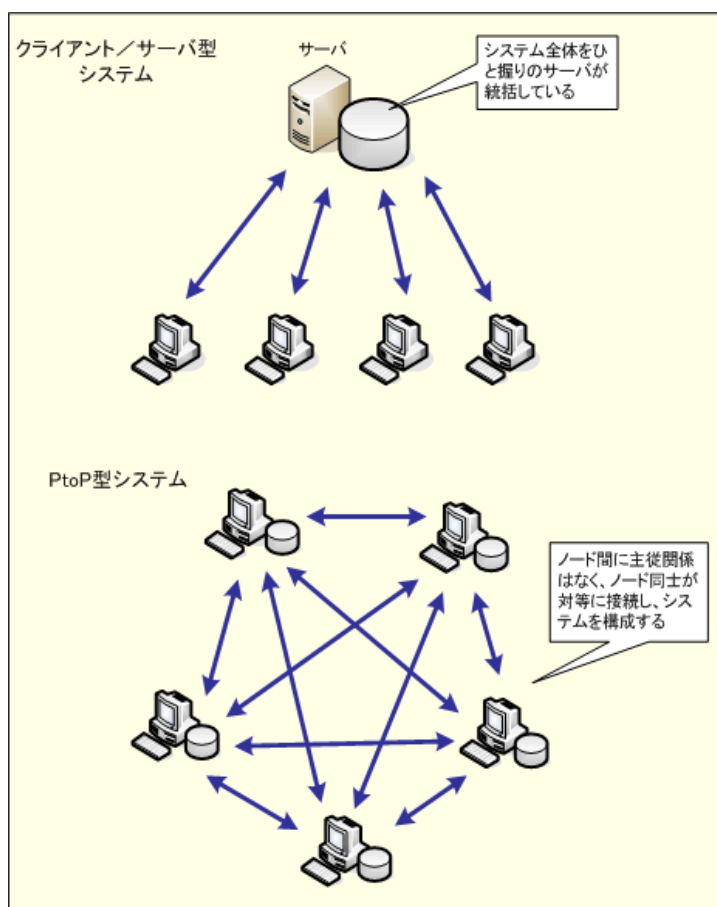


図 3. クライアント/サーバ型システム（上）と PtoP(P2P)型システム（下）の比較[11]

2.3.2. 狭義ブロックチェーン技術

2.3.1 の P2P システムによって各ノードは情報を管理している。その管理形態が「分散型台帳」である。これは、「各ノードが自身の取引情報のみを管理する」台帳ではなく、「各ノードがネットワーク全体の取引情報を共有・管理する」システムである。そして、その「ネットワーク全体の取引情報」の管理のされ方が、「過去のブロックに現在のブロックを連結(更新ではないことに注意)していく仕組み」が、狭義ブロックチェーンである。したがって、ブロックチェーンは「時系列で枝分かれしない」という性質をもつ(図 4 参照)。

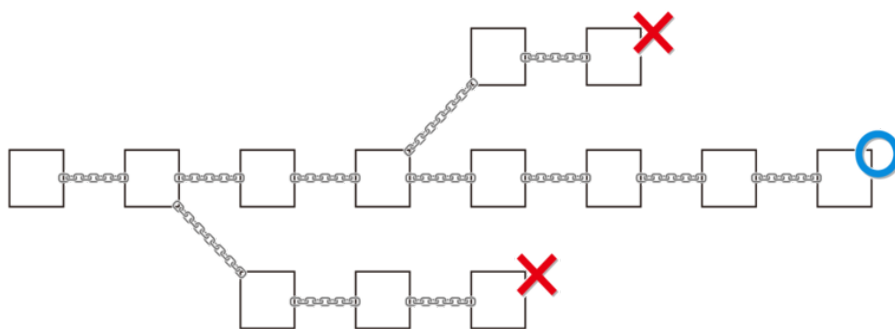


図 4.

これより先、第2章では、

- ・ブロックの生成・ブロックチェーンへの連結までのフロー
- ・コンセンサスアルゴリズム (p10 2.3.3.)
- ・公開鍵暗号方式 (p12 2.3.4.)
- ・インフラとしての新概念 (p13 2.4.)
 - 管理形態
 - トークン・マイニング
 - スマートプロパティ
 - スマートコントラクト
- ・技術・原理から導かれる特徴 (p16 2.5.)

について述べるが、やや細かい技術的説明となるため、
技術の深い理解よりも身近な生活でのブロックチェーンの活用について理解したい者は、

p13 「2.4.1 管理形態」

→ **p16 「2.5 技術・原理から導かれる特徴」**

→ **p18 第3章**

と読むことを勧める。

ブロックの生成・ブロックチェーンへの連結までのフローは以下の(1)~(6)、図5、図6のようになっている。

- (1) 各ノードがトランザクションを行う。取引元が取引内容を指定(インプット)し、取引先(複数可)が指定取引内容(アウトプット)を受信する。
- (2) 同一時間帯内に行われた全ノードの全トランザクションを、一つのブロックに格納する。
- (3) ブロックには、トランザクション情報だけでなく、ブロックヘッダというブロック識別子が格納されている。
- (4) ブロックヘッダを入力値として、ハッシュ関数という処理によってハッシュ値が生成される(図6)。このハッシュ値が、ブロックチェーンが要求する閾値内に収まったとき(=ハッシュ計算をクリアしたとき)、そのブロックは正しいブロックとして認証され、既存のブロックチェーンに最新のブロックとして連結される。
- (5) ハッシュ処理において、インプットとして操作可能なのはブロックヘッダのうち **Nonce** と呼ばれる入力値のみである。それ以外は、既存のブロックチェーンや格納するトランザクションの情報によって一意に定まる既定値である。
- (6) **Nonce** の入力値を入れ替える繰り返し操作でハッシュ処理のクリアを目指すことになる。この作業は任意の計算機で可能な簡易な作業であるため、ブロックチェーンのネットワークへの参加の敷居を低くすることができている。一方で、ハッシュ処理(ハッシュ計算の繰り返し)は膨大な計算負荷がかかることになる。すなわち狭義ブロックチェーン技術においては、「参入障壁を低くする(=ハッシュ処理を単純化する)」ことと「管理者またはハッシュ処理を行うノードの負担を少なくする(=ハッシュ計算量を少なくする)」ことがトレードオフの関係になっている。

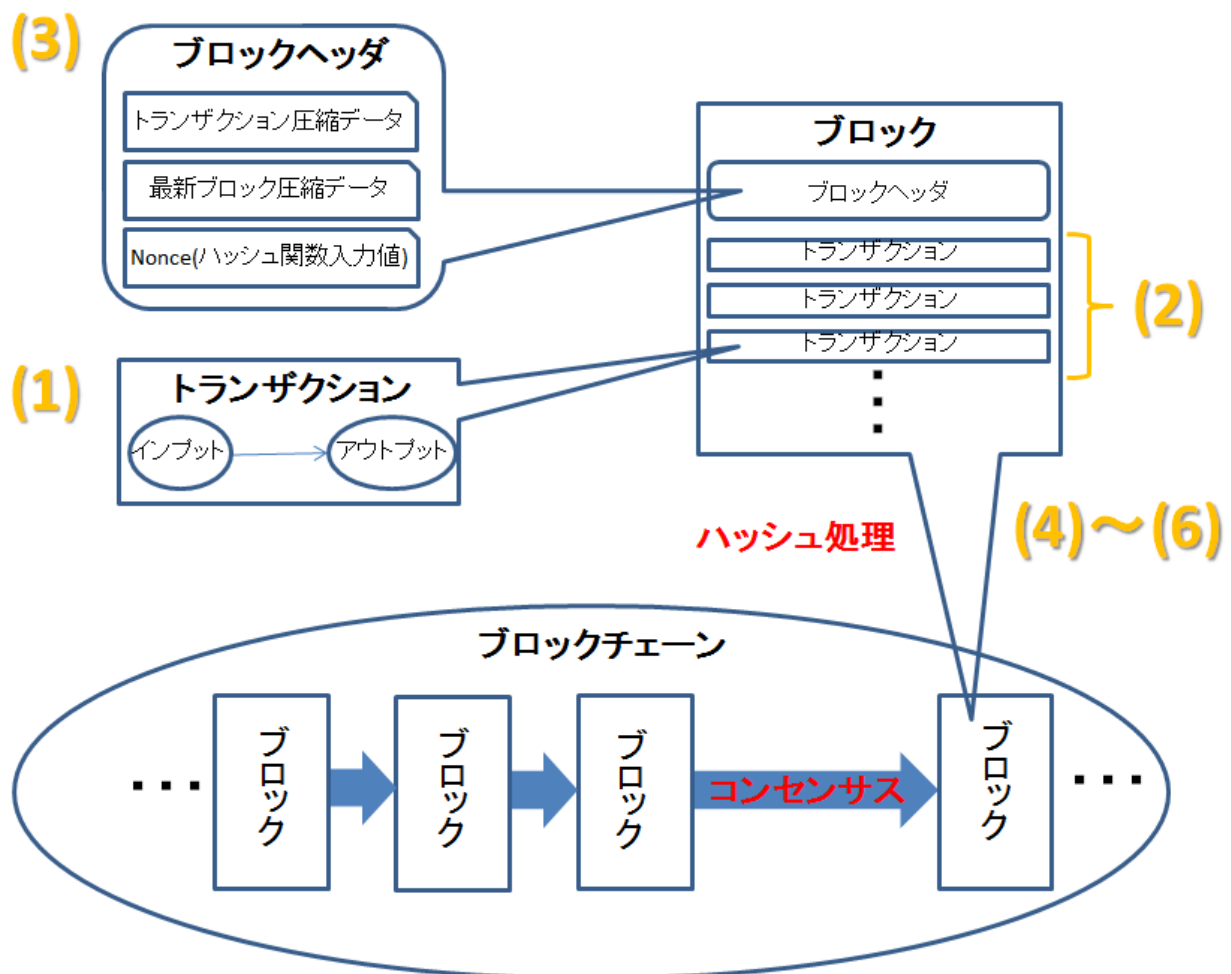


図 5. 狭義ブロックチェーン技術の原理([8][9]等を元に作成)

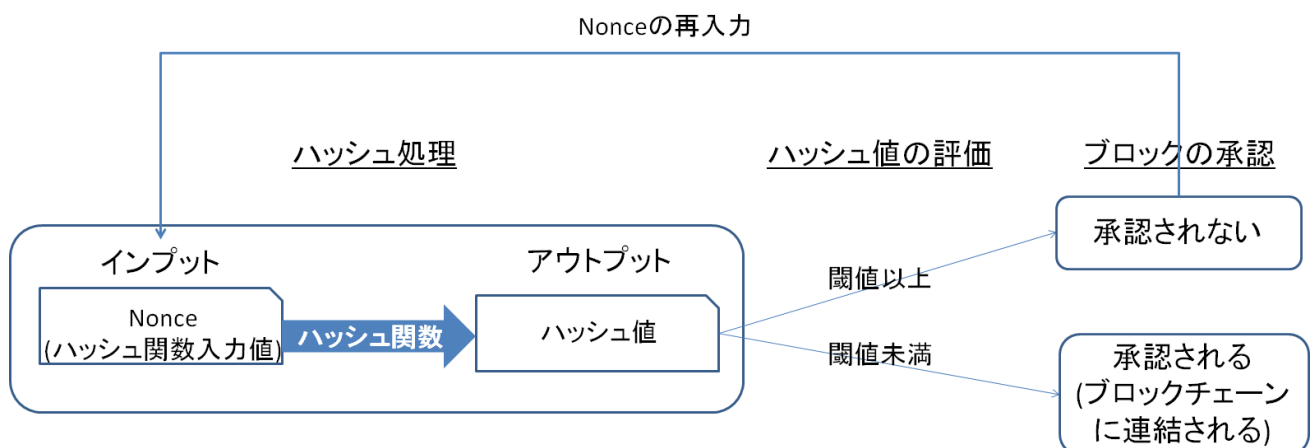


図 6. ハッシュ処理～ブロック生成までのフロー((4)~(6))の概念図

また、ブロックチェーンを具体的なものとしてイメージしやすくなるように、ブロックチェーンの実際の容量に関して述べる。ビットコインを例に挙げると、ビットコインはスパムや DoS 攻撃に備えて、1 ブロック当たりの容量限度を初期の 36MB から 1MB に制限している。その容量制限に対し、実際に取引情報を格納したブロックサイズ(1 日当たりの平均)は図 7 の

ように増加しており、各日ごとの最大ブロックサイズは、図 8 のようにすでに 1MB に達しているのが現状である。

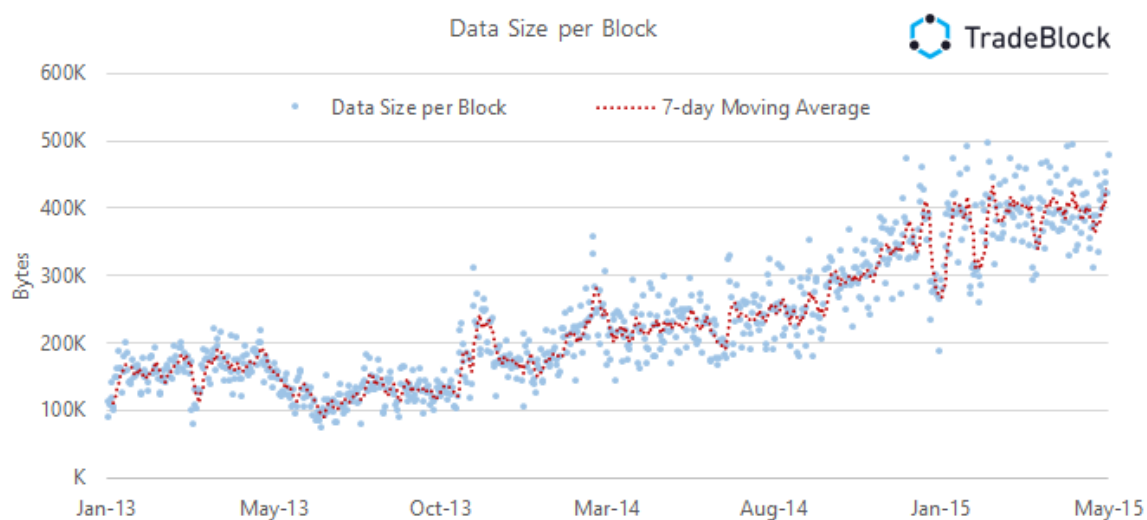


図 7. ビットコインにおけるブロックサイズ(一日当たり平均)の推移(2015)[12]

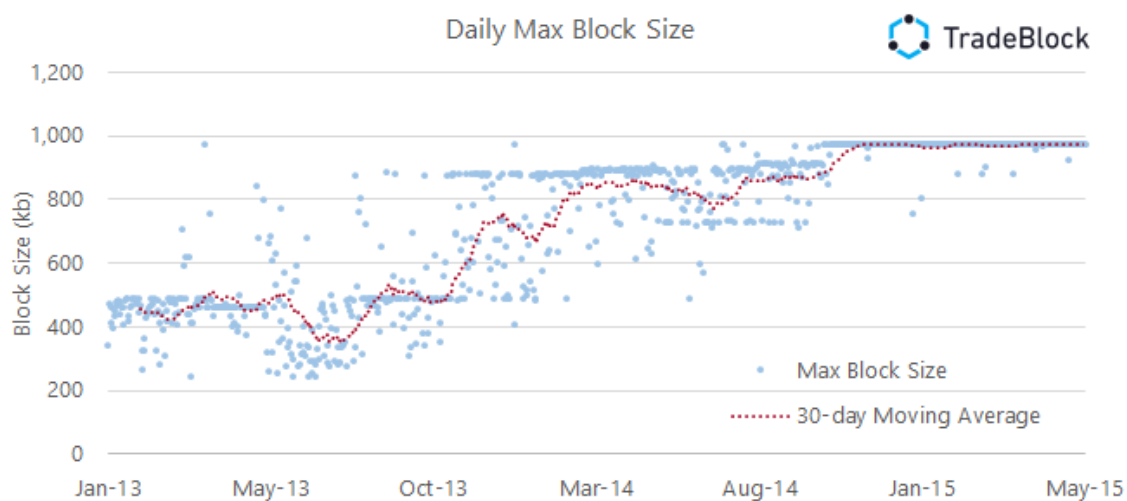


図 8. ビットコインの各日の最大ブロックサイズの推移(2015)[12]

2.3.3. コンセンサスアルゴリズム

2.3.1、2.3.2 の要素を踏まえると、広義ブロックチェーンを成立させるにあたって重要なポイントは、

- 狭義ブロックチェーンに連結する最新のブロックを、
- 複数の情報管理者(ノード)がいる状況で、どのように改ざん・不正の余地なく承認・共有するか？

である。この課題についての解決策として、コンセンサス、すなわち合意形成手法が現在採用されている。コンセンサスといっても、各ノードに「取引情報を集めたこのブロックが、正しいブロックということによろしいですね!？」と直接お伺いを立て、**各ノードの意思決定を求めるわけではない**。ここでのコンセンサスというのは「**ネットワーク上で自動的に最新ブロックの承認・拒否を決めるためのアルゴリズム**」である。以下に実際に活用・検討されているコンセンサスアルゴリズムを挙げる。

(1) Proof of Work (以下 PoW)

最新ブロックを生成しブロックチェーンに連結する権限を、「ハッシュ計算を一番早く処理したノード」に与えるコンセンサスアルゴリズム。ビットコインなどにおいて用いられている。

(2) Proof of Stake(以下 PoS)

最新ブロックを生成しブロックチェーンに連結する権限を、「ブロックチェーンで管理している資産が一番多いノード」に与えるコンセンサスアルゴリズム。「大量の資産を所有する参加者は、その価値を守るために、システムの信頼性を損なうことはしない」という推定概念に基づく[7]。

(3) Practical Byzantine Fault Tolerance(以下 PBFT)

最新ブロックを生成しブロックチェーンに連結する権限は管理者に与えつつ、トランザクションが改ざんされていないかどうかの承認を他のノード(Non-validating peer)に転送・確認する。「改ざんされていない」という承認が多数を占めている場合に、トランザクションの処理を実行する(図 9)。PoW との違いの一つは、特定の管理者が存在し合意形成を行う点である。従って、管理主体が存在するプライベート型・コンソーシアム型ブロックチェーン(2.4.1 で詳述)への活用が期待されている。また、PoW は計算処理にコストがかかったが、PBFT ではそのような難しい計算をするわけではないので、比較的高速な処理が可能となる。加えて、処理における確実性(ファイナリティ)が高い。PoW を使った取引では、通常 6 個の後続ブロックが生成されたことをもって処理が確定するため、この間、トランザクションが覆される可能性がある。しかし、PBFT では、コンセンサスが取れば、即時、処理が完了する。以上のことをふまえ、即時性のある決済、ならびに信用ある管理組織によるチェーン管理という点から、特に金融業務における活用が期待される。

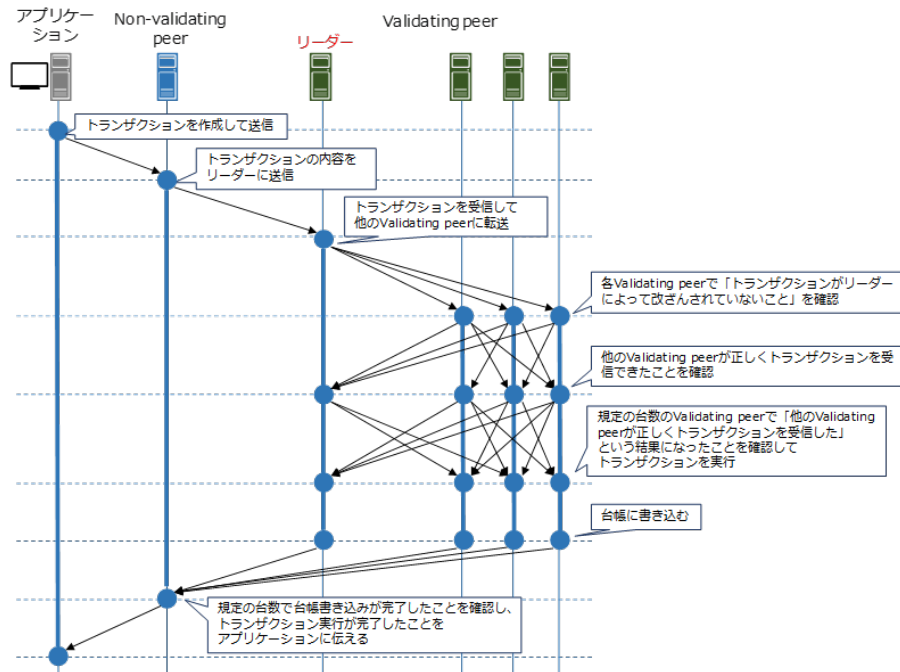


図 9. PBFT の仕組み[10]

(アプリケーション：トランザクション実行リクエストを生成する PC

Non-validating peer(非検証ノード)：トランザクションを実行するリクエストを受け付ける PC

Validating peer(検証ノード)：トランザクションを検証する PC)

(4) その他のアルゴリズム

(1)~(3)が、現在ブロックチェーンにおいて広く採用・実証されているコンセンサスアルゴリズムであるが、これらの他にも、ブロックチェーン内の資産量と取引量などを総合的に勘案する **Proof of Importance(PoI)**なども実用されている。それ以外にも、原理的には「全ノードから完全ランダムで最新ブロック生成者を選ぶ」「各ノードに順番に最新ブロックを生成してもらう」といったシンプルなコンセンサスアルゴリズムも考えられる。

現状では、これらのコンセンサスはアプリケーション次第で一長一短があり、圧倒的に優れているといったものはないが、ブロックチェーンが社会に浸透するにあたっては、このコンセンサスアルゴリズムにイノベーションが起こることがターニングポイントの一つである。

2.3.4. 公開鍵暗号方式

2.3.2 で述べたように、各ノードは他者のノードの取引情報を含めた全情報を、ブロックチェーンという分散型台帳として所持・管理している。しかしこのままでは、「他者に自分の取引情報・内容が完全に公開されてしまう」ことになる。そこで、取引情報の秘匿性を担保するために、ブロックチェーンでは公開鍵暗号方式というセキュリティが採用されている。以下に公開鍵暗号方式の概要を述べる。

通常のセキュリティシステムにおいては、ユーザーは一つの鍵、すなわち共通鍵暗号方式を用いる。例えば、オンラインショップで商品を購入するときも、ユーザーは自らのアカウントにログインする際にパスワード 1 つで認証する。これが共通鍵である。これは家のドアの施錠・開錠に同一の鍵を用いることに相当する。

これに対し公開鍵暗号方式では、ユーザーは「公開鍵・秘密鍵」の二つの鍵を所有する。それぞれの性質は以下のようになっている。

- 公開鍵
 - 情報を暗号化する際に用いられる鍵。ドアの施錠に相当する。
 - 公開鍵は他のノードに公開されている。すなわち、他のノードは「誰が情報を暗号化したのか」を把握することができる。
- 秘密鍵
 - 情報を復号化する際に用いられる鍵。ドアの開錠に相当する。
 - 秘密鍵は他のノードに公開されない。すなわち、あるノードが特定のノードに向けて送信した「暗号化された取引情報」は、その特定のノードしか復号化することができない。

各ノードはこれら二つの鍵を「ウォレット」と呼ばれる管理ソフトウェアに保管し、取引の際に使用する。図 10 に鍵を使用するフローを示す。送信者は「受信者の公開鍵」を用いてトランザクション要求を暗号化し、部外者から秘匿する。正しい受信者のみが、自身の秘密鍵によってトランザクション要求を復号化することができるのである。

公開鍵暗号方式のイメージ

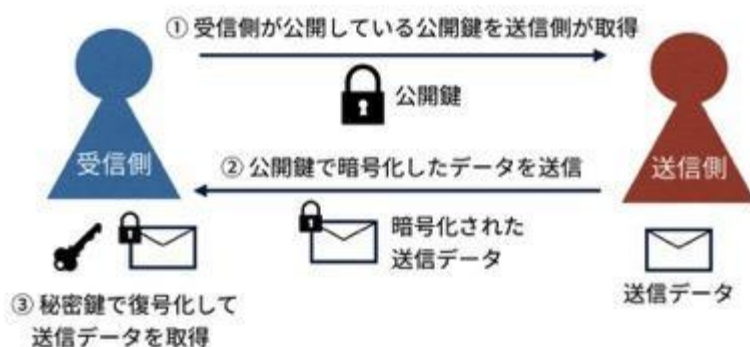


図 10. 公開鍵暗号方式の概念図[2]

2.4. インフラとしての新概念

2.3 ではブロックチェーンを「形成」するために不可欠な要素技術について述べた。本項では、ブロックチェーンを情報・資産管理インフラとして「運用」する際に生じる、既存システムにはない新たな概念について詳述する。

2.4.1. 管理形態

ブロックチェーン技術は各ノードがそれぞれ同一のブロックチェーンを所持する「分散型台帳」として形成されることを 2.3 で述べた。2.5 で後述するが、これは情報の一極集中を防ぎ、より頑丈な管理を可能にする、という従来にはない性質をもつ。したがって原理的には、情報を保持する各ノードは対等である。一方で、ブロックチェーンの普及において、「普及させようとするリーダー(組織・会社・個人など形態は様々だが)」が必要であることも事実である。したがって、少なくともブロックチェーン導入初期においては、ノード間に「管理者」と「参加者」という関係の不均衡が生じざるをえない。このようなジレンマを乗り越えてブロックチェーンを利用するために、以下のような複数のブロックチェーン管理形態が提唱されている。

(1) パブリック型

パブリック型は管理者不在・自由参加のブロックチェーンであり、最も「原理主義的」な形態である。不特定多数のマイナーが管理者不在のネットワークを構成するため、悪意のある参加者を排除する仕組みが存在しない。改ざん等の悪用を妨害するための厳密なコンセンサスアルゴリズムが必要となる。

また、任意のノードが参加可能であるため、ブロックチェーンの規模は大きくなる。そのため、参加者間の取引記録の相互確認などに多く時間を有し、トランザクションの処理速度が他の形態と比べても遅い。

パブリック型の代表的なユースケースとして、ビットコインが挙げられる。

(2) プライベート型

管理主体として個別組織が存在し、参加者を選別することを特徴としているのがプライベート型ブロックチェーンである。規模は小さく、範囲は信頼できる参加者に限定しているため、悪意のあるマイナーが混在するリスクを削ぐことができる。また、PoW などのコンセンサスアルゴリズムに厳密性を求める必要もなくなり、合意に至るまでの処理速度はパブリック型と比べ早い。さらに、ブロックチェーン内で情報が共有されるため、秘匿性を確保できる。

しかし、組織が組織のためだけに運営するブロックチェーンという側面も否定できず、独占を回避するシステムを整備する必要がある。また、ネットワークの分散度が低いため、トランザクションが集中するサーバーがダウンした場合に、全体が停止しやすい脆弱性も課題の一つである。

(3) コンソーシアム型

プライベート型ブロックチェーンの規模及び運営する管理主体を拡張した形態がコンソーシアム型ブロックチェーンである。プライベート型から派生しているため、メリット及びデメリットも類似している。ユースケースとしては、企業や組織間の取引を管理する場合に用いられる。

以上の形態ごとの違いをまとめた図が図 11 である。ここで重要なのは、ブロックチェーンは原理的には管理者不在の(1)パブリック型が本来想定されていた姿だが、これが採用されているのは仮想通貨など一部の分野のみで、その他の分野では既存の組織形態に適した導入として、(2)プライベート型、(3)コンソーシアム型といった管理者を設置した形態が採用されていることである。

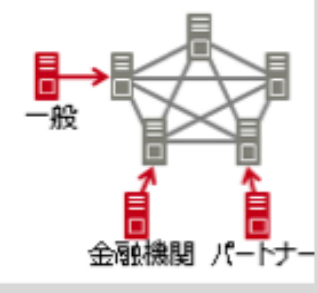
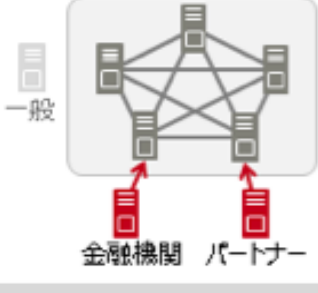
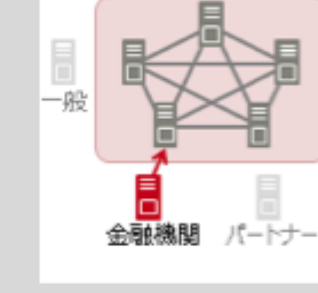
	パブリック	コンソーシアム	プライベート
			
管理者の有無	なし	あり (複数組織内に限定)	あり (1 組織内に限定)
BCN 参加者	不特定多数 (制限なし Permission less)	特定多数 (管理者による許可制 Permission)	特定多数 (管理者による許可制 Permission)
合意形成	厳格な承認が必要 (PoW, PoS など)	厳格な承認は任意	厳格な承認は任意
取引速度	低速	高速	高速
マイニング参加権	制限なし	制限可能	制限可能
マイニング報酬	必要	任意	任意

図 11. ブロックチェーンの管理形態[15]

技術理解よりも、まずは実生活でのブロックチェーンの活用について理解したい者は、
p16「2.5 技術・原理から導かれる特徴」へ読み進めて欲しい。

2.4.2. トークン・マイニング

2.2 で述べたように、ブロックチェーン技術は複数の階層によって構成されるシステムであり、その階層は図 1 以外にも例えば図 12 のように表現することもできる。この階層表現で重要なのは、「新たなブロック生成・連結についてノードにインセンティブを与えるためのトークン」である。管理者不在のオープンな形態であるパブリック型ブロックチェーンでは、わざわざ負荷の大きいハッシュ処理を実行し、コンセンサスを得るまでして新たなブロックを生成・連結するだけのモチベーションがノードにはない。そこで、新たなブロックを生成・連結した際に報酬としてトークンを与えることでインセンティブとするのである。パブリック型ブロックチェーンの代表例であるビットコインでは、トークンとしてビットコインを与えている。ここで与えられるビットコインは、すでにブロックチェーン上で流通・取引されているものとは別の、全く新規に発行されるコインであることから、この作業を採掘(mining)になぞらえて「マイニング」と呼ぶ。マイニングを行うノードのことをマイナー(miner)と呼ぶ。なお、インセンティブのない状態で、ほぼボランティア状態でブロックチェーンの検証を行うノードをフルノードという。

ここで留意してほしいのは、マイニングはビットコインなどのパブリック型ブロックチェーンではインセンティブとして重要な概念であるが、プライベート型やコンソーシアム型のように管理者がブロック生成・連結の権限を持つブロックチェーンでは必ずしも必要ではないという点である。

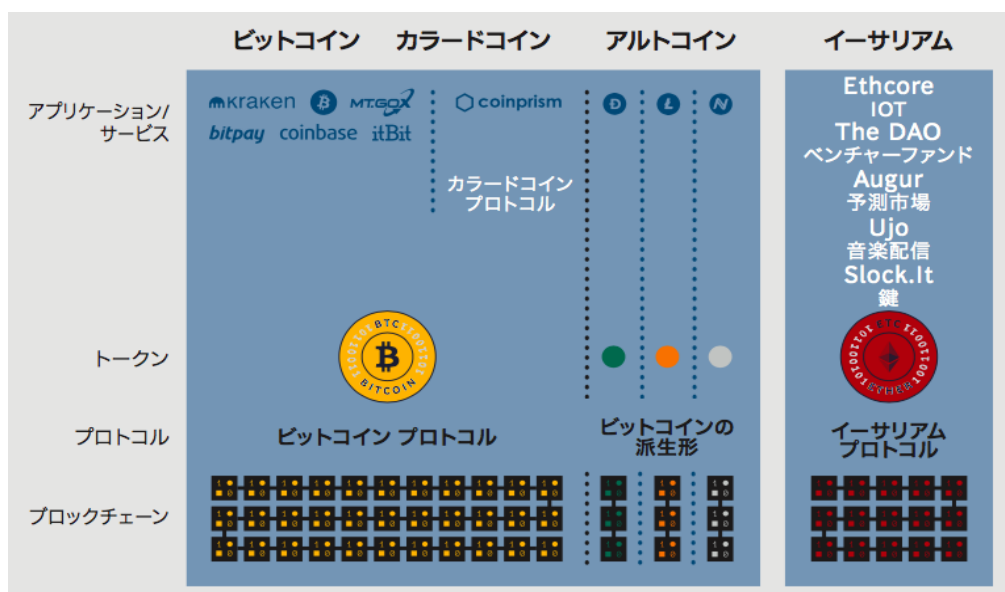


図 12. ブロックチェーンの階層構造の別表現[5]

2.4.3. スマートプロパティ

ブロックチェーンの活用事例として現在最も普及が進み話題となっているのが、ビットコインに代表される「仮想通貨」としての基盤である。しかし、仮想通貨のような貨幣形態の資産に限らず、デジタル化が可能な資産は全てブロックチェーン上で管理(所有権の取引・手続き・登録など)を行うことができる[4]。資産全般のこのような管理形態をスマートプロパティと呼ぶ。ブロックチェーンで管理できる可能性がある対象の例を表 1 に挙げる。

表 1. ブロックチェーンで管理できる可能性がある対象の例[4]

資産の種類	例
一般	エスクロー取引、担保付取引、第三者裁定、複数者取引
金融取引	株、未公開株、クラウドファンディング、債券、投資信託、デリバティブ、年金保険、年金
公的情報	不動産登記、自動車登録、事業者登録、結婚証明、死亡証明
ID	運転免許、ID カード、パスポート、有権者登録
民間	借用証書、ローン、契約、賭け、署名、遺言、信託、エスクロー
各種証明	保険証名、所有証明、公証
有形資産の鍵	家、ホテルの部屋、レンタカー、自動車利用
無形資産	特許、商標、著作権、予約、ドメイン名

2.4.4. スマートコントラクト

ブロックチェーンは、当初はあくまで「情報」を載せ管理する台帳であった。しかしイーサリアムなどで実用化されるに伴って、「情報管理だけでなく情報処理をも実行できる台帳」として発展するに至っている[4]。この「処理も含めた情報の管理形態」のことをスマートコントラクトと呼ぶ。ここでいう情報処理とは、「資産等の取引・契約；利用者登録・所有権変更・契約の実行・契約の履行状況の監視など」のことを指す。

スマートコントラクトの重要なポイントは、契約成立において、その信頼性をコンピュータプログラムが担保し実行されることにある[6]。このことによって、従来契約に必要な第三者の仲介や、身元確認などの諸々の処理が簡略化されることになる。その結果、取引コストの高さがネックで生じ得なかった取引(例えばマイクロペイメント)が新たに行えることになる。

2.5. 技術・原理から導かれる特徴

本項では、2.3~2.4 で述べたブロックチェーンの仕組みを踏まえて、これらの仕組みから生じる、既存技術にはないメリットを 2 点、普及における技術的課題を 4 点まとめた。

【既存技術にはないメリット】

(1) 取引情報の改ざん・ハッキングが困難

ブロックチェーンを用いた取引情報管理は、従来のサーバクライアント型の一極集中情報管理に比べて、以下のような複数の要素によって改ざんを二重三重に困難なものとしている。

- 各ノードがそれぞれブロックチェーンを管理するという分散性により、改ざんするには全ノードの情報を改ざんする必要がある、コストが莫大
- 取引情報はブロックチェーンとして過去～未来全ての情報と連結しているため、改ざんするにはそれら全てとの整合性を保たねばならず、コストが莫大
- コンセンサスアルゴリズムによって正しい取引情報を取捨選択する確実性が向上している
- ハッシュ計算の負荷が大きい

(2) 情報資産と所持者の関係を自動的に紐付けできる

管理者・仲介者による信頼保証に基づく現在の資産取引とは異なり、ブロックチェーンでスマートコントラクトによって、資産とその所持者・所持資格を第三者の仲介なく紐付けることができる。これによって仲介手数料などを大幅にカットできると同時に、取引のための前処理(身元確認など)、後処理(契約成立後の履行の監視など)を省くことができる、というメリットが得られる。

【普及における技術的課題】

(3) ゼロダウンタイム

既存の一極集中サーバ型のインターネットシステムでは、アクセスの集中によりサーバが落ちたり、サーバのメンテナンスのためにシステムを利用できなくなるタイミングがある。ゼロダウンタイムとは、P2P ネットワークを利用することによって、情報管理場所が分散化され、常にシステムが稼働することをいう。この性質によって、取引時間の制限がなくなる。

(4) 取引情報の秘匿性の担保

ブロックチェーンは改ざん困難であるが、取引の秘匿性という観点では、パブリック型ブロックチェーンはセキュリティに課題があると考えられる。なぜなら、取引情報はブロックチェーンとして各ノードで共有されるからである。ただしここで留意してほしいのは、秘匿性に課題があるというのは、「取引情報の内容が公開されてしまう」という意味ではなく、「あるノードが別のノードと取引したという事実が公開されてしまう」という意味である。もちろん、公開鍵・秘密鍵の漏えい・流出によって取引情報の内容までもが流出してしまうリスクはあるが、これは既存のインターネットシステムでパスワードが流出することによるリスクと同じであるため、ブロックチェーンに固有の課題ではない。

なお、コンソーシアム型、プライベート型のブロックチェーンでは、管理者が取引情報の公開・非公開を管理できるため、上記の課題は解決されていると言える。

(5) トランザクションの拡張性・スケーラビリティ

2.3.2 においてブロックチェーンの容量限度について部分的に述べたが、ブロックチェーン技術は、トランザクション処理に限度があるという拡張性の面で大きな課題を残している。例えば、2017 年 5 月時点でのビットコインの仕様では、処理可能な最大取引量は 7tps(取引/秒)であり、クレジットカード VISA の平均約 2,500tps、ピーク時約 4,000tps に比べて圧倒的に少なく、決済サービス paypal の平均約 100tps と比べても非常に少ない値

となっている[13]。この最大取引量をオーバーしてしまうと、取引の確認が遅れてしまうといったリスクをはらんでおり、ビットコインコミュニティ内でも意見が分かれている。その結果、2017 年 8 月には、ブロックの最大容量を巡って仮想通貨ビットコイン(BTC)が分裂し、ビットコインキャッシュ(BCC)が新たに運用を開始するに至った[14]。このように、トランザクションの拡張性への対応はブロックチェーン普及にあたっての重要なポイントである。ただし留意してほしいのは、この取引量の限度は基盤技術の限界によるものではなく、「マイナーやフルノードの負担増加、集中化[13]」を懸念した容量制限だという点である。

また、トランザクション認証に時間がかかるので、大規模に普及すると取引が不可能になるという課題がある。

(6) 異常時の処理

ブロックチェーンは、管理者不在の非中央集権的なシステムである。そのため、情報の管理は自律的に行われるが、「万が一システムがダウンした際には誰が責任(法的責任を含む)をとるのか？」という責任所在の問題が生じている。この問題について、国際標準化機構(ISO)やその他各国の検討委員会が制度整備を進めているが、責任問題への明確な答えは存在していないのが現状である。

3. 活用事例の紹介と未来予測

3.1 分析の共通フロー

本章では、ブロックチェーン技術の応用可能性を、各用途について分析する。ブロックチェーン技術の用途に応じて個別具体的に分析する理由は、ブロックチェーン技術は活用分野によって社会的影響が変わってくるからだ。⁴分析にあたっては、まず大きく、カネ・モノ・ヒト分野に分ける。カネ分野は貨幣、モノ分野は商品、ヒト分野は個人情報、にそれぞれ関連した情報をブロックチェーンによって管理する。さらに、各分野での個別の事例について、以下の項目（以下図参照）の分析を行った。各事例に対して以下の各観点から評価した。

【活用事例】

【ブロックチェーンの固有性】

【社会的影響】

【普及前の障壁】

【普及後のリスク】

【未来予測・提言】

【ブロックチェーンの固有性】では、既存システムをブロックチェーンで代替することの利点、もしくは新システムをブロックチェーンで構築することの利点を意識した。【社会的影響】は短期的な視点から現状分析も含めて考察するが、【未来予測】ではより長期的な視点に立って将来の社会像を描く。

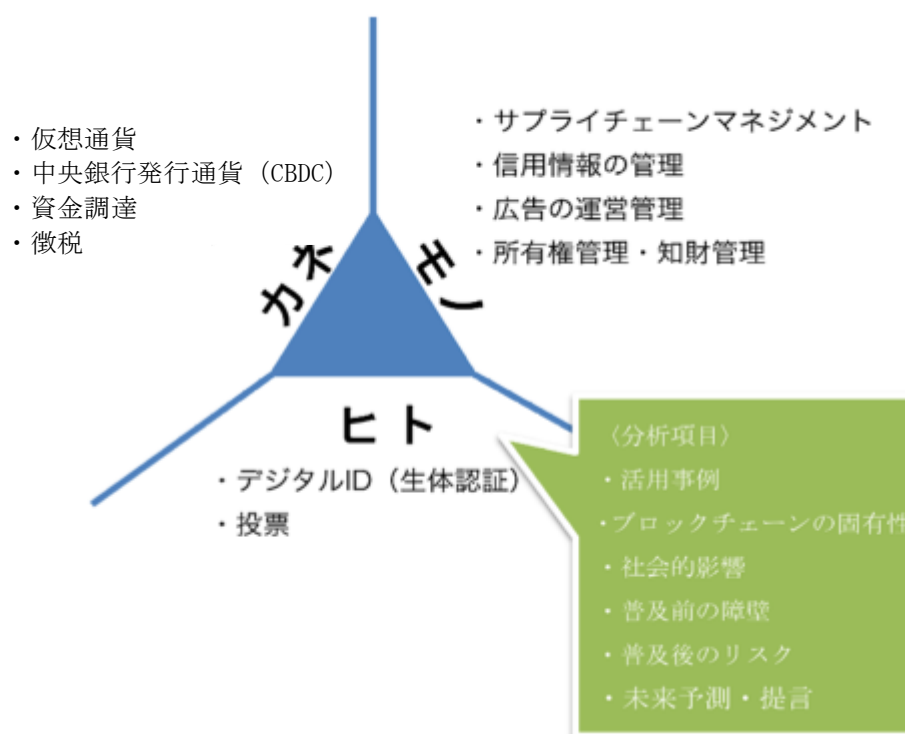


図 13.分析フロー図

⁴高木聡一郎准教授へのヒアリングより

3.2 カネ分野

3.2.1 仮想通貨

仮想通貨とは、電子媒体を用いて決済・交換を行う通貨のことを指す⁵。仮想通貨は、投資対象、決済手段、送金手段として、広まっており、巨大な市場を抱えている。2017年7月17日現在、市場全体では約7兆円、時価総額順で見るとビットコインが約3兆6900億円、次にイーサリアムが約1兆7000億円、リップルが約6700億円[16]でランクインしている。

【活用事例】

ブロックチェーン技術は重層的なスタック構造を有しており、ビットコインとイーサリアムは、その中でプロトコル（いわゆるオペレーティングシステム（OS）に相当するもの）を各自運用している。⁶（2.4.2 図12 参照）カラードコイン、アルトコインはその中でも、ビットコインのプロトコルに新たな情報を付与することで生まれ、仮想通貨の一種として知られている[17]。

【ブロックチェーンの固有性】

□決済機能

貨幣と比べると、取引履歴が公開され、改ざんが困難になる。よって、取引の記録漏れがなくなる。また、銀行口座での決済に比べて、手数料を安く済ませることができる。

□送金機能

送金（特に海外送金の場合）は通常、複数の金融機関をまたがるため、取引に日数がかかり、手数料が高くなる。それに対して、仮想通貨での海外送金は、短期で安価に済ませることができる。（図14 参照）コインチェックというビットコイン取引所曰く、銀行で10万円の海外送金を行なった場合、送金手数料は3750円～5000円かかり、反映に1～2週間必要となる。それに対し、ビットコインでは約9円、反10分～1時間程度の反映時間で済む[18]。

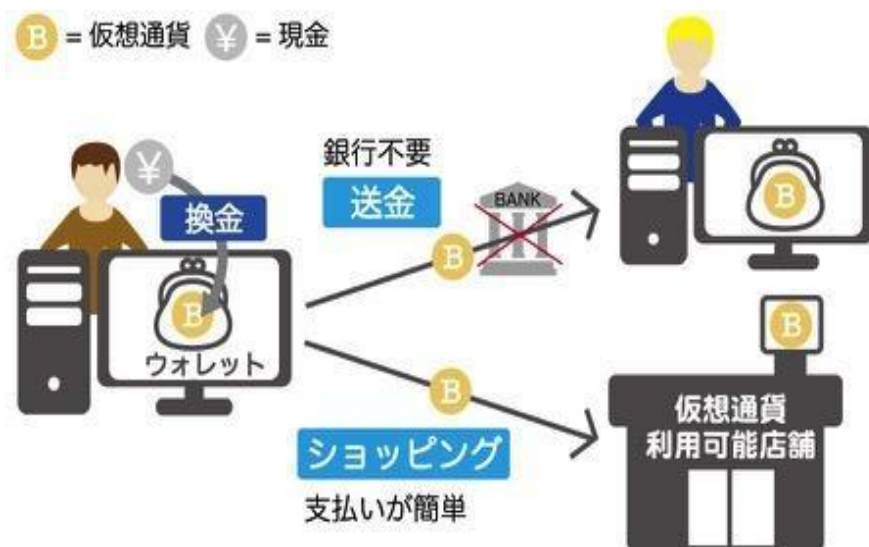


図 14. 仮想通貨利用イメージ⁷

⁵ 資金決済に関する法律第二条によれば、仮想通貨とは、「物品を購入し、若しくは借り受け、又は役務の提供を受ける場合に、これらの代価の弁済のために不特定の者に対して使用することができ、かつ、不特定の者を相手方として購入及び売却を行うことができる財産的価値（電子機器その他の物に電子的方法により記録されているものに限り、本邦通貨及び外国通貨並びに通貨建資産を除く。次号において同じ。）であって、電子情報処理組織を用いて移転することができるもの」となっている。ただし、電子マネーは、「通貨建資産」として定義されており、ここでは除外されている。

⁶ BCG のブロックチェーン技術に関するレポートによる

⁷ <https://gateway.rakuten.co.jp/journal/virtual-currency/>より参照

・マイクロペイメント

マイクロペイメントとは、10分の1円程度の単位で決済を行うことを指す[19]。ブロックチェーン技術が、取引に第三者の承認を必要としないため、手数料は低く抑えられ、少額の金銭の支払いを可能にする。

【普及前の障壁】

- ・スケーラビリティ (2.5 (5) 参照)
- ・認証時間の遅さ

ブロックごとに取りまとめるという設計上、データの確定に時間がかかる（ビットコインだと10分、イーサリアムだと15秒）。東京証券取引所は、株取引において1件当たり1.5ミリ秒での処理を目指しているのと比較すると、株の売買を即時的に繰り返す取引には向いていないと言える。

普及

【社会的影響】

- ・海外取引の増加

手数料が安くなるため、従来の方法よりも安く取引が行えるようになり、より輸出入が盛んになると考えられる。

- ・精度の高い会計処理

取引履歴が残り改ざん困難であるため、決済における抜け・漏れ・数え間違い等が減ると考えられる。そうすれば、帳簿上の不突合が少なくなるため、より精度の高い会計処理が行えるようになる。

- ・マイクロペイメントによる新たな取引

マイクロペイメントが可能になることで、これまで不可能だった取引が行われるようになる。例えば、写真、音楽、動画、記事等のばら売りが可能になるため、1記事を閲覧するのに、0.5円支払うといったことが可能になる。その結果、薄く広くお金を集められる人が、多くの資産を築くことができるようになる可能性がある。

【普及後のリスク】

- ・情報の秘匿性が低い (2.5 (4)参照)

- ・有事（システムエラー）の際の責任問題 (2.5 (6)参照)

運営方法の対立によって分裂したビットコイン事例を見ると、持続性にも疑問が残る。

- ・信用創造の割合の低下

既存貨幣が仮想通貨に置き換わったとき、銀行に預けられるお金が相対的に減少し、銀行の貸し出し機能が低下する可能性がある。そうなった場合、主に間接金融によって資金調達していた中小企業は、資金の工面の方法を変えざるを得ない、もしくは工面ができなくなる。その結果、現在の経済構造が変わり、雇用の喪失等のリスクが考えられる。

【未来予測・提言】

取引コストが下がる等のメリットを享受するには、投資対象ではなく「通貨」、決済手段として機能しなければならない。そのためには、**価格を安定**させる必要がある。しかし、Bank of England のレポートによれば、現在ビットコインはボラティリティが高く、決済手段として機能していない[24]。また、Mt.GOX 事件や、ビットコイン分裂騒動等、仮想通貨を保有することによるリスクは未だ存在している。

ただし、経済産業省ヒアリングによると、草の根レベルの浸透が、仮想通貨の決済手段としての普及を支えているのは間違いない。現在、多くの企業がビットコインの手数料の安さ、便利さに目をつけ、決済手段として使用し始めている。一方で、仮想通貨を取り締まる官庁の姿勢としては、必要以上の規制は行わず、ある程度市場に任せる方針であるとヒアリングで示唆された。これらを踏まえると、価格を安定させるのは、企業等が実際に取引に使い、社会的信頼を得ていくしかない。

以上をまとめると、ビットコイン分裂騒動等の、取引所の信頼を揺るがすような事件がこれ以上出てこない条件で、仮想通貨の決済手段としての利用が増えていけば、取引コストの減少につながり、効率的な経済が実現される。さらに、マイクロペイメントが使用されれば、経済構造の大きな変革にもつながる。

ちなみに、仮想通貨の普及は、金融政策の影響が減少することにつながるともいわれている[26]。そうすれば、中央銀行が次項で述べる CBDC の導入へと進んでいく可能性が高い。

3.2.2 中央銀行発行デジタル通貨（Central Bank-issued Digital Currency、CBDC と略）

日本のみならず世界各国の中央銀行は、貨幣発行や、民間金融機関とのお金のやり取りなどのインフラシステムをより良くするために、銀行業務への技術の活用を検討している。中でも、1990 年代から中央銀行が発行するデジタル通貨（CBDC）の発行に関する議論がなされている。そこで、近年、CBDC 発行を可能にするかもしれない技術の一つとしてブロックチェーン技術への関心が高まっている。

＊コラム -今ある技術との比較-

- ・既存電子マネー（楽天 Edy, パスモなど）：銀行口座を介した現金紙幣による決済や支払い。
↔CBDC：銀行口座は介さず取引情報のネットワークに基づいた取引。
- ・仮想通貨：民間事業者が発行し、法定通貨（円やドルなど国が発行する通貨）と交換できることで価値が生まれる。↔CBDC：中央銀行が発行し、それ自体に価値がある。

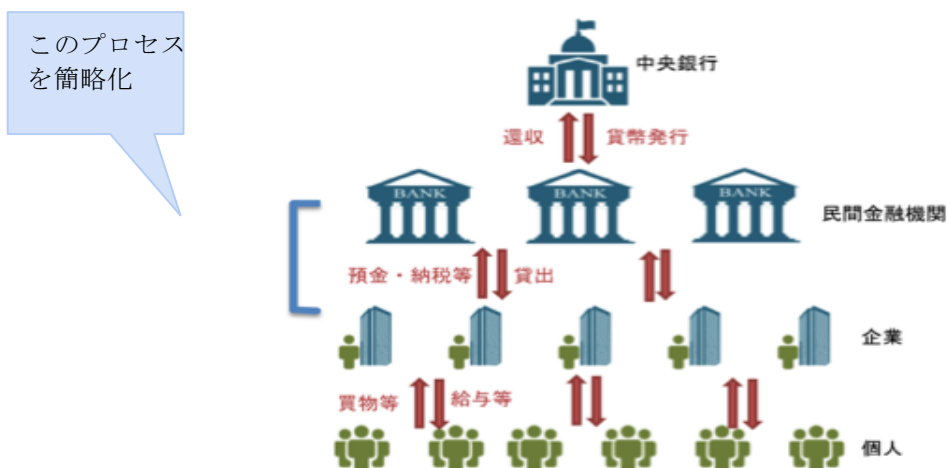


図 15. CBDC 発行のイメージ図（筆者作成）

【活用事例】

ブロックチェーン技術を利用しているか否かに関わらず、CBDC を導入している国は未だない。しかし、日本銀行やイングランド銀行をはじめ、世界各国の中央銀行は実証研究の段階にある。[27]

【ブロックチェーンの固有性】

- ・取引履歴が改ざんされない
→既存の電子マネーに比べて改ざんリスクがないため、通貨に対する信用が高くなる。
- ・P2P ネットワーク
→ブロックチェーンの管理組織が取引者である個人を特定し取引を管理できた場合、不正取引の取り締まりもできるようになる。

【普及前の障壁】

- ・技術的な問題

2.5 の(5)で述べたように、増え続ける取引データの管理方法や取引に十分な処理速度はまだ確立されていない。また、既存の取引データを新たなブロックチェーン技術でどのように扱うか不明確である。

- ・CBDC を実際に使う上で、国民の理解を得なければならない。

普及

【社会的影響】

- ・手数料など仲介コストを削減

銀行口座を介する取引ではないため、手数料など仲介コストを削減し、社会全体の取引量の増加が考えられる。通貨発行のコストを削減できる。

- ・金融政策の効果を把握

中央銀行は、タイムリーな取引状況を確認できるため、金融政策の効果を把握できる。

- ・中央銀行の通貨発行のコスト削減

【普及後のリスク】

- ・個人情報の管理に関するリスク

例えば、サイバー攻撃による秘密鍵流失によって個人情報や CBDC 喪失のリスクがある。

【未来予測】

まず、第一に、CBDC の発行は、現金の取引を代替し、キャッシュレスな社会とするだろう。しかし、この点については、取引の匿名性に対する希望がある限り、デジタル通貨と現金通貨は補完しあう関係にあり共存するとも考えられる。[28]

・また、中央銀行が個人の取引履歴を管理できると、超中央集権的社会が誕生する可能性がある。これにより、脱税や不正取引、汚職などの犯罪対策につながる一方、中央銀行のみが管理する取引情報を悪用して権力を行使するなどの極端な社会も想像し得る。

さらに、従来は取引を行う場合、民間の金融機関や中央銀行の銀行口座にある現金を移行するとき、仲介手数料を払う必要があったが、CBDC では、そのような仲介業者を介すことはなく、事実上、個人がそれぞれ中央銀行に口座をもつような形になり、金融システムが大きく変わることが考えられる。その際、失業や、新たな業務の創出など産業や雇用形態の変化も考え得る。

CBDC 発行の実現には、大量の取引情報や安全な個人情報の管理を行える技術開発の必要性が大きく、今後、世界各国が連携したさらなる共同開発が望まれる。また、中央銀行発行通貨には信用が欠かせず、国民の理解を促す必要がある。

3.2.3 資金調達

【活用事例】

企業や団体が資金調達するのにブロックチェーン上でトークンを発行し、個人など不特定多数に販売する。資金調達をしたい事業者がまず、独自の仮想通貨を発行する。投資家はこの仮想通貨をビットコインやイーサリアムなど流動性の高い仮想通貨で買う。払い込みを受けた事業者はそのビットコインなどを取引所で現金に換え事業資金や商品開発などにあてる。個人が海外の ICO (Initial Coin Offering 新規未上場通貨の上場前売り出し、株式市場でいう IPO に相等する) に参加するのは自由だが、未登録の企業が日本で投資家を募るのは違法[37]である。

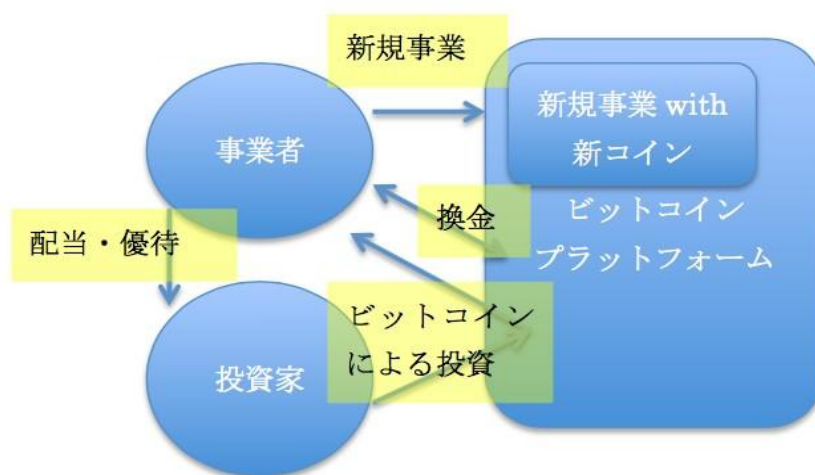


図 16. 仮想通貨を使った資金調達利用の流れ

【ブロックチェーンの固有性】

仮想通貨による支払いを前提とし、取引所で取引される株式とほぼ同じ機能を持っている。例えば、配当を受ける権利や所有権・議決権、値上がり益を手に入れたり、サービスで使用するトークンを販売すること（株式であれば、株主優待に置き換えられる）が可能である。異なる点を挙げるとすれば、株式の上場には条件（例えば、資本金〇〇円以上）があり、取引所の審査を通過して初めて上場ができるという点である。株式の場合、ある程度実績がなければ上場することができないが、ICO の場合は、それがない。

高木（2017）は、ICO のメリットについて、1. ベンチャー投資の民主化、2. 場所を選ばないスピーディな資金調達、3. コインの価値と流動性の確保、の3つとしている。3つ目は、ブロックチェーンが普及したときのメリットであるため、固有性の議論とは関係ないので、説明を省く。1つ目は、ベンチャー企業の資金調達との違いである。ベンチャー企業は資金を持ち、投資家として実績を持つ人にアピールして資金をもらうという性質上、その事業を稼働前に知っているのは限られた投資家のみだが、ICO では不特定多数の投資家から資金を調達できる。二つ目は、上記の通り、投資家から投資を引き出すためには一定の労力と時間が必要であり、地理的な制約があるが、ICO はそれがない。グローバルに資金調達することが可能である。

【普及前の障壁】

- ・仮想通貨の普及を前提とする

仮想通貨の項目で説明したことであるが、ビットコインやイーサリアム等、基本となる仮想通貨の普及がない限り、新規事業の増加が見込めない。なぜなら、それらで支払いが行われるため、コイン自体に価値がなければ、換金することができないからである。

普及

【社会的影響】

- ・新規事業の増加

グローバルな資金調達によって、手軽に投資が可能になり、新規事業が創業されやすくなる。これまで、投資元が見つからず、サービスが始まらなかった事業が表に出てくるようになるため、新規事業が増加する。

- ・間接投資から直接投資へ

これまで銀行からの投資、限られた数の投資家しかできなかった投資が、あらゆる人に開かれる。少額から投資することができるため、直接投資が増え、投資家と企業との距離が近づくことが考えられる。

【普及後のリスク】

- ・問題が起きた場合、自己責任となる。

資金調達だけして、サービスを開始しない等の詐欺行為に対して、現在のところ法的に対処できない。仮想通貨の項目と同様、問題が起こった場合、利用者の自己責任であるという問題がある。

【未来予測・提言】

詐欺コインを除外すること、もしくは投資家の保護がなされるようになれば、起業家も投資家も、手軽に投資できるというメリットを享受することができる。これにより、投資家が増えるだろう。また、仮想通貨という共通の通貨を用いた投資形態であるため為替リスクなどを考慮する必要がなく、ボーダーレスに投資が促進され、国境を越えた取引が増加する見込みがある。

3.3.4 徴税

【活用事例】

個人の納税情報をブロックチェーン上で管理する。エストニアでは、2015 年よりオンラインで確定申告が可能な「e-Tax」というブロックチェーン技術を用いたシステムを導入しており、個人所得税のオンライン申告率は約 95%となっている。その確定申告作業は約 3～5 分で済むという。[38] 現在、日本の国税庁もオンライン上で確定申告を行える「e-Tax」というサービスを提供しているが、個人情報との一体化した情報管理がなされていないため、なりすましなどの問題が懸念されている。[39]

【ブロックチェーンの固有性】

既になされた徴税履歴への改ざん不可能性並びに、個人情報と紐付けた自動的な記帳によって徴税漏れが防止される。また、従来、徴税にかかっていた手続きや中間コストを削減し、行政の業務効率化や国民の利便性向上が期待される。[40]

【普及前の障壁】

- ・国民全体からのコンセンサスを得ることが必要
- ・国民一人一人の膨大な情報量の管理という技術的課題
- ・ブロックチェーン技術を用いた税に関する法整備の必要性

普及

【社会的影響】

- ・税収増加
徴税が正確に行われることで税収の増加が見込まれる。

【普及後のリスク】

- ・秘匿性が確保されず、個人情報が漏洩するリスク
- ・システムを扱えない人への対処

【未来予測・提言】

納税情報のみならず、仮想通貨やデジタル通貨などの通貨に関する情報をブロックチェーン上で管理することで、確定申告という手続きに限らず、納付までを一体化して効率的に行うことができるようになるだろう。また、銀行口座情報とも連動すれば、自動的に徴税するシステムも可能になる。さらに、社会保障サービスなどの公共サービスの提供にも役立てられると考えられ、エストニアのような電子国家社会となり得る。エストニア型の電子国家では、国民が自身の情報にアクセスでき、国民によって国の情報管理が適切に行われているかを管理する逆監視社会の実現が可能となるだろう。

行政の業務効率化のために、ブロックチェーン技術を活用することは既に実現に向けて検討され始めている。[41]

3.3 モノ分野

3.3.1 サプライチェーンマネジメント

【活用事例】

Everledger によるダイヤモンド取引の透明化 [43]

ロンドンを本拠地とする Everledger はブロックチェーンを用いたダイヤモンドのサプライチェーンマネジメント管理を行う。採掘から研磨、供給まで、限られた数のプレイヤーが世代をまたいでビジネスを牛耳ってきたダイヤモンド業界において、強制労働や紛争ダイヤモンドの流通などの問題がある。従来は原本で管理されていた品質証明書をデジタル化し、ダイヤモンドの石にある固有の特徴から個別の ID を与え、原産地から消費者までを網羅した取引の全プロセスで透明性を確保した台帳を作り上げた。結果として、当該ダイヤモンドが強制労働に関わっていないことや鑑定書が本物であることを証明できるなど、流通の効率化だけでなく、品質の担保が可能となった。

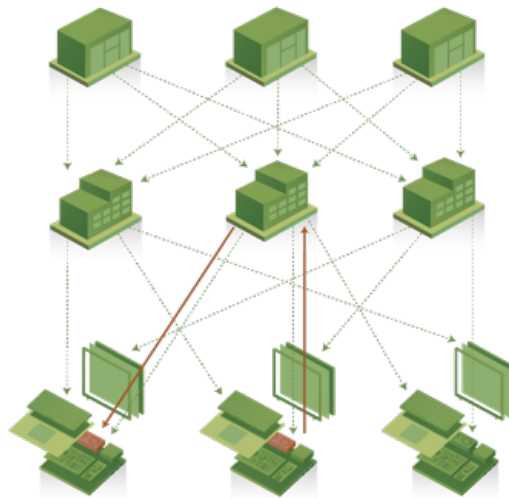


図 17. サプライチェーンマネジメントへのブロックチェーン技術活用のイメージ図 [42]

【ブロックチェーンの固有性】

書き替えができないため、トレーサビリティの担保が可能となる。また、産地や管理情報などの改ざんやミスをなくし、商品情報の信頼性を保証する。さらに、情報のデジタル管理によって、ペーパーワーク由来の管理コストを削減する。

【普及前の障壁】

- ・既存のサプライヤーが管理情報をすべて提供することへの心理的な障壁
- ・ブロックチェーンシステムを導入するイニシャルコストが大きい

普及

【社会的影響】

・生産から消費までのシームレスな情報管理が低コストで行われることで、**商品流通が最適化**されることが期待される。具体的には、税関などの膨大なペーパーワークをスマートコントラクトと組み合わせて自動化し作業量の縮小が可能となる。

・産地や管理情報（管理温度・保管期間等）が書き換え不可能となることで、**商品情報への信頼度が向上**する。特に、Everledger によるダイヤモンド流通管理がモデルケースとなるように、嗜好品や芸術品において、贋作の排除などにも貢献が期待される。

【普及後のリスク】

- ・有事の際の責任の所在が不明確になるというリスクがある。

【未来予測・提言】

長期的には、ブロックチェーンを活用したサプライマネジメントが普及した社会では、仲介業者の淘汰が進み大企業による商品流通の独占が進む可能性がある。商品の流通履歴が消費者からもアクセス可能になると、価格設定の妥当性がよりシビアに問われるようになり、コストカットを追求した低価格帯と付加価値を持つ高価格帯への二分化が進み、商品の淘汰がより激しくなるのではないだろうか。

また、価格だけではなく品質までも含めた、消費者による生産者の評価がよりシビアに行われる社会が登場する可能性もある。消費者と生産者の力関係が逆転し、商品価値が買い叩かれる生産者泣かせのデストピアな世界が現れる危険性もあり、現在よりも生産者を保護する仕組みが必要となるかもしれない。

3.3.2 信用情報の管理（スマートプロパティ）

スマートプロパティによって、デジタル化が可能な物理的な資産は（公文書、契約書、電子カルテなど）ブロックチェーンネットワークで不変な記録として保管できる。

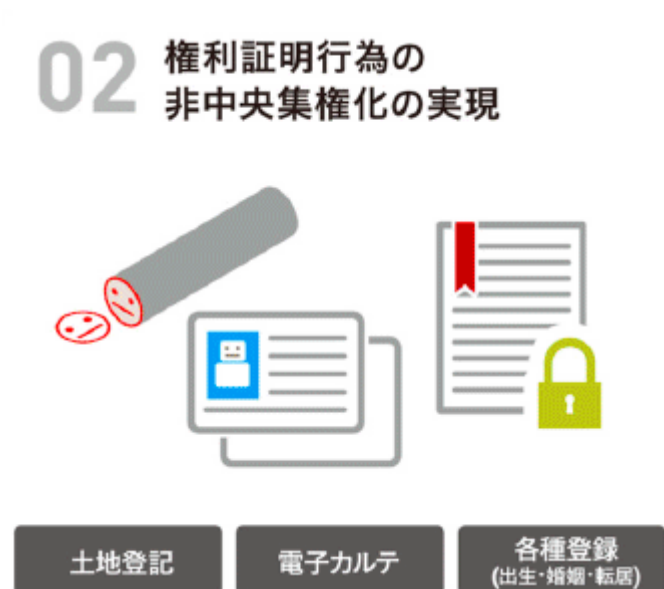


図 18. 信用情報のデジタル化イメージ図⁸

【活用事例】

官では、ドバイ政府が 2020 年までに「ブロックチェーン都市」の目標を発表しており、全ての公文書を分散型台帳に保管する取り組みを行っている。これにより、ペーパーワーク由来の管理費を節約でき、ドバイの競争力を向上させる計画だ。

民間では、書類を分散的に管理するプラットフォーム「Factcom」がすでに提供されている。

【ブロックチェーンの固有性】

暗号化及び分散化されているため、改ざんが不可能な形で、信用情報を保管できる。ネットワーク参加者間で直接、情報を共有するため、P2P 型取引と親和性が高い（スマートコントラクト）。

また、2.5 の(3)で述べたように、ゼロダウンタイムなシステムとして構築されているため、信頼性の高い文章の管理のための保管庫の役割を果たす。

⁸ <https://inforium.nttdata.com/wp-content/uploads/b06-1.gif>

【普及前の障壁】

ブロックチェーン上で記録される情報は、参加者全員で共有されるため、機密情報を管理する場合、**秘匿性を確保できない**。そのため、原本性を保証する信用情報に関しては、ブロックチェーン上で参照できる人を制限する仕組みが必要になってくる。

普及

【社会的影響】

・ブロックチェーン上で管理される信用情報をP2P取引に用いることで、**スムーズな情報共有**が可能となる。具体的に電子カルテで説明する。既存の記録システムの場合、患者情報は共有不可能であったため、医療関係者はデータ入力作業に多く時間を浪費していた。しかし、ブロックチェーンの導入により、電子カルテ処理の効率化を実現でき、医者は無駄な業務から解放され、本業の治療に専念できる。

・**真贋性が仲介業者を介さずに証明**できる。情報が永続的に保管されるため、行政による不正が解消される。例えば、土地権利をブロックチェーンネットワークに登録することで、所有権があやふやになることはなくなる。
が期待される。

【普及後のリスク】

悪意のある参加者でも信用情報にアクセスできるため、内部からの情報の持ち出しに関するリスクがある。

【未来予測・提言】

ゼロダウンタイムによる安定性で、認証に関するすべての書類情報はブロックチェーン内で保管される。しかし、秘匿性の問題を解決できない限り、機密情報などは引き続き紙で運用される。

ターニングポイントとして考えられるのが、書類管理とデジタルIDの紐付けが上手くいくかどうかである。どちらも単体では、基盤技術の側面が強いため、社会的影響はペーパーレスなどに留まり、そこまで大きくない。しかし、長期的にエストニアのような電子国家を目指す場合には、文書管理とデジタルIDの連携は必要不可欠である。

その際、今後重要になるのが国民の理解だ。個人情報や安全な形で管理するのは魅力的だが、共有されることに抵抗を感じる国民は多いだろう。しかし、技術の進歩に反対するのではなく、「自分の情報を権力側からいかに守るか」を意識した発展を目指すべきである。

3.3.3 広告の運営管理

【活用事例】

現時点での活用はあまり進んでいない分野であるが、2017年4月にデジタル・アドバタイジング・コンソーシアム(DAC)によって、この分野において日本初の実証実験が行われた。広告配信の監査・検証(広告配信としてカウントされている非リアルタイムの閲覧から、本当に広告配信が行われたかどうかを判断する)に対してブロックチェーンを活用した取り組みである。

その他にも、マーケティングや消費者データ管理などにおいてもブロックチェーン活用の余地がある。

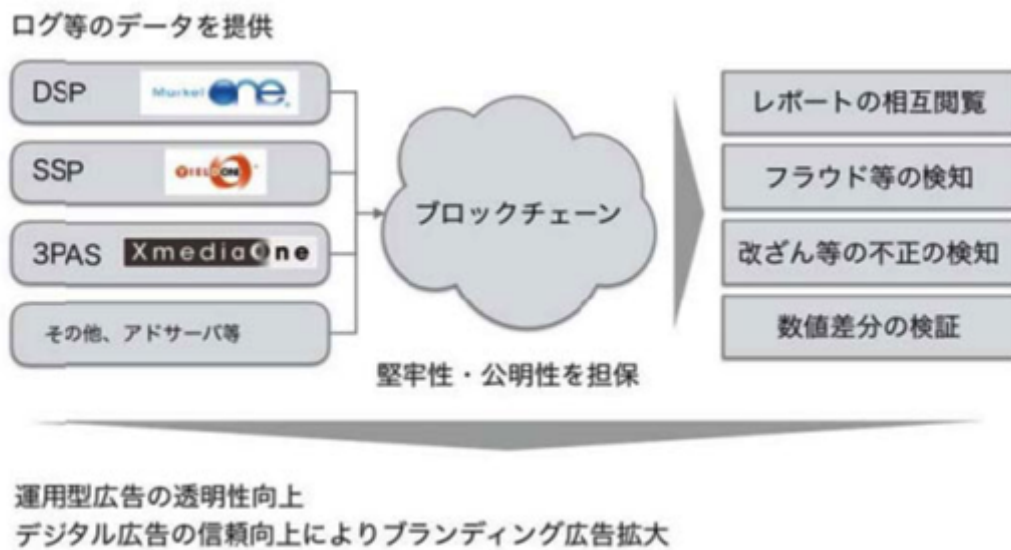


図 19. 広告の運営管理への導入イメージ図[50]

【ブロックチェーンの固有性】

仲介を挟まないやり取りによるコスト削減は、情報の分散管理を行えるブロックチェーン技術ならではといえる。

【普及前の障壁】

- ・スケーラビリティが現状では小さく、大量のデータを扱う広告においては大規模な展開は技術的に難しい。
- ・検証システムには大きな導入コストがかかる。
- ・既得権益を持つ企業が情報のシェアを行うことへの心理的障壁は高い。

普及

【社会的影響】

- ・中央集権的な監視システムよりコスト削減が可能になる。
- ・広告効果の測定精度が向上する。

現在存在する多くの広告効果測定スタートアップなどの淘汰が進むと考えられるだけでなく、企業間で情報の共有が進めば、より効率的な顧客ごとに最適化された広告が可能となる。

【普及後のリスク】

複数の企業が管理していた個人の広告閲覧属性の情報が、分散的とはいえ個人に紐付いたひとつのまとまった情報として管理されることで、プライバシーが丸裸にされるリスクがある。

【未来予測・提言】

特定の管理者がいるわけではないが、個人の情報がすべて一括で管理される準監視社会が実現する可能性がある。ネット社会において完全なプライベート空間が存在しえず、誰もが自分の個人情報にアクセスできるという「気味が悪い社会」が想像できる。対抗として、脱インターネットで自給自足の閉鎖的コミュニティへの回帰を進めるアーミッシュ的な集団が現れるというシナリオも考えられる。

3.3.4 所有権管理・知財管理

【活用事例】

アーティストやクリエイターが自らの作品をドラッグ&ドロップするのみで改ざん困難な共有台帳に自らの作品を登録し、その登録証明書を発行できる。作品創作時点の立証に一定の効果を持つことが期待される。美術品の真贋判定や、イラストなどのオリジナルと二次創作物との派生関係の管理やライセンス料の分配などへの貢献が考えられる。

【ブロックチェーンの固有性】

改ざん不可能性を活かし、以下の点での貢献が期待される。

- ・先使用权の立証
- ・二重譲渡の防止
- ・著作権の帰属の立証

著作物や芸術品に限らず、土地や不動産管理など幅広い用途での技術活用が期待される。

【普及前の障壁】

- ・ブロックチェーン技術による合意形成が、従来の法的な拘束力を持つ契約と同じ程度の社会的な信頼を得られるかどうかは大きな課題である。
- ・仮に、著作権の登録管理にブロックチェーンを用いるとなると、システムの導入コストとスケーラビリティの問題が考えられる。

普及

【社会的影響】

改ざん困難な台帳による情報管理により、以下のようなメリットが予想される。

- ・情報管理のセキュリティの確保
- ・ニセ情報の排除・情報の信頼性
- ・不動産取引（審査等）のスピードアップ
- ・詐欺リスクの減少

【普及後のリスク】

- ・情報管理の責任所在が不明確であり、何らかの形で情報の欠損が起こった場合にどのような対応が取られるのかはリスク要因である。

【未来予測・提言】

アーティストや創造物に対する権利が世界中で保証されるようになる一方で、「権利」「特許」の価値が向上する世の中になりうる。たとえば、具現化されていないアイデアに対して、「権利」のみを獲得しておき、具現化された成果物に対して先行権を主張するアイデアビジネスが市場として拡大するなど、所有権や行動権が必要以上に価値を持つある意味では息苦しい世の中が到来する恐れもある。

3.4 ヒト分野

3.4.1 デジタル ID

一人一人に国民番号をブロックチェーンネットワーク上で付与し、個人間取引における信用の強化に繋げることを目的としている。固有の番号を発行し、氏名、生年月日、性別以外にも、指紋や虹彩などの情報を登録することで、生体認証が可能となる。



【ブロックチェーンの活用事例】

活用事例としては、電子政府を目標としているエストニアの「デジタルネーム」や、すでに 10 億人の生体情報を管理しているインドの「アドハー」などが挙げられる。

【ブロックチェーンの固有性】

既存技術で類似するのがマイナンバーだ。デジタル ID との違いは、データの透明性とトレーサビリティである。利用者自身が、ID へのアクセス履歴をいつでも確認することができ、情報管理を個人で行える。それに対して、マイナンバーに記録されているデータは秘密情報として扱われ、管理主体は国となっている。

もう一つ特徴として挙げられるのが、2.5 の(3)でも述べた、分散型で可能になったゼロダウンタイム機能、つまりシステムが停止しないことだ。デジタル ID が普及するにつれ、大量の照会要求に対応できるプラットフォームが必要になるため、ブロックチェーンの利用価値は大きい。

【普及前の障壁】

日本では、マイナンバー制度が権力による国民監視システムという認識で広まっており、交付普及率は 8.4%にとどまっている。今後、**国民の理解を得る必要**があり、認識を転換させることが、政府に求められる。

普及

【社会的影響】

・デジタル ID 単体では、個人情報の登録や管理と、マイナンバーと同じ機能を提供するに限るため、社会の根本的な変化には繋がらない。しかし、基盤技術として既存のサービスに組み込みやすく、連携がスムーズになるように設計されているため、応用範囲は広く、決済、納税、投票、医療情報などで実行及び検討されている。特に親和性が高い領域は認証分野で、電子署名、有権者登録、パスポート・セキュリティパス・免許証などで導入が進むと言われている。

【普及後のリスク】

・応用範囲が広いため、今後は重要な個人情報がデジタル ID に登録されいく。その場合、情報漏洩が起きると、現在以上に**秘匿性の高い情報が流失するリスク**が高まる。
・また、記録の不可逆性が改ざん耐性を担保しているが、なりすましが生じた際の運用対処が難しくなる。

【未来予測・提言】

未来予想としては、エストニアが目指すビットネイション構想などが有力と考えられる。これまで中央集権的に政府が担っていた認証サービスをブロックチェーン上で自動化し、分散的かつ自律的な国家を実現する計画だ。具体的なメリットとしては、納税、医療、選挙などの公的サービスがペーパーレスで処理することで、手続きが簡素化し、時間の浪費と費用を減らせる。同じく、会社設立のプロセスも効率化し、スタートアップの誘致が進む。長期的には、国籍に縛られない電子移住民で成り立つ共同体が考えられ、国家は領土ではなく、データで定義される時代が到来する可能性がある。

ターニングポイントとして想定するのは、応用分野でのキラーアプリケーションの登場だ。明確なユーザーメリットが存在しない限り、国民の登録率は飛躍的に伸びないだろう。

普及において国民の理解が必要となることは自明である。デジタル ID は、電子国家を目指す上での必要不可欠な基幹技術であるという認識を共有することが重要であると言える。

3.4.2 投票

【活用事例】

ブロックチェーン上での選挙に関しては、エストニアが電子政府構想の一部として検討している。民間では、Voatz と Clear Ballotn のブロックチェーンをベースにした選挙システムの研究の他に、J.P モルガンやサンタンデル銀行などの金融機関が実証実験している議決権行使（議案に対して賛否を表明すること）での応用がある。



【ブロックチェーンの固有性】

ブロックチェーンを介して投票を行うことで、参加者全員同一の情報を共有し、不正が不可能になる。加えて、改ざん耐性が高いため、投票データを登録後に細工することができない。

【普及前の障壁】

- ・投票用紙に慣れ親しんだ高齢者層にとって、情報技術を用いた投票をすぐに行うことはハードルが高い。
- ・また、全国民の投票意思を技術的にオンタイムで処理しなければならないため、技術的ハードルも高い。電子端末のトラブルはすでにフランスで起きている。

普及

【社会的影響】

- ・安全性が高く、遠隔で選挙が可能になることで、投票所、紙や投票箱などが不要になり、税金で賄っている監視員の人件費も削減することができる。
- ・また、選挙離れの原因となっている時間や距離の問題も解消でき、投票率が伸びると予想できる。
- ・投票は全てデータとして記録されるため、手作業での投票用紙の集計は自動化され、ミスの予防及び開票結果がより早く分かる。
- ・ビジネスに関しては、株主総会により国外の投資家がボーダレス投票できるため、グローバルなコミュニケーションを促進する期待ができる。既存の電子投票システムの遠隔で株主総会に参加できないという欠点を補うことができる。

【普及後のリスク】

一度登録した記録を変更することは困難なため、なりすましが起きた場合の運用対処は重要な問題である。

【未来予測・提言】

秘密選挙の確保に関しては、すでに技術的に可能な水準にまで達している。管理者が存在するコンソシアム型やプライベート型であれば、2.3 で述べた公開暗号方式によって投票内容は秘匿化でき、送信先（管理者）以外に投票内容を知られることはない。今後ブロックチェーン上での投票が実現する可能性は高いだろう。

重要なのは、ブロックチェーンはあくまで「投票のしやすさ、結果の正確さ、開票の早さ」を実現するのであって、投票に対する無関心は解決しない。投票が簡単になれば、一票の重みを認識しづらくなるリスクもある。そのため、政治教育を今後も大切に学んでいく必要がある。

4. 総論

本章では、第3章での各ユースケースの分析を踏まえて、ブロックチェーン技術の普及における課題と社会的影響をマクロ的視点で整理する。

4.1 普及における課題

第3章での普及前の障壁と普及後のリスクを図20にまとめた。これらを受けて、普及における課題として主に以下の4点を挙げる。

		秘匿性	スケーラビリティ	責任問題	導入コスト	心理的抵抗	なりすましリスク
カネ分野	仮想通貨	○	○	○			
	CBCD	○	○		○	○	
	資金調達			○			
	徴税	○	○		○	○	
モノ分野	サプライチェーン	○			○		
	信用情報	○					○
	広告の運営管理	○	○		○		
	所有権・知財管理	○		○			○
ヒト分野	デジタルID	○				○	○
	投票	○	○			○	○

図20. 第3章の各事例分析の普及前の障壁と普及後のリスクのまとめ

1. 技術的な課題

第2章で言及した取引の秘匿性の担保や、スケーラビリティ、異常時の処理などの課題があり、これらが改善されない限り、サービスとして成立しない可能性が大きい。

2. 未整備な法

ブロックチェーン技術の応用が社会的な信頼を獲得し普及が進むまでには、関連する法整備が欠かせない。例えば、仮想通貨については、2017年4月に仮想通貨法が施行され、仮想通貨に関する法整備が進んだことで利用者保護の側面が強まった。同様に、個人情報管理や証券取引に関する法制度など、個人情報漏洩や秘密鍵流失などの想定される問題についても責任の所在など、明確な法の言及がなければ、社会的な信頼を得て技術が普及することは難しい。

3. 代替技術としてのメリットの弱さ

既存のシステムを代替する技術としては、ブロックチェーン活用の意義・メリットが不明確・不十分である。改ざんが難しい、ゼロダウンタイム、コスト削減などのメリットがあっても、既存の技術を上回る利点がユーザー目線で認識されておらず、実装に至っていないというのが現状だ。

4. 組織が普及を進めようとする概念的矛盾

現在、民間企業によるブロックチェーン技術の研究・開発が進んでいるが、「ブロックチェーン技術という組織の信用に依らないシステムを組織が形成しようとしている」という矛盾がある。ブロックチェーンの本質は、管理者なくフラットな関係性で情報を分散管理しようとする概念にある。言い換えると、組織によって、管理者としての組織の存在を否定するブロックチェーン技術の導入を進めることは自己矛盾的であると言える。現状の普及に向けた取り組みは「ブロックチェーン技術が一体誰のためなのか」という問いに答えることなく、新規性や話題性に飛びついて進む哲学なき導入である。技術を導入することのメリットを開発者自身が真の意味で認識していなければ、本当の意味でのブロックチェーンの普及は遠いだろう。こうした構造的な矛盾を考慮に入れると、やはりブロックチェーンの普及の鍵となるのは、**アプリケーションレベルでいかに市民を取り込めるか**である。その点で、ブロックチェーンは市民レベルで生まれ市民レベルで草の根的に広がっていくテクノロジーであり、その普及具合は技術への社会的需要に大きく影響するだろう。

4.2 社会的影響・未来予測の総括

P2P ネットワークにより情報を管理するブロックチェーンでは、信用形成のあり方が大きく変わる。従来の組織や国家といった管理者への信頼ではなく、ネットワーク末端の各参加者への信頼が情報への信頼の拠り所となるからだ。

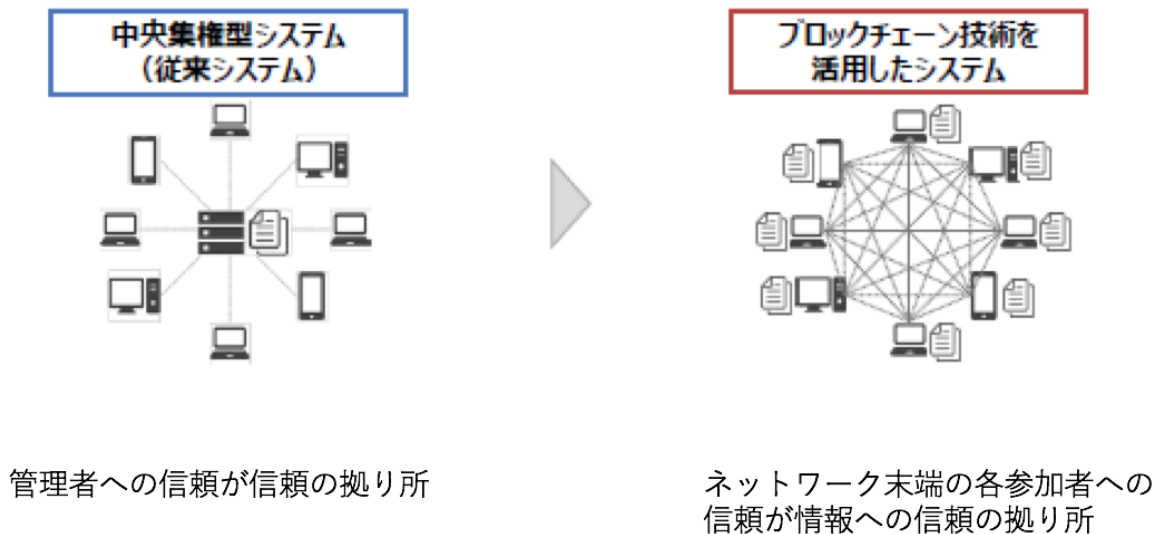


図 21.（経済産業省「ブロックチェーン技術を活用したシステムの評価軸 ver1.0」をもとに筆者作成）

管理者不在のパブリック型ブロックチェーンにおいて、この信用形成のあり方はもっとも劇的に変化するが、管理者を設置したコンソーシアム型、プライベート型が普及しているのが現状であることは前述（2.4.1 参照）の通りである。

コンソーシアム型ブロックチェーンへの社会的受容が進み、本来的ともいえるプライベート型ブロックチェーンの普及が進んだ世の中においては、従来の情報管理者と被管理者の力関係の格差が縮まり、場合によっては従来の被管理者が従来の管理者を監視する社会になることも考えうる。このような社会においては、仲介業者などの中間的役割はその意義を消失し、失業や産業構造の変化に繋がる可能性がある。

コンソーシアム型など管理者ありの形態に限定される場合、ネットワーク形成と信用のあり方は大きく変わらない。しかし、ブロックチェーンの改ざん不可能性という技術利点を活かし、管理組織はより機密性の高い個人情報を保持できるようになる。この形態での技術普及の延長線上として、エストニアのようなデジタル国家社会となり、管理組織による超中央集権的社会の誕生もあり得る。また、一部の企業が情報管理を行った場合、それ以外の企業との情報格差および経済格差につながり、より一層寡占化が進む危険性もあるだろう。（図 22 参照）

現在

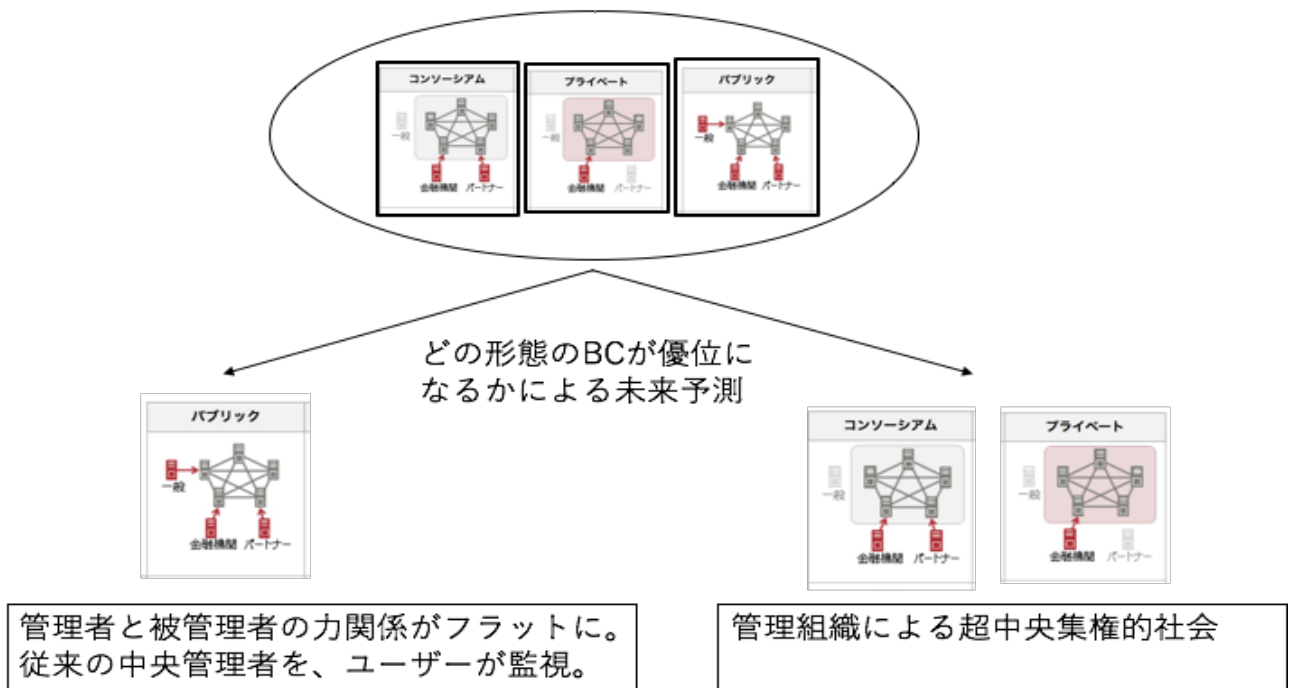


図 22

5.おわりに

我々がこのブロックチェーンプロジェクトに取り組み始めた3ヶ月前、我々自身がこのレポートの読者と想定した「ブロックチェーンの名前は知っているがそれ以上のことは何も知らない大学生」であった。3ヶ月間の間に、書物やオンライン文献を読み漁ることはもちろん、ヒアリングを重ね、ブロックチェーンを利用した地方自治体のスタンプラリーに参加したり、Bitflyerの口座を開設し実際にビットコインの運用を始めたりと、思いつく限りの手段を用いてブロックチェーンと向き合ってきた。3ヶ月を経た今も、ブロックチェーンの全貌を理解したとは言えないが、ブロックチェーンの持つポテンシャルの大きさは十分に体感することができた。

本レポートを読み終えた読者の皆さんは、現在どのように感じているだろうか。やはりブロックチェーンは難しいと感じる人、ユーザーとしての接点は意外と多くないと感じた人、本レポートにとどまらない活用法を思いつき未来に対してワクワクしている人、感じ方は人それぞれであろう。しかしながら、ブロックチェーンという現在進行形で広がり続ける大海原を完全に理解できた人は皆無なのではないだろうか。今感じているモヤモヤ感を忘れることなく、今後もブロックチェーンについて情報収集や機会があれば実際にプロダクトを使用してみることを強く勧めたい。

繰り返しにはなるが、ブロックチェーン技術は草の根的に発展することが期待される技術である。たった一つのキラーアプリケーションの登場で劇的に普及が進む可能性を持っており、我々市民こそがブロックチェーンの未来を作っていく存在である。目先の情報や変化に目を向けるだけではなく、ときには長期的な視点でブロックチェーンを始めとする新技術が未来に与える影響について思いを向けてみて欲しい。今ある情報を鵜呑みにするだけではなく未知に対して勇気を持って向き合い、考え続ける営みこそが、これからの時代を生きる人々に課された義務であるのではないだろうか。本レポートが、そうした営みの一助となることを執筆者一同願ってやまない。

謝辞

本レポートの執筆にあたっては、谷口武俊教授、吉澤剛准教授から様々なご指導、貴重なアドバイスをいただきました。また、経済産業省情報経済課や金融庁総務企画局の方には官庁の視点からのブロックチェーン・仮想通貨の活用について貴重なヒアリングの機会をいただきました。国際大学グローバル・コミュニケーション・センターの高木総一郎准教授にはアカデミアの観点からマクロ視点での貴重なアドバイスをいただきました。オンラインで多くの質問にお答えいただいたブロックチェーンビジネス研究会の皆さまにも深謝申し上げます。そして、推敲にあたって、鋭い指摘をくれた執筆者の友人にも心からの感謝の気持ちを伝えたいと思います。

末筆にはなりますが、ご指導いただいたすべての関係者の皆様に、心より感謝申し上げます。

2017年8月10日 執筆者一同

付録

行政の取り組み

普及における課題を乗り越えるべく経済産業省と金融庁が行っている取り組みを紹介する。経済産業省は、2015年からいち早くブロックチェーン技術に着目し、ブロックチェーン技術を利用したサービスや、ブロックチェーン技術が社会に与える可能性について整理・調査し、その経済的・社会的ポテンシャルを明らかにしている[1]。一方で、既存技術を代替するほどのメリットが不明確であるとの課題を認識し、2016年度には、ブロックチェーン技術に関して、「ブロックチェーン技術を活用したシステムの評価軸 ver1.0」を策定した。評価軸は、「品質」「保守・運用」「コスト」の3つの項目からなり、民間の技術開発企業が、ブロックチェーン技術を活用したシステムに置き換える場合の比較評価やブロックチェーン技術を活用したシステムの実証試験結果の評価をする際に役立てることを期待する。経産省は、草の根的に民間企業からブロックチェーン技術が普及することを促す。

金融庁は、2016年に銀行法を改正し、金融機関とフィンテック企業が連携・協働していくための制度的枠組みを整備。具体的には、金融機関とフィンテック企業の契約締結を促すプラットフォーム（オープンAPI）を構築し、顧客情報ネットワークを持つ金融機関と、技術開発能力をもつフィンテック企業が互いの強みを生かすことを促す。また「ブロックチェーン連携プラットフォーム」の支援も行っている。「ブロックチェーン連携プラットフォーム」は、IT事業者やFintechベンチャー等と銀行が協働・連携してブロックチェーン技術を活用した金融サービスの開発に向けた実証を可能にするプラットフォームであり、金融庁は、ブロックチェーン技術関連事業者と金融機関とのネットワーク形成において、規制面など、課題解決に向け支援する。⁹国際的な研究機関等との共同研究では、金融庁をはじめ、日本銀行、東京大学などの国内機関に加え、米国MITメディア・ラボ、カナダ中央銀行、シンガポール金融管理局、香港の研究者など海外からも多くの利害関係者が参加し、ブロックチェーン技術の活用についての共同研究が進められている。さらに、昨今では「Reg Tech」という新しい概念が導入されている。これは、Regulation（規制）とTechnology（技術）を合わせた造語であり、技術により金融規制を管理することを表す。実現段階にはまだないが、例えば、金融庁が民間金融機関の取引のブロックチェーンの管理組織となることで、取引の規制等が可能となる。

⁹ 全国銀行業界作成資料「「ブロックチェーン連携プラットフォーム」（仮称）の基本構想」より

参考文献：

- [1] 経済産業省 (2016) ブロックチェーン技術を活用したシステムの評価軸 ver1.0
<http://www.meti.go.jp/press/2016/03/20170329004/20170329004.html>
- [2] Blockchain Biz (2017) ブロックチェーンのセキュリティに必要な不可欠な鍵「秘密鍵・公開鍵」
<http://gaiax-blockchain.com/key>
- [3] 岩下直行 (2016) デジタル通貨は経済・社会に何をもたらすか (ブロックチェーン・イノベーション 2016
【GLOCOM View of the World シンポジウム】 パネルディスカッション資料)
http://www.glocom.ac.jp/wp-content/uploads/2016/08/20160908panel1_Iwashita.pdf
- [4] 高木 聡一郎 (2017) 『ブロックチェーン・エコノミクス 分散と自動化による新しい経済のかたち』 翔泳社
- [5] BCG (2017) ブロックチェーンの経営戦略
<https://media-publications.bcg.com/Thinking-Outside-the-Blocks.pdf>
- [6] Swan 2015
- [7] ブロックチェーン技術の活用可能性と課題に関する検討会 (2017) ブロックチェーン技術の活用可能性と課題に関する検討会報告書
- [8] 高木 聡一郎 (2016) ブロックチェーン概要と可能性 (ブロックチェーン・イノベーション 2016
【GLOCOM View of the World シンポジウム】 基調講演資料)
http://www.glocom.ac.jp/wp-content/uploads/2016/08/20160908Lecture1_S.Takagi.pdf
- [9] アンドレアス・M・アントノプロス (2016) 『ビットコインとブロックチェーン 暗号通貨を支える技術』 NTT 出版
- [10] IBM developerWorks ホームページ
- [11] http://www.atmarkit.co.jp/fwin2k/operation/skype02/skype02_01.html
- [12] <https://tradeblock.com/blog/bitcoin-network-capacity-analysis-part-1-macro-block-trends>
- [13] ビットコイン日本語情報サイト ビットコインとは何か? 第 5 回: ビットコインの問題点とこれからの未来
<https://jpbitcoin.com/about/whatisbitcoin5>
- [14] <http://japanese.engadget.com/2017/08/02/2/>
- [15] Fujitsu | 金融ソリューション ～ブロックチェーンの取り組み～
<http://www.fujitsu.com/jp/solutions/industry/financial/concept/blockchain/>
- [16] Crypto Currency Market Capitalizations (2017) <http://coinmarketcap.com/#JPY>
- [17] BCG (2017) ブロックチェーンの経営戦略
<https://media-publications.bcg.com/Thinking-Outside-the-Blocks.pdf>
- [18] coincheck ビットコイン取引所 (2017) <https://coincheck.com/contents/money-transfer>
- [19] みずほ総合研究所 (2017) 『ブロックチェーンがもたらす金融ビジネスの革新』
- [20] 日本経済新聞 8/8/2017 付記事 (2017)
<http://www.nikkei.com/article/DGKKZO19743890X00C17A8L82000/>
- [21] 高木聡一郎 (2017) 『ブロックチェーン・エコノミクス：分散と自動化による新しい経済のかたち』 翔泳社
- [22] 日本経済新聞 7/27/2017 付記事 (2017)
http://www.nikkei.com/article/DGXXKASDC25H2P_W7A720C1EE9000/
- [23] 日本経済新聞 8/8/2017 付記事 (2017)
http://www.nikkei.com/article/DGXLASGD08H6L_Y7A800C1EN2000/
- [24] Bank of England レポート (2017)
<http://www.bankofengland.co.uk/publications/Documents/quarterlybulletin/2014/qb14q302.pdf> Bank of
- [25] 高木准教授へのヒアリングより
- [26] 高木聡一郎 (2017) 『ブロックチェーン・エコノミクス：分散と自動化による新しい経済のかたち』 翔泳社
- [27] Bank of England (2016) 「The macroeconomics of central bank issued digital currencies」
<http://www.bankofengland.co.uk/research/Documents/workingpapers/2016/swp605.pdf>
- [28] 日本経済研究センター (2017) 「2017 年 7 月 21 日 デジタル通貨は現金通貨を置き換えることになるか」 <http://www.jcer.or.jp/column/saito/index967.html>
- [29] ejinsight 記事 (2017) 「Why central bank-issued digital currency will be good」
<http://www.ejinsight.com/20170518-why-central-bank-issued-digital-currency-will-be-good/>

- [30] Bank of England (2016) 「Enabling the FinTech transformation: Revolution, Restoration, or Reformation?」
<http://www.bankofengland.co.uk/publications/Documents/speeches/2016/speech914.pdf>
- [31] 日本銀行 (2016) 日銀レビュー「中央銀行発行デジタル通貨について ―海外における議論と実証実験―」https://www.boj.or.jp/research/wps_rev/rev_2016/data/rev16j19.pdf
- [32] Bank of England (2016) 「FinTech Accelerator Proof of Concept」
<http://www.bankofengland.co.uk/Documents/fintech/fintechpocdlt.pdf>
- [33] 日本取引所グループ (2016) 金融市場インフラに対する分散型台帳技術の適用可能性について
http://www.jpx.co.jp/corporate/research-study/working-paper/tvdivq0000008q5y-att/JPX_working_paper_No15.pdf
- [34] Santander Fintech 2.0 Paper <http://santanderinnoventures.com/wp-content/uploads/2015/06/The-Fintech-2-0-Paper.pdf>
- [35] BCG (2017) ブロックチェーンの経営戦略
<https://media-publications.bcg.com/Thinking-Outside-the-Blocks.pdf>
- [36] ソラミツ株式会社 (2016) ブロックチェーン技術の KYC への応用
https://www.boj.or.jp/announcements/release_2016/data/rel160526b8.pdf
- [37] 日本経済新聞 8/4/2017 付記事 (2017)
<http://www.nikkei.com/article/DGXXKO19634880T00C17A8EE9000/>
- [38] e-estonia ホームページ (2017) <https://e-estonia.com/solutions/business-and-finance/e-tax/>
- [39] 国税庁ホームページ 「e-Tax」 (2017) <http://www.e-tax.nta.go.jp/>
- [40] Fintricity 記事 (2017) 「Blockchain and Tax Fraud」 <http://www.fintricity.com/blockchain-tax-fraud/>
- [41] 日本経済新聞 6/29/2017 付記事「電子申請にブロックチェーン活用 政府、まず入札」
<http://www.nikkei.com/article/DGXLZO18244550Z20C17A6MM8000/>
- [42] https://www-935.ibm.com/industries/jp/ja/blockchain/what_can_blockchain_do_for_you.html
- [43] <https://wired.jp/2017/02/22/blockchain-startup-03-everledger/>
- [44] The Wall Street Journal 4/24/2017 「Dubai Aims to Be a City Built on Blockchain」
<https://www.wsj.com/articles/dubai-aims-to-be-a-city-built-on-blockchain-1493086080>
- [45] ブロックチェーンビジネス研究会 「Factom(ファクトム)とは? ―分散型データ記録プラットフォームの概要と将来性」 <http://businessblockchain.org/about-cryptocurrency-factom>
- [46] ハーバードビジネスレビュー 4/21/2017 「ブロックチェーンが 電子カルテに革命を起こす可能性」
<http://www.dhbr.net/articles/-/4809>
- [47] 野村総合研究所レポート 3/30/2017 「ブロックチェーンの技術的特徴と行政分野における 活用事例」 <http://www8.cao.go.jp/kisei-kaikaku/suishin/meeting/wg/toushi/20170330/170330toushi13.pdf>
- [48] bitFlyer ビットコイン 2.0 がもたらす変化について https://bitflyer.jp/discussion/tetsuyuki_oishi
- [49] <http://news.mynavi.jp/news/2017/04/26/195/>
- [50] <http://markezine.jp/article/detail/26424>
- [51] WIRED (2014) 「エストニア、国外にいても「電子居住」できる国」
<https://wired.jp/2014/12/11/estonia-eresidents/>
- [52] Forbes Japan (2017) 「キャッシュレス社会、最初に実現するのはインドか」
<https://forbesjapan.com/articles/detail/16786>
- [53] ビジネス+IT (2016) 「インドが、国民 ID や行政人員削減に「抵抗がない」理由 篠崎彰彦教授のインフォメーション・エコノミー (80)」 <http://www.sbbi.jp/article/cont1/32932>
- [54] ブロックチェーンビジネスコミュニティ (2017) 「ブロックチェーンは国家を超越するかー Bitnation とエストニアから見る未来国家」 <http://businessblockchain.org/blockchain-can-change-system-of-the-country>
- [55] Fintech online (2016) 「ブロックチェーンを株主総会の投票に? JP モルガンなどが投票システムの概念実証」 <https://fintechonline.jp/archives/101875>
- [56] Forbes Japan (2017) 「ブロックチェーンが 2020 年までに「破壊」する可能性がある 5 つの分野」 <https://forbesjapan.com/articles/detail/15821>
- [57] The Cointelegraph (2017) 「Blockchain Voting May Lead to Liquid Democracy Globally in 20 Years」 <https://cointelegraph.com/news/blockchain-voting-may-lead-to-liquid-democracy-globally-in-20-years>

- [58] AFPBB News 4/7/2007 付記事「＜07 仏大統領選挙＞電子投票は「大失敗」、トラブル多発に批判噴出・フランス」<http://www.afpbb.com/articles/-/2215392?pid=1535357>
- [59] ビットコインニュース 1/25/2017 付記事 「ブロックチェーンは電子投票の解になる」米 NASDAQ がエストニア政府と取り組む理由 <http://btcnews.jp/1dzp2r9610744/>
- [60] 経済産業省ホームページ (2017)
<http://www.meti.go.jp/press/2016/03/20170329004/20170329004.html>
- [61] ブロックチェーン技術の活用可能性と課題に関する検討会 (2017) ブロックチェーン技術の活用可能性と課題に関する検討会報告書
- [62] イノベーターを支援するための次世代知財制度に向けて (2016) 水野祐