平成２７年度　我が国経済社会の情報化・サービス化に係る基盤整備
（ブロックチェーン技術を利用したサービスに関する国内外動向調査）
報告書

平成 28 年 3 月

株式会社野村総合研究所

目 次

1　本調査の背景と目的

ビットコイン等の価値記録の取引に使用されているブロックチェーン技術は、その構造上、従来の集中管理型のシステムに比べ、
①『改ざんが極めて困難』であり、
②『実質ゼロ・ダウンタイム』なシステムを
③『安価』に構築可能
という特性を持つともいわれ、IoT を含む非常に幅広い分野への応用が期待されている。

我が国企業は個別に技術検証が始まった段階であり、あらゆる産業分野における次世代プラットフォームとなる可能性をもつ当該技術において、主導権を海外企業等に握られる恐れがある。

上記のような問題意識をもとに、本調査は、

- 数あるブロックチェーン技術の詳細とその優位性・課題を比較分析する
- 当該技術が活用されるべき有望分野を把握する
- 当該技術が社会経済に与えるインパクトを把握する
- 今後の当該技術を用いた産業促進に向けた政策の指針を得る

ことを目的とし、国内外のブロックチェーン関連企業と有識者へのヒアリングや、2 回の検討会を通して検討を行った結果をとりまとめたものである。

なお、本報告書の内容は、おおむね平成 28 年 2 月末までの情報に基づいている。ブロックチェーンの仕様や各サービスの提供状況などは刻々と変化しているため、ビジネス等への活用の際には必ず最新の状況を確認されたい。

2　本報告書で用いる用語と略語

本報告書で用いる用語および略語について、下記の通り定義する。

用語	説明
BTC	ビットコインの通貨単位として用いられる略号。
FinTech	Finance と Technology を組み合わせた造語。金融業に ICT 技術を応用して、新たなサービスやビジネスを生み出す技術や取り組み。
仮想通貨・暗号通貨	ビットコインなど、ネット上のみで価値が認識される情報を仮想通貨または暗号通貨と呼ぶ。
交換所・取引所	ビットコイン等の仮想通貨同士を交換したり、円やドルなどの法定通貨と交換したりするサービス。 FX（外国為替証拠金取引）のような差金決済取引を提供しているものもある。
コンセンサス	下記のコンセンサスアルゴリズムを用いて、トランザクションを正式なものと認め、さらにその結果を相互に確認するまでの一連の処理を指すものとする。
コンセンサスアルゴリズム	Proof of Work、Proof of Stake などを用いて、分散型台帳を相互承認していくためのアルゴリズム一般を指す。
電子署名	⇒p.7
トークン	ブロックチェーンに固有の仮想通貨のこと。ブロックチェーンで資産管理などを行う場合に、処理料として仮想通貨で手数料を支払う場合、その仮想通貨をトークンと呼んでいる。
ノード	通信ネットワークにおける中継点、分岐点、端末を指す。本報告書においては、ブロックチェーンのネットワークにおける端末として用いる。
ハッシュ値/ハッシュ関数	⇒p.7
パブリック **コンソーシアム** **プライベート**	「コンセンサス（ネットワーク参加者が同一の「台帳」を承認するプロセス）」への参加が誰でも可能であるか（パブリック）、限定されているか（コンソーシアム）、特定組織内の利用に限られるか（プライベート）によって分類する。 ⇒p.26
ビットコイン	仮想通貨のビットコインの構成する仕組み全体の呼称と

	して用いる。個別の要素を示すときは、「仮想通貨としてのビットコイン」「ビットコインのバリュー」などと要素を指定する語句をつける。
プルーフ・オブ・コンセプト（PoC）	「概念実証」とも訳され、新たなサービスやシステムの検討を行うために、簡易なシステムを構築して確認を行うこと。
ブロックチェーン	一般名詞としてのブロックチェーンの呼称として用いる。Ripple などのいわゆる distributed ledger なども含むものとする。ビットコインも含め、個別のブロックチェーンに言及する際は「ビットコインのブロックチェーン」「Ethereum のブロックチェーン」などと明示する。⇒p.11

略語	**元の用語**
BTC	→『用語の説明』参照
IoT	Internet of Things：インターネット・オブ・シングス
P2P	Peer to Peer：ピア・ツー・ピア　⇒p.9
PoC	Proof of Concept：プルーフ・オブ・コンセプト→『用語の説明』参照
PoI	Proof of Importance：プルーフ・オブ・インポータンス　⇒p.25
PoS	Proof of Stake：プルーフ・オブ・ステーク　⇒p.25
PoW	Proof of Work：プルーフ・オブ・ワーク　⇒p.9

3　ビットコインとブロックチェーンの成り立ち

本章では、ブロックチェーンを生み出した「すべての始まり」ともいえる、ビットコイン及びビットコインのブロックチェーンについて概説する。ビットコインの成り立ちの中で、どのようにブロックチェーンが生まれ、用いられているかを整理する。

3.1　Satoshi Nakamoto による論文

2008 年 11 月の末に、暗号技術者が情報交換する米国のメーリングリストにおいて、Satoshi Nakamoto を名乗る人物が、一本の論文についてメールをしたのが、ビットコインの始まりである[1]。「Bitcoin: A Peer-to-Peer Electronic Cash System」と題された論文において、Nakamoto は、ビットコインの特徴として、下記を挙げている[2]。

- 第三者機関を必要としない直接取引の実現
- 非可逆的な取引の実現
- 少額取引における信用コストの削減
- 手数料の低コスト化
- 二重支払の防止

メーリングリストでしばらく議論が行われたのち、2009 年 1 月に、最初のブロックが生成され、ビットコインおよびビットコインのブロックチェーンの運用が始まった。

その後、現在までビットコインのシステムは停止状態になったことはなく（ゼロ・ダウンタイム、等といわれる）[3]、米国だけでなく世界中に利用者が拡大している。日本では 2014 年初頭の交換所の破綻で注目を集めたが、2015 年に入り、FinTech の気運の高まりと共に、ブロックチェーンにも注目が集まるようになってきた。

---

[1] http://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html
[2] https://bitcoin.org/bitcoin.pdf
[3] 一時的に一貫性が失われたことはある。
https://github.com/bitcoin/bips/blob/master/bip-0050.mediawiki

3.2　ビットコインの特徴

ビットコインは、「仮想通貨」や「暗号通貨」などとも呼ばれ、ソフトウェアによって管理されるデータそのものに価値を見いだし、流通させているものであると解釈できる。

ビットコインと、法定通貨である貨幣及び紙幣、電子マネー（資金決済法における第三者型前払式支払手段）との比較を図表 3-1 に示す。ビットコインは、法定通貨や電子マネーのように明確な発行者がおらず、ビットコインというシステムそのものへの信頼が価値の裏付けとなっている。また、法定通貨や電子マネーと異なり、匿名ながら取引履歴が公開されており、履歴の追跡が可能であることも特徴的である。

図表 3-1　ビットコイン、法定通貨および電子マネー

特徴		ビットコイン	法定通貨（日本円）	電子マネー（第三者型前払式支払手段）
発行・管理	発行者	■システムが自動的に発行	■日本政府（通貨） ■日本銀行（紙幣）	■電子マネー事業者（第三者型前払式支払手段発行者）
	管理者	■P2P ネットワーク参加者が管理	■日本政府 ■日本銀行	■電子マネー事業者（第三者型前払式支払手段発行者）
価値	発行上限額	■決まっている（2,100 万 BTC）	■無し	■事前入金された金額（日本円）の範囲で発行
	価値の裏付け	■システムへの信用	■日本政府への信用	■供託された日本円（入金額の 1/2） ■電子マネー事業者への信用
送金処理	送金の方向	■双方向	■双方向	■一方向（利用者⇒加盟店）
	送金の処理時間	■約 10 分間隔でブロックを作成 ■約 60 分で確定と見なす[4]	■直接の受取であれば即時 ■長距離・大量だと時間がかかることもある	■加盟店に支払われるまで数日～1.5 ヶ月程度
	送金の手数料	■少額[5] ■送金者負担	■高額 ■場合によって両方負担	■受取者（加盟店）負担
匿名性	取引の匿名性	■取引履歴は明らかだが、匿名性がある	■高い	■低い（履歴は電子マネー事業者が管理）
	取引履歴の公開	■公開	■非公開	■一般に非公開

ビットコインは、2016 年 2 月末までに約 1526 万 BTC が発行され[6]、その価値は 66.6 億米ドル相当に達している[7]。これまでの価値のピークは 2013 年 12 月で、1BTC あたり 1100

4 「ビットコインは送金が早い」といわれることがあるが、銀行間の国際送金などと比較してのことであり、一般的な決済手段と比べるとむしろ遅い。

5 送金する額に応じてではなく、送金する際のデータ量に応じて手数料が決まる。そのため、少額の送金の場合には、手数料が割高になる場合もある。

6 https://blockchain.info/ja/charts/total-bitcoins

7 https://blockchain.info/ja/charts/market-cap

米ドルを超えるほどの値を付けた。その後、各国の規制の動きや、上述の交換所の破綻のように外部から攻撃される事例が続いたことなどから価値を下げ、2016 年 2 月末時点では 400 米ドル台前半で取引がされている。

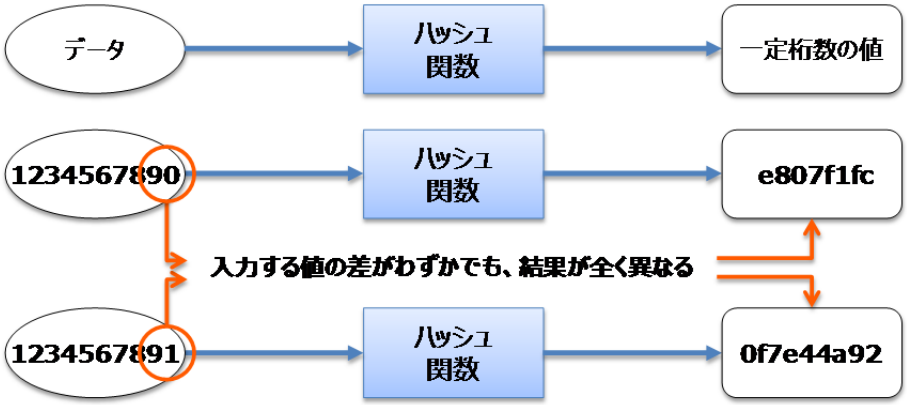
3.3　ビットコインを構成する技術

ビットコインは、既存技術の組み合わせにより、新たな機能が生み出されたと考えることができる。中央管理者なしに電子マネーのような仕組みを運営するためには、データの改ざんや二重支払を防止する措置とともに、悪意を持つユーザがいても、システムが維持される仕組みが必要となる。以下でビットコインを構成する主な個別技術（ハッシュ、公開鍵暗号と電子署名、P2P、Proof of Work）について概説する。

3.3.1 ハッシュ

「ハッシュ関数」にデータを入力すると、一定の桁数の値（ハッシュ値）が出力される仕組みであり、同じデータからは同じハッシュ値が得られるが、わずかでも異なるデータを入力すると、全く異なるハッシュ値が得られるのが特徴である。ハッシュ値から元のデータを推測するのは非常に困難とされる。この特徴を利用して、データの改ざんの検出などに用いられる。ビットコインでは、ブロックチェーンデータの連続性の検証・保証や、ハッシュ値の計算を利用した、Proof of Work によるブロックチェーンの生成に用いられている。

図表 3-2　ハッシュの仕組み

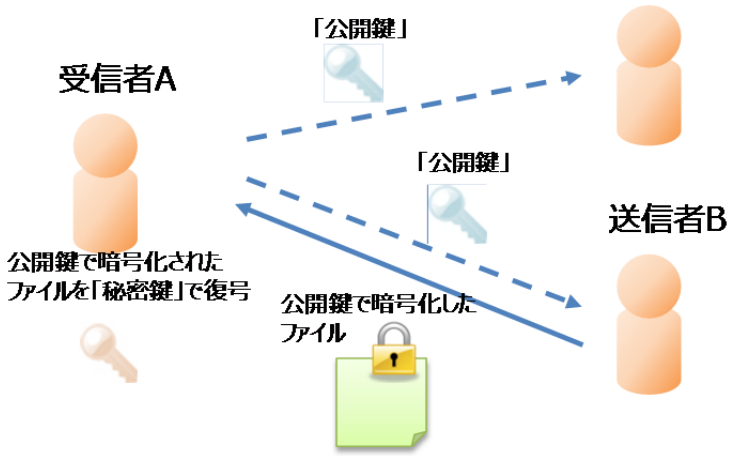


3.3.2 公開鍵暗号と電子署名

公開鍵暗号とは、暗号化と復号に別々の鍵を用いる暗号化方式である。鍵を「本人だけが用いる鍵（秘密鍵）」と「誰でも利用できる鍵（公開鍵）」の二つに分けることによって、鍵の受け渡し問題を解決した。暗号化と復号に同じ鍵を用いる共通鍵暗号の場合、鍵を相手のみに渡すために様々な安全対策が必要になる。それに対して、公開鍵暗号の場合は、

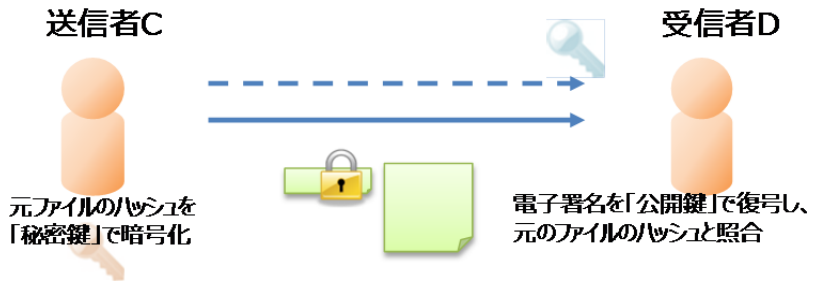
ファイルの授受を行う場合、あらかじめ受信者が両方の鍵をセットで作り、公開鍵を送信者へ配信しておくことで、安全な通信が可能になる。秘密鍵を自分が管理しておけば、公開鍵は別の人に使ってもらっても安全が保たれる。

図表 3-3　公開鍵暗号の仕組み



電子署名とは、ネットワーク経由で送信したデータが正しいものであることを証明する仕組みであり、公開鍵暗号で利用する鍵のペアをここでも利用する。一般的には、受信者へ送付するファイルのハッシュ値を送信者の秘密鍵で暗号化したものを電子署名とし、元のファイルと共に受信者へ送付する。受信者は、送信者と同じハッシュ関数を用いて元のファイルのハッシュ値を自ら生成し、送信者の署名を送信者の公開鍵で復号して得られるハッシュ値と照合することで、送信者の署名が正しいものであることを確認する。

図表 3-4　電子署名



公開鍵式暗号及び電子署名は、ビットコインではトランザクションデータ（ビットコイ

ン取引のデータ）の生成者の本人証明やビットコインのウォレット[8]のアドレス[9]として利用されている。

3.3.3 P2P

一般的なクライアント/サーバ型のネットワークでは、サーバがデータの保持・提供の役割を担い、クライアントはサーバに対してデータを要求・アクセスする。このクライアント/サーバ型では両者の役割分担は固定されている。これに対して P2P 型のネットワークでは、ネットワークに参加するノード（通信を行なう各コンピュータを指す。「ピア」とも呼ばれる）がそれぞれデータを保持し、他のノードに対して対等の関係でデータの要求と提供を行う自律的なネットワークを形成する。P2P 型ではクライアント/サーバ型と異なり、それぞれのノードはサーバまたはクライアントといった役割が固定されない。

P2P の実装においては、大きく分けて「検索方式」と、「データ伝送方式」を考える必要がある。検索方式とは、ノードやデータの所在の管理の方法であり、管理もすべて P2P で行う場合、インデックスサーバを設置する場合、処理力の高いノード（スーパーノード）が管理する場合などが代表的である。データ伝送方式とは、ノード間でのデータ伝送の方法であり、ノード間で直接送受信するか、他のノードを中継に使用するかに分かれる[10]。ビットコインで利用されている P2P は、検索方式は P2P であるが、データ伝送は各ノードを中継しながらおこなっている。

ビットコインにおいて、P2P は、完全分散型ネットワーク基盤の実現、Single Point of Failure（単一障害点）の解消に寄与している。また、後述するブロックチェーンのデータは、ビットコインの P2P ネットワークに参加し、マイニングを行うすべてのノードが同一のデータを保有することになっている。

3.3.4 Proof of Work

Proof of Work（PoW）とは、直訳すると「仕事の証明」となるが、これは一般的には「単純だが手間がかかる、ただし本当にそれを行ったことの検証は簡単な、特定の作業[11]をあえて行わせることにより、悪意のないことを確認する（不正を行う動機を低減させる）」とい

---

8 ビットコインの管理をするためのソフトウェア
9 ビットコインの送付先として指定する ID 番号
10 総務省データ通信課「ネットワークの中立性に関する懇談会　Ｐ２Ｐネットワークの在り方に関する作業部会」資料
http://www.soumu.go.jp/main_sosiki/joho_tsusin/policyreports/chousa/network_churitsu/pdf/wg2_061129_1_si_1_2.pdf
11 以下で説明するハッシュや、CAPTCHA のような画像を用いた例などがある。

う仕組みのことである。たとえば、メール送信では Hashcash[12]という PoW が用いられており、メールを送信する際に、一通毎に一定のハッシュ計算を課すことで、スパムメールの送信者を排除する（大量のメールを配信したいスパマーは、できる限り時間とコストを掛けたくない）、という手法である。

PoW は、ビットコインにおいては「発掘」「マイニング」とも呼ばれている作業である。ネットワーク参加者が、自分の手もとに届いているトランザクションデータの集合[13]に、ナンス（任意の値）を加えてハッシュ値を計算する。「特定の値より小さい値を求める」という条件が与えられており[14]、その値が得られるまで、ナンスの値を変えながら計算を続ける。誰かが求める値を得られたら、それが正しいことをネットワーク参加者で相互に確認したうえで、計算に用いられたトランザクションデータの集合を、新たな「ブロック」として、正式な取引結果と承認し、計算に成功した者に、報酬としてビットコインが付与される[15]。その後は、そのブロックに含まれなかったトランザクションデータと、新たに生成されたトランザクションデータとを用いて、全員が次のマイニングを開始する。

ビットコインでは、PoW により「中央管理者」の存在なしにデータの改ざんや二重支払を防止し、悪意の第三者がいても、システムが維持される仕組みを実現している。

図表 3-5　Proof of Work におけるハッシュ計算のイメージ

[12] http://www.hashcash.org/

[13] ビットコインの送付を行う際は、トランザクションデータを P2P ネットワーク全体に送信する。P2P ネットワークの状態などにより、ある時点で各ノードに到達しているトランザクションデータは異なる場合がある。

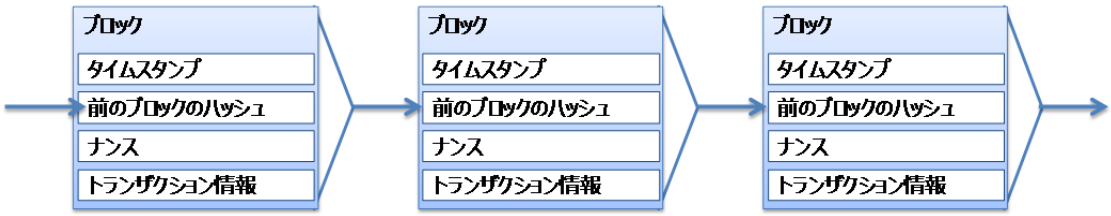
[14] 10 分程度計算し続けると誰かが発見できるように自動的に設定される。

[15] 報酬額は、現在は 25BTC＋ブロックに取り込んだトランザクションの手数料の総額となっている。約 4 年毎に、報酬額（上記の 25BTC）が半減することになっており、次回は 2016 年夏頃とされる。

3.4　ブロックチェーン

PoW により生成されたブロックのつながりがブロックチェーンである。一定期間（ビットコインでは約 10 分間）のトランザクションデータをまとめたブロックを、チェーン状に繋げている。ブロックにはタイムスタンプ、一つ前のブロックのハッシュ値、ナンス、生成されるブロックに含むトランザクションの情報等が含まれている[16]。

図表 3-6　ブロックチェーン



ビットコインのブロックチェーンにおいては、P2P ネットワーク上の二つ以上のノードで、ほぼ同時に PoW に成功したノードが出現した場合などに、一時的に枝分かれ（Fork：フォーク）が発生することがある。その場合、それ以降により早く、長くブロックがつながった方を正当なものと判定する（図表 3-7）。そのため、ある取引が成立したとみなすためには、その取引のトランザクションデータがブロックに取り込まれてから、それ以降に複数のブロックが生成された後に、そのブロックチェーンがフォークしていないことを確認する必要がある。一般的には、6 ブロック程度が生成されれば正当なブロックであるとみなすことが慣習として行われている（ビットコインを管理するウォレットに判定機能として組み込まれていることが多い）[17]。

このように、ブロックが過去の情報を保持した状態で繋がれていくため、ビットコインのブロックチェーンにおいて不正な取引を成立させるには、正当なフォークよりも早くブロックを成立させ続けるか、過去のブロックを全て作り直す必要があり、PoW に参加するすべてのコンピュータのマシンパワー（計算能力）の 50%より大きな割合を確保する必要があるとされる[18]。また、この仕組みにより、後述するビザンチン将軍問題を実用可能な範

---

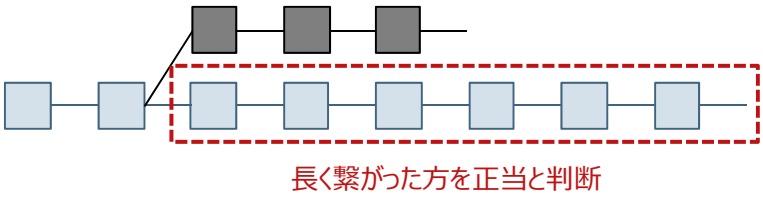
16 より正確には、ブロックにはトランザクションのデータのほか、技術情報、直前のブロックのハッシュ値、マークルルート、PoW のターゲット値、ナンス、タイムスタンプ、ナンス、が含まれている。
https://bitsonblocks.files.wordpress.com/2015/09/bitcoin_blockchain_infographic1.jpg

17 1 ブロックの生成に約 10 分かかることから、6 ブロックで約 1 時間となる。

18 「51%以上」と表記されることも多いが、「50%より大」を整数に丸めた表現であり、正確ではない。ただし、「51%アタック（51%攻撃）」は、ブロックチェーンへの攻撃の名称として一般化しているため、以下でもそのまま用いる。

囲で解決したとされている。

図表 3-7　ブロックチェーンにおけるフォークの様子

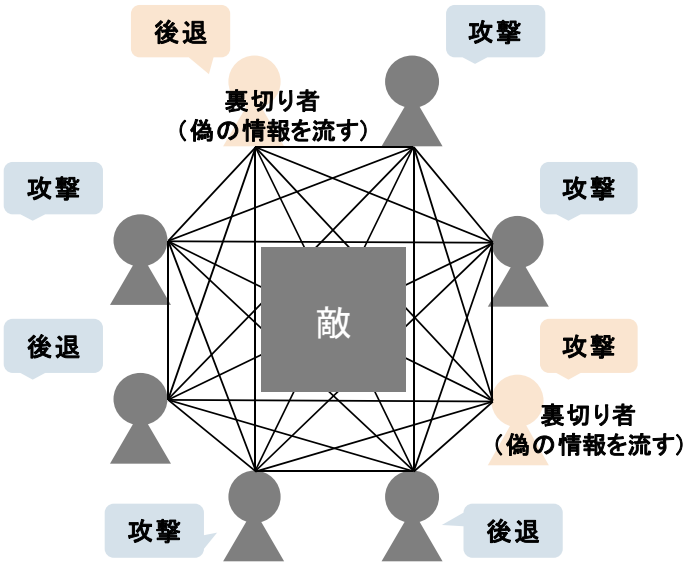


3.4.1 ビザンチン将軍問題

ビザンチン将軍問題とは、Leslie Lamport らにより 1982 年に発表された論文「The Byzantine Generals Problem」[19]にて議論されている、分散システム上におけるコンポーネント[20]群における、信頼性に関する問題である。

互いに敵国を取り囲む「将軍」たちが、彼らの中に「偽の情報を流す裏切り者」が存在する状態で、相互に通信し合うことのみにより、戦略の合意形成に至ることが可能かという考えから、分散システム上におけるコンポーネント群のいずれかが偽の情報を伝達する場合に、全体として正しい合意を形成できるかを問うているものである。

図表 3-8　ビザンチン将軍問題



19 http://research.microsoft.com/en-us/um/people/lamport/pubs/byz.pdf
20 ノードやピアとほぼ同義。ここでは論文にならってこの用語を用いる。

Lamport らによれば、全コンポーネント数のうち、偽の情報を流すコンポーネントが 1/3 未満であれば、解が存在する、つまり全体として正しい合意を形成できるとしている。つまり、参加者の総数における偽の情報を流す参加者の割合が、全体の合意可否を決定している。

ビットコインのブロックチェーンにおいては、全体の合意 ＝ 正しいブロックチェーンの決定を、PoW とその結果の相互承認によって得ている。前述の通り、ビットコインブロックチェーンにおいては、ブロックが過去の情報を保持した状態で繋がれていくため、不正な取引を全体の合意として成立させるには、正当なフォークよりも早くブロックを成立させ続けるか、過去のブロックを全て作り直す必要がある。これには、全体の 50%より大きなマシンパワーが必要とされており、膨大な計算機資源を必要とする。それよりも、正当にマイニングを行って、マイニングによる報酬を得ることのほうが経済合理性が高いため、不正な取引を行うモチベーションが低くなる。この仕組みにより、ビザンチン将軍問題を実用可能な範囲で解決したとされている。

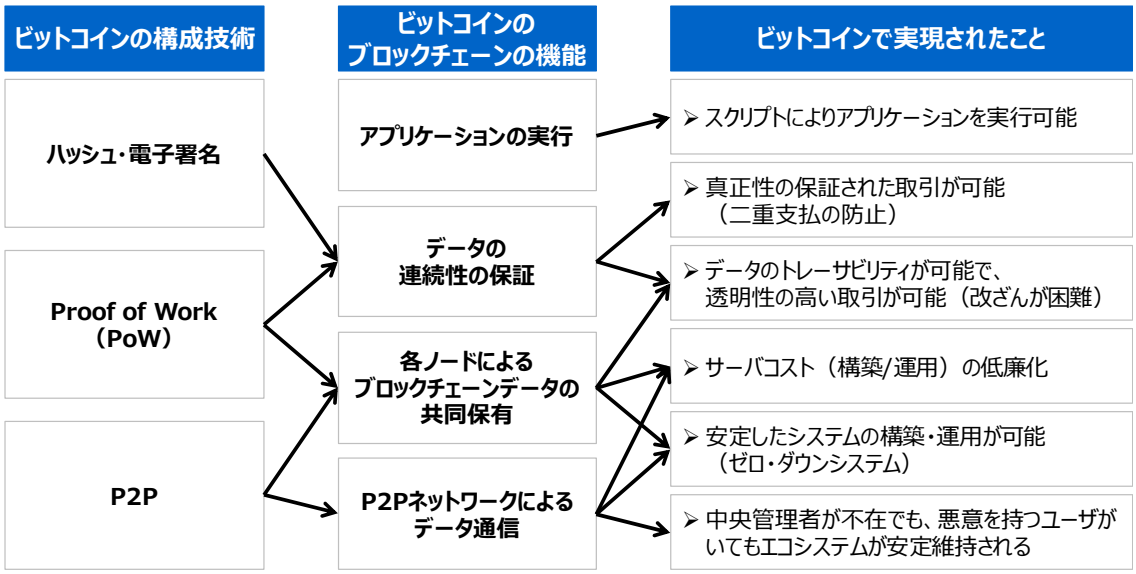
3.4.2 ビットコインブロックチェーンの機能と実現されたこと

ビットコインは、「ハッシュ・電子署名」「PoW」「P2P」といった主な技術により構成されている。用いられている個々の技術に関しては、新規性は殆どないものの、既存の技術の組み合わせにより、ビットコインブロックチェーンにおいて新たな機能が生み出されていると考えることができる。

これにより、中央管理者なしに電子マネーのような仕組みを運営するために必要な、データの改ざんや二重支払を防止する仕組みとともに、悪意を持つユーザがいても、システムが維持される仕組みが形成された。

ビットコインのブロックチェーンの機能は、大きく「アプリケーションの実行」「データの連続性の保証」「各ノードによるブロックチェーンデータの共同保有」「P2P ネットワークによるデータ通信」の 4 つに分類される。これら機能の概要、およびその元となる構成技術を、図表 3-9 に示す。

図表 3-9　ビットコインのブロックチェーンの機能



ビットコインブロックチェーンにおいては、各ノードが P2P ネットワークに接続されている。それにより、クライアント/サーバ型のシステムよりも、高い対障害性が実現されている。それら P2P ネットワークで接続された各ノードが、PoW を経てコンセンサスが得られているビットコインブロックチェーンデータをそれぞれ保有している。

ビットコインブロックチェーン上では、ハッシュ計算と電子署名を連続的に行うことで、ブロック同士（及びブロック内のデータ）が関連づけられている。また、PoW を経て各ブロックのコンセンサスが得られることにより、ビットコインブロックチェーンデータの追跡と検証が可能となっている。

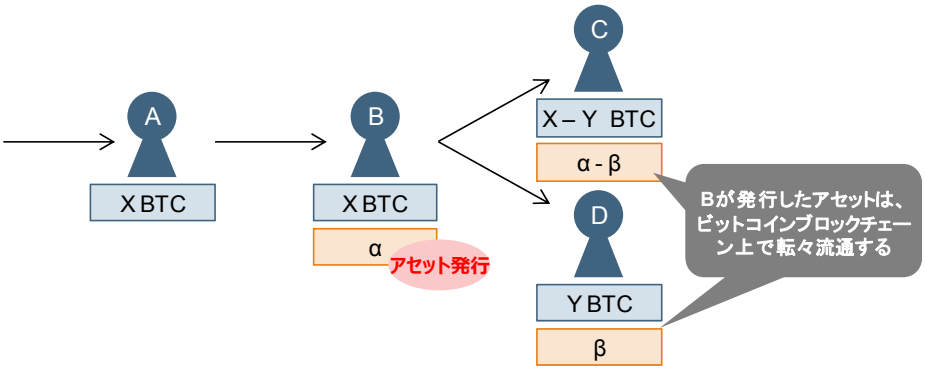
これらの機能により、ビットコインのブロックチェーンでは、中央管理者が不在でも、悪意を持ったユーザがいた場合でもエコシステムを安定維持できるようになり、安定したシステムの構築と運用を可能としている。その結果として、対象とするシステムにも拠るが、一般論としてサーバコスト（構築と運用）の低廉化を可能とするとの意見がある。また、真正性の保証された取引が可能となり、後から検証可能な透明性の高い取引が実現されている。

さらに、ビットコインブロックチェーン上では、専用のスクリプトによって様々な処理を実行可能である。代表的なアプリケーションとして、Colored Coins が挙げられる[21]。Colored Coins は、ビットコインに資産情報など（電子化された債権、デジタルコンテンツ、電子化された実物資産の権利情報など）の「色」を付けることで、ビットコイン上でその資産を転々流通させることが可能な技術である。Colored Coins に発展的に汎用性を持たせ

[21] http://coloredcoins.org/

たのが、Open Assets Protocol である。Open Assets Protocol においては、ビットコインブロックチェーンの利用者が主体となって任意の資産を流通させることが可能となる。Open Assets Protocol や Colored Coins では、それぞれの「色」を識別するための ID が割り振られている。

図表 3-10　Open Assets Protocol の概要図



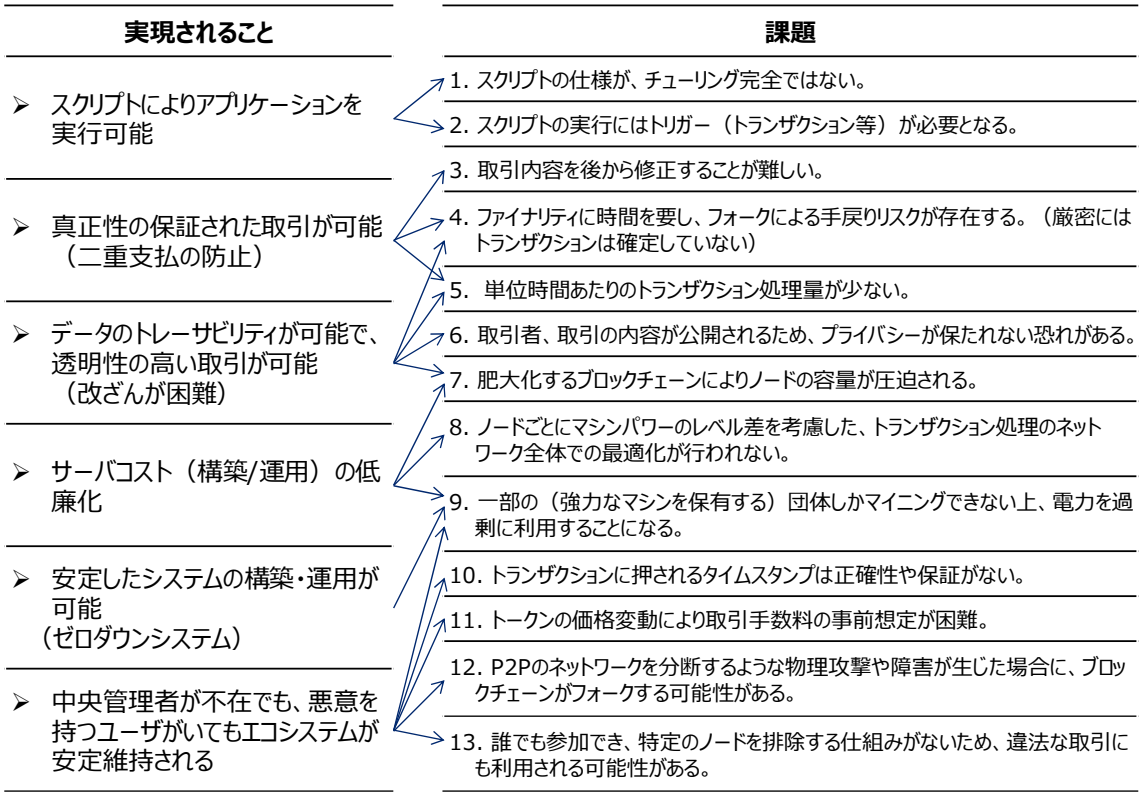
3.5　ビットコインのブロックチェーンの課題

ビットコインのブロックチェーンは、既存の技術を組み合わせることで、中央管理者がいなくても有効に機能する仕組みを実現した非常に画期的なアイデアだが、利用が拡大する過程で各種様々な課題が浮き彫りになってきている。ここでは、ビットコインブロックチェーンが実現した機能に内在する課題を整理する。

前述したビットコインの主要な 4 つの機能より導出したビットコインのブロックチェーンにて実現されることより、ビットコインブロックチェーンにおける 13 の課題を導出した。

実現されることと、広範にビットコインが利用されることによって顕在化した課題の相関を示したのが図表 3-11 である。

図表 3-11　ビットコインのブロックチェーンにおける課題



上記の 13 の課題は、「システムの仕様と実装に起因する課題」、「実ビジネス慣行とのギャップに起因する課題」および「ビットコインブロックチェーンの数理的・情報科学的課題」の 3 つに分類可能である。「システムの仕様と実装に起因する課題」については、課題が広範囲に及ぶため、さらに「スクリプトの実装に起因する課題」「ファイナリティに起因する課題」「P2P システムに起因する課題」に大別した。

3.5.1 システムの仕様と実装に起因する課題

(ア)「スクリプトの実装」に起因する課題

ビットコインのブロックチェーンには、トランザクションの一部に自動的に処理を行わせるためのスクリプト（処理命令の文字列）を記述することが可能となっている。これにより、仮想通貨の授受だけでなく、様々な資産の管理などにブロックチェーンを拡張して利用することが可能になっている。しかし、一般的なコンピュータ言語では、「チューリング完全性[22]」という論理的な処理能力を満たしていることが求められるが、ビットコインブロックチェーンでは、このチューリング完全性は満たせないことが知られている。そのため、これらの処理には一般のスクリプトとは異なった制約が存在する。例えば「ループ」と呼ばれる処理などが代表例である。ループ処理とは、ある一定の条件を満たすまで特定の処理を連続して行なう命令をさす（一番単純な例では、1 から 10 までを順に足す処理などがあげられる）が、このようなループ処理はビットコインブロックチェーンでは一つのブロック内で行えないことが知られている。(課題 1)

(イ) ファイナリティに起因する課題

ビットコインブロックチェーンは、各ブロックが参加者から承認され、正当な取引記録としてコンセンサスが得られるまでに、10 分から 60 分程度の時間が必要とされる。時間の長短はその時のブロックのマイニングの状況に依存する。特に、ブロックがフォーク（同時に二つ以上のブロックチェーンの系列が生じた場合など）した場合、このフォークを解消するには 60 分程度の時間が必要とされる。この「取引が正当なものとして認定される」ことを「ファイナライズ」、これらの一連の過程を「ファイナリティ」[23]と呼ぶが、このファイナリティにある一定の時間が必要な点は実ビジネスへの応用に制約をもたらす可能性がある。実際のビットコインの取引では、ウォレットの管理者による設定にも依存するが、6 回程度の後続ブロック生成が行われたことをもってファイナリティが行われたとみなしている。その間にフォークし、手戻りするリスクを考慮してのことだが、厳密には、どれだけブロックチェーンが連なったとしても、フォークする確率がゼロにはならないため、トランザクションが取り消されるリスクも非常に小さな確率で残る。

ひとつの思考実験として、自動販売機へのブロックチェーン適用問題がある。現行の自

---

[22] チューリングマシン（Alan Turing により考案された仮想的な計算機、http://kitchom.ed.oita-u.ac.jp/jyo/proh09/mkiribu/kaisetu.html）が計算できる問題全てが記述、計算でき、もしメモリが無限にあり、計算時間が無限にかかって良いならば解けることをチューリング完全という。
（http://www-hiraki.is.s.u-tokyo.ac.jp/lectures/prog_giho/3.pdf）

[23] 決済の完了を指す。

動販売機はその自動販売機に現金を入れてボタンを押した場合、自動販売機は投入された金額が商品の売価を満たしている時には即時に商品を排出する。一方、ブロックチェーンで管理されている自動販売機の場合、現金を自動販売機に投入した時点で、まず現金が投入されたことをブロックチェーンに記載し、そのブロックが承認されるまで処理を待つ必要がある。この承認までのコンセンサスプロセスはビットコインブロックチェーンでは最短で 10 分程度の時間を有する。そして投入金額が確定した時点で今度はボタンを押すことになるが、この注文処理もまたビットコインブロックチェーン上に記録する場合、これにも同様の時間が必要となる。さらにその注文処理が実際に正確に履行されたか、お釣りはいくらか、といった各工程それぞれがブロックチェーンでのコンセンサスを必要とするような場合、それぞれの処理に 10 分以上の時間が必要だとすると、そのような取引は実ビジネスでは成立しないであろう。このように即時性が要求される取引にはビットコインブロックチェーンは向いていないとの指摘がある（課題 2）（課題 4）

また、実ビジネスではその取引が行われた日時が正確にいつであったかを特定し、記録することが重要となるケースが考えられる。しかしビットコインブロックチェーンでは、取引が記録されるトランザクションに押されるタイムスタンプは、その取引が発生した時刻ではなく、新しいブロックが生成されるタイミングとなる。新しいブロックが生成されるタイミングは、それ以前の複数のブロックの時間および各ノードから承認の応答があった時間に左右されるため、実際の取引時間とは異なる時間が記録される可能性が高い。さらに、各ノードのもつ時刻については、TSA（Time-Stamping Authority）[24]の利用や TAA(Time Assessment Authority)[25]などとの連動が必須とされていない。そのため、タイムスタンプの時刻も正確である保証はない（課題 10）。

（ウ）P2P システムに起因する課題

ビットコインのブロックチェーンは、P2P の分散システムで情報を保持するため、各ノードそれぞれがこれまでのトランザクションデータが全て含まれたブロックチェーンを保有することになる（2016 年 2 月末時点で、ビットコインブロックチェーンでは 60GB 超のデータを各ノードが保有している[26]）。現行のビットコインブロックチェーンのような、すべての取引内容を保存する仕組みでは、ノードの容量が圧迫されることとなる。そのため、例えばモバイル端末などの比較的容量が少ないノードがビットコインブロックチェーンへ参加することは難しい。また、今度普及が予測される IoT のような、より処理能力、データ保存容量が少ないノードが想定されるネットワークでは、現行のビットコインブロックチェーンは応用が難しい可能性が指摘されている（課題 7）。

---

[24] 時刻認証局。信頼できる第 3 者としてタイムスタンプを発行する。
[25] 時間配信局。タイムスタンプサーバーが UTC（協定世界時）と規定の精度以内で同期できているかの監査を行う。
[26] https://blockchain.info/ja/charts/blocks-size

さらに、ビットコインブロックチェーンは、各ブロックに保存できるトランザクション件数の上限がおおよそ定められていることと（約 1,000 件程度が上限）[27]、新たなブロックが生成される時間間隔がおおよそ決まっている（おおよそ 10 分間隔）ことから、1 秒間に処理できるトランザクション件数が 5~7 件程度といわれている。現状のビットコインの利用量では、まだ問題は顕在化していないが、将来的に利用が拡大した場合に処理能力が足りなくなり、処理が遅延する可能性が指摘されている[28]。参考までに、大手クレジットカードネットワークである VISA の決済システムは、平均して毎秒 3,600 件[29]、ピーク時の処理能力は毎秒 65,000 件以上の決済処理能力を有している[30]（課題 5）。

一方、P2P でシステムを構成するビットコインブロックチェーンでは、P2P を構成する各ノード間のネットワークを分断するような攻撃が行われるリスクが常に存在する。仮にネットワークが分断された場合、ノード間においてブロックチェーンデータの同期が行われない、もしくは同期が遅延する可能性がある。ネットワークが分断されている間に新たなブロックの生成が続けられてしまうと、一方のノードでは正とされたブロックチェーンデータが、他のノードでは正とされない可能性がある。これは分散システム上では「エクリプス問題」として知られているが、ビットコインブロックチェーンでの解決方法が確立されていないのではないかとの指摘がある（課題 12）。

ビットコインのシステムでは、参加している各ノードそれぞれのマシンパワーに差がある。各ノードのマシンパワーがほぼ等しい分散システムでは、それぞれのノードの状況に応じて処理の分配を最適化する仕組みを導入することが可能だが、ビットコインブロックチェーンでは、マシンパワーが異なる各ノードで構成されるネットワーク全体の最適化を行う事は難しい。そのため、計算の重複などのロスが発生している可能性が指摘されている（課題 8）。

現行のビットコインブロックチェーンは、各ブロックのトランザクションデータのコンセンサスのために大量のマシンパワーが必要となる仕組みを採用している。PoW に参加しているノードは「マイナー（採掘者）」と呼ばれ、ビットコインのマイニング専用のコンピュータを備えた専門業者が多くのシェアを占めている。これらの一部の専門業者がほぼ独占的にビットコインブロックチェーンの PoW を行っているのが現状である[31]。また、PoW に使用される計算資源としては計算に使用されるコンピュータと、そのコンピュータで使

---

27 実際には、ブロックの容量が約 1MB となるように調整されている。

28 すでに遅延が発生し始めているとの指摘もある。

29 2015 年 10 月から 12 月の平均値。
http://s1.q4cdn.com/050606653/files/doc_financials/2016/Q1/Visa-Inc.-Q1-2016-Financial-Results-Conference-Call-Presentation.pdf

30
http://s1.q4cdn.com/050606653/files/doc_financials/2016/Q1/Visa-Inc.-Q1-2016-Financial-Results.pdf

31 https://blockchain.info/ja/pools

用される電力が含まれるが、電力に関しては 2013 年時点で一日あたり 15 万ドルに上るとの推計も発表されている[32]。このような資源の浪費を懸念する声は強い（課題 9)。

さらに、現行のビットコインブロックチェーンには、どのようなノードであっても参加可能である一方で、そのような仕組みの裏返しとしてある特定のノードを排除できるような仕組みがない。したがって、上述したようなネットワークを分断するようなノードを事前・事後で排除する仕組みが存在しない。また、ある一定以上の（たとえばネットワークに参加しているノード全体のマシンパワーの 50%より大きな割合を占めるような）マシンパワーを持つノードが不正にブロックを書き換えるような行為を選択することも理論上は可能となるが、このような違法な取引を行おうとするノードを排除することもできない（課題 13)。

3.5.2　実ビジネスの慣行とのギャップに起因する課題

ビットコインのブロックチェーンでは、改ざんに対する耐性が強い反面、一度ブロックに取り込まれたトランザクションデータの内容を書き換えることが非常に難しいという性質を持つ。そのため、ビットコインブロックチェーンを活用して取引内容を記録した際には、一度トランザクションが確定した後に、遡って後からその内容を修正することが難しい。そのため、内容を修正することが生じ得る取引に利用することは難しいほか、個人のプライバシーのような公開したくない情報を取り扱う場合には、慎重な対応が必要となる（課題 3)。

これに関連して、現行のビットコインブロックチェーンでは、各ブロックに記録されたトランザクション部分は全ての取引内容が誰でも確認できる状態となっていることも問題となりうる。各取引の送り先・受け手に関しては、匿名のアドレスが用いられるものの、取引内容はすべて公開されている（アドレス A からアドレス B にいつ、いくらの金額が送金されたかはすべて公開されている)。このように取引記録がすべて公開されると、ビジネス上秘匿したい取引内容や、プライバシーに関わる取引を行なうことが難しい可能性がある。例えば、競合他社に受注金額を知られたくない取引などは、ビットコインブロックチェーン上では秘匿できない可能性がある[33]。また、病院への診察の支払などの情報もビットコインブロックチェーン上では特別に秘匿されるわけではない。匿名のアドレスの利用を前提としても、長期の履歴から個人が特定される可能性はゼロでない為、プライバシー保

---

[32] http://www.bloomberg.com/news/articles/2013-04-12/virtual-bitcoin-mining-is-a-real-world-environmental-disaster

[33] 同一のビットコインアドレス（あるいは同一の IP アドレスで利用されている複数のビットコインアドレス）の取引履歴を時系列に多数追跡することで、利用者を特定できる可能性がある。

護の観点から懸念が指摘されている（課題 6)。

一般の取引ではその取引に起因する手数料が必要なケースが多い。例えば銀行口座への振込手数料や為替の手数料などである。これらの手数料は一般に定額・定率のものが大半であり、取引に際して予測可能である。しかしビットコインを用いた取引の場合、ビットコインの価値が変動する（トークンとしての価値が変動する）ため、事前に取引手数料の予測が困難となる可能性が指摘されている。これらの取引手数料が変動することは、税務上の処理を煩雑化させるなどの副作用も考えられる（課題 11)。

3.5.3　ビットコインブロックチェーンの数理的・情報科学的課題

より根本的な問題として、情報理論上、「各ノードにおいて時刻が一致していない分散システムにおいては、ある情報が正しいと確認できるようなコンセンサスを実現することは不可能である」との証明が存在し、ビットコインブロックチェーンもこの証明を逃れることはできない。現在のビットコインブロックチェーンは、この証明の条件を一部ゆるめた環境下でコンセンサスを実現していると見るべきである[34]。

同様に、分散型システムに関して、一貫性、可用性、分断耐性を同時に満たすことはできない、という CAP 定理も知られている。この定理に従うと、ビットコインのブロックチェーンでは一貫性は満たせないことになる。

CAP 定理

CAP 定理は、2000 年に The Symposium on Principles of Distributed Computing にて Eric Brewer により予想され、2002 年に Seth Gilbert、Nancy Lynch により証明された、共通のデータを扱う複数ノードで構成された分散システムに関する定理である。分散システムは下記の 3 つの性質のうち、完全に満たせるものは 2 つのみであることが示されている。

- C（Consistency、一貫性 : 全てのノードで最新のデータを同時に保持していること。そのため、各ノードによる読み出しは直前の書き込みの内容を返す状態となっていることを指す。）
- A（Availability、可用性 : 特定のノードの障害により、他のノードが影響を受けない状態であること。そのため、各ノードは必ず有限時間内に応答する状態にあることを指す。）

[34] 分散システムにおけるコンセンサスは、FLP impossibility Theorem（非同期システムでは、ノードが 1 台でも停止する可能性がある場合、100%合意に至るコンセンサスアルゴリズムは存在しないとする定理。Michael J. Fischer, Nancy A. Lynch, Michael S. Paterson により 1985 年に提唱された。）を前提とする。そのため、条件を絞った上で成立しているものとされる。

- P（Partition-tolerance、分断耐性：ネットワークに障害などがあっても継続して動作すること。そのため、各ノードはネットワークが分断されても動作する状態にあることを指す。）[35]

分散システムの 1 つであるとみなされるビットコインブロックチェーンは、A（Availability,可用性）、P（Partition-tolerance,分断耐性）を満たすことはできるものの、C（Consistency,一貫性）を満たすことができていない。代わりに、ネットワーク分断が有限時間内に解消される場合においては、結果整合性を保持していると考えられている[36]。結果整合性とは、時間的な差はあるにせよ、結果的に一貫性が保たれる（保たれればよい）とする考え方である。

[35] 第 2 回検討会における委員資料より引用

[36] ビットコインブロックチェーンにおいては、ネットワーク分断を検証する仕組みが搭載されていないため、必ず結果整合性を保持すると保証されているわけではない。

4　ブロックチェーンの応用

3.5 章で整理したとおり、現段階ではビットコインブロックチェーンには様々な課題が存在する。その一方で、これらの課題を解決もしくは回避した上で、様々なビジネス領域に適用しようとする動きも活発に起きている。本章ではこれらの取組を「ブロックチェーンの応用」という視点から整理する。

「システムの仕様と実装に起因する課題」のうち、「スクリプト実装に起因する課題」については、チューリング完全なスクリプトを実装したブロックチェーンが開発されている。「ファイナリティに起因する課題」では、コンセンサスに関するアルゴリズムを工夫することでファイナリティの効率化・高速化を実現するための取り組みが行われている。また、「P2P システムに起因する課題」に対しては、参加者を選択・制限することで上記の課題を解消しようとする検討がなされている。

一方、「実ビジネスとのギャップ」の存在が認知されたことで、あらゆる取引にブロックチェーンが適用できるといった「ブロックチェーン万能説」をより冷静に検討する機運も高まっている。ブロックチェーンの効果と限界を見極めつつ、どうすれば「ギャップ」を埋めることが可能かという検討が現在活発に議論されている。

また残された課題として、「ブロックチェーンの数理的・情報科学的な課題」が存在する。この課題に対してどのような取組が行われているのか、またどのような取り組みが求められているのかは、本章で簡単に触れた後、主に 6 章で整理する。

4.1　ブロックチェーンの応用

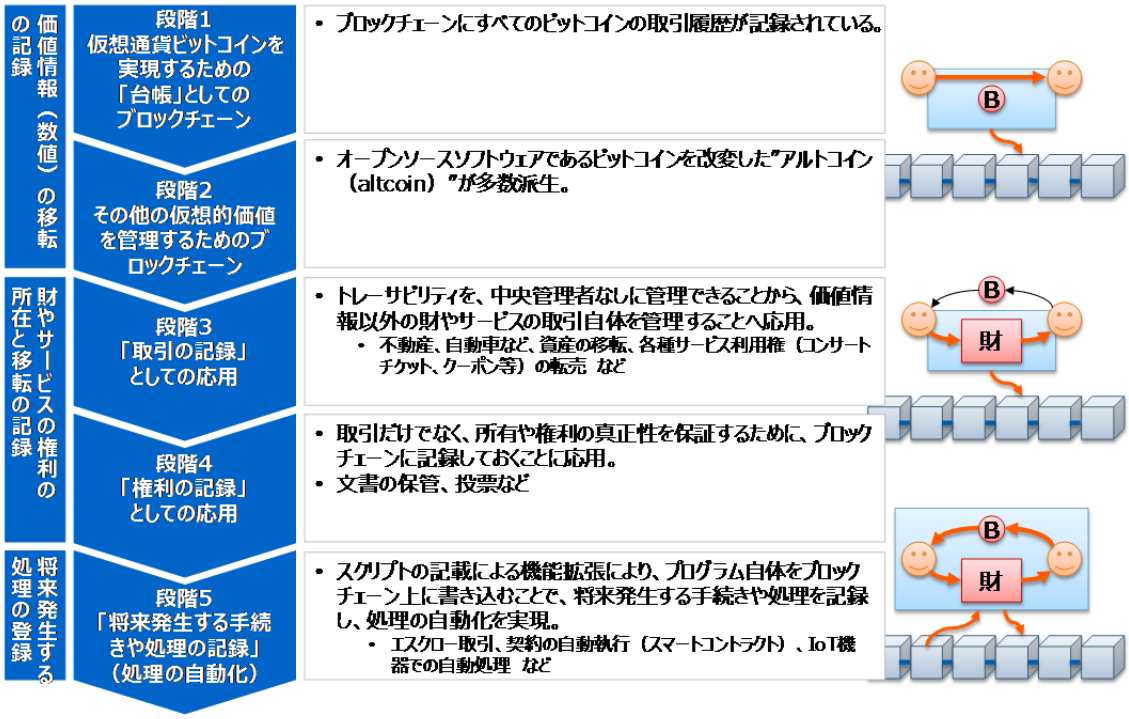
ビットコインを発端として、様々なブロックチェーンが提案されている。3.5 章に挙げた様々な課題を解決しながら、ブロックチェーンの機能が拡張され、多様な用途に応用されようとしている。

ブロックチェーンの拡張の方向性として、大きく 3 つの軸が考えられる。一つは「ブロックチェーン上での記録・交換対象の拡張・汎用化」である。価値情報だけでなく、様々な財の所有権やサービス（役務提供）を受ける権利（所有権、利用権など）の移転や証明にもブロックチェーンを応用しようという動きである。二つ目は、「コンセンサスアルゴリズムの改変・高性能化」である。ビットコインの PoW の課題に対応した、新たなコンセンサスアルゴリズムを採用する動きである。三つ目は「ネットワークへの参加を制限し、参加者の信頼度を向上」する方向性である。不特定多数に参加を認めるのではなく、ある程度制限を掛けることで、コンセンサスの効率化とトランザクション処理の高速化を目指している。

4.1.1 ブロックチェーン上での記録・交換対象の拡張・汎用化

トレーサビリティや真正性の保証ができる機能や、スクリプトの機能を活用して、仮想的価値の交換にとどまらず、様々な取引の記録や、何らかの権利や主張も、ブロックチェーンで管理する、というアイデアへと発展している。

図表 4-1　ブロックチェーン上での記録・交換対象の拡張・汎用化



(ア) 段階 1　　仮想通貨ビットコインを実現するための「台帳」としてのブロックチェーン

3 章で見たとおり、ビットコインのブロックチェーンにはすべてのビットコインの取引履歴が記録されている。ここでは、ブロックチェーンは仮想通貨であるビットコインの台帳として機能しているのみであった。

(イ) 段階 2　　その他の仮想的価値を管理するためのブロックチェーン

ビットコインは、オープンソースソフトウェアとして開発されている。そのため、ビットコインの有用性や可能性が認められると、様々なパラメータや暗号化のアルゴリズムな

どを改変した”アルトコイン（altcoin）”が多数派生した。その数は 600 以上にのぼる[37]。

(ウ) 段階 3　　「取引の記録」としての応用

ブロックチェーンが、取引の記録を、中央管理者なしに管理できることが認識されると、仮想通貨などの価値情報だけでなく、財やサービスの取引自体を管理することへ応用する動きが発展した。不動産、自動車など、資産の移転、各種サービス利用権（コンサートチケット、クーポン等）の転売などに応用する等のアイデアが現れた。

(エ) 段階 4　　「権利の記録」としての応用

取引だけでなく、所有や権利の真正性を保証するために、ブロックチェーンに記録しておくことに応用するという段階である。文書の保管、投票などに利用することが想定されている。

(オ) 段階 5　　「将来発生する手続きや処理の記録」（処理の自動化）

スクリプトの記載による機能拡張により、プログラム自体をブロックチェーン上に書き込むことで、将来発生する手続きや処理を記録し、処理の自動化を実現することを目指す動きが活発化している。

エスクロー取引、契約の自動執行（スマートコントラクト）、IoT 機器での自動処理などが検討されている。

4.1.2 コンセンサスアルゴリズムの改変・高性能化

ビットコインのブロックチェーンの課題のうち、

- ビットコインの PoW は、10 分間単位になっており、即時性が求められる処理に向かない。
- 1 ブロックのサイズが 1MB 程度であり、大量のトランザクションを捌けない。
- 大量のマシンパワーを必要とするため、エネルギー効率が悪い。
- ネットワークの参加者の 50%より大きなマシンパワーを占有されると、ブロックチェーンのコントロール（改ざん等）が可能になる。

等に対応し、代替するアルゴリズムが提案されている。

[37] https://coinmarketcap.com/currencies/views/all/

(ア) Proof of Stake（PoS）

仮想通貨の保有割合などに応じて、ハッシュ計算の優先権を与える方法。

大量の仮想通貨を持つノードが不正を働くと、自ら仮想通貨の信頼を低下させ、価値を下げることになるため、不正をしないインセンティブが働く、という考え方。ただし、ブロックチェーンを不正に操る方法がいくつか指摘されており、それらへの対策が必要となるとされる[38]。Ethereum、Bitshares、NXT 等に採用されている。

(イ) Proof of Importance（PoI）

ノードごとの取引額・残高を指標とした取引グラフ分析[39]により、残高と取引状況をクラスタリング[40]して、個別のノードの重要性を計算し、より重要なノードにハッシュ計算の優先権を与える（より難易度の低いハッシュ計算問題を割り当てる）方法である。また、クラスタリングにより、違法な取引を行う可能性のあるノードを検出することも可能とされる。NEM で採用されている。

(ウ) Practical Byzantine Fault Tolerance（PBFT）

「ビザンチン将軍問題」に起因する合意形成の失敗による「ビザンチン障害」を解決するためのアルゴリズム。理論上での解決アルゴリズムは計算量が膨大になるため実用化が難しいとされていた。1999 年に合意形成の可否を判定する際に微小なラグを加える事で「ビザンチン障害」を回避できるとする「実用的（Practical）」なアルゴリズムが提唱され[41]、現在ブロックチェーンへの応用が進められている。

ノードの総数が既知で、不正ノード数の上限が決められるなどの条件が必要であり、パブリックなシステムへの適用は難しいとされる。Ripple や Stellar で採用されており、Orb でも今後採用する予定とされている。

4.1.3 ネットワークへの参加を制限し、参加者の信頼度を向上

ネットワークへの参加を制限して参加者の信頼度を高めることで PoW の負荷を下げ、ま

---

[38] https://blog.ethereum.org/2014/07/05/stake/

[39] 分析対象間の関係の強さ、頻度などを分析することで、影響力や連携の強弱などを明らかにする分析手法。ここでは、ノード間の影響力や親密度などを分析している。

[40] 様々なデータを分析することにより、似通った特徴を持つ分析対象をグループ（クラスター）に分類する分析手法。

[41] http://pmg.csail.mit.edu/papers/osdi99.pdf

たコンセンサスに報酬を必要としない、簡略化されたコンセンサスアルゴリズムを採用し、高トランザクション処理を可能にする「コンソーシアム型/プライベート型」の仕組みが提案されている。ただし、コンソーシアム型やプライベート型では、ブロックチェーンの本来の意義（中央管理者不在での利用）を活かせない、という指摘もある。

図表 4-2　パブリック / コンソーシアム / プライベートの比較[42]

パブリック	コンソーシアム	プライベート
■ ネットワーク（コンセンサス、マイニング）への参加が誰にでも開かれている ■ 悪意を持った参加者を排除するために、コンセンサスの手法が重要となる	■ 特定の企業グループなど、ある程度信頼の置けるメンバでコンセンサスを形成しながらブロックチェーンを利用する ■ 身元のわかっている参加者しかいないため、コンセンサスはとりやすい	■ 特定の組織の内部でブロックチェーンを利用する ■ 組織内に閉じているため、合意形成はとりやすい

[42] パブリック/コンソーシアム/プライベートの定義には定まったものはなく、本表は一例である

4.2　ビットコインのブロックチェーンの課題への対応

3.5 章で整理したビットコインのブロックチェーンにおける課題に対しては、その他のブロックチェーン基盤提供サービスにより解決されているものも存在する。仕様と実装に起因するものとして 3 つに大別された課題ごとに、提案されている解決方法を以下に示す。また、様々なブロックチェーンによる各課題への対応状況について、図表 4-3 に整理した。

4.2.1 システムの仕様と実装に起因する課題への対応

(ア) スクリプトの実装に起因する課題への対応

ブロックチェーンの応用・拡張の方向性の 3 つの軸の中では、主に「ブロックチェーン上での記録・交換対象の拡張・汎用化」で対応がされている領域である。

ビットコインのブロックチェーンでは「チューリング完全性」を満たせていないことは前述の通りだが、ブロックチェーンシステムのひとつである Ethereum は「チューリング完全性」を満たしたシステムである。ビットコインブロックチェーン上では実現できないようなスクリプトの実装が可能となっているため、より広範なユースケースへの適用が可能になると期待されている。(課題 1)

ビットコインのブロックチェーンに対しても、Sidechain や Counterparty ではチューリング完全なスクリプトが実装されており、これらで拡張を行うことにより、様々な処理を行うことができるようになるとされる。

(イ)「ファイナリティ」に起因する課題への対応

ブロックチェーンの応用・拡張の方向性の 3 つの軸の中では、主に「コンセンサスアルゴリズムの改変・高性能化」で対応がされている領域である。

ビットコイン以外のブロックチェーンにおいては、PoS や PoI などのコンセンサスアルゴリズムを採用することにより、マイニングコストを低減し、電力の過剰な利用を避けられるとしている。とはいえ、PoS においては、残高の多い一部の団体しかマイニングできない問題は依然として残存している。(課題 9)

一部のコンソーシアム型/プライベート型のブロックチェーンにおいては、ファイナリティの条件を、ブロックチェーン開発者側で決定する、もしくは PBFT などのコンセンサスアルゴリズムを用いることにより、ビットコインブロックチェーンを利用する際に要する 10 分から 60 分程度の時間を軽減させることが可能であるとされている。一方で、ファイナリティの時間は短縮可能であるものの、ミリ秒単位までの時間の短縮は難しい。そのため、即時性が求められる取引の中でも、特に時間の制約が厳しい取引には向いてないとされている。(課題 4)

タイムスタンプにおける時間の正確性を担保する方法として、ブロックチェーンの P2P

ネットワークに接続されている各ノードが認識している時間をアンケート的に収集し、統計的に処理することで正確な時間を導出し、タイムスタンプに利用する方法が考えられている。また、TSA、TAA と連携して正確な時間の情報を得ることも可能である。(課題 10)

(ウ) P2P システムに起因する課題への対応

ブロックチェーンの応用・拡張の方向性の３つの軸の中では、主に「ネットワークへの参加を制限し、参加者の信頼度を向上」で対応がされている領域である。

前述した通り、ビットコインのシステムでは参加している各ノードのマシンパワー差からネットワーク全体の最適化を行う事が難しく、計算の重複などのロスが発生している可能性が指摘されているが、コンソーシアム型/プライベート型のブロックチェーンにおいては、ノードの参加を許可制としているため、マシンパワーのレベルを揃え、CPU のマルチコア化や GPU コンピューティングを行うことによりトランザクション処理を高速化することが可能であると考えられている。(課題 8)

一部のコンソーシアム型/プライベート型のブロックチェーンにおいては、各ノードのブロックに格納されているデータを圧縮したり、他サーバへアップロードしたりするなどし、データサイズを軽減可能な環境が構築可能であるとされている。また、伝送負荷を軽減可能な独自のデータ管理フォーマットを用いることで、単位時間あたりのトランザクション処理量を向上させることが可能である。(課題 5)

パブリック型のブロックチェーンにおいては、ノードへの参加が自由であれば、特にシステムの立ち上げ時においては全体のマシンパワーが小さいため、51%アタックを受けるリスクを高めてしまう。そのため、初期段階のみノードへの参加を限定し、信頼できる参加者のみでシステムを構築することでそのリスクを軽減することが可能である。また、コンソーシアム型/プライベート型のブロックチェーンにおいては、はじめから参加者が制限されており、悪意を持ったノードは参加しにくい環境であるため、攻撃を受ける可能性は低いといえる。同様に、悪意を持つ者による不正な取引を防ぐため、パブリック型ブロックチェーンにおいては、ノード毎の取引高や残高をクラスタリング分析することにより、違法な取引を行う可能性のあるノードをあらかじめ検知することが技術的には可能である。また、コンソーシアム型/プライベート型・ブロックチェーンにおいては、管理者が存在するため、違法な取引の可能性のあるノードを管理者が排除することは可能である。(課題 13)

ビットコインにおいては、前述のとおりトランザクション量の増加に伴ってブロックサイズが逼迫しつつあるとの指摘がなされており、コア開発者を中心に、ブロックチェーンの容量不足問題を解決する方法が議論されてきた。現時点では、Segwit（Segregated Witness）がまず実装された後、正式にシステムに組み込まれるようリリースされることで、容量不足問題を解決する予定である。Segwit とは、ブロックに格納されるトランザクション情報の中から、署名に関する情報データを取り除くことで、現在のデータ容量を最大 25%まで圧縮するアイデアである。また、Segwit に加え、Bitcoin Classic というアイデアの実

装に関しても議論されている。Bitcoin Classic とは、ブロックサイズを現状の 1MB から 2MB へと引き上げるアイデアであり、Segwit とは異なる方法で容量不足問題を解決する施策である[43]。両者が共に実現すると、1 ブロックに取り込めるトランザクションが最大で 8 倍になるため、ブロックサイズの問題を当面の間解決できるとみられている。（課題 7）

4.2.2 実ビジネスの慣行とのギャップに起因する課題への対応

前述の通り、ビットコインのブロックチェーンにおいては、ブロックに書きこまれた内容を後から遡って修正することが難しい。一方で、Ethereum など、一部のブロックチェーンシステムにおいては、特定のスクリプトによりプログラムが記載されることにより、コンセンサスに失敗した場合、ブロックが発生したタイミングなどで、前段のブロックまで遡って修正を行う可能性があることが公表されている。また、コンソーシアム型/プライベート型のブロックチェーンにおいては、間違ったトランザクションを訂正するための修正手続きを、管理者側で任意に実施する仕組みを組み込むことが可能である。

また、取引におけるプライバシーを保つため、一部のパブリック型ブロックチェーンにおいては、トランザクションの追跡不可能特性を付与させ、トランザクションデータを秘匿化したサービスを展開している[44]。コンソーシアム型/プライベート型のブロックチェーンにおいては、そもそも限られた範囲でのブロックチェーンの利用となるため、プライバシーの侵害を恐れる必要がない。

ビットコインブロックチェーンでは、ビットコインの価値が変動するため取引手数料の想定が難しいが、法定通貨と連動させないことで、相場と連関性をもたせず、従って価格変動が生じることのないトークンを、自社で用意し、発行して利用してもらうことは可能である。

4.2.3 ビットコインブロックチェーンの数理的・情報科学的課題への対応

FLP impossibility や CAP 定理に対して完全な解決はできないが、いくつかの条件を付けることで対応が可能と言われている。ただ、これらについて理論的な議論が深まっているとは言えない状況である。

---

[43] Bitcoin Core の方法は、現在のブロックチェーンと互換性のない新たなブロックチェーンに移行する方法であるため（ハードフォークと呼ばれる）、スムーズに移行できない可能性を懸念する声も多い。

[44] たとえば Zcash では、ゼロ知識証明が採用されている。ゼロ知識証明は、1985 年に提案された証明方法の 1 つ。ある人が他の人に自分の命題が真であることを伝えるのに、真であること以外何の知識も伝えることなく証明するプロトコルである。
http://pdf.landfaller.net/80/80-4.pdf

図表 4-3　ビットコインのブロックチェーンの課題への対応

課題		その他のBCによる課題の解決	残存課題
1. スクリプトの仕様が、チューリング完全ではない。	Pub	チューリング完全であるため、任意の処理をスクリプト上に記述可能。（Ethereum）	–
	C/Pri	–	スクリプトをのせ、自動実行可能な環境を構築中のサービスもある（チューリング完全か否かは確認の必要あり）。（mijin等）
2. スクリプトの実行にはトリガー（トランザクション等）が必要となる。	Pub	–	スクリプトの実行にはトリガー（トランザクション等）が必要となる。
	C/Pri	–	スクリプトの実行にはトリガー（トランザクション等）が必要となる。
3. 取引内容を後から修正することが難しい。	Pub	特定のスクリプトによりプログラムが記載された場合、コンセンサスに失敗し得るため、ブロックが発生したときなどに遡って修正を行う。（Ethereum）	–
	C/Pri	C/Priにおいては、間違ったトランザクションを訂正するための手続きを決められる。	–
4. ファイナリティに時間を要し、フォークによる手戻りリスクが存在する。（厳密にはトランザクションは確定していない）	Pub	–	ファイナリティに時間を要する。
	C/Pri	スーパーノードの導入により、ファイナリティの時間を短縮し、フォークによる手戻りリスクを低減可能。（Orb）C/Priであれば、ファイナリティの条件を決定すれば課題は解決可能。	ファイナリティの時間を短縮可能だが、ミリ秒単位までの短縮は難しいため、迅速な取引に向かない。
5. 単位時間あたりのトランザクション処理量が少ない。	Pub	–	ブロックサイズを大きくすることにより、処理可能なトランザクション量を増やすことが提案されているが、賛否が分かれている。
	C/Pri	伝送負荷を軽減可能な独自のデータ管理フォーマットを採用したことにより、単位時間あたりのトランザクション処理量を向上。（mijin等）	–
6. 取引者、取引の内容が公開されるため、プライバシーが保たれない恐れがある。	Pub	ゼロ知識証明を用いることで、取引の追跡不可能特性を付与したサービスを開発。（Zcash等）	–
	C/Pri	限られた範囲でのブロックチェーンの利用となるため、プライバシーの侵害を恐れる必要がない	–
7. 肥大化するブロックチェーンによりノードの容量が圧迫される。	Pub	–	Segwitにより、トランザクション構造の中で、署名を分離しブロックの容量削減を行う方法が実装された。
	C/Pri	各ノードのブロックを圧縮/他サーバへアップロードするなどし、データサイズを軽減可能な環境を構築可能。（mijin）	–
8. ノードごとにマシンパワーのレベル差を考慮した、トランザクション処理のネットワーク全体での最適化が行われない。	Pub	–	ノードごとにマシンパワーのレベル差を考慮した、トランザクション処理のネットワーク全体での最適化が行われない。
	C/Pri	参加するノードは許可制であるためハードウェアの仕様を揃え、CPUのマルチコア化やGPUコンピューティングによりトランザクション処理を高速化。（mijin等）	–
9. 一部の（強力なマシンを保有する）団体しかマイニングできない上、電力を過剰に利用することになる。	Pub	Proof of Stake, Importanceの採用により、マイニングコストを低減し、電力の過剰な利用を避けられる。（Ethereum, NEM等）	Proof of Stakeにおいては、残高の多い一部の団体しかマイニングできない。
	C/Pri	Proof of Stake, Importanceの採用により、マイニングコストを低減し、電力の過剰な利用を避けられる。（Orb, mijin等）	Proof of Stakeにおいては、残高の多い一部の団体しかマイニングできない。
10. トランザクションに押されるタイムスタンプは正確性や保証がない。	Pub	各ノードの認識している時間をP2Pネットワークを介してアンケート的に収集し、統計的に処理するサービスにより補完する可能性あり。（NEM）	–
	C/Pri	タイムサーバと連携して、タイムスタンプ打つことにより時刻の正確性を保持。	–
11. トークンの価格変動により取引手数料の事前想定が困難。	Pub	相場によって価格変動しないトークンを自前で用意可能。（colored coins等）	–
	C/Pri	相場によって価格変動しないトークンを自前で用意可能。（Orb, mijin等）	–
12. P2Pのネットワークを分断するような物理攻撃や障害が生じた場合に、ブロックチェーンがフォークする可能性がある。	Pub	特にシステム立ち上げ時には、51%アタックをうけやすいため、立ち上げ時にはTrustedな環境にすることもある。	システム立ち上げ時には、51%アタックをうけやすい。
	C/Pri	悪意を持ったノードが参加出来ない環境のため攻撃をうけない（mijin等）	–
13. 誰でも参加でき、特定のノードを排除する仕組みがないため、違法な取引にも利用される可能性がある。	Pub	ノードごとの取引額・残高をクラスタリング分析することにより、違法取引を行う可能性のあるノードを検出することが可能。（NEM等）	–
	C/Pri	Centralizedな環境のため違法取引の可能性のあるノードを排除可能。（Orb, mijin等）	–

4.3　ブロックチェーンの分類とユースケース

4.2 章で見たように、ビットコインのブロックチェーンの課題を解決するために、様々なブロックチェーンが開発されており、それぞれのブロックチェーン上で、様々なサービスが提案されている。それらを 4.1 章の軸に添って整理したのが図表 4-4 である。

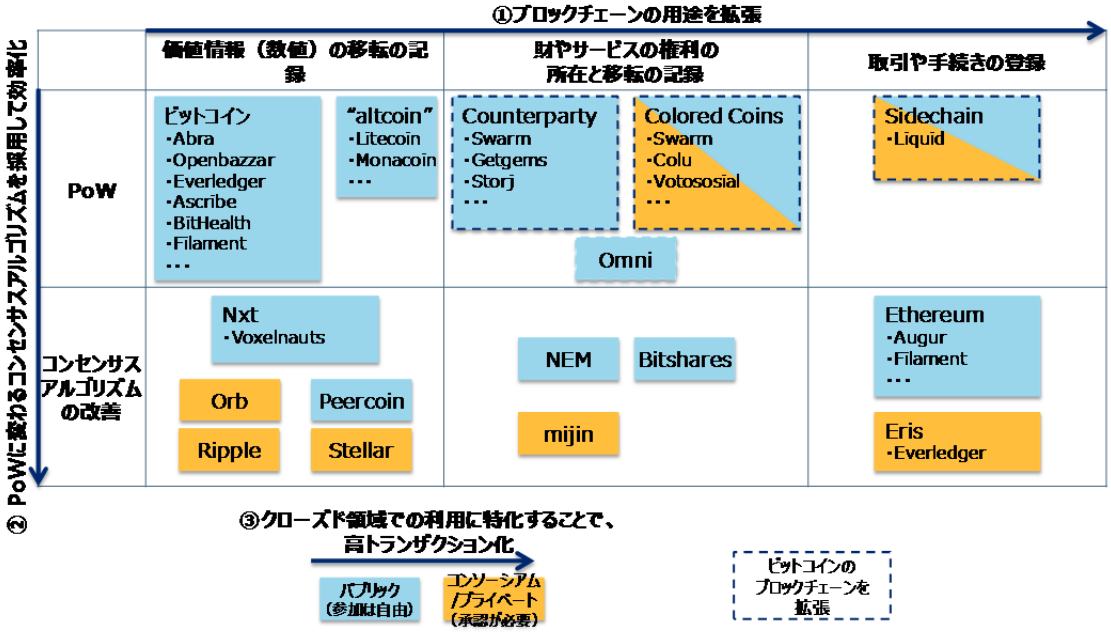
価値情報の移転の記録を主とし、PoW を用いているのは、ビットコインとそこから派生しているアルトコインである。ビットコインのブロックチェーンを活用したサービスはすでに多数存在し、Abra（イスラム送金）、Openbazzar（マーケットプレイス）、Everledger（所有権の証明）などがある。

ビットコインのブロックチェーンから、利用範囲を拡大していったものとして、Omni などがある。また、独自のブロックチェーンではないが、ビットコインのブロックチェーンを拡張する方法が提案されており、Counterparty や、Colored Coins、Sidechain などが実際に利用されている。Counterparty では、Swarm（クラウドファンディング）、Getgems（SNS）、Storj（ストレージ）等のサービスが、Colored Coins では、Swarm、Colu（所有権の証明）、Votososial（電子投票）などが、Sidechain では、Liquid（取引所間決済）が提供されている。

ビットコインのブロックチェーンからコンセンサスアルゴリズムを改変したものとしては、Proof of Stake を採用した Nxt、Peercoin、Orb などや、独自のアルゴリズムを採用している Ripple や Stellar などがある。このうち、Orb、Ripple、Stellar は参加者が限定的なコンソーシアム型/プライベート型のブロックチェーンとすることで、より高速な処理が可能となっている。

さらに用途を財やサービスの権利まで拡張しようとしたものとして、NEM や Bitshares、NEM のコンソーシアム型/プライベート型への転用である mijin などがあり、スマートコントラクトなど、将来発生する処理をブロックチェーンに取り込み、自動化することを前提としたものとして、Ethereum や Eris などが構築されている。Ethereum 上では、Augur（予測市場）や Filament（センサーネット）、Eris では Everledger などが提供されている。

図表 4-4　ブロックチェーンの分類



上記以外にも、様々な分野でブロックチェーンを活用した多くのサービスが提案されている（図表 4-5）。

図表 4-5　ブロックチェーンのユースケースとサービス事例

(ア) 金融系

決済をはじめとした金融分野におけるユースケースは非常に多い。仮想通貨としてのビットコインも、ブロックチェーンの一ユースケースと捉えることができる。送金や決済のほか、証券、債権、各種金融派生商品の取引、イスラム金融など、様々な利用方法が提案されている。Ripple などが代表例である。

(イ) ポイント／リワード

ポイントサービスやリワードを、ブロックチェーン上で提供している。決済とも近いが、用途や利用者に制限をかけるなど、特定の領域のみで利用することを前提としたサービスとなる。

GyftBlock は、ブロックチェーンを利用したギフトカードの交換サービスを提供している。ギフトカードの発行・送信・交換などをブロックチェーン上で行えるほか、利用者のコントロールや、利用状況のモニタリングも可能となっている。

(ウ) 資金調達

アーティストへの投資や、クラウドファンディングにブロックチェーンを活用する試みである。管理者が不要または簡易になるため、集まった資金に対して、アーティストや事業者の取り分が大きくなるメリットが期待される。

Swarm は、ブロックチェーン上でクラウドファンディングによる資金調達を行うためのサービスである。スマートコントラクトにより、出資者は配当を受け取ることができる。

(エ) コミュニケーション

ブロックチェーンを用いてメッセージングサービスや SNS（ソーシャルネットワーキングサービス）を実現している。(ア)の送金や(イ)のリワードサービスなどとも組み合わせて利用される。

Getgems は、SNS サービスを提供している（SNS 自体はブロックチェーンとは別に提供されている）。独自の仮想通貨である GEMZ トークンが広告の閲覧などで付与され、SNS でコミュニケーションしながらトークンのやりとりができる。

(オ) 資産管理

土地の登記など、資産の所有と移転をブロックチェーンで管理する。Factom 等がサービ

スを提供し始めている。

(カ) ストレージ

ブロックチェーンを利用してネット上のデータ管理を行うサービスである。データそのものをブロックチェーンに保管すると、ブロックチェーンの容量を肥大化させるため、データそのものの管理は別の手法をとる場合もある。

Storj は、ブロックチェーンで様々な電子ファイルを管理するサービスを提供している。データそのものは暗号化され、P2P 上に分散した状態で保管されるため、他人には閲覧不可能で、障害耐性も高いストレージサービスとなっている。

(キ) 認証

商品などの正当性の認証を、ブロックチェーンを用いて管理する仕組みが提供されている。アート作品や薬品、デジタルコンテンツなど、適用範囲は広い。

Ascribe はアート作品などの著作権管理をブロックチェーン上で提供するサービスである。アーティストが自分の作品を登録すると、所有権の管理と移転、利用履歴の管理などが可能になる。

(ク) シェアリング

カーシェアリングなど、いわゆるシェアリングエコノミーにおいて、共有されるものの利用権をブロックチェーンで管理する。

La'ZooZ は、シェアリングサービスをブロックチェーンの活用によって提供することを目指している。現在は Uber のようなライドシェアのアプリケーションを提供している。

(ケ) 商流管理

いわゆる EDI をブロックチェーンに置き換えるだけでなく、原材料から最終製品までの加工の履歴もブロックチェーンに登録することで、トレーサビリティを実現する。(キ)と同様、デジタルコンテンツなどにも適用されている。

Everledger は、ダイヤモンドの個品管理を行うシステムを提供している。個々のダイヤモンドのシリアル番号やカラット数、様々な商品情報の他、そのダイヤモンドの所有権と流通履歴を管理している。

(コ) コンテンツ

ネット上でのコンテンツ配信にブロックチェーンを利用する。ストリーミング放送に対して時間単位で課金したり、オンラインゲーム内のアイテムを管理したり、といったサービスが提供されている。

Streamium は、コンテンツ配信を支援するサービスを提供している。動画配信など向けに、秒単位での課金（ビットコイン払い）システムを構築した。

(サ) 将来予測

世の中の様々な事案について、「将来どうなるか」を投票し合い、結果によって報酬を分け合う、というサービスが出現している。「予測市場」とも呼ばれている。英国のブックメーカーをブロックチェーン上で置き換えたもの。

Augur は、様々なイベントについて参加者が予測を投票し合うことで、「群衆の英知（Wisdom of the Crowd）」によって将来を予測する、分散型の予測市場プラットフォームを提供している。

(シ) 公共分野

自治体の予算管理、投票、届出の管理、社会保証など、公共サービスをブロックチェーン上で実現しようとする試みも多い。ロンドンの市長選では、前述の通り候補者の一人が予算管理をブロックチェーン化することを公約として掲げているほか、エストニア、ホンジュラスなど、公共システムへのブロックチェーンの採用に関心を表明している国も現れている。

Neutral Voting Bloc（NVB）は、オーストラリアで提供されているサービスで、自らを新たな政党であるとしている。NVB の議員は、ブロックチェーン上で投票された結果に従って、実際の議会での活動を行うとしている。

(ス) 医療分野

電子カルテや投薬記録など、医療に関するデータをブロックチェーンで管理するアイデアである。プライバシーを守るため、医療データそのものはブロックチェーンには記録せず、カルテが管理されている医療機関等へのパスのみを管理していく、といった方法が提案されている。

BitHealth は、ブロックチェーンを使って、世界中から自分のカルテのデータを安全に参

照できるようにすることを目指している。

(セ) IoT 分野

IoT においても、ブロックチェーンが利用されうるとされている。センサーなどが、中央サーバを介さずに、個別にやりとりをしながらあらかじめ決められた処理を行っていく、という利用方法が想定されている。

IBM と Samsung による ADEPT などが注目されている。

4.4　既存企業によるブロックチェーン活用の取り組み状況

4.3 章で言及した通り、ブロックチェーン技術を活用した様々なユースケースが世界中で生み出されており、サービスとしてローンチされているものも既に存在する。その中で、国内外の既存の企業や団体においても、ブロックチェーン技術の活用に取り組むものが現れ始めている。その多くは実証実験段階であるものの、既存業務における新たな付加価値の創出や、コストの削減などを目標としてブロックチェーン技術を利用していくとされているものが多い。国内では個別企業単位での取り組みが中心となっているのに対し、海外では企業グループなどによる業界横断的な取り組みが増えつつあるのが特徴的である。主な事例を、4.4.1、4.4.2 に示す。

4.4.1 国内既存企業による主な活用検討事例

2015 年 5 月に、NTT サービスエボリューション研究所は、ブロックチェーンを活用したコンテンツ利用許諾管理に関する研究結果を発表した。本技術は、同社によるイマーシブテレプレゼンス技術「Kirari!」開発の一環で行われているもので、多様な映像を安心して利用するにあたっての、手軽な映像利用許諾管理技術が求められている中でのソリューションとして位置付けられている。同社は、このようなコンテンツ管理の仕組みが世の中に受け入れられるためには、技術の良し悪しだけでなく、普及に向けたコミュニティ活動も重要になると考え、今後はコンテンツ制作者やメーカーなど多くのステークホルダーと連携した取り組みを進めて行く予定であるとしている[45]。

2015 年 10 月より、野村総合研究所は、証券業務でのブロックチェーン技術の利活用に向けた実証研究を実施してきた。また、2015 年 12 月より、住信 SBI ネット銀行と協業し、ブロックチェーン技術を活用した業務シナリオの作成と検証事項の洗い出しを実施し、その上でその業務シナリオに沿った検証用プロトタイプを構築し、成果や課題を検証したうえで、銀行業務におけるブロックチェーン技術の適用シーンの具体化を推進するとしている。ブロックチェーン技術の実装に際しては、Dragonfly FinTech などへの委託を行っている[46,47]。,

2015 年 12 月に、さくらインターネットとテックビューロは、さくらインターネットが運営する「さくらのクラウド」上にて、テックビューロによる「mijin クラウドチェーン」の実証実験環境「mijin クラウドチェーンβ」を 2016 年 1 月より無料提供すると発表した。プライベート型ブロックチェーン環境が、実用レベルのクラウドサービスとして一般向けに無料で提供されることは世界初であるとしている。本実証実験環境の提供を通じ、プラ

[45] http://www.ntt.co.jp/journal/1505/files/jn201505010.pdf
[46] http://www.nri.com/jp/news/2015/151005_1.aspx
[47] http://www.nri.com/jp/news/2015/151216_1.aspx

イベート型ブロックチェーンの可能性をユーザに感じてもらうとともに、幅広い分野でのプライベート型ブロックチェーンの利用促進に貢献することを目指すとしている[48]。

2016 年 1 月に、ソフトバンクは、ブロックチェーン技術を活用してインターネット上で信頼性の高い取引を実現するプラットフォームの研究開発を行うと発表した。本研究開発においては、通信事業者としてブロックチェーン技術が生み出す新たな価値を理解し、それを活用した具体的なサービスをいち早く創出・提供することを目的とするとしている。研究開発の第一弾として、コンセンサス・ベイス、アピリオの協力の下、ブロックチェーン技術を利用した国際募金プラットフォームのプロトタイプを開発するとしている。[49]

2016 年 2 月に、GMO インターネットとテックビューロは、業務提携により、ゲーム用バックエンドエンジンを共同開発すると発表した。ブロックチェーン技術のゲーム用バックエンドエンジンへの応用により、運用コストが従来の半分未満へと圧縮が見込める上、ダウンタイムをできる限り抑える”ゼロ・ダウンタイム環境”の実現が可能になるとしている。2016 年秋を目途に、ゲーム・アプリ専用クラウドサービス「GMO アプリクラウド」において、PaaS 型バックエンドエンジンとして販売開始する予定である。[50]

2016 年 2 月に、三菱東京 UFJ 銀行が独自の仮想通貨の開発を進めていると報じられた。当面は、「行内通貨」と位置づけるが、将来的には円と交換できるようにし、利用客らに発行する構想もあるという。当該仮想通貨は「MUFG コイン」と名付けられており、コインをスマートフォンに取り込むアプリケーションの試作品もほぼ完成しているとされる[51]。

2016 年 2 月に、みずほフィナンシャルグループは、電通国際情報サービス、カレンシーポート、日本マイクロソフトと協働し、ブロックチェーン技術の実証実験に取り組むと発表した。本実証実験においては、ブロックチェーン技術、およびスマートコントラクトの特性を活かし、関係当事者が多く事務効率化等が見込まれるシンジケートローン業務を対象として、技術の理解、金融業務への活用に関する実証実験を行い、適用可能性を検証の上、金融に革新をもたらすようなモデルの創出を目指すとしている[52]。

4.4.2 海外既存企業による主な活用検討事例

米国のフィンテック企業である R3 CEV は、世界各国の 42 社（2016 年 3 月現在、日本からの参加企業は野村ホールディングス、三井住友銀行、三菱東京 UFJ フィナンシャル・グループ、みずほフィナンシャルグループ等）の金融機関が参加するコンソーシアムを主導しており、参加している企業群による Private Distributed Ledger を構築、複数の実証

48 http://www.sakura.ad.jp/press/2015/1216_mijin_cloud_chain/
49 http://www.softbank.jp/corp/group/sbm/news/press/2016/20160106_01/
50 https://www.gmo.jp/news/article/?id=5146
51 http://www.asahi.com/articles/ASJ1W4RWKJ1WULFA012.html
52 http://www.mizuho-fg.co.jp/release/20160216release_jp.html

実験を実施している。R3 による Private Distributed Ledger は、Chain、Eris Industries、Ethereum、IBM、Intel によって開発されたものであり、実証実験を実施するにあたり活用されるクラウドコンピューティングのリソースは、Microsoft Azure、IBM Cloud、Amazon AWS によって提供されている。同社の CEO である David Rutter は、世界規模での金融機関と技術提供企業が、産業を超えて Private Distributed Ledger を採用することで、意義ある機運が組成され、金融業界においては、電子取引の出現が与えたメリットと同等の効果、透明性、スケーラビリティ、セキュリティがもたらされるとしている[53]。

MIT Media Lab は、2015 年 4 月に、ビットコインや暗号通貨全般を扱うイニシアチブを設立することを発表した。このイニシアチブでは、メディア・ラボのメンバ企業の支援や参加を受けて、MIT の教員や学生が研究に取り組む。活動のゴールとして、

①より多くの学生を巻き込みながら、特にセキュリティ、安定性、スケーラビリティ、プライバシー、経済モデルに関する課題に重点を置いた研究を行う。

②政府、NPO、民間企業を招集し、社会的インパクトの大きな概念実証を行う。

③現在と将来の政策や標準化のために、科学的根拠に基づく研究を実施する。

という 3 つが設定されている[54]。

2015 年 10 月に、Nasdaq は、Chain と提携し、ブロックチェーン技術を活用した未公開株式取引システム「Nasdaq Linq」を発表した（2015 年 5 月時点で開発を発表済み）。本システムは、Nasdaq が運営する未公開株式取引市場「Nasdaq Private Market」に参加する株式未公開企業が使用するシステムであり、従来は株式未公開企業が同市場に参加するためのクラウドベースのシステムとして提供していた「Exact Equity」を補完するシステムとなる。当面、本システムは、Chain、ChangeTip（電子マネー関連スタートアップ）、PeerNova（暗号化台帳技術関連企業）、Synack（サイバーセキュリティ関連企業）、TangoMe（メッセージングアプリケーション関連企業）、Vera（企業向けメッセージングアプリ関連企業）の 6 社によって利用されるとしている[55]。

Linux Foundation は、Linux の成長促進に取り組む非営利のコンソーシアムであり、2000 年に設立された。その中で、2015 年 12 月にブロックチェーン技術を活用した共同開発プロジェクト「Openledger」プロジェクトを発表した。本プロジェクトにおいては、商取引を支える堅牢な業界専門プありケーション、プラットフォーム、およびハードウェアシステムの構築をめざし、企業グレードのオープンソース分散型台帳（Distributed Ledger）フレームワークとその開発者の育成を行うとしている。本プロジェクトへは 20 社以上が参

53 http://r3cev.com/

54 https://medium.com/mit-media-lab-digital-currency-initiative/launching-a-digital-currency-initiative-238fc678aba2

55 http://ir.nasdaq.com/releasedetail.cfm?releaseid=938667

加しているが、日本企業では富士通、日立製作所、NEC、NTT データが参加している[56,57]。

W3C（World Wide Web Consortium)は、Blockchain Community Group を設立。ISO20022 に基づいた、ブックチェーンにおけるメッセージフォーマットの標準化を目指し、ガイドラインの作成を実施している。また、ブロックチェーン関連の新しいテクノロジーの勉強や評価をするグループであるとしている[58]。

オーストラリア証券取引所（ASX、Australian Securities Exchange）は、既存のシステムの更新に際し、ブロックチェーン技術の採用を検討してきていたが、2016 年 1 月に Digital Asset Holdings への出資・提携を発表、同社の技術を活用するとした。これにより、ハウス電子サブレジスターシステム（CHESS、Clearing House Electronic Subregister System）を置きかえることで、リアルタイムに近い株式取引を行えるようにするとともに、システムの管理コストを削減する予定であるとしている[59]。

---

56 http://www.linuxfoundation.jp/news-media/announcements/2015/12/jp_linux-foundation-unites-industry-leaders-advance-blockchain

57 https://www.hyperledger.org/

58 https://www.w3.org/community/blockchain/

59 http://www.smh.com.au/business/banking-and-finance/asx-builds-blockchain-for-australian-equities-20160121-gmbic0.html

4.5　ブロックチェーンの発展の方向性

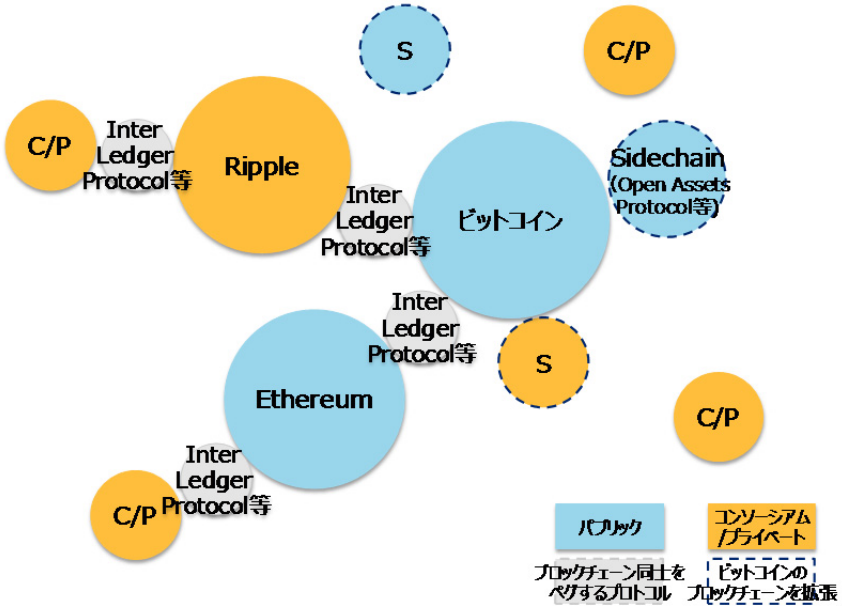
今後、ブロックチェーンがどのように発展していくかについては、主に利用されるブロックチェーンによって、いくつかのシナリオが考えられる。しかし、これらのシナリオはあくまでブロックチェーンというインフラの階層での議論であり、個別のサービス自体はどのシナリオ上でも提供されうる。

現在のところ、ビットコインのブロックチェーンのみが安定的に稼働しているとされている。ビットコインのブロックチェーンの周辺では、様々な価値を記録していく Sidechain や Open Assets Protocol を活用し、ビットコインのブロックチェーン自体にはそれらのスクリプトが挿入されていくと考えられる。この場合、様々なサービスは、Sidechain や Open Assets Protocol のシステム上で主に提供されることが想定される。ビットコインのブロックチェーンはオープンな仕組みであるが、Sidechain や Open Assets Protocol を活用することで、ちょうどインターネットと社内 LAN の関係のように、公開の度合いがコントロールされた仕組みが運用されていくと思われる。

一方で、Ethereum や Ripple など、個別のブロックチェーンとは、Sidechain や Inter Ledger Protocol[60]などを介して連携が図られる可能性がある。また、これまで言及してきたとおり、ビットコインのブロックチェーンには様々な課題が指摘されており、それらに対応した新たなブロックチェーンも多数提案されている。新たなブロックチェーンのいくつかが、実際の運用に耐えうると評価され、利用されていくことも考えられる。コンソーシアム型やプライベート型の、クローズドな仕組みが主に利用される場合は、様々な企業により提供される様々なコンソーシアム型/プライベート型のブロックチェーンを、一部ではカスタマイズしながら社内システムとして利用していくことも考えられる。その場合には、共通の仕様などはほとんど必要なくなり、各社各様にブロックチェーンを構築し、その上でサービスを提供する、という活用形態となると思われる。また、新たなパブリック型のブロックチェーンが開発され、世に普及していくことも考えられる。

[60] Ripple が提唱している、ブロックチェーン間で情報を交換するためのプロトコル

図表 4-6　ビットコインのブロックチェーンを含めた、
様々なブロックチェーンが活用される世界



注）C/P：コンソーシアム型またはプライベート型のブロックチェーン
S：Sidechain または Open Assets Protocol ベースのブロックチェーン

5　ブロックチェーンの活用

5.1　ブロックチェーンの機能とユースケース

4 章で見たとおり、すでにブロックチェーンのユースケースとして、様々なものが提案されている。

図表 5-1　ブロックチェーンのユースケースとサービス事例（再掲）

一方で、国内外の実務者へのヒアリングからは、ブロックチェーンを用いることが必ずしも必要ではない場合や、既存のシステムを置き換えるのに多大なコストがかかってしまう可能性があることが指摘された。

そこで改めて、3.4.2 で整理したブロックチェーンの機能から、上記のユースケースを整理すると、必ずしもすべての機能を必要としていない場合があることがわかる。これらの中でも、「真正性の保証された取引が可能（二重支払の防止）」や「データのトレーサビリティが可能で、透明性の高い取引が可能（改ざんが困難）」、「中央管理者が不在でも、悪意を持つユーザがいてもエコシステムが安定維持される」機能は、特にブロックチェーンに特徴的であると目される。

一方で、しばしば喧伝される「サーバコスト（構築/運用）の低廉化」については、実際にどの程度のコストが削減可能なのかについて、今後の実証が必要であり、特に、既存のクライアント/サーバ型の基幹系システムを置き換える場合に、情報系などの周辺のシステムとの整合をとる必要性などを考慮しなければならない場合には、必ずしもコストメリッ

トが得られない可能性も考えられる。

図表 5-2　ユースケースとブロックチェーンの機能の対応

	地域通貨	土地の登記	サプライチェーン	シェアリングエコノミー	スマートコントラクト
➢スクリプトによりアプリケーションを実行可能			○		○
➢真正性の保証された取引が可能（二重支払の防止）	○	◎		○	○
➢データのトレーサビリティが可能で、透明性の高い取引が可能（改ざんが困難）	○	○	○	◎	○
➢サーバコスト（構築/運用）の低廉化	実証による検証が必要				
➢安定したシステムの構築・運用が可能（ゼロダウンシステム）	○				
➢中央管理者が不在でも、悪意を持つユーザがいてもエコシステムが安定維持される		○	○	○	○

5.2　期待されるユースケース

ブロックチェーンとの適合性が高いと期待されるユースケースについて、以下で利用メリットと課題の整理を試みた。

5.2.1 地域通貨

自治体等が発行する地域通貨を、ブロックチェーン上で流通・管理することが可能である。一定の手続きを経て住民に地域通貨が付与され、それを地域内の商店や公共サービス等での支払に利用する。住民から住民へ譲渡をしたり、店舗が支払いで受け取った地域通貨を利用（地域内での原材料の調達に利用したり、地域内に在住する従業員への給与として支払ったりするなど）したり、当該通貨で納税した場合には、税の優遇も認めるといった使い方も考えられる。また、利用期限を設けたり、徐々に価値が減衰していく設定にしたりすることも技術的には可能であり、これらを総合的に組み合わせることで、地域通貨の流通量を上げることも可能と考えられる。

(ア) ブロックチェーンで管理される主な情報

ブロックチェーンでは、地域通貨の付与（誰が発行し、いつ、誰に付与したか)、譲渡（地域通貨が誰から誰に渡ったか)、利用の履歴（いつ、どこで、何に利用されたか）が管理されるほか、地域通貨の有効期限や価値の減衰速度、地域通貨の付与条件（所得、年齢など、特定の条件を満たしたときに付与額が上がる、など）も管理することが可能であろう。

(イ) 活用するブロックチェーンの機能（図表 5-2 との対応）

ブロックチェーンの機能のうち、地域通貨サービスの提供において重要となるのは「真正性の保証された取引が可能（二重支払の防止)」「データのトレーサビリティが可能で、透明性の高い取引が可能（改ざんが困難)」「安定したシステムの構築・運用が可能（ゼロダウンシステム)」の三つであると想定される。

・真正性の保証された取引が可能（二重支払の防止）

地域通貨を発行する上で、特定の付与条件が満たされた場合に、正しく 1 回だけ地域通貨が付与されなければならない。また、地域通貨を譲渡したり、利用したりする場合にも、二重支払が起きてはならない。この点で、ブロックチェーンにより真正性が保証され、二重支払が防止できることは有用である。

・データのトレーサビリティが可能で、透明性の高い取引が可能（改ざんが困難）

地域通貨の転々流通を認めるような場合、上記の二重支払の防止に加えて、実際に二重

支払が起きていたいことを確認できることが求められる。また、地域通貨の総発行額や用途が決まっているなどの場合に、正しく発行され、利用されているかを第三者が確認できることが重要になる。この点で、ブロックチェーンによりトレーサビリティが可能で、透明性の高い取引が可能になることは有用である。

・安定したシステムの構築・運用が可能（ゼロダウンシステム）

法定通貨による決済の代替として利用されることが想定されるため、相応に高い可用性が求められる。これは、ポイントサービスよりも地域通貨でより強く求められると想定される。この点で、ブロックチェーンにより安定したシステムの構築・運用が可能になることは有用である。

（ウ）ブロックチェーン活用時の留意点

地域通貨にブロックチェーンを活用する場合には、下記の点に留意する必要がある。

①　トランザクションに押されるタイムスタンプの正確性

地域通貨がいつ付与され、いつ利用されたかについて、正確な時間を把握する必要がある。そのため、ブロックチェーンに記録されるトランザクションのタイムスタンプについて、正確性が要求されることになるが、たとえばビットコインのブロックチェーンでは、トランザクションの時刻はそのトランザクションを作成した参加者に依存しているため、第三者が客観的に時刻の正しさを確認することが可能な仕組みが必要である。

②　一定時間を要するファイナリティ(取引確定・完了)

たとえばビットコインのブロックチェーンの場合、あるトランザクションがいつブロックチェーンに取り込まれるかは、トランザクション送信時点ではわからない。また、ブロックチェーンに取り込まれたとしても、そのチェーンがフォークする可能性を考慮し、一般的には後続する 6 ブロックが生成されるまでは様子を見るべきとされている。そのため、取引の確定までに最低 1 時間程度は待つ必要がある。

この点について、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、強制的にブロックチェーンを確定させていくなどの手法により、ファイナリティの時間を短縮させることが可能になっているものもあるが、それでも、中央集権型のシステムに比べて、不確定な要素が残ることに留意が必要である。

③　単位時間当たりのトランザクション処理量

ビットコインのブロックチェーンでは、1 秒間あたり 5～7 件のトランザクションしか処理できないとされる。地域通貨では、これ以上のトランザクションも想定されることから、ビットコインのブロックチェーンそのものを利用するのではなく、Open Assets Protocol

や Sidechain、他のブロックチェーンなどの活用が想定される。

④　付与条件を満たしたことの判定

地域通貨の付与を行うための条件（地域通貨購入手続き）は、ブロックチェーンの外部で起きることが想定される。この、「外部で起きたこと」をブロックチェーンに伝える（トランザクションを発生させる）ことが必要であり、それを誰がどのように担うかについて、サービス毎に事前の取り決めが必要となる。

（エ）類似の応用ケース

地域通貨の他、下記のサービスでも同様にブロックチェーンの活用が可能であると考えられる。

- 送金

送金サービスは、法定通貨の送金にとどまらず、地域通貨や、様々な仮想通貨など、あらゆる価値情報の授受に利用可能となる。パブリック型のブロックチェーンを採用すれば、送金の対象は自ずと全世界となる。

- 証券取引

電子化された証券は、ブロックチェーンを活用して取引を行いやすい。取引頻度の比較的低い社債などから、ブロックチェーンへの対応が進むと見込まれる。

- ポイントサービス

企業等が発行するポイントサービスを、ブロックチェーン上で提供することが可能である。特に、異なる種類のポイントを利用者間で交換することが可能となれば、ブロックチェーンを利用するメリットをより享受できると考えられる。

- 電子クーポン

飲食店、小売店等が発行する電子クーポンについても、ほぼ同様の仕組みで発行と利用の管理が可能であると考えられる。特に、クーポンの転々流通を認めるような場合に、中央集権型のシステムではなく、ブロックチェーンを利用するメリットが見込める。

（オ）市場へのインパクト

当該サービスがブロックチェーンによって実現される場合、地域通貨や送金、証券取引、ポイントサービス、クーポン、商品券等の市場が影響を受けることになる。それぞれの市場規模は下記の通りである。

● 地域通貨流通量：約 3 億円～10 億円（2015 年）[61]　※地域通貨発行数は全国で約 600、1 通貨当たり年間 500~2000 万円規模で流通している。
● 送金：4216 億円（2014 年度）[62]　※資金移動業者による年間取扱高。
● 証券取引：745 兆円（2015 年）[63]　※売買代金
● ポイントサービス市場：8,500 億円以上（2015 年度）[64]
● クーポン市場：約 400 億円（2013 年）[65]
● プレミアム付き商品券等：1700 億円（平成 26 年度補正予算）

（カ）産業構造へのインパクト

（1）当面の影響

地域通貨の価値を交換することができるプラットフォームが出現し、地域経済の活性化に寄与することが見込まれる。また、海外で利用可能な電子クーポンを、未使用時には国内で別の価値に移転することも可能となり、多様なマーケティング手法が生まれる。

（2）将来の可能性

● 多様な価値のポイント化

ブロックチェーンによる地域通貨やポイントサービスが基礎インフラ化して安価に提供できるような世界では、多様な価値（個人のアイデア・行動といった従来捕捉できていなかったものを含む）を誰もがポイント化し、換算・管理することが可能になり、そのポイントは発行体以外との取引にも利用され、転々流通することになる。

● ポイントと貨幣の境界の希薄化

その結果、ポイントで通貨に近い利用が可能となるとともに、ポイント発行額以上の経済波及効果が生じる可能性がある。例えば、国が発行した省エネポイントや商店街等の地域が発行したふるさとポイントを、民間企業が発行するポイントや貨幣に近い価値等と直接変換・管理することができるとすると、通貨に近い利用とともに消費行動の活発化につながることが想定される。

また、行政においては地域独自のポイントを発行することが可能となることで、これまでは高いシステム構築コストがかかるなど、展開が難しかった、局地的な、又は特定のグ

61 NRI 推計、2015 年
62 日本資金決済業協会
63 日本取引所グループ
64 野村総合研究所 ICT・メディア産業コンサルティング部　「IT ナビゲーター2016 年度版」　東洋経済新報社　2015 年
65 クーポンサイト.jp　http://couponsite.jp/news/2014/02/2013.html

ループを対象とした経済活性化施策が容易となる。

- ポイントによる信用創造

さらには、上述のように、ポイントサービスがより一般的な通貨と利用形態が似てくることにより、預金・貸出に類する機能を備えるようになると想定すると、信用創造の機能をも獲得し、日銀による景気対策（金融政策）以外にも、民間企業による金融政策的な仕掛けができるようになる可能性もある。

5.2.2 土地の登記

土地の物理的現況や権利関係の情報を、ブロックチェーン上で登録・公示・管理することが可能である。土地や建物、所有者に関する情報のほか、それらの移転や抵当権の設定なども記録、管理することも考えられ、関連する業務の効率化が図れると想定される。

(ア) ブロックチェーンで管理される主な情報

土地や建物の情報、譲渡の履歴を管理する。そのほか、現在登記簿で管理されている土地の分割・統合（分筆・合筆）のほか、所有権や抵当権などの情報も管理する。これらの情報は、現在の登記簿と同様、誰でも閲覧可能とする。

(イ) 活用するブロックチェーンの機能（図表 5-2 との対応）

ブロックチェーンの機能のうち、土地の登記への応用において重要となるのは「真正性の保証された取引が可能（二重支払の防止)」「データのトレーサビリティが可能で、透明性の高い取引が可能（改ざんが困難)」「中央管理者が不在でも、悪意を持つユーザがいてもエコシステムが安定維持される」の三つであると想定される。

・真正性の保証された取引が可能（二重支払の防止）

土地の譲渡が行われる場合に、当然のことながら、正しく 1 回だけ実行されなければならず、同じ土地が複数の相手に渡るような手続きが実行できてはならない。この点で、ブロックチェーンにより真正性が保証され、二重支払が防止できることは有用である。

・データのトレーサビリティが可能で、透明性の高い取引が可能（改ざんが困難）

登記簿に記載されている事項について、譲渡の経緯や、抵当権の設定などが、正しく記録され、過去の履歴が確認できることが必要となる。この点で、ブロックチェーンによりトレーサビリティと透明性が確保されることは有用である。

・中央管理者が不在でも、悪意を持つユーザがいてもエコシステムが安定維持される

現在、登記簿は各地の法務局が管理をしている。このシステムをブロックチェーンに置き換えるとき、どこかに中心となるサーバを置かなくても、システムが安定的に稼働する。今の場合、ノードとなるのは公的機関のみなので悪意のあるサーバは参加していないと見なせるが、仮にサーバが故障したりした場合にも、システム全体は継続的に運用される。

(ウ) ブロックチェーン活用時の留意点

ポイントサービスや地域通貨にブロックチェーンを活用する場合には、下記の点に留意する必要がある。

① トランザクションに押されるタイムスタンプの正確性

抵当権の取り消しや設定などが連続的に行われる場合、それらの手続きの順序が重要になる。複数の地点から処理を実行した場合に、正しい順序で処理されるためには、処理の時刻が重要となる。

② 当事者間の金銭授受などとの連動の必要性

土地の譲渡の場合、金銭の授受も同時に行われることが想定される。ローンを組む場合には、抵当権の設定もされることが多い。これらの金銭授受や金融取引と、ブロックチェーン上の移転の手続きとを、正確に連動させる必要がある。金銭授受そのものもブロックチェーン上で処理することも可能である。

(エ) 類似の応用ケース

下記のサービスでも同様にブロックチェーンの活用が可能であると考えられる。

- 特許情報

特許に関する情報についても、ブロックチェーンで管理することが可能であると考えられる。特許の内容だけでなく、所有権についても管理すれば、権利の売買もブロックチェーンで管理可能となることが想定される。

- 電子カルテ

個人の医療情報をブロックチェーンで管理することも可能であると考えられる。カルテの詳細な内容は個別の病院で管理し、ブロックチェー上で管理する情報は通院履歴などに制限することで、個人のプライバシーに配慮しながら、複数医療機関での一貫した治療に役立てることができる可能性がある。

- 文書管理（証憑等の真正性担保）

様々な文書について、作成、更新の履歴をブロックチェーンで管理することが考えられる。一方で、データそのものはブロックチェーンとは別の管理方法を用いる(分散 DB など)

ことで、ブロックサイズの肥大化を防ぐことも検討すべきであると思われる。

- 各種届出（出生、転居、結婚など）

主に行政における各種の届出を、ブロックチェーン上で管理することが考えられる。たとえば住民票をブロックチェーン化すれば、本人と転居前後の自治体の電子署名により、移転の手続きを完了させる、というようなことができる可能性がある。

- 投票

選挙における投票権をブロックチェーンで管理することも考えられる。(電子署名が安全に管理されている限り)なりすましによる二重投票を防ぐことが可能になるが、一方で、現在はできない「投票の委任」なども実現可能になると思われる。

(オ) 市場へのインパクト

関連する市場規模はそれぞれ以下の通りである。

- 土地の登記

法務省「登記情報システム」: 194 億円（平成 26 年度）[66]　※運用コストのみ

- 類似サービス

特許庁「特許事務システム」: 169 億円（平成 26 年度）[67]　※運用コストのみ
電子カルテ：約 2,000 億円（2018 年推計）[68]

（参考）地方自治体のシステム予算（H26 年度）[69]
市区町村：約 5,200 億円（うち運用約 3,300 億円）
都道府県：約 1,910 億円（うち運用約 1,270 億円）

- 投票

2012 年 12 月に実施された衆議院議員選挙では、587 億円の費用がかかっている。[70]

(カ) 産業構造へのインパクト

（1）当面の影響

対抗力を持つ土地の登記や特許等の権利登録や各種証明を、オープンな分散システムに

66 財務省「国・地方のＩＴ投資について」2015 年
67 財務省「国・地方のＩＴ投資について」2015 年
68 シードプランニング、2015 年
69 財務省「国・地方のＩＴ投資について」2015 年
70 http://www.soumu.go.jp/main_content/000235283.pdf

より安価に管理できることになるとともに、証明行為も必ずしも行政当局によるものではなく民間でも可能になる。その結果、法務省の土地登記システム等が不要になったり、地方自治体による証明・登録管理機能が不要となったりするので、政府・自治体の役割が狭まる可能性がある。

また、パスポート等をブロックチェーンで管理することで、偽造を防止できるようになる可能性もある。

（2）将来の可能性

- 本人証明・本人確認

本人証明としての印鑑文化や、各種契約時（携帯電話、銀行口座開設等）の際の本人確認のための書類提出等のプロセスが変化・代替される可能性がある。その結果、印鑑のメーカーなど、本人証明に係わる企業等が淘汰される可能性がある。同様に、金融機関等での口座開設時等に行う本人限定受取郵便等のオペレーションが代替される可能性がある。

- 権利証明

従来、登記対象にならなかった二者間の契約関係についても、ブロックチェーンを適用することで共有・追跡可能となり、その結果、契約上の権利についても対抗力を持たせることが可能となるなど、究極的には権威や信用力をもつエンティティが存在しなくても、権利証明等が対抗力を持つことになり、オープン且つ廉価な分散システムで行政機関等の役割を代替可能となる可能性もある。

5.2.3 サプライチェーン

製品の原材料からの製造過程と流通・販売までを、ブロックチェーン上で追跡可能であると考えられる。

(ア) ブロックチェーンで管理される主な情報

取引記録（受発注、納品予想/到着日時等）、加工品の加工履歴、個品単位の識別情報（ロット番号、仕様）、純正品であることの保証情報等、工業製品の製造から流通までの過程を逐一ブロックチェーンで管理することが可能である。

(イ) 活用するブロックチェーンの機能（図表 5-2 との対応）

ブロックチェーンの機能のうち、サプライチェーンの提供において重要となるのは「スクリプトによりアプリケーションを実行可能」「データのトレーサビリティが可能で、透明性の高い取引が可能（改ざんが困難）」「中央管理者が不在でも、悪意を持つユーザがいてもエコシステムが安定維持される」の三つであると想定される。

・スクリプトによりアプリケーションを実行可能

たとえば、製造工程において、二つの部品を別々に作り、それらを組み合わせる、という工程がある場合、部品の加工工程がそれぞれ完了するまで、組み合わせる工程に進まない、というような処理を、ブロックチェーン上で管理できる。

・データのトレーサビリティが可能で、透明性の高い取引が可能（改ざんが困難）

製品に不具合が見つかった場合に、原材料の単位までさかのぼってチェックが可能となり、たとえばリコール対象の範囲を特定しやすくなる。

・中央管理者が不在でも、悪意を持つユーザがいてもエコシステムが安定維持される

多くの原材料納入者、加工事業者、流通事業者が参加するサプライチェーン上で、特定のステークホルダーに依存しないシステムが運用可能となる。

(ウ) ブロックチェーン活用時の留意点

サプライチェーンにブロックチェーンを活用する場合には、下記の点に留意する必要がある。

① 記録の更新・追記権限の管理の必要性

誰が、どのタイミングで、どんな情報を記録できるのか、という権限管理が必要となる。

② 実際の加工プロセス・タイミングとの整合をとる必要性

上記①とも関連して、たとえば、加工が終了していないのに終了の記録をしてしまう、ということのないように、実際のプロセスとの整合をとる必要がある。

(エ) 類似の応用ケース

サプライチェーンの他、下記のサービスでも同様にブロックチェーンの活用が可能であると考えられる。

- 貿易取引

船荷証券（B/L）や信用状（L/C）をブロックチェーンで管理し、取引をスクリプトで管理することにより、従来では依然としてマニュアル的で非効率であった手続きの円滑化が可能になると考えられる。

- 貴金属・宝石類の管理

金やダイヤモンドなどの貴金属・宝石について、加工工程から単品管理していくために

ブロックチェーンを活用することで、購入者が加工の履歴まで確認することができるようになり、商品としての信頼性が増す可能性がある。

- 美術品等の真贋認証

美術品や工芸品に作成者の署名を付してブロックチェーンで管理することにより、その美術品が転々流通していった先においても、真正性を確認できるようになり、著作権管理の効率化が実現され、美術品等に関連した贋作事件等も減少すると考えられる。

(オ) 市場へのインパクト

関連する市場規模はそれぞれ以下の通りである。

GMS 全店売上高：約 13 兆円（2015 年度）[71]
コンビニ全店売上高：約 10 兆（2015）[72]
家電小売市場：7 兆 1,100 億円（2015）[73]
宝飾品市場：9,726 億円（2014）[74]
美術市場：1000 億円[75]
国内 SCM ソフトウェア：約 339 億円（2014 年度）[下記共に76]
製造管理ソフトウェア：約 318 億円（2014 年度）

(カ) 産業構造へのインパクト

（1）当面の影響

発注、見積、納品、検品、支払といった会計・経理プロセスや、トレーサビリティ品質管理業務が効率化されることが想定される。さらに、不正・不具合商品があった場合のトラッキングが容易になるほか、購入者へのコンタクトも容易になると思われる。

取引先履歴（トラックレコード）が参照できることで、情報の非対称性が解消され、取引先の選択リスクが軽減される。

（2）将来の可能性

- 流通・小売の商習慣の転換

現状は小売店（川下）、卸（川中）、製造（川上）で分断されている在庫情報や、川下に

---

71 日本チェーンストア協会　https://www.jcsa.gr.jp/public/data/tokei_H27.pdf
72 日本フランチャイズチェーン協会　http://www.jfa-fc.or.jp/particle/320.html
73 GfK ジャパン　http://www.gfk.com/jp/insights/press-release/2015-it-1/
74 矢野経済研究所　https://www.yano.co.jp/press/press.php/001365
75 日経 BP　http://business.nikkeibp.co.jp/article/manage/20091125/210545/
76 IDC Japan　http://www.idcjapan.co.jp/Press/Current/20150804Apr.html

集中していたタイムリーな商流情報（売れ筋情報）が、管理者不在で中立的に運営されるブロックチェーン上で共有・追跡可能となることで、サプライチェーン全体が活性化・効率化するとともに、川上の交渉力の強化につながる可能性がある。さらには、系列を飛び越えた新たなサプライチェーンシステムの構築も進む可能性がある。

- プレイヤーの交代

最終消費者と川上の製造者がより直接的に繋がる流通プラットフォームが誕生し、Amazon のような大規模な中間流通業者の存在意義が相対的に薄れる可能性がある。

電化製品等は、IoT の進展や製品保証とも連携することで、最終消費者への販売後のプロダクトライフサイクルをトラッキング可能となり、売切りではないビジネスへ転換することが容易になると考えられる。

5.2.4 シェアリングエコノミー

資産等の利用権移転情報、提供者や利用者の評価情報をブロックチェーン上に記録することが可能であると考えられる。現在は Uber や AirBnB のような特定の企業が運営するプラットフォームにより提供されている、いわゆるシェアリングエコノミー型のサービスにおいて、利用権の管理および取引を、ブロックチェーン上で行うことを想定する。

(ア) ブロックチェーンで管理される主な情報

シェアリング対象資産の利用権利等の保有者情報と、利用権利等の移転情報、金銭授受の情報が主に管理される。さらに、提供者および利用者の評価情報（口コミ情報）なども管理可能である。

(イ) 活用するブロックチェーンの機能（図表 5-2 との対応）

ブロックチェーンの機能のうち、シェアリングサービスの提供において重要となるのは「真正性の保証された取引が可能（二重支払の防止）」「データのトレーサビリティが可能で、透明性の高い取引が可能（改ざんが困難）」「中央管理者が不在でも、悪意を持つユーザがいてもエコシステムが安定維持される」の三つであると想定される。

・真正性の保証された取引が可能（二重支払の防止）

たとえば宿泊サービスの場合、特定の日に宿泊する権利が複数のグループに渡されてはならない。ブロックチェーンにより真正性が保証され、二重支払が防止できることは有用である。

・データのトレーサビリティが可能で、透明性の高い取引が可能（改ざんが困難）

流通する権利が、正当に流通していることが確認できることで、利用者の安心感が増す。

・中央管理者が不在でも、悪意を持つユーザがいてもエコシステムが安定維持される

現在のシェアリングサービスでは、プラットフォーム管理者が貸し手と借り手の仲介を行っているが、ブロックチェーンを用いることで管理者が不在でも取引が成立する仕組みが実現可能になる。

(ウ) ブロックチェーン活用時の留意点

シェアリングサービスにブロックチェーンを活用する場合には、下記の点に留意する必要がある。

① 記録の更新・追記権限管理の必要性

利用の開始、終了など、シェアされる対象物に関する情報の記録権限の管理が必要となる。

② 実際の利用・権利移転プロセス・タイミングとの整合をとる必要

場所や物品の明け渡しなどのタイミングで、正確にブロックチェーンに記録を残す必要があり、そのための手続きの明確化が必要となる。

③ 当事者間の金銭授受などとの連動の必要性

上記②と同様に、利用権の移転に伴って金銭の授受が発生する場合に、決済との連動をとる必要がある。決済もブロックチェーン上の仮想通貨で行うことも可能である。

④ プライバシーへの配慮

提供者、利用者とも、個人のプライバシーが安易に公開されないようなサービス設計が求められる。利用履歴の追跡が可能であることに留意したデータ管理の設計がされる必要がある。

⑤ ブロックチェーンへの手数料の支払い方法

採用するブロックチェーンによっては、サービスの利用料以外に、ブロックチェーンのトークンを支払う必要がある。多くの場合、トークンは取引の生成者が支払うことになり、今の場合は利用者になる可能性もある。そのときのトークンの負担条件等について、事前の取り決めが必要である。

(エ) 類似の応用ケース

シェアリングエコノミーの他、下記のサービスでも同様にブロックチェーンの活用が可能であると考えられる。

● C2C オークション

オークションにおいて、出品された商品をブロックチェーンで管理することにより、その商品の利用履歴などを残していくことが可能になると考えられる。

● 電子図書館

電子書籍の閲覧権をブロックチェーンで管理することで、電子図書館を実現可能になる可能性がある。

● スマートロック、コンセント

鍵を解除できる権限やコンセントから電気を利用する権限など、家庭に関するシーンでも様々な利用シーンが想定されると同時に、これらをシェアリングサービスとして応用するビジネス形態が出てくる可能性がある。

● デジタルコンテンツ

上記の電子図書館と同様、コンテンツの利用権をブロックチェーンで管理することで、著作権者を保護しながら、利用の促進を図れる可能性が考えられる。

● チケットサービス

転々流通可能なチケットをブロックチェーン上で正式に発行、管理することで、違法なダフ屋などの介在なしに、チケットの効率的な流通販売管理が可能になる可能性がある。

(オ) 市場へのインパクト

【シェアリングエコノミー】

市場規模（国内）：約 230 億円（2014 年）[77]

※うち、自動車：約 180 億円、賃貸：約 4 億円、衣類等：約 6 億円、人材：約 27 億円、金融：約 11 億円

2018 年度の同市場の市場規模（国内）は 462 億円と予想されている

【類似サービス】

C2C オークション：約 1 兆円（2014 年）[78]

スマートロック：約 500 億円（2014 年）[79]

---

[77] 矢野経済研究所

[78] 2014 年 10 月 31 日　日経 MJ

チケットサービス：約 5000 億円（2013 年）[80]
デジタルコンテンツ：約 12 兆円（2014 年）[81]
図書館：公立図書館の経常図書館費のうち、臨時経費を除いた額は約 1000 億円（2014 年）[82]
※クラウド型図書館情報管理システムは約 9 億円（2014 年）[83]

（カ）産業構造へのインパクト

（1）当面の影響

新興市場としてのシェアリングエコノミーの成長促進に寄与する可能性がある。例えば、シェアリングエコノミー関連ビジネスにおいて、コンシューマからのセキュリティに関する信用が一般論として低い場合に、ブロックチェーン利用によるセキュリティへの信頼度向上が図れる可能性がある。

また、ブロックチェーン活用による自社システムへの投資コスト低減により発生する余剰資金のビジネスへの投資促進が進む可能性もある。

異なるシェアリングエコノミー間で参加者の評価・口コミが共有されることで、情報の非対称性が解消され、より取引が活発化し、市場が拡大することも想定され得る。

（2）将来の可能性

- シェアリングエコノミー・サービス事業者の不要化

遊休資産の稼働率向上のほか、入場券、客室、レンタカー、レンタルビデオ等の利用権限管理に劇的な効率化がもたらされることが期待される。一方で、究極的には C2C 取引が、現在のシェアリングエコノミーのプラットフォーム事業者を介在せずに行われる環境が構築される可能性も存在すると考えられる。

- プロシューマの台頭

「生産者/サービス提供者」と「消費者」の境界がなくなることで、「プロシューマ」というあり方が一般化する可能性がある。

---

[79] フォトシンス
[80] 2014 年 5 月 12 日　The Bridge、
http://thebridge.jp/2014/05/startups-trying-to-ticket-business
[81] デジタルコンテンツ協会　「デジタルコンテンツ白書 2015」　2015 年
[82] 日本図書館協会図書館調査事業委員会　「日本の図書館　統計と名簿」　2015 年
[83] 富士キメラ総研

5.2.5 スマートコントラクト

契約条件、履行内容、将来発生するプロセス等をブロックチェーン上に記録することが可能であると考えられる。スマートコントラクトという発想は 1990 年代にはすでに提唱されていたが[84]、ブロックチェーンにより、第三者を介在させずに実現させることが可能になった。

(ア) ブロックチェーンで管理される主な情報

契約条件、履行内容、各種手続き、業務のプロセスが記録される。

(イ) 活用するブロックチェーンの機能（図表 5-2 との対応）

ブロックチェーンの機能のうち、スマートコントラクトの提供において重要となるのは「スクリプトによりアプリケーションを実行可能」「真正性の保証された取引が可能（二重支払の防止)」「データのトレーサビリティが可能で、透明性の高い取引が可能（改ざんが困難)」「安定したシステムの構築・運用が可能（ゼロダウンシステム)」の四つであると想定される。

・スクリプトによりアプリケーションを自動実行

スマートコントラクトは、様々な処理を自動実行するため、事前に処理をスクリプトとして登録しておく必要がある。スクリプトは、条件が整った段階で、逐次実行される。

・真正性の保証された取引が可能（二重支払の防止）

状況にもよるが、同じ処理が複数回実行されないような仕組みが必要となる。また、契約の履行が後から証明できるという点も重要である。

・データのトレーサビリティが可能で、透明性の高い取引が可能（改ざんが困難）

スクリプトそのものの更新や、処理の履歴などがトレースできることが重要である。

・中央管理者が不在でも、悪意を持つユーザがいてもエコシステムが安定維持される

契約の管理などでは、個々の企業がブロックチェーンを持つのではなく、オープンなブロックチェーン上で契約の記録が残ることが重要である。

(ウ) ブロックチェーン活用時の留意点

スマートコントラクトにブロックチェーンを活用する場合には、下記の点に留意する必

[84] http://szabo.best.vwh.net/smart.contracts.html

要がある。

① 記録の更新・追記権限管理の必要性

契約内容が不正に書き換えられることのないよう、スマートコントラクトの更新について、権限管理が重要となる。

② 資産の権利保有者の情報、資産の権利移転の情報、資産の権利移転に要する金銭授受の情報の管理の必要性

スマートコントラクトで対象とする資産や金品の移転について、それぞれの管理が必要となる。

③ 金銭授受に用いるクレジットカード等の情報、その他個人の資産（株式等）の情報等の管理の必要性

資産の授受に伴い発生する決済について、法定通貨を使うのか、仮想通貨を使うのか、等についても、事前の取り決めが必要である。

④ データの修正が困難

一旦ブロックチェーンに記録した情報を修正するのは困難なため、スマートコントラクトの内容に間違いがあったり、処理を誤って実行してしまったりした場合などの対応策が必要である。

(エ) 類似の応用ケース

スマートコントラクトでは、契約に関連する業務全般のほか、下記のサービスでも同様にブロックチェーンの活用が可能であると考えられる。

- デリバティブ（金融派生商品）

デリバティブ取引では、様々な条件で資金のやりとりが行われる。それらの条件をスマートコントラクトによって定めておけば、すべて自動的に条件判断と決済処理が行うことが可能になると考えられる。

- エスクローサービス

取引の仲介に、第三者をたてなくても、ブロックチェーン上のスマートコントラクトにより、エスクローを実現できると考えられる。

- エネルギー管理

ブロックチェーンに接続された電気機器（家電や電気自動車など）がスマートコントラ

クトによって、利用状況などに応じて自動的に充電を行い、あらかじめ決められた方法で決済を行ったりすることが具現化される可能性がある。

- 遺言

遺言をあらかじめスマートコントラクトとして定めておくことにより、当人が死亡したことをきっかけとして、遺言が自動的に執行されるようにすることが可能になると考えられる。

- 会社清算

会社精算時の資産や各種の権利の配分を、スマートコントラクトによって自動的に処理することができるようになると考えられる。

(オ) 市場へのインパクト

【スマートコントラクト】[85]
財務・会計ソフト：約 700 億円
連結会計ソフト：約 75 億円
人事・給与ソフト：約 540 億円
※上記はいずれもパッケージソフト＋クラウドサービスの合計値。
電力サービス：8 兆円[86]　※2016 年 4 月に自由化される電力小売の市場規模。
IoT：5185 億円（2015 年）[87]
相続税：11.6 兆円（2013 年度）[88]　※課税価格

(カ) 産業構造へのインパクト

（1）当面の影響

各企業におけるバックオフィス業務（契約や取引の執行、支払・決済、稟議などの意思決定フローなど）の大半を置きかえることが可能であると考えられる。また、契約の履行を監督する第三者機関が必要なくなるため、エスクローサービスなどが不要になる可能性がある。

契約が自動執行されることで、契約相手の信頼性に依存せずに契約内容が履行されるた

---

85 富士キメラ総研

86 http://www.enecho.meti.go.jp/category/electricity_and_gas/electric/electricity_liberalization/pdf/summary.pdf

87 野村総合研究所　桑津浩太郎　「2030 年の IoT」　東洋経済新報社　2015 年

88 国税庁　https://www.nta.go.jp/kohyo/tokei/kokuzeicho/sozoku2013/sozoku.htm

め、契約不履行に起因する係争案件が減少し、結果的に係争費用が抑えられる可能性がある。

（2）将来の可能性

- 契約執行の自動化

現時点で書面としての契約形態をとらない様々な取引シーンが、スマートコントラクトとしてブロックチェーンに書き込まれるようになることで、数多くの取引が自動で実行され、取引の効率性が飛躍的に高まる可能性がある。例えば、取引相手との実績等に関わらず、自動的に最適条件で取引・決済がされるようなもので、機器間での余剰電力売買や機器に必要な補充剤購入などが考えられる。そうした世界では、各企業・組織は、その仕組みに対応した製品・サービスを志向するようになると考えられる。

- 徴税と公的サービスの最適化

IoT 活用の世界にスマートコントラクトによるマイクロペイメントを組み合わせることで、受益者負担をより正確に反映したコスト負担の仕組みが構築可能となり、自治体行政の見える化を図ることが可能となると考えられる。例えば、ごみの量に応じて料金徴収等が可能であり、住民税徴収の在り方が変化する可能性もある。同様に、道路の利用量に応じた料金徴収により、有料道路の料金所が不要になったり、自動車税やガソリン税等の在り方が変化したりする可能性もある。

- 管理者不在の IoT 機器管理

センサーなど無数のノードが膨大化する IoT 活用の世界で、管理者不在でこれらの不特定多数のノードのみならず、ノード間の通信を含むあらゆるプロセスや取引を管理し、データの信頼性・セキュリティ上の問題を担保するブロックチェーン技術を用いたミドルウェアが登場する可能性がある。個々のデータの権利情報をトラッキングして権利者へフィードバックするなど、全く新たな機器管理・データ管理手法が生まれる可能性がある。

6　社会へのインパクトと中長期課題

ここでは、ブロックチェーンが社会に与えるインパクトと中長期的な課題を、①技術、②ビジネス・業務、③制度・産業政策の三つの視点で考える。

6.1　社会へのインパクト

5.1 章でも述べたとおり、技術的には、

- 真正性の保証された取引が可能（二重支払の防止）
- データのトレーサビリティが可能で、透明性の高い取引が可能（改ざんが困難）
- 中央管理者が不在でも、悪意を持つユーザがいてもエコシステムが安定維持される

という点について、ブロックチェーン活用の可能性が見込まれる。

より発展的には、ブロックチェーンは、ある一定規模の参加者が存在する系において、特定の主体やシステムに依存することなく、ネット上の価値や情報について相互に承認するプロトコルである、とも定義できる。

一方で、国内外の実務者へのヒアリングからは、ブロックチェーンを用いることが必ずしも必要ではない場合があることや、既存のシステムを置き換えるのに多大なコストがかかってしまう可能性があることが指摘されたのも前述の通りである。

短期的には、ブロックチェーンを活用して、個別用途のサービスが多数出現する。地域通貨などの価値情報の取引を扱うサービス、シェアリングサービスを取り扱うサービス、商流管理を行うサービスなどである。同様に、土地の登記や特許、各種証明書などの管理についても、それぞれ個別にサービスが立ち上がる。共通するのは、それぞれの事業分野において、「中間的な第三者」が不在でも成立するビジネスモデルが考案され、サービスが提供されるということであり、その場合の当該市場への影響は大きいものと考えられる。また、ブロックチェーンの採用により、システムの構築・運用のコストが下がる可能性もある（図表 6-1）。

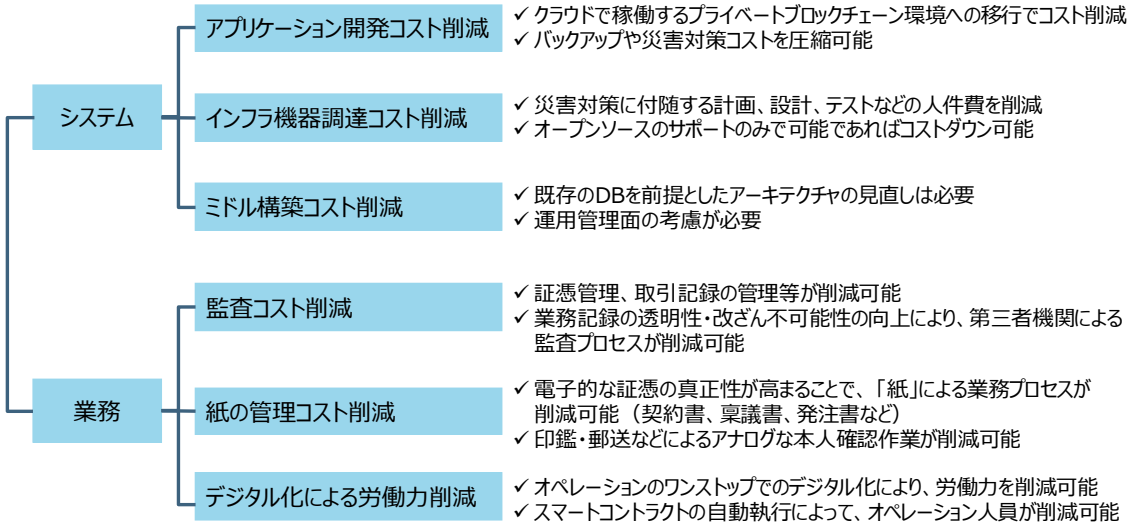
2016 年 5 月に開催予定のロンドン市長選挙において、候補者の一人である George Galloway は、市政予算利用使途の可視化を、ブロックチェーン技術を用いて実施することを表明しており、本プロジェクトを「MayorsChain」と名付けている。MayorsChain により、公共支出の記録を行うとともに、誰にでも追跡可能な環境を構築するとしており、これにより約 5%の予算削減が可能であるとしている[89,90]。このような、行政システムにブロ

[89] http://mayorschain.com/

[90] http://uk.businessinsider.com/george-galloway-blockchain-bitcoin-mayorschain-london-

ックチェーンを採用する動きも、順次進んでいくと想定される。

図表 6-1　ブロックチェーンの導入により期待されるコスト削減効果



中長期的には、それぞれ独立していたサービスが、相互に連携を始めることが想定される。そうすると、ブロックチェーン上に流通させた「権利」や「情報」が、それぞれのブロックチェーン上で価値を判定され、その価値によって、また別の「権利」や「情報」と交換する、ということが起きるようになる。たとえば、民泊のサービスと、地域通貨のサービスとが接続されることにより、A 氏が保有している「B 氏の別荘に 1 泊する権利」で、「C 市の市営プールの回数券」を支払う、というようなことが、中間事業者を介さずにできるようになる。これは、ブロックチェーンにより、物々交換が復権する、とも言えるだろう。仮想通貨や法定通貨は、価値交換の差分を補うためだけに必要となる。

ビジネス領域においては、様々な取引がスマートコントラクトとしてブロックチェーンに書き込まれるようになることで、自動化、省力化されていくだろう。原材料の輸入から、加工、販売、サポートに至るまで、個品単位でのトラッキングが自動で可能になり、かつ、この過程でも中間的な事業者が排除されていく。特に流通においては、生産者と最終消費者が直接取引を行えるようになる。ここでは、IoT の発展とも密接に関わってくる。材料や備品の受発注、利用量の測定と課金、警告の通知と一次対応など、様々な場面で、ブロックチェーンに接続されたセンサーが、自律的に業務を行うようになる。

消費者向けサービスと同様に、企業が持つ様々な資産（自社や他社の株式、特許、不動産など）がブロックチェーン上で流通を始めると、それに基づいた価値の流通や、信用創

造なども行われるようになる。大きな資産と信用力を持つ企業は、一国の政府に匹敵する金融コントロール力を持つようになる。

そして、これらの進展は、サービス面でも、ビジネス面でも、すべて世界規模で拡大していくと想定される。

当然、行政のあり方も大きく変わる。土地の登記、特許の管理、婚姻など、行政が（状況の把握は必要であっても）必ずしも事務処理を担う必要がないものについては、順次ブロックチェーンに移行していく可能性が考えられる。役所などでは、印鑑の代わりに、スマートフォン等のデバイスに格納したウォレットで電子署名する、というのが当たり前になっていくことも想定される。また、サービス領域、ビジネス領域のブロックチェーンのサービスに、納税の仕組みをトークンの支払いという形で組み入れることで、税金徴収の自動化と効率化が実現され、受益者負担の仕組みを確実に実現できるため、税のあり方へも影響を与える可能性がある。

6.2　中長期的な課題

ブロックチェーンに関連する課題が、様々なアプローチにより対策がとられているのは前述の通りである。しかし、上記課題に関わらず、中長期的な課題も存在する。

6.2.1 技術面での課題

(ア) 実世界との整合

実世界との整合については、先の自動販売機の例のように、外部から適時ブロックチェーンに指示を出していかなければならず、かつ、それがブロックチェーンに取り込まれるタイミングが事前にわからない、といった問題がある。特に時刻との整合について、同期をとるのが非常に難しくなっている。たとえば、『5 月 1 日の 10 時に処理 A を実行する』というような処理は、10 時ちょうどに処理が動き始めることを保証できない。類似の課題として、CAP 定理によれば、ファイナリティは確定しない。よって、サービス毎に運用で対応することになる。たとえば、ビットコインの取引では、6 ブロック確定すれば処理が確定できるものと見なしている。これは、次のブロック以降で別のフォークが優位になることを否定していないことに注意が必要である。

(イ) 情報の修正

記録が改ざん不可能な形で残るのはブロックチェーンの大きな特徴であるが、これは逆にいえば、後からこの記録を修正することができない、ということでもある。操作のミス、スクリプトのバグ等にどう対応するかであったり、個人情報やプライバシーに関する情報がブロックチェーン上で公開されてしまった場合にどのように保護していくのか、といった検討が必要である。

(ウ) 個別技術の適切な応用

P2P ネットワークの分断耐性の確保や、タイムスタンプの正確性の保証、秘密鍵の安全な管理手法など、過去からの技術的知見が十分に活用されていない課題が見られ、ブロックチェーンの開発者コミュニティと既存の研究者コミュニティとの交流が必要と考えられる。

(エ) コストダウンについての具体的な検証

しばしば喧伝される「サーバコスト（構築/運用）の低廉化」については、既存のクライアント/サーバ型の基幹系システムを置き換える場合に、情報系システムなどの周辺のシステムとの整合をとる必要性などを考慮しなければならない場合には、必ずしもコストメリットが得られない可能性も考えられる。実際にどの程度のコストが削減可能なのかについ

て、個別事例毎の検証が必要である。

6.2.2 ビジネス面での課題

(ア) リアル取引との連動性の確保

ビジネス面においても、リアル取引との連動性をどう確保するかは大きな課題である。特に即時性が求められる動作の保証がされない点は大きな課題となる。この課題はファイナリティの問題と密接に関連している。ファイナリティが一定の時間内になされることをどう担保するかという点に関しては、コンセンサスアルゴリズムにおいて、PoW を改善・拡張する方向、つまり PoI や PoS などの新たなアルゴリズムを導入する方向を目指すやり方と、PoW に依存しない PBFT といったファイナライズを極めて短時間で実施可能なアルゴリズムを搭載することにより対応を目指すやり方の二つに大別される。現時点で両者の優劣は不明だが、これらの取り組みがファイナリティの課題に対する本質的なアプローチであることは間違いない。一方で、コンソーシアム型/プライベート型のブロックチェーンの場合、0rb のように、特定のノードが強制的にフォークを修正していく、という方法も可能である。あるいは、ビジネスルールとして、ファイナリティの確認方法や、フォークが起きた際のルールを事前に決めておく、ということもあり得る。これらの二つは、より現実的な対応といえる。

今後は、実際のビジネスの各領域で実際に必要とされるファイナリティの要求によって、それぞれのアプローチの有効性が検証されることが望ましい。

(イ) SLA の整備

ブロックチェーン上でサービスを提供するにあたり、SLA（Service Level Agreement）の整備も必要である。現状では、ブロックチェーンのダウンタイムが何を指すのか、遅延処理はどの程度の頻度で発生し、解消にどの程度かかるのかといったサービスレベルの定義が曖昧である。実ビジネスに適用する際にはこれらのブロックチェーンに関わる各性能要件や仕様を明確にしていく必要がある。そのためにはブロックチェーンの適用業務の分類を行い、それぞれの業務のクリティカル度合いに応じた SLA の雛形を整備することも必要となる。

これらの SLA の整備には業界ごと、さらには業界横断的な専門家の協議が必要となることは過去の様々なシステム領域での SLA の整備の経験から明らかであろう。一方で、ブロックチェーンは既存の分散システムとは異なる特性を持つことにも留意が必要である。既存のシステムの評価指標を単純にブロックチェーンの評価指標として用いると、ブロックチェーンの特性を効果的に表現できず、結果として当該技術の活用を妨げる可能性もある。ブロックチェーン領域の専門家と、既存のシステムの専門家の広範な情報共有・議論の場を整備することが必要である。

さらには、整備されたSLAに基づく人材育成も急務である。現在のブロックチェーンの技術者は既存のカリキュラムで育成された人材ではなく、自ら進んでブロックチェーン技術を追求してきた経緯を持つ。今後は産学官それぞれの分野できちんとデザインされたブロックチェーン技術者を要請するプログラムが必要となるであろう。

（ウ）ブロックチェーン領域の標準化活動

ブロックチェーンは分散システム領域におけるイノベーションであり、多くの課題があるものの非常に大きな可能性を秘めている。ただ現状では標準化に対する活動がなされているとは言いがたい状況である。ブロックチェーンはその技術的な特性上、各ノードはネットワークへの参加者ではあっても、システム構成を決める主体とはなりにくい構造を持っている。そのため、ブロックチェーンの技術的な改善・拡張についての効率的な意思決定プロセスはいまだ模索中である。ブロックチェーンを活用したいと考える企業にとっては、技術仕様の将来像の予測可能性、もしくはコントロール可能性は非常に重要な点である。

MIT Media LabのJoi Itoはブロックチェーンの発展とインターネット黎明期を対比させ、ブロックチェーンのコミュニティ活動の活性化の促進と同時に、国際的な標準化活動の必要性を唱えている。現在様々なブロックチェーンの拡張が試行されているが、これらの試行を放置したままでいると、互換性・発展性のない規格が乱立する状況に陥る可能性もある。市場の効率的な発展のため、なんらかの標準化の活動が求められている。

（エ）取引コスト負担ルールの明確化

ビットコインブロックチェーンでは、今までの金融システムを介して行なう送金よりは遥かに低額な手数料で取引が可能になったというイノベーションをもたらしたことは事実である。一方で現行のビットコインブロックチェーンでは、取引を行なう際の情報の送信時に、手数料（ネットワークトランザクション手数料）としてビットコインの支払いが要求される仕様となっている。そのため、ビットコインで物品を購入する際は、物品の代金に加え、手数料が必ず必要となる。

しかもビットコインでは、この取引手数料は送金を行なう側に負担させることが一般である。通常のビジネス取引では、送金側に手数料負担を強いるケースは限られており、現行のビジネス慣習との整合性をどう整理するのかという点を検討する必要がある。

また、ビットコインをはじめとしたブロックチェーンでは、送金の手数料は、送金の「額」によらず、送金の「情報量」に比例する。既存の金融システムの送金の手数料が、おおよそ送金する金額に比例することと比較すると、少額の取引に関する送金手数料の負担をどうすべきか、という点は重要である。特に、ブロックチェーン技術のIoTへの適用が議論されているなか、マイクロペイメントの観点から、どのような送金手数料負担のルール化を行なうべきかという議論は今後ますます重要性を増していくと考えられる。

（オ）法定通貨との交換比率の明確化

ビットコインに代表される仮想通貨は、法定通貨との交換比率が必ずしも一定していない。そのため、法定通貨のみで規定されている商品やサービスなどを取引する際に、決済の仕組みが煩雑になるおそれがある。たとえば株券をビットコインに類する仮想通貨で買い付ける場合、どのようなレートで法定通貨を換算するのかについて、あらかじめ関係者間の合意ができていることが必要となる。

さらには、ビットコインに代表される法定通貨と連動した仮想通貨は、その価値変動が非常に大きい状態が続いている。このような価値変動が続いた場合、一般の企業にとっては手数料（もしくは取引金額）の変動が大きくなるため、取引金額の予測可能性が低下するリスクが高まってしまう。このような課題を解決するための検討が必要である。

（カ）匿名性・プライバシーの保護と本人確認などとのトレードオフ

現行のビットコインでは、取引の主体の匿名性はある程度担保されているが、トランザクションデータは公開されており、その点でのプライバシーは保証されていない。このようなトランザクションの内容が公開される仕組みでは、取引の詳細を秘匿したい場合には活用できない。例えば競合他社には知られたくない企業の契約内容などをどう保護するのかといった観点は重要である。

一方で、ビットコインは本人確認などのプロセスを経ないまま取引への参加が可能であり、金融システムの観点からすればアンチマネーロンダリングといった点での懸念が強い。プライベート型もしくはコンソーシアム型でのブロックチェーンの運用であればこれらの懸念はある程度解消されると思われるが、より広範な議論が必要であろう。

6.3　行政への期待

ブロックチェーンについて、中長期での社会へのインパクトと、残存する課題とから、行政に期待されるのは下記であると考えられる。

(ア) ユースケースの蓄積支援

残念ながら、現在我が国のブロックチェーンに関連する領域において、海外と比較して人材・モノ・金・情報面での支援が少ないとの意見もある。特に、ベンチャー企業への投資額もブロックチェーン領域に関しては質・量のどちらも低調であるとの指摘もなされている。ブロックチェーン技術の可能性を早期に判断するためには、様々な領域での実証実験による仮説検証が不可欠である。仮説検証の数を早期にいかに増やすかが喫緊の課題である。

一方で、現在の我が国のブロックチェーンの実証実験の取り組みは、個別企業との散発的な取り組みが多く、業界横断的もしくは業務プロセス横断的な取り組みは少ないといわざるをえない。個別企業との取り組みの重要性を否定するものではないが、限られたブロックチェーン技術者のアウトプットを最大化するためには、業界横断的な、核となるユースケースを素早く検証することが求められる。そのためには、所轄官庁および業界団体などが率先して、インパクトが大きいユースケースを想定し、それらのユースケースに対する検証を行なう体制構築が急務である。

(イ) ブロックチェーン技術開発・蓄積の支援

ブロックチェーン技術に利用されている暗号技術、データベース技術は決して目新しいものではない。一方で日本には暗号技術、データベース関連の研究者の蓄積は諸外国と比較しても決して遅れをとるものではない。また、ブロックチェーン技術の領域で今後より重要性を増すであろうヒステリシス署名分野や、暗号化を行ったままでの演算技術分野などにおいても、世界に対して強みがある。しかし、これらの分野において、ブロックチェーン技術が評価の俎上に上っていない。

電子署名に関して、当初は公開鍵証明書が必要だとは考えられていなかったように、技術が提唱された初期段階では想定されない問題点が存在することは往々にしてある。技術の確からしさに関する共通認識の構築、およびそれによる標準化作成において、暗号・電子署名技術者および彼らの技術的蓄積を活用することで、国際貢献に資する体制の構築が可能である。また、体制の構築に当たり、政府としての支援も行えるであろう。

さらには、日本のブロックチェーン関連ビジネスの発展及び国際競争力強化に寄与するため、国内の産業界の要請があれば、ブロックチェーン技術の国際的な標準化に対する活動へのプレゼンスを確保するためにも、関連する技術等への支援を積極的に行なうことが求められる。

（ウ）基礎研究の充実

ブロックチェーン技術は、情報理論上様々な課題を抱えているという指摘がなされている。分散システムの理論上の定理との整合性などを検証することが求められている。我が国の重点的な研究分野としてブロックチェーン関連の数理・情報理論面の研究を支援することは、ひいては国際的な貢献にも繋がる重要な領域である。

（エ）既存の行政システムの見直し

ブロックチェーン技術は「中央管理者を必要としない相互承認インフラ」として機能する可能性を持つ技術である。この技術を適用することで、既存の行政手続きの飛躍的な効率化が達成される可能性が指摘されている。

一方で、我が国の既存の行政システムの電子化はまだ途上である。現在進められている行政システムの電子化をさらに推し進めるためにブロックチェーン技術を活用することが可能である。民間の例ではあるが、ブロックチェーンを用いて株式の発行・売買を行なうようなケースでは、株式の電子化がそもそも必要となるように、行政においても、様々な権利の保有を証明するために「券」が必要であったアーキテクチャから、「権利の保有」を記載する「名簿化」への移行があらゆる領域で進展することが望まれる。より広範な観点として、本人確認などに活用できるブロックチェーンを用いた「パブリック公示ブロックチェーン」システム等の導入・構築も考えられる。既存のアナログな行政システムを電子化する際には、将来的なブロックチェーン技術の活用を見越した検討が必要であろう。

（オ）税法の最適化

多くのブロックチェーンでは、処理を実行する際に、トークンを消費する仕組みになっている。これを、徴税に活用することが考えられる。納税が必要な手続きにブロックチェーンを利用することにより、トークンの形で徴税を行うことが可能になる。たとえば、自動車の登録番号をブロックチェーンで管理することを考えたとき、新たに自動車を登録したり、利用者の変更の手続きをしたりする際に、トークンによって税相当額（自動車税など）を支払うような仕組みが考えられる。これにより、事務手続きと徴税とを一体化できる。また、スマートコントラクトが普及すれば、契約手続き等に伴う印紙税の徴収も同様に自動化が可能となる。この場合、印紙税のあり方も含めた議論が必要となる。

（カ）技術進歩を見据えた法規制の検討

法規制を検討する際の、「法と経済学」的な観点（規範、市場、アーキテクチャ、制度）での検討の必要性も指摘されている。株式、債券のように、管理を名簿方式に移行できるのであれば、適用領域は広がると見込まれる。

民事訴訟法 228 条によれば、押印した文書に認められている 2 段の推定に相当する電子

データは、電子署名法で認められた認証局より発行された電子証明書のみである。ブロックチェーン上に記録されたデータが、どのような要件を満たしていれば、民放でどの程度の証拠能力が認められることとなるのかの整理が必要である。

また、消費者保護の観点からは、トークン市場でアセットを発行した場合の規制法が不明であるとの指摘もある。ブロックチェーン上でのシェアリングエコノミーが発達すると、「A を利用する権利」で「B を利用する権利」を購入する、というようなことが可能になると考えられるが、この場合の消費税をどう考えるか、ということも整理が必要となる。資金決済法だけでなく、税法との関係の整理が必要である。

さらには、様々なブロックチェーンが、国境を越えてサービス展開されることが想定される。その場合の規制や税制のあり方について、国際間で連携した検討が必要となる。

7　まとめ

7.1　ブロックチェーンとは何か

P2P ネットワークを利用して、

- 真正性の保証された取引が可能（二重支払の防止）
- データのトレーサビリティが可能で、透明性の高い取引が可能（改ざんが困難）
- 中央管理者が不在でも、悪意を持つユーザがいてもエコシステムが安定維持される

という仕組みである。

より発展的には、インターネット上において、価値情報を相互承認するプロトコルである、といえる。

7.2　誰が、何に使えるのか

民間企業は、様々なサービスにおいて、『中間的な第三者』が介在しない形でのサービスを提供できる可能性がある。すでに様々な分野への活用方法が提案されており、実際に応用した場合にどのくらいのインパクトがあるのかの検証が始まりつつある。

企業や行政機関は、既存の業務をブロックチェーンに置き換えることにより、コストの削減ができる可能性がある。いくつかの国では、実際に公共インフラとしての採用を検討し始めている。

7.3　どんな影響があるのか

様々な分野で、「中間的な第三者」が存在しない、新たなビジネスモデルが出現し、より効率的なサービス提供がされるようになり、当該分野におけるエコシステムが変わる。

「価値」のとらえ方が変容する。仮想通貨を介して、様々な資産や情報を直接交換することが可能になる。

企業内及び企業間の様々な仕組みが自動化され、事務手続きなどの効率化が進む。

行政や自治体の仕組みとして導入されると、様々な事務処理が簡素化され、コストが削減され、その結果として、行政はより実体的な業務に集中することが可能になると同時に、徴税の仕組みについて、税のあり方も含めた再検討が必要となる可能性がある。

7.4　課題は何か

理論的な検証がなされていない。同時に、実サービスへ応用した場合の実証も少ない。既存のシステムと考え方が大きく異なるため、サービスレベルやセキュリティ確保の方法

論なども定まっていない。

よって、技術面、ビジネス面の双方で、より詳細な検討が必要である。

7.5 政府は何をするべきか

暗号分野など、既存の技術的蓄積を、ブロックチェーンに応用するための誘因を行うことで、ブロックチェーンの発展に寄与できる。同時に、国内におけるブロックチェーンの仮説検証の促進と成果及び課題の集積を行い、広く公開していくことで、市場の発展を効率よく促すことができる。

また、行政分野におけるブロックチェーン活用の検討をすすめることで、行政の効率化、高度化を推進可能である。これには、税制を含めた制度設計のあり方にも一石を投じる可能性がある。

さらには、上記のような様々な変化が、国境を越えて世界規模で起きることが想定されるため、各国間で協調的に対応をとっていく必要がある。

参考資料1　　ブロックチェーンに関する検討会

本調査にあたっては、国内のブロックチェーン企業関係者、有識者による「ブロックチェーンに関する検討会」を 2 回実施した。概要は以下の通りである。

参考1.1　　委員

朝山 貴生　　テックビューロ株式会社　代表取締役社長
岡田 仁志　　国立情報学研究所　准教授
楠 正憲　　ヤフー株式会社　CISO Board　/　内閣官房　情報通信技術（IT）総合戦略室　政府 CIO 補佐官
栗元 憲一　　株式会社 Nayuta　代表取締役社長
斉藤 賢爾　　株式会社 Orb　Chief Consultant
志茂 博　　コンセサス・ベイス合同会社　CEO
杉井 靖典　　カレンシーポート株式会社　代表取締役 / CEO
肥後 彰秀　　株式会社ガイアックス　技術開発部長
藤村 滋　　NTT サービスエボリューション研究所　研究主任
本間 善實　　一般社団法人日本デジタルマネー協会　代表理事
増島 雅和　　森・濱田松本法律事務所　弁護士
（50 音順、敬称略）

参考1.2　　第 1 回検討会

日時：平成 28 年 2 月 22 日（月）15:30 - 17:30
会場：経済産業省本館 17 階　第 2 共用会議室

議題
1. 開会挨拶・趣旨説明
2. 「ブロックチェーンとは」「適合分野と社会の将来像」
   「社会に与えるインパクト」（事務局説明）
3. 委員プレゼンテーション
   委員 B プレゼンテーション
   委員 C プレゼンテーション
   委員 D プレゼンテーション
4. ディスカッション
5. 次回について

配布資料
資料 1　議事次第・委員名簿
資料 2　事務局説明資料
資料 3　委員 B　御提出資料
資料 4　委員 C　御提出資料
資料 5　委員 D　御提出資料

参考1.3　　第 2 回検討会

日時：平成 28 年 3 月 7 日（月）17:00 - 19:00
会場：経済産業省本館 9 階　西 8 共用会議室

議題
1. 前回の振り返り（事務局説明）
2. 委員プレゼンテーション
   委員 J プレゼンテーション
   委員 F プレゼンテーション
   委員 K プレゼンテーション
3. ユースケースの紹介（事務局説明）と議論
4. 課題の整理と政策対応のまとめ
5. 検討会終了後の進め方
6. 閉会挨拶

配布資料
資料 1　議事次第・委員名簿
資料 2　事務局説明資料
資料 3　委員 J　御提出資料
資料 4　委員 F　御提出資料
資料 5　委員 K　御提出資料

参考1.4　第 1 回検討会　議事録

ブロックチェーンに関する検討会
第 1 回議事録

日　　時：　平成 28 年 2 月 22 日（月）15:30 – 17:30
場　　所：　経済産業省本館 17 階第 2 共用会議室

出席委員：
NTT サービスエボリューション研究所
株式会社 Orb
株式会社ガイアックス
カレンシーポート株式会社
コンセンサス・ベイス合同会社
テックビューロ株式会社
株式会社 Nayuta
一般社団法人日本デジタルマネー協会
ヤフー株式会社　/　内閣官房
欠席委員：
国立情報学研究所
森・濱田松本法律事務所
（以上、50 音順）

事務局　：　経済産業省
株式会社野村総合研究所

資　　料：　1.　議事次第・委員名簿
2.　事務局説明資料
3.　委員 B　ご提出資料
4.　委員 C　ご提出資料
5.　委員 D　ご提出資料

議　　題：　1.　開会挨拶・趣旨説明
2.　「ブロックチェーンとは」、「適合分野と社会の将来像」、「社会に与えるインパクト」（事務局説明）

3. 委員プレゼンテーション
    ・委員 B プレゼンテーション
    ・委員 C プレゼンテーション
    ・委員 D プレゼンテーション
4. ディスカッション
5. 次回について

1. 開会挨拶・趣旨説明

始めに、経済産業省　情報経済課より、本検討会の開会挨拶、趣旨説明が行われた

情報経済課：

本日は第 1 回検討会につきまして、お忙しい中、お越しいただきありがとうございます。

趣旨説明は資料 2 の P3 にも記載しているが、ビットコインの取引に使用されているブロックチェーン技術に関して、様々な分野への応用が期待されている。一方で、やや過大な期待や、十分に見極められていない部分があり、見極める必要があると考えている。

検討会は 2 回しかないが、活発に議論いただき、新しいブロックチェーン技術について、ユースケースも含めて、見極めて行きたいと考えている。

本日は、ヒアリングもしながら議論していただくが、議論のやりとりは非公開ということにさせていただいている。堅苦しい場に感じるかもしれないが、活発に議論していただければ幸いである。

2. 「ブロックチェーンとは」、「適合分野と社会の将来像」、「社会に与えるインパクト」（事務局説明）

事務局より、各委員に対し資料の確認、及び資料 2「ブロックチェーンに関する検討会　第 1 回討議用資料」に関する説明が行われた。それに基づき、以下の議論が行われた。

委員 A：

ビットコインの運用について、これまでダウンタイムゼロと言う説明がされてきたが、ダウンタイムの定義をしておいた方が良いのではないか。約定していくのが平均 10 分とはいえ、difficulty と計算量により、その時々の実際にコンファームされるまでの時間は異なる。SLA（Service Level Agreement）が定義されていないなかで、100%ダウンタイムがゼロであると、言及するのは難しいのではないか。

事務局：

今後検討していくこととする。

3.　委員プレゼンテーション

続いて、委員 B より資料 3 に関する説明が行われた。説明後に、委員 B より自己紹介が行われた。

委員 B：

弊社は、主には 2 つの事業を実施している。1 つは、暗号通貨のプラットフォームであり、ビットコインの取引所として機能している。為替エンジンを自社で作るための機能を保有する目的もある。もう 1 つは、企業用のネットワークで利用可能なブロックチェーンで、クラウド上でもオンプレミスでも勘定エンジンとして利用できるサービスを提供している。加えて、それらに付随するコンサルティング等も実施している。

続いて、委員 C より下記の自己紹介の後、資料 4 に関する説明が行われた。

委員 C：

当社は、デジタル資金・資産等をブロックチェーン上に記録し、移転するプラットフォームを提供している。当社には、本日委員として列席している委員 F が CTO として参画しているほか、流通に強い人材で構成されている。

続いて、委員 D より下記の自己紹介の後、資料 5 に関する説明が行われた。

委員 D：

元々は当社から、委員 J が出席する予定であったが、本日は欠席ということで、代理で参った。私自身は技術者ではないが、今回は簡単に事業をまとめたものを紹介させていただき、ディスカッションの中でも触れさせていただければと考えている。

4.　ディスカッション

上記に基づき、以下の議論が実施された。

委員 E：

弊社が実施しているのは、使用権を管理できるコンセントの提供である。権利をもらった人のみ、コンセントが使用可能となる。コンセントはわかりやすいものを作るという目的で作成されたプロトタイプであり、IoT のインフラをゆくゆくは手掛けて行きたいと思っている。

ブロックチェーンには、分野として 2 つ有望なものがあると考えている。

1 つは IoT のインフラである。少額のお金が動きまわることを考えている。そのインフラを作って行きたい。もうひとつはシェアリングエコノミーなどに相性が良いと考えている。

何かサービスを作らなければ、最初の入り口とならないので、そのようなことを実施している。

事務局：

既存のビジネスプロセスを、ブロックチェーンを用いることで効率化する以外に、IoT が挙げられるだろうが、現状まだインフラが整理されたとも言いづらく、有望というより新しいタイプの活用先だという認識である。

今、仮に、既存のビジネスプロセスに論点を絞るとすると、ブロックチェーンの技術的な課題、限界は解決されたと見るべきか、そうではないのか。コンセンサス層とデータ層は分けて考えるべきではないかという意見などもあり、また他にも、処理的な話となるかもしれないが、ダウンタイムをどのように定義するのかなど、ご意見があればお伺いしたい。

委員 C：

ファイナライズの問題は重要なものである。どの時点で確定し、動作するかの情報はとれない。トリガーは、ブロックチェーン上で何らかの定義しなければならない、あるいはこうなればこうせねばならないというルールを作る必要がある。

D 社のスーパーピアを作ったファイナライズの仕組みには一定の評価をしている。

委員 D：

IoT でも金融でもそうだが、ブロックチェーンは状態の遷移が確率的にしか生じない。一定以上時間を経れば、参加者間の合意をとる、という仕組みであればワークするのかもしれないが、当事者のコンセンサスにすぎず、技術的にひっくり返り得ることは変わらない。スーパーピアはあくまで、弊社が取った手段の一つであり、他にもアイデアはあり得る。データベースに入れる情報は何かを決める作業は、金融系等の社会が実時間で動いていく中で、合わせてブロックチェーンを動かしていくことを考える際に、必要になるのではないかという問題意識を持っている。

とはいえ、全ての社会におけるビジネス領域が全てデータを確定させていかなければならないものでもないとも考えている。それ以外で言えば、ブロックチェーンはユーティリティが高いとも考えている。

データを確定させる必要性のあるビジネスモデル、例えば金融や、リアルタイムで動かさなければならないものなどには必要になる。予約が可能なものはその限りではない。そういった考え方をしている。

委員 C：

自動販売機を 1 つ取っても、タイミングは難しい。

委員 D：

上空にドローンがコーヒーを抱えている中で、決済をする、というプロセスに関する思考実験をすると、決済の確定がなされないので、ドローンはいつまでたっても缶コーヒーをリリースできないと言う事も考えられる。

IoT の中でも、ADEPT などは予約を用いる仕組みなので、実現可能かもしれないが、今すぐ何かをしなければならないという動作の保証はできない

委員 E：

一旦関係性ができてしまえば、定期的に IoT と連動するということになると、micro payment channel のように瞬時に起動することはできる。ある分野に関して言えば、IoT でもリアルタイムにできるはずである。

委員 D：

やり方はあると思う。

委員 F：

弊社はブロックチェーン専門の会社であり、企業へのコンサルティング等を実施している。現在、某企業と連携して Ethereum を用いた研究開発を実施している。

ファイナリティの問題はパブリック・ブロックチェーンの問題であり、プライベートチェーンでは問題にならない話だと理解しているので、あまり重要視していない問題である。

委員 G：

パブリックチェーンは、Six confirmation までいけば、ファイナリティだと考えているか。それとも、Six confirmation までいっても、ファイナリティはできないという認識か。

委員 F：

後者である。Confirmation や Validation は、ファイナライズとは異なるという認識である。

委員 G：

弊社は情報発信を 2 年ほど行ってきた。最近になって、新たな企業を設立した。Proof of Concept を提供するところまで踏み込んでサービスを実施している。更に、プライベートチェーンも提供可能であるし、その他パブリックチェーンも提供している。Trustless な部分と TTP（Trusted Third Party）な部分をワンストップで提供する PoC 企業であるといえる。

本日の議論は、主に TTP の話をしているが、一方で Ethereum など Trustless なものに

よって、TTP がない、という環境の構築ができるようになった。それによる opportunity は今まで見たことがないと言えるものである。そちらの方が、魅力があるのではないかと思うが、プライベートチェーンやコンソーシアムチェーンなど、多様性を認めつつ多様的な情報により、個々のマーケットに対して、実用解をだすことができればよいと考えている。
特に、金融以外でやるのであれば、エネルギーや IoT に opportunity はある。そこを目指したい。

事務局：

Trusted か Trustless かに関して、極端に言えば Trustless ではないブロックチェーンはブロックチェーンではないという意見などもある中で、それぞれのブロックチェーンは互換性を想定せずに動くことになると思うが、もし繋ぐとすれば、Trustless な仕組みを接続するのか、別の進化をさせていずれ作り直しが要求されるものか。

委員 A

その辺りは問題の生じない部分であると考えている。Interoperability をどの次元で実験するかによるが、古い系のシステムで Proof of Burn である権利をきっちり消したことを確認し、その権利を別の系にもってくる技術もあるし、テクニカルにはプロトコルレベルの Interoperability を書くのは難しいが、複数の系でデータの一貫性が保たれているように感じられることを実験することはそこまで難しくないのではないか。

一方で、ファイナリティの例が出てきていたが、分散データベースの世界は昔から CAP 定理がある中で、ビットコインの秀逸なところは自分たちのつくったところの弱点を良く理解し、それに合わせたルールを作っているところである。例えば、ビットコインで当然フォークは生じるが、乗っている記録そのものが権利関係そのものなので、枝が湧かれて無効になった取引はあきらめてくださいという世界である。ナカモトサトシはスプリットが生じることを理解して設計したのではないかと感じられる。一方で、銀行で使い始めると、自社の情報システムは当然、法律上の権利関係が前提としてあった上で、リアルな世界のものとロジカルな世界のものを如何に近づけて行くかがシステム運用で最もお金のかかる部分である。

それぞれのブロックチェーン技術に関し、CAP のどこに強みがあるのか、正確に理解した上で、業務側の要件に落としていくというのを検討していかなければ、きちんとしたシステムは作れない。例えばファイナリティも非常に重要な問題であるし、それぞれの技術が、自分たちの何をきり落とすことで効率性を実現しているのかをご説明いただく必要があるのではないか。

委員 H：

当社では、コンテンツ流通にブロックチェーンを利用できないかと考えている。イメージでいうならば、Ascribe などのように、権利の移転などに使えないかということである。

ファイナリティの話題の中で、個人的に思っているのは、ビットコインのブロックチェーンなどで、権利の情報を載せて行くときに、乗せて行くものの価値が大きくなればなるほど、究極的にはビットコインの時価総額と同等になると、ビットコインであれば所有者が価値を落としたくないと考え、不正や攻撃へのモチベーションを下げる、一方で価値が大きくなれば、ひっくりかえすことを考える人がでてくるのではないかと考えている。Trustless なものの上に、実装ができるのか、と言う事に関しては考え中である。

委員 I：

弊社は、サービス事業者であり、昔は HP 作成のサポートをしていた。最近ではソーシャルメディアに力を入れており、昨年頃からシェアリングエコノミーに注力し始めた。そのバックグラウンド技術としてブロックチェーンが役に立つのではないかと考え、調査している。昨年の 12 月にはブロックチェーンサミットを開催し、海外からスピーカを招いて、お話していただく機会を設けた。

サービスを提供する側からすると、サービスのスタイルによって、どのチェーンを使うのかを考えることは非常に大きな問題であり、選択を誤るとサービスは上手く回らなくなるため、何か考えるときに最初に考えることである。

シェアリングエコノミーは、資産の中で空いているものを有効活用しようというものである。人と人が繋がって、例えば権利やモノをやりとりし、対価としてお金をもらうということが発生してくる。それに関して、お金の信用をブロックチェーン上で持たせることを目指す必要があるが、チェーンが多数あると、動く通貨も変わる。サービスの展開としてはやりづらい。サービスごとにチェーンが変わると、他のサービスとも連携しづらい。一括で繋げるようなバックグラウンドのチェーンがあるとよいのではないか、というアイデアもある。沢山選択肢が存在してしまうと言う事に対して、大きなデメリットを感じている。

事務局：

p21 の表を整理するにあたり、非常に苦労した。同じセグメントに分類しているものでも、使い勝手が違ったり、できることが異なったりするものが含まれているであろうし、どちらかといえば技術的な側面にある種着目せざるを得なかったものである。何かしらガイドライン的なものがあれば本当は良いのかもしれない。考えていきたい。

p22 にユースケースを記載しているが、その中で公共の分野がある。イギリス政府は業務にブロックチェーンを適用することは親和性が高いのではないかと言及しているが、このあたりがビッグプレイヤーとして存在する場合、公共分野が一歩先んじて関与していくことに関して、メリット、デメリットをどのように考えていらっしゃるか。

委員 A：

あまり役所としての立場で本日は参加していないため、純粋に個人として話すとするならば、政府の持っている台帳の多くは、基本的に紙の時代からのものなので、後から書き足していく形で作られていくものである。その意味では、ブロックチェーンに非常に親和性の高いものであり、ファイナライズに時間がかかっても問題ないユースケースが多いと思う。現実にパブリック・ブロックチェーンで実行していくのは難しいかもしれないが、統制をいれていくことで、割と安全なものを、それほど高くない技術で構築することは可能ではないか。

一方で、悩ましいことがある。純粋に運用コストを考えた場合、国であれば決めてしまえば、一箇所でやりますということもできる。KVS でなどで東西にデータセンターを持つケースと、ブロックチェーンを利用するケースの、どちらがコスト的に安いのか、というのはもう少し考える必要がある。おそらくデータの性質やユースケース上、ブロックチェーンの利用は親和性が高いと思う反面、技術をいれることによって本当に最終的にコストが低減するならどういう要素によるのかを考えて行く必要がある。

委員 C：

今のお話は、聞いていると、1 つの組織、例えば 1 つの自治体が取り組むことを想定されているイメージに感じたが、恐らくブロックチェーンはそのような利用にあまり向かないのではと考えている。むしろ、コンソーシアム的に、同じルールで運用する、例えば投票などであれば、糸口としてやりやすいと考えている。また、ちょうど良い塩梅に機能できるとかんがえているが、メンテナンスが必要だと考えると、1 つの市町村や自治体だけでなく、共通事務のような形でやらなければブロックチェーンを使う必要はないのではないかと考えている。

事務局：

公共で、もう一つの側面として、法定通貨とのペグが将来的に必要になるのではないかと言う話がある中で、Factom が実施しているような登記情報の管理などは、元々 Authorized された機関が発行するものである。単純な質問ではあるが、土地台帳や宝石の鑑定書などは、発行者がいるのであれば、その人たちがブロックチェーンを構築すればよいのではないか、もしくは発行者がいなければサービス自体がそもそも存在しないのではないかという議論がある。クリアな説明ができていない。発行団体が必要なサービスは、ブロックチェーンで理論的に置き換えられるものなのか、発行団体がある程度競争のような事をする必要があるのか、ご意見を伺いたい。

委員 A：

ブロックチェーンを使う理由は、複数団体が扱おうが、集中管理で登記する団体が扱おうが、そもそもの使う理由は2つある。1つは情報の透明性、あとは、所謂オペレーション上の不正を限りなく小さくしようというものである。ただ、人が扱う限りそのような問題はゼロにはならない。1団体が作ったサービスを自由化することに、あまり意味がないのではないかと考えている。

事務局：

法定通貨とのペグに関して考えると、究極的には中央銀行的な機関が必要になるのか。

委員A：

取引所が世界中に分散していて、どこかの取引所が1対1で保証された状態でエクイティがない限り成立しない。

委員D：

仮想通貨と法定通貨をペグさせるメリットは何か。究極的には、今ある技術の上に法定通貨をのせると、他のトークンとペグさせる理由はあるのか。

委員A：

サービス提供者の謳い文句としては、ボラティリティがなく、かつ金融機関に頼らず手数料が極めて低くて、プライバシーも保たれるとしている。

委員D：

それは、ブロックチェーンの上に法定通貨を直接のせることで、実現できないものか

委員G：

技術的には可能。Colored Coins、Sidechain、Rippleなど、既にテクニカルな解があるから技術的にはできる。IOUで行うパターンとアトミックに行うパターンの二つある。

委員D：

中央銀行がブロックチェーン技術を採用し、全銀ネットと日銀システムをつくり、その上で法定通貨を発行して転々流通します、となったときに、法定通貨以外のトークンが必要になるケースは何か。

中国で人民銀行が発行したり、イギリスでも似たケースが出てきたりしているようではあるが。

委員C：

企業通貨に置きかえると良いのではいか。企業通貨は地域通貨と同様、極小的なところでしか通用しないが、存在そのものは世界中に認識されている。その状態が非常に重要。今までのデータベースに記録されたものは、その中でしか見られないため、どの程度発行されているのかはわからないが、パブリックチェーン上でトークンが発行され、扱われれば、実際に発行されているのか、どの程度発行されているのか、がわかる。

例えば、当社の例で恐縮だが、プレミアム付きの法定通貨を地域通貨として発行する場合。例えば、静岡県におけるみかん付きの法定通貨と、沖縄県における紅芋たると付きの法定通貨と交換できるなどのユースケースも考えられる。

発行主体が限定的なエリアにあって、保証され、発行量そのものがブロックチェーン上で確認されるということはあり得る。

委員 A：

今の話は非常に示唆的。かつて地域振興券などがあり、プレミアム商品券もあったが、予算の範囲でシステムを作り、全て実施していたが、そういうところで、いつでもトークンが発行できる基盤があると、色のついた期限中に使用せねばならないお金を経済政策としてやっていくのはメリットがあるかもしれない。

結局のところ、単純にマネーサプライだけを増やしていくと資産バブルを発生させてしまうなどデメリットも多い。デメリットを減らすためには、地域を絞るなど規模を小さくして実施し、ピンポイントで施策を打っていくのは、Colored Coins の延長上でやりやすくなる可能性は十分にある。そういったインセンティブは、地方団体だけでなく、中央銀行など様々な団体でもあり得る。

また、日本においては歴史的に日銀の設立にも苦労したし、全銀協やほふり（証券保管振替機構）も時間とお金を使った組織だが、そういった仕組みを持っていない途上国も世の中には沢山あり、そのようなところで legal entity を、時間をかけて立ち上げ、集中管理していくよりは、小さな政治的・経済的コストで実現が容易になる可能性はあるし、日本国内でも legal entity が出来ていない分野で、スモールスタートしていくために活用するということはあり得るかもしれない。

委員 D：

私も反対しているわけではなく、実際に弊社でも地域通貨を取り扱っている。前払い式支払い手段、もしくは銀行の為替業務の範囲内で提供するという意味でいうと、委員 C がおっしゃったような形で実施している。委員 A がおっしゃったように、それ自体に意味もあると考えている。

最初に、不動産の登記をすると、登記識別情報通知を法務局から受け取り、それによって所有権の移転が完了するというのが今の法的な立ちつけであるが、例えば、不動産の売買を当事者間で行うとき、ブロックチェーン上でお金のやり取りと権利の移転が行われ、

それにより土地取引が完了したと法制上認められ、Confirmation が 6 回行われれば確定するというコンセンサスが取られたら、ブロックチェーン上の記録を登記識別情報通知として利用できるならそれは確かに意味があると思うし、シビックテックとして小さな政府を実現するというメリットを国民に対して提供できる。

ホンジュラスでも Factom が登記簿の仕組み構築に取り組んでいるが、自治体ごとに導入するのか、国としてばらまくのか。全体のコストと運用も含め、考えて行く必要がある。シビックテックはそこが最後の問題になると考えている。

事務局：

P35 の社会に与えるインパクトをこの先議論していきたい。既存のシステムが置きかえられる、新市場の発展/付加価値の創出の他に、社会的な構造が変わるのではと言う話もある。Legal entity がより置きかえられることを考えると、ある程度の水準を満たしたものが発展途上国でも享受できるなどの話があるが、どのようなインパクトが考えられ得るか、ご意見をいただきたい。

委員 B：

システム面の話というのが注目されがちだが、一番インパクトが大きいのは、既存のビジネスプラクティスが、ブロックチェーンの手順に置きかえられることで、ハンコのサインのような手順が大きく減ること、もうひとつはブロックチェーンの特性を利用し、不正や係争等のあらゆるリスクが軽減されることによる市場インパクトが大きいのではないか。あとは、なりすましの防止などが考えられる。

事務局：

過去に、証券会社ではペロという伝票にタイムスタンプを押していたが、注文を受けた時間の前後で押すなどの不正が横行していたこともあった。また、保険業界では、ホールインワン保険を、ホールインワンを打った後に売るなどの話もあった。

きちんとした監査などに技術を適用させるのは、皆様非常に関心が高く、人件費やコンプライアンスコストなどの低減に対する効果は大きいのではないか。どのように算出するかは知恵を絞らなければならないと考えているが、メリットは大きいと考えている。

委員 H：

ビットコインのサトシナカモト論文で主張されていることの 1 つに、元々の使われ方として、ブロックチェーンの入力に制約がかかる、ロールバックが出来ないと言うところで、ロールバックをしてほしいと言う問い合わせコストを減らせるのではないか、という話があるが、真を得ているように思う。

不自由なシステムであるが故に、そういうものだからというコンセンサスを全体で取れ

ていれば、問い合わせコストを減らせる。

委員 C：

ビットコインはトランザクションがないため、逆に戻すというトランザクションをつくるだけだが、Ethereum や mijin でやる場合、トランザクションの種別をいくつか定義し、ブロックチェーンに書き込んで行くので、ずっと残るように思われる。

委員 B：

高機能になればなるほどそうなるように思われる。

事務局：

ある書類の日付を遡って請求するということが原理的にできなくなった場合、ネガティブなインパクトも想定されるのか、ルールとして厳密にやりましょうとなるのか。

委員 C：

細かいことをいうと、ブロックチェーン上の時間トランザクション発行者により言及されている。沢山の情報から、大体の時間を決めているだけである。何時何分何秒だというのを電子署名法にもとづいてやると、TAA のような機関から受けた情報をトランザクションにこめておくらないとだめだよね、という仕組みがあるのではないか。

委員 A：

今のお話は、テクニカルリクワイアメント、ビジネスリクワイアメントが混ざっている。

ビジネスリクワイアメントとしてバックデートした契約書を結ばなければならないことは現実的にはある。システム上のタイムスタンプは後になるが、メタデータで契約年月日を Open assets protocol で書く場合は、メタデータの日付をバックデートした形でかくことができる。改竄ができないことが、イコールとしてビジネス上の制約が生まれると言う事ではないと思う。逆にいうと、今の RDB システムは自由に定義できてしまうので、ビジネスリクワイアメントを勘違いしてシステムにそのまま実装されるケースが多いように思われるが、御指摘があったように、ブロックチェーンの上に構築する、制約を設けることで、簡単に監査できる環境を整えるのは大きなメリットである。逆に言えば、PKI やヒステリシス署名などの技術は昔からあったが、現実には情報システムの開発の現場で、難しい、面倒臭い等の理由で使われてこなかった。そういったものを、強制技術的に入れて行くのは非常にメリットがあるのではないか。

事務局：

先ほど保留していたが、IoT についてどのようなインパクトがあるのか。切り口の設定に

悩むほど幅広い話ではある。ご意見があればお伺いしたい。

委員 E：

IoT のネットワークは世界中を覆っていく。色んな機械が自動でやりとりしていく。今はデータを集めて見せる程度のシステムだが、確実にデータを分析して、次の機械を起動させる、という世界になっていく。そういうときに、少額のマネーがそこを動いていくのは確実である。そこで利用されるのが、”Google Money”や”Facebook Money”でいいのかというと駄目だと思う。パブリックチェーンのマネーじゃないと無理なのではないか。長期的にみれば、それをやり取りするように持っていかなければ駄目なのではないか。

委員 A：

今のお話は非常に共感できる。私がなぜ Mac を使うかというと、世界で Mac だけが、世界中どこで壊れても、その日のうちに修理できるためである。アップルストアは、全世界の売上データが集約されており、世界のどこかでバッテリーが壊れた場合、別の国でのアップルストアで対応してもらうことができる。

他のベンダーがそのようなサービスを提供できていないのは、保証書のデータがバックエンドで共有されていないためである。モノを売る際に、それに付随するデータがある中、自分の持っている電化製品情報を小売店に知られることは問題ないと考えている人が多い。一方で、POS システムは流通チェーン店ごとに異なるし、日本のメーカーは Apple なみのサポートを提供できていない。

こういったところは、スマートコントラクトで解決できるのではと考えている。

事務局：

ブロックチェーンの課題の一つに、スケーラビリティがどこまでいけるのか、という話があったかと思うが、IoT ではどうなるのか。

委員 B：

その観点では、IoT が、プライベートチェーンとパブリックチェーンが最も混ざりあう分野であるといえる。共通のお金が必要であれば、パブリックチェーン、ビットコインが使われるべきだろうし、かといって内部データに関しては、共通のプロトコルができるかは分からないが、企業ごと、メーカーごと、ユーザごとに分かれるべきであるし、そうなるとプライベートチェーンになる

ただ変わらないのは、マイクロトランザクションと勘定概念が必要なことであり、そうなると各端末に勘定機能をもたせ、仕事に対する対価を、オーナー毎に計上するにはブロックチェーンが最適になる。

事務局：

今、ビットコインユーザはウォレットの中に大量データを保有しているが、IoT 分野で使われる場合、どうなるのか。

委員 B：

今研究しているところである、ブロックチェーンというと全端末が同じデータをもっていることが常識になっている中で、複数のデバイス、ネットワークで分散する技術も研究されている。

技術の進化により、制約は徐々に解決されるのではないか。

委員 G：

ただ、実際にフルノードを持っているのはマイナーである。今までの IoT はクライアント・サーバの世界で TTP が必要であったが、そうでなく、Trustless なものをインフラとして IoT をつくりたいというのが IBM の考えであり、それはおそらく大体共有され始めたと言えるのではないか。

委員 E：

ポインタだけ持って置き、その先を P2P のディスクで持って置けばよいので、ディスク容量自体は気にしないで良いと思う。ただ。本当に大量のトランザクションをこなせるのかというのが課題として残っているのではないか。

委員 G：

そこは、ビットコインブロックチェーンがいくつか解を出しており、ビットコインが最初に解決する問題ではないか。そうすると、その成果が IoT 向けのブロックチェーンにも適用され、スケールすると思われる。

委員 A：

あまり心配していない。というのも、ビットコインの場合、他にいくらでも悪用することができる上、攻撃を受けやすいアプリケーションでかつ時価総額が大きくなったことにより、ステークホルダー間のコンセンサスがとりにくくなり、スケーラビリティの問題が生じている。恐らく、スマートコントラクトのどれくらいの経済的価値をやり取りするかという話になる。例えば保証書の情報でも、物理的な ID と紐づけている限り、悪用のしようはあまりない。スケーラビリティの問題は、むしろ要件としての信頼性や、攻撃されるリスクと見合いで考えて行くこと。IoT の多くの用途では、何となく十分にスケーラビリティが高いパラメータでブロックチェーンが使われることは可能であるように思う。

委員 G：

IoT が、ビットコインのブロックチェーンを利用するのか、新規のブロックチェーンを立ち上げるのか。世界でどう議論されているのだろうか。

事務局：

MIT メディア・ラボの伊藤穰一先生は、ブロックチェーンのフォークをなるべく抑える、もしくは用途ごとに規格を定める、という議論をされている。そういった話は議論すべきだという意見の方が多いのか、否か。

委員 G：

開発陣自体を decentralize したいのか、そうでないかの 2 派存在する。開発陣自体を decentralize したいのが、ハードフォークを許容している人たちである。ノードは分散している中で、開発主体自体を分散するのかは議論中である。

事務局：

開発の体制、作り方をどうするかという議論になる、IoT ほどの巨大なマーケット、インパクトがあれば議論を進めておくべきなのか。

委員 G：

IoT はビジネス主体が沢山いるので、むしろマーケットニーズの方が重要である。トップダウンでやろうとしても結局ペイしないと言う事もあり得る。ただ、恐らく、ビットコインと違って IoT は開発陣を centralize しやすいため、むしろビジネス主体があつまり、マーケットリクワイアメントに対して、十分に安い解を提供していけばよいのではないか。

委員 C：

IoT のブロックチェーンは好きな人が好きなように作ればよい。その中で、処理をどうするのか、もそれぞれが自由に作ればよい。あとは、パブリックチェーンに対してアンカーをする。

委員 E：

Sidechain であればよいが、実際に実用に近いのは、クライアント・サーバやプライベートチェーンである。そのあたりのルールはどうなるのかが気になっている。例えばアンカーすれば信用すればよいのかというのは理論も法的な根拠もない。

委員 C：

法的な部分は、タイムスタンプの例にせよ、色々な担保の方法があると思う。

たとえば、ビットコインと Ethereum と NEM の 3 方向をペグする、など。

委員 E：

パブリックチェーンではないものをどのように考えるのかがはっきりしない。

委員 A：

2 つの議論をわける必要があって、ビットコインとブロックチェーンのガバナンスの問題はかなり異なる。

ビットコインがインターネットとよく似ているのは、非常に短期間で時価総額があがり、ステークホルダーが増え、インターネット以上に多くのお金が流れ込んでいるところである。その中で、どのようにガバナンスを確率し、技術仕様を決めて行くのかは、かなり政治的なイシューであり。日本国内だけでは解決されない問題である。

ブロックチェーンに関しては、CAP のどこをどうあきらめたのかという事に関して、表示も含めて十分にできておらず、技術が安全化どうかの数学的な評価もまだ定まっていない。かつて、経済産業省が暗号分野で CRYPTREC を立ち上げ、国内でもきちんと技術評価をしたように、日本には暗号の研究者もデータベースの研究者も沢山いる中で、ブロックチェーン技術が評価の俎上に上がっていない。

ヒステリシス署名など、本来日本が強い技術力を持っているところなのに、自前の見識がない部分が若干弱い部分である。技術の確からしさに関して、コンセンサスを作っていく分野において日本は非常に大きな国際貢献ができると思うし、政府としての役割もあると思われる。

5. 次回について

事務局：

p41 以降に、ビットコインにおける課題を整理している。此方に関してもご意見があるかとは思うが、こうした課題に関して、課題であるか否かも含め、次回の検討会ではここから議論を開始する。お時間無い中恐縮ではあるが、課題に関して議論の頭出しをしていただければ幸いである。

第 2 回は、3 月 7 日、17:00-19:00 に開催する。本日の議論をまとめ、振り返りを行った上で、課題と限界、インパクトの評価に関してもフレームをお見せすることになるかと思う。また、政府としてどういう取り組みが求められるのかというところにもご意見を頂きたい。

委員 F：

最後に、本検討会の収支における背景に関して、「改ざんが極めて困難である」というの

は正しいのか、検討する必要がある。パブリックチェーンでも変えることは可能である。「実質的なゼロ・ダウンタイム」も先ほどの議論であったような考え方がある。「安価」に関しても、何に対して安価なのか、皆意見が異なる。システム自体が安価になるのか、人権費の話なのか。細かく決めなければ、どの程度正しいのかの議論ができないのではないか。

以上

参考1.5　第 2 回検討会　議事録

ブロックチェーンに関する検討会
第 2 回議事録

日　　時：　　平成 28 年 3 月 7 日（月）17:00 – 19:00
場　　所：　　経済産業省本館 9 階西 8 共用会議室

出席委員：

NTT サービスエボリューション研究所
株式会社 Orb
株式会社ガイアックス
カレンシーポート株式会社
国立情報学研究所
コンセンサス・ベイス合同会社
テックビューロ株式会社
株式会社 Nayuta
一般社団法人　日本デジタルマネー協会
森・濱田松本法律事務所
ヤフー株式会社　/　内閣官房

（以上、50 音順）

事務局　：

経済産業省
株式会社野村総合研究所

資　　料：

1. 議事次第・委員名簿
2. 事務局説明資料
3. 委員 J　ご提出資料
4. 委員 F　ご提出資料
5. 委員 K　ご提出資料

議　　題：

1. 前回の振り返り（事務局説明）
2. 委員プレゼンテーション
・委員 J プレゼンテーション
・委員 F プレゼンテーション
・委員 K プレゼンテーション
3. ユースケースの紹介（事務局説明）と議論
4. 課題の整理と政策対応のまとめ
5. 検討会終了後の進め方
6. 閉会挨拶

1. 開会挨拶・趣旨説明

始めに、事務局より、資料 2「ブロックチェーンに関する検討会　第 2 回討議用資料」に基づき、第 1 階検討会の振り返りが行われた。

2. 委員プレゼンテーション

続いて、委員 J より資料 3 に関する説明が行われた。
続いて、委員 F より資料 4 に関する説明が行われた。
続いて、委員 K より資料 5 に関する説明が行われた。

以上の委員プレゼンテーションをもとに、以下の議論が行われた。

委員 J：

各委員のプレゼンテーションを興味深く拝聴した。委員 F のプレゼンテーションはビジネス観点のものということで共感をした。ビジネスの応用に関して言うと、何をやりたいかということに対して技術を適切に選んでいくということを考えなければならない。また、委員 K のプレゼンテーションは、スマートコントラクトについて改めてしっかり考えるきっかけとなった。これは、ある意味法律家から見た要求仕様になっており、技術者としては、こういうものを作ればよいと考える助けになる。私は大学の政策メディア研究科出身で、ここでいうメディアとは技術を意味するが、ガバナンスとは切り離せないものである。ブロックチェーンのガバナンスを考えて行かなければならないと考えると同時に、ブロックチェーンの出現により喚起されるものが非常に多くあったと思うが、社会の側からどのような要請があるかによって、現状のブロックチェーンの在り方に関わらず、どのような技術をうみだしていくか、また、生み出された技術もまたガバナンスと切り離せないのだということを考えなければならない。

委員 K：

ビットコインを前提に委員 J のプレゼンでは議論されていた、という話だったと思う。何をもってブロックチェーンとするかにもよるが、開発方法は無限にある中で、テクニカルには解決出来ていて、ブロックチェーンで実現したいということは、仕組みの作り方次第でできると認識してよいのか。感覚的な話である。

委員 J :

ブロックチェーンが目指しているのは、参加者の総数が分からない状況下かつ障害をもっている参加者の割合もわからない中でコンセンサスを実現したいと言う事だろうと思うが、これは非同期システムでは不可能である。完全なる非同期システムは、すなわち時計が同期していないシステムでは不可能だと証明されている。だが、その中で、如何に条件を狭めていき、実現できる環境を構築すること、それが技術的に可能なのかという問題だと思うが、恐らく可能だと考えている。それにおいては、全順序を辞めるということが重要である。やめないことには、グローバルに同一の運用しか許されず、日本の中で運用するときに日本の法律にそぐわない可能性が生まれる、ということである。ネットワーク技術が実社会に適応するためには分権が必要だが、分権していくという構造を持たせられれば、大きな問題であるネットワーク分断に対する耐性も解決できるのではないか。また、チェーンにより相対時刻を定義していくことに関して、元々管理者がいる中でハッシュチェーンとして実現すると、全体が管理されない中で、全員で正当性を保つということが実現できない。かといって、管理者がいない状況では改竄を防ぐのは不可能であり、常にリスクがあるということがビットコインの場合ですら顕在化してきていると認識している。ただ、改竄ができない状態の度合いを上げて行くことはできると思う。改善する余地はかなりあると言う認識。ただ、社会に役立つかは別の問題で、社会の側から要求があることは大事で、そうすれば技術は向上していく。

委員 L :

委員 J のお話の中に、分権できないという話があったと思う。分権というのは、用途を限ったり、色んな要件（制約）に対して様々な実装がでてくるという話があると思うが、分権の中に、運用している、適用している分野ごとにするというのも分権の中の一つか。

委員 J :

弊社の仕組みはそういう考えで作っているが、あまりよろしくないと思う。一つの応用の中で、トータルオーダー（全順序）を実現してしまうと、運用の中で分断があり得る。ただ、根本的な解決でないにせよ、一つのハックのような、場当たり的な解決策としては有効ではないか。

ここで、委員 J が退出された。

3.　　ユースケースの紹介（事務局説明）と議論

続いて、事務局より、資料 2「ブロックチェーンに関する検討会　第 2 回討議用資料」に基づき、ユースケースの紹介（事務局説明）が行われた。それに基づき、以下の議論が行われた。

委員 E：

ポイントサービスとは、家電販売店などのポイントサービスと認識した。1 対 1 が確定している場面ではリアルタイムで可能だが、システムがうまくつくられるのであれば、タイムスタンプをあまり気にする必要はないと考えているがいかがか。

委員 C：

タイムスタンプはついていればよいというのが、従来のポイントカードと同じくらいの認識ではないか。

委員 E：

私のイメージでは、転々流通するようなところはリアルタイムが動いていないが、先に前もってやりとりする相手が決まっている場合は、前処理をしておけばリアルタイムに取引できると言えるのではないか。それを、できないと言ってしまうと適用範囲がせばまってしまう。

委員 C：

取引の契約をするときに、時間は非常に問題になるが、おまけポイントのようなものは、十分に機能するだろうと言う認識で扱っていけばよいのではないか。

事務局：

委員 F のプレゼンにもあったが、意外と手数料が高いケースもあり得る。

委員 F：

1 ポイント送るのに 5 円かかるのであれば意味がない。パブリック・ブロックチェーンでは殆ど使えないのではないかと考えている。ビットコインのようなものでポイントシステムを作るのはほぼほぼ不可能ではないか。

委員 G：

Gems などは実現していると言って良いのではないか。

サーバサイドで処理しているが、どこかでブロックチェーンと同期している。

委員 E :

Colored Coins でデポジットして、どんなデータかを検討していけば、マイクロペイメントできるのではないか。

委員 C :

Lightning Network や、Sidechain など、色々と方法はあるだろう。

委員 F :

前のところはオフチェーンでやって、結果をブロックチェーンに乗せるなどのパターンはあるだろう。

委員 A :

テクニカルには色んな方法があるが、ビットコインに触発されて、あたかも安くできる、違う事ができるなどの先入観が強いように感じる。いわゆるポイントプログラムを運用する際の、データベースのコストはごくごくわずかである。結局のところ、カードを何千枚配ったり、POS システムを改修したり、契約内容の変更をパンフレットにして告知するなどのコストが殆どで、バックエンドのデータベースはほぼほぼボトルネックになっていない。議論を絞っていかなければ地に足のついた議論になりにくい。ブロックチェーンの特徴によってコストインパクトを与える分野がどこかというのが、議論の判断軸になるかもしれない。

委員 G :

ポイントは前払い式支払い手段のみか。

委員 C :

今回の場合は違うのではないか。

委員 G :

転々流通を許せばブロックチェーンを使うメリットは大きい。

前払い式支払い手段に限るのであれば、現在のシステムで十分である。技術的には既に解が沢山ある。

委員 C :

弊社の事業の一部はポイント関連だが、ビットコインだと高いという話があったが、ポイントをおまけとして、高くても良いポイントを付けることができると思う。プレミアム

を付けたポイントだったら、十分支払われる、など。そういった類のポイントであれば、転々流通も含めて、トレーディングポイントや、スタンプとなっていくと、別のビジネスモデルがあり得るのではないか。

事務局：

既存のポイントのように、モノを代替する用途ではあまりないか。

委員 B：

一定規模を超えるのであれば損益分岐点を超える。

事務局：

別の要素を持たせる、転々流通であったりトレードであったり、そのような付加を付けるのであれば、ブロックチェーンの特性が活かせそうだということか。

委員 C：

パブリック・ブロックチェーンを前提とするならそうである。ポイントなどは存在を認証される必要があり、それなら皆で確認する必要があるため、パブリック・ブロックチェーンである必要があるが、パブリック・ブロックチェーンでやるとなると、先ほど言ったように、高価な価値を生むような、新しいサービスとか転々流通をするようなサービスでないといけない。ただ、それとは別の方法があるのではないかということである。パブリック・ブロックチェーンだけを使わなければならないのでなく、パブリック・ブロックチェーンとプライベート・ブロックチェーンをハイブリッドで使うということである。Sidechain の実装でもあるかもしれないが、Sidechain に限らない話で、その実装のようにすることもある。そこでは、ペグをしたりするなど技術があって、ペグの技術をちゃんと使う事で、どっちにつけたという話があり、高速で取り扱うものは、プライベート・ブロックチェーンで取り扱うなどという話になる。

事務局：

マイクロペイメントの話と手数料の話に矛盾を感じる。マイクロペイメントの場合、現実問題として、できているのかできないのか。

委員 E：

出来ている。ただ、前もってデポジットしないといけない。Lightning Network みたいに、誰から誰に対してもすぐに送れるというのはコンセプトレベルである。

事務局：

転々流通みたいなところを考えると、地域通貨はそこに非常にマッチしたものだと考えてよろしいか。

委員 G：
マッチしていると思う。J 社のやりたい分野はそこではないか。

委員 K：
彼らはそこを目指していると思われる。

事務局：
ポイントサービスの類似例として挙げているが、そちらのほうがコア、メインストリームなのか。

委員 K：
ポイントというと漠然とするが、目的がいわゆるお金の代わりなのか無償ポイントなのか。無償ポイントはエンゲージメントの領域で、機能が異なる。モノが買えるというのは似ているが、性質は違う。
エンゲージメントは、転々流通しながら何かを作るというサービスで、ビットコインが当時やっていたことと同じようなことを実装できるという発想もあるだろう。お金の話は転々流通という意味で同じなので、同じ仕組みでできるのではというところがあるが、意図が違うので同じものとして議論をすると混乱をするのではないか。

事務局：
土地の登記に関して、法務省等の仕組みを介さずにできるのではないか。Factom がやっていることをベースとしている。将来的な話として、ブロックチェーンがこういうものを代替していけるのかに関して御意見をいただきたい。そもそも前提条件として色々無いと無理だということだとはおもう。その辺りのご指摘もいただきたい。

委員 F：
良くある問題はプライバシーである。名前や住所を誰にでも見える状態にしてよいのかなどが問題となっている。

委員 K：
ただ、登記簿はそもそもそういうものである。

委員 L：

履歴情報が重要なものは登記簿のように扱えるなど、いくつか分類できるのではないか。

委員 A：

非常に向いていると思うのが、現状プライバシーが必要とされていない領域ではないか。一方で、登記の仕組みは、明治時代に作られており、当時プライバシーの概念はなかった。おそらく登記簿を登記簿として機能させるために、本名が公開されている必要があるのかというのは、元々のビットコイン論文にあったプライバシーモデルを使って議論できると思う。つまり、権利の移転を適切に行うことと、本人を結びつけることは分けてできるはずだし、マイナンバができたことによって、実現可能性が高まったと思われる。ブロックチェーンに向いた領域であり、将来どうかという議論があっても良いのではないか。

事務局：

資料に記載している投票は、国政選挙のようなものをイメージしているが、権利の譲渡はできない、投票先では自動的に正しい投票が集計されて結果は改竄不可能である、権利と本人を結びつけないモデルとして、これはメイクセンスと言えるか。

委員 L：

本人証明次第だと思っている。投票の集計部分なり、投票の一票の確認は、別の手段で実現可能だと思っている。履歴を蓄積し、取り扱う登記簿のユースケースとは、質的に異なるケースではないか。

委員 A：

現状の選挙においては、本人確認をしていない。葉書がなくてもその場で投票できるし、身分証を見せる必要もない。

事務局：

コストの話をすると、選挙一回で 400 億とか 600 億と言われるが、削減できること自体のメリットはあるか。

委員 L：

あると感じる。

委員 A：

一方でブロックチェーンは巨大なアノニマスデータであり、その人の実態とアドレスが結びついていないということでブロックチェーンのプライバシーは担保されている。分かった瞬間に過去の投票行動がすべてばれるというのはどきどきする。

委員 C：

それは、鍵をその都度作れば解決されるのではないか。

委員 A：

その通り。ただ、その場合は正しい投票権と結びつけられる形でだけ、鍵が作られなければならない。

委員 C：

それは出来ると思う。

委員 M：

北九州のラーメン選手権で、投票をしているが、ただ単に投票するなら普通にやった方が簡単である。重みづけをするとか、電子投票じゃないとはかれないようなものを図るとか、途中経過をあえて見せるとか、そういうところに面白みを感じる。通常の投票だとあまり削減ということに繋がらないのではないか。

我々は、Open Assets Protocol で、一回一回まじめに、パブリック・ブロックチェーンに乗せているので、非常に高いコストがかかっている。予算で払えないので、ポケットマネーである。

委員 K：

私たちは、土地の登記の話があると、実態の権利関係と登記はずれているのがあたりまえだという感覚がある。登記と言うのは所詮対抗要件である。何を実現したいのかと感じるところがある。

例えば、株式に関して、昔は株券が存在した。名簿に書いてあるから株主だというわけではなかった。ところが、株券をやめましょうということで、やめられるようになった。そのときに誰が株主ですか、を決めるために、名簿にかいてあるのが株主ですという社会に移った。

債権の世界でも債権譲渡というものがあって、債権を譲渡したときに譲渡が対応力をもちますかというのは、確定日付を打って通知するか、債務者が承諾をするという話になってきた。さらに電子記録債権みたいな話になると、今度は記録・帳簿が正しいという話になった。

土地は相変わらず登記簿が対抗要件ですと言う話になっているが、土地を誰が持っています、権利状態どうなっていますという話は、実態の話でなくここにかいてあるのがそうです、という領域に移ることができれば、土地とブロックチェーンみたいな話が現実味を帯びてくるかもしれない。土地とその債権でなにがちがうかというと、債権はどうにでも

なるが、今回民放の債権で再建法というものがあるが、土地というのは物件法とかプロパティの重い議論が存在していて、物件のほうをかえるのは大変だよね、というのが法律家の間では言われている。物件法を変えるというのが民放でててくるが、議論をしていくためのハードルとしては高くて、株や債権なら比較的社会の制度との整合性は、色々できるが、物件の話だと、少なくとも日本で議論するにあたっては、物件法の問題などを克服せねば先にすすまないと思われる。

どうしても、法制度との統制を意識しなければ、ユースケースの実現性がピンときにくい領域なのではないか。

事務局：

次に、サプライチェーンに関して。前回、C 社より船荷に関する取り組みを発表していただいた。情報を改竄できない、マルチシグのような形で保証する、ということでサプライチェーンに適用できるのではないかと考えた。

どちらかというと商流にフォーカスして資料を作成しているが、他にこのようなインパクトがある、と言うご意見があればいただきたい。

委員 H：

昨今であれば、3D プリンタで簡単にモノの部品をつくれるが、それがちゃんと設計されたどおりにつくられているか。要は真贋証明みたいな形で、ハッシュ値を利用するというのが、イメージとして有っても面白いと感じている。正しく作られたもののハッシュ値であれば、保証がきくとか、独自の改造を施すと責任を負えないなど。

委員 C：

船荷の話があったが、それに加えて、サイレントチェンジの話をした。これは、今の話に若干似ている。実は、書類そのものは正しいが、モノの部品の強度が規定に向いていない別のモノである、もしくはその逆のパターンが考えられる。そこで、部品表に関する話を先日別のセミナーでしたが、非常に樹上構造になったデータベースが出来上がる、従来の RDB ではどこがどうなったのかを管理するのが非常に難しい。ブロックチェーンでやると、やりやすいブロックチェーンとやりづらいブロックチェーンがあるが、そのとき例にあげたのが、NEM、mijin のトークンである。これは、それらのトークンがモザイクタイプの構造をもっていて、樹上構造をとっているので、部品管理に向いているためである。

この分野はメーカーにとって非常に大きいインパクトだと思っている。金融よりも大きいインパクトがあるのではないか。

委員 A：

同じような話で、引越しの話がある。最近新居を購入したが、KING ファイルに取扱説

明書が大量にあり、保証は全てバラバラであった。蛇口のユーザ登録、食洗機の登録、など 10 数枚のはがきを送る必要がある。これを、部品のサプライチェーンとして、1 箇所で登録してほしいと感じた。現状バラバラに管理されていて、リンクされていなくて、商品の末端に負担がいっているもの、実は非常にあるのではないか。これまで管理されていなかったものを管理していくということで、彼らにしてみれば一度売ればそこで利益を得る機会が終わるので、ずっと運営していくのはお金的にも難しい分野だと思うが、逆に、プライバシーをうまくクリアしながら、リンク構造をクリアしていければ、簡単で便利で安心して使えて、リコールがあったときにすぐ連絡できる仕組みが作れないかと考えている。

事務局：

シェアリングエコノミーについて、実態として法規制の問題など別のレイヤで議論されてしかるべきだが、遊休設備を上手く管理するためのインフラとして、何かしら社会的な要請はあるだろうと考えている。そちらの観点から産業的なインパクトに関してご意見頂きたい。

委員 L：

書いていただいている例はあると思うが、シェアリングエコノミーの文脈で話すときに、ブロックチェーンからみて何が重要かというと、C2C で C が契約主体になることがかなり重要。個人間の役務の提供、物品の貸し借りが行われる。これまでは事業者、例えばオークション事業者のもとに、公式ユーザがいたり、エスクローしていたりしたものが、C 間でやっていかなければならなくなる、そこをスマートコントラクトしていく、という文脈の方がより重要ではないか。

遊休資産の貸し借りをブロックチェーンで管理するのも面白い話題だとおもうが、空いている時間をチケットにして、取引すればいいのかというとしっくりこない。役務なり貸し借りなどの契約をコード化するという考え方で捉えて行く方がしっくりくるのではないか。

事務局：

コード化すれば課題が出てくるだろうと言う話があったが、シェアリングエコノミーの領域とはトレードオフがあると言えるのか。

委員 K：

消費者契約は、シェアリングエコノミーとは異なる、事業者 vs 消費者という枠組みの話である。シェアリングエコノミーの議論に置いておかしい点は、全てが事業者と消費者という考えで捉えられている点である。シェアリングエコノミーは業の話がはまらない世界

である。今の消費者保護とは異なるお話であるということである。その意味では、先ほどから消費者保護の観点で、と言っているのは、シェアリングエコノミーの話は当てはまらないのではないか。

事務局：

先ほど、登記のところで、本人確認のためのインフラをどうするかという話があった。ブロックチェーンで解消可能なものがあるのか、このあたりの意見をいただきたい。

委員 E：

その辺のサービスをやって、ID をとるのがお金になると思っている。

要するに、ブロックチェーンは史上初、インターネット上で、これが本物ですよ、という価値のやり取りが初めてできたものである。ただ、それを現実と繋げるというところで断層がある。結局そこの ID を獲得した人がビジネスで有利になる。Facebook が取りに行く可能性はある。

国の議論なので発言するが、たいしたことのないサービスで良いので、頻繁/大量に使われるもので、ID や reputation の情報をとっていくのがよいのではないか。ID は非常に大事である。

事務局：

フォーマルなハッシュ値を本人の ID の代わりにつかい、真正性が保たれるなら良いのではないか。

委員 A：

日本は割と伝統的には、同一性を問うてなかった時代が長い。例えば、親父が死んで、銀行にいって、名義を変えようとしてもそのまま使ったりする世界だった。事業者からみると、結局のところ相手がいれかわってなければなんでもよい。ただ、それではテロ対策にならないということで本人確認法ができて変化し、今回ビットコインでもそのような議論がされている。

わけて議論することとして、ブロックチェーンのレイヤでカバーされるものとは、identify されたものを、改竄されないように記録していくおとやっていく技術。それと実態としての entity がどのように結びついているのかはコントロールしていない。それを、海外では、取引所に本人確認義務を課すことで、間接的に枠をあてはめ、できるだけ見つけたいロードに対して、短いステップでたどり着けるような世界にしようとしている。そこは、混同されて議論されがち。どのようにビットと atom をむすびつけるかという話と、どのようにビットの世界で一貫性を担保していくかは技術的には異なるものが求められている。ブロックチェーンは後者に対して非常に強力な技術であろうと思う。

逆にいえば、そこに本人確認の世界を持ちこみたいのであれば、マイナンバカードを利用して署名したものでブロックチェーンを利用するなどすればよいのではないか。

4.　　課題の整理と政策対応のまとめ

続いて、事務局より、資料 2「ブロックチェーンに関する検討会　第 2 回討議用資料」に基づき、課題の整理と政策対応のまとめに関する説明が行われた。それに基づき、以下の議論が行われた。

委員 F：

もうひとつ、日本円で決済するとなったときに、それをブロックチェーンにどうのせるのかという話はよく出てくる。株券をブロックチェーンで買いたいが、買う際の日本円をブロックチェーンにどうのせますか、と言う話は良くでてくる。それができれば色んな決済などが、ブロックチェーン上でまわるようになるのではないか。

委員 C：

それは、ISO ができるのではないか、ということも合わせての話か。

委員 A：

Open Assets Protocol でできないのか。

委員 C：

できるが、例えば資金決済法にもとづくようなオペレーションにするのか、中央銀行が発行するのか、銀行が発行にするのか、にもよるが、フォーマットそのものは紳士協定である。

Coin Prism などに発行できるが、Coin Prism というデファクトといったように、ある団体のつくったフォーマットに準拠しているだけで、標準化されたものではない。そこを標準化したほうがビジネスには使いやすいのではないかと考えている。

委員 G：

今デジタルアセットで本当に使えるのはビットコインだけ。円だったり、ユーロだったり金だったりが、本当に信用できるデジタルアセットとして使えると、スマートコントラクトでできることは非常に増える。

委員 C：

トークンのフォーマット化は非常に重要だと思う。通貨にもいくつか種類はあると思う

が、チケットなのか株券なのか証券なのか色々あるかとは思うが、分類した上で、トークンの発行コードを、世界中の ISO などの機関で標準化した上で、発行できるのであれば、あとは発行主体だけの問題となる。

委員 E：

弊社ではコンセントを 2 種類作っている。1 つは弊社サービスに依存しているもの。1 つは P2P で駆動するもの。ブロックチェーンを使うのだから、P2P でやりたいのだともおもうが、P2P バージョンは課金型にするとビットコイン払いにしなければならなくなる。そうすると、マーケットがあるの、と言う話になるその壁が乗り越えられない。円が仮想通貨になって、ブロックチェーン上にのっていたら、本当の P2P のマシンで、マーケットに入るモノが作れる。

委員 C：

それは R3 でやっていることと関係があるのか

委員 G：

R3 は、おそらく、円、ドル、ユーロなどのデジタルアセット化は視野に入っていると思う。MUFJ コインなのか、Goldman がやるのか、Morgan がやるのかはわからないが、いずれにせよ法定通貨のデジタルアセット化はいつか誰かがやるだろう。中央銀行がやるのが一番良いが。

委員 K：

ビットコインはたかだか時価総額が 7000 億のシステムだが、法定通貨のせると、何千兆のもの時価総額になる。ハックされると大変なことになる。

委員 A：

Open Assets Protocol の、裏付け資産の記述だけであれば、準備金の分しか被害をうけないと思う。Open Assets Protocol は、裏付け資産とブロックチェーンを結びつけるためのプロトコルでしかない。

委員 C：

信託保全された金額と、信託されているステートメントを、例えば Factom の要領で証明すると、発行された金額と証明された金額を比べ、証明された金額の方が大きければ保全金の方が大きいよ、というものである。

委員 K：

ハックされて何千倍に増えると、皆が按分するという仕組みか。

委員 C :

そもそもハックできるのかという話はある。

委員 G :

リザーブ分しか保証されない。

委員 K :

ハックされて増えても、皆で分散処理するということで理解した。

委員 F :

Open Assets Protocol で、100 円使おうとしたら、ビットコインを購入して、一緒に送らなければならない。

委員 B :

同じ問題に戻る。

委員 A :

信託銀行におさめている準備金と、Open Assets Protocol 上の何かのディスクリプションが 1 対 1 対応するような、制度上の裏付けと、技術的な保護を決めるだけでできることなので、決めの問題である。

委員 K :

銀行系のモデルならわかりやすい。銀行が倒れるだけなのであり得る。

委員 M :

ISO で、仮想通貨に通貨記号を付けるかどうかという議論がなされている。大体結論は決まったところであり、4 月位に公表されるはずである。国番号と通貨番号は連番であり、国連と ISO が、番号が重複しないように決定している。商品貨幣の中で、金とか銀とかプラチナとか、あの辺の並びに入れる需要があるかという話である。これに入れば、銀行のシステムにはデフォルトで通貨記号が準備される。定義することは、簡単なことだけど大きい話である。

委員 B :

今、バーツが被害を被っている。

事務局：

少し頭を切り替えて、制度面、産業政策面に話を移すこととする。資料に記載しているのは暗号等の話で、前回の議論に依拠するものだが、今回の議論で、基礎研究とユースケースを同時に進める体制の構築や、スタートアップ支援等の話が出てきたかと思う。試していかないとわからないものがあれば、何かしら手を打たなければならない。

委員 K の話にもあったが、法規制に関して、アーキテクチャで解決可能なものが非常に重視されている分野であると思う。そこに、市場的な考えを組み込むという考えもあると思っている。これに関して、所謂検討会で呼ぶべき人間を広げて行く、違う観点の人間を組み入れるという観点もあるかと思う。

また、本人確認と権利の移転に関してだが、印鑑証明に根拠法がないのではという議論もあったかと思う。本人確認のきちんとしたインフラを構築することが、ブロックチェーンの普及に繋がるのだろうと言う話も報告書に記載する予定である。

株式債券、実物と連動させるのでなく、どこに権利があるのかを管理する仕組みがあるのであれば、適用領域を広げることで、ブロックチェーンの適用範囲も広げて行くであろうため、検討する必要があるだろう。

また、シェアリングエコノミーの項に関して、消費者保護の文脈をブロックチェーンに入れ込むべきかというと、そうではないのでは、という考えもある。

委員 A：

委員 K のスマートコントラクトの話に繋がると思うが、民事訴訟法 228 条との関係をどうしていくのか。現状、押印した文書に認められている 2 段の推定に相当するものの電子データは、所謂電子署名法で認められた、認定された認証局より発行された電子証明書だけである。

これは、いってみれば公証されているものなので、効力としては実印のようなものである。ただ、実際の社会的な取引においては、銀行登録印にしても、文房具屋の三文判にしても、非常に多くの経済活動を支えている。例えば、ビットコインで使われているようなキーペアにしても、文房具屋の三文判よりははるかに強力なトークンだと思う。

もしスマートコントラクトの話を真面目にするのであれば、ブロックチェーン上に記録されたものが、どういう要件を満たしていると、民放でどの程度の証拠能力が認められるのか。最終的には裁判官の自由心証に委ねられるべきものであるのか、目安として何かでてくると話が変わってくるのではないかと考えている。

委員 C：

検討したことがある。電子署名法に基づく署名された文章は証拠能力がある、と推定される。であれば、そのハッシュを間接的に証明することができるのではないかと考えてい

た。間接的にその状態を作ることである。

委員 C による資料「ブロックチェーン技術はエンタープライズ用途に耐えうるか」が示された。

委員 C :

法的証拠能力に関する課題の部分に記している。グラフでいうと、4 行目の部分である。

委員 K :

書類におけるハンコのはなしは、どこまでいっても推定の問題。推定がきかなければ証明すればよいというだけの話。昔、文書は手書きでうつしたりしていたので偽造だという話があったと聞いているが、今 PDF になっているので、偽造といっても勝ち目がない。真正の部分は争われなくなっている。保険のような大きな買い物でも、電子署名法では全くないようなものでも、一応契約になっている。何故それができるかというと、全体のシステムとしていえば、それなりに証明できるという話がある。その仕組みの中でやっているからこれで良い、ということにすれば、裁判での証明が出来てしまうという世界がある。とはいえ、民事訴訟法に特権として与えられているものであって、電子的なものに関して、法制度としてもっと考えなければいけないのではないのかというのはおっしゃる通り。それの象徴的なものになる可能性はある。そうでないものが、劣っているということになると、実際はこちらのほうが、証明度が三文判より高いという事にもなる。

委員 A :

本当に法律がわかっているとこういう議論ができるが、民間企業の大半は誰もやっていないとか、契約の相手方がハンコ欲しい、凡例はあるのか、などそういう議論になり得る

委員 K :

法制度が支えるということでいえば、おっしゃる通りである。

委員 A :

加えて、公示の問題がある。官報にお金を払って公示をのせる、ホームページに公示を載せるなどの話があるが、ホームページはいつでも消せる上、人によって見せ方も異なる。パブリック・ブロックチェーンを利用して公示ができれば、コストも小さく、フェアなものが実現できるのではないか。

委員 C :

私の資料に記載しているのは、どちらかと言えばそれに近い内容の話である。

事務局：

例えば犯罪による収益移転防止法で多少ハードルが高い、とか、貸金業法で矛盾がある、とかなどあるかと思うが、行法的にブロックチェーンが直面しているハードル、問題点はなにか。

委員 F：

Augur のコードを書くとつかまりますか、とか。

委員 B：

運営者の観点から言いたいことも多い。本人確認の話や KYC（Know Your Customer）の話など。

委員 F：

アセットを勝手に発行したときにどのような法律で罰せられるか。

委員 B：

トークン市場は、この 2 年で大きく広がっている。Spells of genesis などでは、サトシカードが 6 万 5000 円もする。デジタルの価値に value がつくと、それを発行したらどうなるのか。そういう発言が、こういう場ではし辛い。

私も、アドレスを公開していると、勝手に MUFG コインという名前のものを勝手に作って送られてくる。権利を侵害したものを勝手に送られて所有してしまう。

委員 K：

多分、仮想通貨にまずあたるかという論点がこれから出てくる。定義があいう状態で困るということがあるが、曖昧である。どこから当たるのか、はよくわからない。どこまでいっても曖昧な法律である。

委員 B：

そのアセットに配当がくることもある。株と一緒で、利益がでると配当がでてくる。この申告はどうするかなど。

委員 A：

日本円と両替するまでは、すんでいる土地が値上がりする問題と同じか。

委員 B：

そのまま買物もできてしまう。

委員Ｃ：

日本円という概念とわざわざ分ける必要があるのかという話だと思う。

事務局：

次に、政策対応をどうすべきかを考えたい。

委員Ｂ：

法規の明瞭化は必要である

委員Ｋ：

法規の明瞭化との関係で、日本の法制は、具体的な事象に照らして、個別具体的に検討するといういつものパブリックコメントのような状態になっている。これが極めてよくない。デジタルの世界の中では白か黒かしかない。法制そのものの作りが、実質的な妥当性をすごく確保しようとして、個別具体的に検討するようになっているが、丸いモノを八角形でとりあえず切り取って、例えば民拍でも、1年何泊以上と書けば、法律にあたるかあたらないのかがはっきりする。ただ、何泊というものにあまり意味がないが、それによる効率化による価値の大きさはある。

デジタルにあった感じの法制度というのが、先ほどの明瞭化はまさにそこだが、法律の仕組みがそうなっているべき。アメリカの法制度はそうなっている。数字で規律されている。変な結果が導かれることもあるが、それ以上の効率性が実現されている。そういう事を考えて行くべき

委員Ｂ：

マーケットサイズと流動性で対象にするか否かという話は今回盛り込まないのか。
1円でも発行すると、仮想通貨は仮想通貨か。

委員Ｋ：

色はついていない。ビットコインとモナーコインに違いがあるのか、などの区別はつけられていない。

ただ、国際的には日本は対応したと言えるので、国としては良い。

事務局：

次に、国際的な標準化の話で、政策として対応すべきという論点はあるのか、事業者が頑張ると言う話なのか。

委員 M：

公表前なので言いにくいが、ISO の TC68 というのは、日本標準化業界から、日本銀行が受託している。SC7 という委員会が通貨番号を取り扱っていて、やっぱりセキュリティの話とかちゃんと議論してもらったほうがいいよね、専門のワーキングで検討した方が良いのではないですか、という連絡をした

それをうけて、ISO という場所で、仮想通貨のセキュリティに関して議論しようと言う流れになれば、こちらで扱っていただく領域が大きくなるのではないか。

事務局：

標準化の話も当然あるが、EU などでは、FinTech プレイヤーみたいな中間的事業者として定義づけましょうという議論があったり、法的な性格を決めようと言う話があるだろうが、ウォッチするだけで良いのか、議論に参加すべきか。

委員 K：

ブロックチェーンは、場所があまり関係ない。どこかでやると、根こそぎもっていかれる領域のもの。日本でなにかしましょうというのは全く意味がない。どの国と組んでルールをとるかというのを戦略的に考えなければならない。日本だけだとたいしたことはできない。本気でやっているパートナーをみつけ、win-win になるように組めば、日本は経済規模が大きいので、レバレッジをきかせればやっていける。FinTech だと UK だが、ブロックチェーンもそれに相当する発想は重要ではないか。

委員 G：

ワシントン DC と UK など。

委員 K：

誰が取っていくのかを見極めつつの話かと思うが、勝ち馬にのらないとだめなのではないか。

事務局：

経済産業省においても、FinTech 委員会でもでたが、FCA と接触はしているかと思われる。

その他に、メールを後ほど事務局宛てにいただければ、報告書に載せるかは別として経済産業省へのインプットは可能である。

5.　検討会終了後の進め方

事務局より検討会終了後の進め方に関する説明があった

委員 K :

ブロックチェーンの領域は、国際的な競争をしていると思っている。アウトプットが、英語ででるかどうかは極めて大事。このコミュニティの人たちは、外国の議論の資料を全て読んでいる。英語になってでると、日本がここまで検討されている、ということを国際的に示すことになる。国際的なアライアンスを目指すのであれば、アウトプットの出し方は大事である。NRI の契約の中に入っているかはわからないが、どうしても英語で出していただいた方が良いのではないか。

委員 A :

ダイジェスト版でも英語版で出すべきである。

委員 K :

日本が検討しているという事実が日本語版では知られない。

委員 B :

向こうのメディアにも働き掛けられる。

情報経済課 :

概要版の英語版の公表に関しては検討する。

6. 閉会挨拶

以上