CRDS-FY2019-SP-09

戦略プロポーザル

次世代ブロックチェーン技術

～個人や社会のデータ共有・価値交換を安全で高信頼に実現する～

STRATEGIC PROPOSAL

The Next Generation Blockchain Technology

- To establish secure and trustworthy infrastructures for data-sharing and value-exchange among people and society -

国立研究開発法人科学技術振興機構 研究開発戦略センター
Center for Research and Development Strategy, Japan Science and Technology Agency

研究開発戦略センター（CRDS）は、国の科学技術イノベーション政策に関する調査、分析、提案を中立的な立場に立って行う公的シンクタンクの一つで、文部科学省を主務省とする国立研究開発法人科学技術振興機構（JST）に属しています。

CRDSは、科学技術分野全体像の把握（俯瞰）、社会的期待の分析、国内外の動向調査や国際比較を踏まえて、さまざまな分野の専門家や政策立案者との対話を通じて、「戦略プロポーザル」を作成します。「戦略プロポーザル」は、今後国として重点的に取り組むべき研究開発の戦略や、科学技術イノベーション政策上の重要課題についての提案をまとめたものとして、政策立案者や関連研究者へ配布し、広く公表します。

公的な科学技術研究は、個々の研究領域の振興だけでなく、それらの統合によって社会的な期待に応えることが重要です。「戦略プロポーザル」が国の政策立案に活用され、科学技術イノベーションの実現や社会的な課題の解決に寄与することを期待しています。

さらに詳細は、下記ウェブサイトをご覧下さい。

https://www.jst.go.jp/crds/

エグゼクティブサマリー

本提言書では、ブロックチェーン技術を個人および社会の重要データの共有と価値の交換を安全かつ高信頼に実現するための基盤技術と位置づけ、その確立に向け実施すべき研究開発課題を特定し、研究開発の推進方法を提言する。

ブロックチェーンは、ネットワーク上に「ブロック」と呼ばれるデータのかたまりを「鎖（チェーン）」のように連結していく分散台帳の一つの形態である。2008 年に Satoshi Nakamoto が書いた論文により Bitcoin が生まれた。翌年にはオープンソースとして公開され、今日まで 10 年以上実運用されている。そこで使われた、暗号、P2P ネットワークと分散システムなどの技術群と、分散合意形成と継続的運用のためのインセンティブの仕組みは特に新しいものではないが、Bitcoin を実現するものとして、「ブロックチェーン技術」とひとかたまりで総称される。これを第 1 世代のブロックチェーン技術とする。

Bitcoin の成功が明らかにしたことは、インターネット上で、信頼できる第三者機関の代わりに暗号技術を使うことで通貨の直接取引を可能にしたことである。その中核たるブロックチェーン技術は、分散台帳、改ざん不可能性、追跡可能性、分散合意形成、取引機能など魅力的な機能と特長を有する。そのため、暗号資産以外にも適用可能な汎用技術としての期待が高まり、新たなブロックチェーン技術が研究・実装された。その代表がスマートコントラクトである。スマートコントラクトは、取引情報中に、ある種のプログラムを組み込むことにより、価値交換以外の情報管理や処理を可能にする仕組みである。また、Bitcoin が設計思想上、1 秒間に 7 トランザクション程度の取引しか処理できないので、もっと高頻度な取引に対応可能とするために、高速に処理する仕組みも実装された。これらを含めた第 1 世代の拡張を第 2 世代とする。現在はまだこの段階にあると言える。世界中で行われているさまざまな実証実験やプラットフォームは主にこの段階の技術に基づくものである。

本提言書で提案する第 3 世代のブロックチェーン技術は、インターネットを超えて、より安全かつより高信頼な社会基盤となることが期待されている。そのためには規模の拡大に伴うスケーラビリティーの確保、公開すべきでない個人データの扱い、量子計算機時代の暗号への対応など根本的な技術課題に加えて、新技術に対応した商習慣や制度の見直しなど解決すべき課題は多岐にわたる。

本提言書では、ブロックチェーン技術を「個人および社会の重要データの共有と価値の交換を安全かつ高信頼に実現するための基盤技術」と位置づけている。インターネットが情報伝達の基盤とすると、ブロックチェーンは価値交換の基盤である。しかし、現状のブロックチェーン技術は、初期のインターネットがそうであったように要素技術も応用技術も未熟である。理由は、現状、エンジニアリングが先行し、基礎・基盤的な研究開発が追い付いていないこと、通貨以外の応用開発が開発途上であること、および、研究者コミュニティーが分散していることに集約することができる。

ブロックチェーン技術は右図に示すような技術から構成される。最も基盤となるのは、ブロックチェーンが依拠する技術である。暗号技術、P2P ネットワーク技術、運用管理に関わる技術である。その上に位置するのは、ブロックチェーンをブロックチェーンたらしめる固有技術であり、分散台帳、分散合意形成、スマートコントラクトに関わる技術を含む。また、これらの技術を使ってアプリケーションを効率的に実現するための実行環境としてプラットフォームと制度設計がある。

図 ブロックチェーン技術の俯瞰

本提言書では、研究開発による基礎基盤の確立、わが国の国家的社会基盤への適用、および、ブロックチェーンの活用と影響を議論する場の設定を国の事業として推進することを提案する。

（1） 研究開発による基礎基盤の確立

自由な発想に基づく基礎研究を推進すると同時に、研究者が集うインキュベーションプラットフォームを構築することで、多種多様な研究成果の創出と新たなコミュニティーの育成を行う。これにより、現状エンジニアリングが先行し、基礎・基盤的な研究開発が追い付いておらず、研究者コミュニティーが分散している状況を打開する。代表的な研究課題として以下のようなものが挙げられる。

暗号技術：危殆化への対応（量子計算機、暗号プロトコル）、準同型暗号
P2P ネットワーク：可用性維持、攻撃耐性、IoT や 5G への対応
運用管理：鍵管理、版管理
分散台帳：スケーラビリティー、ファイナリティー、匿名性
合意形成：コンセンサスアルゴリズム、インセンティブ設計、攻撃耐性
スマートコントラクト：プログラミングモデル/言語、正当性検証、相互運用・移植性
プラットフォーム：非機能要件（性能、信頼性）、相互接続性、継続性、互換性
制度設計・トラスト： 社会システム／制度設計、トラストフレームワーク

（2） わが国の国家的社会基盤への適用

わが国の国家的社会基盤を確立することで、わが国が目指す社会像 Society 5.0 の具現化の一環として、安全で透明性の高い効率的な次世代の電子政府を世界に先駆けて実現することができる。そのためには、まず、次世代の電子政府のグランドデザイン、特にデータ戦略が重要である。その下で、ブロックチェーンによるデータ交換基盤を構築し、国家的社会基盤に適用する。電子政府と民間サービスとを連携させたアプリケーションは特区制度などを活用して開発する。社会基盤の再構築には長い時間がかかるため、実現には行政の強い意志が最も重要である。日本においても既にデジタルガバメントの議論が始まっていることから、その議論の俎上に載せることが必要である。また、構築に際しては、国家的社会基盤活用の知識体系の構築と使いこなせる人材の計画的育成も同時に図る必要がある。

（3） ブロックチェーンの活用と影響を議論する場の設置

ブロックチェーン技術の潜在的な革新性を考慮すると、人工知能の人間や社会的影響に関する議論と同様の議論の場が必要である。ブロックチェーン技術の本質的な洞察（真価の発現とリスクの回避など）を議論する場をもうけて、定期的にワークショップやセミナーを開催し、質の高い報告書や提言書を発行することが望ましい。

インターネットは社会や人々の生き方を大きく変えた。世界中の計算機や機器をつなげることで、誰もが簡単に情報を発信・検索・活用できる「情報伝達のプラットフォーム」となった。一方で、ブロックチェーンはデータの真正性を保証して価値の共有と交換が簡単にできる基盤を提供する。それにより、誰もがそこにある情報を信用できる、いわば「信頼のプラットフォーム」となる可能性がある。

しかし、そこに至るには、ブロックチェーンの真価を生かす社会システムのあり方に関する議論と、それを実現するための人文・社会科学を含めた広範な分野における研究開発、実証実験が必要である。インターネットの黎明期を世界中で育てたような、長期的な視野に立ったグローバルな活動が望まれる。幸いまだ GAFA[1]のような覇者はいない。わが国が国を挙げて取り組む意義も勝機もそこにある。本提言書はそのような思いをこめて書かれている。

[1] GAFA は米国の IT 企業 4 社（Google、Amazon、Facebook、Apple）頭文字を並べた造語で世界のサイバービジネスを支配する。

Executive Summary

Blockchain technology serves as a fundamental technology for sharing data and exchanging value among people and society. In this proposal we identify issues for basic research and application development, and propose strategies for technology development toward the secure and trustworthy social infrastructure.

Blockchain is a form of distributed ledger in which blocks of data are “chained” consecutively in a network. In 2008 a paper written by Satoshi Nakamoto gave rise to Bitcoin, the first implementation of Blockchain. The following year he released an open source of Bitcoin, which has been in operation for more than 10 years to date. Technologies used in Bitcoin, such as cryptography, P2P networks and distributed systems, the mechanism of incentives for distributed consensus building, and continuous operation are not particularly new. These technologies which enabled Bitcoin are collectively referred to “Blockchain technology”, especially the first generation blockchain technology in this proposal.

The success of Bitcoin has revealed that cryptographic proof of trust allows direct transactions between parties on the Internet without trusted third parties. Blockchain, the core technology of Bitcoin, has attractive functions and features such as distributed ledger, immutability, traceability, distributed consensus mechanism, and transaction functions. For this reason, expectations as general-purpose technology applicable to other than crypto-assets have increased, and emerging blockchain technology have been researched and implemented. Moreover, Blockchain itself is evolving by introducing new technology. One example is smart contract, which is a program incorporated in transaction data to enable exchange various values automatically. Another is a second layer technology which accelerates transaction speed much faster than Bitcoin which intentionally processes only about several transactions per second due to its design philosophy. These extensions to the first generation lead the Blockchain to the second generation. We are now still at this stage. Accordingly, the various demonstration experiments and platforms conducted around the world are mainly based on this stage of technology.

We believe the basic research and application development to establish secure and trustworthy infrastructures for data-sharing and value-exchange among people and society. To this end, there lies a wide variety of issues to be solved from basic research to application development such as securing scalability with the expansion of use of data, handling personal data that should not be disclosed, supporting cryptography in the quantum computer era and so on, as well as re-designing business practices and systems corresponding to completely new technology.

In this proposal we position the blockchain technology as "a fundamental technology for safely and reliably realizing the sharing of important personal and social data and the exchange of value." While the Internet is the basis for information exchange, the Blockchain will be the basis for value exchange. However, current blockchain technology is as immature as the dawning of Internet in senses both fundamental and application technology. The

reasons can be summarized as follows: engineering is ahead and basic research is not keeping up; applications other than cryptocurrency are under development; and research community is dispersed in silos.

The blockchain technology stack is shown in the figure. The foundation stack contains technologies on which the blockchain rely such as encryption technology, P2P network technology, and system management. On top of it lays the blockchain core technology that make blockchain itself, including technologies related to distributed ledgers, distributed consensus building, and smart contracts. There are also platforms and institutional designs as execution environments for efficiently realizing applications using these technologies.

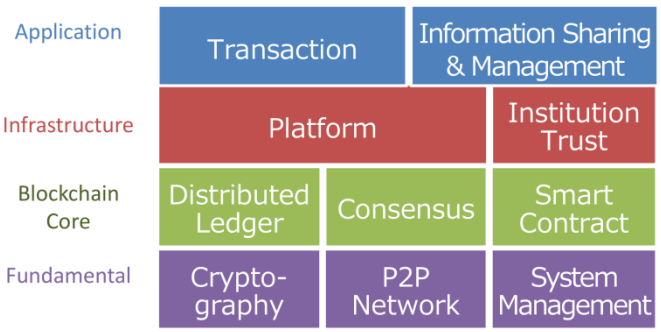


Figure Blockchain Technology Stack

We propose that the nation should promote as national projects 1) to establish Blockchain technology foundation through research and development, 2) to apply to the national social infrastructure, and 3) to initiate forum activity for continuous discussions regarding the social visionaries and impacts of the future.

（1） Establish Blockchain technology foundation through research and development

It is vital to promote curiosity driven basic research and to build an incubation platform where researchers gather in order to create a wide variety of research results and foster new research communities. This breaks the situation where engineering is ahead of basic research as well as the research community is dispersed in silos.

（2） Apply blockchain to the national social infrastructure

By establishing Japan's national social infrastructure using Blockchain, it is possible to realize a safe, transparent, and efficient next-generation digital government ahead of the rest of the world as part of the realization of "Society 5.0", the future social image that Japan aims for. To do so, first, we need the grand design of the next generation digital government, especially data strategy is critical. Then the data exchange infrastructure based on blockchain is to be built and applied to the national social infrastructure.

Applications that link digital government services and private services will be developed in some specific test areas. However, seeing the case of Estonia, rebuilding the social infrastructure takes a long time. Strong will of the government is crucial for its realization. Discussions on digital government have already begun in Japan regardless of emerging technology such as Blockchain. It is important to take technical discussion into consideration. In addition, it is necessary to simultaneously build a body of knowledge for utilizing the national social infrastructure and strategically develop human resources.

（3） Initiate forum activity for continuous discussions

Given the potential innovations of blockchain technology, there is a need for discussions similar to that for the human and social impact of artificial intelligence. Regular workshops and seminars to publish high-quality reports and recommendations, with the opportunity to discuss the essential insights of blockchain technology (e.g., realizing value and avoiding risks) are crucial.

The Internet has transformed society and the way people live accordingly. By connecting computers and devices around the world digitally, it has become the "information exchange platform" that allows anyone to easily send, receive, search and use information. Blockchain, on the other hand, will provide the basis for ensuring the authenticity of data and making it easy to share and exchange values. This could be the "trustworthy platform" that anyone can trust the information on the blockchain based infrastructure.

However, in order to reach that point, intensive discussion should be continued regarding how social systems can make full use of the potential of blockchain, while conducting R&D and proof of concept experiments with the cooperation of Social Science and Humanity. It is also imperative that Blockchain-related communities work together from global and long-term perspective, as were done to foster the Internet by all around the world from its dawn. Fortunately, there is no champion like GAFA so far. There are both significance and opportunities for Japan to lead the world. This proposal was written for “The Blockchain” with such thoughts in mind.

目　次

1. 研究開発の内容

1.1 ブロックチェーンとは

ブロックチェーンは、ネットワーク上に「ブロック」と呼ばれるデータのかたまりを「鎖（チェーン）」のように連結していく分散台帳の一つの形態であり、仮想通貨[2]（暗号資産）Bitcoin の実装で初めて用いられた。一般に、分散台帳とは、ネットワーク上の複数のノード間で共有されつつ同期されることで同じ状態が保たれるデータの集合である。整合性を保つために P2P（Peer to Peer）ネットワーク技術と合意形成アルゴリズムが使われるので、分散システムとみることもできる。Bitcoin では、信頼できる第三者機関が存在しない状況でも、個々のデータと系全体のデータの真正性を保証することができるよう高度な暗号技術を採用している。ブロックチェーンに関する基礎から応用までさまざまな研究開発が世界中で行われており、ブロックチェーンそのものの実態も今後変化する可能性が高いため、本提言書では現在および将来にわたってブロックチェーンを構成する可能性のある技術を広く含めてブロックチェーン技術と呼ぶこととする。

ブロックチェーンは Bitcoin を実現するために設計された。暗号資産自体は暗号技術の応用として古くから考えられてきたが普及には至らなかった。ところが、2008 年に Satoshi Nakamoto が書いた論文[3]とその実装により、Bitcoin が生まれた。実装はオープンソフトウエアとして公開された。そのなかで使われた、暗号技術、P2P ネットワーク技術と分散システム技術などの技術群と、分散合意形成と継続的運用のためのインセンティブの仕組み（プルーフ・オブ・ワーク）がブロックチェーン技術の基礎となった。

ブロックチェーン技術は進化し続けている。Bitcoin および Bitcoin から派生した暗号資産で使われるブロックチェーン技術を第 1 世代とする。Bitcoin の成功が明らかにしたことは、インターネット上で、信頼できる第三者機関の代わりに暗号技術を使うことで通貨の直接取引を可能にしたことである。その中核たるブロックチェーン技術は、分散台帳、改ざん不可能性、追跡可能性、分散合意形成、取引機能など魅力的な機能と特長を有する。そのため、暗号資産以外にも適用可能な汎用技術としての期待が高まり新たなブロックチェーンが研究・実装された。その代表がスマートコントラクト（契約の自動化）である。スマートコントラクトは、取引情報中にある種のプログラムを組み込むことにより、価値交換以外の情報管理や処理を可能にする仕組みである。また、Bitcoin が設計思想上、1 秒間に十数取引程度しか処理できないため、もっと高頻度な取引に対応可能とするために、高速に処理する仕組みも実装された。これらを含めた第 1 世代の拡張を第 2 世代とする。現在はまだこの段階にあると言える。世界中で行われているさまざまな実証実験（PoC）やプラットフォームは主にこの段階の技術に基づくものである。

第 3 世代のブロックチェーン技術は、現状の PoC を超えて安全かつ高信頼な社会基盤となることが期待されている[4]。そのためには規模の拡大に伴うスケーラビリティーの確保、公開すべきでない個人データの扱い、量子時代の暗号への対応など根本的な技術課題に加えて、新技術に対応した法制度の見直しなど解決すべき課題は多岐にわたる。

---

[2] 仮想通貨（Virtual Currency）という呼称は、法定通貨との誤認の可能性を排除するために改正資金決済法（2019 年 5 月）にて名称を暗号資産（Crypto-asset）と名称を変更した。本提言書でもそれに従う。
[3] S. Nakamoto,” Bitcoin: A Peer-to-Peer Electronic Cash System”, https://bitcoin.org/bitcoin.pdf
[4] 特に熱心なのは欧州委員会である Blockchain Initiative の下、複数のプロジェクトを実施している。

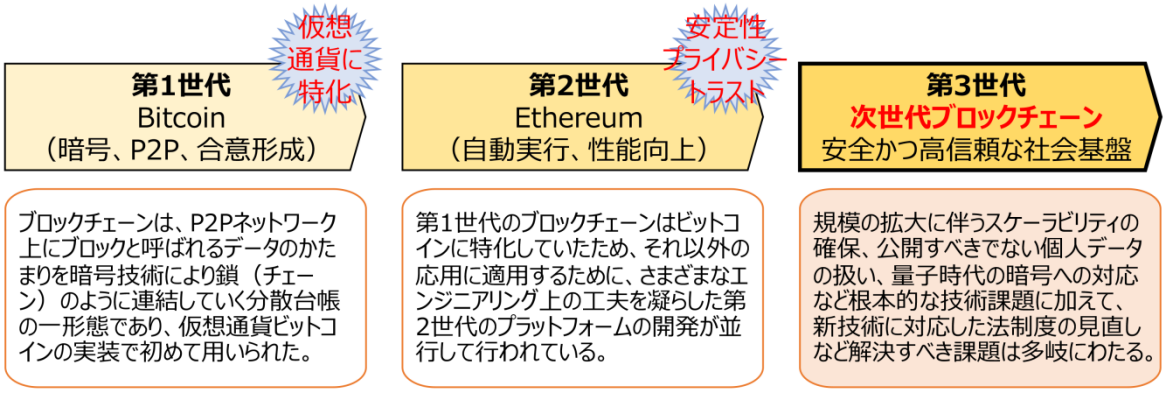


図 1.1 次世代ブロックチェーン技術とは

1.2 提案する研究開発の概要

本提言書では、ブロックチェーン技術を「個人および社会の重要データの共有と価値の交換を安全かつ高信頼に実現するための基盤技術」と位置づけている。従来のインターネットが情報伝達の基盤として歩んできた歴史を概観すると、現状のブロックチェーン技術は、インターネットの黎明期がそうであったように要素技術も応用技術も未熟である。研究開発の現状は以下の３点に整理できる。

- エンジニアリングが先行し基礎・基盤的な研究開発が追い付いていない
- 通貨以外の応用は開発途上である
- 研究者コミュニティーが分散している

（１）研究開発課題の俯瞰

科学技術的課題を述べるのに先だってブロックチェーンに関わる技術を俯瞰する（右図）。最も基盤となるのは、ブロックチェーンが依拠する技術である。暗号技術、P2P ネットワーク技術、運用管理に関わる技術群が挙げられる。これらは、計算機科学の分野においてそれぞれ 30 年以上の歴史を持つ。その上に位置するのは、ブロックチェーンをブロックチェーンたらしめる固有技術群である。具体的には、分散台帳、分散合意形成、スマートコントラクトに関わる技術である。また、これらの技術を使って特定の応用を効率的に実現するための実行環境として、ソフトウエアとしてのプラットフォームと制度設計や信用モデルがある。

図 1.2　ブロックチェーン技術の俯瞰

ブロックチェーンの応用は、ブロックチェーン上に記録されるデータの種類により、取引管理

と情報共有・情報管理の二つに分類できる。取引管理は、複数の当事者間のやり取りの記録を管理し、情報共有・情報管理は、特に取引に関わらない種々の情報の記録を管理する。情報共有と情報管理の違いは、一般に記録された情報を、公開情報として扱うか、個人情報として扱うかの違いである。

（２）ブロックチェーンを構成する技術

ブロックチェーンを構成する技術は、大きくブロックチェーンが依拠する基盤技術とブロックチェーンの中核となる固有技術に分けることができる。これらは、相互に依存する個別の技術の集合であり、暗号資産や特定の応用システムを構築するために適宜取捨選択されるものである。研究開発は独立して実施することも可能であるが、得られた研究成果は個別の研究者コミュニティーで共有するだけでなく、より上位のより広い場に公開され議論されることが望ましい。

【ブロックチェーンが依拠する基盤技術】

この領域の技術は、ブロックチェーンの実現に特化したものではないため、技術そのものの視点や、広く応用を意識した視点による、研究者および研究コミュニティーの好奇心や自由な発想に基づく研究開発により促進される。本領域に関する研究開発課題は以下の通りである。

- 暗号技術：危殆化への対応（量子計算機、暗号プロトコル）、準同型暗号
- P2P ネットワーク：可用性維持、攻撃耐性、IoT や 5G への対応
- 運用管理：鍵管理、版管理

【ブロックチェーンの中核となる固有技術】

この領域の技術は、ブロックチェーンをブロックチェーンたらしめている技術である。個別にはブロックチェーン以前からある技術だが、ブロックチェーンの普及に合わせて特に重要性が高まったといえる。単独の研究開発というより、既存のプラットフォームの改良や、新たなプラットフォームの開発に関する研究が盛んに行われている。具体的な応用分野を想定したプロジェクトタイプの研究開発促進が望ましい。本領域に関する研究開発課題は以下の通りである。

- 分散台帳：スケーラビリティー、ファイナリティー、匿名性
- 合意形成：コンセンサスアルゴリズム、インセンティブ設計、攻撃耐性
- スマートコントラクト：プログラミングモデル／言語、正当性検証、相互運用・移植性

（３）プラットフォームおよびアプリケーション

ブロックチェーンのプラットフォームは、中心となる管理者が存在せずに誰でも参加できるパブリック型（例：Bitcoin や Ethereum）と、管理者がいて参加に許可が必要なプライベート型（例：HyperLedger Fabric）に大別できる[5]。さらに、プライベート型のブロックチェーンを企業間で共有する場合は特にコンソーシアム型と呼ぶ。現状、代表的なブロックチェーンのプラットフォームは OSS（オープンソースソフトウエア）である。OSS としての一般的な課題として、ベンダーのサポートや継続性に対する保証がない。したがって、例えば電子政府など継続的な運用を前提とした場合に、性能、信頼性、拡張性、運用性などの非機能要件や相互接続性、継続性、互換性が課題となる。そのため、企業のサポートのないプラットフォームにおいては非機能要件等が不

[5] 参加に許可が必要か否かという意味で前者を Permissionless 型、後者を Permissioned 型と呼ぶこともある。

十分であることを前提にいかに上手に利用するかといった知識体系ガイド[6]が必要となる。一方で、利用側の立場からするとプラットフォームやそれを使ったシステムを利用する際のトラスト（信頼を担保する仕組み）をいかに設計・構築するかという課題にも取り組む必要がある。

- プラットフォーム：非機能要件（性能、信頼性）、相互接続性、継続性、互換性
- 制度設計・トラスト：社会システム/制度設計、トラストフレームワーク

一方で、アプリケーションに関しては、ブロックチェーンが有する分散台帳や取引機能、改ざん困難性や追跡可能性、分散合意形成などを生かすべくさまざまなアプリケーションが PoC（Proof of Concept）として世界中で実施されている。しかし、暗号資産への適用を除いて、多くはブロックチェーン技術を使わなくても実現できると言われている。その理由は、既存のシステムの一部にブロックチェーンの要素技術を適用したにすぎないからであり、ブロックチェーンの革新性を享受するためには、ビジネスプロセスそのものの再構築が必要であり、現状はまだそのための意義の普及や、方法論が確立していないことによる。

1.3 推進方法

本提言書では、研究開発による基礎基盤の確立とわが国の国家的社会基盤への適用を国の事業として推進することを提案する。

- **研究開発による基礎基盤の確立**

  自由な発想に基づく基礎研究を推進すると同時に、研究者が集うインキュベーションプラットフォームを構築することで、多種多様な研究成果の創出と新たなコミュニティーの育成を行う。これにより、現状エンジニアリングが先行し、基礎・基盤的な研究開発が追い付いておらず、研究者コミュニティーが分散している状況を打開する。

- **わが国の国家的社会基盤への適用**

  わが国の国家的社会基盤を確立することで、わが国が目指す社会像 Society 5.0 の具現化の一環として、安全で透明性の高い効率的な次世代の電子政府を世界に先駆けて実現することができる。そのためには、まず、次世代の電子政府のグランドデザイン、特にデータ戦略が重要である。その下で、ブロックチェーンによるデータ交換基盤を構築し、国家的社会基盤に適用する。電子政府と民間サービスとを連携させたアプリケーションは特区制度などを活用して開発する。

  社会基盤の再構築には長い時間がかかるため、実現には行政の強い意志が最も重要である。日本においても既にデジタルガバメントの議論が始まっていることから、その議論の俎上に載せることが必要である。また、構築に際しては、国家的社会基盤活用の知識体系の構築と使いこなせる人材の計画的育成も同時に図る必要がある。

- ブロックチェーンの活用と影響を議論する場の設置

  ブロックチェーン技術の本質的な洞察を議論する場を設置し継続的に議論することで、技術の真価を引き出しつつ想定されるリスクに備えたグランドデザインにつなげる。

インターネットは社会や人々の生き方を大きく変えた。世界中の計算機や機器をつなげることで、誰もが簡単に情報を発信・検索・活用できる「情報伝達のプラットフォーム」となった。一

[6] 専門領域に関する観念、ガイド、手法、方法論、ベストプラクティスなどをまとめたもの。プロジェクト管理の PMBOK が有名。

方で、ブロックチェーンはデータの真正性を保証して価値の共有と交換が簡単にできる基盤を提供する。それにより、誰もがそこにある情報を信用できる、いわば「信頼のプラットフォーム」となる可能性がある。

しかし、そこに至るには、ブロックチェーンの真価を生かす社会システムのあり方に関する議論と、それを実現するための人文・社会科学を含めた広範な分野における研究開発、実証実験が必要である。インターネットの黎明期を世界中で育てたような、長期的な視野に立ったグローバルな活動が望まれる。幸いまだ GAFA のような覇者はいない。わが国が国を挙げて取り組む意義も勝機もそこにある。本提言書はそのような思いをこめて書かれている。

2．研究開発を実施する意義

ブロックチェーンは非中央集権的な仕組みで価値の交換を記した台帳を分散共有することを可能にしたことに本質がある。これまで、例えば銀行が中央集権的に担ってきた「信頼」を、中央集権的な組織なしで、安全に共有することができる。すなわち、デジタル技術によって人と人を信頼でつなぐことができるようになったともいえる。中央集権的に保証や仲介をしてきた事業者は不要になり、これまでと違った、分散と自動化による新たなビジネスが可能になる。いわば、紙をベースに人間が関わる仕事の進め方から、完全にデジタルなビジネスへの移行であり、大きな社会変革の可能性を秘めている。

一方で、科学技術的課題は山積しており、プログラムによる自動取引（スマートコントラクト）などの機能的要件に加えて、性能、安全性などの非機能的要件もまだまだ改良、改善が必要である。また、金融取引にとどまらず、有形無形資産の取引、デジタルコンテンツの流通、保険や身分の証明など、さまざまな応用に対応するためには、サービス全体の設計・実装基準などの見直しや整備が必要となる。さらに、これまでとはスキームの異なるビジネスとなることを勘案すると、従来の商習慣や法制度との兼ね合い、それらの刷新も含めて社会との共創が重要なテーマとなる。これらの課題を解決することによって、ブロックチェーン技術は新しい法、経済、社会制度を生み出す基盤となることができる。

2.1 現状認識および問題点

ブロックチェーンは最初のユースケースとして Bitcoin が社会実装され、世界中のマイナー（採掘者）がマイニング（採掘）と呼ばれる取引を承認する処理を競い、投機的な価値を持つ暗号資産を獲得するためにハードウエアが急速に進化した。ブロックチェーン技術により実現されている 4 つの主要暗号資産システム(Bitcoin、Ethereum、Litecoin、Monero）で使用されているマイニングにかかる消費電力が年間約 16.6 テラワット時にもなり、スロヴェニアの電力量と同程度といった莫大な電力消費量となっている。世界の電力消費への脅威だけでなく、地球環境への影響についても喫緊の改善が必要である。

ブロックチェーンを構成する要素技術は、暗号技術・P2P ネットワーク・分散合意形成、社会システムデザインなど、これまで相互に交わる機会のあまりなかった研究コミュニティーに属する。ブロックチェーンを将来の社会インフラ技術の重要コンポーネントとするために、準備段階として研究開発や社会実装の環境整備が不可欠である。わが国では、総務省、経産省が動向調査や実証実験を実施し、日銀は欧州中央銀行と分散型台帳の金融分野への応用を調査するなど、産官学が独立して動いている。

現状は、ブロックチェーンは、情報だけでなく価値交換の基盤から社会基盤そのものになる可能性があるとして将来性を期待する声は大きく、東京大学はさいたま市で電力ルーターを用いた電力取引の検証も開始している。改ざん困難な分散台帳の応用は、取引管理だけでなく情報共有・情報管理まで広範であり、世界中で PoC が行われているが、Bitcoin などの暗号資産は除き、ブロックチェーンを構成する全ての機能をつかったものはまだ存在せず、ブロックチェーンを使わなくても実現できるケース（Blockchain Inspired Solution と呼ばれる）、既存の手段で実現できるものがほとんどである。

ブロックチェーンをつかって再構築された新たな社会システムにおいては、ブロックを生成す

るインセンティブを確保し続けることが課題となる。分散合意形成が PoW 等ではうまくいかない場合には、例えば、PoA（Proof of Authority）[7]のような別の仕組みが必要となり、その際にはオーソリティーとしての国や自治体などの存在があらためて重要となる。後述するエストニアなどの取り組みを参考にした施策の検討が望まれる。

２.１.１ 諸外国の政策や動向の俯瞰

（１）米国

米国は産と学が積極的に関与し、官は金融関係で規制を実施している。Bitcoin network、Ethereum、Hyperledger Fabric 等のプラットホーム囲い込みが進行し、米 JP モルガンは独自プラットフォーム Quorum を開発し送金業務に適用し、米 Walmart と IBM が食品追跡システムを共同開発している。米 Ripple 社が「大学ブロックチェーンリサーチ構想」を呼びかけ第 4 の勢力に浮上、標準化 ISO/TC307「ブロックチェーンと電子分散台帳技術に係る専門委員会」を立ち上げた。

Microsoft は、Azure 上で動作する BaaS（Blockchain as a Service）の開発・展開に加え、分散台帳技術を開発するエンジニアに向けて新たに Azure Blockchain Workbench を公開した。Google は、ブロックチェーンを用いて改変を検知できるログに署名を保管し、システムに保管された情報が修正されていないことを保証するか、何の情報がいつ変更されたかを追跡可能とする技術に関する特許を 2017 年 9 月に申請した。

米国 IEEE（Institute of Electrical and Electronics Engineers）は、ブロックチェーン技術の開発と採用において重要な役割を果たすことを考えており、2018 年 1 月に IEEE Blockchain Initiative（BCI）を発足させた。BCI は IEEE におけるブロックチェーンの全てのプロジェクトおよび活動のベースとなる。BCI は、標準化、教育、イベント、コミュニティー開発とアウトリーチなどといったさまざまな活動で構成されている。また、BCI 発足後最初のシンポジウムを 2018 年 7 月に Blockchain-2018: The 2018 IEEE International Conference on Blockchain として開催した。

（２）欧州

欧州は欧州委員会（EU）や国が主導している。EU Blockchain Initiative は EU 全体の基盤構築を検討しつつ、複数のプロジェクトを走らせている。2018 年には、ブロックチェーンによるイノベーションの加速と EU 内のブロックチェーンエコシステムの開発を目的とした EU Blockchain Observatory and Forum を設立した。100 名規模の有識者によるフォーラム活動を精力的に実施し、”Blockchain Innovation in Europe”、”Blockchain and the GDPR”、”Blockchain for Government and Public Services”等の質の高いレポートを発行している。Digital Single Market も 2017 年の中間評価でブロックチェーンに関連づけられた。他にも、”Horizon Prize on Blockchains for Social Good”や暗号資産に関するプロジェクトもイニシアティブの下で開発が進められている。

Wien 工科大学の Matteo Maffei 教授が率いる研究グループが、Ethertrust プロジェクトにより、Ethereum のスマートコントラクトのセキュリティーを向上させる研究成果を 2017 年 11 月末に発表した。スウェーデンのチャルマース工科大学（Chalmers University of Technology）では、公平なモビリティサービスに向けた MaaS（Mobility as a Service）におけるブロックチェーン技術の役割について研究している。フィンランドの Aalto 大学は、Pekka Nikander 教授をリー

[7] PoA では、トランザクションとブロックは、バリデーターと呼ばれる承認済みのアカウントによって検証される。

ダーとして、2018 年から SOFIE と呼ばれる 3 年間の EU Horizon 2020 プロジェクトを立ち上げ、技術的および商業的にオープンなフレームワークを創造し、IoT を統合するためのオープンなビジネスプラットフォームの創出に関する研究を行っている。

IoT のための暗号資産 IOTA と有向非巡回グラフを応用した IOTA のコア技術 Tangle に関するプロジェクトが、ベルリンを拠点にして 2015 年に始まった。EU の DECODE（Decentralized Citizens Owned Data Ecosystem：分散型市民所有データエコシステム）プロジェクトが 2017 年に開始した。個人データを米国大手 IT 企業から取り戻し、データ主権を個人にもたらすことを目的としている。現在、EU Horizon 2020 プログラムの一環として、14 のコンソーシアムメンバーに総額 500 万ユーロ（約 6 億円）の資金が 2019 年末まで提供され、プロジェクトが進行中。分散型台帳技術と組み合わせて実現する DECODE の新技術は、アムステルダムとバルセロナで実証実験が行われる予定である。My Health My Data (MHMD) プロジェクトは、医療データのプライバシーとセキュリティーにおける新しいパラダイムシフトを目指した EU Horizon 2020 プロジェクトであり、2016 年 11 月にスタートした。EU から総額 400 万ユーロ（約 5 億円）の資金が 2019 年末まで提供され、機密データとしての医療データの共有方法を根本的に変えることを目指している。フランスの銀行グループ Société Générale とオランダの金融サービス会社 ING が協力して、石油取引に焦点を当てた Easy Trading Connect プロジェクトとして、ブロックチェーン技術の導入により商品取引の処理時間を 3 時間から 30 分未満に短縮できることを 2017 年 2 月に実証した。デンマークのコペンハーゲンに本社を置く海運業界のスタートアップ Blockshipping は、世界中の 2700 万個のコンテナをリアルタイムで追跡、記録する世界初のブロックチェーン・プラットフォーム（Global Shared Container Platform: GSCP）を開発中。オランダ最大級のスーパーマーケットチェーン Albert Heijn は、2018 年 9 月、清涼飲料水を専門とする充填事業者 Refresco と提携して、プライベートブランドのオレンジジュースを対象に、ブロックチェーン技術を活用して、ブラジルのオレンジ農園から各店舗に陳列されるまでのサプライチェーンをすべてデータ化することで、サプライチェーンの透明化を開始した。

エストニアはブロックチェーンを活用した国家基盤を世界に先駆け構築したブロックチェーン先進国で人口 132 万人（2018 年）の小国である。エストニアは、国を挙げて電子政府化に取り組んでいるデジタル先進国である。ブロックチェーンにおいても先進的なチャレンジを続けており、Bitcoin の登場よりも早い 2008 年に、ブロックチェーンの原型とも言える “hash-linked time-stamping” 技術の試験的実装を開始した。2012 年には正式に実装され、エストニアは世界初のブロックチェーン導入国家となった。エストニアにおけるブロックチェーン導入と深く関係しているのが、2006 年に同国に設立された Guardtime 社である。同社は、Keyless Signatures Infrastructure (KSI)という独自のブロックチェーン技術を強みとしている。従来のブロックチェーン技術は公開鍵暗号方式を採用してきたが、KSI はハッシュを台帳の維持管理にのみ利用している点に特徴がある。KSI はブロックチェーンのもつ改ざん耐性をもちつつ、限られた機関でのみ利用可能とした技術であり、例えば医療情報のような高度な個人情報を有するデータも取り扱い可能である。KSI ブロックチェーン技術は、e-ヘルスレコード、e-処方箋データベース、e-Law／e-Court システム、e-Police データ、e-バンキング、e-ビジネス登録、e-Land などのエストニア電子政府の多くのサービスを保護している。また、タリン工科大学（Tallinn University of Technology）では、e ヘルス実現のために、すべての医療データの完全性をブロックチェーン技術によって保証する研究が進められている。

英 DeepMind 社や米 MIT がヘルスケアデータの共有と活用を行い、独 Data Management Hub は、研究データの検索、アクセス、再利用などが可能な研究データ用分散データ基盤を構築している。

（３）その他

中国、カナダは Bitcoin のマイニングで世界をリードし、同時に大量な電力を消費している。中国の清華大学 Li Liao 教授らは、世界初のパーソナル AI 技術を開発しているベンチャー企業 ObEN とともに、ブロックチェーンの多くの課題（セキュリティー、トランザクション速度、容量、スケーラビリティー、およびエコシステム構築）を探求している。中国初のブロックチェーン実験特区が 2018 年 10 月、海南省海口市に正式にオープンした。暗号資産取引所 Huobi（火幣）は、国内本社を移し、Tianya Community（天涯社区）とともにブロックチェーン研究室を設立するとともに、10 億ドル規模のグローバルブロックチェーン業界ファンドを創設する計画である。Alibaba（阿里巴巴）が提供するクラウドサービス Alibaba Cloud's BaaS の提供地域が、2018 年 10 月、米国、ヨーロッパ、東南アジアなどを含む国際市場にまで拡大した。なお、本技術は、Hyperledger Fabric に加え、Ant Blockchain（Alibaba グループの金融関連会社 Ant Financial Services が独自開発した Blockchain プラットフォーム）に基づいたものである。Web サービス会社 JD.com（京東商城）は、米国 New Jersey 工科大学と中国科学院ソフトウエア研究所（ISCAS）と協力してブロックチェーン研究所を 2018 年 10 月に設立。分散型アプリケーション（DApps）の基本的なコンセンサス・プロトコル、プライバシー保護、セキュリティーなどに関する研究を長期的に行っていく計画である。

２.１.２ 論文や特許の動向

2008 年 Bitcoin の登場とその後の普及に呼応するように、この 10 年で急速に立ち上ってきており、基礎研究はこれからである。慶應義塾大学と東京大学国際産学連携グループが BASE アライアンスを設立し、研究者コミュニティー（学会など）は立ち上がったばかりである。さまざまな課題を解くための研究が進められ、技術的な課題は認識され着実に改良が進み、エンジニアは新たな技術を生み出そうとしている。利用者がビジネスとして使いにくいところを直し、使っていく中で標準化が進み、複雑でグローバルなデータや価値の共有と流通に必要な新たなプラットフォームに進化することが期待されている。

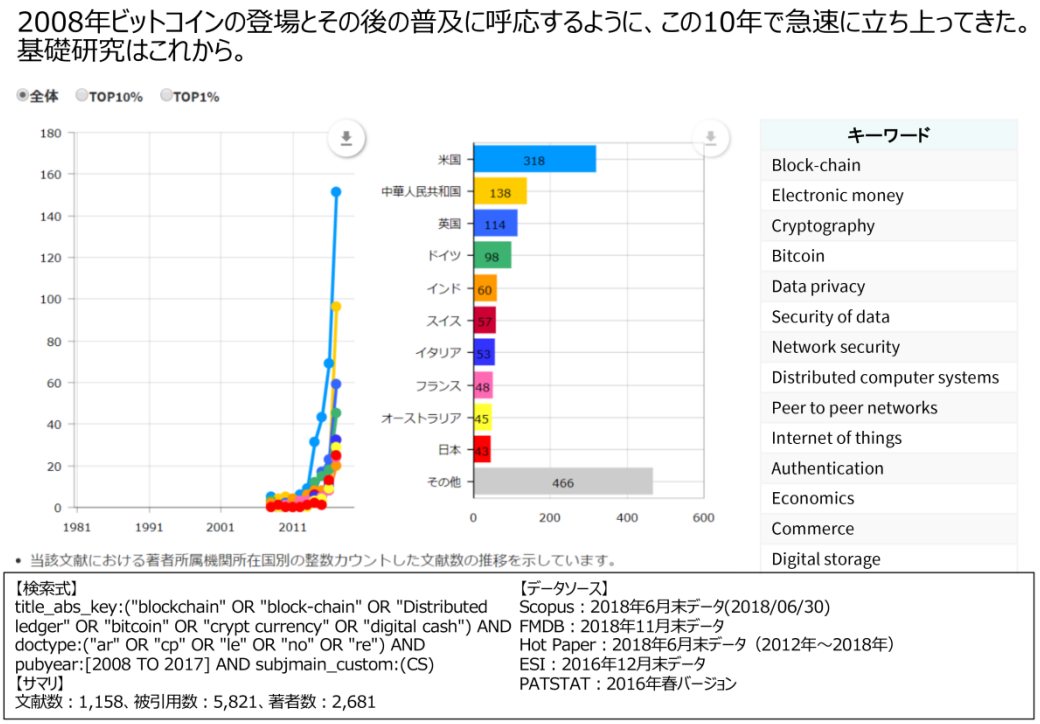


図 2.1　論文の動向

2.2 社会・経済的効果

ブロックチェーンは暗号、P2P ネットワーク、分散合意形成などの技術を基盤とするものであり、「情報を共有しても改ざんされない」、「価値流通の仕組みを簡単に作れる」、「価値のトレーサビリティを担保できる」というメリットを有する 。さらにこれらのメリットを活用することによって、①分散台帳、②改ざん不可能、③追跡可能、④合意形成、⑤デジタル資産化、⑥取引などの機能が実現され、これらの機能を組み合わせることによって、図 2.2 に示すよう、「創造的破壊」、「デジタル資産の市場」、「プロセスの効率化」、「記録の保存」などの社会的なインパクトのある応用が生みだされる。

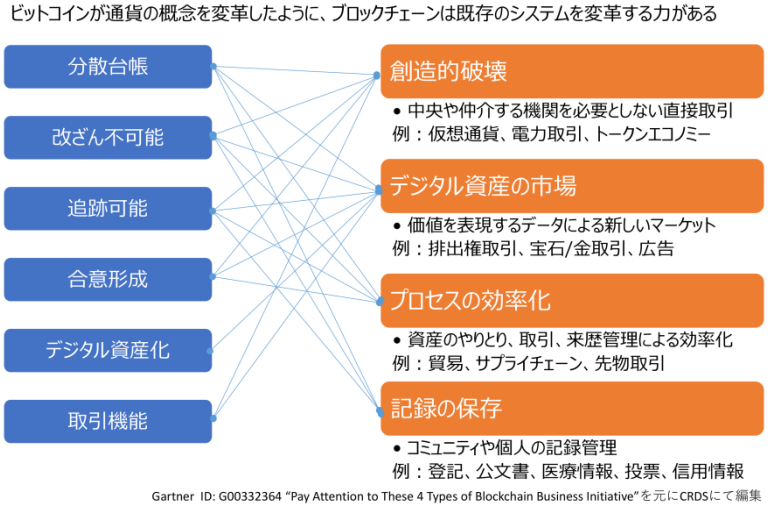


図 2.2　ブロックチェーンの機能と社会・経済的的インパクト
Gartner Pay Attention to These 4 Types of Blockchain Business Initiative”を元に編集

以下に応用例を示す。

- **サプライチェーンへの応用**

IBM と、海運大手の Maersk（マースク）は 2018 年 1 月に貿易分野でブロックチェーンを活用する共同ベンチャー『Maersk TradeLens（マースク・トレードレンズ）』の設立を発表した。貿易管理においては、商品の発送、通関、荷役、受取などの膨大な手続きを、いくつもの国と機関をまたがって行わなければならない。現状では紙の資料を使って、時には数百にものぼる手続きを進めている。ここにブロックチェーンを適用することによって、すべての関係者に対して、手続き情報が改ざんされることなく開示されるようになり、劇的な貿易管理業務の効率化が期待される。中央集権的な仕組みを必要としないため、多くの国と機関をまたがっても、情報流通の仕組みを比較的手軽に構築することができる。またブロックチェーンの提供するトレーサビリティによって、手続きの間違いや、商品の不備なども追跡することができ、トラブル対応の迅速化・効率化も実現される。

このほかにも、車両や航空機の利用状況管理、ダイヤモンドなどの高級品の真贋証明、食品のトレーサビリティなどへ応用されようとしている。

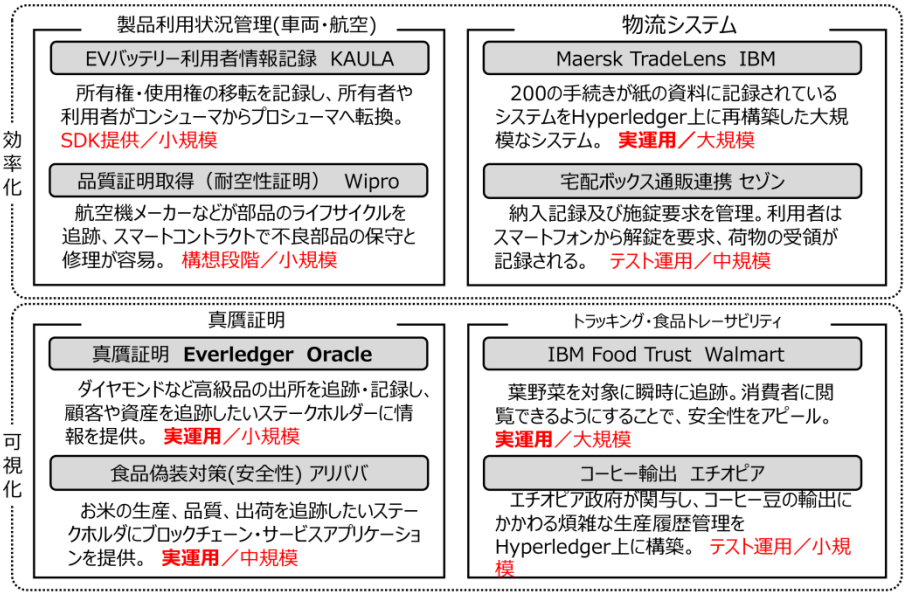


図 2.3　サプライチェーンにおける適用の分類

安心、安全な社会を実現するために、製品利用状況管理と物流システムは効率化、真贋証明とトラッキング・食品トレーサビリティは可視化を目的としている

経済的なインパクトは、経済産業省の試算によると、サプライチェーン管理、プロセス自動化/効率化、シェアリング、価値流通、権利証明などにおいて 67 兆円にのぼるといわれている[8]。また、世界経済フォーラムのレポートでは、ブロックチェーンによる障壁の撤廃により、今後 10 年間に 1 兆ドル規模以上の貿易が新たに生まれる可能性があると指摘されている[9]。

[8] 経済産業省、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、2016 年 4 月 28 日
[9] World Economic Forum, “Trade Tech – A New Age for Trade and Supply Chain Finance”, Sep. 2018

【コラム】木材産業サプライチェーンへの適用事例

近年、SDGs の浸透により、違法伐採対策の強化・輸入材の合法性確認が求められる機会が増えている。現状は FAX を使って製造履歴、流通経路などの情報を追跡するために多くの時間とコスト、事務作業が発生している。そこで、市場での決済履歴をブロックチェーンに記録することで、与信管理や事業体の評価（評判管理）も実現し、CoC 認証（Chain of Custody Systems）で定められている要件を満たすためのデータの登録なども自動化する取り組みが始まっている。従来市場が担ってきた限定的な需給調整機能に換わる効率的な仕組みを、関係者の利益を最大化できるようにブロックチェーンで構築する。デジタルによる流通基盤の実現は利用者間のマッチング、商品・サービスとその対価の交換を促進し、関係者全員にとっての新たな価値創造の礎となることが期待されている。

海外では、スペインの農林水産省が、透明性を高め発展に役立つ技術を創出するために、ブロックチェーンを適用したアプリを開発した。このプロジェクトを担当しているのはスペインの農林水産省により設立された ChainWood グループで、8 つのさまざまな地域パートナーで構成され、木材供給のトレーサビリティと効率を向上させるために、ブロックチェーンの技術を物流に導入することを検討している。森林資源から得られる木材、セルロース、バイオマスなどは、製造・加工プロセスが多段階であり、ブロックチェーンで構築することで、より透明性が高まる。

国内では、サプライチェーンにおける木材デジタルトラッキング情報の改ざん防止に向けた研究が進行している。木材を識別する方法として、バーコードや IC タグなど外から ID を与える方法が従来一般的だが、ここでは物質そのものの個体差を画像情報から導き出し識別する物体指紋認証を利用する。具体的には、年輪や木目などの画像を使用した物体指紋により真正性を担保することで、バーコードや IC タグなどの脱落・損傷や、悪意を持ってはがしたり、付け替えられたりする不正にも耐えうる。物理的な検証と認証のために物理的な証拠（DNA プロファイルや画像を暗号形式のハッシュとするデジタル形式）をブロックチェーンにリンクさせ、読み取り時にリーダーのデジタル署名を付与すれば、より確実にデータを保護できる。また、バリューチェーンにおける森林製品の管理と検証は、しばしば簡単に操作できる改ざん可能な文書管理やデジタルトラッキング手法、CoC 認証に依存しているが、スマートコントラクトにより入力データの検証を行い、消費者が複合製品の履歴をブロックチェーンに問い合わせして証明書が発行されるような、オンライントレーサビリティシステムが実現できる。ブロックチェーン技術を活用した改ざん防止デジタルシステムの開発による、木材を追跡する新しい手段の実現が期待される。

図　木材の表面性状（年輪等）を個体識別してブロックチェーンとリンク

バーコード方式ではラベルの脱落や貼り間違いなどのリスクはあるが、ブロックチェーンと個体識別技術を組み合わせることで、真正性が担保された品質情報を可視化できる。

(参考文献)

・Bitcoin Exchange Guide News Team , Spanish Ministry of Agriculture, Fisheries and Food Develops Blockchain App with ChainWood For Forestry Transparency, September 24, 2018
・川崎貴夫、森づくり・木づかい”の「見える化」促進に向けた IT 化の最前線、美しい森林づくり全国推進会議 , グローバル時代の森林 CSV シンポジウム, 29 Aug 2016

● 製造業への応用

インダストリアル・バリューチェーン・イニシアティブ（IVI）」が中心となり、国内の電機メーカーが連携して、ブロックチェーンを用いた製造情報の共有を実現しようとしている。設備の稼働状況や、生産にかかわる情報を関連する企業間で共有し、生産効率の改善を目指している。

● 電力分野への応用

エネルギー分野におけるブロックチェーンを用いた検討の多くは電力に関連したものであり、①電力使用量の記録・認証、②課金とその支払い（暗号通貨）、③スマートコントラクトによる家庭内電力の自動制御などの多岐にわたっており、今後、信頼性・透明性のある取引を可能にする技術として電力システムに取り込まれていく可能性がある。特に今後予想される家庭内の分散型エネルギー機器（太陽光発電（PV）、電気自動車を含む蓄電池、ヒートポンプなどの電力消費機器など）の増加に伴い、これまで中央管理型の既存の電力システムでは対応が難しいとされた近隣の家庭間での PV などの余剰電力の取引（P2P 取引：中央管理者を通さない直接取引）を可能にできると考えられており、消費者側のメリットだけでなく、電力の需給バランスの調整が必要な供給者側にとってもメリットをもたらす可能性がある。

以下に電力分野でのブロックチェーン技術の応用検討例を示す。

表 2.1　電力分野でのブロックチェーン技術の応用検討例

1	LO3 Energy（米国）	分散型エネルギーアプリケーション TransActive Grid プラットフォームを開発。太陽光で発電した電力を地域で融通する Brooklyn Migrogrid プロジェクトを実施。
2	Power Ledger（豪州）	需要家が投資した太陽光や蓄電池の価値を最大化するための電力取引プラットフォームを開発。リアルタイム決済に伴う需要家同士の P2P 取引をサポート。
3	Grid+（米国）	トランザクティブエネルギー（市場メカニズムを基に系統を運用する仕組みとして米国で提唱されている方法）の実現に向けた課題をブロックチェーン技術で対応。
4	Conjoure（ドイツ）	Innogy(電力会社 RWE の子会社）と東京電力ホールディングスが出資。P2P 取引プラットフーム事業を開始。
5	東京大学・デジタルグリッド（日本）	電力融通決済システムを開発。環境省の浦和美薗プロジェクトで実証。イーサリアムベースのブロックチェーン技術におけるスマートコントラクトと電力ルータによる電力潮流制御も実施。これにより PV 等の余剰電力の P２P 取引において、購入先が決まっている電力のみを流す仕組み。
6	Leap（米国）	デマントレスポンス（DR)のためアグリゲーション方法としてブロックチェーン技術を利用。カリフォルニア州の電力需給調整メカニズムの実証化試験で契約獲得。イーサリアムベースのブロックチェーン技術を利用。
7	東京大学・日本ユニシス・関西電力・三菱 UFJ 銀行（日本）	家庭の PV での余剰電力を、電力の消費者とプロシューマーの希望価格から、各種方式（オークション、ザラバ、ダイナミックプライシング）により取引価格を決定し、ブロックチェーンを用いて模擬的に取引を行い、複数の電力消費者宅へ送電する。関電・巽実験センター内での模擬試験

（出典）:新電力ネット HP, 「ブロックチェーンを使った電力ビジネスとは」https://pps-net.org/column/60520 などを参考に作成

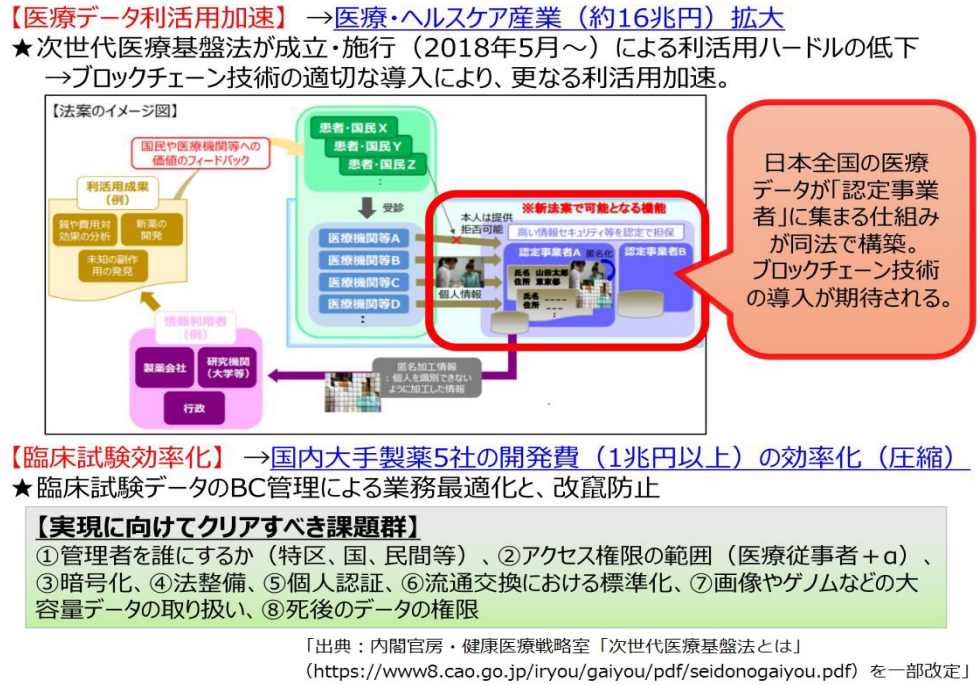
電力取引におけるブロックチェーン技術の活用としては、短期的にはアグリゲータが介在する

DR[10]/VPP[11]のアグリゲーションビジネスのプラットフォーム（計量の記録、認証、支払などを自動化）として活用が中心であり、長期的には電力 P2P 取引のみならず、需要家の分散エネルギー資源を、電力ネットワーク全体を支える能動的システムとして活用するためのプラットフォーム（上記に加え、電流制御の自動化も含む）として活用が期待される。

- **ヘルスケアへの応用**

臨床試験データをブロックチェーンで管理することによって、業務の最適化改ざん防止を実現し、国内大手製薬 5 社の開発費（1 兆円以上）の効率化が図れると試算されている。2018 年 5 月に次世代医療基盤法が成立し、医療データ利活用のハードルが低下し、実現性を帯びてきた。日本全国の医療データが「認定事業者」に集まる仕組みが同法で構築され、ブロックチェーン技術の導入が期待されている。

しかし、実現に向けては①管理者を誰にするか（特区、国、民間等）、②アクセス権限の範囲（医療従事者＋α）、③暗号化、④法整備、⑤個人認証、⑥流通交換における標準化、⑦画像やゲノムなどの大容量データの取り扱い、⑧死後のデータの権限、などの課題がある。



「出典：内閣官房・健康医療戦略室「次世代医療基盤法とは」（https://www8.cao.go.jp/iryou/gaiyou/pdf/seidonogaiyou.pdf）を一部改定」

図 2.4　法案のイメージ

- **金融への応用**

ブロックチェーンは暗号資産を実現するために開発された技術であり、金融への応用は当初から盛んにさまざまな検討が加えられ、多くの実証実験が行われている。中でも、Project Stella は日本銀行と欧州中央銀行による分散型台帳技術に関する共同調査であり、2016 年から 3 つのフェーズで実験が行われた。第 1 フェーズにおいては、RTGS(Real Time Gross Settlement)サービスを対象とし、分散台帳を用いた資金決済システムが、現状のシステムとほぼ同等の水準を満たす可能性が示された。第 2 フェーズにおいては、資金と証券の受け渡しを紐付ける DvP（Delivery

[10] DR：デマンドレスポンス（電力供給のひっ迫度に応じて、需要側がその調整を行う方法）
[11] VPP：バーチャルパワープラント（需要側のエネルギー機器を統合的に活用した仮想的発電所）

versus Payment）について、分散台帳技術を用いて実現できることが示された。第 3 フェーズにおいては、異なる通貨圏をまたぐクロスボーダー支払いを対象として、分散台帳技術によって実現可能であることと、支払い方法を工夫することで、現行の取引の安全性を技術的に改善できることが示された。ただし、これらの検証結果は、分散型台帳技術の金融市場インフラへの応用可能性を示したものであり、実用化にあたっては、法律や規制面などのさらなる検討が必要である。

- **デジタルガバメントへの応用**

産業応用だけではなく、国家のデータ交換基盤に適用することで政府のデジタル変革を推進することも期待される。一例として、北ヨーロッパ、バルト三国の一つエストニアの電子政府である。第二次世界大戦以前フィンランドとエストニアの国民一人当たりの GDP は同じだったが、1992 年には、22,337USD 対 2,832USD と大きく引き離されていた。これを挽回するためにインターネットの技術進歩に合わせて、まず学校をオンライン化、公衆のアクセスポイントを整備しようとしたが、問題はセキュアかつユニークなデジタル・アイデンティティーだった。そこで、End-to-End Encryption ID と mobile Sim card にチップを埋め込み、認証には物理的な何かと知っている何かによる 2 要素認証によるデジタル・アイデンティティーを実現することにした。この結果、パラレル処理による迅速化、透明性と自動化による汚職の削減という劇的な効果が表れ、さらに、電子投票、電子処方箋、電子住民票、データエンバシー[12]へと適用が拡大された。エストニア電子行政サービスの多くは、Guardtime 社(2006 年設立)が開発した、ハッシュを台帳の維持管理にのみ利用するブロックチェーン技術で保護されている。現在では ID カード保有率 98.2%、2,375 行政サービスの電子化、電子投票利用率 31.7%に達し、GDP の 2%に相当する費用削減を実現している。

[12] 電子政府のデータのコピーを国外にバックアップすることで、国内のデータを守るエストニア独自のデータ戦略。

【コラム】Bitcoin、Libra、中央銀行デジタル通貨に見る技術の多目的性

幻滅期に入ったともいわれたブロックチェーン技術だが、2019 年以降、急速にメディアを賑わせ、再び存在感を回復したようにも見える。その最大の立役者の一つは、Facebook を中心とする企業コンソーシアムが打ち出した仮想通貨「Libra」だろう。Libra を巡っては、その構想が発表されて以来、公的機関や米国議会による強い懸念と批判を受けてきた。これまで、実社会に影響を与えるようなユースケースが足りないと批判を受けてきたブロックチェーンだが、今度は潜在的なインパクトが大きすぎて批判を受けるという状況となっている。

一方、Libra と同時期に再び注目を集めるようになったのは、従来フィアット通貨（中央銀行が発行した通貨、法定通貨ともいう）を発行してきた各国中央銀行が、ブロックチェーン技術を利用して発行するデジタル通貨、いわゆる「中央銀行デジタル通貨」である。これまでも中国、英国、スウェーデンなどにおいて真剣に検討されていると報じられてきたが、カンボジアの中央銀行が日本のブロックチェーン企業であるソラミツと組み、2020 年にも中央銀行デジタル通貨を発行するとみられている。

こうした中、元祖デジタル通貨である Bitcoin も、2018 年の暴落とその後の価格低迷から抜け出し、2019 年 7 月には 1 万ドル台を回復した。この Bitcoin に加えた Libra、中央銀行デジタル通貨への注目は、ブロックチェーン技術の「幻滅期」を乗り越えさせるインパクトを持つ可能性がある。

しかし、この 3 つの利用形態には、ブロックチェーンの存在意義をあらためて考えさせられる大きな違いが存在する。Bitcoin はその誕生時から、草の根的なハッカー文化により支えられてきた。確かに普及とともにマイニング事業者が商業化・巨大化し、運営面では寡占化されつつある状況にあるが、開発者コミュニティーは多様性とギーク精神により支えられてきた。また、当初からユーザーの決済情報やプライバシーを、いかにして単独の中央集権的組織から守るかという観点が強く意識されて開発されてきた経緯がある。

これに対して、Libra は Facebook や決済・金融機関がコンソーシアムを組成して開発・運用にあたっている。Facebook は、今や世界中で 25 億人以上が使うコミュニケーションツールとなっており、そこで決済機能を付加することは自然な流れである。ただし、そこで使われる通貨をどこか一国のフィアット通貨に絞ることは、多国籍のユーザーが縦横無尽に利用するプラットフォームとしては大きな制約となる。また各国通貨に対応した場合、両替に手数料と手間がかかることになり、プラットフォーム上での取引を円滑に行うことを阻害する要因となる。こうしたことを考えれば、Facebook が Libra のようにどこの国にも依存しない新しいグローバル通貨を導入しようとすることには、サービス提供者の立場からすれば一定の合理性がある。その一方で、全世界での利用者の決済情報を Libra 財団（およびその構成企業）が管理することとなり、プライバシー上の懸念が浮上することとなった。

こうした企業が提供するデジタル通貨が広範囲に普及すると、フィアット通貨を中心に構築されてきた各国の金融・財政制度に大きな影響を及ぼす可能性が出てくる。現在各国で盛んに調査・研究が行われている中央銀行デジタル通貨には、広範囲に普及する可能性のある民間デジタル通貨への対抗策という側面もあるだろう。しかし、技術の採用範囲にもよるものの、Libra の場合と同様に一般市民の決済情報を国が管理することへのプライバシー上の課題は依然として残ることになる。

このように、Bitcoin、Libra、中央銀行デジタル通貨は、「通貨をデジタル化する」という点では一致しているものの、それらが重視する目的や効果は異なるものである。これらの事例は、同じ技術であってもさまざまなコンテクストや目的で使われうることを示している。デジタル技術の普及によって、制度やガバナンスの境界が融解していくなかで、新たな枠組みをめぐって壮大な綱引きが始まっていると見ることができるだろう。

2.3 科学技術上の効果

ブロックチェーン技術は俯瞰図（3 章）に示した通り、暗号技術、P2P ネットワーク技術、分散合意形成、システム運用管理、分散台帳、スマートコントラクト、プラットフォーム、制度設計・トラストなどの多くの技術群により構成される。このため従来往来のなかったこれらの異分野の研究者がブロックチェーンをハブに集うことにより、次世代ブロックチェーンの研究分野および研究者コミュニティーを醸成することができる。これによりインターネットの黎明期にアカデミアが中心となって活躍した米国 NSFNet や日本の WIDE プロジェクトが果たした役割のように、キーアプリケーションや社会変革に繋がる萌芽的成果（インターネットにおける例：Unix、TCP/IP、DNS、WWW、HTTP など）が生み出されることが期待できる。

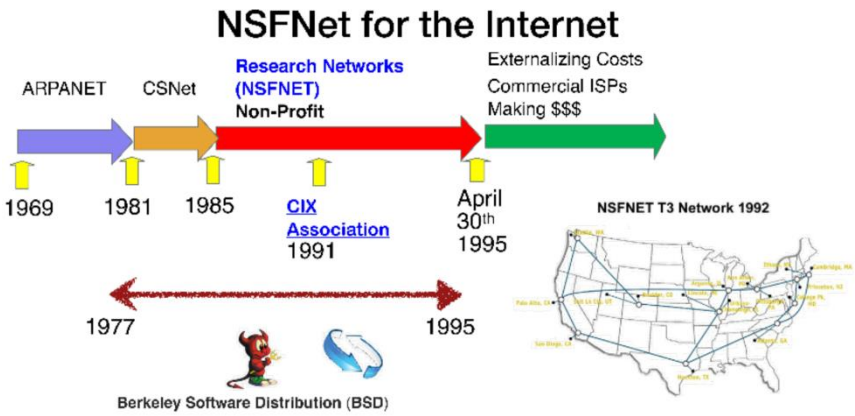


図 2.6　インターネットにおける NSFNet の歴史と役割

また上記に加え、大学・研究機関での直接的な活用も始まっている。ブロックチェーン技術の記録性（耐改ざん性）や ID と組み合わせた認証性を生かして、学位・経歴証明や研究データ不正問題に対応するため、ブロックチェーン技術の試験的な活用も検討されている。

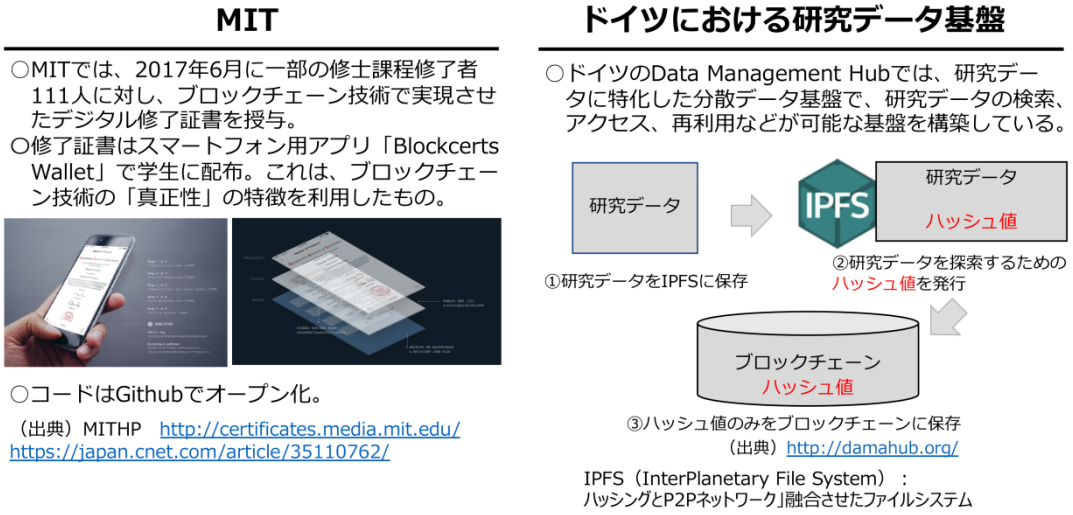


図 2.7 大学・研究機関でのブロックチェーン技術の活用例

【コラム】Bitcoin とブロックチェーン技術の系譜（過去と新技術）

Bitcoin に至る仮想通貨の歴史は失敗の連続であった。その中核技術たるブロックチェーンが The Blockchain として成就するためには失敗を恐れない新たな技術開発への挑戦が必要である。

通貨はものやサービスの交換において、決済のための価値交換媒体として機能する。紙幣や硬貨などの物理的な通貨を使わずに電子的な手段で価値交換が可能であれば、便利になると思われた。しかし、電子的な手段には二重払いの危険性や、匿名性の確保といった困難な問題があった。

1983 年デビッド・ショーンによって、暗号技術を応用したデジタル通貨が提案された。二重払いを防ぐためにブラインド署名という技術が使われていた。しかし、銀行のような中央集権的な組織がすべての取引を管理する必要があったし、利用者の匿名性についても問題があった。その後いくつかのデジタル通貨が提案されたが、どれも広まるまでには至らなかった。

2008 年にサトシ・ナカモトが Bitcoin に関する論文を発表した。いくつかの暗号技術を精緻に組み合わせたブロックチェーン技術によって、二重払いを防ぎながら中央集権的な管理を必要としないというこれまでに無かった特徴を実現した。また、ある程度の匿名性も備えていた。

2009 年には Bitcoin のソフトウエアが公開され、暗号通貨として流通し始めた。いくつかの企業やサイトで Bitcoin による支払いが受け付けられるようになったが、Bitcoin 自体の現実通貨に対する価値の変動が大きく、取引の決済に利用されることは少なく、もっぱら投機の対象となっていた。Bitcoin 以外にも Ethereum や Litecoin、Monacoin などのアルトコインと呼ばれる Bitcoin 以外の暗号通貨が開発され、人々の自由な送金を実現するということが可能になったが、マネーロンダリングや違法な取引、さらに交換所への攻撃による多大な損失など陰の部分も目立ってきた。しかし、技術としてのブロックチェーンは 10 年にわたって Bitcoin などの暗号通貨を下支えし続けている。

Bitcoin には Bitcoin スクリプトと呼ばれる、一種のプログラミング言語が実装されている。この機能を使うことによって、エスクロー取引などのスマートコントラクトが実現できる。

ただし、Bitcoin スクリプトの記述力は限定されていた。そこで、Ethereum ではチューリング完全なプログラミング言語がサポートされ、スマートコントラクトや分散アプリケーションを実装することができるようなった。さらに、Bitcoin ではプルーフ・オブ・ワークと呼ばれる合意形成が行われ、多大の電力を要していたが、Ethereum では電力を大量に消費しないプルーフ・オブ・ステークによる合意形成も可能になる。

今後は、暗号通貨としての利用だけではなく、資産の取引、情報の記録や分散 ID などへの活用が期待され、それに向けて、スケーラビリティー、セキュリティー、プライバシー保護や使いやすさなどの課題解決が望まれる。

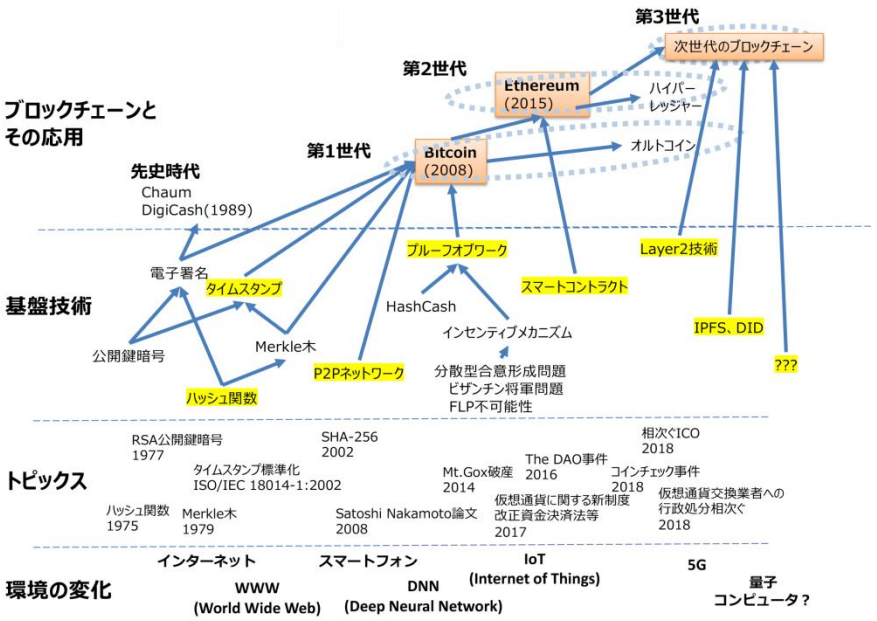


図 ブロックチェーン技術の系譜

3. 具体的な研究開発課題

3.1 問題点と研究開発課題の俯瞰

3.1.1 ブロックチェーン技術の俯瞰

科学技術的課題を述べるのに先だってブロックチェーンに関わる技術全体を俯瞰する（図 3.1）。最下層にあるのは、ブロックチェーンが依拠する技術（暗号技術、P2P ネットワーク、運用管理）であり、計算機科学の分野においてそれぞれ 30 年以上の歴史を持つ。その上に位置するのは、ブロックチェーンをブロックチェーンたらしめる固有技術（分散台帳、分散合意形成、スマートコントラクト）である。また、これらの技術を使って特定の応用を効率的に実現するための実行環境を応用分野との間に定義した。ソフトウエアとしてのプラットフォームと制度設計やトラスト（信用モデル）から成る。

ブロックチェーンの応用は、ブロックチェーン上に記録されるデータの種類で、取引管理と情報共有・情報管理の二つに分けられる。取引管理は、複数の当事者間のやり取りの記録を管理し、情報共有・情報管理は、特に取引に関わらない種々の情報の記録を管理する。情報共有と情報管理の違いは、一般に記録された情報を公開情報として扱うか、個人情報として扱うかの違いであるが、厳密には決められないものもあるため、ここではまとめて扱う。

図 3.1　ブロックチェーン技術の俯瞰

3.1.2 研究開発課題の俯瞰

科学技術的課題をブロックチェーンの応用の面から整理して考える。

A)　取引記録に関わる課題には、まず暗号資産 Bitcoin そのものに関わる課題としてスケーリ

ングが挙げられる。時間あたりの処理可能な取引数が少ないことや取引が確定されるまでの時間が現実のクレジットカード等に比べてはるかに長いことがよく指摘される。信頼できる第三者機関を不要にするために Satoshi Nakamoto が考案した設計思想によるものであるが、頻繁な取引管理に使おうとすると問題になる。ただし、稼働後 10 年の実績を持つ Bitcoin の仕様変更は非常に困難であるため、Bitcoin 以後の登場したオルトコインや Ethereum などが、Bitcoin の仕様の変更や拡張に挑戦している。例えば、時間のかからない合意形成、自由なプログラミング環境などである。さらに、サプライチェーンのような取引管理の場合には、情報が平文で見えてしまうブロックチェーンの仕組みが問題となり、秘匿化やアクセス制御などが必要であると言われている。

B) 情報共有・情報管理は基本的に個人から派生した情報を扱うことが多いため、アイデンティティー管理が特に重要になる。また、IoT や外界に関連したデジタルな情報に関しては、それらが参照・制御する実体との連携が適切であることが求められる。

C) 応用によらない課題として、俯瞰図の一番下の層の基盤技術に関わる課題がブロックチェーンを含めた社会的基盤の安定化、持続性を維持するために必要であると言える。

表 3.1　応用分野による科学技術的課題の整理

応用分野	科学技術的課題
A) 取引管理	
A-1) Bitcoinの課題	スループットと応答性能 51%攻撃耐性
A-2) Bitcoinが諦めた課題	ファイナリティー 合意形成 スマートコントラクト
A-3) 取引管理に共通する課題	情報の秘匿化とアクセス制御
B) 情報共有・情報管理	アイデンティティー管理 プライバシーとアクセス制御 サイバーとリアルの連携 大容量化
C) 応用によらない課題	暗号の危殆化 P2Pネットワークの信頼性 システム運用管理、非機能要件

3.2 ブロックチェーンを構成する技術

3.2.1 ブロックチェーンが依拠する基盤技術

- **暗号技術：危殆化への対応（量子計算機、暗号プロトコル）、準同型暗号**

各ノードから発信されるトランザクションの対改ざん性はハッシュ技術によって担保されており、発信者の正当性は電子署名によって検証される。Bitcoin をはじめとする暗号資産においては、現時点での暗号解読技術・能力に耐えるように、ハッシュ関数、署名方式の選択が行われている（Bitcoin ではハッシュ関数として SHA-256 と RIPEMD160 が使われ、公開鍵暗号としては secp256k1（楕円曲線 DSA(ECDSA)の一種）が使われている）が、将来の暗号解読能力の進歩（量子計算機が特に注目されている）によって、これらの暗号技術が破られる危険性（危殆化）がある。暗号技術の危殆化に対しては、新たなハッシュ関数、署名方式の開発など暗号技術そのものの研究と、すでに動いているブロックチェーンの内容を新方式に安全に移行する仕組みに関

する研究の両方の側面がある。

- **P2P ネットワーク：可用性維持、攻撃耐性、IoT や 5G への対応**

各ノード間の通信（新規ノードにはそれまでの全ブロックチェーン、既存ノードに対しては、新規トランザクションおよび新規ブロックを知らせる）には P2P ネットワークが用いられる。この P2P ネットワークにおける通信経路（各ノードが他のどのノードと通信するかのネットワーク構成）が、上記分散合意形成におけるマイニングノード間の公平性に影響を与える可能性がある。マイニングに参加するノード間で公平な条件になるような P2P ネットワークの構成が課題となる。また、DNS ハッキングのような手法で、P2P ネットワークが歪められて、分散合意形成が機能しなくなる可能性があるため、これらの対策も必要である。また、各種攻撃（51%攻撃、二重払い、自己中採掘、Sivil 攻撃）に対応する技術的な対策に関する研究も重要な研究課題である。

- **システム運用管理：鍵管理、版管理**

システム運用管理の課題としては、まず鍵管理があげられる。Bitcoin のようなパブリック型のブロックチェーンを利用した暗号資産においては、秘密鍵の管理は所有者自身の自己管理にゆだねられているが、取引所を利用するユーザーの鍵管理（有効期限、更新、失効）には何らかの規制が必要である。また、プライベート型ブロックチェーンを用いた他の用途でも鍵管理は厳密に行われねばならない。ブロックチェーンそのもののソフトウエアの改定が行われる場合、新旧版が共存する期間の運用ポリシーやバージョン管理（版管理）も課題としてあげられる。

3.2.2 ブロックチェーンの中核となる固有技術

- **分散台帳：スケーラビリティー、ファイナリティー、匿名性**

暗号資産に用いられるパブリック型においては、ブロックに格納されるトランザクションの真正性を確定することをファイナリティーと呼ぶ。P2P ネットワーク上で異なるマイニングノードが異なる時間関係で受信したトランザクション情報をもとに新規ブロック候補を作成するので、本来同一のブロックチェーンを分散して持つべきなのに、各マイニングノード間で新規ブロックの内容に差異が出ることは避けられない。Bitcoin では、新規ブロック候補に、さらに新たなブロックが 6 個つながったら当該ブロックが確定したものとみなしているが、これは確率的な判断であり、絶対的な確定とは言えない。なお、マイクロペイメント（実店舗や EC サイトにおける少額決済）においては、ブロックに組み込まれる前のトランザクションを、暗号資産の受け取り手がリスクをとって、当該トランザクションだけの真正性確認を行う場合もある。パブリック型の場合、参加するノードの数が増え、発生される総トランザクション数が増えた場合、その処理能力が課題（スケーラビリティー）となる。Bitcoin の場合、ブロックサイズ（1MB）、トランザクションの平均サイズ（300B）、ブロック生成時間（約 10 分）から、7 トランザクション／秒が、その性能限界となる。

一方でクレジット決済などの処理能力は数千トランザクション／秒以上を必要としており、Bitcoin においても、ライトニングネットワーク（レイヤ 2 技術の一種）を用いて、この課題を解決しようとしているが、まだ実験検証の段階である。分散台帳に関する三つ目の課題が、匿名性・プライバシーの問題である。Bitcoin では、ユーザーの ID として公開鍵暗号の公開鍵のハッシュ値を用いることによってユーザーの実名は秘匿している。ただし、トランザクションはすべ

て公開されており、特定のユーザーID の入出金履歴をたどることによって実名が類推される恐れがある。

- **分散合意形成：合意形成アルゴリズム、インセンティブ設計、攻撃耐性**

パブリック型においては、複数のトランザクションをまとめて新たなブロックを作成する際に、どのトランザクションを真正なトランザクションとして認めるかについて、多くのノードによって分散的に行われる合意形成が必要になる。Bitcoin においては、この検証作業への報酬として新規暗号資産を与えることとしている（マイニング）。このマイニングに多大の計算機パワーと電力を消費することが課題となる。他の暗号資産(Ethereum)においてはこの点を解決するために合意形成の決定権を多くの通貨を持つノードにより多く与えるという分散合意形成アルゴリズムが提案されているがその実効性は今後の課題である。プライベート型（コンソーシアム型）においては有限の管理ノードにおいて合意形成を行うのでこの問題はない。

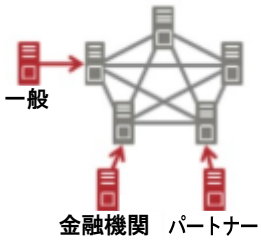
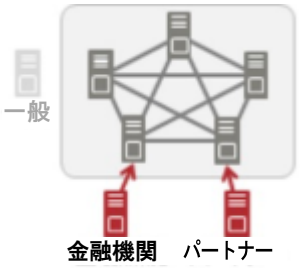
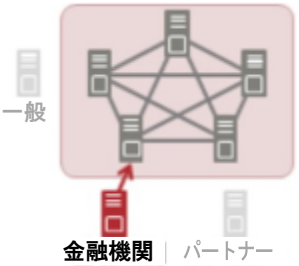
- **スマートコントラクト：プログラミングモデル／言語、正当性検証、相互運用・移植性**

スマートコントラクトに関しては、使用する言語の選択が課題となる。Bitcoin では非チューリング完全型のスクリプトを用いて簡単なスマートコントラクトが可能となるが、ループ処理が行えずその機能には限界がある。Ethereum ではチューリング完全型の EVM が用いられるが、チューリング完全性ゆえにその結果がユーザーの意図したものか否かの検証（正当性検証）に課題がある。（プログラムのバグに過ぎないという意見もあるが）また、その複雑性のため、ハッカーに攻撃される可能性も高くなる（DAO 事件がその例）。もう一つの課題として、スマートコントラクトを実行する外部プログラムを合わせたプログラムモジュールの配置およびプログラムインターフェースの最適化（プログラミングモデル）もあげられる。

3.3 プラットフォームおよびアプリケーション

ブロックチェーンのプラットフォームは、中心となる管理者が存在せずに誰でも参加できるパブリック型（例：Bitcoin や Ethereum）と、管理者がいて参加に許可が必要なプライベート型（例：HyperLedger Fabric）に大別できる。さらに、プライベート型のブロックチェーンを企業間で共有する場合は特にコンソーシアム型と呼ぶ。パブリック型の場合は、ブロックチェーンの仕様変更を行う際に不特定の参加者の賛同が必要であるため一般には仕様変更は難しい。合意できない場合は、過去 Bitcoin で起こったような分裂（フォークという）が発生する。プライベート型の場合は管理者の決定で変更できため、柔軟なシステムの運用が可能である。また、新しい技術の検証などがしやすく、企業が中心として、契約、取引そのほかの実証実験のベースになっていることが多い。

表 3.2 参加モデルによるプラットフォームの分類

参加モデル	パブリック型	コンソーシアム型	プライベート型
構成			
管理者の有無	なし	あり（複数企業）	あり（単独）
参加者	不特定多数 (Permission less)	特定複数 (Permissioned)	組織内 (Permissioned)
合意形成の仕組み	PoW / PoS など （厳格な承認が必要）	特定者間のコンセンサス （厳格な承認は任意）	組織内承認 （厳格な承認は任意）
代表的なプラットフォーム	Bitcoin、Ethereum	Hyperledger Fabric	Ripple

このように、「完全に自律分散的なブロックチェーン」と「中央管理に適したブロックチェーン」とでは、全く異なる性格が表れる。パブリック型は、そもそも中央や仲介機関など既存の枠組みに根本的に相容れないモデルであり、既存の枠組みを破壊しながら発展し普及すると言われている。この結果、将来的には分散化による完全な仲介者の排除が実現されるかもしれない。一方で、プライベート型は、既存の枠組みを大きく変えずに効率化を進めることができるため、企業や銀行等におけるプライベート型の採用が急激に進む可能性もある。

現状、代表的なブロックチェーンのプラットフォームは OSS（オープンソースソフトウエア）である。OSS としての一般的な課題として、ベンダーのサポートや継続性に対する保証がない。したがって、例えば電子政府など継続的な運用を前提とした場合に、性能、信頼性、拡張性、運用性などの非機能要件や相互接続性、継続性、互換性が課題となる。そのため、企業のサポートのないプラットフォームにおいては非機能要件等が不十分であることを前提にいかに上手に利用するかといった Body of Knowledge（知識体系）が必要となる。一方で、利用側の立場からするとプラットフォームやそれを使ったシステムを利用する際のトラスト（信頼を担保する仕組み）をいかに設計・構築するかという課題にも取り組む必要がある。

- プラットフォーム：非機能要件（性能、信頼性、拡張性、運用性など）、相互接続性、継続性、互換性
- 制度設計・トラスト：社会システム／制度設計、トラストフレームワーク

一方で、アプリケーションに関しては、ブロックチェーンが有する分散台帳や取引機能、改ざん困難性や追跡可能性、分散合意形成などを生かすべくさまざまなアプリケーションが PoC（Proof of Concept）として世界中で実施されている。しかし、暗号資産への適用を除いて、多く

はブロックチェーン技術を使わなくても実現できると言われている。その理由は、既存のシステムの一部にブロックチェーンの要素技術を適用したにすぎないからであり、ブロックチェーンの革新性を享受するためには、ビジネスプロセスそのものの再構築が必要であり、現状はまだそのための意義の普及や、方法論が確立していないことによる。アプリケーションモデルに関する研究が必要である。

アプリケーションモデルに関する研究はまだ緒に就いたばかりであるが Gartner は、次のようにブロックチェーンのアプリケーションの進化の可能性を整理している[13]。

- ブロックチェーン・インスパイアド・アプリケーション
  改ざん不可能性や追跡可能性などブロックチェーンの機能・特長を部分的に取り込んで既存のアプリケーションを再構成するものである。目的は、プロセスの効率化や記録の保存で、具体的には、貿易や食品の原材料追跡のアプリケーションなどすでに実用化されたものが含まれる。

- ブロックチェーン・コンプリート・アプリケーション
  上記に加え分散合意形成やトークン化などブロックチェーンのもつ機能・特長をすべて生かしたアプリケーションであり、2.2 社会・経済的効果に示したように、既存の枠組みの創造的破壊や新たなデジタル資産の市場の形成など社会的インパクトのある応用が生み出される。現状、実現されているのは Bitcoin などの暗号資産のみといえる。

- 拡張されたブロックチェーンアプリケーション
  AI や IoT などの技術との統合により新たな付加価値がブロックチェーンネットワークにもたらされる。IoT におけるモノ（Things）がセンシングデバイスから AI を搭載するなどスマート化することで、ブロックチェーンネットワークにおいて、人やサービスシステムと対等に取引を行うようになる。まったく新しいビジネスシーンが開ける。

[13] David Furlonger and Christophe Uzureau, The Real Business of Blockchain: How Leaders Can Create Value in a New Digital Age, (Harvard Business Review, 2019).

4. 研究開発の推進方法および時間軸

本提言書では、研究開発による基礎基盤の確立とわが国の国家的社会基盤への適用を車の両輪とした推進すること、および、ブロックチェーンの活用と影響を議論する場を設置することを提案する。

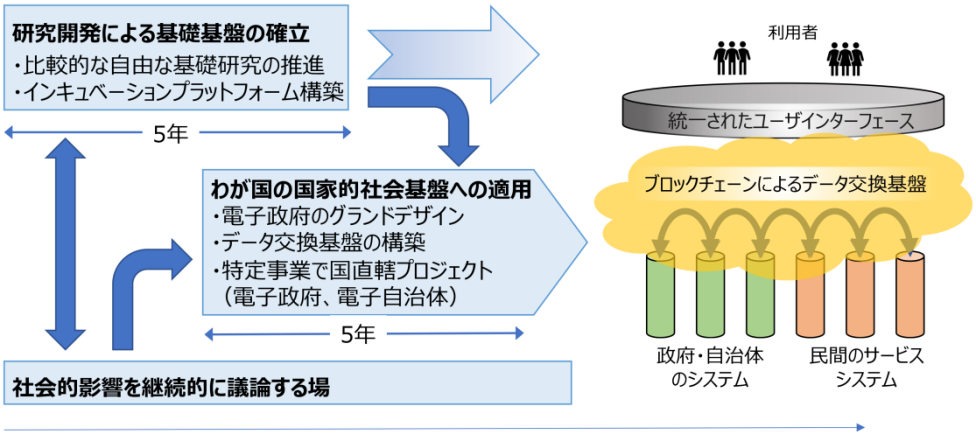


図 4.1　研究開発の推進方法

- 研究開発による基礎基盤の確立
  自由な発想に基づく基礎研究を推進すると同時に、研究者が集うインキュベーションプラットフォームを構築することで、多種多様な研究成果の創出と新たなコミュニティーの育成を行う。
- わが国の国家的社会基盤への適用
  国家的社会基盤はわが国が目指す社会像 Society 5.0 の具現化の一環として、安全で透明性の高い効率的な次世代の電子政府の実現の礎である。次世代の電子政府のグランドデザインを策定し、その下で、ブロックチェーンによるデータ交換基盤を構築する。政府・自治体と民間サービスとを連携させたアプリケーションを開発する。
- ブロックチェーンの活用と影響を議論する場の設置
  ブロックチェーン技術の本質的な洞察を議論する場を設置し継続的に議論することで、技術の真価を引き出しつつ想定されるリスクに備えたグランドデザインにつなげる。

4.1 研究開発による基礎基盤の確立

自由な発想に基づく基礎研究を推進すると同時に、研究者が集うインキュベーションプラットフォームを構築することで、多種多様な研究成果の創出と新たなコミュニティーの育成を行う。これにより、現状エンジニアリングが先行し、基礎・基盤的な研究開発が追い付いておらず、研究者コミュニティーが分散している状況を打開する。

インキュベーションプラットフォームとは、従来往来のなかった暗号技術・P2P ネットワーク・分散合意形成・制度設計等の異分野の研究者がブロックチェーンをキーワードにして集って切磋琢磨する研究開発ハブである。次世代ブロックチェーン技術の研究分野および研究者コミュニ

ティーを醸成する。その結果、かつて、インターネットの黎明期にアカデミアが中心となって活躍した米国 NSFNet や日本の WIDE プロジェクトが果たした役割、例えば、キーアプリケーションや社会変革に繋がる萌芽的成果が生み出されることを期待する[14]。

すでに機能している研究開発ハブ拠点としては、2016 年に MIT が中心となって設立した Bsafe.network、2018 年に米国 Ripple 社が大学に呼びかけて設立した University Blockchain Research Initiative: UBRI）などがある。以下に述べるわが国の国家的社会基盤に関する応用開発を考慮すると、これらとは別の枠組み、例えば、学術情報ネットワーク（SINET）上に構築することも一つの候補ではあるが、参加できる機関が大学や研究機関に限定されるため、産業技術総合研究所人工知能研究センター（AIRC）の計算資源のような産学共同の研究開発基盤をブロックチェーン専用に構築するのが望ましい。そうすることで社会基盤に要求されるセキュリティー要件に対する安全性評価の研究も行うことができる。実際には、研究成果の蓄積と再利用が促進できるように競争的資金も準備して研究開発のファンディングも必要と考える。

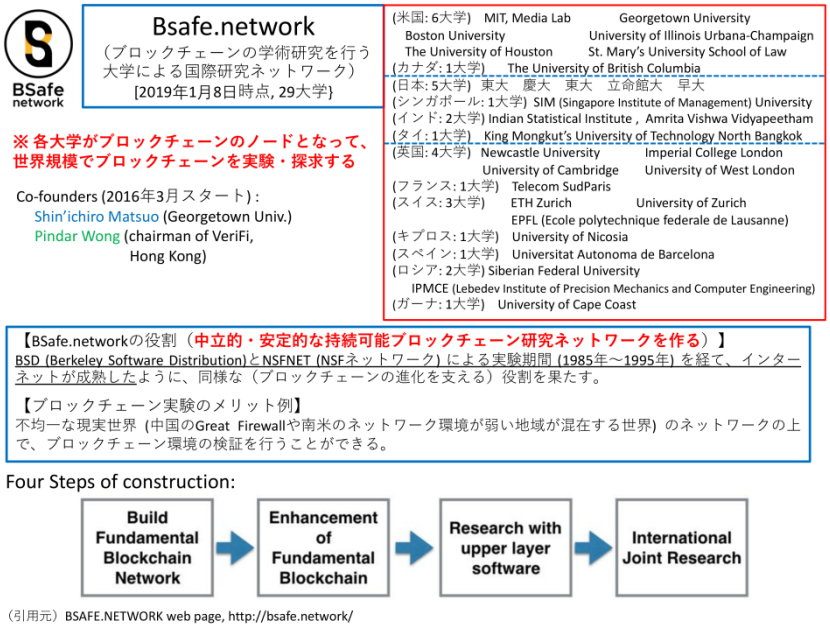


図 4.2 Bsafe.network

4.2 わが国の国家的社会基盤への適用

わが国では、2019 年に行政の手続きをワンストップ化する通称「デジタル手続き法案」が成立した。また、安倍首相は、信頼ある自由なデータ流通として DFFT（Data Free Flow with Trust）構想について、ダボス会議（2019 年 1 月 23 日）や G20 大阪サミット（2019 年 6 月 29 日）で世界に提唱した。どちらも今後は、生産性向上やイノベーションにおいて、デジタルデータの活用と流通がキーであり、改ざん、プライバシー、データ保護などのセキュリティーに関わる課題の対処が必要であると提言した。ブロックチェーン技術はこれらの課題に対するソリューションを提供することが可能である。

[14] ここで直接、間接的に生み出された成果として Unix, TCP/IP, DNS, WWW, HTTP などが挙げられる。

● 電子政府のグランドデザイン

電子政府への適用については第1回のワークショップにて政府CIO補佐官はじめ電子政府に関わりの深い有識者にて議論し、数十年にわたる戦略的な取り組みが必要であることを再認識した。一方で、まず現実の課題、例えばデータの品質の問題への対処が喫緊であることも指摘された。政府はデジタル・ガバメント実行計画にてオールデジタル化を進めている。2019 年 7 月には内閣官房 IT 戦略室にてデジタルガバメントのグランドデザインの検討も始まった。現状、まだブロックチェーン技術の適用は入っていないが、将来に向けて、安全で効率的なデジタルガバメントに向けた検討が進行していることは意義深い。

先行するエストニアにおいても長期の取組が必要だったように、社会基盤の再構築には長い時間がかかる。そのため、実現には行政の強い意志が最も重要であると言われている通りである。日本においても既にデジタルガバメントの議論が始まっていることから、その議論の俎上に載せることが必要である。

● データ交換基盤の構築

電子政府は止まることが許されないミッションクリティカルシステムであることを考えると、既存のブロックチェーンのプラットフォームをそのままデータ交換基盤として利用することは考えられない。一方で、従来のように特定のシステム構築業者に個別発注することはコスト面から望ましくない。今後何十年も利用し続けるためには、最初からそれを意識した設計思想に基づき、かつ当事者能力のあるプラットフォームを新たに構築する必要がある。と言っても一からから作る必要はなく、既存のプラットフォームは OSS なのでそれをカスタマイズすることで開発可能である。これを仮に、National Data Exchange Infrastructure と呼ぶとするとその要件は以下の通りである。

○ アプリケーションレベルの継続性の保証
○ テストベッドと実運用が自由にできる開発環境
（インキュベーションプラットフォームの活用）
○ 基盤活用の知識体系の構築と使いこなせる人材の計画的育成

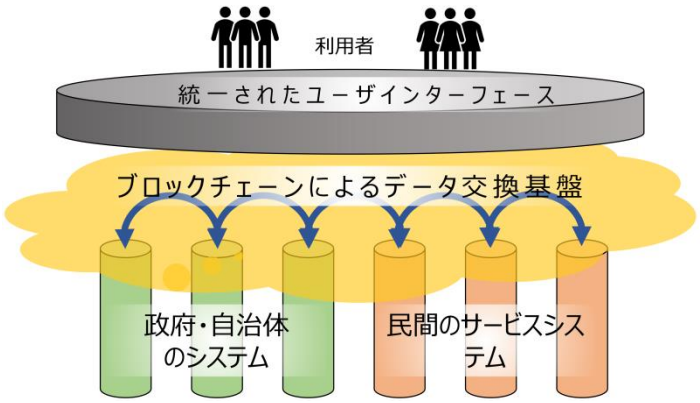


図 4.3 ブロックチェーンで実現するデータ交換基盤
さまざまなシステムのデータを交換するための基盤上で、政府/自治体のシステムと民間のサービスがスムーズに連携する。また、利用者には、ワンストップ、ワンスオンリーを統一されたユーザーインターフェースを提供する。

● 特定事業で国直轄プロジェクト（電子政府、電子自治体）

ブロックチェーンの応用可能性のある分野として、創造的破壊（暗号資産等）、デジタル資産の市場（排出権取引等）、プロセスの効率化（貿易等）、記録の保存（登記等）を既に挙げている。

電子政府で利用する場合でも、基本的にブロックチェーンの特長を生かしたものでなければ意味がない。その上で国としての公共性を考えると、各種台帳関係、申告・申請関係等での利用が考えられる。具体的には、各種台帳関係としては、登記簿、農地台帳などの台帳管理や、個人認証、法人認証などのアイデンティティー管理がある。申告・申請関係では、税申告、施設予約、廃止鍵管理（長期のデータ保存は想定しないもの）、公的記録の管理・保全・時刻証明（公文書・情報提供記録として）、貿易事務、電子申請、テロ対策、情報開示（多数の参加があるもの）、その他として、マイナンバー制度の情報提供記録、オープンデータの公開、公示送達が想定される。

表 4.1　電子政府における適用候補

各種台帳	●登記簿・農地台帳・固定資産税台帳 ●個人認証、法人認証
申告、申請	●税申告、施設予約、廃止鍵管理 ●公的記録の管理・保全・時刻証明（公文書・情報提供記録） ●貿易事務、電子申請、テロ対策
情報開示	●マイナンバー制度の情報提供記録 ●オープンデータの公開、公示送達

最近の動向では、日銀が電子マネーの研究を欧州の中央銀行と共同で行うことが発表された[15]。電子マネーへの動きは加速すると思われるが、その動きと並行して、政府として直接関係する納税の部分において、その記録台帳としてブロックチェーンの活用を念頭においてどう対応するか、検討していくべきである。

ブロックチェーン技術を電子政府の中で採用するに際し、制度設計にあたっては、Bitcoin ブロックチェーンで標準的に使われていない暗号が政府推奨暗号になっていない、法規制との整合性を取る必要がある、技術者の単価が高いにもかかわらず、スキルレベルがまちまちである、のような課題が指摘されている。また、制度運営にあたっては、入れるべきデータがない、もしくはあっても品質が悪い、現状のウォレットの操作や鍵管理の仕組みが複雑であり、実際の利用者（住民や府省・公共団体等の担当者）が使う際には適度なインターフェースにしないと使いきれない、アクセス権限管理が難しく、プライバシー保護・機密保持が難しい、スマートコントラクトの機能が限定的で、改修が難しく、制度変更への対応が難しい、のような課題が指摘されている。

国の台帳は長期に、しかも、多くの人が使うものであるので、まずは特定のパイロットプロジェクトを定め、小規模かつ既存のシステムへの影響が少ないものから順次、新しいシステムを構築して問題点の洗い出し、実規模での適用につなげていくことが望ましい。

4.3 ブロックチェーンの活用と影響を議論する場の設定

ブロックチェーン技術の潜在的な革新性を考慮すると、人工知能の人間や社会的影響に関する議論と同様の議論の場が必要である。ブロックチェーン技術の本質的な洞察（真価の発現とリスクの回避など）を議論する場をもうけて、定期的にワークショップやセミナーを開催し、質の高い報告書や提言書を発行することが望ましい。ここで参考となるのは、ブロックチェーンによるイノベー

[15] 日銀や欧州中央銀行（ECB）など 6 つの中央銀行は 21 日、中銀によるデジタル通貨の発行を視野に新しい組織をつくると発表した。2020/01/22 付け日経新聞

ションの加速とEU内のブロックチェーンエコシステムの開発を目的に設立されたEU Blockchain Observatory and Forum の活動である。100名規模の有識者によるフォーラム活動を精力的に実施し、”Blockchain Innovation in Europe”、”Blockchain and the GDPR”、”Blockchain for Government and Public Services”等の質の高いレポートを発行している[16]。

具体的な会議の母体は基本的に以下に示すような既存の組織において定常的に実施する形でよい。

- 電子政府に関する議論：内閣府IT戦略室など
- 金融分野における議論：金融庁Fintech室、日本銀行金融研究所など
- イノベーションに関する議論：経済産業省RIETIなど

情報交換・議論の機会を設けたり、社会からの意見を聞く機会として、合同でセミナーやワークショップを開催することも重要である。また、情報システムにおける議論に関しては、EU Blockchain Observatory and Forumやコンサルファーム（Gartnerや Deloitte トーマツ、など）と意見交換する必要がある。

また、情報システムにおける議論に関しては、EU Blockchain Observatory and Forumやコンサルファーム（Gartnerや Deloitte トーマツ、など）と意見交換する必要がある。

[16] EU Blockchain Observatory and Forum An Initiative of the European Commision, https://www.eublockchainforum.eu/.
発行されたレポート:Blockchain innovation in Europe,Blockchain and the GDPR,Blockchain for Government and Public Services,Scalability, interoperability and sustainability of blockchains(2018),Blockchain and Digital Identity (2019)

付録１．検討の経緯

国立研究開発法人科学技術振興機構（JST）研究開発戦略センター（CRDS）では、2018 年度の戦略スコープ策定委員会において、戦略プロポーザルを作成すべきテーマの候補として、本テーマを選定し、検討チームを発足させた。本検討チームは 2018 年 5 月から活動を開始し、俯瞰活動含め約 2 年間にわたって検討を進めてきた。その間、有識者インタビューやワークショップも開催し、本テーマの研究開発状況の把握や研究課題・方向性の議論を深めてきた。

付録１.１ 有識者インタビュー

本提言書の作成にあたり、研究内容や推進体制、研究シーズ等について意見をうかがうため、関連する研究領域に高い専門性を有する有識者への個別インタビューを実施した。2018 年 6 月～2019 年 10 月に実施し、以下の方々からお話を聞いた（50 音順、敬称略、所属・役職はインタビュー実施当時）。

付表 1.1　インタビューした有識者

氏名	所属・役職
赤羽　喜治	株式会社 NTT データ　金融事業推進部　部長
岩下　直行	京都大学 公共政策大学院　教授
岡田　仁志	国立情報学研究所 情報社会相関研究系　准教授
面　和成	筑波大学 システム情報系情報工学域　准教授
岸上　順一	室蘭工業大学大学院 工学研究科　教授
楠　正憲	Japan Digital Design 株式会社　CTO
Chris DAI	株式会社 LONGHASH　CEO
越塚　登	東京大学 情報学環 副学環長・教授
小西　弘一	日本電気株式会社　セキュリティ研究所　部長
斉藤　賢爾	慶應義塾大学 SFC 研究所　上席所員
坂井　豊貴	應義義塾大学 経済学部　教授
佐古　和恵	日本電気株式会社 セキュリティ研究所　特別技術主幹
佐藤　一郎	国立情報学研究所 情報社会相関研究系　所長補佐
座間　敏如	内閣官房　政府 CIO 上席補佐官
首藤　一幸	東京工業大学 情報理工学院　准教授
庄司　昌彦	武蔵大学 社会学部メディア社会学科　教授
鈴木　雅喜	ガートナー ジャパン株式会社 リサーチ＆アドバイザリー部門 バイスプレジデント
鈴木　茂哉	慶應義塾大学大学院 政策・メディア研究科　特任准教授
高木　聡一郎	東京大学大学院 情報学環　准教授/国際大学 GLOCOM　主幹研究員
田中　圭介	東京工業大学 情報理工学院数理・計算科学系　教授
田中　謙司	東京大学 技術経営戦略学専攻　特任准教授
徳田　英幸	情報通信研究機構　理事長
橋田　浩一	東京大学大学院 情報理工学系研究科 附属ソーシャル ICT 研究センター　教授

平本　健二	内閣官房 政府 CIO　上席補佐官
藤村　滋	日本電信電話株式会社 NTT サービスエボリューション研究所　主任研究員
松浦　幹太	東京大学 生産技術研究所　教授
松尾　真一郎	Georgetown University Department of Computer Science Research Professor
水島　洋	国立保健医療科学院 研究情報支援研究センター　センター長
宮前　剛	株式会社富士通研究所 ソフトウエア研究所　シニアリサーチャー
森川　博之	東京大学大学院 工学系研究科　教授
矢野　誠	経済産業研究所　所長
山崎　重一郎	近畿大学 産業理工学部情報学科　教授
山下　克司	日本アイ・ビー・エム株式会社 グローバル・テクノロジー・サービス事業本部　技術理事
山田　仁志夫	株式会社日立製作所 システムイノベーションセンター　主任研究員
吉濱　佐知子	日本アイ・ビー・エム株式会社 東京基礎研究所 FSS&ブロックチェーンソリューション担当部長
渡辺　太郎	株式会社デジタルガレージ　Chief Technology Officer

付録１.２ 科学技術未来戦略ワークショップ

本提言書の作成にあたり、下記の通り、科学技術未来戦略ワークショップを開催した。その詳細についてはワークショップ報告書（2020 年発行予定）を参照されたい。

（１）ブロックチェーンによる社会基盤の構築に関する議論

概要

日時：2019 年 8 月 30 日（金）13:30～18:00
場所：JST 東京本部別館 4 階 F 会議室

招聘有識者（50 音順、敬称略、所属・役職は開催日時当時）

（発表者）

岡田　仁志	(国立情報学研究所 情報社会相関研究系　准教授)
岸上　順一	(室蘭工業大学大学院工学研究科　教授)
楠　正憲	(Japan Digital Design 株式会社 CTO)
高木　聡一郎	(東京大学大学院 情報学環　准教授/GLOCOM)
平本　健二	(内閣官房　政府 CIO 上席補佐官)

（コメンテーター）

首藤　一幸	(東京工業大学 情報理工学院　准教授)
西村　秀和	(CRDS　特任フェロー/慶應義塾大学)

プログラム

13:30～13:35	開催挨拶 木村康則（CRDS）
13:35～13:50	開催趣旨説明・参加者紹介　茂木強（CRDS）

● 招聘者からの発表（30 分/人＝発表 15 分＋質疑）

13:50～14:35 基調講演 高木聡一郎（東大/GLOCOM）
14:35～15:15 マイナンバー、ID 基盤とブロックチェーン 楠正憲（JDD）
15:25～15:55 ブロックチェーン経済圏 岡田仁志（NII）
15:55～16:25 研究開発・生涯教育とブロックチェーン 岸上順一（室蘭工大）
16:25～16:55 データ戦略とブロックチェーン 平本健二（内閣官房）
16:55～17:55 全体討議 高木聡一郎（東大/GLOCOM）・茂木強（CRDS）
17:55～18:00 閉会挨拶 木村康則（CRDS）

（２）次世代ブロックチェーン技術に向けた基礎・基盤的な研究開発に関する議論

概要

日時：2019 年 9 月 12 日（木）13:00～18:00
場所：JST 東京本部別館 2 階セミナー室

招聘有識者（50 音順、敬称略、所属・役職は開催日時当時）

（発表者）

岸上　順一 (室蘭工業大学　大学院　教授)
楠　正憲 (Japan Digital Design 株式会社　CTO)
佐古　和恵 (日本電気株式会社　技術主幹)
首藤　一幸 (東京工業大学 情報理工学院　准教授)
高木 聡一郎 (東京大学大学院 情報学環　准教授/GLOCOM)
藤村　滋 (日本電信電話株式会社　NTT サービスエボリューション研究所 主任研究員)
松浦　幹太 (東京大学 生産技術研究所　教授)
吉濱　佐知子 (日本アイ・ビー・エム株式会社　東京基礎研究所　FSS&Blockchain 部長)

プログラム

13:00～13:10 開催挨拶 木村康則（CRDS）
13:10～13:30 開催趣旨説明・参加者紹介 茂木強（CRDS）
13:30～13:50 ワークショップ（第 1 回）の報告 高木聡一郎（東大）

● 招聘者からの発表（30 分/人＝発表 20 分＋質疑）

13:50～14:20 ブロックチェーンの課題（暗号鍵管理） 楠正憲（JDD）
14:20～14:50 ブロックチェーンの課題（トラスト、デジタル ID） 佐古和恵（NEC）
14:50～15:20 ブロックチェーンの課題（暗号技術） 松浦幹太（東京大）
15:30～16:00 ブロックチェーンの課題（P2P ネットワーク） 首藤一幸（東工大）
16:00～16:30 ブロックチェーンの課題（スマートコントラクト） 藤村滋（NTT）
16:30～17:00 ブロックチェーンの課題（分散台帳） 吉濱佐知子（日本 IBM）
17:00～17:55 全体討議 岸上順一（室蘭工大）・茂木強（CRDS）
17:55～18:00 閉会挨拶

付録１.３ 俯瞰活動

本提言書に先だって、国内外の社会や科学技術イノベーションの動向およびそれらに関する政策動向を把握・俯瞰・分析し、その結果を研究開発の俯瞰報告書「システム・情報科学技術分野（2019 年）」CRDS-FY2018-FR-02 にまとめた。詳細については当該報告書を参照されたい。

付録２ 国内外の状況

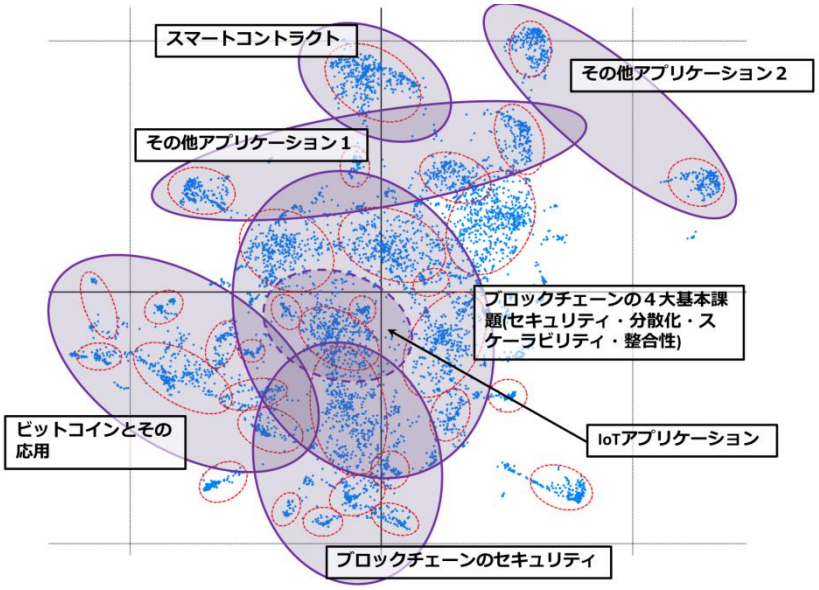
付録２.１ 論文・特許で見た国内外の状況

（１）ブロックチェーン関連論文分析

ブロックチェーン技術分野の文献として、2001 年以降に発行された種別が Article、会議録、レター、研究ノートのうち、関連するキーワード17でタイトル、アブストラクト、キーワードでヒットするものとした。なお、分野として Computer Science に含まれるものに限定し、データベースとしてエルゼビア社の Scopus を用いた。

- **俯瞰解析**

ブロックチェーンに関する論文について、文書の類似度に応じた俯瞰解析を行った結果、右図に示すように 7 領域に分かれた。基本的な概念が図の中央に位置されるが、今回は、ブロックチェーンの基本課題である、暗号技術、分散システム、スケーラビリティー、合意形成に関する論文が位置した。スマートコントラクト、システムセキュリティー（鍵管理、攻撃耐性）、Bitcoin とその応用、その他アプリケーション（医療、スマートシティー、サプライチェーン）が外側に配置された。なお、IoT アプリケーションはひとかたまりとなって中心に位置し、その関心度と高さが伺える。

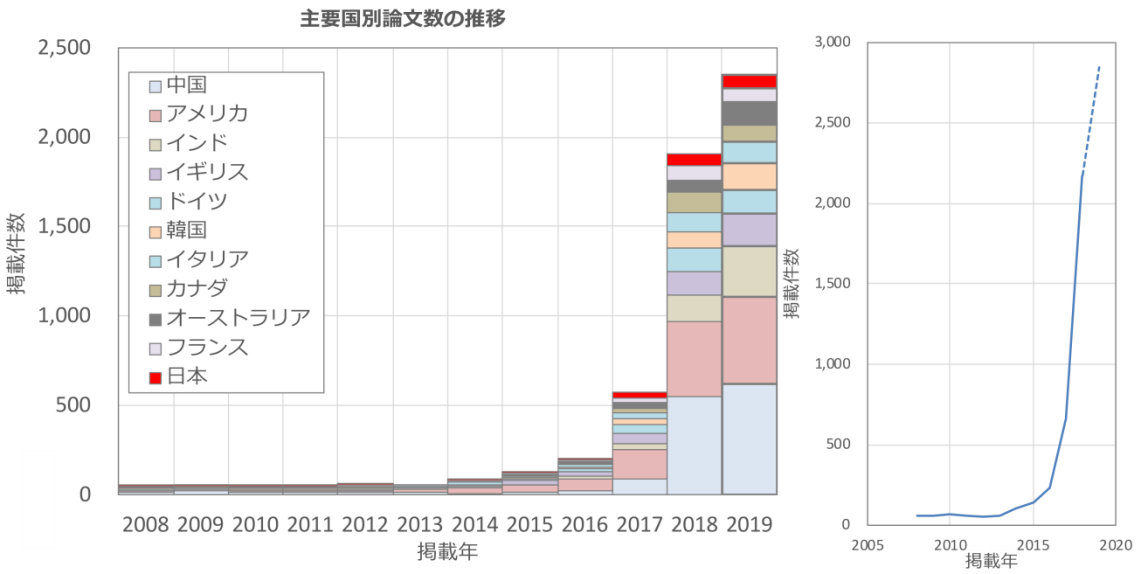


付図 2.1　論文の俯瞰解析

- **主要国別論文数**

ブロックチェーン関連論文の年次推移を下図に示す。2005 年以降現れ、2017 年を境に急増している。特に中国、アメリカの論文が多いが、第 3 位にインドが入っているのは新しい知見である。研究機関別に見ると上位にはアメリカの企業大学が並ぶ一方、中国に研究機関もランクインする。

[17] 検索キーワード（blockchain* OR "block chain"* or "distributed ledger"* OR "smart contract"* OR bitcoin* OR "digital cash"* OR "crypto currency"* OR criptocurrenc* OR "hash chain"* OR hashchain* OR "virtual currency"* OR virtualcurrenc* OR Ethereum* OR hyperledger* OR "hyper ledger"* OR "lightning network"* OR corda）



付図 2.2　ブロックチェーン関連論文数の推移

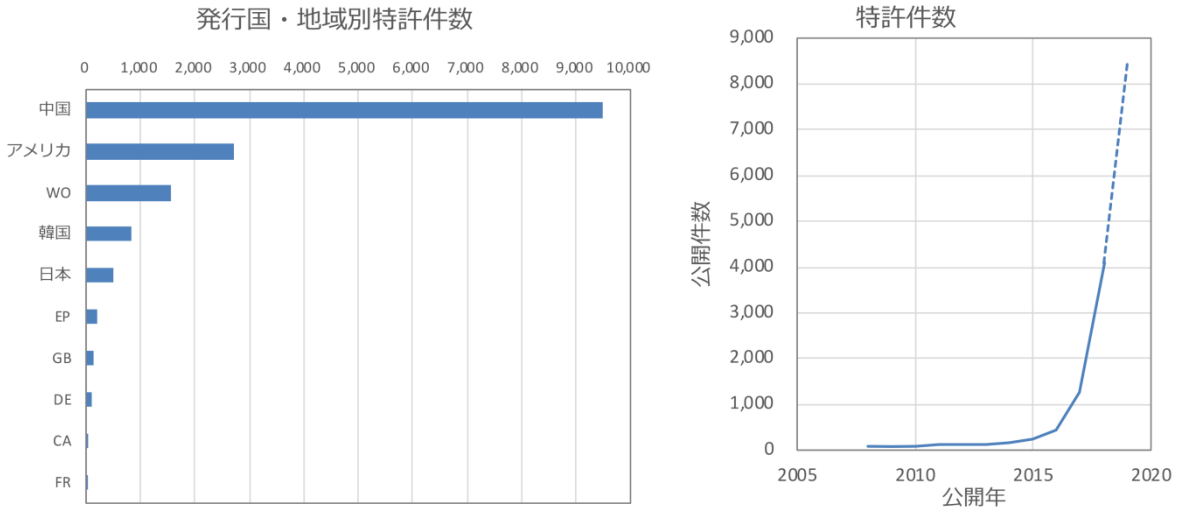
（2）ブロックチェーン関連特許分析

ブロックチェーン技術分野の特許として、発行国・機関が US、EP、WO、CN、JP、KR、DE、FR、GB、CA で、2001 年以降に発行された公開公報のうち、論文検索と同様のキーワードで発明の名称、要約、請求項でヒットするものとした。なお、データベースとして LexisNexis 社の TotalPatentOne を用いた。

- **主要国別論文数**

特許件数は、論文同様に 2016 年を境に急激に増加している。なお、その増加割合は論文を超えている。発行国別集計では、特許では中国が圧倒的である。論文では中国と米国の 2 強であったのと対照的である。

国別の公開件数推移では、ほぼ一貫して中国が首位で、2016 年以降の上昇率も中国が最大である。2 位 US、3 位 WO も増加しているが、4 位 KR の上昇が著しい。



付図 2.3　ブロックチェーン関連特許の分析

- **主要出願人別分析**

ブロックチェーン関連の特許を出願した機関ランキングを求めた。上位はほぼ中国の企業となったが、例外として米国や韓国の企業がランクインした。

首位はアリババ、2 位は IBM、3 位はテンセント、4 位に韓国ビズモードライン、5 位に中国の Hangzhou FUZAMEI Technology となった。これら上位の領域を合わせて示す。

付表 2.1 主要出願機関

No.	研究機関	件数
1	ALIBABA GROUP HOLDING LTD	662
2	IBM	263
3	TENCENT	251
4	BIZMODELINE CO LTD	223
5	HANGZHOU FUZAMEI TECH CO LTD	214
6	CHINA UNICOM	194
7	PING AN TECH SHENZHEN CO LTD	186
8	BAIDU ONLINE NETWORK TECHNOLOGY	143
9	SHENZHEN LAUNCH TECH CO LTD	142
10	NCHAIN HOLDINGS LIMITED	137
11	ONECONNECT	136
12	ZHONGAN INFORMATION TECH SERVICE CO LTD	127
13	WALMART	117
14	BANK OF AMERICA CORPORATION	97
15	SHENZHEN QIANHAI WEBANK CO LTD	96

付録２.２ わが国における活動状況

民間の調査会社 Gartner の発行した報告書 “Blockchain Trials Across Industries Show a Market in Transition”, 20 March 2018 では、全世界でブロックチェーン関するコンサルティングやコンセプト実証、実装、実ビジネスなどのフェーズにおいて、198 の事例について、製造や流通、輸送、通信、証券、金融などの産業別に調査が行われた。ブロックチェーンの提供するスマートコントラクト、取引管理、ID 管理・トークン、情報・資産管理という機能についてマッピングをしている。この結果からは下記の事項が観察される。

- 業種を問わず、情報・資産管理に用いようとしている
- 銀行はほぼすべての機能を試そうとしている
- ID 管理、トークンとしての利用は進んでいない
- スマートコントラクトはまだ少ない

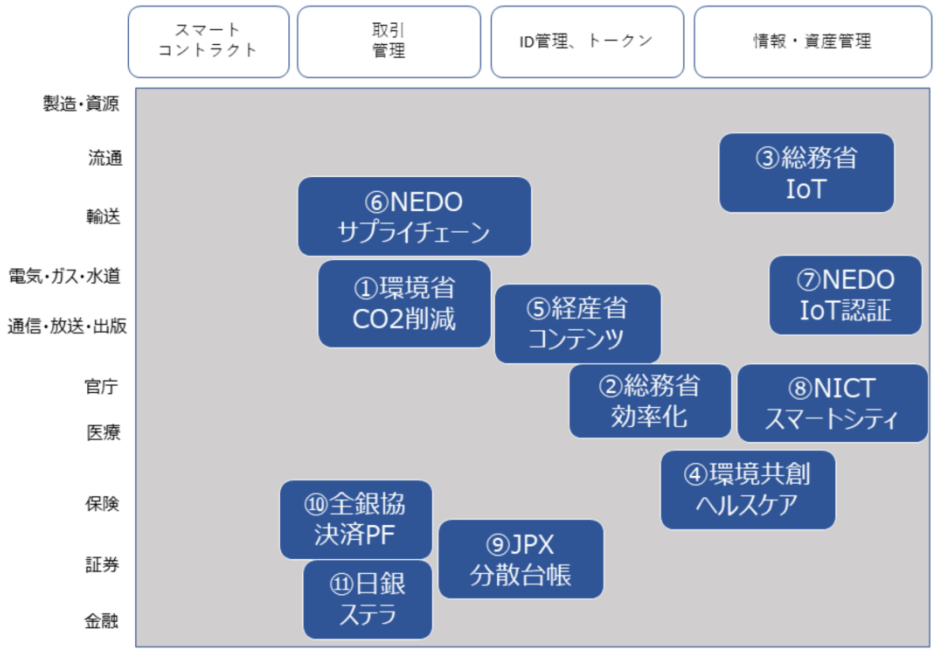
本節では、わが国において実施された実証実験のうち、主に官庁系の取り組みを下表に示す。

付表 2　わが国における実証実験（官庁系の取り組み）

	主体	タイトル	目的
1	環境省	ブロックチェーン技術を活用した再エネ CO2 削減価値創出モデル事業	・自家消費される再エネの CO2 削減にかかる環境価値を創出し、当該価値を低コストかつ自由に取引できるシステムをブロックチェーン技術を用いて構築し、実証。 ･低コストに再エネの CO2 削減価値をデータ化し、売り手と買い手が指定した条件に従い自動的に取引・精算
2	総務省	ブロックチェーン利活用推進事業	官民の幅広い分野においてブロックチェーン技術の活用について実証・検証を行い、運用面、ルール面及び技術面の課題を抽出する。
3	総務省	ブロックチェーン技術を利用した中食・外食の食材トレーサビリティーの社会実装	産地情報を川上・川中・川下に至る垂直的なサプライチェーン全体で、取引における情報伝達の正確性を相互監視し、消費者が信頼できる原料原産地情報を元に食材を選択できるトレーサビリティシステムを構築
4	一般社団法人環境共創イニシアチブ	ブロックチェーン活用によるヘルスケアデータ共有モデル構築事業	企業･自治体･健診機関等が分散管理する個人のライフログデータを、個人の要請に基づき PDS（Personal Data Store）に集約し、データ流通基盤を構築。円滑・セキュアなデータ収集・利活用を可能とし、BtoG、BtoB、BtoC ビジネスモデル構築の実現を支援する。
5	経済産業省（経産省）	ブロックチェーン技術を活用したコンテンツビジネスに関する検討会	ブロックチェーン技術に着目し、これを活用したサービス・アプリケーションに必要となる基礎的な機能や著作権法との関係を議論。
6	新エネルギー・産業技術総合開発研究機構（NEDO）	輸出手続き向けにブロックチェーンを活用した情報共有基盤	貨物や手続きに関する情報を関連事業者間で安全かつ正確にやりとりできる情報システムを構築し、国内の特定の港湾で 2018 年度末まで実証を行い、事業者の生産性向上や輸出リードタイム短縮への効果などを検証。

7	新エネルギー・産業技術総合開発研究機構（NEDO）	IoT 認証プラットフォームの処理高速化と省電力化に関する研究開発	ブロックチェーンを使った IoT 認証セキュリティープラットフォームで、IoT デバイスのセキュアな相互接続性を実現
8	情報通信研究機構（NICT）	ブロックチェーン・ビッグデータ・クラウド及び IoT を使用したハイパーコネクテッドスマートシティを実現するマルチレイヤセキュリティ技術	セキュリティー、IoT、クラウド及びビッグデータを組み合わせた先端技術の研究開発及び実証を、実データに基づいて実践的に行う。
9	日本取引所グループ	業界連携型 DLT 実証実験	ブロックチェーン/分散型台帳技術の金融インフラへの適用可能性に関する実証実験や調査・検討
１０	全国銀行協会（全銀協）	ブロックチェーン技術を活用した新銀行間決済プラットフォーム実証実験	振り込みの際に、銀行間で行われる資金清算業務を効率化できるかを検証し、銀行の負担軽減につなげる
１１	日本銀行・欧州中央銀行	Project Stella 日本銀行・欧州中央銀行による分散型台帳技術に関する共同調査	金融市場インフラへの DLT の応用可能性を調査するための共同調査

これらの取り組みを先の前述の Gartner のブロックチェーン適用の枠組みにマッピングしてみると、付図 2.4 の様になる。



付図 2.4　わが国における実証実験（官庁系の取り組み）

このマッピングからは、情報・資産管理への適用が比較的多いが、製造業、ヘルスケアなどへの取り組みが少ないことが分かる。主に民間で行われていると思われる。しかし、スマートコントラクトはまだ少なく、今後の展開が期待される。

付録３ 専門用語

可用性：必要なときにいつでも安全なアクセスができることを指す情報システムの非機能要件。

危殆化：暗号アルゴリズムの文脈で使われ、新しい攻撃手法の発見や演算能力の飛躍的向上によって、安全性が低下した状態を指す。

合意形成：ブロックチェーンでは、複数のノードで協調してブロックを維持するために、ブロックを誰が追加するかを明確に決める必要があり、そのルールを指す。プルーフ・オブ・ワーク、プルーフ・オブ・ステークなどがある。

攻撃耐性：ブロックチェーンでは多数の者が参加できるが故に、悪意を持って参加する者も許してしまう。それにより、正常なブロックチェーンの形成が妨害されるが、悪意ある者の行為に対して、防御できることを耐性があるという。

真正性：記録されたデータがその通りであることを示す特性で、いわゆる「なりすまし」や虚偽の入力、データの書き換え、削除がないことをいう。

スケーラビリティー：情報システムの拡張性のこと。システムは、利用者数や処理量の増大、用途の拡大などに応じてそのシステムを拡張できるかどうかが重要である。ビットコインにおいては、ブロックの大きさに制限があることから、そのスケーラビリティーに問題があると言われている。

スマートコントラクト：ブロックチェーンネットワーク上で動作するプログラム、および、それによって表現された契約。契約に関する一連の流れが自動的で高速かつ効率よく行われることを目的にする。Bitcoin の取引記述機能の制約を大幅に緩和した Ethereum で発案したことで有名になった。

耐量子計算機暗号：量子計算機が実用化された場合のリスクに対応した暗号技術。なお、ここでいうリスクは、ブロックチェーンに関しては、公開鍵から秘密鍵が計算できてしまうこと、および、プルーフ・オブ・ワークにおけるナンスの計算が一瞬でできてしまうことと言われている。

タイムスタンプ:あるイベントが記録された時刻を示すための情報。公開鍵基盤（PKI: Public Key Infrastructure)を利用し、改ざんされないように工夫されている。

デジタル・アイデンティティー（DID：Digital Identity）：人間などの主体性を表す情報を計算機で処理できるようにしたデジタル情報。通常は単一の管理主体が管理するが、自分の情報のコントロール権を確保するという流れから、ブロックチェーン技術を活用した分散型アイデンティティー（Decentralized Identity）の検討が進んでいる。

トラスト：情報システムや情報サービスにおける安心や信頼の概念の総称。情報セキュリティーやディペンダビリティーのみならず、心理学や社会学の概念を含む。

ハッシュ値、ハッシュ関数：ハッシュ値は、データのまとまりから作り出す、そのデータの中身を示す値。ハッシュ関数は、メッセージから暗号学的にハッシュ値（ダイジェストと呼ぶ）を算出する。ハッシュ値から元のメッセージを復元できないこと、異なるメッセージから同じハッシュ値を生成しないこと、メッセージを少し変えるだけでハッシュ値が異なること、などの特性を持つ。

ファイナリティー：ブロックチェーンに記録されたトランザクションの真正性が確定すること。金融取引においては一旦完了した決済が二度とくつがえらないことをいう。

プルーフ・オブ・ワーク（PoW: Proof of Work）：分散合意形成のアルゴリズムの一つで、必要な計算を成功させた人が、そのデータを承認して正しくブロックチェーンにつなぎこむ役割を担う仕組み。作業証明ともいう。Bitcoin の場合、約 10 分に一つのブロックが生成されるよう計算の難度が巧妙に調整される仕組みを有する。

分散台帳：ネットワーク上の複数のノード上にそれぞれ台帳を用意し、その台帳に記載される情報を共通化して、台帳間で共有されつつ同期されることで同じ状態が保たれる状態を指す。

マイニング：プルーフ・オブ・ワークにおけるデータ承認作業をマイニングと呼び、成功者には新しく発行された仮想通貨が与えられる。作業には総当たり的にある数値（ナンス）を求めるアルゴリズムが採用されており他者より早く成功させるために膨大な計算が必要となり電力問題を引き起こしている。

IPFS（InterPlanetary File System）：サーバーを介さずに、データを利用するものとデータを提供するものが直接データのやり取りを行う、分散型のファイルシステム。ファイルのハッシュをそのコンテンツのアドレスとすることから、Web の高速化、安全化が図れるとされる。

Layer2 技術：ブロックチェーンそのもののネットワークとは別のところで取引などを行うための技術。ブロックチェーンとは別の仕組みで取引を行っておき、あとでブロックチェーンのネットワークに取引を反映する。少額の取引や、取引の高速化を実現する。

P2P（Peer to Peer）ネットワーク：複数の端末間で通信を行う際の通信方式のひとつで、対等の者（Peer、ピア）同士が直接通信をすることを特徴とする。

Satoshi Nakamoto：2008 年に発表された論文 “Bitcoin: A Peer-to-Peer Electronic Cash System” の著者で Bitcoin の提案者とされる。年齢、性別、国籍など一切不明で、特定の個人か複数の人物かも不明である。

付録４ 参考文献

[1] Arvind Narayanan, Joseph Bonneau, and Edward Felten, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*, (Princeton Univ. Pr., 2016); 長尾高弘(訳),『仮想通貨の教科書』(日経 BP, 2016).

[2] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", https://bitcoin.org/bitcoin.pdf (accessed 2020-3-4)

[3] 岡田仁志, 高橋郁夫, 山崎重一郎,『仮想通貨―技術・法律・制度』(東洋経済新報, 2015).

[4] 佐藤雅史, 長谷川佳祐, 佐古和恵, 並木悠太, 梶ヶ谷圭祐, 松尾真一郎, セコム(株) (編), NEC (編),『ブロックチェーン技術の教科書』(シーアンドアール研究所, 2018).

[5] 松尾真一郎, 楠正憲, 崎村夏彦, 佐古和恵, 佐藤雅史, 林達也, 古川諒, 宮澤慎一,『ブロックチェーン技術の未解決問題』(日経 BP, 2018).

[6] 赤羽喜治, 愛敬真生,『ブロックチェーン 仕組みと理論』増補改訂版（リックテレコム, 2019).

[7] 山際貴子, "スマートコントラクトとは？ブロックチェーン活用の仕組みと KDDI の実証実験を紹介". ボクシルマガジン・ビヨンド (2018.01.10) https://boxil.jp/beyond/a3594/ (accessed 2020-3-4)

[8] Karen D. Frazer, *NSFNET: A partnership for high-speed networking：final report, 1987-1995* (Merit Network, 1996).

[9] 砂原秀樹, 村井純, "WIDE プロジェクトの 25 年 日本とインターネットのこれまでとこれから", 情報管理 Vol. 56 No. 9 (2013) pp.571-581.

[10] David Chaum, "Blind Signatures for Untraceable Payments", Advances in Cryptology: Proceedings of Crypto 82 (Santa Barbara, California, August 23-25, 1982) pp 199-203.

[11] e-Governance Academy, "e-Estonia: e-Governance in Practice" https://ega.ee/publication/e-estonia-e-governance-in-practice-2/ (accessed 2020-3-4)；三菱 UFJ リサーチ&コンサルティング（訳), 山田美明（訳), 杉田真（訳), 芝瑞紀（訳),『e-エストニア デジタル・ガバナンスの最前線』(日経 BP, 2019).

[12] Ahto Buldas, Andres Kroonmaa, and Risto Laanoja, "Keyless Signatures' Infrastructure: How to Build Global Distributed Hash-Trees", Proceeding of 18th Nordic Conference on Secure IT Systems (NordSec 2013; Ilulissat, Greenland, October 18-21, 2013) Vol. 8208, pp. 313-320.

[13] MIT Technology Review Japan (編), "Blockchain 分散型元帳テクノロジーは社会をどう変えるのか", MIT テクノロジーレビュー Special Issue Vol. 2 (角川アスキー総合研究所, 2017).

[14] MIT Technology Review Japan (編), "Blockchain 2「非中央集権化」の先にあるもの", MIT テクノロジーレビュー Special Issue Vol. 10 (角川アスキー総合研究所, 2018).

[15] EU Blockchain Observatory and Forum, Thematic reports on "Blockchain innovation in Europe" (2018), "Blockchain and the GDPR" (2018), "Blockchain for Government and Public Services" (2018), "Scalability, interoperability and sustainability of blockchains" (2019), "Blockchain and Digital Identity" (2019), "Legal and regulatory

framework of blockchains and smart contracts" (2019), "Blockchain in trade finance and supply chain" (2019), and "Blockchain and the future of digital assets" (2020). https://www.eublockchainforum.eu/reports (accessed 2020-3-4)

[16] Rajesh Kandaswamy and David Furlonger, Gartner Research on "Pay Attention to These 4 Types of Blockchain Business Initiatives" (Gartner, 2018).

[17] 経済産業省, 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 (2016).

[18] World Economic Forum, White Paper "Trade Tech – A New Age for Trade and Supply Chain Finance" (2018). https://www.weforum.org/whitepapers/trade-tech-a-new-age-for-trade-and-supply-chain-finance (accessed 2020-3-4)

[19] Bitcoin Exchange Guide News Team, "Spanish Ministry of Agriculture, Fisheries and Food Develops Blockchain App with ChainWood For Forestry Transparency", (September 24, 2018). https://bitcoinexchangeguide.com/spanish-ministry-of-agriculture-fisheries-and-food-develops-blockchain-app-with-chainwood-for-forestry-transparency/ (accessed 2020-3-4)

[20] 川崎貴夫, "森づくり・木づかいの「見える化」促進に向けた IT 化の最前線" グローバル時代の森林 CSV シンポジウム (August 29, 2016).

[21] BSafe.network, "Current Member Universities (29 Universities, As Of January 08, 2019)" http://bsafe.network/member-university/ (accessed 2020-3-4)

[22] 富士通, "金融ソリューション ～ブロックチェーンの取り組み～" https://www.fujitsu.com/jp/solutions/industry/financial/concept/blockchain/ (accessed 2020-3-4)

[23] 日本経済新聞, "日欧中銀など、デジタル通貨発行へ共同研究 中国やリブラに対抗" (2020/01/21).

[24] Don Tapscott and Alex Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*, (Portfolio, 2016); 高橋璃子 (訳), 『ブロックチェーン・レボリューション ――ビットコインを支える技術はどのようにビジネスと経済、そして世界を変えるのか』(ダイヤモンド, 2016).

[25] 高木聡一郎,『ブロックチェーン・エコノミクス 分散と自動化による新しい経済のかたち』(翔泳社, 2017).

[26] 高木聡一郎, ラニー・スワン, 岩村充, 前川徹, 松尾真一郎, 楠正憲, 田中秀幸, 藤井靖史, 武宮誠, 岩下直行, 榊原彰, 佐野究一郎, 高城勝信,『智場#121 ブロックチェーンのフロンティア』 (GLOCOM, 2017).

[27] 飯田泰之,『日本史に学ぶマネーの論理』 (PHP 研究所, 2019).

[28] 坂井豊貴,『暗号通貨 VS.国家 ビットコインは終わらない』(SB クリエイティブ, 2019).

[29] David Furlonger and Christophe Uzureau, *The Real Business of Blockchain: How Leaders Can Create Value in a New Digital Age*, (Harvard Business Review, 2019).

上記文献を含め本文中のURLは、2020年3月1日時点のものである。

■作成メンバー■

総括責任者：木村 康則	上席フェロー	（システム・情報科学技術ユニット）
リ ー ダ ー：茂木　強	フェロー	（システム・情報科学技術ユニット）
メ ン バ ー：尾山 宏次	フェロー	（環境・エネルギーユニット）
周　少丹	フェロー	（海外動向ユニット、中国総合研究交流推進室）
高島 洋典	フェロー	（システム・情報科学技術ユニット）
辻　真博	フェロー	（ライフサイエンス・臨床医学ユニット）
日江井 純一郎	フェロー	（科学技術イノベーション・政策ユニット）
的場 正憲	フェロー	（システム・情報科学技術ユニット）
高木 聡一郎	特任フェロー	（システム・情報科学技術ユニット）
畠山 靖彦	主任調査員	（監査・法務部）（～2019 年 3 月）
川崎 貴夫	JST PM 育成・活躍推進プログラム研修生（～2019 年 3 月）	

※お問い合わせは、下記までお願い致します。

CRDS-FY2019-SP-09

戦略プロポーザル

次世代ブロックチェーン技術

～個人や社会のデータ共有・価値交換を安全で高信頼に実現する～

STRATEGIC PROPOSAL

The Next Generation Blockchain Technology

— To establish secure and trustworthy infrastructures for data-sharing and value-exchange among people and society —

令和 2 年 3 月　March 2020

ISBN 978-4-88890-676-0

国立研究開発法人科学技術振興機構　研究開発戦略センター

Center for Research and Development Strategy, Japan Science and Technology Agency

〒102-0076　東京都千代田区五番町 7　K's 五番町

電　話　03-5214-7481

E-mail　crds@jst.go.jp

https://www.jst.go.jp/crds/

ISBN-978-4-88890-676-0