2.5.7 ブロックチェーン

（1）研究開発領域の定義

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 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。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様々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、本項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含め広く俯瞰することとする。

（2）キーワード

分散台帳、公開鍵暗号、ハッシュ関数、P2P ネットワーク、合意形成、インセンティブメカニズム、スマートコントラクト、仮想通貨、Bitcoin、Libra（Diem）、中央銀行デジタル通貨（CBDC：Central Bank Digital Currency）、分散型アイデンティティー（DID: Decentralized Identity）、自己主権型アイデンティティー（SSI：Self-Sovereign Identity）

（3）研究開発領域の概要

［本領域の意義］

ブロックチェーンはその生い立ちから仮想通貨 Bitcoin との関係が特に深い。 Bitcoin はブロックチェーン技術に基づく仮想通貨であり、2008 年に Satoshi Nakamoto 論文[1)] によるアイデアの発表があり、翌年に Bitcoin のソフトウェアが公開された。ブロックチェーンには様々な実現形態があるが、Bitcoin においては、仮想通貨を送金したという取引データをまとめたものをブロックとする。そして、そのブロックを次々と連結し、それらをコンピューターネットワーク上の複数のサーバーに分散して保管することによって、Bitcoin の取引全体を記録する分散台帳が実現される。ここで、暗号技術、P2P（Peer to Peer）ネットワーク技術、分散合意形成技術および継続的運用のためのインセンティブなどのメカニズムを利用することによって、「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ーを担保できる」というブロックチェーンのメリットが実現される。ブロックチェーン技術は、仮想通貨はもとよりそれ以外への適用が期待されており、さまざまな分野で新たなサービスの開発や実証実験が進められている。

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、たとえば銀行が担ってきた「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、人と人をデジタル技術に基づく信頼によって結ぶ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。紙をベースとした仕事の進め方から、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、科学技術的な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・実装基準などの整備も必要である。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。さらに、ブロックチェーン技術により実現されている主要仮想通貨システム（Bitcoin、Ethereum）で使用されているマイニングにかかる消費電力が2020年時点で、それぞれ年間約77.8TWh（テラワット時）と13.8TWhといった莫大な電力消費量となっており[2)]、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。これらの課題を解決し続けることによって、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。

［研究の経緯］

ブロックチェーンに関わる技術の系譜をたどる。ブロックチェーンは仮想通貨Bitcoinを実現するために設計された。仮想通貨自体は暗号技術の応用として古くから考えられてきた。David Chaumのブラインド署名技術を用いたDigiCash は暗号技術に基づく仮想通貨の草分けである。DigiCash[3)] はさまざまな理由から普及には至らなかったが、2008 年に Satoshi Nakamoto が書いた論文とその実装により、Bitcoinが生まれた。当初のブロックチェーンは、Bitcoinの実現に特化して設計された、暗号技術と P2P ネットワーク技術、分散合意形成技術などの既存技術の統合といえる。Satoshi Nakamoto の功績は、通貨の発行をProof of Work と呼ばれる分散台帳の整合性維持に対する作業への対価とすることで、継続的に運用できるインセンティブメカニズムを考案したことである。本稿では、BitcoinおよびBitcoinから派生した仮想通貨（オルトコイン）で使われるブロックチェーン技術を第1 世代とする。

Bitcoinの成功により、ブロックチェーンに対して、仮想通貨以外にも応用できる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。たとえば、ある一定の条件を満足した場合に支払いを行うというような契約を自動的に実行することもできる。これを第 2 世代とする。

ブロックチェーンは汎用的な情報処理の技術基盤であると考えると、今後、第3世代としてさらに広範な応用が広がるだろう。どのような応用が生まれるのか、そのためにはどんな技術的発展が必要かということは今後の研究開発、ビジネス開発にかかっている。

また、仮想通貨（近年は暗号資産を呼ばれる）に関しては、Facebookが発表したLibraに刺激されて、各国の中央銀行がデジタル通貨の発行を検討する動きが加速している。その他、GAFAによるデータ覇権に伴うプライバシー情報の占有に対する動きとして、自己主権型アイデンティティー、また、そのブロックチェーン技術による実現としての分散型アイデンティティーの仕様策定も進んでいる。ブロックチェーン技術の応用は新たな広がりを見せている。

［研究開発の動向］

プラットフォーム化するブロックチェーン

Bitcoinの技術基盤として生まれたブロックチェーンの汎用性を活用した応用が次々に生まれ、また、同時にBitcoin以外のブロックチェーンを処理する実行基盤（プラットフォーム）も登場した。現時点での代表的なプラットフォームとして、Bitcoin、Ethereum、Hyperledger Fabric があげられる。次項に述べるように、それぞれ管理者の有無と参加者の参加方法やできることが異なる。Ethereumは、Bitcoinの課題解決や新たな拡張性を目指して全く新規に設計された。独自仮想通貨イーサーの実行基盤でもあるが、契約、権利管

理等への利用をめざして開発が進められている。Hyperledger Fabric は主に企業でのブロックチェーンの活用を目指して OSS（Open Source Software）プロジェクトとして開発が進められている。表 2-5-1 にプラットフォームとしての Bitcoin、Ethereum、Hyperledger Fabric の特徴をまとめた。

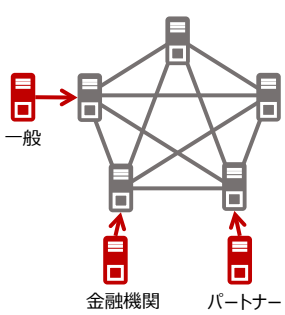
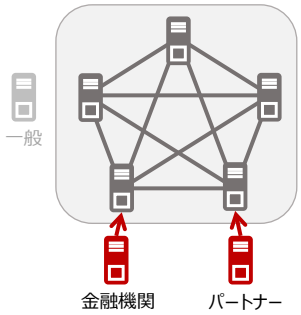
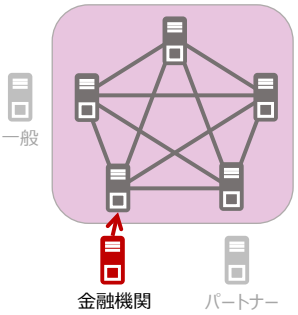
表 2-5-1　　代表的なブロックチェーン・プラットフォーム

	Bitcoin	Ethereum	Hyperledger Fabric
開始年	2009	2015	2015
開発主体	Satoshi Nakamoto 他	Ethereum 財団	LINUX、IBM、Intel、ソラミツ他
形態	パブリック型	パブリック型	パブリック型・プライベート型
内容	仮想通貨としての流通	仮想通貨を含めた取引一般	様々なソリューションの技術基盤
合意形成方式	Proof of Work	Proof of Work。 今後 Proof of Stake へ変更予定。	PBFT（v0.6）、 EndorcementPolocy（v1.0）
通貨	BTC（Bitcoin）	ETH（イーサー）	通貨なし／あり
プログラミング	スクリプト（scriptSig）による限定されたプログラム	スマートコントラクト言語による自由なプログラム	スマートコントラクト言語による自由なプログラム

パブリック型からプライベート型、コンソーシアム型へ

Bitcoin は、管理者に相当する組織が存在せず、誰もが平等で、誰からも許可を得ることなくネットワークに参加できる、非中央集権な P2P ネットワークである。このようなオープンなブロックチェーンはパブリック型やパーミッションレス型と呼ばれる（以下、本項ではパブリック型と呼ぶ）。一方、例えば、米国 Ripple Labs が運営する仮想通貨 Ripple のようなケースでは、管理者がおり、参加できるのは特定の限られた者のみである。このような、中央管理者を置き運営しているブロックチェーンはプライベート型やパーミッションドと呼ばれる（以下、本項ではプライベート型と呼ぶ）。また、プライベート型の派生形で複数の管理者からなるコンソーシアム型もある。これらについて、表 2-5-2 に整理した。

表 2-5-2　　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（Permissionless）	特定複数（Permissioned）	組織内（Permissioned）
合意形成の仕組み	PoW / PoS（※ 2）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）
参加者のアクセス権	全員がフルアクセス	管理者が決める	管理者が決める
プラットフォーム	Bitcoin（※ 1 BCN） Ethereum	Hyperledger Fabric	Hyperledger Fabric Ripple

※ 1 BCN：ブロックチェーンネットワーク ※ 2 PoW：Proof of Work / PoS：Proof of Stake

画像：富士通　金融ソリューション　～ブロックチェーン技術への取り組み～　を参考に作成
（https://www.fujitsu.com/jp/solutions/industry/financial/concept/blockchain/）

パブリック型の場合は、参加者の賛同が必要であるため、ブロックチェーンの仕様変更は一般には難しい。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自由に変更でき、柔軟なシステムの運用が可能である。プライベート型の場合は、新しい技術の検証などがしやすく、企業を中心に、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。

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」という全く異なる性格が表れる。パブリック型ブロックチェーンは、そもそも中央集権機関などの既存の枠組みとは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可能性もある。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。一方でパブリック型ブロックチェーンには合意形成に時間がかかる等の現実的な課題があるため、それを解決する一つの手段としてプライベート型のブロックチェーンが考案された。プライベート型ブロックチェーンは、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ブロックチェーンの採用が今後急激に進む可能性もある。

ブロックチェーンのメリットと応用

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ーを担保できる」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、

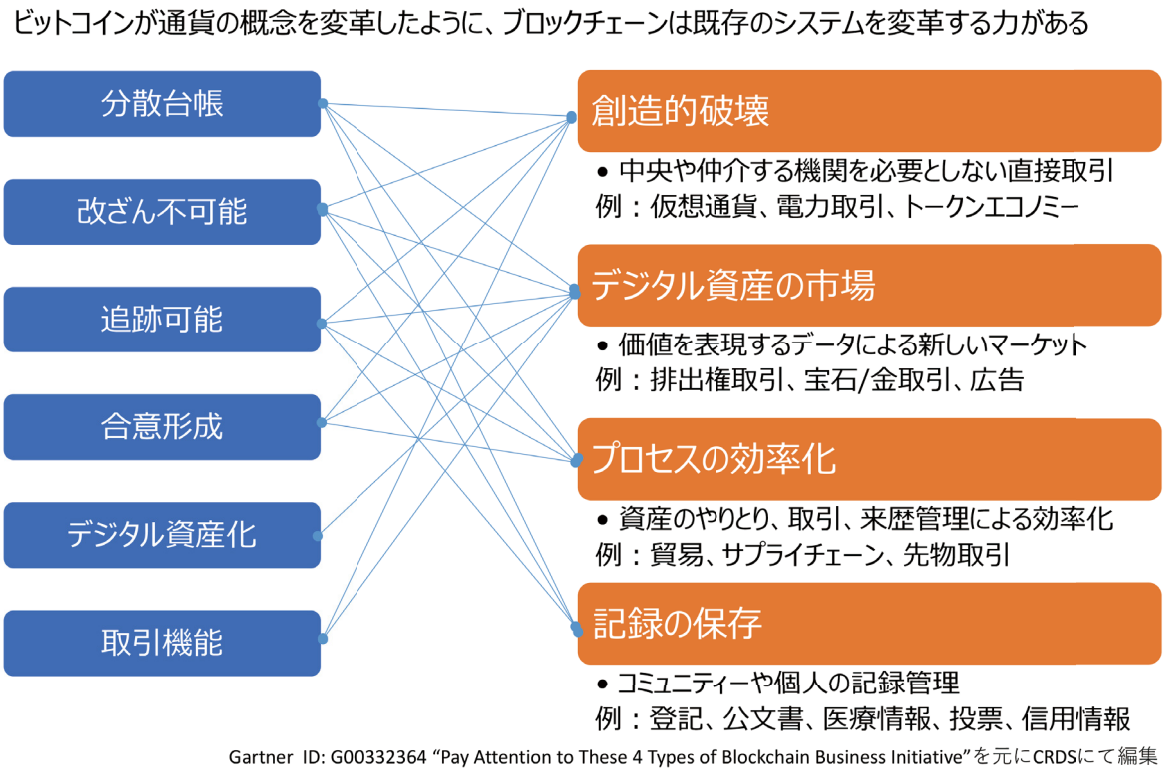


図 2-5-3　　ブロックチェーンの機能と社会・経済的インパクト

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 2-5-3 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可能性がある[4)]。

［標準化の状況］

ブロックチェーン技術関連の標準化は主に国際標準化団体において活発に進められている。ISO では 2016 年 9 月に ISO/TC307 Block-chain and electronic distributed ledger technologies[1] を設置し、ブロックチェーンと電子分散台帳におけるシステム、アプリケーション，ユーザー間の互換性やデータ交換にかかわる国際標準化活動を開始した。IETF（The Internet Engineering Task Force）では 2018 年より分散化技術に関する研究課題を調査している[2]。ITU（International Telecommunication Union）では、分散台帳技術の適用に関する ITU-T フォーカスグループ（FG DLT）[3] を 2017 年 5 月に設立し、DLT ベースのアプリケーションとサービスを特定した分析と、アプリケーションとサービスのグローバル規模での実装をサポートするベストプラクティスとガイダンスの作成を向けた活動を実施している。また、W3C（World Wide Web

1 https://www.iso.org/committee/6266604.html
2 Decentralized Internet Infrastructure Proposed RG, https://datatracker.ietf.org/doc/charter-irtf-dinrg/
3 Focus Group on Application of Distributed Ledger Technology DLT, https://www.itu.int/en/ITU-T/focusgroups/dlt/Pages/default.aspx

Consortium）では、分散台帳におけるデータモデルやシンタックス（The Web Ledger Protocol[4]）や分散ID（Decentralized Identifiers[5]）に関する標準の策定を行っている。

（4）注目動向

［新展開・技術トピックス］

スマートコントラクト[5), 6), 7)]

スマートコントラクトは「契約の締結と実行の自動化」であり、1994年にNick Szaboという法学者・暗号学者により提唱された。本項ではブロックチェーン上であらかじめ設定していたプログラムにより自動的にトラストレス（信用を考慮する必要がないこと）で取引を実行する仕組みを指す。 Bitcoinの使用言語（スクリプト）は分岐やループを持たないため、実行できる処理は限定される。 Vitalik Buterinが Bitcoinシステムを応用したプロジェクトに参画する中で、より制約の少ない汎用的な Bitcoin ライクなシステムとしてEthereum を発案した。スマートコントラクトはその中核的な要素である。 Ethereumは自由なスマートコントラクトを書くためのチューリング完全と呼ばれるプログラム言語を提供し、さまざまな契約を仲介者無しで自動的に実行するためのプログラムが作成できる。例えば、レンタカーを借りる場合を考えてみる。貸し手はスマートフォンなどの電子鍵で車のカギをロックできるとする。スマートコントラクトにより借り手が契約条件通りの金額を支払うと、そのイベントを検知して自動的にカギを借り手に送付し、それにより借り手のスマートフォンなどの電子鍵で解錠可能となり、すぐに運転ができるようになる。このように一定の取引条件を満たしたことを確認して契約を自動的に執行できる仕組みが可能になる。しかし、実際にスマートコントラクトが機能するためには、取引条件を満たしていることを現実世界にアクセスして保証する信頼できる第三者（オラクルと呼ばれる）が必要となる。

DAG（有向非巡回グラフ：Directed Acyclic Graph）[8), 9), 10)]

ブロックチェーンは基本的に複数の取引（トランザクション）をブロックとしてまとめて、それをチェーン状につなぐ構造を持つが、DAG は一つ一つの各取引をユニットとして巡回しないよう一方向に複数のチェーンでつなげた構造を持つ。 DAG では取引をまとめたブロック生成が不要なので、その報酬を目的とした Proof of Work の概念がない。 DAG を用いた分散台帳には、2016 年に公開された仮想通貨 IOTA、Byeball などがある。 IOTA では DAG を用いた Tangle と呼ばれる技術を用いており、取引を行う自分自身が過去の二つの取引を承認しながら DAG への組み込みを行う。一定時間内に多くの取引を取り込めるとともに、パブリック型の課題とされるインセンティブ不整合（ブロックチェーンの承認機能を支えるマイナーのインセンティブは報酬であり、取引台帳の維持ではないこと。このため報酬の低下がブロックチェーン自体の機能不全を引き起こす）が回避でき、手数料が掛からない高速な取引が実現できる。このように IOTA は、名前の由来通り IoT におけるマイクロペイメントと呼ばれる少額取引に特化した仕組みになっている。ただし DAG を用いた分散台帳技術は歴史が浅く、セキュリティー、信頼性等についてはまだ十分検証されているとは言えない。

4 The Web Ledger Protocol 1.0, https://w3c.github.io/web-ledger/

5 Verifiable Credentials Data Model 1.0, https://www.w3.org/TR/vc-data-model/

Bitcoinブロックチェーンを用いたオフチェーン技術

Bitcoinブロックチェーンを少額取引（マイクロペイメント）として利用する場合、手数料が高いことや取引のスループットが低い（約7取引 / 秒）という課題がある。この問題点を解決するために基盤レイヤー（ レイヤー1）となるBitcoinブロックチェーンの外に、レイヤー 2 として新しいシステムを設けることで対応するオフチェーン技術が検討されている。有名なものとしてはライトニングネットワークがある。すでにいくつかの実装プロジェクトが進んでいるが、開発途上であり、実現にはBitcoin本体の仕様変更を必要とする。しかし、将来的にBitcoinのスケーラビリティーの問題を解決し、多様な用途でマイクロペイメントを実現できると期待される。

自己主権型ID（SSI：Self-sovereign Identity）[11]、分散型ID（DID：Decentralized IDentity）、

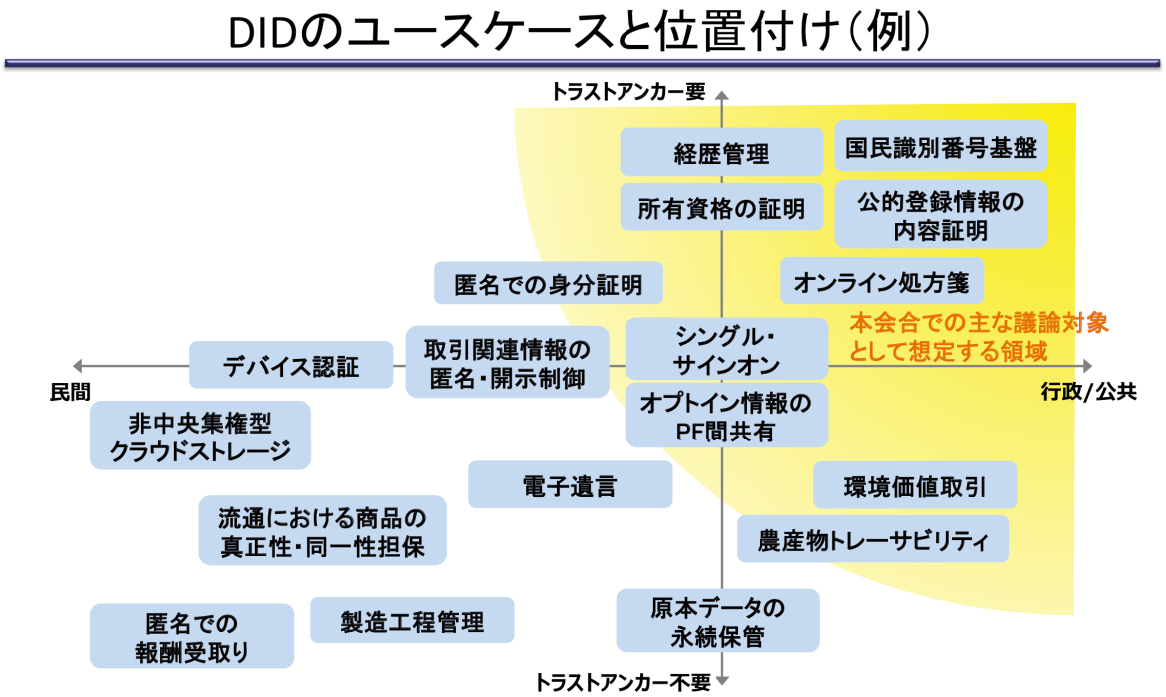
デジタルID（アイデンティティー）は、免許証のような物理的媒体を持たないIDであり、サイバー空間における個人や組織の認証や認可に用いられる。デジタルIDは、個人を特定するための識別子（アイデンティファイヤー）、クレデンシャル（IDの正当性を示す情報）と属性（IDに関わる付帯情報）を含む。現在、日常的に使われているデジタルIDは、国や金融機関や企業などのIDを発行する主体が本人確認した上で発行する集中型ID、あるいは、それらを相互認証させることでSSO（Single Sign-On）を実現するフェデレーテッドIDである。それに対して、個人が管理し個人の意思で企業などに情報を提供するデジタルIDが、自己主権型IDである。データ保護関連法（GDPR,CCPA等）の普及・浸透や、GAFAをはじめとする海外プラットフォーマーが 席巻している集中型IDへのアンチテーゼとして注目されている。

分散型アイデンティティー（以下DID）は、SSI概念に基づいて開発されている。 W3Cは「暗号化されて生成及び／又は登録されるため、中央の登録機関を必要としないグローバルに一意の永続的な識別子」と定義している[6]。DIDはデジタルの世界で同一の人物であることを特定することに使われる。ブロックチェーンの技術から発展したDIDは、登録機関を必要としない点がこれまでのデジタルIDと本質的に異なる。本人確認や修了証明などのクレデンシャルは、それぞれの発行機関からDIDに関連づけられた形で発行してもらう。なお、クレデンシャルそのものは暗号技術により守られているので改ざんも盗み見もできない。また、個人情報の部分的な開示（例えば、年齢は明かさず成人であること、学校名は示さず学歴を示す）や自分のデータについての自由なアクセス、データの消去などが可能になる。例えば、DIDを公的個人認証（例えば日本におけるマイナンバーカード）と紐づけることで、行政／公共から民間に至るまで広範で、基本的に全ての個人のサービスをグローバルに一元管理することができる。図 2-5-4には、その他の様々なユースケースがまとめられている。現在W3Cでは詳細な仕様を策定中である[7]。

欧米においてDIDやSSIの標準化や実証実験が盛んなのは、欧州の一般データ保護規則（GDPR）や米国のカリフォルニア州 消費者プライバシー法（CCPA）に対する具体的なソリューションになりうると考えられているからである。

6 Decentralized Identifiers（DIDs）, https://www.w3.org/TR/did-core/

7 Verifiable Credentials Data Model, https://www.w3.org/TR/vc-data-model/



※ W3CにおけるDID及びVCのユースケース文書、本会合で紹介された事例を参考に内閣官房IT総合戦略室にて作成
（参考）W3C “Use Cases and Requirements for Decentralized Identifiers,” W3C Working Draft 02 September 2020
W3C “Verifiable Credentials Use Cases,” W3C Working Groupt Note 24 September 2019

図 2-5-4　DIDのユースケースと位置付け

（一般社団法人 新経済連盟主催第３回ブロックチェーン官民推進会合資料より抜粋）

［注目すべき国内外のプロジェクト］

本項では主に応用に向けた取組みを紹介する。

デジタル通貨（Bitcoin、Libra/Diem、CBDC）

Bitcoinは、「同意している二者が信頼できる第三者を必要とせず，直接取引が可能な，トラストの代わりに暗号的証明に依拠する電子支払いシステム」として開発された[12]（2008年発表）。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。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、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（2020年12月1日Diemに改称された[13]）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（2019年発表）。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法定通貨に絞ることは、多国籍のユーザーが自由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財団らが管理する

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、法定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、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中央銀行デジタル通貨の運用を開始した。わが国でも、日本銀行が「現時点で中央銀行デジタル通貨（CBDC：Central Bank Digital Currency）を発行する計画はないが、決済システム全体の安定性と効率性を確保する観点から（略）しっかり準備しておくことが重要であると考え」日本銀行の取り組み方針を公開した[14)]。

このように、Bitcoin、Libra、CBDC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。また、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。

デジタルガバメント ×ブロックチェーン

デジタルガバメント（電子政府、電子自治体）での取り組みにおいてはエストニアの成功事例（後述）がめざましいが、ここでは我が国における取り組みを紹介する。内閣官房 情報通信技術（IT）総合戦略室は、世界最先端デジタル国家創造宣言・官民データ活用推進基本計画[15)] を受けて、第2回ブロックチェーンに関する官民推進会合を開催した（2020年度6回開催予定）。本会合は、「ポストコロナ、ウィズコロナの社会課題の解決手段として、ブロックチェーンの有用性を官民共同で検討するとともに、地方自治体と協力することにより、スマートシティー、スーパーシティーを含む実装に向けた提案につなげること」を目指す[8]。具体的には、スマートシティー、分散ID、教育、中央省庁取組の各事例が議論される予定である。

サプライチェーン ×ブロックチェーン

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ーによって、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、食品トレーサビリティーでは、米IBMがスーパーマーケットチェーンWalmartと組んで、葉野菜を対象に瞬時に追跡できるシステムを開発し、ブロックチェーンソリューションとして提供している。また、真贋証明では、Everledgerがダイヤモンドなどの高級品の出所を追跡、記録し、顧客や資産を追跡したいステークホルダーに情報提供するシステムを開発した。

8 https://jane.or.jp/proposal/pressrelease/12039.html

電力取引×ブロックチェーン

日本でのフィードインタリフ制度（固定価格買取制度）の導入を契機に、蓄電池や分散型電源、再生エネルギーの普及を促進するため、新たな電力取引の仕組みを考える動きが出てきた。分散型電源を利用し「地産地消」を図るコンセプトは従来からあったが、関連技術の進展により取引システムが安価に構築可能になったことから、ブロックチェーンの利用を含め検討が加速している。多くは電力取引システムへの応用であるが、一歩踏み込んだ非同期連携技術の検証を行っている事例を紹介する。東京大学はメーカー・電力会社などと提携し、さいたま市美園地区（みそのウィングシティ）で電力取引システムの検証実験を 2017 年から始めた。これは、DGR（デジタルグリッドルーター：系統に接続する電力変換器がそれぞれ固有のアドレスを持ち、ブロックチェーンを介して取引し、電力ルーターを同時に動作させる）を用いた電力潮流制御を用いた仕組みである。太陽光発電、蓄電池の電力を株式市場のようなザラ場で価格を決め、売りと買いの約定が成立したもの（同時同量）のみが流れるようになっており、引き取り手がない電気は入れないようにしている。このため系統への負担を抑えられる。この技術により電力は通信におけるパケットのように取り扱われる。

医療・ヘルスケア×ブロックチェーン

取り扱いの難しい医療ヘルスケアデータの共有、医薬品モニタリング、保健、健康管理への適応が検討・実証されている。主にデータの改ざん防止やセキュリティー強化、複数機関での安全なデータ連携が主目的であるが、患者側のメリットの訴求と経済的効果の有用性確認が課題である。いくつか代表的な事例を以下に示す。米国 MedRec[9]（2016）はEHR（Electronic Health Record：電子健康記録）の記録管理にEthereumベースのブロックチェーン技術を利用している。草分け的存在であり、現在はアクティブでない。英国 MedicalChain[10]（2018）は、医療機関や薬局、保険会社の間で、患者の健康情報をシームレスかつ安全に共有できるブロックチェーンである。 HyperLedger FabricとEthereumを使い分ける。またERC20ベースの MedToken を提供している。同じく、英国のMyPCR[11]はエストニア初のスタートアップ Guardtime が立ち上げた、イギリス国民保健のサービス利用者を対象とした医療データ記録提供プラットフォームで、最大3,000万人の英国民を対象に稼働しており、世界最大級規模の医療データ共有プラットフォームである。中国では Ali Health（阿里健康）[12]は2017年8月に江蘇省の常州市と提携し、医療データの保護と連携のための実証実験を実施した。地域の保健センターの健康診断で心血管疾患とされた患者の電子カルテを、より専門性の高い医療機関に安全に転送できるかが確認された。このように、ブロックチェーンが、医療・ヘルスケアに徐々に浸透しつつある。

一方で、わが国では実際に当該領域に取り組む研究者は、アカデミア、企業とも極めて少ないのが実態である。2018 年 9 月時点で、「医療・ヘルスケア×ブロックチェーン」を研究実施対象と明言した唯一のプロジェクトが、戦略的イノベーション創造プログラム（SIP）「AI（人工知能）ホスピタルによる高度診断・治療システム」である。同プロジェクトの研究開発計画書（平成 30 年 7 月 19 日）では「サブテーマ A：セキュリティの高い医療情報データベースの構築とそれらを利用した医療有用情報の抽出、解析技術等の開発」の

9 https://medrec.media.mit.edu/
10 https://medicalchain.com/ja/
11 http://mypcr.org/
12 https://ir.alihealth.cn/en/ir_index.php

中に、「⑦トレーサビリティー、スマートコントラクトを内包するブロックチェーン技術等を応用した通信プロトコルの開発」が公募対象として掲げられている[16), 11)]。わが国の医療・ヘルスケアに様々な課題があるが、ブロックチェーンは、そのような状況に大きな風穴をあける、破壊的な技術としてのポテンシャルを有すると期待されている。

教育×ブロックチェーン

教育分野では、学位・履修履歴証明、研究データの信頼性確保に向けた取り組みが進んでいる。大学・研究機関では、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が始まっている。MITでは、ブロックチェーン技術の「真正性」の特徴を利用し、2017年6月に一部の修士課程修了者111人に対し、ブロックチェーン技術で実現されたデジタル修了証書を授与した。 MIT Media Lab と Learning Machine社が開発した Blockcerts[17)] というブロックチェーンのプラットフォームを利用している。また、ドイツのData Management Hub[18)] は、研究データに特化した分散データ基盤で、研究データの検索、アクセス、再利用などが可能な基盤を構築している。研究データは、IPFS（InterPlanetary File System）と呼ばれるハッシングとP2Pネットワークを融合させたファイルシステムに保存し、ハッシュ値のみをブロックチェーンに保存することで、データの肥大化を防ぐ。我が国でも、2020年10月より慶應義塾大学が中心となり卒業見込証明書などをスマートフォンアプリへ発行する次世代デジタルアイデンティティー基盤の実証実験を開始するなど取り組みが本格化している[19)]。

［諸外国の政策や海外動向］

エストニア～ブロックチェーン先進国～[20), 21)]

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）[22)] 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[23), 24)]。

EU Blockchain Initiative

EU は Blockchain Initiative として複数のプロジェクトを並行して走らせている。2018 年 2 月には、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[25)]。 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”や仮想通貨に関するプロジェクトもイニシアチブの下で開発が進められている。

BSafe.network[13]

Bitcoinは当初一個人や企業を中心に開発がなされ大学等の研究機関の関与はあまり見られなかった。ブロックチェーン技術の不安を解消し、誰からも信頼できる技術とすべく、2016 年、BSafe.network が MIT からの呼びかけに応じて設立された。これは研究用のブロックチェーン専用のネットワークである。日本（東大、慶大、東邦大、立命館大、早大が参加）を含むアジア、ヨーロッパ、北米、そしてアフリカの29 の大学が参加している。参加機関は研究成果を実装したソフトウェアをインストールして実行することで研究成果の有効性を確認できる。このプロジェクトでは、セキュリティー、ネットワーク技術、コンセンサスメカニズム、ゲーム理論、経済学、および規制など、ブロックチェーンに関わるあらゆる要素が研究と実験の対象になっている。インターネットのための技術開発を行う際に NSFNet が果たしたのと同じ役割を担うことを想定している。

米国 IEEE（Institute of Electrical and Electronics Engineers）

米国 IEEE 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 イニシアチブ（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様々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。

その他の注目動向

Shawn Fanning（音楽ファイル共有ソフト Napster の開発者）らが創業した米国 IoT スタートアップ Helium は、ブロックチェーンの仕組みを利用して、安価でどこででも利用可能なIoT デバイス向けのネットワーク網を新たに構築するための研究開発を行っている。彼らが開発するシステムは、「Proof of Coverage」と名付けられ、低消費電力ゲートウェイが分散型元帳を管理するためのマイナー的な役目を担う。

また、Matthew Spoke が創業した米国スタートアップ Aion は、ブロックチェーンの相互運用のための「token bridge（トークン・ブリッジ）」を開発し、Ethereumベースのトークン保有者が、Aion のブロックチェーン上に資産を実際に移動することなくバックアップする実証実験を行っている。

（5）科学技術的課題

ブロックチェーンに関わる技術全体を俯瞰する（図 2-5-5）。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

13 http://bsafe.network/

JST/CRDSにて作成

図 2-5-5　　ブロックチェーン技術の俯瞰

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。ソフトウェ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。

以下、個々の技術的課題について列挙する。

［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）

ブロックチェーンの各ノードから発信されるトランザクションの耐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をはじめとする仮想通貨では、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、署名方式が選択されている（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（楕円曲線暗号の一種）が使われている）が、将来の暗号解読能力の進歩、例えば、量子コンピューターによって、これらの暗号技術が破られる危険性がある（危殆化）。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

ブロックチェーンの各ノード間の通信には 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、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、DOS 攻撃や 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。

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ェ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。

［ブロックチェーン固有技術］

分散台帳：ファイナリティー、スケーラビリティー、匿名性

仮想通貨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。このため、Bitcoin の場合、ブロックサイズ（1 MB）、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いわれる。一般に、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／秒以上を処理できるため、それと比較してあまりに貧弱な性能しか確保できないことをスケーラビリティー問題と呼ぶ。Bitcoin においても、ライトニングネットワーク（レイヤー 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。トランザクションは公開されているため他の情報と突合することでユーザーを特定することが可能である。また、そもそも取引内容を公開したくない場合も多い。

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システムとして採用すべきプログラミングモデルの選択といかなるプログラミング言語を実装すべきかが課題となる。 Bitcoinではスクリプト型のプログラミングを用いて簡単な取引処理が記述可能だが、分岐やループ処理が行えずその記述範囲には限界がある。そこで、Ethereumではチューリング完全型のプログラミング言語（Solidity）を実装したが、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。また、自由度が高い分、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）。

（6）その他の課題

ブロックチェーンはBitcoinの成功により仮想通貨への応用が注目されがちだが、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い。しかし、現実には仮想通貨以外の応用に関しては、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）も多く、新たな応用の開拓に苦慮している。

根本的な原因は、ブロックチェーンが基盤技術も応用技術も未熟なことにある。投機的な価値を持つ仮想通貨をともかく獲得するためのエンジニアリング技術、特にマイニング技術の進化は専用の ASIC を開発するまでに至る。一方で、すでに見たように科学技術的な課題も山積している。そもそもブロックチェーンは総合格闘技と呼ばれることがあるように、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必要である。以下にそれらの課題のうち特に重要と考えるものを記述する。

インキュベーションプラットフォームによる人材育成とキラーアプリの創出

ブロックチェーンの現状は 1990 年代のインターネットに似ていると言われる。電子メールが使われ始め、ブラウザや HTTP サーバーによる WWW の実装が始まったころ、我が国ではWIDE プロジェクトとして大学や研究機関などを対象とした非営利目的のインターネット利用技術の開発が行われた。その後、インターネットの商用利用が始まり、新たなアイデアをもったベンチャー企業が登場し、グローバルな情報処理・情報通信のインフラとしての基盤が成立した。30 年前とは環境がまったく違うため同じアプローチが成功するとは思えないが、多種多様な動機や興味をもった人材が、さまざまなアイデアを試行しお互いに切磋琢磨する「るつぼ」のような環境が必要である。人材が育まれ次世代のキラーアプリが生まれ始めるのにある程度、例えば 5 年から 10 年程度の、時間がかかることを考えると待ったなしの状況であると言える。

法制度とシステム開発のコ・デザインによる社会システムの再構築

経産省がとりまとめた「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」[18), 26)] では、

ブロックチェーンが起こす社会変革の可能性として、地域通貨、土地等の登記、C2C（個人間）取引、開かれたサプライチェーン、取引の自動化などを具体例として挙げているが、いずれも既存の法規制や商習慣の枠組みを逸脱する可能性が高い。このような新たな社会システムを構築するためには、設計の段階から法制度の再設計とシステムの開発とを同時にデザインすることが不可欠である。

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潜在的な革新性を考慮すると、人工知能の人間や社会への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。関連した取組として、ブロックチェーン官民推進会合（前述）がある。

（7）国際比較

国・地域	フェーズ	現状	トレンド	各国の状況、評価の際に参考にした根拠など
日本	基礎研究	○	→	・慶應義塾大学の大槻知明教授らのグループは、ブロックチェーン技術を応用し、製品が消費者の手に渡った後も偽物製品の検知が可能な所有権管理システム（POMS：Product Ownership Management System）のプロトタイプを開発し、2017 年 7 月に発表[27)]。 ・慶應義塾大学の斉藤賢爾らは、プライベート型とパブリック型双方の良さを併せ持つハイブリッド型の日本発の次世代ブロックチェーンBBc-1（Beyond Blockchain One）を2017年2月に発表。
	応用研究・開発	○	→	・東京大学は電力会社などと提携し、さいたま市美園地区で電力ルーターを用いた電力潮流制御を含む電力取引システムの検証実験を 2017 年から始めた。 ・トヨタと Toyota Research Institute（TRI）は 2017 年 5 月、自動運転車の開発に使う走行データの取引市場やカーシェアリングの運用などに、ブロックチェーン技術の適用を検討すると発表。2019年には「トヨタ・ブロックチェーン・ラボ」を設立し実証実験を実施した。 ・2018 年 2 月、NEC および NEC 欧州研究所は、取引記録に参加するノード数 200 ノード程度の大規模接続環境下で毎秒 10 万件以上の記録性能を達成する世界最速のブロックチェーン向け合意形成アルゴリズムを開発し、世界規模のクレジットカード取引を支えるシステムとして必要とされる毎秒数万件を超える性能を実現。 ・富士通は、2017 年 11 月、ブロックチェーン同士を安全につなげるセキュリティー技術「コネクションチェーン」を開発。JCB、BOOSTRY、アクセンチュアらと共同プロジェクトを実施するなど積極的に活動している。
米国	基礎研究	◎	→	・UCB の Dawn Song 教授らの研究グループは、Ethereum の根本的な制約を克服する新たな「プライバシーを重視した」スマートコントラクト技術を探求。 ・MIT の Thomas Hardjono 教授らの研究グループは、データグラム（ネットワーク間を行き来できる情報の共通単位）と呼ばれるインターネット・プロトコル・スイートの概念を提案し、現在のブロックチェーン開発者はデータグラムの概念を取り入れるべきだと主張。

	応用研究・開発	◎	→	・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。 ・ベリディウム基金（Veridium Foundation）は IBM と提携して、公開型の Stellar ブロックチェーンを使って、「二酸化炭素排出権（炭素クレジット）のトークン化」を計画している（2018 年後半発行予定）。これは、IBM にとっては、公開型ブロックチェーンと許可型ブロックチェーンとを組み合わせる実証実験であり、炭素クレジットを他の商取引と組み合わす実証実験でもある。
欧州	基礎研究	○	→	・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。 ・スウェーデンのチャルマース工科大学（Chalmers University of Technology）では、公平なモビリティーサービスに向けた 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。
	応用研究・開発	◎	↗	・IoT のための仮想通貨 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（Decentralised 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。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。 ・フランスの銀行グループ SociétéGénérale 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。

中国	基礎研究	○	→	・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。
	応用研究・開発	◎	↗	・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。仮想通貨取引所 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。 ・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。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なっていく計画である。
韓国	基礎研究	△	→	・2018 年 6 月、高麗大学は、世界第 4 位の取引量を誇る Huobi（火幣）の子会社 Huobi Korea とブロックチェーン開発の分野での産学連携に合意。 Huobi Korea は、高麗大学を、韓国国内でのブロックチェーン技術の研究と技術教育の提携を拡大するための基盤とみなしている。
	応用研究・開発	△	→	・サムスン SDS は、2018 年 6 月に、ブロックチェーンを基盤にした金融プラットフォーム Nexfinance を発表。同社は、Nexfinance を通じ、デジタル金融ビジネスを立ち上げることを計画中。 ・サムスン SDS は、ブロックチェーンを活用した銀行向けの個人認証ツール BankSign を開発し、2018 年 8 月に発表。全銀行間で個人認証を一括で行える技術革新を目指している。 ・サムスン SDS は、自社のブロックチェーン・プラットフォーム Nexledger を輸出税関ロジスティクス・サービスに活用することに、2018 年 9 月、韓国税関と合意したと発表。

（註1）フェーズ

基礎研究：大学・国研などでの基礎研究の範囲

応用研究・開発：技術開発（プロトタイプの開発含む）の範囲

（註2）現状　※日本の現状を基準にした評価ではなく、CRDS の調査・見解による評価

◎：特に顕著な活動・成果が見えている　　○：顕著な活動・成果が見えている

△：顕著な活動・成果が見えていない　　×：特筆すべき活動・成果が見えていない

（註3）トレンド　※ここ1～2年の研究開発水準の変化

↗：上昇傾向、→：現状維持、↘：下降傾向

参考文献

1）Satoshi Nakamoto,”Bitcoin：A Peer-to-Peer Electronic Cash System”, https://bitcoin. org/bitcoin.pdf（accessed 2019-1-20）

2）Bitcoin / Ethereum Energy Consumption Index, https://digiconomist.net/bitcoin-energy-consumption（accessed 2020-12-21）

3）David Chaum,“Blind Signatures for Untraceable Payments”, Advances in Cryptology：

Proceedings of Crypto 82（Santa Barbara, California, August 23-25, 1982）pp 199-203.
4）JST CRDS,“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～」”,CRDS-FY2019-SP-09（2020年3月）
5）Aram Mine,“ブロックチェーン上で契約をプログラム化する仕組み「スマートコントラクト」”, http://gaiax-blockchain.com/smart-contract（accessed 2019-1-20）
6）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 社 , 2016）.
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 2019-1-20）
8）Hayata,“DAG 通貨の種類とそれぞれの特徴について”, Crypto Times（2018-03-02）https://crypto-times.jp/explain_dag/（accessed 2019-1-20）
9）おくなも ,“DAG 型暗号通貨のすすめ ブロックチェーンを代替しうる新技術”, BTC News（2017.09.22）https://btcnews.jp/2x5fpwlo12702/（accessed 2019-1-20）
10）Serguei Popov,“The Tangle”, IOTA Whitepaper Ver. 1.4.3（update：April 29, 2018）, https://forum.helloiota.com/732/The-Tangle-whitepaper; IOTA Fan Site（ 訳 ）, https:// iotafan.jp/wp-content/uploads/2018/06/iota1_4_3jp.pdf（accessed 2019-1-20）
11）株式会社野村総合研究所, デジタルアイデンティティー～自己主権型／分散型アイデンティティー～, , 2019年11月, https://www.nri.com/-/media/Corporate/jp/Files/PDF/service/ips/technology_1.pdf（accessed 2020/12/15）
12）松尾 真一郎, 5分で分かる！？有名論文ナナメ読み：Satoshi Nakamoto：Bitcoin：A Peer-to-Peer Electronic Cash System, 情報処理 Vol.61 No.2 Feb. 2020
13）Announcing the name Diem. Executive leadership in place in preparation for launch., https://www.diem.com/en-us/updates/diem-association/
14）日本銀行, 中央銀行デジタル通貨に関する日本銀行の取り組み方針, 2020年10月9日, https://www.boj.or.jp/announcements/release_2020/rel201009e.htm/
15）政府CIOポータル, 世界最先端デジタル国家創造宣言・官民データ活用推進基本計画（令和2年7月17日閣議決定）
16）内閣府 , 戦略的イノベーション創造プログラム（SIP）「AI（人工知能）ホスピタルによる高度診断・治療システム」研究開発計画（平成 30 年 7 月 19 日）
http://www8.cao.go.jp/cstp/gaiyo/sip/keikaku2/10_aihospital.pdf（accessed 2019-1-20）
17）https://www.blockcerts.org/（accessed 2020/12/14）
18）http://damahub.org/（accessed 2020/12/14）
19）慶應義塾大学、次世代デジタルアイデンティティー基盤の実証実験を開始, https://www.ctc-g.co.jp/news/press/20201026a.html（accessed 2020/12/14）
20）e-Estonia guide, https://e-estonia.com/wp-content/uploads/eestonia-guide-2018.pdf（accessed 2019-1-20）
21）e-Estonia FAQ, https://e-estonia.com/wp-content/uploads/faq-a4-v02-blockchain.pdf（accessed 2019-1-20）

22）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.
23）E-estonia,“Estonian Healthcare：e-Health record and e-Prescription took over,” Youtube（July 10, 2013）, https://www.youtube.com/watch?v=2XOqsJh4Abg（accessed 2019-1-20）
24）E-estonia,“E-health – Estonian Digital Solutions for Europe,”https://e-estonia.com/e-health-estonian-digital-solutions-for-europe/（accessed 2019-1-20）
24）EU Blockchain Observatory and Forum An Initiative of the European Commision, https://www.eublockchainforum.eu/（accessed 2019-1-20）
25）経済産業省、「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）http://www.meti.go.jp/press/2016/04/20160428003/20160428003.html（accessed 2019-1-20）
26）Kentaroh Toyoda, Panagiotis Takis Mathiopoulos, Iwao Sasase, and Tomoaki Ohtsuki, “A Novel Blockchain-Based Product Ownership Management System（POMS）for Anti-Counterfeits in The Post Supply Chain”, IEEE Access, Vol. 5,（2017）pp. 17465-17477. DOI：10.1109/ACCESS.2017.2720760