米国におけるブロックチェーンの現状

中沢 潔
JETRO/IPA New York

1　サマリー

世界のブロックチェーン市場は 2016～21 年までの 5 年間で年平均 81.2%のペースで成長し、2017 年時の 9 億 4,500 万ドルは、2021 年には 97 億ドルに達することが予測されている。地域別では、2021 年時に、米国が最大市場として世界全体の 40%以上、次に西欧諸国、中国、（日本・中国を除く）アジア太平洋諸国が続く。大きな支出の伸びが予想されている地域は、南米と日本であり、2016～21 年までの年平均成長率はそれぞれ 152.5%、127.3%となっている。

ブロックチェーンは、仮想通貨以外にも活用が期待されており、今回、仮想通貨、銀行間取引、ヘルスケア、不動産、サイバーセキュリティ、IoT の事例を取り上げた。

連邦法で規制する動きなどはこれまでみられていない。トランプ政権はブロックチェーン技術の活用に積極的に取り組んでいる一方、仮想通貨がマネー・ロンダリングやテロ組織への資金源、租税回避、詐欺等に悪用されることを懸念し、連邦政府レベルでは、各関連規制当局において仮想通貨に対する規制を見直す動きがみられるようになっている。州政府レベルでは、これまでに大多数の州が仮想通貨及びブロックチェーン技術に関する何らかの法規制を施行又は整備しつつあるが、こうした規制のほとんどは、既存の送金法における仮想通貨の取引について明確にする内容である。他方で、統一州法委員会は 2017 年 7 月、仮想通貨に関する州法間の整合性を図るため、「仮想通貨事業法に関する統一規則」を発表したが、これに対し、ビットコイン財団は、同規則の内容がニューヨーク州のビットライセンス規制と酷似している悪法として、州議会議員・関係者から構成される全米州議会議員連盟に対し、これを採択しないよう呼びかけている。

ブロックチェーンの課題として、以下が挙げられている。

- ***スケーラビリティ問題***― 大規模なデータベースに変わり得るか
- ***セキュリティ上の問題***― 個人情報や機密データを保存できるセキュリティ機能は強固か
- ***技術的な複雑性***― ユーザー側により多くの技術的知識を要求
- ***ガバナンスの必要性***― 規制当局による一定の標準策定及び制御の必要性

日本は「仮想通貨取引の主要中心地」とされている中、2018 年 1 月にコインチェック取引所におけるハッキング事件（被害額およそ 580 億円）、5 月 13～15 日にかけて発生した国産仮想通貨「モナコイン（MONA）」のブロックチェーンのマイニングに対する攻撃（被害額およそ 1,000 万円）が起き、ハッキングの懸念が広がっている。特に後者は、ビットコインと同じ仕組みのブロックチェーンの改ざんを可能にする「Selfish Mining（又は Block withholding attack）」と呼ばれる手法の攻撃が成功した初の事例であり、同じ仕組みを採用する全ての仮想通貨に起こり得る問題とされている。

また、Gartner Japan 社が 2018 年 4 月に発表した従業員数 500 人以上の日本企業を対象としたブロックチェーンへの取組み状況に関する調査結果によると、調査など初期的なものも含め、ブロックチェーンに何らかの形で取り組んでいる企業が全体の 42.6%に上ることが明らかになっており、同社は今後 3 年以内にブロックチェーンに取り組む日本企業は 60%程度に達すると予測している。

まだ技術として歴史の浅いブロックチェーンが現在のインターネットのような存在になるのか、その動向が注目される。

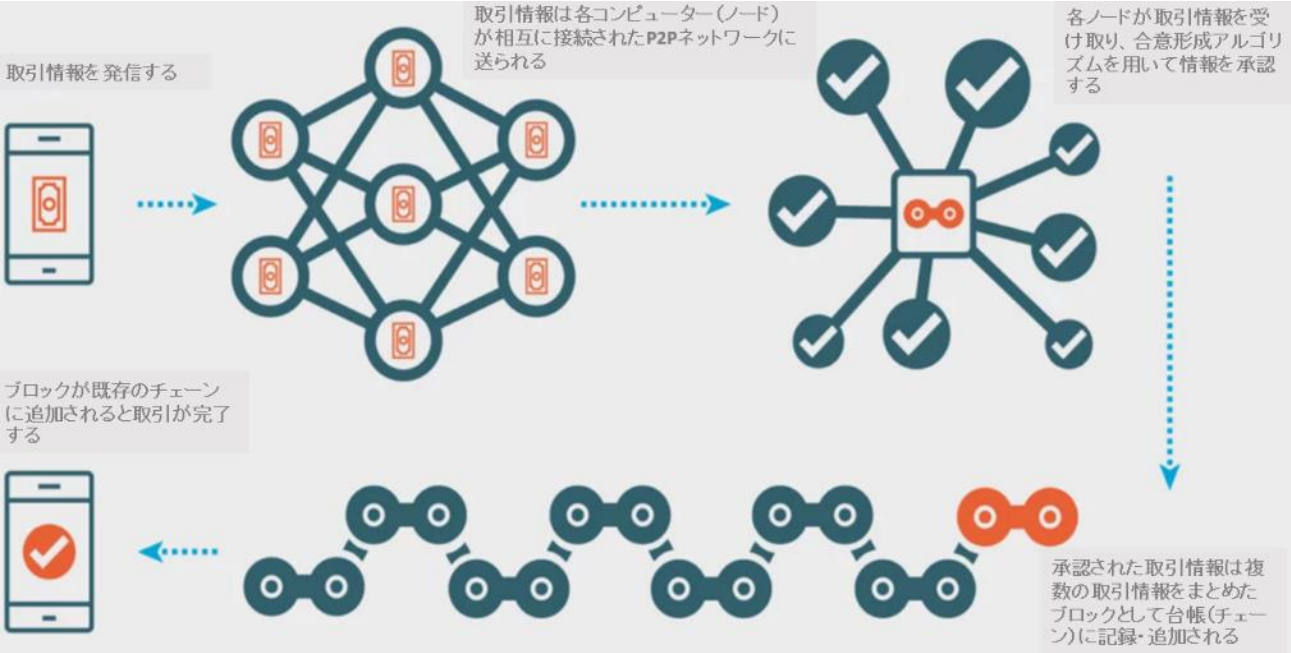
2　ブロックチェーン技術の特徴と市場動向

（1）　ブロックチェーンの仕組み

ブロックチェーン（blockchain）とは、P2P（peer-to-peer）ネットワーク[1]につながった複数のコンピュータデバイス（ノード）で取引情報を記録・共同管理する分散型デジタル台帳技術である。ブロックチェーンは、政府による通貨規制や銀行等の第三者機関による決済プロセスへの介入なしにオンライン上で安全に取引できる手法として開発された仮想通貨「ビットコイン（Bitcoin）」の中核技術として、2008 年にサトシ・ナカモト（Satoshi Nakamoto）と名乗る謎の人物[2]が発表した論文「P2P 電子キャッシュシステム（A Peer-to-Peer Electronic Cash System）[3]」が誕生の発端となっている[4]。

ブロックチェーンでは、ネットワークに参加する全てのノードが、ユーザー間でやり取りした決済関連の取引履歴を共有・管理することで各取引の安全性を担保している。発信された取引情報は、ブロックチェーンのネットワークに参加する全てのノードに通知され、取引の正当性を確認するための既定のルール（合意形成アルゴリズム）に従って特定のノードが、承認された複数の取引情報を「ブロック」として台帳に記録できるようになっている。ここでの台帳とは、ある程度の取引情報をまとめたブロックを時系列に沿ってチェーン（鎖）状につながったデータベースを指し、取引情報が新たなブロックとして追加登録されると取引が完了し、ネットワーク上の全てのノードで情報が共有される仕組みである[5]。

図表 1:ブロックチェーンの仕組み



[1] ネットワーク上で対等の機能・関係にあるコンピューターデバイス（ノード）間を相互に直接接続してデータを送受信する通信方式。P2P はネットワークに参加している各コンピューターがデータを保持し、他のコンピューターに対して対等にデータの提供や要求・アクセスを行う自律分散型のネットワークモデルであり、機能や情報を提供するサーバ（server）と、（その機能・情報を用いる）ユーザーが操作するクライアント（client）をネットワークで接続し、クライアントからの要求にサーバが応答する形で処理するクライアント・サーバ型モデルとは異なる。

[2] 「サトシ・ナカモト」については、それが個人であるかグループ名であるかも含め、詳細は明らかにされていない。

[3] https://bitcoin.org/bitcoin.pdf

[4] https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-bitcoin-and-blockchain-for-business/

[5] https://www.ibm.com/developerworks/cloud/library/cl-blockchain-basics-intro-bluemix-trs/

出典：G2 Crowd[6]

ブロックチェーンの安全性は、取引の正当性を確認する合意形成アルゴリズムのほか、データの改ざんやなりすましを防止するためのハッシュ関数及び電子署名技術により支えられており、対等な関係にある膨大な数のノードによって取引履歴を分散共有する仕組みが一度記録されたデータの改ざんを不可能にし[7]、第三者機関の介在なしに各取引の信頼性を保証できるようになっている。こうした技術的特徴を持つブロックチェーンを利用する利点としては、主に以下が挙げられる[8]。

- 全ての情報を集中的に処理・記録する中央集権的なサーバを必要としない（ブロックチェーンでは一部のノードが機能しなくなっても、他のノードが機能していれば処理が続行される）ため、サイバー攻撃やシステムの不具合等によるダウンタイムが発生しない
- ユーザー同士が主体的に全ての取引情報を管理・監視することで情報の透明性を高め、信頼できる情報を永続的に記録できる
- セキュリティ等のシステム面でのコストや取引手数料を低減できる

一方で、ブロックチェーン技術は、ネットワークに参加するノード全てでコンセンサスを取りながら処理が進められる設計となっていることなどを背景に、取引記録が承認・記録されるまでに一定の時間を要するなど、パフォーマンスの低さが欠点の一つとして認識されている。仮想通貨の基盤技術として高い注目を集めているブロックチェーンであるが、近年は様々な業界で同技術の応用可能性を模索する動きが加速しており、その動向については次章で紹介する。

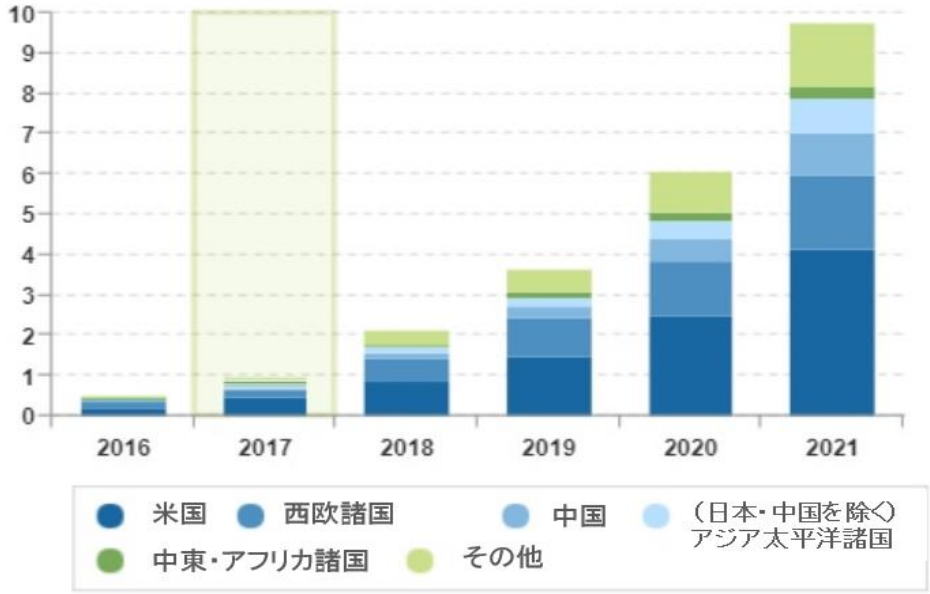
（2） 世界のブロックチェーン市場動向

米 IT 市場調査会社 IDC 社が 2018 年 1 月に発表した世界のブロックチェーンに対する支出（ソフトウェア、国際送金・決済、経路追跡等）予測によると、2018 年の支出額は、2017 年時（9 億 4,500 万ドル）の 2 倍以上となる 21 億ドルとなる見込みであり、世界のブロックチェーン市場は 2016～21 年までの 5 年間で年平均 81.2%のペースで成長し、2021 年には 97 億ドルに達することが予測されている[9]。なお、IDC は同調査において、ビットコイン等の各種仮想通貨に関連する支出は対象に含めていない。

世界のブロックチェーン市場を地域別にみると、2021 年までの予測期間を通じてブロックチェーン支出規模が世界全体の 40%以上を占める米国が最大市場となっており、次に西欧諸国、中国、（日本・中国を除く）アジア太平洋諸国が続く（図表 2 参照）。同調査でカバーされている世界 9 地域において、今後ブロックチェーンに対する大きな支出の伸びが予想されている地域は、南米と日本であり、2016～21 年までの年平均成長率はそれぞれ 152.5%、127.3%となっている。また、業界分野別では、2018 年に最も多くの支出が予想されるのは金融分野（7 億 5,400 万ドル）で、流通・サービス分野（5 億 1,000 万ドル）、製造・資源分野（4 億 4,800 万ドル）におけるブロックチェーン支出が次いで多くなっており、ユースケース別では、金融分野における国際送金・決済と貿易金融及び取引／取引後決済、流通分野におけるロット管理や経路追跡への支出が最も多く、これらのユースケースに対する支出は 2021 年においても最大の支出分野となる見通しである。また、テクノロジー別では、予測期間を通じて IT サービス及びビジネスサービスの支出合計が全体のおよそ 75%を占め、これらのサービス以外では、ブロックチェーンプラットフォームソフトウェアの支出が最も多く、セキュリティソフトウェアと同様、最も成長の著しいカテゴリとなっている。

[6] https://blog.g2crowd.com/blog/trends/cybersecurity/2018-cs/blockchain/
[7] ブロックチェーンでは、直前のブロックをハッシュ関数で暗号化したものを次のブロックに格納する構造になっており、過去のブロックを改ざんするには、それ以降の全ブロックを書き換える必要がある。また、一部のコンピューターで取引データを改ざんしても、データを共有する他のコンピューターとの多数決によって正しい取引データが選ばれる仕組みとなっており、事実上改ざん等の不正を行うことが困難になっている。
[8] https://blockchaintechnologycom.wordpress.com/2016/11/21/advantages-disadvantages/
[9] https://www.idc.com/getdoc.jsp?containerId=prUS43526618

図表 2:世界におけるブロックチェーン支出の推移予測(地域別)(単位:10 億ドル)



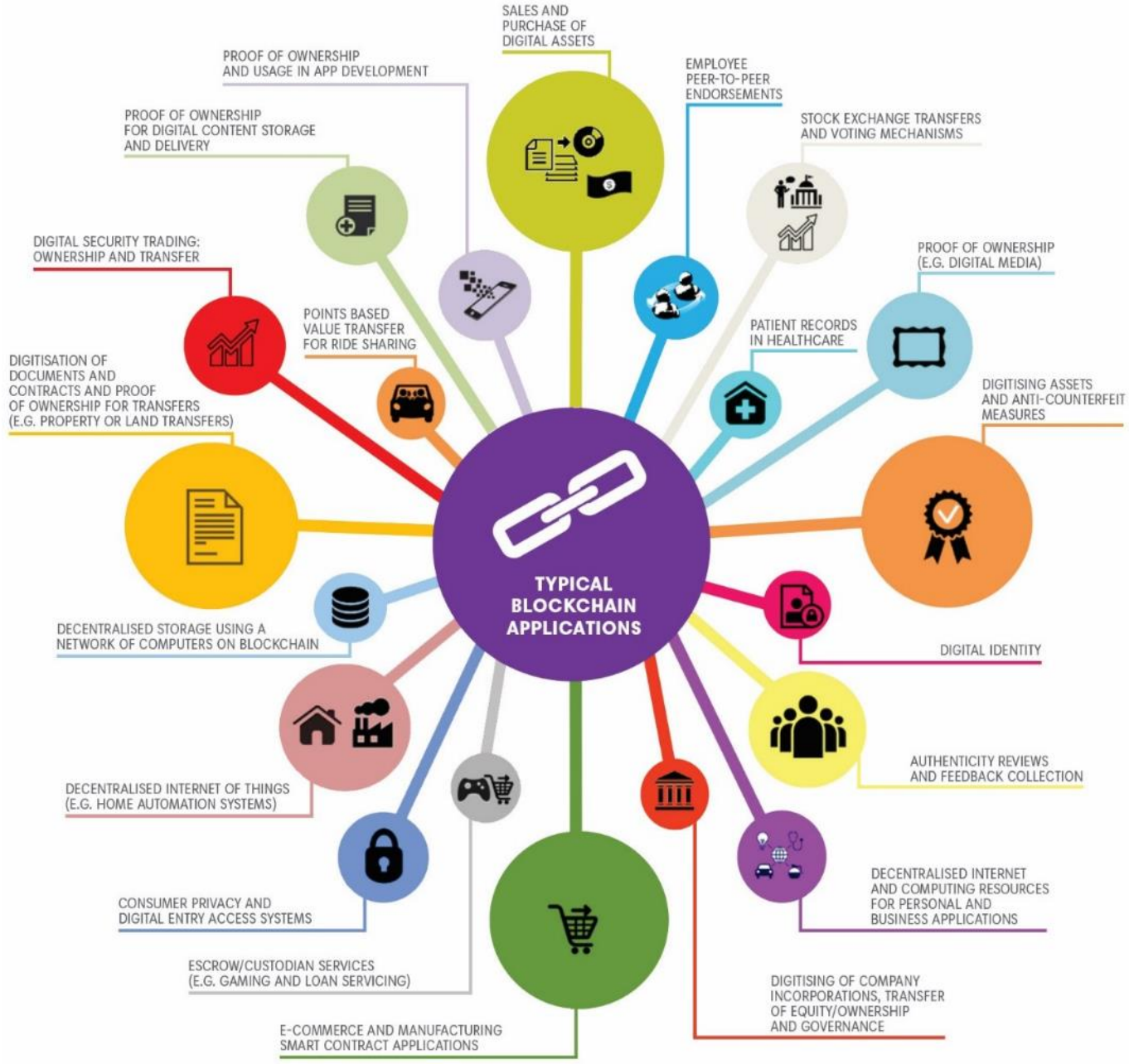
出典:IDC

IDC 社の顧客インサイト・分析担当リサーチマネージャーである Stacey Soohoo 氏は、「2017 年はブロックチェーンの実験的取組みを通じてその技術的利点と課題を企業が認識した年であったが、2018 年は概念実証段階から本格的な導入が行われる飛躍の年となる」とした上で、世界のブロックチェーン市場を牽引する米国では、金融サービスや製造分野のほか、既存業務の効率化や新たな収益創出を狙って他の業界分野における支出も拡大する見込みであり、他の諸外国では今後も米国の動向を注視しながらブロックチェーンプロジェクトへの投資が推進されるとの見通しを示している。

3 ブロックチェーン利用の現状と新たに活用が期待される分野

ブロックチェーンは、ビットコインの取引の安全性を担保するために用いられている革新的な技術として知られているが、低コストで信頼性の高いデータ保存・管理システムを構築できる高い利便性を背景に、近年は金融サービス分野以外への適用も期待されるようになっている。以下では、仮想通貨をはじめとする様々な業界分野において活用されている(又は活用が期待されている)ブロックチェーンの主な適用事例を紹介する。

図表 3:ブロックチェーンの主な応用分野



出典:Grant Thornton[10]

（1） 金融サービス分野

a. 仮想通貨

サトシ・ナカモトが発表した論文を基に 2009 年より運用が開始されたビットコインは、ブロックチェーン技術の最初の活用事例である。運用開始当初は 1 ビットコイン（BTC）当たり 10 セント程度の価値しかなかったが、2012 年以降、取引は次第に拡大し、2013 年に入ってから取引が爆発的に増加、2017 年 12 月にビッ

[10] http://www.grantthornton.com.mt/service/it-and-technology/blockchain-technology/

トコインの価格は過去最高の 1BTC 当たり 2 万ドルを突破するなど、激しく乱高下しながらもその価格は急騰しており話題を集めている。ビットコインは、第三者機関の介在なしに、安全で検証可能かつデータの改ざんが不可能な方法で、円やドル、ユーロなどと同じく、世界中で電子的に商品の購入や取引などを行えるようにすることを目的として作られたものであるが、従来の仮想（デジタル）通貨とは以下の点で異なる[11]。

- *通貨発行上限*― 発行主体のないビットコインでは、プログラム内のコードにより発行上限が 2,100 万枚に定められており、この通貨の発掘は、取引履歴の検証と一定期間の取引履歴をブロックとしてつなげて記録するための「採掘（マイニング）」作業を必要とし、膨大な計算処理が求められる複雑な数学的計算問題をいち早く解いた人（マイナー[12]）への報酬という形で発行される「Proof of Work（PoW）」と呼ばれる仕組み[13]である
- *分散型仮想通貨*― ビットコインの全ての取引記録は P2P 型のオープンな分散ネットワークで管理されており、PoW を通じた各取引履歴をネットワークに参加する誰もが見えるように公開・監視する仕組みにより、電子通貨の二重支払い問題[14]を防いで、一定期間に発生した全ての取引データの整合性を図りながら正確にデータを記録することを可能にしている
- *取引の匿名性*― ビットコインは理論的には個人情報を登録せずに保有・送金を行うことが可能であり、匿名性が高いことが大きな特徴の一つである。一方で、ブロックチェーン上にはユーザーのアドレス間の取引に関する情報が全て記録されており、特定の個人情報とアドレスが結びつけば、アドレスからその人の全ての取引記録を追跡することが可能であるほか、現在、大部分の合法的なビットコイン取引所は、個人情報の登録による本人確認をユーザーに義務付けているため、匿名性はあるようでないというのが実情である
- *取引の不変性*― ネットワークに一度記録されたビットコインの取引データを変更又は取り消すことは不可能である
- *少額決済の実現*― ビットコインには 1 ビットコイン（BTC）よりも小さい単位が存在し、その最小単位である「Satoshi」は 1BTC の 1 億分の 1（1Satoshi=0.00000001BTC）であり、少額決済にも対応できる設計となっている

ビットコインは、取引履歴を秘匿できる利点から、各国の政府・企業・宗教などに関する機密情報公開サイト WikiLeaks の寄付に利用されるなど、当初は一部の闇市場で流通している通貨というイメージが強かった。しかし、同仮想通貨に対する需要がその後大きく拡大した背景には、2008 年のリーマンショックを契機とした経済危機を受けて、世界中で国や銀行に対する信頼が揺らぐ中、こうした発行元のない仮想通貨の取引の利便性と各取引の安全性を担保する仕組みへの信頼性が高まり、既存の管理通貨に代わる通貨として注目されるようになったことが大きな要因の一つであると考えられている。これは、2013 年 3 月に発生したキプロスの金融危機で同国のユーロ離脱が危惧された直後にビットコインの取引が活発化した[15]ことのほか、金融危機下で銀行等の出金制限下にあるギリシャやアルゼンチンにおいて、自己資産を保護するためにビットコインの取引が急増していることからも明らかである[16]。その他、世界規模でビットコインの人気が高まっている理由として、米国や欧州諸国ではビットコインを含む仮想通貨取引に対する消費税を免除してい

[11] https://www.coindesk.com/information/what-is-bitcoin/
[12] マイニングを通じた報酬（新規通貨）の受け取りを目的として、ビットコインの P2P ネットワークに参加し、コンピューターの計算能力をブロックの追記作業に提供する人を指す。
[13] 通貨供給量を安定させ価格の変動を抑制するため、マイニングによる難易度は、その時マイニングに参加している全てのコンピューターの計算力に応じて調整されている。また PoW のシステムでは、ビットコインの採掘量はマイナーの仕事量に応じて上がる仕組みとなっており、高性能コンピューターを数多く導入しその余剰能力を採掘に回すことができれば、理論的には他の人より早く問題を解いて採掘できる量を上げることが可能である一方、こうした高性能コンピューターを継続して稼働することでより多額のコスト（電気代）がかかる。
[14] 電子上で通貨をやり取りする際、データを容易にコピーすることが可能であるため、同一の通貨を異なる相手に再利用することができる。
[15] https://www.theguardian.com/technology/2013/apr/03/bitcoin-reaches-record-high-currency
[16] https://www.thebalance.com/is-bitcoin-the-answer-in-a-financial-crisis-391275

ることや、小売店、レストラン、カフェなど、一般消費者がビットコインを用いて決済できる店舗[17]が増えていることなども挙げられる[18]。

図表 4:ビットコインを巡る主な出来事

出典:The Harriman Stock Market Almanac[19]等の情報を基に作成

ビットコインの成功を機に、ビットコインから分裂して誕生したビットコインキャッシュ(BCH)やネームコイン(NMC)、ライトコイン(LTC)、イーサリアム(ETH)など、世界では様々な機能をもつ仮想通貨(アルトコイン)が作成されており、2018 年 5 月時点において、ビットコインを含む仮想通貨の種類は 1,600 以上に上っている[20]。これらのアルトコインの内、近年特に注目を集めているのが時価総額でビットコインに次ぐ第 2 位の仮想通貨であるイーサリアムである。イーサリアムの特徴は、ブロックチェーンを利用したアプリケーションの作成や、多様な取引に関する契約内容をブロックチェーン上に記録できる「スマートコントラクト(smart contract)」と呼ばれる機能[21]を実現するプラットフォームを提供していることにあり[22]、イーサリアムの機能を利用して生み出された「新規コイン公開(Initial Coin Offerings:ICO)」は、仮想通貨を用いた画期的な資金調達方法として投資家等の間で近年高い関心を集めている[23]。

仮想通貨については、「次世代のお金」と称賛する声から「全くの詐欺」と一蹴する声まで、専門家の間でも評価は分かれている。2017 年における仮想通貨市場は、ビットコインやイーサリアム等の主要アルトコイン

[17] https://99bitcoins.com/who-accepts-bitcoins-payment-companies-stores-take-bitcoins/
[18] https://www.newsbtc.com/2016/02/27/bitcoin-continues-become-increasingly-popular/
[19] http://stockmarketalmanac.co.uk/2017/11/history-of-bitcoin/
[20] https://coinmarketcap.com/all/views/all/
[21] イーサリアムのスマートコントラクト機能では、例えば A が B に対して 10 ドル分のコインを借りた際、金銭上の取引だけでなく、「A は B に 1 年後に 20 ドル分のコインを返済する」といった契約内容もイーサリアム上に記録できる。
[22] イーサリアムのプラットフォーム開発は、2014 年にスイスに設立された非営利組織のイーサリアム財団(Ethereum Foundation)により管理されている。https://www.ethereum.org/
[23] https://www.forbes.com/sites/bernardmarr/2017/12/06/a-short-history-of-bitcoin-and-crypto-currency-everyone-should-read/3/

が史上最高値を記録するなど、活況を呈していたが、2018 年に入ってからビットコインの暴落[24]をはじめ、全体的に下落基調にあり、この理由として英国、米国、日本などで仮想通貨を規制する動きが強まったことが影響したとみられている[25]。仮想通貨の取引量が増加傾向にある中、その投機熱や通貨悪用のリスク等への懸念から、各国で仮想通貨の規制強化への動きが顕著になっており、今後も国際的な規制動向を注視する必要がある。

b. 銀行間取引

仮想通貨の人気の高まりを受けて、金融業界ではその根幹であるブロックチェーン技術の活用を模索する動きが活発化しており、特に、ブロックチェーン技術を用いて国際送金などの金融取引・決済にかかるプロセスを効率化（自動化）し、時間やコストの削減につなげることを狙いとする金融機関向けシステムの構築を目指す取組みが積極的に進められている。

現行の国際送金システムでは、世界中の金融機関に対し通信メッセージの送受信サービスを提供する国際銀行間通信協会（Society for Worldwide Interbank Financial Telecommunication：SWIFT）のネットワークを通じて送金指示が出されるが、SWIFT では送金指示が出されるだけで、国際送金の場合、送金側の金融機関から送金先の金融機関への実際のお金の移動は各機関と取引関係にある複数の中継金融機関を経由して行われ、各機関がそれぞれ管理する異なる台帳で残高の増減を確認しながら、最終的に送金人・受取人の残高を正しく増減する仕組みとなっている。国際送金に平均 3 日間もの時間を要するのは、この複雑なプロセスにあり、各中継機関を経由する際にも異なる手数料が発生する。金融業界では、共通の同じ台帳を分散管理するブロックチェーン技術を導入することで、銀行間で管理するブロックチェーン上で全ての取引履歴を共同で追跡・監視しながら即時に決済を完了することが可能となり、現行の SWIFT 体制下におけるグローバル金融ネットワークのシステム維持・運用にかかる費用をはじめ、少なくとも 200 億ドルのコストを削減できると推定している[26]。

国際送金等の銀行間取引におけるブロックチェーン技術の導入・実用化に向けた取組みの例としては、企業向けブロックチェーンサービスプロバイダの米 Ripple 社[27]や、ニューヨークに拠点を置く米フィンテック企業 R3 CEV 社が主導する金融機関向けブロックチェーンコンソーシアム[28]の活動が挙げられる。Ripple 社は、時価総額でビットコインとイーサリアムに次ぐ第 3 位の仮想通貨「リップル（XRP）」を提供していることで知られているが、同社は幅広い取引に対応できる送金システムの開発に注力しており、業界の期待を集めている。同社は、「RippleNet」と呼ばれる金融機関及び決済企業の分散型グローバルネットワークを開発しており、その中核ソリューションの一つである「xCurrent」は、金融機関の既存の台帳システムに直接統合することで銀行間の双方向通信が可能となり、銀行による国際送金時における送金情報の通知と決済をリアルタイムで実現することが可能である[29]。また、Barclays、J.P. Morgan、UBS、Credit Suisse など、世界的な金融機関 9 行が 2015 年 9 月に共同で立ち上げた R3 コンソーシアムは、金融及び商取引を記録・処理するための分散台帳技術プラットフォーム「Corda」を開発しオープンソース化しており、金融機関やソフトウェア開発者は、同技術を用いて銀行間取引の認証や銀行間取引金利の自動化等の独自のアプリケーション及びサービスを開発することが可能となっている[30]。また R3 は、政府機関によるブロックチェーン技術の容認にも注力しており、ブロックチェーン技術の使用に関する政府コンプライアンスにおいて大転換を図ろうとしている[31]。

[24] ビットコインは 2018 年 2 月、6,000 ドル割れとなる過去最大級の暴落を記録した。
[25] https://cryptocurrencynews.com/price-analysis/bitcoin/bitcoin-price-watch-04-09-18/
[26] https://www.cbinsights.com/research/blockchain-disrupting-banking/
[27] https://ripple.com/
[28] https://www.r3.com/
[29] https://ripple.com/solutions/
[30] https://www.r3.com/technology/
[31] https://techcrunch.com/2018/01/28/bank-based-blockchain-projects-are-going-to-transform-the-financial-services-industry/

Ripple 社と R3 コンソーシアムは、誰もが参加可能な従来のパブリック型ブロックチェーンと異なり、既に信頼関係を確立している金融機関のみが同一の台帳で取引の承認を行う小規模な許可型ブロックチェーン（プライベートブロックチェーン）構造に基づく分散型システムにおいてより迅速かつ効率的に取引を処理することを目指している。Ripple 社と R3 コンソーシアムには、いずれも世界主要銀行を含む多数の大手金融機関などがシステムの実用化に向けて協力しており、今後の動向が注目される。

図表 5：ブロックチェーン技術を活用した効率的な銀行間決済システムの構築を目指す Ripple 社及び R3 コンソーシアムの概要

	Ripple 社	R3 コンソーシアム
設立年	2012 年	2015 年
拠点	カリフォルニア州サンフランシスコ	ニューヨーク州ニューヨーク
提携機関	100 社以上の世界の大手金融機関及び決済企業	世界の大手金融機関、テクノロジー企業、規制当局など 200 以上の組織
主要システム	金融機関及び決済企業の分散型グローバルネットワーク「RippleNet」と、3 種類の中核ソリューション（①「xCurrent—銀行間の送金を効率化するシステム」、②「xRapid—資金の流動性を高めコストを最小限にするシステム」、③「Xvia—法人がウェブ上で重い請求書データを添付して支払いを送金できるグローバル決済システム」）	金融機関向け分散型台帳プラットフォーム「Corda」
最近の主な動き	・2018 年第一四半期に、AK Bank、Axis Bank、UBS、SBI Remittance、Mizuho、Standard Chartered、Santander といった大手金融機関と契約を締結 ・2018 年 3 月、韓国の大手金融機関 Woori 銀行が Ripple 社のソリューションを用いた国際送金テストに成功する ・2018 年 4 月、Apple 社が自社決済サービス「Apple Pay」に Ripple 社の支払システムを採用する	・2017 年 5 月、Bank of America、Merrill Lynch、HSBC 等から 1 億 7,000 万ドルを調達する ・2018 年 3 月、Credit Suisse と ING はフィンテック企業 HQLAx が開発したソフトウェアと R3 のプラットフォームを用いて 2,500 万ユーロの有価証券取引に成功する ・R3 は FX、貿易金融、担保付き貸付及びシンジケートローン市場での Corda プラットフォームの 2018 年内の商用化を目指している

出典：各種資料を基に作成

（2） 金融サービス以外の業界分野

a. ヘルスケア

米国では、経済的及び臨床的健全性のための医療情報技術に関する法（Health Information Technology for Economic and Clinical Health Act：HITECH 法）や米国医療保険制度改革法（Affordable Care Act）により、患者の医療情報の電子化が急速に推進されてきた。しかし、これらの患者の医療データは、様々な医療機関や医師が相互運用性のないデータベースに個別に記録・管理している場合が多く、Premier Healthcare Alliance[32]によると、医療情報システムの互換性の欠如により、毎年 15 万人の患者が生命を失い、医療関係者による 186 億ドルのコスト負担につながっているという[33]。暗号化した分散型の台帳で個々のデータを安全に管理することが可能なブロックチェーン技術は、強力なプライバシー保護体制下における

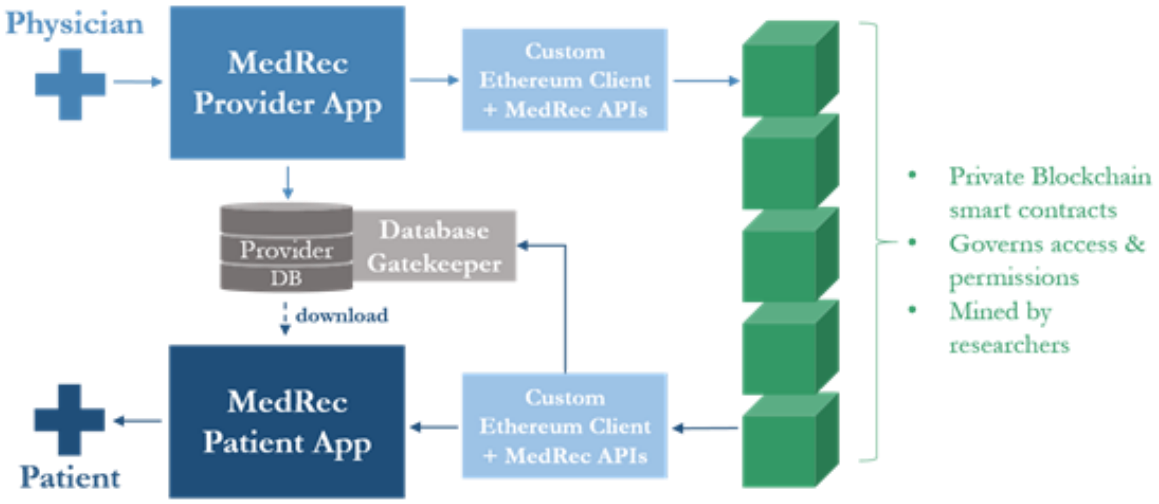
[32]米国のおよそ 3,900 の病院と 15 万を 超える医療関係機関がヘルスケアサービスの向上を目指して結成した組織。 https://www.premierinc.com/about-premier/about-us/

[33] https://www.dr-hempel-network.com/digital_health_events_news/national-blockchain-alliance-for-healthcare/

患者の医療データ管理が求められるヘルスケア業界に大きなメリットをもたらすと考えられており、業界では、医療データの保管にブロックチェーン技術を活用するための取組みが開始されている。

こうした取組みの例として、マサチューセッツ工科大学メディアラボ（MIT Media Lab）とボストンのベス・イスラエル・ディーコネス医療センター（Beth Israel Deaconess Medical Center：BIDMC）が共同で開発し実証実験を進めている「MedRec」プロジェクトが挙げられる[34]。イーサリアムのブロックチェーン（スマートコントラクト）技術を基盤とする MedRec のシステムでは、プライベートブロックチェーン上に患者の医療データは実際に保存されず、様々な医療機関及び医師の既存データベースに保存されている患者の医療データにアクセスするためのインターフェースとして機能する。同システムでは医療データの閲覧及び変更権限を誰に付与するかを患者自身が決定できるようになっており、ブロックチェーン上には医療機関の関係者や患者及びその家族など、許可された人物のデータ閲覧又はデータ変更の履歴が記録される仕組みである。BIDMC の CIO である John Halamka 氏は、「医師がブロックチェーン上で記録したデータポインタは患者の医療データとして記録されることになり、電子カルテシステムの種類は問わないことから、MedRec はシステムの互換性問題への懸念がない」と述べている[35]。また、MedRec システムは、ブロックチェーンの記録を承認するマイナーに医療研究者などを想定しており、マイニングに成功した研究者は報酬として患者（匿名）の医療統計データにアクセスできる設計となっている。

図表 6：「MedRec」のシステムアーキテクチャ



※医師が MedRec の医療サービスプロバイダ向けアプリケーションを通じて患者の医療データを追加すると、当該データが医師の既存データベースに保存され、暗号化されたデータポインタがブロックチェーンに掲示される。患者による医療データへのアクセスは、「Database Gatekeeper」と呼ばれるシステム層を通じてブロックチェーン上でアクセス権の承認処理を行った後、患者が要求した関連データをダウンロードする仕組みとなっている。

出典：MIT Media Lab

MedRec はまだ初期段階のプロトタイプであり、実際のシステム展開の見通しは立っていない。BIDMC では、同システムを用いて 6 カ月間にわたり入院患者と外来患者の血液検査、予防接種履歴、処方箋その他の治療処置に関する医療データを追跡した。MedRec のチームリーダーである Ariel Ekblaw 氏は、この実験では、BIDMC 内にある 2 つのデータベースを用いて医療機関間のデータ交換をシミュレーションし、非常に良好な結果を得られたとしており、今後、より大規模な医療機関ネットワークを持つ病院でさらなる実証実験を進める計画であるという[36]。

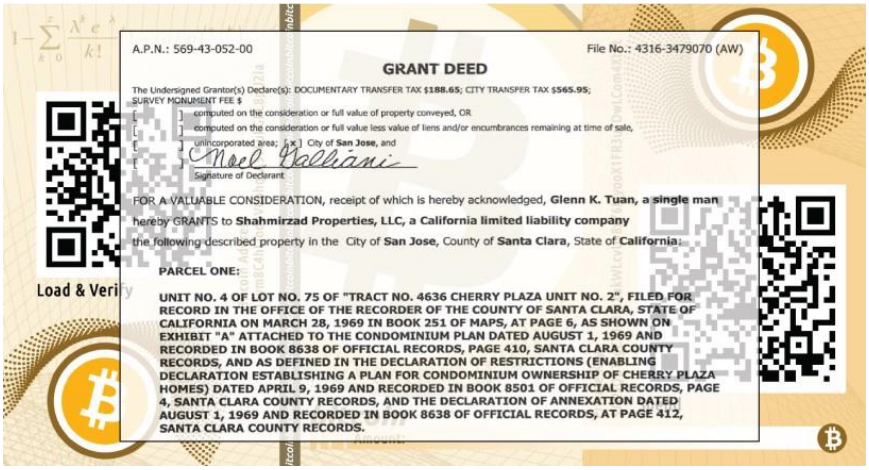
[34] https://viral.media.mit.edu/pub/medrec
[35] https://www.technologyreview.com/s/608821/who-will-build-the-health-care-blockchain/
[36] https://www.wired.com/2017/02/moving-patient-data-messy-blockchain-help/

b. 不動産

米国では、不動産の譲渡証書（deed）や石油・ガスの採掘権申請、賃貸契約書などの土地利用に関する記録は、全米の 3,000 以上の郡庁舎及び市役所が保存しており、書類をスキャンしてデジタル化されているものもあるが、古い記録文書を中心に大部分の不動産取引は紙ベースの書類に依存している。そのため、土地の所有権を有する人物を把握することが非常に困難な場合があり、記録エラーや詐欺の可能性など、多くの問題が存在する。ビットコイン等の仮想通貨の取引履歴を記録・追跡できるブロックチェーン技術を不動産の取引記録に応用し取引記録を電子的に管理することで取引の透明性が高まり、こうした問題の改善と、取引・記録にかかるコスト削減につながると考えられている[37]。

520 万人の住民が暮らすイリノイ州シカゴのクック郡証書記録管理局（Cook County Recorder of Deeds：CCRD[38]）は、不動産ブロックチェーンの技術開発を手がけるスタートアップ米 velox.RE 社[39]と共同で、ブロックチェーン上で不動産取引における権利移譲の履歴を記録する試験プロジェクトを 2016 年 10 月から 8 カ月間にわたり実施した。ブロックチェーン技術を用いたこの試験プロジェクトは、全米の郡で初のケースであり、業界団体の国際ブロックチェーン不動産協会（International Blockchain Real Estate Association：IBREA）や不動産の権利サービス企業である Armour Settlement Services 社、国際法律事務所の Hogan Lovells なども参加している[40]。米国の不動産取引は、まず、不動産資産の譲渡が売り手と買い手の間で直接行われ、その後、買い手は当該不動産の譲渡証書を郡の証書記録管理局に提出し、公文書として記録されるという 2 段階のプロセスを経るのが一般的である。同プロジェクトでは、Velox.RE 社が独自に実装しているカラード・コイン（colored coin）[41]向けソフトウェアを用いて、不動産資産を記録したデジタル不動産譲渡証書として機能するカラード・コインを発行し、ビットコインのネットワークで売り手と買い手がコインの取引を行い、その取引の承認及び記録がブロックチェーン上で自動的に処理されるかがテストされた[42]。

図表 7：ビットコインのペーパーウォレットに統合されるデジタル不動産譲渡証書（データ）のイメージ図



出典：Medium

[37] https://www.fastcompany.com/40449268/will-blockchain-revolutionize-global-real-estate-next
[38] CCRD は全米で 2 番目に大きい組織である。
[39] https://www.velox.re/
[40] https://bitcoinmagazine.com/articles/chicago-s-cook-county-to-test-bitcoin-blockchain-based-public-records-1475768860/
[41] 「カラード・コイン」は、ビットコインのブロックチェーン上に、ビットコインの取引記録以外の付加情報を記録できるレイヤ（層）を活用し、金・株式・証券をはじめとするビットコイン以外の様々な資産の取引データの記録を実現することを目的に開発されたアーキテクチャで、「オープンアセット・プロトコル（Open Assets Protocol）」と呼ばれるシステムを用いて様々な価値を記録した独自コインを発行し、ビットコインのブロックチェーン上で取引できる仕組みとなっている。
[42] https://medium.com/@RagnarLifthrasir/permissionless-real-estate-title-transfers-on-the-bitcoin-blockchain-in-the-usa-5d9c39139292

Velox.RE 社によると、同プロジェクトにおいて、プロジェクトの参加機関の間で合意された法・プロセス・システム条件などを全て満たした上で、シカゴの商用不動産業者がハードウェア型のビットコインウォレット「Trezor」などを用いて財産移譲を行うことに成功したとしている。ブロックチェーン技術を不動産取引における権利移譲に応用するメリットは高いが、システムの完全な実用化には、各不動産の所有権の変遷記録をすべて電子化してデータベースに統合することや、州法及び各管理局における取引慣行を変える必要があり、全米レベルでのシステム運用にはまだ時間がかかるとみられている[43]。

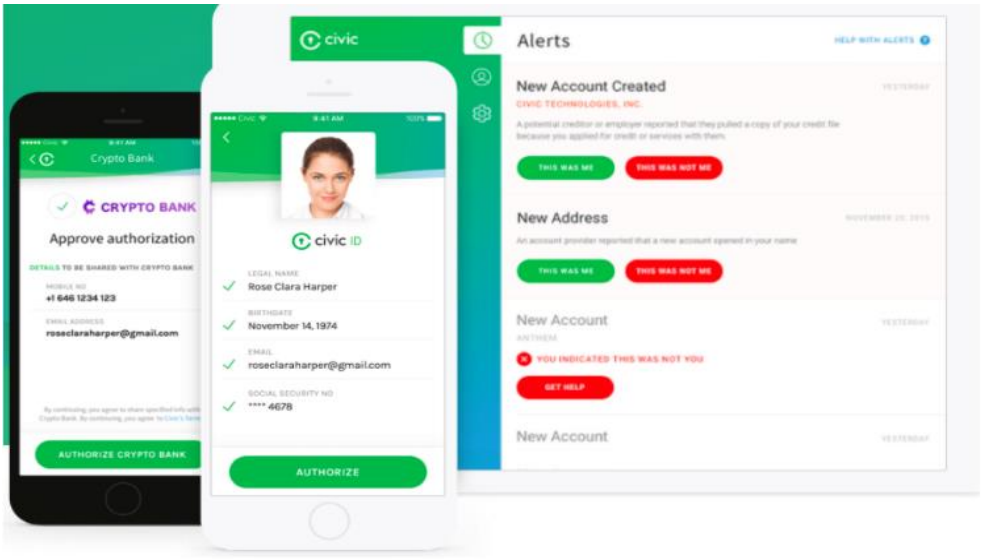
c. サイバーセキュリティ

ヒューマンエラー等による情報漏洩リスクへの懸念が高まる中、記録データの不変性や、あらゆるデータを仲介者なしに共有・分散管理する方式、改ざんがほぼ困難であるといった特徴を持つブロックチェーンは、サイバーセキュリティ分野における理想的な基盤技術の一つとして、技術の応用可能性に期待が集まっている[44]。デジタル ID 管理／認証ソリューションはその代表的な例であり、最近では Microsoft 社が分散型 ID システムの開発を推進することを発表し[45]、話題を集めている。ブロックチェーン技術を用いた新たなデジタル ID システムでは、ID 情報を集中管理する企業・組織が不要となり、ユーザーは、個人情報に誰がアクセスできるかを自ら管理し、パスワードや他の個人認証情報を入力する必要なく、自身で本人確認に必要な身分証明を行う「自己証明型身分証明（self-sovereign identity）」システムの実現が想定されている[46]。

ブロックチェーンを基盤とするデジタル ID プラットフォームの開発を手がける企業には、シリコンバレーに拠点を置くスタートアップ Civic 社[47]が挙げられる。同社のプラットフォームは、デジタルウォレットと同様、専用のアプリケーションを通じてスマートフォンに社会保障番号やパスポート、免許証等の身分証明書情報を含む個人情報をデジタル ID データとして一括保存し、ユーザーはバーチャル ID カードとして機能する同アプリケーションを通じて、異なるサービスプロバイダーが必要とする認証情報を効率的に提供できるようになっている。スマートフォン端末に保存される個人情報は暗号化されており、そのアクセス保護には（ユーザー名とパスワードではなく）指紋認証が用いられている。また、アプリケーションを介して ID 情報が使用された際にはユーザーに通知することで、ユーザーはリアルタイムで ID 情報を保護・許可することが可能であるほか、Civic 社はクレジットレポートのアラートやなりすまし被害、24 時間年中無休での詐欺被害サポートなども提供している[48]。

[43] https://www.fastcompany.com/40449268/will-blockchain-revolutionize-global-real-estate-next
[44] https://thenextweb.com/contributors/2018/03/20/cyber-security-blockchain-evolving-technology-safety/
[45] https://cloudblogs.microsoft.com/enterprisemobility/2018/02/12/decentralized-digital-identities-and-blockchain-the-future-as-we-see-it/
[46] https://www.forbes.com/sites/rogeraitken/2018/01/07/blockchain-to-the-rescue-creating-a-new-future-for-digital-identities/#5c725cb25492
[47] https://www.civic.com/
[48] https://medium.com/@VerthagOG/civic-investment-analysis-a46a668fb89f

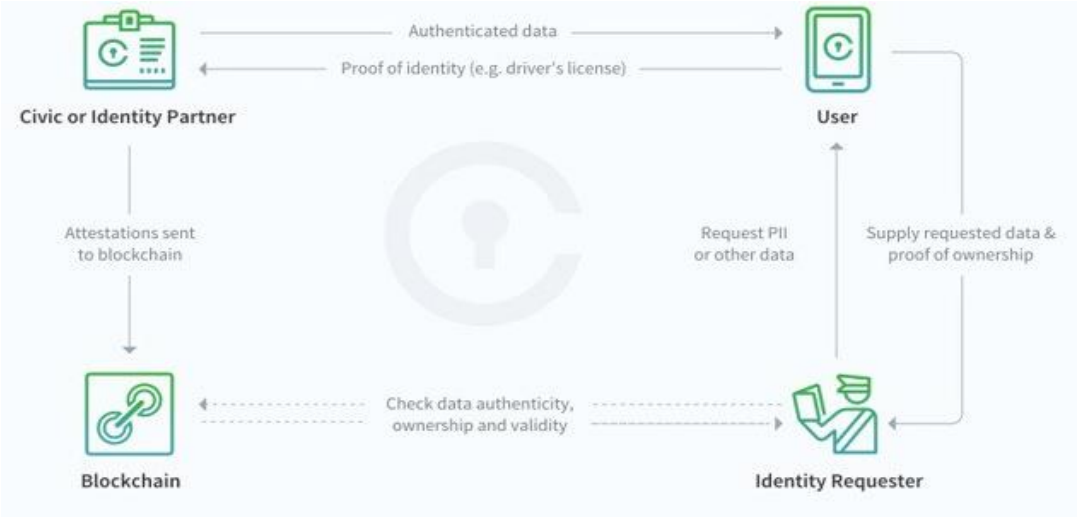
図表 8：Civic 社の「Secure ID」モバイルアプリケーション



出典：Medium

Civic 社のデジタル ID 管理プラットフォームでは、ユーザーにより ID 情報が登録されると、当該情報が政府機関又は ID 認証サービス機関等により送られ、認証が完了すると、パブリックブロックチェーン上に暗号化された ID 認証証明記録が追加される。そして、ユーザーは、銀行やホテルなど、ユーザーの身分証明が必要なビジネスサービスプロバイダーに特定の情報を共有することが可能であり、サービスプロバイダーによるデータ受信が完了すると、ユーザーとサービスプロバイダーとの ID 情報の取引記録がブロックチェーン上に記録される仕組みとなっている。

図表 9：Civic 社のデジタル ID 管理プラットフォームの仕組み



出典：Medium

Civic 社の創設者兼 CEO である Vinny Lingham 氏は、「社会保障番号等の消費者の個人情報の利用について責任ある企業は、当該情報が使用された際に持ち主にその旨を通知しなければならない」としており、同プラットフォームを企業が利用する利点として、リアルタイムで各個人情報の活用状況を把握できるシス

テムにより、なりすましなどの詐欺行為を即座に検知できることを挙げている[49]。Civic 社のプラットフォームは、KYC（Know Your Customer）規則[50]に基づいて、新規に口座を開設する顧客の十分な身元確認を行うことが義務付けられている銀行など、サービスプロバイダーの身元確認プロセスにかかる時間とコストを大幅に軽減できることが期待されており[51]、身分証明が必要なあらゆる企業・組織と提携し、パートナーシップネットワークを拡大することを目指している。

d. IoT

様々な業界分野に革新をもたらすことが期待されているモノのインターネット（Internet of Things：IoT）であるが、膨大なデータ処理能力とストレージ容量を持つクラウドサーバーを通じてネットワークにつながる全てのデバイスの識別や認証を行う現行の中央制御型システムでは、巨大なサーバーファームやネットワーク機器などのインフラ構築・維持に高いコストがかかり、1 箇所で生じた障害がネットワーク全体をダウンさせる可能性があることなどが主な課題として認識されている。ブロックチェーン技術を用いた分散型システムは、ネットワークに接続する各デバイスが相互に情報を共有し、自律的に連携・動作することが可能になることから、IoT との親和性が高く、IoT ネットワークにつながるデバイスが増えても、ネットワークを構成する各デバイスに必要な処理能力とストレージ容量を分散させられることから、巨大なデータセンターを新設することなく、インフラにかかるコストを大幅に削減することが可能であり、システムダウンのリスクも低い。また、ビットコインで証明されている強固なセキュリティシステムにより IoT の抱えるセキュリティ問題にも対応できると考えられている[52]。

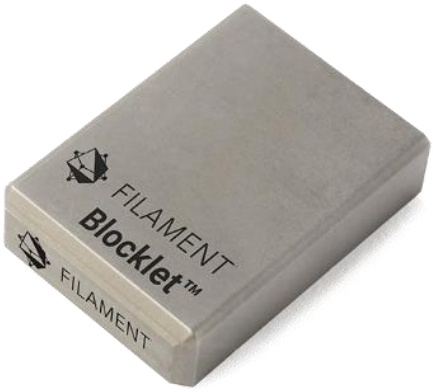
IBM 社や SAP 社など、IoT 事業に積極的に投資している大手 IT 企業は、ブロックチェーン技術を IoT プラットフォームに統合したソリューション開発に注力するようになっている[53]一方、一部のスタートアップにおいても、IoT のブロックチェーンに特化したソリューションを開発する企業が出現している。ネバダ州リノ（Reno）に拠点を置く Filament 社[54]はこうしたスタートアップの一つで、産業用機器メーカーを主な対象とした IoT のブロックチェーンハードウェア／ソフトウェアの開発を手がける。インターネットに接続されていないオフライン環境でも、IoT デバイスが自律的に相互通信を行える分散型 IoT プラットフォームの開発に注力してきた同社は 2018 年 1 月、産業用機器や輸送コンテナなどを相互に接続し、ブロックチェーン上での通信を可能にする新マイクロチップ「Blocklet Chip」のベータ版を発表した[55]。同チップにより、ネットワークに接続されたデバイスが自律的に通信し、運用者が設定した規則とプロセスに基づいてコントラクトを作成し、ブロックチェーン上に記録することが可能となる。例えば、輸送コンテナが港から倉庫に運ばれるまでの輸送経路上の位置情報が自動的に記録・共有されることで輸送プロセスの透明性を高めることや、工場などの製造機器が古くなった部品を交換しパフォーマンスを上げるために自動で部品の注文を行うことなどが実現できる見込みであるという[56]。

また Filament 社は 2018 年 5 月、同チップを基盤とする USB デバイスを発表した。同社の CEO である Allison Clift-Jennings 氏は、「産業部門の事業者の多くは十年以上の耐用年数を想定して構築した設備機器を用いており、（USB ポートを搭載した）既存のデバイスへの導入を容易に行える Blocklet USB デバイスにより、事業者は各デバイスや自動化されたスマートコントラクトベースのシステムとの相互通信が可能に

[49] https://techcrunch.com/2016/07/19/civic-launches-a-free-service-that-aims-to-stop-identity-theft-before-it-happens/
[50] マネー・ロンダリング等のリスクを防ぐため、顧客の本人特定事項のほか、事業及び金融取引の内容、預金や送金原資について把握するための一連のプログラム。
[51] https://www.coinbureau.com/review/civic-cvc/
[52] https://techcrunch.com/2016/06/28/decentralizing-iot-networks-through-blockchain/
[53] https://blog.g2crowd.com/blog/trends/cybersecurity/2018-cs/blockchain/
[54] https://filament.com/
[55] https://globenewswire.com/news-release/2018/01/16/1289884/0/en/Filament-Introduces-Next-Generation-Blockchain-Technology-Transforming-Connected-Industrial-and-Enterprise-Devices.html
https://internetofthingsagenda.techtarget.com/news/252435289/Blockchain-and-IoT-edge-connected-by-Filament-chip
[56] http://www.businessinsider.fr/us/startup-filament-new-chip-connects-blockchain-to-the-iot-2018-1

なり、デバイスの価値を即座に高めることができる」と述べている。同社によると、Blocklet USB デバイスは、2018 年 6 月にベータテスト／パイロットプロジェクト向けに利用可能となる見込みである[57]。

図表 10：Filament 社の「Blocklet Chip」を基盤とする USB デバイス



出典：Filament[58]

4　米国におけるブロックチェーン規制の動向

（1）　連邦政府レベルでの動き

ブロックチェーン技術について連邦法で規制する動きなどはこれまでみられていない。トランプ政権内では 2017 年 9 月、米行政管理予算局（Office of Management and Budget：OMB）の連邦 CIO 代理の Margie Graves 氏（当時）が、「AI とブロックチェーンは連邦制に大きなメリットをもたらす可能性のあるテクノロジーである」と発言[59]するなど、トランプ政権はブロックチェーン技術の活用に積極的に取り組んでいる[60]。一方で、ビットコインをはじめとする仮想通貨の価値が急騰し一般の関心が高まる中、匿名性の高い仮想通貨がマネー・ロンダリングやテロ組織への資金源、租税回避、詐欺等に悪用されることを懸念し、連邦政府レベルでは、各関連規制当局において仮想通貨に対する規制を見直す動きがみられるようになっている。

図表 11：仮想通貨規制に対する各連邦規制当局の立場と関連動向

規制当局	仮想通貨規制への立場及び関連動向
証券取引委員会（SEC）	・ SEC は仮想通貨（又は仮想通貨関連資産）ETF（上場投資信託）を含む上場投資商品（ETP）の上場又は取引を承認していない ・ SEC は新規コイン公開（ICO）について「公正かつ合法的な投資機会となる一方で、不適切な資金調達に用いられる可能性があるとして投資家に注意喚起を行っており、ICO 詐欺の取り締まりを強化している。SEC 委員長 Jay Clayton 氏は、ICO を証券として規制（ICO は SEC に登録）すべきとの立場を示している

[57] https://www.enterprisetech.com/2018/05/14/iot-blockchain-merge-in-usb-device/
[58] https://filament.com/products/
[59] https://www.coindesk.com/trump-white-house-doubles-us-commitment-blockchain/
[60] また、トランプ大統領は 2017 年 12 月に署名した総額 7,000 億ドルに上る防衛支出法案において、ブロックチェーンをはじめとする分散型データベース技術を連邦政府システム及び重要インフラのサイバーセキュリティ強化に用いる研究を義務付けている。https://www.coindesk.com/trump-signs-defense-bill-authorizing-blockchain-study/

商品先物取引委員会（CFTC）	・ CFTC は、ビットコイン等の仮想通貨をコモディティ（商品先物取引所で取引される商品）と認定し、仮想通貨の先物取引と派生商品の取引は CFTC の規則に基づいて監督管理を受ける必要があるとの立場を表明している ・ CFTC は米先物取引所運営大手 CME グループと、シカゴ・オプション取引所を運営する CBOE グローバルマーケッツに、ビットコインの先物上場を認める決定を下しているほか、デリバティブ商品取引プラットフォームを提供する米 LedgerX 社を初のビットコインオプション取引決算機関に認定している
米財務省	・ 財務省監察官は、仮想通貨がマネー・ロンダリングやテロリストの資金源に利用される可能性があることから、米金融犯罪取締ネットワーク（Financial Crimes Enforcement Network；FinCEN[61]）による仮想通貨対策を見直す考えを明らかにしている[62] ・ Steven Mnuchin 財務長官は、ビットコイン等の仮想通貨の動きに注目してワーキンググループを結成し、その悪用の可能性や投機リスクなどを主な問題として認識しているとコメントしている
内国歳入庁（IRS）	IRS は、仮想通貨を「財産・資産」と定義し、1 年以上保有された仮想通貨の売却・使用時にその値上がりによる収益を得た場合、キャピタルゲイン税の課税対象としている

出典：MarketWatch[63]等の情報を基に作成

米国の仮想通貨規制においては、特に、ICO により発行された仮想通貨を証券として規制すべきとして取り締まりを強化する証券取引委員会（Security Exchange Commission：SEC）と、仮想通貨をコモディティと位置付ける商品先物取引委員会（Commodity Futures Trading Commission：CFTC）の動きが注目されている。SEC の Robert Jackson 委員は 2018 年 4 月末、ICO に関して、SEC では投資家の保護を最優先に、今後仮想通貨への投資活動を証券取引法に準拠させる[64]考えであることを明らかにしている[65]。また、過度の規制には消極的な立場をとる CFTC[66]は、仮想通貨に関連した詐欺行為や市場操作などの問題に対応するため、SEC と協力する必要性を強調しており、CFTC の Brian Quintenz 委員によると、両機関では関連する規制監督権を調整する取組みが進められているという[67]。

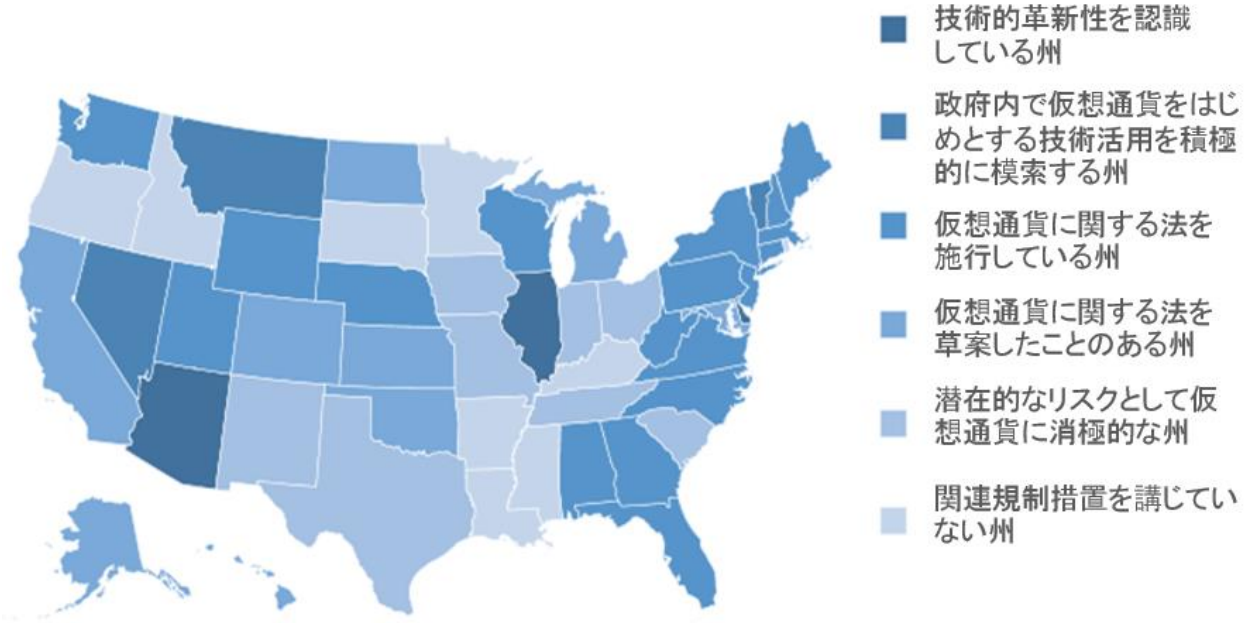
米議会は 2018 年 3 月、米国経済に影響を及ぼす重要な要素や変化について取りまとめた「年次合同経済報告書（2018 Joint Economic Report[68]）」を発表したが、同報告書では初めて 1 章分が仮想通貨とブロックチェーン技術に関する内容に割かれたことで話題を呼んだ[69]。同報告書は、ブロックチェーン技術が仮想通貨のみの活用にとどまらず、ヘルスケアやサイバーセキュリティなどの他の分野に応用することでより大きな経済効果を生むことを認識する一方、複数の規制当局が仮想通貨を個別に定義し混乱を招いていることから、規制の協調を進めることを奨励している[70]。

[61]米財務省の下部組織で、マネー・ロンダリングに関する資金情報機関。
[62] FinCEN の仮想通貨の管理、交換、又は使用に対する規制の適用に関する 2013 年のガイダンス（FIN-2013-G001）では、「仮想通貨はいかなる法的管轄領域においても法定通貨として認められていない」としている。
[63] https://www.marketwatch.com/story/heres-how-the-us-and-the-world-are-regulating-bitcoin-and-cryptocurrency-2017-12-18
[64] Jackson 委員は、これは、さらなる規制及び ICO の禁止を意味するものではないことを強調している。
[65] https://www.cnbc.com/2018/04/30/sec-is-cautious-but-open-to-crypto-fundraising-commissioner-says.html
[66] CFTC の J. Christopher Giancarlo 委員長は、2018 年 2 月に上院で開かれた仮想通貨に関する公聴会で、「ビットコインがなければ分散型台帳技術も存在し得なかった」と発言し、連邦レベルでの仮想通貨規制の策定は関連リスクに対して慎重に調整することが必要との見解を示している。https://www.coindesk.com/cftc-chair-us-tread-carefully-crypto-exchange-rules/
[67] https://www.coindesk.com/cftc-officials-want-close-cooperation-sec-crypto-rules/
[68] https://www.congress.gov/115/crpt/hrpt596/CRPT-115hrpt596.pdf
[69] https://cointelegraph.com/news/us-congress-includes-crypto-in-its-joint-economic-report-for-the-first-time
[70] https://blog.volkovlaw.com/2018/03/congress-and-the-blockchain-the-2018-joint-economic-reports-discussion-on-cryptocurrency/

（2） 州政府レベルでの動き

州政府レベルでは、これまでに大多数の州が仮想通貨及びブロックチェーン技術に関する何らかの法規制を施行又は整備しつつあるが、こうした規制のほとんどは、既存の送金法における仮想通貨の取引について明確にする内容である。米シンクタンクのブルッキングス研究所（Brookings Institution）が 2018 年 4 月に発表した米州政府のブロックチェーン規制に関する調査結果によると、米国では、2014 年頃から 20 以上の州で仮想通貨関連の規制措置が講じられると同時に、カリフォルニア州やニューメキシコ州など 10 以上の州で仮想通貨への投資に警告を発する例がみられるようになった。そして、ここ 2 年の間に、仮想通貨にとどまらず、ブロックチェーン技術に焦点を当て、公共／民間サービスへの技術応用の可能性を探る州も出始めている[71]。

図表 12：米各州におけるブロックチェーンに対する規制等の対応状況



出典：Brookings Institution

ニューヨーク州では、記録用途などにブロックチェーン技術を採用する州法は制定されていないが、ニューヨーク州金融サービス局（New York State Department of Financial Services：NYDFS）は 2015 年 6 月、仮想通貨がマネー・ロンダリングや違法取引に用いられることを防ぐため、同州の全ての仮想通貨関連企業[72]を対象とする営業許認可制度「ビットライセンス（BitLicense）」を他の州に先駆けて導入・施行した。同制度については、ビットライセンスの取得には、高額の申請費用（5,000 ドル）のほか、詐欺防止やマネー・ロンダリング対策、サイバーセキュリティ、プライバシー・個人情報保護など厳しい取得条件を満たす必要があり、企業にかなりの負担を強いるものであることから、これまでに認可を受けた企業はごく少数で[73]、Bitfinex 社や Shapeshift 社等の大手取引所が同州から次々と撤退する結果を招いており、批判も多い[74]。

[71] https://www.brookings.edu/blog/techtank/2018/04/17/blockchain-and-u-s-state-governments-an-initial-assessment/
[72] ニューヨーク州在住者に対し通貨交換等の仮想通貨ビジネスを行う全ての企業が対象となる。
[73] これまでにライセンスを認められた企業は、米仮想通貨決済事業者 Circle 社、Ripple 社、米仮想通貨取引事業者 Coinbase 社、bitFlyer 社の米国法人の 4 社である。
[74] https://www.coindesk.com/contortions-compliance-life-new-yorks-bitlicense/

一方で、2017 年には、バーモント州、アリゾナ州、メーン州、ネバダ州など 8 州で仮想通貨及びブロックチェーン技術の利用を推進する法の策定・施行を目指す動きがみられている[75]。特に重要な動きとしては、アリゾナ州で 2017 年 3 月、ブロックチェーンとスマートコントラクトを法的に定義し、ブロックチェーン化されたすべてのデータを正式な電子記録とみなす法が施行されている[76]ほか、バーモント州においても同年 6 月、ブロックチェーン化されたデータを法的効力のある正当な記録として法廷で承認する法が施行されている[77]。また、デラウェア州では、2016 年にブロックチェーンイニシアチブを立ち上げ、Fortune 500 企業の 60%以上が拠点を置き、多数のスタートアップが集結する同州において、Jack Markell 州知事の下、ブロックチェーン及びスマートコントラクト技術の政府及び民間セクタにおける採用と技術発展に積極的に取り組んでおり、同年 7 月、州内の企業がブロックチェーン技術を用いて記録管理や株式の取引を許可する州法改正案が可決されている[78]。

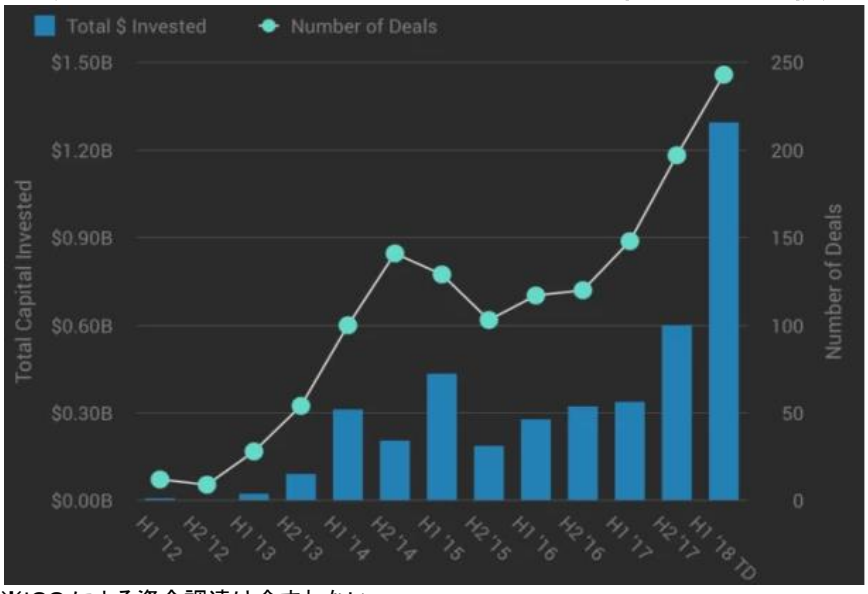
このように、米国では、各州が個別に仮想通貨やブロックチェーンを規制している状況にあるが、統一州法委員会（Uniform Law Commission：ULC[79]）は 2017 年 7 月、仮想通貨に関する州法間の整合性を図るため、「仮想通貨事業法に関する統一規則（Uniform Regulation of Virtual Currency Businesses Act）」を発表した[80]。ULC が 2014 年からおよそ 2 年間にわたる作業期間を経て完成させた同規則は、ライセンスが必要な送金事業を営む仮想通貨関連事業者をより明確に定義しているほか、3 階層のライセンス構造を提案し、大手事業者には完全なライセンス取得を義務付ける一方、個人及び小規模事業者はライセンスを免除、年間収益 3 万 5,000 万ドル未満のスタートアップには規制のサンドボックス[81]を設けている。実際に同規則を州法に適用するかは各州の判断に委ねられており、ULC の顧問を務める米国法曹協会（American Bar Association）の Stephen Middlebrook 氏は、「同統一規則が出されるまで州法の制定を保留していた州が複数あり、それなりに高い需要がある」との考えを示している。これに対し、ビットコインの世界的な普及を目指す非営利機関であるビットコイン財団（Bitcoin Foundation）は、同規則の内容がニューヨーク州のビットライセンス規制と酷似している悪法として、州議会議員・関係者から構成される全米州議会議員連盟（National Conference of State Legislatures：NCLS）に対し、これを採択しないよう呼びかけており[82]、仮想通貨に関連した規制をこれまで策定していない州や業界への影響が注目される。

5　今後の展望と日本への示唆

ビットコインの成功で一躍脚光を浴びたブロックチェーン技術は、現代の経済、法、政治システムを支える契約や取引及びその記録方法に変革をもたらし、様々な業界分野での応用が期待されている。こうした期待の高さを背景に、世界のベンチャーキャピタルからブロックチェーン関連企業への投資額は近年増大傾向にあり、2018 年における投資額は、5 月半ば時点で 2017 年の総額を上回るおよそ 13 億ドルに達しており、前年の実績をはるかに上回る見通しである（図表 13 参照）[83]。

[75] https://bravenewcoin.com/news/us-states-working-on-blockchain-legislation-in-2017/
[76] https://legiscan.com/AZ/text/HB2417/2017
[77] https://buckleysandler.com/blog/2017-06-14/vermont-governor-enacts-law-including-blockchain-application
[78] https://www.coindesk.com/delaware-house-passes-historic-blockchain-regulation/
https://www.coindesk.com/delaware-introduces-bill-legally-recognize-blockchain-stocks/
[79]州法間で不明瞭な規定部分について明確化し、法的安定性を確保するため 1892 年に設立された非営利機関。全米の弁護士およそ 350 名から構成されている。
[80]http://www.uniformlaws.org/shared/docs/regulation%20of%20virtual%20currencies/2017AM_URVCBA_AsApproved.pdf
[81] 規制のサンドボックス（regulatory sandbox）とは、革新的な新事業の創出を後押しするための規制緩和策のこと。
[82] https://www.coindesk.com/a-bitcoin-law-for-every-state-appetite-and-animosity-greet-model-us-regulation/
[83] https://techcrunch.com/2018/05/20/with-at-least-1-3-billion-invested-globally-in-2018-vc-funding-for-blockchain-blows-past-2017-totals/

図表 13:世界のベンチャーキャピタルによるブロックチェーン関連企業への投資状況推移



※ICO による資金調達は含まれない。

出典:TechCrunch

Facebook 社による個人データの不正流用問題[84]を受け、中央集権的な管理者が存在せず、取引データをユーザー同士が独自に管理できるブロックチェーン技術が最近新たに注目を集めている[85]。一方で、ブロックチェーンがメインストリームの技術として普及し、一般に活用されるようになるまでにはいくつかの課題が指摘されており、業界関係者の中には、現在のテクノロジーの欠点に作用する万能薬であるかのように、その技術活用に過度な期待と信頼を抱くことに警鐘を鳴らす声もある。ブロックチェーンの開発者が指摘する同技術の課題には、主に以下が挙げられる[86]。

- ***スケーラビリティ問題***— 2017 年末にビットコインの取引量が大幅に増大した際、取引処理プロセスの遅延が大きな問題となったが、ビットコインに用いられているブロックチェーン技術は情報量が急激に増えると、採掘のシステムが処理に追いつけず、処理速度の低下及び送金遅延などの事態が発生することが問題の一つとして認識されている。従来のデータベースシステムと比べ、ブロックチェーン技術は膨大なコンピューティングリソースを必要とし、大量のコンピュータハードウェアシステムとシステム動作に必要な電力に高いコストがかかる。また、一般的な企業が必要とするデータ容量はビットコインのブロックチェーン容量(およそ 150GB)をはるかに上回ることから、現時点では、大規模なデータベースに代わるソリューションではないとの見方もされている
- ***セキュリティ上の問題***— 透明性の高い安全な取引を行える技術として注目されるブロックチェーン技術であるが、個人情報や機密データを保存できる強固なセキュリティ機能を備えた成熟した技術ではないことから、その用途にはまだ限界がある
- ***技術的な複雑性***— 他のデジタルプラットフォームと比較して、ブロックチェーン技術を用いたサービス/ツールは、ユーザー側により多くの技術的知識が求められ、ソフトウェア開発等のテクノロジー分野に精通していないユーザーがビットコイン及びブロックチェーンの仕組みを理解することは容易でない。仮想通貨の不正流出等が紙面を賑わせる中、一部の取引所などでのセキュリティ問題がブ

[84]米ニューヨークタイムズ紙と英オブザーバー紙は 2018 年 3 月、2016 年の米大統領選で、共和党のドナルド・トランプ大統領候補(当時)が契約していた英政治データ分析企業 Cambridge Analytica 社が、同大統領候補を当選させるため、Facebook の米国人ユーザー5,000 万人以上の個人情報を収集、不正利用していたことを暴露し、一大スキャンダルに発展した。

[85] https://www.cnbc.com/2018/03/21/facebooks-pain-could-be-blockchains-gain-analyst.html

[86] https://www.digitaltrends.com/computing/blockchain-problems-how-to-solve-issues-with-the-latest-vogue-tech/

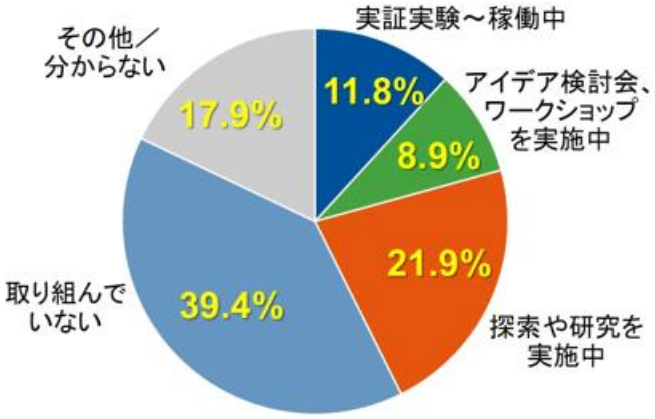
ロックチェーンに対する悪いイメージを植え付け、将来的な技術普及を妨げる要因となる可能性が懸念されている

- ***ガバナンスの必要性***— 集権的な第三者機関を不要とする点がブロックチェーンの大きなメリットの一つとして認識されている。しかし、特定の技術的知識を持たないユーザーが、ICO など、同技術を基盤とするサービスを信頼して使うようになるには、規制当局による一定の標準策定及び制御が必要であると考える技術開発者が増加傾向にある

日本においては、2018 年 3 月末時点で、少なくとも 350 万人が国内の 17 の取引所で仮想通貨の取引を行っており、国内におけるビットコインの取引量は 2014 年 3 月時の 2,200 万ドルから 2017 年 3 月には 970 億ドルに達するなど、仮想通貨ブームが続いており、米 Fortune 誌は日本を「仮想通貨取引の主要中心地」と評している[87]。こうした仮想通貨の取引が活発化する中、2018 年 1 月に発生したコインチェック取引所における仮想通貨システムの脆弱性を突いたハッキング事件（被害額およそ 580 億円）、5 月 13～15 日にかけて発生した国産仮想通貨「モナコイン（MONA）」のブロックチェーンのマイニングに対する攻撃（被害額およそ 1,000 万円）など、ハッキングの懸念が広がっている。特にモナコインのハッキング事件は、ビットコインと同じ仕組みのブロックチェーンの改ざんを可能にする「Selfish Mining（又は Block withholding attack）」と呼ばれる手法の攻撃[88]が成功した初の事例であり、業界では、同じ仕組みを採用する全ての仮想通貨に起こり得る問題として、対応策への議論が今後高まることが予想されている[89]。

また、ブロックチェーン技術については、Gartner Japan 社が 2018 年 4 月に発表した従業員数 500 人以上の日本企業を対象としたブロックチェーンへの取組み状況に関する調査結果によると、調査など初期的なものも含め、ブロックチェーンに何らかの形で取り組んでいる企業が全体の 42.6%に上ることが明らかになっており、同社は今後 3 年以内にブロックチェーンに取り組む日本企業は 60%程度に達すると予測している[90]。

図表 14：日本企業のブロックチェーンへの取組み状況



出典：Gartner Japan

[87] http://fortune.com/2018/04/10/cryptocurrency-trade-statistics-japan/

[88] Selfish Mining 攻撃は、仮想通貨の PoW の仕組みにおいて、採掘したブロックが分岐した場合に、最も長いチェーンを正しいチェーンとし、直近の取引記録を置き換え消失させるルールを突いた攻撃手法（攻撃者は無効化前に取引所でコインを換金することで利益を得る）。理論的に、全体のハッシュパワー（マイニング処理能力）の 33%以上を持つことで、マイナー自身で最長のチェーンを生成し続けられることが可能であると言われてきたが、同攻撃が実現したのはモナコインのケースが初となる。ビットコインでは、世界中から数多くのマイナーが参加し、膨大なハッシュパワーが集まるため、全ハッシュパワーの 33%を 1 グループが押さえることは不可能に近く、これまで 1 度もハッキング事件は起きていない。モナコイン攻撃の背景には、同仮想通貨の時価総額増大に伴う攻撃インセンティブの高まりや、マイナーが相対的に少なく、ハッシュパワーが一部に集中しやすい環境だったことなどが挙げられている。https://japan.cnet.com/article/35119425/

[89] http://techwave.jp/archives/monacoin-block-withholding-attack.html

[90] https://www.gartner.co.jp/press/html/pr20180405-01.html

同調査を受けて Gartner Japan 社は、ブロックチェーンへの理解や試行を進めようとしない企業の IT 部門のほとんどが 2021 年までに自社のデジタル・ビジネスに向けた活動をリードできない状況に陥るほか、2023 年までに日本企業の 3 割以上が、海外の大企業又はテクノロジーに強みを持つグローバル企業が作り上げるブロックチェーンを用いたデジタルプラットフォームの影響を受けるようになるとの展望を示しており、同社のリサーチ＆アドバイザリ部門バイスプレジデントである鈴木雅喜氏は、「まだ多くの部分が未知数とはいえ、ブロックチェーンを無視するのはすべての企業において危険なことであり、企業は、ブロックチェーンへの理解を社内に広げて機会／リスク分析を進め、社内外に向けた活用機会を探索していくことが望ましい」と述べている[91]。

ブロックチェーンは、低コストのソリューションを武器に従来のビジネスモデルを攻撃し、既存企業のビジネスを一夜で覆す可能性のある破壊的技術（disruptive technology）ではなく、我々の経済・社会システムの新たな基盤技術となることが期待されている[92]。社名に「ブロックチェーン」を含む企業の株価が急伸するなど、近年のブロックチェーンブームは 1990 年代のインターネットバブルに例えられることが多い[93]。まだ技術として歴史の浅いブロックチェーンが現在のインターネットのような存在になるのか、その動向が注目される。

[91] https://www.gartner.co.jp/press/html/pr20180405-01.html
[92] https://hbr.org/2017/01/the-truth-about-blockchain
[93] https://www.reuters.com/article/us-blockchain-companies/blockchain-name-grabbing-has-echoes-of-dotcom-bubble-idUSKBN1FS1F3