ビットコインのブロックチェーン技術

若原 恭◉著

CUTT
カットシステム

・本書の内容についてのご意見、ご質問は、お名前、ご連絡先を明記のうえ、小社出版部宛文書（郵送または E-mail）でお送りください。
・電話によるお問い合わせはお受けできません。
・本書の解説範囲を越える内容のご質問や、本書の内容と無関係なご質問にはお答えできません。
・匿名のフリーメールアドレスからのお問い合わせには返信しかねます。

まえがき

昨今、情報通信技術が急速に発展しその活用による情報社会が益々高度化する中、仮想通貨がグローバルなスケールで話題になっている。ドルや円などの通常の法定通貨との交換レートが大きく変動したり、不正アクセスによって巨額の流失事件が発生したりして、報道メディアで扱われることも少なくない。世界で2,000 を超えると言われる仮想通貨の内、最初に出現したビットコインが最も有名であろう。ビットコインを実現するための中核にはブロックチェーンと呼ばれる新しい技術がある。ブロックチェーンは仮想通貨を用いた取引の記録をいくつかまとめたブロックを鎖状に連結して蓄積するデータベースであり、ビットコイン以外の仮想通貨でも中核技術になっていることが多く、仮想通貨に限らず他にも幅広い応用が可能である。本書はそのような観点からブロックチェーンの技術を解説するが、ブロックチェーンはビットコインとともに一体として考案され開発されたもので、ビットコインの理解なくしてブロックチェーンを理解することは現実的でないため、本書はビットコインの解説書でもある。

ビットコインおよびブロックチェーンに関する書籍や雑誌はすでに多く出版されている。当初は技術的な解説というより、ビットコインという新しい電子的なデジタル通貨が持つ社会的意義・効用や、主に投機対象としての観点からその社会的インパクトを強調することが多かった。その後、技術的な解説を主目的とする書籍も続々と出版されるようになった。

ビットコインは多くの技術を集大成した一システムである。その中には、分散処理・暗号方式・ネットワーク技術など、特に 20 世紀から 21 世紀にかけて研究開発され、情報社会の中核を担っている多くの新しい基盤技術が含まれている。したがって、ビットコインおよびブロックチェーンを十分深く理解するためには、このように多様な基盤技術の理解も必須である。しかし、これまでに出版された書籍や雑誌などでは、動作の原理・仕組みの全貌、技術の本質、他技術との関連や位置づけ、限界や課題に関する整理などについて断片的あるいは明確で

ない説明が多く、例えば、ブロックチェーンの改善や発展・応用を検討するうえで不十分さや物足りなさを感じることが少なくない。本書は、このような問題を解決した総合的な技術解説を特徴とする学術書の実現を目的としている。

ビットコインの技術の鍵は、多くの参加者がブロックチェーンを分散して個別に管理し更新し続けていくのにもかかわらず、常にほぼ同一の正しいブロックチェーンを保管し続けることにある。つまり、一時的に異なってもすぐに余分な部分が削除されて結果的には同一のブロックチェーンに速やかに収束するという動作を繰り返す。この動作は合意形成と呼ばれ、分散処理において本質的であるものの解決が困難な技術課題であることが知られている。その基本であるビザンチン将軍問題を参照して説明した書籍は少なくないが、その問題自体の記述があいまいであったり、この基本問題に対する解について小規模で簡単な具体例の紹介で済ませ明確な説明を省いたりすることが多く、ビットコインの中核技術の本質を理解するうえで十分とは言えない。総じて合意形成に関し多くの書籍は部分的な説明や表面的な説明に終始することが多く、理由を含めた総合的な動作を確実に理解できる書籍や解説は著者の知る限り皆無である。

本書では、合意形成に関する具体的な動作を例を含めて詳細かつ丁寧に説明し、分散的に管理されるブロックチェーンの収束および再収束の仕組みを明らかにしている。これによってビットコインにおける合意形成の全貌が総合的に理解できることを狙った。また、合意形成に係わる動作を基に、ビットコインにおける合意形成の現実的で明確な新しい定義づけを試みた。さらに、ブロックチェーン技術の学術的な位置づけを明確にする記述も盛り込んだ。一方、このように重要な合意形成や現実的なビットコインの利用を効率よく実現するために、ブロックがヘッダとボディから構成されヘッダとボディの関係やブロック間の関係には大きな特徴があるが、その理由や意義についても具体的に説明しており、ブロックの構成が巧みなシステム設計の結果であることを示している。これらの解説は、他の書籍や解説などには見られないユニークな内容であり、ビットコインの技術の本質を理解することを意図する読者にはぜひ味わっていただきたいと願っている。

一方、ビットコインに係わる広範な技術すべてを一冊の書籍でカバーすること

は現実的でないので、技術の詳細をブラックボックスとして扱い、外から見た技術の要点を中心に理解し把握するだけで十分と著者が判断した場合はそのような記述に留める方針とし、ブラックボックスの中身に関する詳細は別の書籍や論文に譲ることとした。また、説明がやや長くなりビットコインとブロックチェーンの本質を理解する最初の段階ではスキップしても基本的には問題がないと判断した場合は、本文での記述は最小限に留めそれ以上の記述は付録としてまとめることとした。

ビットコインとブロックチェーンは、本質的には新しい電子的なデジタル通貨である仮想通貨とその実現手段を新たに提起するものであるが、通貨に関連する様々な概念や考え方をも新たに提起している。また、実現技術として多くの既存技術を巧みに組み合わせて工夫することによって、これまでにない特性を達成し、実システムの運用を通してその正しさや有効性を実証するものととらえることもできる。本書では、このような観点での説明を明確に記述することにも留意した。

このように本書はブロックチェーン自体の技術に加え、その基盤技術や周辺技術の解説にもページをある程度割く方針とした。逆に言えば、本書を一通り理解することによって、ブロックチェーンとそれを実現する技術の本質的理解が総合的に得られるものと考えている。

なお、本書はビットコインの経済面や社会的なインパクトを主目的として解説するものではない。ビットコインとブロックチェーンの実装、およびビットコインを実際に利用する実務上のマニュアル的な説明やノウハウも本質的にカバーしていない。また、ビットコインの運用に係わる統計情報も掲載していない。これらの説明については他の書籍や雑誌などを参照することが可能であり、また、ビットコインを運用管理する組織が提供する Web サイトから関連情報を入手することも可能である。

本書は全 9 章と付録から構成されている。第 1 章は序章で、ビットコインの概要と歴史を簡単に紹介する。これによって、実質的に初めてビットコインに触れる読者がビットコインとその技術について興味を持っていただければ幸いである。第 2 章は、ビットコインの持つ独創的な技術の動作の仕組みの基礎を説明

する。多忙な読者が例えば 1 時間程度でビットコインの仕組みを理解する場合に役立つと考えている。また、基礎を理解することによってビットコインの技術への興味を強くし、技術に関し詳しい解説を具体的に記載した以降の章に進むことを願っている。

第 3 章ではビットコインというシステムの初期動作を説明するが、動作全体に係わる技術を理解するうえで必要となる暗号方式の基本も合わせて紹介する。第 4 章は、ビットコインの中核データである取引の記録（トランザクション）とその扱いについて解説する。これによって通常の通貨や電子マネーなどとの本質的な差異も理解できる。第 5 章は本書の主要部であり、複数のトランザクションをまとめたブロックをネットワーク全体で並行的に分散処理することによって、正当なトランザクションをブロックチェーンというデータベースに保管し更新していく合意形成の仕組みと技術を紹介し、合意形成の定義を提示する。これらの記述は本書を初めて読む場合、やや難解に感じる可能性もあるが、ブロックチェーンが広範で深い熟慮のうえ設計された非常に巧みなシステム技術であると理解できるであろう。第 6 章では、このような分散処理による合意形成が持つ本質的な技術問題を明らかにした後、その正しい解の導出が容易でないことを示し、ブロックチェーン技術による解の位置づけを整理する。第 7 章では、ビットコインの分散処理を担うコンピュータが現実的には性能や容量に限界があるものが多いことを踏まえ、そのようなコンピュータにおける特徴的な動作の仕組みや技術を説明する。

第 8 章では、益々発展するとともに急速に応用が拡大し続けるブロックチェーン技術の主要な動向を紹介する。ブロックチェーンの改善や活用を考えていくうえでの参考になると期待する。最後の第 9 章では、ブロックチェーン技術が将来さらに健全に発展することを願って、現在考えられる限界や課題を論じる。

付録 A は、ブロックチェーンの運用で顕在化した問題の一例として、トランザクション展性と呼ばれる脆弱性とその対策について紹介する。巧みに設計されたシステムでも実装において脆弱性を含むことが避け難いことや、その対応についての教訓も説明する。付録 B では、分散システムにおける合意形成の解について具体例を中心にして詳説する。特に理論に興味を持つ読者に有益であろう。

付録Cでは、ビットコインでの採否に拘らず、ブロックチェーンについて取り組まれてきた主な改善や拡張について解説する。

本書は特にブロックチェーン技術の本質を見極めたうえで、ブロックチェーン技術の応用や発展について検討していくことを意識した技術者・研究者向けの入門書である。ブロックチェーンは、決して完成した技術ではなく限界もあり課題も少なくないが、オリジナリティが高く将来的に発展の余地も大きいと判断され、著者から見ると非常に興味深い技術である。本書によってビットコインとブロックチェーンの仕組みを理解し技術の本質を把握したうえで、特にブロックチェーンの健全な活用・応用やさらなる発展を検討いただくことになれば著者の大きな喜びである。

基本的な用語と略語

本書では多くの用語と略語を使用している。それらは原則として最初に出てくる箇所で意味や原型語を説明するが、一部は複数の意味を持つうえ多用するので本文に進む前に理解しておくことが望ましく、ここでまとめて説明しておく。

ビットコイン・BTC（bitcoin）

『ビットコイン』という用語を、次に示す３通りの意味で使用する。

① 通貨としての名称
② 通貨ビットコインの単位
③ 通貨ビットコインを実現するためのネットワーク、ソフトウェア、コンピュータ、および通信プロトコルを総合したシステム

本書では、ビットコインを BTC と略すことが多いが、意味の区別があいまいになると判断される場合は『通貨 BTC』・『システム BTC』などと記述する。

トランザクション・Tr（transaction）

システム BTC では『通貨 BTC の授受』という取引を実現するが、そのような取引自体および取引の記録のいずれもトランザクションと呼び Tr と略す。なお、データベースの分野で使われているトランザクションとは意味が異なるので注意が必要である。

ブロック（block）と**ブロックチェーン**・BC（blockchain）

Tr をいくつかまとめた集まりをブロックと呼ぶ。ブロックには、Tr 以外にブロックの改ざん対策やブロックの連結を実現するなど、Tr とブロックの様々な管理や制御のために必要な情報が含まれている。鎖状に連結された複数個のブロックをブロックチェーンと呼び、そのようなブロックチェーンを核として Tr を分散的に管理するシステムをもブロックチェーンと呼ぶ。いずれのブロック

チェーンも BC と略すが、両者の区別があいまいな場合は、『鎖状連結 BC』、『システム BC』と記述する。なおチェーンをチェインと表記することも少なくないが、本書では関連する分野の学会（電子情報通信学会・情報処理学会）を含めすでに広く使われているチェーンを採用した。

目　次

第1章

ビットコインの概要と歴史

1.1 ビットコインの概要

1.1.1 仮想通貨とビットコイン

現代社会における様々な活動において、多様な物やサービスの価値の定量化を可能とし取引を容易にする通貨（貨幣）は必須と言える。これまでの通貨は、円やドルのように、法律によって定められ、使用に関して強制力（強制通用力）を持ち、国家によって価値が保証される法定通貨(legal currency/tender)であった。しかし、近年コンピュータ技術の発展に伴って、物理的な物として存在しないうえ法的な強制通用力も持たずコンピュータ上の仮想世界のみにデータとして存在するデジタル通貨（digital currency）が使われるようになってきた。デジタル通貨は電子通貨（electronic currency）とも呼ばれ多種多様でありその定義も確立しているとは言えないが、ここでは大雑把に「電子的なデータとしてのみ存在する通貨」と位置付ける。仮想通貨（virtual currency）はこのようなデジタル通貨の一種であり、2017 年 4 月に施行された「資金決済に関する法律（資金決済

法)」の第二条５によって次の通り定義されている。

一　物品を購入し、若しくは借り受け、または役務の提供を受ける場合に、これらの代価の弁済のために不特定の者に対して使用することができ、かつ、不特定の者を相手方として購入および売却を行うことができる財産的価値（電子機器その他の物に電子的方法により記録されているものに限り、本邦通貨および外国通貨並びに通貨建資産を除く。次号において同じ。）であって、電子情報処理組織を用いて移転することができるもの

二　不特定の者を相手方として前号に掲げるものと相互に交換を行うことができる財産的価値であって、電子情報処理組織を用いて移転することができるもの

本書では理解を容易にするため、次の２点を特徴とする通貨を仮想通貨と定義する。

① ネットワークを介した分散処理を基盤として、その通貨の発行とその通貨による取引が電子的に実現されること。
② 他の通貨とは独立してその通貨自体を新たに発行することが可能で、不特定の者との間で通貨を含む物品やサービスの対価として使用可能であること。

①は、仮想通貨が従来の法定通貨と異なりコンピュータなどの上の仮想空間で扱われ、その発行や取引が集中処理でなく分散処理によって実現することを意味し、②は、仮想通貨がいわゆる電子マネーやポイントなどと異なり他の通貨とは独立した存在であることを意味している。仮想通貨の定義は時代とともに変化する可能性がある。例えば、従来は『国家や法律による裏付けがなく、国家や法定通貨とは独立に管理され、法律や条例などに基づく強制的な通用力がない』という主旨を含んでいたが、中国ではデジタル人民元を国家として発行し法定通貨と

する動きがあり他の国も追随する可能性があるため、本書ではこの主旨を除外した。なお、仮想通貨は物品やサービスの対価以外に法定通貨や他の仮想通貨との交換によって入手可能であることが多い。

世界で初めて考案され実用化された仮想通貨は、ビットコイン（BTC：bitcoin）[1] である。当初 BTC は仮想通貨と呼ばれていたが、2018 年に開催された「先進国首脳会議 G7」（Group of Seven：フランス、アメリカ、イギリス、ドイツ、日本、イタリア、カナダ）では暗号資産（crypto asset）と呼ばれ、これを受けて仮想通貨に代わって暗号資産と呼ぶ動きが出てきた。暗号資産という呼称の由来は、BTC などの仮想通貨の運用では暗号技術が必須で実際に多用されているため「仮想」でなく「暗号」を採用する一方、イーサリアムなど BTC と同様な、または類似のシステムでは通貨以外に契約を履行するための権利を表すように概念が拡張されたトークン（token）を通貨の代わりに使用していることから、「通貨」を「資産」に変更したと推測される。しかしながら、本書では次の理由から「仮想通貨」を採用している。

- 「仮想通貨」がすでに広く使われている。
- コンピュータ上の世界を意味する「仮想」は、本書の対象である BTC の基本的な特質を適切に表しており、上述した「仮想通貨」の特徴①と整合する。
- BTC には、「資産」の一つである「通貨」の方がより具体的で適している。
- BTC では確かに暗号技術が多用されているが、通貨（金額）自体を暗号化することは本質でなく、実際誰もが金額などの取引内容に自由にアクセスできるので、「暗号通貨／資産」という表現によって「暗号化されている通貨／資産」あるいは「暗号化されている取引」などとの誤解を招く恐れがある。

1.1.2 トランザクションと鍵

システム BTC では法定通貨と本質的に異なる特徴を持つ仮想通貨を実現するため新しい技術が導入されたが、その中核技術がブロックチェーン（BC：

blockchain）である。BC は「分散台帳」とも呼ばれ、この名称や仮想通貨の特徴①からも想像できるように、運用管理が特定の組織によって集中的に行われるのではなく、ネットワーク上の多くの参加者によって分散的に行われる。言い換えると、BC の本来の目的は、トラストレス（trustless）すなわち信頼（信用）できる第三者（中央の集中管理機構）を必要とせず、当事者間での取引（とその検証）が可能な通貨 BTC を実現することにある。

通貨 BTC は仮想的であり物理的に存在するものではなく、支払者と受領者の間で授受するという取引を電子的に実現する。このような取引やその記録をトランザクション（Tr：Transaction）と呼ぶ。BTC の所有者は、その安全な使用を可能とするため、他者には秘密扱いの鍵を持つ。この鍵を使って、正当な所有額のうち任意の額を特定の相手（受領者）だけが受領可能な支払いに充てることができる。つまり、Tr によって支払者・受領者・支払額が明確に指定される。鍵はユーザに管理が委ねられており、もし鍵が他ユーザに知られるとその鍵を使って通貨を使われ（盗用され）てしまう。したがって、鍵の管理は極めて重要であり、通常はユーザ自身が管理するコンピュータに保管される。

1.1.3 ブロックチェーンと合意形成

システム BTC は物理的にはネットワーク上に分散配置されたコンピュータの集合で、これらコンピュータは基本的にいずれも同じ機能を持つ。このように対等な機能要素から構成された分散システムは P2P（peer-to-peer）システムと呼ばれており、すでに述べた通り中央集権的な機能や役割を持たない点が大きな特徴である。

P2P システムでは基本的にあらゆる処理が複数のコンピュータでほぼ同時に並行して実行され、これらコンピュータはネットワークの観点からノード（node）と呼ばれる。一般にノード間での情報授受を司るネットワークは必ずしも信頼性が高くなく不達・順序逆転・伝送遅延などがあり得、ノード間での確実な時刻同期は現実的に不可能である。その結果、特別な処理を施さないと、整合しない取引をノードで実行する恐れがある。例えば、二つの異なる取引 Tr1 と Tr2 につ

いて、あるノードでは Tr1 のみ、別のノードでは Tr2 のみ実行するようなことが起き得る。これでは客観的にどの取引が正当か判別できず混乱が生じ、信頼できる取引が実現できない。したがって、独立並行的に実行される各ノードでの処理に関し、不整合が生じないように同一の取引を確定できるための特別な処理が必須となる。このようなネットワークに接続された複数のノードが並行して分散処理した結果同一の正しい取引を判別して承認し確定できるための仕組みを『合意形成』（consensus）と呼ぶ [1], [2]。

合意形成は厳密には第 5 章で定義するが、分散処理に特有な重要機能で、これまで広く採用されてきた中央処理サーバによるシステムでは必要なかった。システム BTC では、このような合意形成によって取引だけでなく通貨の正当な発行と管理も可能となっている。各ノードは基本的に過去の正しい Tr をすべて保管する BC を共通に持つ。BC は Tr を複数個まとめたブロック（block）が鎖（chain）状に連結された構造となっており、この構造が BC と呼ばれる所以である。

BC は言わば Tr の分散データベースであり、合意形成によって各ノードが持つ分散データベース BC のコンテンツは基本的に同一となる。合意形成はこれまで分散処理の研究の一環として検討されてきた。その結果、正しい合意形成の実現は一般に容易でないことが分かっている。BTC の合意形成は理論的に完全に正しいとは言えないが、統計的にはほぼ正しいと考えられており、実際、稼働が開始して以来合意形成に関してシステムが破綻するような本質的な問題は生じておらず、実用性の高い現実的な合意形成法として実証されつつあると言えよう。

一方、通貨 BTC はシステム BTC の中で合意形成に伴って発行される。このような新規発行は、いわば自然界に眠っていた貴金属などの価値ある鉱物を採掘し、それを活用できるよう市場マーケットに供することに相当するため、合意形成のためのブロック作成動作を金や銅などの採掘にたとえてマイニング（mining）と呼び、マイニングを行うノードをマイナー（miner）またはマイニングノード（mining node）と呼ぶ。具体的には、BC に連結されるブロックを逸早く完成することによって合意形成に貢献したマイナーは報酬を獲得するが、その報酬には、Tr の支払者が支払う手数料に加え、ブロック作成に伴ってシステム BTC が新たに発行する通貨 BTC が含まれる。手数料はシステム BTC として

は 0 でも構わない。つまり、新たに発行される報酬が主な動機づけとなって各マイナーがブロック作成を競争する。

このように BC に基づくマイニング競争によって合意形成を実現し取引を確定していくというかつてないユニークなアイデアは、システム BTC の大きな特徴である。マイニング競争にはどのノードも参加できるが、実際には多量のコンピュータ処理が必要となるため、処理能力の高いコンピュータを持つノードがその処理能力に応じて勝利する仕組みとなっている。言い換えると、BTC は取引を実現するために新たな通貨を発行し、それをマイニング競争に勝ち抜いたマイナーに与えることで分散処理による合意形成を実現し取引を承認し確定するシステムと言える。

仮想通貨 BTC を実現する中核技術はシステム BC であり、BC によって BTC を用いた価値の保管（保有）と交換（移転）が可能となり、通常の法定通貨で可能なことは、BTC でもほぼすべて可能である。法定通貨との大きな差異は、BTC 自体が電子的なデータでコンピュータを通して取引が行われること、取引処理自体は一般に高速で、適切な安全対策によって高い安全性を保てること、そして法的な根拠や政府・日本銀行のような中央集権的な組織の裏付けと保証がなくても、関与する全ノードあるいはそれらを所有する参加者の総意によって運用管理されることにある。

1.1.4 ビットコインの特徴

以上で述べた通り、システム BTC はこれまでの多くのシステムとは大きく異なっており、様々な特徴を有している。それらをまとめると以下の通りで、アンダーラインは他のシステムや技術にないユニークな特徴であることを示す。

- P2P 型の分散処理システムで、構成する各ノード（コンピュータ）がサーバでありクライアントでもある。
- PC や専用コンピュータなどの処理装置上のソフトウェアによって実現される。

- 通貨発行機能があり、外から通貨が与えられることはない。
- ノード間の共同処理によって、正当な取引とその記録（台帳）を承認して確定でき、いったん確定した取引は非可逆（取り消しや変更が不可能）で、通貨の多重使用ができない。
- 各ノードに全取引記録が格納されており、ユーザはいつでも自由にアクセスできる。

1.2 ビットコインの歴史

システム BTC は、分散処理、計算科学、コンピュータ、暗号技術、無線・有線通信技術、インターネットなど、いわゆる 20 世紀から 21 世紀にかけて発案され飛躍的に発展した情報通信技術（ICT：Information and Communication Technology）をベースとし、それらを組み合わせて活用することによって考案され開発された。BTC と BC の歴史の概略は以下のとおりである。

- 2008 年 10 月、Satoshi Nakamoto の著者名で BTC と BC に係わる最初の論文 [1] が発表された（BTC の検討開始は 2007 年と言われている）。集中的な機能を持つ中央の組織を不要とし参加者全体による分散的な管理によって、デジタル通貨の多重支払い問題を初めて実用レベルで解決可能としたことから、以降、特に金融分野の新技術として注目され始めた。
- 2009 年 1 月、システム BTC が実装され、誰もが利用できるようになった。最初のユーザは Nakamoto 氏であり、仮想通貨 BTC を最初に受領したユーザも Nakamoto 氏である。その後、多くの技術者によって、システム BTC の改良と拡張が進められた。
- 2009 年 10 月、通貨 BTC と法定通貨との交換レートが初めて公開され、実質的に法定通貨との交換が可能となった。
- 2010 年 5 月、商品購入に BTC が初めて使われた。ただし、この最初の使

用は直接ではなく、第三者が仲介した。いずれにせよ、法定通貨との交換と実用の実績によって BTC の普及が始まり、後の爆発的ブームのきっかけとなった。

- 2011 年 4 月、システム BTC の運用管理は Nakamoto 氏から離れ、ボランティアによるコミュニティに移った。Nakamoto 氏は身を引いたが、正体は現在も不明のままである。名前からは日本人とも考えられるが、国籍だけでなく個人かグループなのかについても一切明らかとなっていない。
- 2013 年 3 月、実装ソフトウェアのバグによって鎖状連結 BC に分岐が発生した。この頃から通貨 BTC の利用が着実に拡大するとともに、法定通貨との為替レートが変動制であることを踏まえバブル的な投機が始まった。テレビや雑誌などで BTC に関する報道が行われるようになり、投機を含む利用が益々拡大していった。これに伴って BTC の高騰だけでなく、システムへのハッキングや通貨の漏洩（流失）などのトラブルが増加するようになった。トラブルを受けて仮想通貨に関する規制の検討も始まった。一方、BTC 以外への BC の応用の期待が大きくなるとともに、仮想通貨としての実用が拡大していった。
- 2014 年頃から、Dell や Microsoft などの大手グローバル企業が BTC による支払いの受付を開始した。
- 2015 年 8 月にはシステム BTC の分裂が生じ始め、新しいソフトウェアヴァージョンがリリースされた。ただし、新ソフトウェアは必ずしも利用されなかった。並行してセキュリティ事件など多様な課題が次々と顕在化し始めた。特に 2016 年には、BTC ではないが BC に基づくプラットホーム上の投資ファンド The DAO（Decentralized Autonomous Organization）がサイバー攻撃を受け、多額の仮想通貨が流失するという事件が起き、社会に大きなショックを与えた。このような状況を背景として、仮想通貨に対する規制についての検討や議論が活発化するとともに、多額事業資金による BC の応用の発展、学術面での検討や研究も一層活発化してきた。また、BTC/BC に関する解説記事や書物が刊行されるようになった。
- 2017 年 4 月、BTC を含む仮想通貨に対する法律「改正資金決済法」が国

内で初めて施行された。この法律の目的はユーザを保護することにあり、取引所に対する規制を制定したものである。

- 2017 年 8 月、BC の人為的な分岐が行われ、新たな通貨 Bitcoin Cash が誕生した。その大きな特徴は、処理能力の増大を目的としてブロックの大きさの上限を 1 MB から 8 MB に拡張したことである。2018 年 11 月には Bitcoin Cash がさらに分裂して、新たに Bitcoin SV が誕生した。
- 2019 年 6 月、SNS（Social Network System）を運用する Facebook が BC に基づく新しい仮想通貨 Libra の構想を発表した。同年 10 月、中国が BC に基づくデジタル人民元の開発を進めていることを正式に公表した。これらの発表により、国レベルでの仮想通貨の発行や運用の議論が広く本格化することとなった。2020 年 6 月にデジタル人民元の実証実験が開始した。
- 2020 年 7 月、国内の新興企業ソラミツなどが BC に基づく仮想通貨「Byacco/ 白虎」を開発し、会津大学内で正式運用を開始した。

BTC に関する統計情報を含む最新の情報は、いくつかの Web サイトから常時入手することができる [3]。その中には、通貨 BTC の為替レート、ネットワーク内ノード数、BC・ブロック・Tr などに関するデータのリアルタイム値も含まれる。