BOJ
Reports & Research Papers

2020 年 1 月

ブロックチェーン技術のスケーラビリティ問題への対応

日本銀行決済機構局
田中　修一
菅山　靖史

2020 年 1 月
日本銀行決済機構局
田中　修一*
菅山　靖史†

ブロックチェーン技術のスケーラビリティ問題への対応‡

■要　旨■

ブロックチェーン技術は決済・金融分野での活用が展望され、応用研究や実証実験が進められている。参加者が自由にネットワークに加わることが可能なタイプはパブリック型と呼ばれ、特定の管理者や参加者間の信用に依存することのない分権的な枠組みや、障害耐性、悪意を持った参加者による改竄耐性などがメリットと考えられている。

一方、パブリック型は処理性能の拡張性が乏しく、暗号資産取引においては処理遅延が生じるようになった。処理能力拡張の難しさはスケーラビリティ問題と呼ばれており、当初の対応としては、ブロック容量とブロック生成間隔に関する制約を緩和することで、処理能力を高める手法が用いられた。しかし、ブロックチェーンの分裂や分権構造の後退といった問題が発生し、処理能力を柔軟に拡張させることは難しかった。

このため、近年では、一定の分権構造を確保しつつ、スケーラビリティの改善を図る手法が提案されている。代表的なものとしては、（１）ブロックチェーンの外に一部取引を移管する手法（オフチェーン・スケーリング）、（２）既存のブロックチェーンから新たに構築したブロックチェーンに資産を移管し取引を処理する手法（サイドチェーン・スケーリング）、（３）検証対象取引と検証参加者（ノード）を複数のグループに分割し検証作業を分担する手法（シャーディング）が挙げられる。

パブリック型の長所を活かした技術の広がりは、決済・金融システムへの応用可能性を高めることにつながり得るものであり、今後の動向が注目される。

* 日本銀行決済機構局　＜E-mail: shuuichi.tanaka@boj.or.jp＞

† 日本銀行決済機構局　＜E-mail: yasushi.sugayama@boj.or.jp＞

‡ 本稿の執筆に当たっては、日本銀行スタッフを含め、ブロックチェーンの専門家から有益な助言やコメントを頂いた。ただし、残された誤りは全て筆者らに帰する。なお、本稿の内容と意見は筆者ら個人に属するものであり、日本銀行の公式見解を示すものではない。

［目　次］

１．はじめに 3
２．スケーラビリティ問題とは 4
３．これまで実施された主な対応 6
（１）　ブロック容量の拡大 6
① 単純なブロックサイズの拡大 6
② ブロック内の構造変更によるブロック容量の拡大 7
（２）　ブロック生成間隔の短縮 8
４．現在検討が進められている主な取組み 9
（１）　オフチェーン・スケーリング 9
（２）　サイドチェーン・スケーリング 11
（３）　シャーディング 13
５．おわりに 15

１．はじめに

ブロックチェーン技術は、情報を記録・共有するための新たな仕組みとして世界的に注目が集まっており、さまざまな分野でその応用可能性にかかる研究や実証実験が進められている。

ブロックチェーンは、ネットワークに加わることのできる参加者の範囲に応じて大きく２つの種類に分けることができる。まず、参加者が自由にネットワークに加わることが可能なタイプは、パブリック型ブロックチェーン（以下、パブリック型）と呼ばれる。現在広く利用されているものとしては、例えば暗号資産のビットコインやイーサリアムで用いられている処理基盤（これらを本稿ではビットコイン・ブロックチェーン、イーサリアム・ブロックチェーンと呼ぶ）が挙げられる。一方、参加者を予め限定したプライベート型やコンソーシアム型（以下、これらをパーミッション型と呼ぶ）も広く活用が検討されている[1]。

パブリック型では、情報を検証・記録する参加者を多数確保することで、特定の管理者や参加者間の信用に依存することのない分権的な枠組みを実現することが想定されている。このような環境が確保されると、参加者やネットワークの一部が障害に見舞われてもサービスが維持されやすく、こうした可用性の面で利点があると言われている。また、悪意を持った参加者による改竄や、情報の欠落も生じにくくなるため、データの完全性も確保されやすいと考えられている。

このように、パブリック型は、参加者が限定されるパーミッション型に比べ、分権構造の確保を重視した設計といえるため、障害や改竄への耐性が相対的に高く、さまざまな分野への応用が検討されている。例えば、決済・金融サービスにおける資産の記録・移転のほか、各種契約の締結・履行等への活用も展望した取組みが続けられている。現状、暗号資産取引を除けば、これらの多くは実証実験や導入後の初期段階にとどまっているが、パブリック型の持つ可用性や完全性のメリットを活用できれば、ブロックチェーンという新技術を活用した決済・金融システムの可能性が広く展望できるようになるため、各国の中央銀行や当局は強い関心を持って最新動向の把握に努めている。

---

[1] パーミッション型は、プライベート型（単一管理者）とコンソーシアム型（複数管理者）の２タイプに分けられる。いずれも、単一または複数の参加者がネットワークを管理・運営する中核的な役割を担い、ネットワークへの参加許可の管理も行うため、パーミッション型と呼ばれる。

一方、不特定多数の参加者間で情報を共有・記録するパブリック型には、処理性能の制約や、仕様変更時等に必要となる関係者間の合意形成（ガバナンス）の難しさなどの課題もあり、関係者が対応に取組んでいる。本稿では、これらのうち、パブリック型の円滑な運用に不可欠である処理性能の拡張性に関する課題に注目する。これは、スケーラビリティ問題と呼ばれ、パブリック型の利用拡大や決済・金融分野への応用を図るうえで、重要な課題の１つと位置付けられており、既に一部の対策も講じられている。本稿では、ビットコイン・ブロックチェーン、イーサリアム・ブロックチェーンを対象に、業界におけるこれまでの取組状況や、現在検討が進められている主要な対応手法の概要を整理する。

２．スケーラビリティ問題とは

ブロックチェーンでは、ある程度の時間間隔をもって生成されるブロックに、新たに発生した取引に関する情報や、取引を行う際に必要となる署名データ、前回生成されたブロックに関する情報等が記録される。ただし、ビットコイン・ブロックチェーン、イーサリアム・ブロックチェーンでは、いずれもブロックに記録可能な情報量に実質的な上限が設定されているため、取引量の拡大に伴い記録すべき情報量が上限を超過すると、ブロックに全ての取引情報を記録することが困難になる。記録されなかった取引は、次回以降のブロック生成時に記録されるまで処理されず、その間放置されることになる。

このような、ブロック容量の制約とブロック生成間隔の存在に伴って発生する処理能力面での課題は、スケーラビリティ問題と呼ばれており、パブリック型では特に大きな課題になりやすい。パブリック型ではユーザー数や取引量を制限する仕組みがないため、取引需要が高まるにつれ処理遅延を引き起こすようになった。また、ユーザーが自らの取引を優先的にブロックに記録させるため検証参加者（以下、ノード）に支払う手数料を引き上げ、その結果、取引手数料が上昇するという副次的な問題も発生した[2]。

こうした問題に対応するため、ブロック容量と生成間隔の制約を緩和させると、時間当たりの処理対象取引を増やすことができる。その一方で、ネットワーク帯域幅などの計算資源の大きい一部のノードの優位性が高まり[3]、パブリック

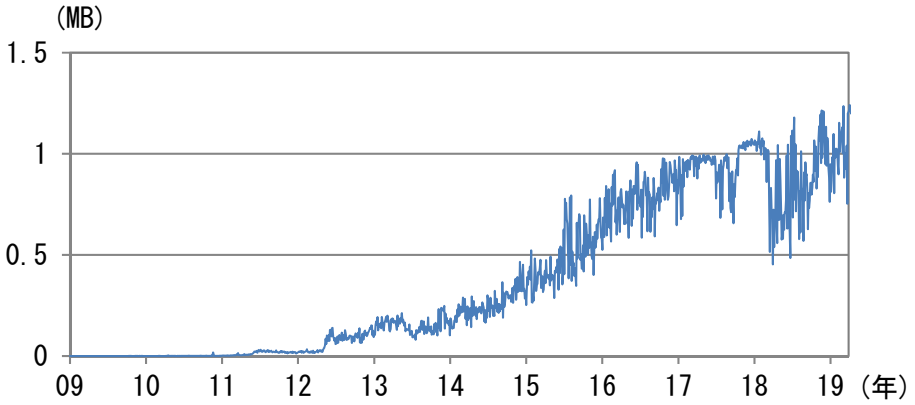
[2] ビットコイン・ブロックチェーンとイーサリアム・ブロックチェーンでは、ユーザーは取引の処理を行うノードに対して費用を支払っている。ノードにとっては、高い価格が提示された取引から順にブロックへの記録を行うことが合理的であり、スケーラビリティ問題が顕現化する際には、こうした行動が取引費用を高めてしまう可能性がある。

[3] ブロック容量の拡大や生成間隔の短縮は、時間当たりの処理対象取引を増加させる。この

型のメリットである分権構造が後退してしまう可能性がある[4]。

スケーラビリティ問題がビットコイン・ブロックチェーンで表面化したのは2017 年であった。同年、ビットコイン価格の急騰に伴い、ブロックサイズの上限（1MB）を上回る取引量が発生し、ブロックサイズが上限に達した（図表 1）。その結果、大量の取引が未処理となるとともに、取引手数料が高騰した（図表 2）。また、同年には、イーサリアム・ブロックチェーンを利用したゲームアプリの利用が高まり、その関連データがブロックの容量を圧迫した結果、未処理の取引が大量に発生する事態も生じている。

（図表 1）ビットコイン・ブロックチェーンのブロック平均サイズ



（出所）Blockchain.com 社

決済・金融システムにおいては、十分な取引数への安定的かつ効率的な対応が不可欠である。関係者の間ではスケーラビリティ問題への懸念は根強く、差し当たりパブリック型の活用を断念し、パーミッション型の活用に取組む先も少なくない[5]。一方、パーミッション型では、十分な分権構造が確保されなくなり、

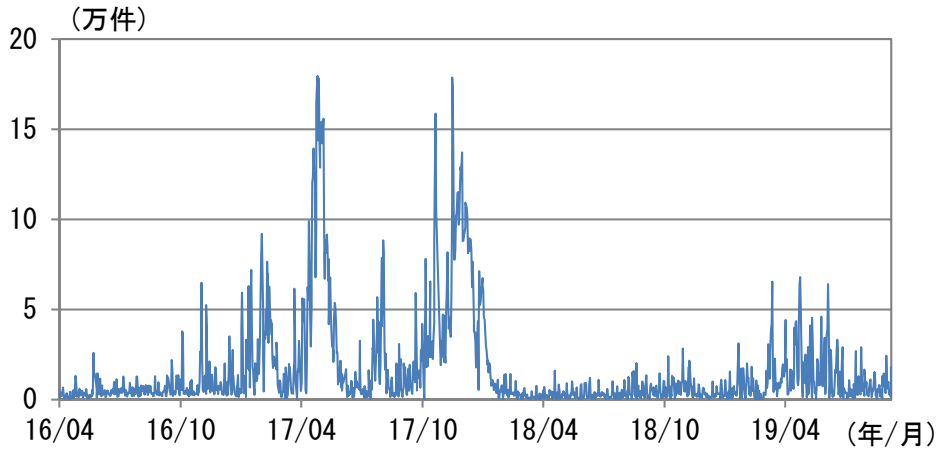
ため、検証対象を短時間で処理できる計算資源の大きいノードの優位性が高まりやすい。また、ノードの優位性には、計算資源の他に、他のノードとの接続形態やノードの稼働時間なども影響する。

[4] ブロック容量と生成間隔の制約は、分権構造の維持に加え、台帳間の整合性の確保や脆弱性対策のためにも必要と言われている。整合性確保については、ブロック容量を拡大すると台帳を同期させるための時間が長くなるほか、ブロック生成間隔を短縮する場合は、ブロックチェーンが一時的に分岐する現象がより頻繁に発生するといった問題がある。こうした問題はブロックチェーンの脆弱性を高めてしまう危険性もある。例えば、DDoS（分散サービス拒否）攻撃やリオルグ（ブロックチェーンの再編成）を悪用した攻撃への脆弱性が増す可能性がある。

[5] パーミッション型の中には、悪意を持った参加者が入り込む余地を事前に排除することで、コンセンサスアルゴリズムの負荷軽減を目指したものもある。

ブロックチェーンが本来持つ可用性や完全性のメリットが得られにくくなってしまうとの指摘も聞かれている。

（図表 2）ビットコイン・ブロックチェーンの未処理取引件数



（出所）Blockchain.com 社

３．これまで実施された主な対応

ビットコイン・ブロックチェーンでは、スケーラビリティ問題への対応として、幾つかの対策が講じられている。代表的な対応としては、（１）ブロック容量の拡大、（２）ブロック生成間隔の短縮、が挙げられる。これらはいずれも、既存のブロックチェーンにおける仕様変更を通じて処理能力の向上を図る取組みであり、オンチェーン・スケーリングなどと呼ばれている。

もっとも、仕様変更に関する参加者間の合意形成は容易ではなく、ブロックチェーンの分裂（ハードフォーク）と、これに伴う混乱が生じてしまった。また、ハードフォークによるノード数の減少に伴う分権構造の後退といった問題も発生した。これらの対応では、取引増加の都度、副作用を伴う仕様変更が必要になり、処理能力を柔軟に拡張させることが難しい。以下では、上記２タイプのオンチェーン・スケーリングの手法と問題について解説する。

（１）ブロック容量の拡大

①　単純なブロックサイズの拡大

ブロックサイズの拡大は、スケーラビリティ問題への対応としては概念的に最も単純な手法であり、処理可能な取引量の増加をもたらす。こうした仕様変更は、技術的なハードルが他の手法に比べて相対的に低かったこともあり、暗号資

産の取引が増加した局面などで実施されている。例えば、ビットコイン・ブロックチェーンでは、もともと 1MB だったブロックサイズ上限を 8MB に引き上げるために、既存の仕様に変更を加えたビットコイン・キャッシュと呼ばれる構想が提案され（参考文献[1]）、2017 年 8 月に実現した。

しかし、ブロックサイズの大幅な拡大は処理対象取引数の増加につながるため、計算資源の大きい一部のノードが取引検証の面で優位性を高める可能性があり、その結果、パブリック型の特徴である分権構造が損なわれやすくなる。また、パブリック型では、事前に設定されたルール（コード）に、仕様変更に関する参加者間の合意形成手順が記載されていないことが多く、新たな仕様の提案に伴いブロックチェーンが複数に分岐する事態を回避しにくい。特定の提案に対する支持が十分得られなければ、既存のノードが分岐したブロックチェーンごとに分かれてしまい、この点でも分権構造が後退することになる。例えば、ビットコイン・キャッシュ・ブロックチェーンは、ビットコイン・ブロックチェーンとは別物であり、互換性は確保されていない。こうした分岐は、事前には発生タイミングが不確定で、ブロックチェーン上で処理される取引に混乱をもたらすおそれがあり、暗号資産取引業者が一時的に取引を停止する事態も生じている。

さらに、本手法では、取引量が増加する度に、ブロックサイズの拡大を目的とした仕様変更が必要になり、取引量の変化に応じた処理性能の柔軟な拡張性が確保されているとはいえない[6]。頻繁な仕様変更を回避するために、予め非常に大きな容量を確保しておくという対応も考えられるが、その場合、処理能力の高いノードの優位性に対する懸念が一段と高まると考えられる。

② ブロック内の構造変更によるブロック容量の拡大

ブロック容量の拡大を目的とした別の取組みとして、ブロック構造の見直しを通じた Segregated Witness（通称 SegWit）と呼ばれる仕様変更が挙げられる。ブロックに格納される個々の取引情報には、取引を行ったユーザーを証明するための署名データが含まれているが、そのサイズは比較的大きいうえ、保管領域に関するセキュリティ面での脆弱性を抱えていた。SegWit では、この署名データを元の保管場所から分離し別の領域に移管することで（Segregate）、セキュリティ面での課題を解消するとともに、ブロックに格納可能な情報量を拡大させる操作が提案された（参考文献[2]）。

[6] ビットコイン・キャッシュ・ブロックチェーンは、その後もハードフォークを繰り返している。そのなかにはスケーラビリティ向上を目指した新技術導入を伴ったものもあれば、関係者の利害対立や設計思想対立が複雑に絡んだものもあるとされている。

しかし、スケーラビリティ問題が緩和することで、ノードが得ることのできる手数料収入の減少が見込まれたため、参加者間の合意形成が難航した。さらに、SegWit 対応の結果、利用不能となってしまうマイニング機器を保有するノードからの支持も得られにくかったことも、SegWit 導入にネガティブに作用した。もっとも、その後、取引量の更なる増加を受けて処理の遅れへの懸念が強まったほか、SegWit 導入に伴って署名管理に関するセキュリティが向上する利点が強く意識されるようになった。また、SegWit の導入により、本稿後半で紹介するオフチェーン・スケーリングの利用が展望された点もメリットと受け止められた。最終的には SegWit 導入に関する参加者からの十分な支持が得られ、2017 年 8 月にビットコイン・ブロックチェーンにおける仕様変更が実施された。

ただし、SegWit 利用に伴うブロック容量の拡大効果は一度限りに過ぎず、その結果生まれた容量も、取引量の増加に伴い再び圧迫され得る。このため、ブロック構造を見直す手法では、今後の拡張余地が限られていると考えられている。

（２）ブロック生成間隔の短縮

ブロック生成間隔を短縮させると、一定期間内で処理可能な取引量が増加するため、スケーラビリティ問題の緩和につながる。こうした手法を採用した事例としては、例えば暗号資産ビットコイン・キャンディの取引基盤となるブロックチェーンが挙げられる。これは、2018 年 1 月に、元々ブロック生成間隔が約 10 分であった前述のビットコイン・キャッシュのブロックチェーンの仕様を変更し、ブロックを約 2 分毎に生成することで、取引データの処理量を増加させた事例である（参考文献[3]）[7]。

もっとも、こうしたアプローチでも、ブロックサイズの拡大同様、取引増加の都度、仕様変更が必要になることから、取引量の変化に応じた処理性能の柔軟な拡張性が確保されたわけではない。また、計算資源の大きい一部のノードの優位性が高まり、分権構造が後退する可能性もある。なお、本提案も多数の参加者の支持を確保しない状況で実施されたため、その後に生まれたブロックチェーンと既存チェーンが異なるブロックチェーンとして併存する状況となり、これもノードの分割に伴う分権構造の後退といった課題を伴う対応となった。

[7] ビットコイン・キャンディ・ブロックチェーンでは、ブロック生成間隔の短縮に加え、ブロック容量の拡大も合わせて実施された。

４．現在検討が進められている主な取組み

前節で見てきたオンチェーン・スケーリングの取組みには、ブロックチェーンの分裂や拡張性の乏しさといった課題があるため、関係者の間ではこれらに代わる新たな手法を模索する動きが続いている。いずれも実装に当たってクリアすべき課題が今なお残されており、研究・試行段階にあるものの、アプローチに関する概念的な整理や技術面での進展もみられつつある。

本節では、ビットコイン・ブロックチェーンとイーサリアム・ブロックチェーンを対象とした主な取組みを３つ取上げ、それぞれの概要を紹介する。それらのコンセプトを予め示すと、（１）ブロックチェーンの外に一部取引を移管する手法（オフチェーン・スケーリング）、（２）既存のブロックチェーンから新たに構築したブロックチェーンに資産を移管し取引を処理する手法（サイドチェーン・スケーリング）、（３）検証対象取引とノードを複数のグループに分割し検証作業を分担する手法（シャーディング）である。

（１）オフチェーン・スケーリング： ブロックチェーンの外に一部取引を移管する手法[8]

全ての取引をブロックに格納せず、一定期間内に実行された複数の取引をネットアウトし、その結果のみをブロックチェーンに記録すれば、処理対象となる取引情報量を削減できる。こうしたアイデアを実現するために、ユーザー２者間で取引を行うことができる「ペイメントチャネル」と呼ばれる仕組みをブロックチェーンの外に設け、ここで両者間の取引をネットアウトする取組みが提案されている。このようなブロックチェーンの外に何らかの仕組みを設けるというスケーラビリティ対応は、オフチェーン・スケーリングなどと呼ばれている。

暗号資産ビットコインやイーサリアムの取引の場合、それぞれのユーザーは、①双方の署名によってのみ管理可能な口座（マルチシグアドレス[9]）に、自らの取引ニーズに応じた規模の資産を預託し、②取引相手との間でペイメントチャネルを開設する（図表 3）。ユーザーは、③預託資産を上限に、ペイメントチャネルで接続されたユーザーに資産を送付できるほか、取引相手のユーザーから

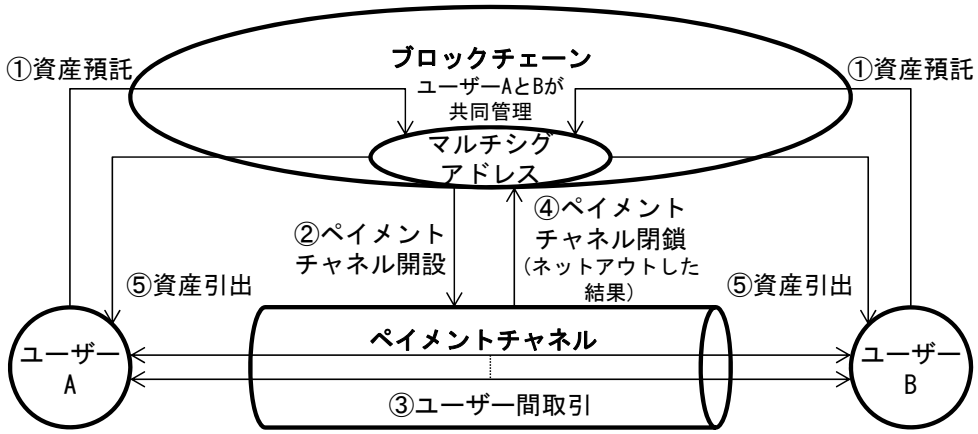
[8] 代表例としては、ビットコイン・ブロックチェーンの Lightning Network やイーサリアム・ブロックチェーンの Raiden Network と呼ばれる手法が挙げられる（参考文献[4][5]）。

[9] 本口座は、取引の管理に複数（multiple）ユーザーの署名（signature）が必要な仕組みとなっているため、マルチシグアドレス（multi-signature address）と呼ばれている。ペイメントチャネル上のアドレスから資産を引き出す際には、双方のユーザーによる署名の利用を義務付けることにより、預託された資産の安全性を確保する仕組みとしている。

資産を受け取ることもできる。ペイメントチャネルが開設された期間中のユーザー間取引は、何度行われてもブロックチェーンに記録されることはなく、④ペイメントチャネルを閉鎖すると、⑤それぞれのユーザーは資産を引き出すことができ、この間の取引をネットアウトした最終的な結果のみがブロックチェーンに記録される[10]。

ユーザーは、取引相手となり得る複数のユーザーとの間でそれぞれペイメントチャネルを開設することで、２者間にとどまらない取引を行うことも可能である。取引相手となるユーザーとの間にペイメントチャネルが直接設置されていない場合でも、取引当事者同士を間接的につなぐペイメントチャネルを持つユーザーが存在すれば、この先を経由した取引を行うこともできる。こうした取引では、経由ユーザーが元々の取引当事者の意図と反する取引を行う事態などを回避するための仕組みを設けておくことが重要となる[11]。

（図表 3）オフチェーン概念図



[10] ブロックチェーンには、①ペイメントチャネルの開設は双方のユーザーからマルチシグアドレスへの送金、②チャネルの閉鎖は当該アドレスから双方のユーザーへの送金として記録される。

[11] こうした仕組みの実現手法として、Hashed Time Lock Contract が考案されている。取引が正しく実施される、もしくは、予め定めた期間内に取引が実施されない場合に送付側に資産を戻す、のいずれかの結果を約束する機能を提供するものであり、複数ユーザーを経由する一連の取引が終始正しく実行されるように誘導する仕組みである。このため、悪意のあるユーザーが存在するといったユーザー同士が互いを信用できない環境であっても、円滑な取引を実現できる利点がある。事前にこうした仕組みが設けられていないと、例えば、送金元のユーザーが送った資産が経由地点のユーザーに届いたにもかかわらず、経由ユーザーが最終的な送金先であるユーザーに当該資産を送らないといった事態が発生するおそれがある。

このほかのメリットとしては、①ブロックチェーン上では取引の記録に一定の時間がかかっていたが、ペイメントチャネル上では速やかに処理されることから、取引の高速化が期待できる。さらに、②取引手数料に関しても、ペイメントチャネルの開設・閉鎖に要する費用と、送金時に経由するユーザーから課金される手数料以外は不要となるため[12]、取引増加時に送金コストが上昇しがちなブロックチェーン取引に比べて費用を節約できる可能性がある。

こうしたオフチェーン・スケーリングは、ビットコイン・ブロックチェーン、イーサリアム・ブロックチェーンでは、開発初期段階の試用版が既に稼働しているが、主にテストを目的としていることもあり、預託された資産は限定的な水準にとどまっている[13]。関係者の間では、利用拡大の制約になり得る要因として、①ペイメントチャネル開設に伴って預託負担が発生するため、規模の大きい取引を機動的に実行しにくい点、②預託する資産を多く持つユーザーが多数のユーザーとペイメントチャネルを開設すれば、同ユーザーは取引の経由先として中心的に利用されることになり、分権構造が後退するリスクなどが指摘されている[14]。例えば、ハブとなるユーザーの障害等により、ネットワークの可用性が低下する可能性などが挙げられる。

ユーザーは、こうしたメリット、デメリットを踏まえ、ブロックチェーン上の取引とペイメントチャネル上の取引を使い分ける可能性もある。例えば、早期の取引処理が必要な小規模取引を手掛けるユーザーにとっては、ペイメントチャネル上の高速取引や安価な手数料が大きなメリットと受け止められるかもしれない。このように、ユーザーが自らの取引ニーズに応じて利用可能なサービスを選択できる環境が整備されていくことは、パブリック型を活用するうえで、重要な論点となるように思われる。

（2）サイドチェーン・スケーリング： 既存のブロックチェーンから新たに構築したブロックチェーンに資産を移管し取引を処理する手法

ブロックチェーンの外へ新たに別のブロックチェーンを構築し、スケーラビリティ問題の緩和を図る試みは、サイドチェーン・スケーリングと呼ばれている

---

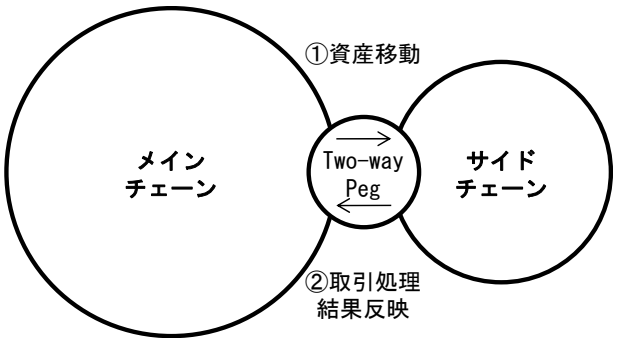
[12] もっとも、多くのユーザーとペイメントチャネルを開設している先は、自らを経由する取引に対して高額の手数料を課す可能性もある。こうした独占的な支配力を持つユーザーを発生させにくくするために、健全な競争環境を確保するための工夫が必要になる。

[13] 例えば、ビットコイン・ブロックチェーンを対象とした Lightning Network の場合、預託されたビットコインは約 860 ビットコインと極めて少額にとどまるなど（総発行量：約 1,800 万ビットコイン、いずれも 2019 年 12 月時点）、利用は限定的である。

[14] その他の課題としては、例えば、取引の経由先が増加する結果、取引を実行するための最適ルートが探索しにくくなり、効率性が低下するリスクが指摘されている。

（図表 4、参考文献[6]）。ここで、既存のブロックチェーンをメインチェーン、取引処理を分担する別のブロックチェーンをサイドチェーンと呼ぶ。サイドチェーン技術は、①メインチェーン上の資産をサイドチェーン上に移動させ、②サイドチェーン上で実施された当該資産の取引処理結果をメインチェーンに反映する機能が基本となる。

（図表 4）サイドチェーン概念図



サイドチェーン・スケーリングが有効に機能するには、まず、取引の対象となる資産が双方のブロックチェーン間を円滑・安全に往来できる環境を確保する必要がある。こうした機能は Two-way Peg と呼ばれている。ブロックチェーン間で資産を移動させる手法としては、単一の管理者が一方のチェーンで資産を預かり、もう一方のチェーンに移動させる仕組みが考えられる。しかし、同管理者が悪意を持って改竄を行うリスクが排除できないといった課題があるため、複数の管理者による相互監視の仕組みが提案されている。もっとも、こうした仕組みを採ったとしても、管理者の数が限定される限り、取引検証の分権構造が確保されにくい（管理者の共謀による改竄を排除できない）という難点がある。一方、メインチェーン上のノードを検証作業に参加させる構想もあり、この場合も十分な数のノードを確保することが重要である。

ブロックチェーン間の取引の検証と同様、サイドチェーン上の取引の検証でも、十分な分権構造を確保する必要がある。例えば、サイドチェーン上の取引の検証作業を行うノードの数が限定される場合、悪意のあるノードによって、サイドチェーン内の取引の安全性が損なわれる可能性が高くなる。一方、メインチェーン上のノードが、サイドチェーンにおける検証作業に加わるよう誘導するには、双方のブロックチェーンの仕様を共通化するといったノードの検証負担の抑制や、ノードへの十分な報酬の提供等の工夫が必要となる。

こうした課題がある一方で、サイドチェーンにはオフチェーン・スケーリングにはなかった利点も存在する。オフチェーン・スケーリングでは、ペイメント

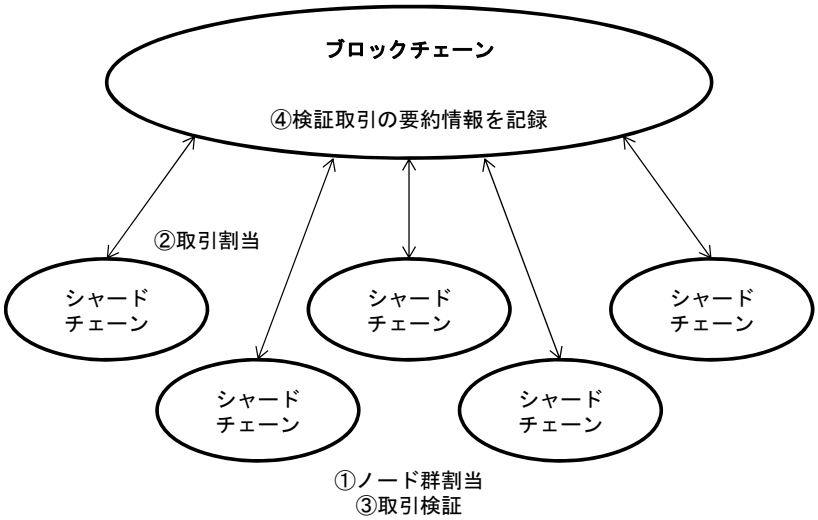
チャネル毎に資産の預託が必要であり、大口取引が機動的に実行されにくかったが、サイドチェーンを利用した手法ではこうした制約がなく、規模の大きな取引も行われやすくなる可能性がある。

取引所のようなノードでは、大口取引の遅延に伴う決済リスクの負担や、取引手数料の上昇がとりわけ重要となる。こうしたノードにとっては、分権構造の後退等の課題を考慮しても、サイドチェーンの利用に伴うメリットが魅力的と受け止められる可能性もあり、実際、サイドチェーン上の取引にユーザーとして参加することや、ノードとして加わることに関心を寄せる取引所等もみられている。

（３）シャーディング： 検証対象取引とノードを複数のグループに分割し検証作業を分担する手法

別のアプローチとして、①ノード群を定期的に入れ替えながらランダムに複数のグループ（シャードチェーン）に分割し、②これらに検証対象取引を割り当てることで、③取引検証作業を分担し、④ブロックチェーン上に検証取引の要約情報を記録する概念も提案されている（図表 5）。作業を複数のグループに分割し処理を並列化させることで作業効率を改善させる手法は、シャーディングと呼ばれ[15]、データベース分野などで広く利用されている。イーサリアム・ブロックチェーンへの応用が代表事例であるが、現時点では実用化に至っておらず、設計や仕様の検討が続いている（参考文献[7]）。

（図表 5）シャーディング概念図



[15] 処理対象となる作業を Shard（破片）と呼ばれる小さいグループに分割するため、Sharding（シャーディング）と呼ばれている。

前述のブロック容量の拡大やブロック生成間隔の短縮（オンチェーンの仕様変更）では、取引量の増加が続く場合は、いずれ限界に達する恐れがあることから、同様の仕様変更を何度も繰り返す必要がある。一方、本手法では、ブロックチェーン本体において、一度大幅な仕様変更が必要となるが、それを乗り越えれば、将来の取引量増加に対応する拡張性が確保される可能性がある。

取引検証は、ブロックチェーン上のルール（コード）によって分割された複数のシャードチェーンで行われ、それぞれのチェーンを担当するノード群が、ランダムに割り当てられた取引の検証作業を行う。元のブロックチェーンには、個々のシャードチェーンで検証された取引の要約情報のみが記録されることになるため、スケーラビリティ問題の解決につながり得る。サイドチェーン・スケーリングで課題として挙げられたブロックチェーン間の取引の検証における問題（ノードの悪意をもった振る舞い）についても、ランダムに選ばれ直されるノード群が情報の移転機能を担うことから、特定のノードに検証を依存する事態はある程度回避される設計となっている。

こうした機能を十分発揮するために、シャーディングの導入に際しては、シャードチェーン内の特定ノードの優位性が不正に直結しにくい環境を実現する必要がある。例えば、イーサリアム・ブロックチェーンのシャーディングにおいては、ノードが事前に差し入れる資産の大きさに応じて検証成果が向上する手法の導入が検討されている[16]。この手法のもとでは、ノードが差し入れる資産の大きさが事前に明らかにされる。このため、ノードをシャードチェーンに割り振る際に、シャードチェーンごとにノード群内の検証能力をある程度均衡させることが可能になり、大きな資産を持つノードによる不正を抑止する効果が期待できる。

ただし、ノード群内の検証能力の均衡を図ったとしても、大きな資産を持つノードはより多くの資産を獲得し、一段と検証成果を高める傾向があるため、分権構造が後退する恐れが残る。また、資産差し入れに伴い、市場で取引される当該資産が減少すると、市場流動性の低下や効率的な価格形成が阻害される可能性もある。このため、ノードが差し入れる資産の最低金額を引き下げることで、大きな資産を持つノードの独占力の緩和を図る工夫や、ノードによって差し入れられた資産が取引可能になるまでの期間を短縮化し、流動性の改善を図るといった対応も検討されている。

---

[16] こうした手法は、持ち分による検証（Proof of Stake）と呼ばれている。従来、イーサリアム・ブロックチェーンでは、作業量による検証（Proof of Work）が用いられていたが、ノードの計算資源に応じて取引検証の優位性が高まるという問題を抱えていた。ただし、Proof of Stake を採用するには、イーサリアム・ブロックチェーンの仕様変更が必要になる。

５．おわりに

ブロックチェーン技術はさまざまな業務やシステムへの応用が期待されている。その適用領域は、暗号資産取引にとどまらず多様な分野が考えられ、決済・金融分野と関連の深い資産や権利の記録・移転のほか、各種契約の締結・履行等への活用も展望されている。こうした取組みは、決済・金融システムの改善につながる可能性があることから、各国の中央銀行や当局も最新動向の把握に努めている。

パブリック型のブロックチェーンは、信頼のない（悪意を持った参加者が入り込む）環境において、中央集権的管理者が存在せずとも、可用性・完全性を備えた自律的分散型システムの構築を目指すものである。こうした分散型管理のメリットを追求するパブリック型は、スケーラビリティやガバナンスなど複数の課題を抱えている。本稿で扱ったスケーラビリティ問題に関しては、既存のブロックチェーン上で課題の軽減を図るオンチェーン・スケーリングに加え、ブロックチェーンの外で取引の処理を分担する手法などが提案されている。本稿では、その代表的な３つの手法の概要を解説した。

そうした技術改善が進む過程においては、ユーザーの用途や目的に応じて、パブリック型のメリットである分権構造の確保とスケーラビリティの改善という２つの目的の間で適切なバランスを探る機運も生まれている。ノード数の減少や検証能力の一部ノードへの偏りを部分的に許容しつつも、ブロックチェーンの処理速度の向上や取引費用の低下を享受しようという意見も聞かれている。このように、パブリック型の長所が活かされた技術が利用可能になれば、決済・金融システムの改善が図られる可能性もある。

日本銀行は、決済システムの安全性と効率性を改善していくために、新しい技術の動向やこれが決済手段に与える影響等について十分に把握しておく必要がある。欧州中央銀行との間で、分散型台帳技術に関する共同調査（「Project Stella」）に取組んでいるのも、その一例である。

日本銀行としては、今後も新技術の動向や影響等について積極的に調査を行っていく方針である。

以　上

【参考文献】

[1] bitcoincash.org, “UAHF Technical Specification”, 2017
(https://www.bitcoincash.org/spec/uahf-technical-spec.html)

[2] Eric Lombrozo, Johnson Lau, and Pieter Wuille, “Segregated Witness (Consensus layer)”, 2015
(https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki)

[3] BitcoinCandy, “Bitcoin Candy Whitepaper”, (https://cdy.one/whitepaper.pdf)

[4] Joseph Poon, and Thaddeus Dryja, “The Bitcoin Lightning Network”, 2016
(https://lightning.network/lightning-network-paper.pdf)

[5] Brainbot Labs Establishment, “What is the Raiden Network?”,
(https://raiden.network/101.html)

[6] Adam Back, Matt Corallo, Luke Dashjr, Mark Friedenbach, Gregory Maxwell, Andrew Miller, Andrew Poelstra, Jorge Timón, and Pieter Wuille, “Enabling Blockchain Innovations with Pegged Sidechains”, 2014
(https://blockstream.com/sidechains.pdf)

[7] “Sharding introduction R&D compendium”,
(https://github.com/ethereum/wiki/wiki/Sharding-introduction-R&D-compendium)