FERI INFORMATION

# ビットコインの難易度調整アルゴリズムが抱える潜在的リスク

野田　俊也
東京大学大学院経済学研究科講師

ビットコイン（BTC）などの Proof-of-Work （PoW)型の暗号資産では、台帳の管理を信頼された特定の管理者に委ねず、誰もがマイナーと呼ばれる管理者になれる。マイナーはいわば独立事業主であり、強い裁量を持つ。例えば、個々のマイナーは設備投資をいつ・どのぐらい行うか、操業するかしないか、どの暗号資産に貢献するかなどを自分で選択する。ゆえに、システムがきちんと構想通りに機能するかどうかを判定するためには、暗号資産のシステムが作り出すマイニング市場の中で、マイナーがどのような行動を取るかの分析が欠かせない。

筆者は制度と市場の設計の専門家として、PoW の仕組みとマイナーの行動、そして暗号資産の安定性について複数の論文を執筆してきた。まず奥村恭平氏・橋本欣典氏との共同研究では、BTC の難易度調整の在り方が、マイナーへのインセンティブづけに失敗し、システムを不安定な状態に陥らせる可能性があることを指摘した。

暗号資産のセキュリティを保つため、PoW 型の暗号資産は、ブロック追加を人為的に難しくする仕組みを導入している。難易度（difficulty）とは、ブロック生成の難しさを定めるパラメータだ。ブロック生成の速度は難易度と、ハッシュレート（hash rate）と呼ばれるマイナーが記帳作業に注ぐエフォートの総量の比率によって決まるが、ハッシュレートは時々刻々と変化する。BTC などの暗号資産は平均して 10 分に 1 度、新しいブロックを追加することを目指しており、このためにアルゴリズムを用いて難易度を調整する。

BTC の難易度調整の方法は非常に単純だ。難易度の更新は 2016 ブロックに 1 度（ブロックが理想的に 10 分に 1 度生成されているなら2週間に 1 度に相当）行われる。BTC の方式では、過去の 2016 ブロックの生成にかかった時間と、理想的な時間である 20160 分との比率を求め、これを元の難易度に掛けた値を新しい難易度とする。過去 2016 ブロックの生成が遅すぎれば難易度を下げ、速すぎれば難易度を上げるというわけだ。

注意すべきなのは、難易度を下げる調整がブロック生成に対して2つの異なる効果を持つことだ。1つ目は、ブロックを作りやすくしてブロック生成を直接的に加速する効果。2つ目はマイニングの収益性を上げ、操業を促してハッシュレートを上昇させ、間接的にブロック生成を速くする効果だ。マイナーはブロックを生成して得られる報酬を

目的に活動するため、容易にブロックを作って報酬を得られるようになれば、非効率的なマシンも操業したくなる。このため、難易度が下がればハッシュレートは上がり、この効果によってブロック生成がさらに加速されるのだ。

BTC の難易度調整の設計では、間接効果の存在が完全に無視されており、「間接効果がゼロならば、即座に『10 分に1度』を達成する難易度を選べる」ように設計されている。したがって、ハッシュレートの変化を通じた間接効果が大きすぎれば、調整は想定通りに機能しない。間接効果の大きさは、「難易度が1%下がったとき、ハッシュレートは何%上がるか」を表す弾力性(elasticity)で測ることができる。弾力性が1よりも大きい場合、BTC は過剰に難易度を調整してオーバーランを引き起こしてしまい、ブロック生成速度を「10 分に1度」からむしろ遠ざけてしまう。結果として、いつまで経っても目標となる速度を達成できない。

BTC のハッシュレートの弾力性は、マイナーの産業構造によって決まるが、現状どの程度の値なのだろうか？ 筆者の川口康平氏との共同研究では、BTC と、そこから分岐した暗号資産であるビットコインキャッシュ(BCH)・ビットコイン SV(BSV)のハッシュレートの弾力性を、2020 年の半減期(halving)の前後におけるハッシュレートの変化を観察することにより、推定した。半減期では、難易度ではなく、ブロック生成に対する報酬の調整が行われるが、いずれの調整も報酬の期待値の変化であり、ハッシュレートに対して同様の効果をもたらすと考えられる。ゆえに、このデータを使えば弾力性を正確に推定できるのだ。

推定結果によれば、BTC のハッシュレートの弾力性は 0.63 であり、閾値である1よりも小さい。加えて、BTC の難易度の変化は、市場を通じて BCH や BSV の難易度調整にも影響を与え、そしてその揺り戻しを受ける。この影響を加味した弾力性は 0.63 よりさらに小さくなる。この非弾力的なハッシュレートのおかげで、BTC は原始的な難易度調整の方法でも生き延びてきたが、この状態が未来永劫続く保証はない。ハッシュレートの弾力性はマイニング市場の状況によって決まるが、これが現在と同じであり続けると考える理由はまったくない。現に、これまでもマイニング市場の在り方は時勢とともに大きく変化してきた。

実際、BTC 以外の暗号資産に対するハッシュレートの弾力性は1よりもはるかに大きい。BCH と BSV の弾力性はそれぞれ 5.4 と 4.9 と推定された。にもかかわらず、BCH や BSV が安定している理由は、高い弾力性のもとでも機能する難易度調整の方法を採用したからだ。裏を返せば、BTC の難易度調整が抱える潜在的なリスクは、後発の方式を採用するだけで簡単に取り除ける技術的には簡単な問題だ。

筆者がむしろ懸念するのは、このような「明確な解決策が存在する潜在的なリスク」が放置されている状態そのものである。通貨システムは、潜在的なリスクを放置してよい種のサービスではなく、危険因子をあらかじめ徹底的に潰すことができなければ、将

来大きな問題を発生させうる。暗号資産が「顕在化していないリスクを未然に、素早く潰す」ことを徹底できなければ真に安定なシステムとなる日は来ない。システムが修正されないのは、単に開発コミュニティが問題を認知していないためかもしれないが、修正のための意見統一が難しいという分権的なシステム特有の事情に起因する可能性もある。もし後者の仮説が正しければ、これは暗号資産の致命的な弱点となりうる。

参考文献

Noda, S., K., Okumura, and Y. Hashimoto (2020): "An Economic Analysis of Difficulty Adjustment Algorithms in Proof-of-Work Blockchain Systems," in Proceedings of the 21st ACM Conference on Economics and Computation. https://ssrn.com/abstract=3410460

Kawaguchi, K., and S. Noda (2021): "Miners' Reward Elasticity and Stability of Competing Proof-of-Work Cryptocurrencies," Working Paper. https://ssrn.com/abstract=3974376