# ブロックチェーンのトリレンマを表現する数式を発見

## ―性能・安全性・分権性のうち２つだけが成立することを立証―

**概要**

ブロックチェーンのトリレンマ（図 1）は、2017 年に提唱されて以来、開発者・研究者の間で広く信じられています。これは、性能（scalability）と安全性（security）、そして分権性（decentralization）の 3 つにはトレードオフがあり、同時には 2 つまでしか成立しないという経験則です。ただし、あくまで経験則であり、これまで数理的に表現されたことはありませんでした。

京都大学 大学院情報学研究科 中井大志 博士課程学生、櫻井晶 同博士課程学生、京都大学 学術情報メディアセンター 廣中詩織 助教、首藤一幸 同教授らの研究グループは、ブロックチェーンのトリレンマを表現する数式を発見しました。具体的には、Proof of Work 型のブロックチェーン（例：Bitcoin）において、安全性を下げるフォークという現象が起きる確率の逆数を安全性の指標とした場合に、その項と、性能を表す項、分権性を含む項、それら 3 項の積が一定である、つまり 3 項がトレードオフであるという数式を得ました。

本研究成果は、2024 年 6 月 5 日に、国際学術誌「IEEE Access」にオンライン掲載されました。

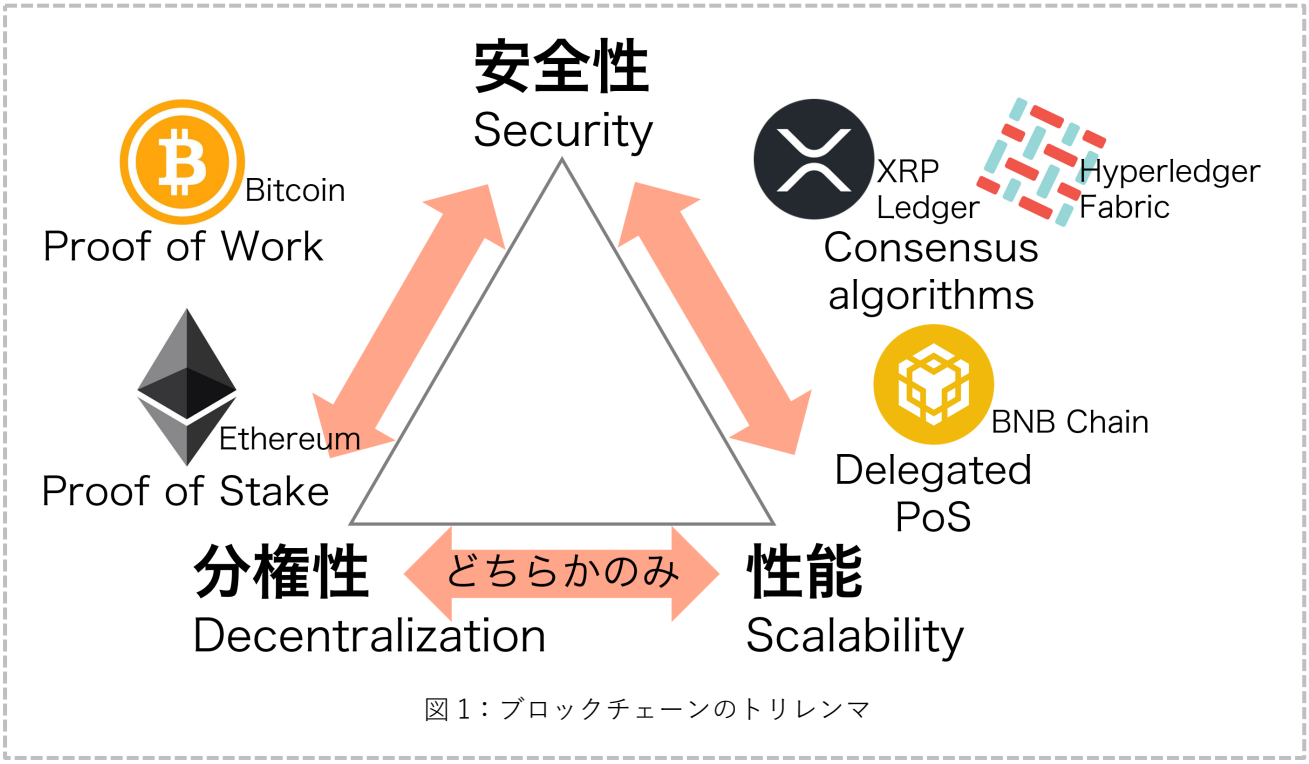


図 1：ブロックチェーンのトリレンマ

## 1．背景

ブロックチェーンは、2008 年に Bitcoin が提案されて以来、暗号通貨のみならず、スマートコントラクト、NFT、DeFi（分散型金融）、新しい形の人間組織 DAO など様々なイノベーションの基盤となってきました。当初、Bitcoin の性能はとても低く、1 秒間に処理できるのはわずか 7 トランザクションでした。そのため、性能向上の試みが盛んになされました。現在、あるブロックチェーンは数千、数万トランザクション毎秒（TPS）をうたい、Ethereum はシャーディングという技術を導入予定で 10 万 TPS を目指しています。

しかし、情報システムの設計にはトレードオフが付きものです。性能向上が、その陰でひそかに何を犠牲にしているか、あまり明らかではありません。そんな中、2017 年、Ethereum 創始者の 1 人である Vitalik Buterin 氏が、ブロックチェーンのトリレンマを提唱しました。つまり、性能（scalability）、安全性（security）、分権性（decentralization）の 3 つはトレードオフの関係にあり、同時には 2 つまでしか成立しない、という法則です。これは経験則であって、これまで数理的、定量的な裏付けはありませんでした。3 要素の定義もおおざっぱなもので、例えば安全性は「システム規模 n に比例するリソースを持つ攻撃者に対して安全」といった具合いです。どういう攻撃なのか、安全とはどういう状態なのかについては、何も述べていません。

## 2．研究手法・成果

我々の研究グループは、ブロックチェーンの安全性について研究を進める中で、安全性を表すフォーク発生確率 F を厳密に算出する数式を見出していました（櫻井 2023）。F を表す数式をよく観察すると、その中に、安全性だけでなく性能も現れていることに気が付きました。安全性と性能といえばトリレンマに現れる 3 要素のうちの 2 要素です。ということは、この数式を適切に変形することで、トリレンマを表す数式を得られるかもしれない、と着想しました。

$$\frac{B_h + B_{tx} \cdot n_{tx}}{T} \cdot \frac{1}{F} \cdot \boldsymbol{H}^\top \boldsymbol{P} \boldsymbol{H} = 1$$

TPS

性能 Scalability　安全性 Security　分権性 を含む項 Decentralization

$B_h$ : ブロックヘッダのサイズ　　$T$ : ブロック生成間隔
$B_{tx}$ : トランザクションのサイズ　　$F$ : フォーク発生率
$n_{tx}$ : ブロックに含まれるトランザクションの数

$$\boldsymbol{H} = \begin{pmatrix} H_1 \\ H_2 \\ \vdots \\ H_n \end{pmatrix} \qquad \boldsymbol{P} = \begin{pmatrix} 0 & t_{12} & \cdots & t_{1n} \\ t_{21} & 0 & \cdots & t_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ t_{n1} & t_{n2} & \cdots & 0 \end{pmatrix}$$

$H_i$ : ノード $i$ の
ハッシュレート割合
$\Sigma H_i = 1$

$t_{ij}$ : ノード $i$ が生成したブロックが
ノード $j$ まで到達するのに要する時間
/ ブロックのサイズ

図 2：トリレンマを表現する数式

そして、変形によって得たのが図 2 の数式です。性能は素直にトランザクション毎秒で表されます。安全性を下げるフォークという現象の発生確率 F の逆数が、この式における安全性の表現です。

そして、第 3 項が分権性を表します。この項は、ブロックチェーンを構成するマイナー（コンピュータ）群

のハッシュレート［用語 1］と、マイナー間の通信性能を含みます。通信性能はインターネットの状況などによって千差万別ですが、もし、どのマイナー間でも通信性能（$t_{ij}$）が等しいとしたら、第 3 項は「定数 ×（1 - ハッシュレートのハーフィンダール・ハーシュマン指数)」という形をとります。ハーフィンダール・ハーシュマン指数（以降 HHI）は経済分野の概念で、ある業界の市場がどのくらい一部企業に集中しているか、を表す集中度合いの指標です。第 3 項はハッシュレートの HHI、すなわち集中度合いに負の符号が付いており、つまり、ハッシュレートが一部のマイナーに集中しているほど値が小さくなる、という形で分権性を表します。

**３．波及効果、今後の予定**

トリレンマを表現した式を観察することで、安全性と分権性を犠牲にせずに性能を向上させるための方針が見えてきます。それは、ブロックそれ自体やトランザクション（$B_h$ や $B_{tx}$）を小さくする方針と、ブロックの送受信（**P**）を速くする方針です。また、既存の手法がどういった原理で性能向上を果たしているのかを分析できます。例えば、Bitcoin が採り入れた Compact Block Relay という手法は、トランザクションのサイズ $B_{tx}$ を小さくすると同時に通信にかかる時間 **P** の値を小さくすることで性能向上を果たしています。また、新手法への示唆も得られます。例えば、第 3 項の値を効果的に小さくするためには、ハッシュレートの大きいマイナーを対象として重点的に通信性能を向上させればよいことがわかります。これは、現実世界では、マイニングプール［用語 2］間の通信を速くすることに相当します。

今回の成果は Proof of Work（PoW）型ブロックチェーンが対象です。一方、2022 年 9 月、Ethereum が Proof of Stake（PoS）に移行したことが示す通り、PoS 型の重要性も増しています。今後、PoW 型以外のブロックチェーンについてもトリレンマの数理的表現を探していきます。

**４．研究プロジェクトについて**

本研究は次の御支援の元、実施されました。
・JSPS 科研費 JP21H04872、JP24H00691
・JSPS 特別研究員奨励費 JP24KJ1517
・JST 次世代研究者挑戦的研究プログラム JPMJSP2110

**＜用語解説＞**

[用語 1] ハッシュレート：　ブロックチェーンに参加するマイナー（コンピュータ）は、ブロックの生成に成功すると報酬を得られます。各マイナーは、ハッシュ値計算という処理を行うことでいわばくじを引き、当たりを引くとブロックを生成でき、暗号通貨の報酬を得られます。ハッシュレートとは、このハッシュ値計算を 1 秒あたり何回行えるか、という性能値です。

[用語 2] マイニングプール：　1 人で用意できる機材でハッシュ値計算を行って自分自身で当たりを引ける、そんなことが起こる確率は天文学的に低いものです。マイニングプールというサービスに参加して、その一員としてハッシュ値計算を行うと、自分自身で当たりを引かずとも、計算による貢献に応じて報酬の分配を受けることができます。

**＜研究者のコメント＞**

2008 年に Bitcoin が提案されて以来、ブロックチェーンの周辺領域ではイノベーティブな試みが絶えません。理由の 1 つは、ブロックチェーンが備えるトラストレスという性質でしょう。この性質が、それまで国や大組織にしかできなかったこと、つまりはお金（のようなもの）の発行や金融サービスを個人にまで開放しました。ブロックチェーンと表裏一体である暗号通貨が人々の欲望を刺激するという点も見逃せません。資本主義が人の欲望を燃料に社会を前に（？）進めるのと似たものを感じます。

ものすごいスピードで様々なトライが行われる一方、成果を人類の知識として積み重ねていく営み、つまり研究の方が追いついていない感があります。我々も、新しいトライに直結する工学的な研究とともに、今回の成果のような、裏側にある構造を解明する理学的な研究も一層進めていきます。

**＜論文タイトルと著者＞**

タイトル：A Formulation of the Trilemma in Proof of Work Blockchain（Proof of Work 型ブロックチェーンにおけるトリレンマの定式化）

著者：中井大志, 櫻井晶, 廣中詩織, 首藤一幸

掲載誌：IEEE Access　DOI：10.1109/ACCESS.2024.3410025