

BTCC “**新規口座開設限定**”

BTCC口座開設&入金で、最大**17500USDT**が獲得できる。  
お友達を紹介するとさらにボーナスをプレゼント!

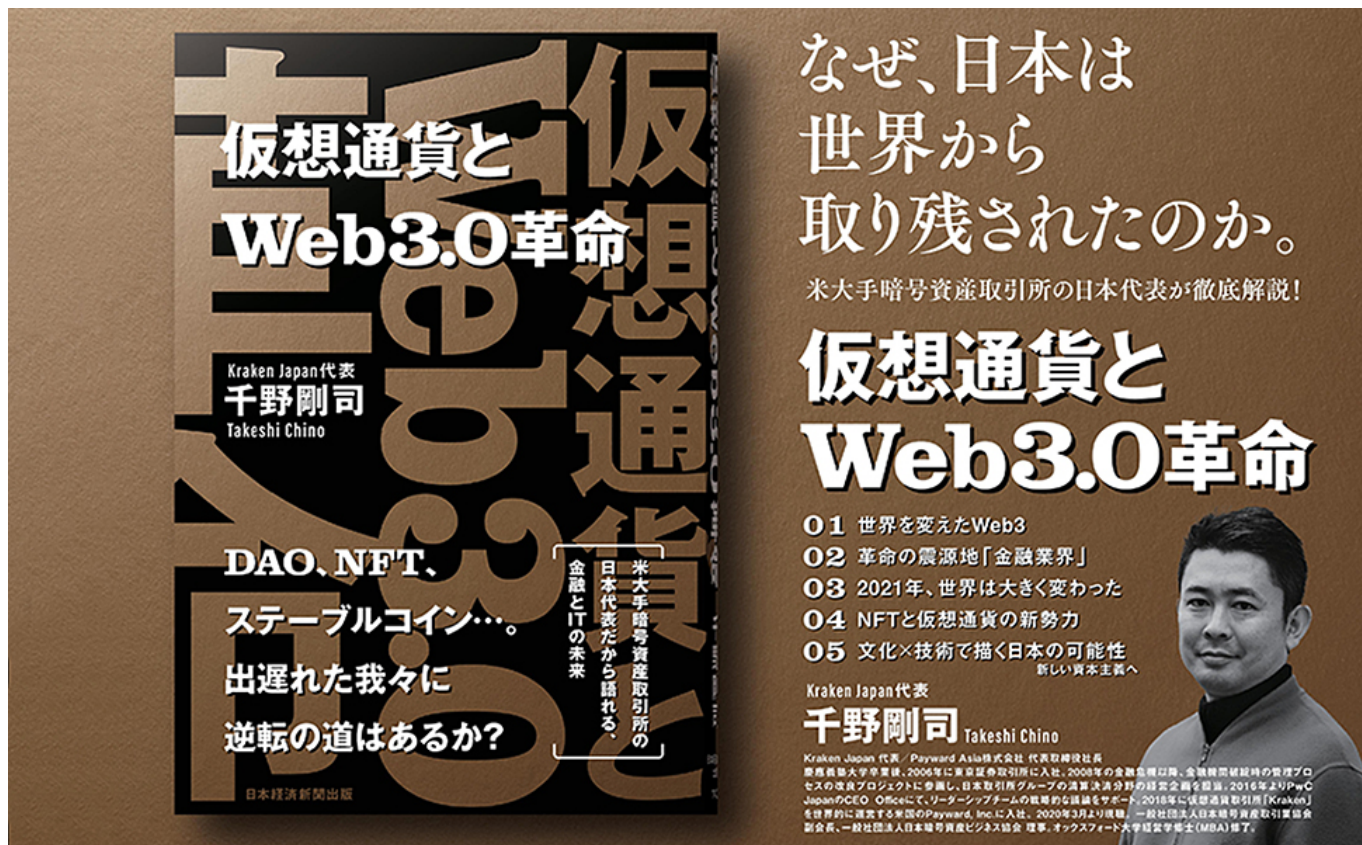
今すぐ口座開設/詳細はこちら



## 「イーサリアム2.0で何が変わるのか」：千野剛司

原文:

<https://www.btcc.com/ja-JP/academy/research-analysis/what-will-change-with-ethereum-2-0>



## 「仮想通貨とWeb3.0革命」：千野剛司

米大手暗号資産取引所「Kraken（クラークン）」の日本法人 Kraken Japan 代表である千野剛司氏が、先日初の著書『仮想通貨とWeb3.0革命』を上梓した。

古くから金融業界に身を置いてきた千野氏独自の視点で、これまでの暗号資産（仮想通貨）市場の歴史や、[DAO](#)、[NFT](#)、[ステーブルコイン](#)ほか、仮想通貨とWeb3をめぐると最新の動向を解説した書籍だ。

千野氏は書籍を通じ、かつての仮想通貨大国だった日本がこれから復活の道があるのか、その課題や可能性について語っている。

### イーサリアム2.0で何が変わるのか？

今回は著書『仮想通貨とWeb3.0革命』の「第4章 NFTと仮想通貨の新勢力」の「2 イーサリアム2.0で何が変わるのか」の内容を公開する。

注目すべきは「ステーキング」と「シャーディング」

---

[イーサリアム](#)は、このままイーサリアムキラーにやられっぱなしというわけではありません。スケーラビリティの問題を認識し、取引記録を保管するブロックスペースで発生する「渋滞」を解消しようと既に動き出しています。これが「イーサリアム2.0」と呼ばれる大型アップグレードです。

イーサリアム2.0は、最近、コンセンサスレイヤーという名称に変更されました。理由は、今のイーサリアム（イーサリアム1.0）と異なるものができるわけではなく、あくまでももともとあったイーサリアムの構想の一つとしてのアップグレードだからといわれています。しかし「イーサリアム2.0」は既に業界的に定着した用語であることから、本書では、便宜上「イーサリアム2.0」を使いたいと思います。

イーサリアム2.0の目玉となるのが、イーサリアムの「[ステーキング](#)」と「シャーディング」です。ステーキングは、一定の仮想通貨をネットワークに保管して取引記録の検証に貢献することで報酬をもらう行為です。シャーディングとは、データベースを分割することで負荷を分散させる技術を指します。

## 取引記録に関する合意形成で重要な2つのアルゴリズム

---

まずは、「ステーキング」を理解する上で、取引記録にまつわる合意形成に関する2つのアルゴリズムであるプルーフ・オブ・ワーク（PoW）とプルーフ・オブ・ステーク（PoS）の違いについて押さえましょう。ブロックチェーンは「みんな」で取引記録の台帳を管理するため、合意を得る必要がありますが、ブロックチェーンごとにそのルールが異なります。

時価総額1位の[ビットコイン](#)が採用しているのがPoWです。先の章で解説した通り、世界中に個別に存在する「見知らぬ」コンピューター同士が取引記録の承認をめぐって合意する[マイニング](#)という仕組みがビットコインのネットワークを支えています。PoWは、マイニングを機能させるための経済的なインセンティブを定めたアルゴリズムです。

先の章では、マイニングとは、コンピューターを使って難解なパズルを解くことでブロックをブロックチェーンに追加する作業と説明しました。これは、具体的には、ハッシュ値という64桁の数字とアルファベットの羅列を探す演算競争なのです。

ハッシュ値には一方向にしか演算できないという特性があり、ハッシュ化されたデータから逆方向に元データを推測することは、現在のコンピューターでは不可能といわれています。この点が、ブロックチェーンの記録は改竄不可能といわれるゆえんです。

64桁の数字とアルファベットの羅列であるハッシュ値に関する話は数学や暗号学が関連するので難しくなりますが、マイナーが条件を満たすハッシュ値を見つけるには「スピード」と「運」が必要と覚えてください。このため、マイニングを事業とする場合、処理能力の高い複数のコンピューターを同時に稼働させて、「どれかが当たる」確率を上げようとするのが通常です。このため、マイニングには大量の電力が必要なのです。

## 世界中の企業が巨額の資金を投じるマイニング設備

---

現在、世界中の企業がマイニング施設の建設や機器購入に巨額のマネーを投じています。

米国ではナスダック市場を中心にマイニング企業が複数上場しています。

マイニングで消費する大量の電力が環境に悪いとの声が世界中から出ています。有名なのは、テスラのイーロン・マスク氏が、「環境への負荷」を理由にテスラ車を買う際の支払い手段としてのビットコインの受け入れを取りやめたことでしょう。

ただ、最近では北米を中心に再生可能エネルギーを使ったマイニングへの意識が高まっています。ビットコイン・マイニング協議会によりますと、2021年時点で既に世界のマイニングに必要な電力の56%が再生可能エネルギーでまかなわれています。

対照的にPoSは、環境フレンドリーな合意形成アルゴリズムといわれています。イーサリアム財団は、PoSに移行したらPoWで使う電力消費量の99.95%を削減できるという試算を発表しました。PoSは、高性能のコンピューターを必要とせずスマートフォンからの参加が可能です。

PoSにはマイナーが存在しておらず、代わりにバリデーターと呼ばれる存在が取引記録の検証を行います。一定の仮想通貨をPoSのネットワークで長期保有（ロック）することで、バリデーターとしてブロックを検証・承認するタスクがランダムに割り当てられます。

その対価として仮想通貨を報酬として受け取ります。これが、ステーキングと呼ばれます。これにより、PoWで見られたようなマイニング事業者の競争がなくなり、電力の消費量が大幅に削減されることになります。

イーサリアムのステーキングは、一部で既に開始されています。これは、2020年12月に立ち上がったイーサリアム2.0の基盤となるブロックチェーン（ビーコンチェーンと呼ばれる）を使って行われています。これを現在のイーサリアムのブロックチェーンと統合することで、イーサリアムのPoSへの完全移行が実現します。イーサリアムのPoSへの移行は、「統合（TheMerge）」と呼ばれており、2022年中に実施される予定です。

さて、環境問題もちろん大切ですが、PoSはスケーラビリティ問題の解決とどのように関係しているのでしょうか？ PoSは、イーサリアム2.0のもう一つの目玉であるシャーディングを実施するために必要であり、シャーディングが直接的なスケーラビリティ問題への対策として位置づけられます。

## 取引処理能力はどこまで改善されるのか

---

シャーディングとは、データベースを分割することで負荷を分散させる技術を指します。イーサリアムの場合、シャーディングによりネットワークをさらに64の新しいチェーンに分割することで、取引処理能力向上を目指します。分割されたチェーンを「シャード」と呼びます。

それぞれのシャードは、独自のブロックチェーンとして機能し、それぞれバリデータがランダムに割り当てられます。バリデータは、各シャードで取引記録の検証・承認を行いブロックを追加します。シャードのおかげで、イーサリアムの過去の取引記録を分散して保管することができます。バリデータはブロックチェーン全体ではなく、各シャードの取引記録を検証すればよくなります。

### シャーディングの仕組み

---

先ほど、PoSとシャーディングが補完的な関係にあると話しました。なぜならもしPoWのままシャーディングを導入すれば、高いコンピューティング力を用意したマイニング業者が、一つのシャードを乗っ取ってしまう可能性があるからです。

ブロックチェーンを64分割すれば、そのうちの一つで51%以上のハッシュレートを獲得するのは比較的容易になるというわけです。PoSの場合は、ステーキングを行うバリデータは「ランダム」に選ばれるので、この危険性はなくなります。

イーサリアム財団によりますと、シャードチェーンの導入は2023年と推定されています。現在イーサリアムは、開発者のリソースや利用者数で他を圧倒しており、NFTなど業界最先端技術の受け皿となっています。

あまりにも人気が続いたために取引承認の「渋滞」というスケーラビリティの問題に直面していますが、改善に向けて実際に動き出しています。

「秒進分歩」で進む仮想通貨業界において、問題なのは開発スピードでしょう。イーサリアム2.0の進捗が予定通り進んでいることで開発者や利用者を安心させ、ガス代高騰が長続きしないことを示すことが、イーサリアム成功のカギとなるかもしれません。

## 【仮想通貨とWeb3.0革命】書籍情報

---

千野 剛司（著）/日経BP 日本経済新聞出版

## 【内容紹介】

出遅れた我々に復活の道はあるのか？

2014年頃、日本には世界一のビットコイン取引所があった。2017年末に仮想通貨相場の盛り上がりを牽引したのも日本の投資家だった。その後、仮想通貨の「冬の時代」を経て、2020年末、米国を中心に世界が再び仮想通貨に目覚めた。しかし、かつての仮想通貨大国の日本は眠りについたらまだだった……。

DAO、NFT、ステーブルコインほか、仮想通貨とWeb3をめぐる最新の動向を解説。  
米大手暗号資産取引所の日本代表だから語れる、金融とITの未来！

[→書籍を購入する \(Amazon\)](#)

## 著者千野剛司について

---

Payward Asia株式会社 代表取締役社長 / Kraken Japan 代表

慶應義塾大学卒業後、2006年に東京証券取引所に入社。

2008年の金融危機以降、金融機関破綻時の管理プロセスの改良プロジェクトに参画し、日本取引所グループの清算決済分野の経営企画を担当。

2016年よりPwC JapanのCEO Officeにて、リーダーシップチームの戦略的な議論をサポート。

2018年に仮想通貨取引所「Kraken」を世界的に運営する米国のPayward, Inc.に入社。

2020年3月より現職。一般社団法人日本暗号資産取引業協会 副会長、一般社団法人日本暗号資産ビジネス協会 理事。オックスフォード大学経営学修士（MBA）修了。

### ▶ 仮想通貨の将来性・買い方など

[仮想通貨ファイルコイン\(FIL\)は怪しい？ 将来性や買い方・おすすめ取引所を徹底解説](#)

[仮想通貨BSV\(ビットコインSV\)の将来性は？ 今後予想や買い方など徹底解説](#)

[エイプコイン \(ApeCoin/APE\) の将来性は？ 今後予想や買い方など徹底解説](#)

[ユニスワップ \(Uniswap/UNI\) とは | 仕組み・特徴・将来性](#)

[暗号資産NEAR\(NEAR Protocol\)とは？ 特徴と用途を解説 | 用語集](#)