GLOBAL X ETFs リサーチ

イーサリアム：基礎編

執筆：
デジタル資産チーム
GLOBAL X リサーチ

日付：2022 年 3 月 1 日
トピック：デジタル資産

編集者注記：オレンジ色で表示された用語は、すべて用語集を掲載されています。

2009 年に誕生したビットコインは、ブロックチェーン技術を使用した有限供給型の分散型通貨として、最初の成功を収めました。重要なのは、誰もが利用できるということでした。ビットコインは、ブロックチェーン技術の安全性、透明性、拡張性に裏付けされた幅広いツールやアプリケーションが開発されるきっかけとなりました。ビットコインのネットワークは、交換媒体の基盤を提供する一方で、若いプログラマーたちは、経済全体の中央集権的な存在に挑戦できる手法と捉えました。

わずか 19 歳のヴィタリック・ブテリンは、2013 年にイーサリアムに関するホワイトペーパーを発表し、開発者がプログラム可能な条件とアプリケーションを構築できる斬新で汎用性のあるブロックチェーンネットワークを紹介しました。要は、ブロックチェーン技術についての考え方、構築の仕方、そして展開の仕方に革命をもたらすプログラム可能な通貨システムを創出したのです。

イーサリアムについて知っておくべきこと、その構造と機能

イーサリアムのステイタスが高まり、今後投資も増えると考えられることから、本稿ではまずイーサリアムネットワークについて、基本的な質問にお答えします。

- **イーサリアムとは何か？**：スマートコントラクト機能を持つ分散型ブロックチェーンです。
- **イーサ（ETH）とは何か？**：イーサリアムのネイティブ通貨です。
- **ノードとは何か？**：取引やブロックを検証するためにイーサリアムクライアントが稼働しているコンピュータのことです。
- **マイニングとは何か？**：特殊なノードが、数学的パズルを解き、チェーン上で次のブロックを創り出すことです。
- **本当の意味での決済タイミングはいつか？**：取引によって十分な数のコンファメーションが発生したときです。
- **スマートコントラクトとは何か、それが重要なのはなぜか？**：あらかじめ定義された条件に基づいてプログラム可能な契約のことです。
- **分散型アプリケーション（DApps）とは何か、それが重要なのはなぜか？**：スマートコントラクトを利用して構築されたアプリケーションのことです。
- **イーサリアムネットワークは今後どうなるか？**：ネットワークのスケーラビリティと環境に配慮したコンセンサスメカニズムに移行します。
- **ETH に価値があるのはなぜか？**：ネットワークの経済を左右するものであるからです。
- **なぜ今、イーサリアムなのか？**：最大で最も利用されているスマートコントラクトのブロックチェーンであり、価値の可能性と成長をもたらすからです。

イーサリアム：スマートコントラクトの機能を持つブロックチェーン

2015 年 7 月に登場したイーサリアムは、チューリングコンプリート言語を組み込んだ斬新なブロックチェーンを採用しています。この言語は、ロジックを組み込むことにより、単純な決済よりも高度な取引を完結させることのできるプログラミング言語です 。この言語の導入により、開発者たちはアプリケーションを作成してイーサリアムに統合することにより、スマートコントラクトや分散型アプリケーション（DApps）をホストできるオープンなエコシステムのベースレイヤーとして機能させることができるようになりました。

イーサリアムの価値提案の大部分はスマートコントラクトにより成立しています。スマートコントラクトは、プログラムされた条件に基づいて自己実行する定義済みの基準を持ち、合意事項はブロックチェーンに記録されます。スマートコントラクトは、第三者の介入を排除します。

DApps は、スマートコントラクトのプログラマビリティから作り出され、展開されるフロントエンドのユーザー対象型アプリケーションです。こうしたプログラム可能なコントラクトは、分散型金融サービスアプリケーション（DeFi）や、唯一無二の資産のデジタル所有権を表す非代替性トークン（NFT）を生み出すために使用されます。また、スマートコントラクトは、自律分散型組織（DAO）と呼ばれる分散型ガバナンスエンティティを生み出し、連携させるためにも使用されます。ネットワーク内の DApps のユニバースは、イーサリアムのエコシステムを表しています。

イーサリアムのネットワークは、完全に透明性を持つブロックチェーン技術を使用して、取引を記録し、台帳上でその状態を追跡します。ネットワーク参加者は、取引とブロックをプロトコルのルールに照らして独自に検証することで、ブロックチェーンの分散型台帳上で合意した状態（コンセンサス状態）を見つけることができます。ブロックは、集合的な取引リストから構築される個々のデータ構造であり、その親ブロック、つまり前のブロックへの参照も含まれています。

イーサリアムの分散型ステートマシンであるイーサリアム仮想マシン（EVM）は、ネットワークのデータ構造と標準を維持する役割を担っています。つまり、EVM はブロック間の状態の遷移を計算するためのルールを定義しています。状態の遷移は、口座残高の単純な変化であったり、より複雑なスマートコントラクトの相互作用の結果である場合もあります。

イーサ（ETH）：イーサリアムネットワークを支えるネイティブ暗号通貨

イーサ（ETH）は、ビットコインと同様、単純な支払送金に使用できますが、主としてイーサリアム上で分散型コンピューティングの支払いに使用されるため、通貨というより商品に近い存在と言えます。イーサリアム上のすべての取引とスマートコントラクトの展開には、ETH で支払うべき変動手数料が必要です。単純な支払いは通常、スマートコントラクトのやり取りよりも安価で実行できます。イーサリアムの DApp のエンドユーザーは、プラットフォームとやり取りを行うためには ETH を購入する必要があるため、こうした支払いスキームは ETH に対する自然な需要を生み出します。

ETH は物理的な存在ではなく、対応する秘密鍵を持つ人が所有する無記名のデジタル資産です。ビットコインと同様、イーサリアムは公開鍵暗号方式とデジタル署名を使用して、悪意を持つ者が他人の ETH を使用することを防ぎます。公開鍵暗号方式とデジタル署名の詳細については、「ビットコインの 基本」をご覧ください。

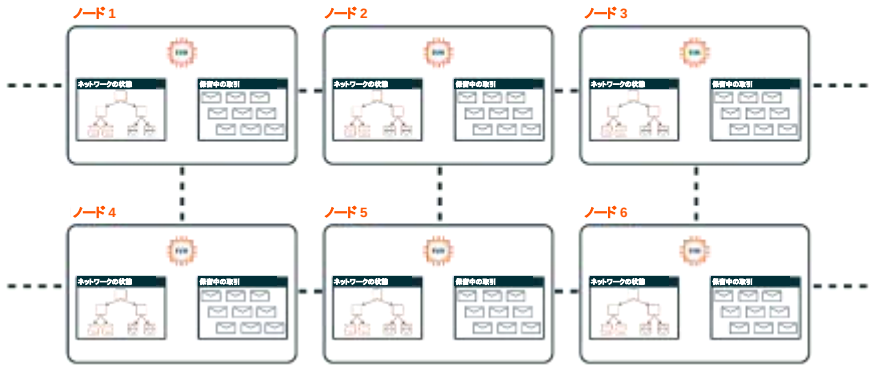
ETH は、1 ビットコイン（BTC）当たり 2,000ETH の価格で 2014 年 9 月 2 日に初めて市場に登場しました。現在、ETH は時価総額 3,560 億ドルの第 2 位の暗号通貨となっています [1]。

イーサ（ETH）の現在の価格
出所：Etherscan.io、2022 年 3 月 1 日現在

ノード：コンピュータが取引を検証し、ネットワークを保護

ノードとは、イーサリアムクライアントを稼働させているイーサリアムネットワークの中のコンピュータを指します。イーサリアムクライアントは、イーサリアムプロトコル、つまりネットワークのルールを実行させるソフトウェアです。イーサリアムネットワークは、接続されたノードの集合体であり、各ノードは、受け取った取引やブロックがプロトコルのルールの下で有効であることを検証した上でブロックチェーンに記録します。

相互に接続されたノードのネットワーク
出所：Global X ETFs

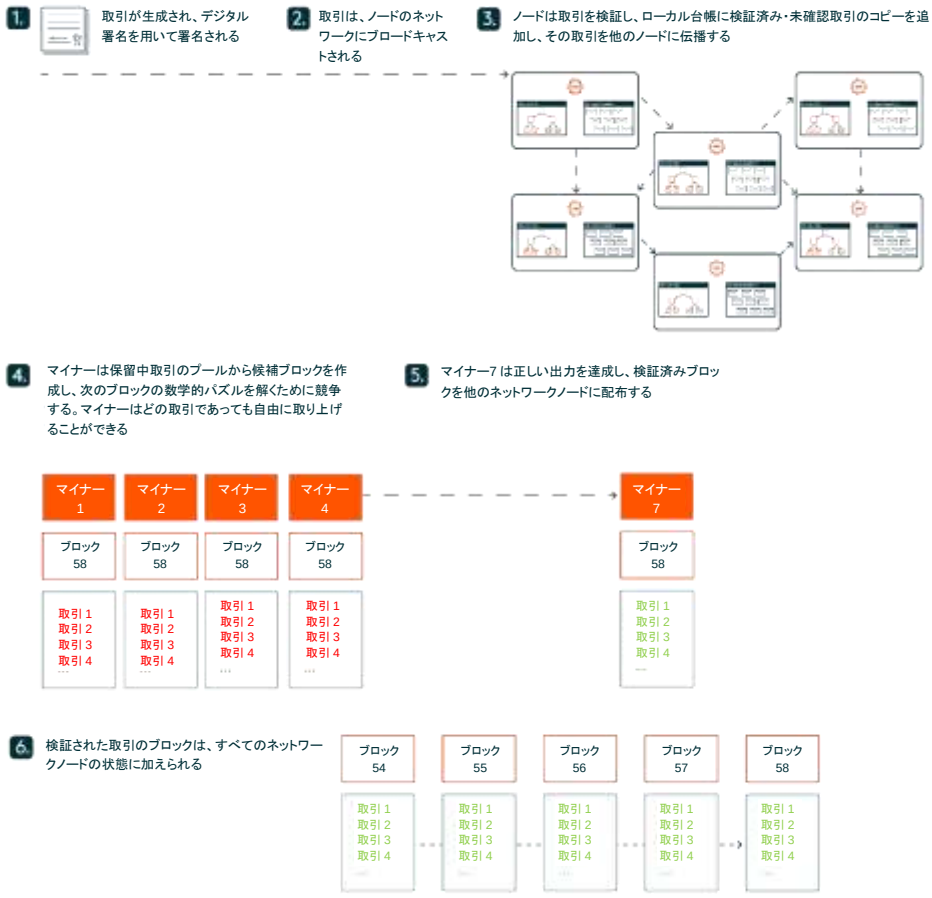


取引はネットワーク内のデータの状態を変更するものであり、一般的にはデジタル資産の移転やスマートコントラクトの実行が関係しています。すべての取引には、ガス代と称される ETH 建て取引手数料を含める必要がありますが、これはブロックチェーン上で取引を公開、検証、実行、保存するためのコストです。

取引がユーザーの秘密鍵で電子署名されると、接続されたノードのネットワークにブロードキャストされます。ノードが新しい取引を受け取ると、イーサリアムクライアントは、デジタル署名の評価を含め、プロトコルのルールに概説されている一連の包括的基準に照らしてこの取引の有効性を独自に検証します。取引が有効であれば、ノードはその取引を保留中の取引のローカルプールに保存し、さらに隣接する全ノードに伝播します。このように相互接続されたノードのネットワークにより、すべての参加者が数秒のうちに取引を分散し、検証し、記録することが可能になります。

イーサリアム取引の流れ

出所：Global X ETFs



マイニングノード：数学的パズルを解き、次のブロックを作成する特殊なノード

全てのイーサリアムノードは独自に取引の検証を行いますが、マイニングノードは特殊なタイプのもので、ブロック内に取引を集め、これらのブロックを決済のためにブロックチェーンに記録する役目を果たします。その意味で、マイニングノードはチェーン内でブロックを作成するという点において、他とは区別されます。

各ノードは、検証済みだが保留中の取引のプール（メモリプール）を維持します。マイナーが採掘したブロックにその取引を含めると、その取引はメモリプールから削除されます。マイニングノードは、難解な数学的パズルを誰よりも先に解くため、計算のためのリソースを大量に必要とします。パズルの解は、ネットワークの整合性を確保するためのコンセンサスメカニズムであるプルーフ・オブ・ワークと呼ばれています。

このパズルは激しい競争の末に解明されることになるのですが、マイニングノードはなかなか得られないアウトプット（ハッシュ値）を求めて、暗号学的ハッシュ関数を通して多くの異なる入力を繰り返すことになります。イーサリアムはビットコインとは異なる暗号ハッシュ関数に依存しており、マイナー同士が直接競争を繰り広げることはありません。プルーフ・オブ・ワークを見つけ出すのは難しいのですが、どのノードもわずかながら、マイニングノードがこの解明法を見つけ出そうと計算リソースを消費していることを検証することができます。有効なデジタル署名がある場合にのみ取引が有効であるとみなされるのと同様、候補ブロックが有効になるには、プルーフ・オブ・ワークが必要となります。他の参加者よりも早くプルーフ・オブ・ワークを通じて特定のアウトプットを達成することで、マイナーは候補ブロックを検証、記録、伝搬することができます。

マイナーが次のブロックの数学的パズルを最初に解いた場合、ネットワークを通じて検証済みブロックをブロードキャストします。それぞれのノードは新たに受領したブロックの有効性を検証し、自身のブロックチェーンのコピーの中に取り込みます。新たに有効なブロックが取り込まれれば、ここでマイニングゲームは終了します。すべてのマイナーが、取引の新たな候補ブロックを作成し、ブロックチェーンに含まれるべき次のブロックのパズルをいち早く解こうとします。通常 12 秒から 14 秒のブロックタイムが、こうした新しいブロックの絶え間ない流れを決定づけます。さらに、ブロックサイズは制限されており、保留中の取引のすべてがブロックに含まれるわけではありません。

マイナーは、このパズルを最初に解くことで金銭的なインセンティブを得ることができます。新たなブロックを、有効なプルーフ・オブ・ワークとともに最初に送信したマイナーは、2 ETH のブロック報酬とそのブロック内の全てのガス代の一部を要求することができます。さらに、ブロック内の取引に順序を設定することや、フロントランニング戦術により、マイナーはマイナー抽出可能価値（MEV）と呼ばれる増分収益の流れを生成することができます。

ブロック内のガス代は、基本料金とチップに分別され、いずれもブロックスペースの需要に応じて価格が変動します。チップは、ブロックに取引を優先的に組み込むことのインセンティブとしてマイナーに直接支払われます。基本料金は、燃やされ、対応する ETH は流通量から削除されるという点で、自社株買いに似ています。

イーサリアム改善提案（EIPs）は、ネットワーク参加者やビルダーが常にイーサリアムネットワークの改善を進めることができるよう、インセンティブを付与する設計になっています。そのような提案の 1 つが、こう

したガス代の構造です。2021 年 8 月のイーサリアム改善提案 1559（EIP-1559）を通じて実施された改善により、ネットワーク使用量と ETH 発行量の間に直接的な相関関係が生まれました。

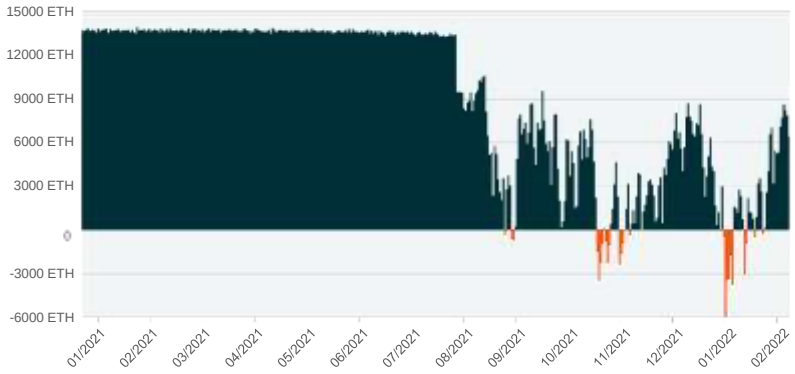
EIP-1559 は、燃焼メカニズムを介して正味の供給発行率が低下するため、ETH 保有者に価値が生じます。より多くの取引がオンチェーンで行われることで、より多くのガスが燃焼され、ブロック報酬から生まれる新たな ETH の供給の影響を減少させるか、排除される可能性が生じます。ネットワークへの需要が高く、燃焼メカニズムがブロック報酬による新規発行を上回った場合、

ETH はデフレ資産になる可能性があります。EIP-1559 のロールアウト以降、現在までに 190 万 ETH 以上が燃やされ、ETH の純発行量は 68%以上減少しました [2]。

NFT の人気の高まりと、NFT が生み出す取引量により、ブロックスペースへの需要は高まり、燃やされる ETH の量も増加しています。NFT のマーケットプレイスである OpenSea は、EIP-1559 のロールアウト以降、最も多くのガス代を燃やしており、その合計は 230,041 ETH に達しています [3]。

燃焼が発行率に及ぼす影響（取り扱い開始以来）

出所：Etherscan.io、2022 年 3 月 1 日現在



本当の意味での決済：取引によって十分な数のコンファメーションが発生したとき

取引がブロック内に取り込まれ場合、「決済された」としばしば言われます。しかし、ブロックチェーンが一時的に分岐したり、短時間のうちに組成しなおされたりする場合もあるため、本当の意味で決済が成立するためには、いくつかの条件が満たされる必要があります。

十分な数のコンファメーションを受領して（具体的な取引を含むブロックの先に複数のブロックが追加されることによって）、はじめて本当の意味で決済が成立することになります。既存のブロックが、新たにマイニングされたブロック（その前のブロックのハッシュ関数を参照している）と相互に結びついていることを前提とすれば、そこに埋められているブロックの数が増えれば増えるほど、取引はより安全かつ不変のものに

なります。ちなみに、一般的な中央集権的取引所では、20～50 回のコンファメーションが記録された時点で取引が有効とみなされますが、イーサリアムのブロックタイムでは数分しかかかりません。

例えば、悪意を持った者が取引を覆そうとするならば、改竄しようとする取引を含むブロックに遡る必要があります。したがって、ある取引で 50 回のコンファメーションがあった場合、50 ブロック遡る必要があります。次に、当該ブロックと、分岐されたチェーン上の後続ブロックについて、それぞれ有効なプルーフ・オブ・ワークを探して再度マイニングし直さなければなりません。同時に、プロトコルのルールに従う善良な者たちは、最も累積的なマイニングが行われているチェーンであるメインチェーンのマイニングと拡張を行いことになります。

悪意を持った者がメインチェーンに対するブロック不足を克服するには、ネットワーク上の総計算能力の 50%超を相当長い期間にわたってコントロールする必要があります。さらに、悪意を持った者がこれに失敗した場合、ETH の報酬を得ることなく電力を浪費することになるため、重大なリスクに直面することになります。

スマートコントラクト：DApps 向けのプログラマブルなインフラストラクチャ

スマートコントラクトは、EVM 標準に準拠した特定のプログラミング言語を介して、イーサリアムに自己実行型プログラムや合意事項をスクリプトする機能を提供します。開発者たちは専用のプログラミング言語である Solidity を使用することができます。この言語は、高度な知識を持たない参加者がスクリプトツールにアクセスしやすくするために開発されたものです。また、Vyper や Yul など、より高度な言語を使用することもできます。

別の言い方をすれば、スマートコントラクトとは、コードに基づいてプログラムで実行される契約のことです。契約に埋め込まれたデータフィード、条件、ルール、合意事項は、信頼できる仲介者が契約を実行しなくても、自動的に事前に定義された結果を導き出します。どの分散型アプリケーションでも、スマートコントラクトを展開し、アセットスワップやレンディングプリミティブのサポートといった機能を構成することができます。

イーサリアムのスマートコントラクトは、契約を一つの取引として送信することで有効化され、展開されます。また、ETH の残高も持っており、契約の条件が満たされると、ネットワークを通じて取引を開始することができます。ネットワークはオープンソースであるため、開発者は実装されたスマートコントラクトのライブラリを参照できるようになっており、アプリケーション開発のコンポーザビリティを高めています。

スマートコントラクトは、現実世界のデータフィードを入力変数として取り込み、契約のアウトプットを決定することが多々あります。オラクルは、ブロックチェーンと外部システムの接続と相互運用性を促進するエンティティです。オラクルによって、スマートコントラクトはブロックチェーン上でネイティブに利用できない入力データに基づいて実行することが可能になります。一般的な例として、価格データ、気象データ、選挙結果、モノのインターネット（IoT）センサーの読み取り値、顧客確認（KYC）基準の ID 検証、検証可能なランダム関数などを挙げることができます。

オラクルが提供するデータは多くのスマートコントラクトのアウトプットを決定することができるため、中央集権的なエンティティにこうした情報を提供することを可能にすると、トラストレスブロックチェーンを使用す

る目的が失われます。Chainlink は、この問題を解決するために設計された分散型オラクルネットワークの好例です。Chainlink は、正確な実世界データをトラストレスな方法でオンチェーンに提供するよう金銭的インセンティブが付与された独立したオラクルノードのネットワークに依存しています。

DApps：スマートコントラクトを用いて構築されたアプリケーション

スマートコントラクトは、分散型アプリケーションが様々なユースケースやルールを持つプロトコルを作成することを可能にします。DApps はデータの保存とセキュリティにイーサリアムのブロックチェーンを使用し、アプリケーションロジックにスマートコントラクト技術を使用します。要するに、DApps は Web 上でホストされるユーザーインターフェースを持つアプリのようなものですが、コンピュータの分散型ネットワーク上で動作するスマートコントラクトは DApp のバックエンドの計算を容易にします。

コードの実行は中央集権的なクラウドプロバイダーに依存しないため、この機能は DApps に弾力性を与えます。イーサリアムネットワークには、金融アプリケーション、ガバナンス構造、サプライチェーン管理プロジェクト、ファイルストレージ、非代替性トークン化イニシアチブなど、一連の DApps が含まれています。

分散型金融サービスアプリケーションは、イーサリアム DApp エコシステムの中で重要な地位を占めています。こうした DeFi プロトコルのいくつかはネイティブトークンを備えており、上位の DeFi アプリの多くは ERC-20 の標準に準拠しています。USDT、USDC、DAI など、人気のステーブルコインも ERC-20 トークン標準を使用しています。ERC-20 標準は、開発者が同じガイドラインと互換性の枠組みの下で相互運用性と代替性トークンを構築することを可能にし、アプリケーションとスマートコントラクトのコンポーザビリティに最適な条件を作り出しています。

DeFi アプリケーションは、借入や貸付、資産交換、デリバティブ、保険、資産運用など、多くの伝統的な金融取引を分散化します。現在最も広く受け入れられているアプリケーションは、Uniswap と Aave の 2 つです。Uniswap は、資産の交換を求める買い手と売り手に流動性プールを提供する非管理型かつオープンソースの分散型自動マーケットメーカーです。Uniswap は、個人が取引プールに流動性を預け入れることによりマーケットメーカーとして行為することを可能にし、ユーザーの流動性に対する取引から取引手数料を得ます。Uniswap の 2022 年 1 月の流動性プール取扱高は、およそ 580 億ドルでした [4]。Aave は、デジタル資産を貸借するための分散型、非管理型流動性・短期金融市場です。例えば、市場参加者は Aave を利用することで、デジタル資産を担保としたローンを即時に調達することができます。

もう一つの人気の高いスマートコントラクトのアプリケーションには、イーサリアム代替トークン標準があります。ERC-721 は、非代替性トークン（NFT）の作成を標準化しています。NFT は複製不可能な非交換型トークンであり、同じトークンは存在しません。現時点では、デジタルアートが NFT の主な用途となっています。しかし、NFT の潜在性の幅広さを考えると、ゲーム分野におけるプレイ・トゥ・アーンのコンセプト、不動産のトークン化、チケット販売、体験、ID タグ、独占アクセス、メンバーシップ、サプライチェーンのタイムスタンプなど、より創造的な用途が生まれると思われます。

また、オンチェーン自律分散型組織（DAO）も、議決権や意思決定にイーサリアムのブロックチェーンインフラとスマートコントラクト技術を利用しています。人気の高い使用例としては、参加者がデジタル資産をガバナンストークンと交換できる DeFi DAO があります。トークン保有者は、蓄積された資産の宝庫から

の資産配分や投資決定に投票することができ、そうした配分からの利益について支払いを受けることができます。

イーサリアムネットワークの今後：スケーラビリティの向上を目指したアップデート

イーサリアムネットワークの成長を踏まえ、開発者たちはいくつかのアップデートのためのロードマップについて合意しました。これらのアップデートには、ネットワークのスケーラビリティを向上させ、環境に優しいものにするためのコンセンサスメカニズムの変更が含まれています。

プルーフ・オブ・ワークからプルーフ・オブ・ステークへのシフト

以前イーサリアム 2.0 と呼ばれていたイーサリアムコンセンサスレイヤーは、イーサリアムが新たな状態に移行する際にネットワークに加えられる変更を含めたイーサリアムのアップグレードのロードマップです。このアップグレードにより、より適度なハードウェアとエネルギー使用で、より優れたスケーラビリティを実現することができます。

プルーフ・オブ・ワークは強力なセキュリティを保証しますが、高額のハードウェアとエネルギーを必要とします。プルーフ・オブ・ステークは、これとは対照的に最小限のエネルギーしか必要としません。プルーフ・オブ・ステークのコンセンサスにおけるバリデーターは、プルーフ・オブ・ワークコンセンサスにおけるマイナーと類似しています。バリデーターは取引の順序づけ、新たなブロックの作成、さらには他のバリデーターが作成したブロックの認証を担当します。

プルーフ・オブ・ステークでは、ネットワークの改竄防止に電気を使用する代わりに、バリデーターは ETH を担保として提供することで、ネットワークのセキュリティを維持します。バリデーターは自らの資産を担保として提供することにより、悪意ある行動を取った場合や責任を果たせなかった場合に資産が差し押さえられることを承諾しています。このプロセスはスラッシングとして知られています。こうしたスラッシングのリスクが存在するため、バリデーターはプロトコルのルールに従い、ネットワークの最良の利益のために行動しようとします。バリデーターになるためには、市場参加者は 32 ETH を出資する必要があります。小規模な市場参加者は、Lido のようなプラットフォームを通じてリキッドステーキングプールに参加し、少量の ETH を 32 ETH 単位に集約し、それに応じて報酬を分割することができます。

バリデーターはプロポーザーとアテスターの 2 つカテゴリーに分けることができます。プロポーザーはバリデーターの集合からランダムに選ばれ、チェーンの次のブロックを提案します。プロポーザーに選ばれなかったバリデーターは、その提案に対して証明する必要があります。アテスターは提案されたブロックを検証し、プロトコルのルールに従って有効であることを証明します。プロポーザーとアテスターは、参加することで ETH の報酬を得ることができます。しかし、悪意ある行動を取った場合や責任を果たせなかった場合、担保として差し出した資産は危険にさらされます。明示的な悪意ある行動や意図的な共謀があった場合、バリデーターは全ステークを失う結果となります。サーバーの停止によるバリデーションの失敗など、悪意性がそれほどない行為については、ステークのごく一部を失うだけです。

イーサリアムのスケーリングに使用されるソリューション

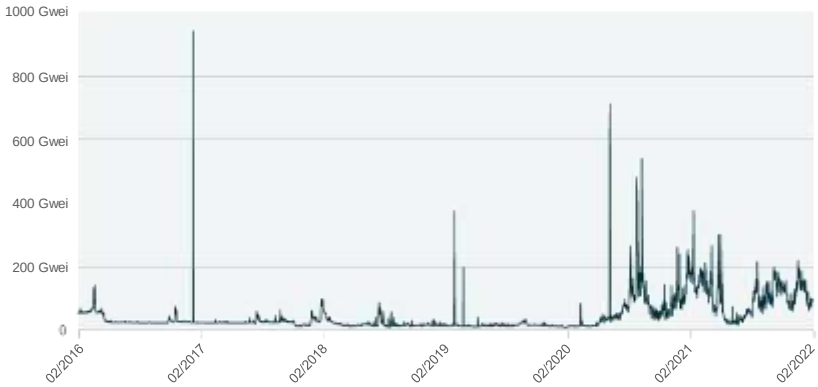
イーサリアムネットワークは、ユーザーベースの拡大に伴い、DApps 数が増加していることから、容量の限界に達しています。イーサリアムの限られたブロックスペースに対する需要が拡大したことで、近年の

ガス価格はボラティリティが高まり、最大の市場参加者を除くすべての参加者にとって、ネットワークは法外に高価なものとなっています。

イーサリアムのガス代は Gwei 単位（1 ETH の 10 億分の 1）で表示されています。途方もないガス代であるため、ユーザーは容量拡大やコスト削減のために別の方法を求めています。

需要の強さがもたらすガス価格のボラティリティ

出所：Etherscan.io、2022 年 3 月 1 日現在



EIP-1559 は、ガス価格の予測可能性を向上させた優れた価格体系を提供していますが、ガス価格の低下を保証するものではありません。現在、イーサリアムをコスト効率よくスケールするために用いられているソリューションとして、オンチェーンスケーリングとオフチェーンスケーリングの 2 つがあります。オンチェーンスケーリングでは、イーサリアムのベースレイヤーでコストとスループットを向上させる方法を探求します。例えば、イーサリアムコンセンサスレイヤーの展開の一環として、イーサリアムネットワークはシャードチェーンの導入を計画しています。シャードチェーンとは、データベースを水平方向に複数に分割するプロセスを指すものであり、これによりネットワークの混雑を緩和し、秒あたりの取引数を増やします。シャーディングには、プルーフ・オブ・ステークへの移行が前提条件となります。プルーフ・オブ・ワークシステムでは、シャーディングによりセキュリティ特性が希薄化され、悪意を持つマイナーは個々のシャードを容易に破損させることができるようになります。

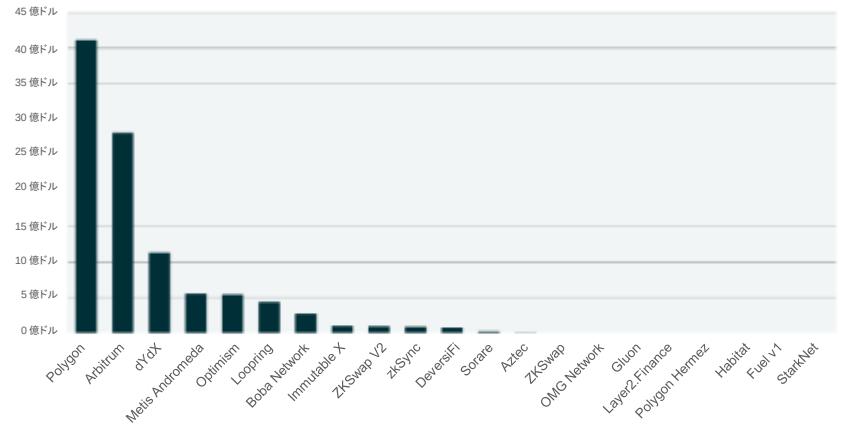
オフチェーンスケーリングは、イーサリアム上にレイヤー1（L1）と呼ばれる代替スケーリングプロトコルを構築します。イーサリアムの外で実行されるソリューションは、レイヤー2（L2）と呼ばれています。レイヤー2 のセキュリティは、最終的にイーサリアムの主要ネットワークであるメインネットに由来します。これらのアプリケーションは通常、個々の取引を別の状態で処理し、決済するためソリューションの種類に応じて、様々な方法でイーサリアムのメインネットと通信します。

L2 ソリューションは、セキュリティと透明性を求めてイーサリアムのメインネットを活用しますが、小規模取引をより迅速かつ安価に処理することができるため、ますます人気が高まっています。開発者が最小限の取引手数料でスケーラブルな DApps を構築することを支援する Polygon は、主要な L2 ソリューションの 1 つです。Solana のような競合スマートコントラクトプラットフォームは、一定程度の分散化を犠牲にして取引のスループット向上に成功していますが、L2 ソリューションはイーサリアムのエコシステムにとどま

りながらも、安価な取引方法を提供しています。L2 は、そのプラットフォーム上に多額の TVL（Total Value Locked）、つまり暗号資産の全価値を有しています。

レイヤー2 ソリューションのエコシステムは、100 億ドルの TVL を有している

出所：DeFillama.com および L2beat.com、2022 年 3 月 1 日現在



ETH の価値：ネットワークの成長志向型経済を後押し

ETH は、決済通貨として、イーサリアムネットワークに対する需要からその価値を得ています。ETH は、一般的に以下の目的で使用されます。

- 取引、ガス代金の支払い
- DeFi DApps とのインタラクション
- スマートコントラクトをブロックチェーンに展開するための支払い
- NFT マーケットプレイスと取引における主要な勘定単位

DApps にロックされたイーサリアムの総価値は約 1,140 億ドルに達しており、暗号資産界をリードする存在になっています [5]。DeFi にロックされた総価値は、アプリケーションに預け入れられた金銭的価値についての洞察を提供するものであり、センチメントと成長振りに関する信頼に足る測定値として機能することから、重要な指標となっています。プロトコル内でロックされた資産は、エコシステムの成長性、有用性、およびユーザーの確信度を示唆するものです。さらに、およそ 280 億ドルに相当する約 970 万 ETH がプルーフ・オブ・ステークのバリデーター契約の下でロックされており、将来的にネットワークを保護する役割を担っているほか、ETH の流通量を一段と減少させています [6]。

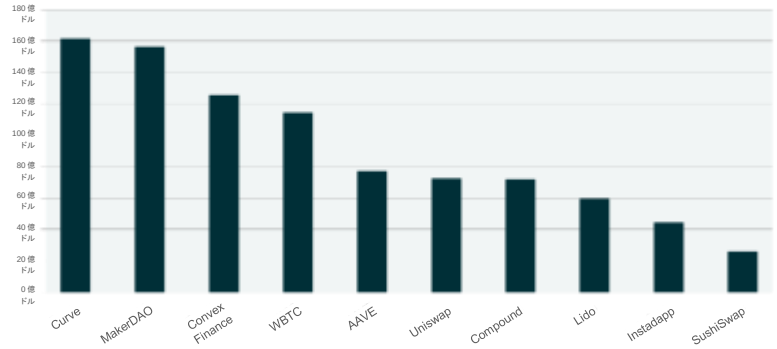
DeFi にロックされた 2,110 億ドルの総価値の中で、イーサリアムは先頭を走っている

出所：Defillama.com、2022 年 3 月 1 日現在

イーサリアムの優位性は、TVL が多くの DeFi DApps に分散されていることにあります。

イーサリアムの 1,140 億ドルに寄与するトップ 10 の内訳
スマートコントラクトの DApps にロックされた総価値

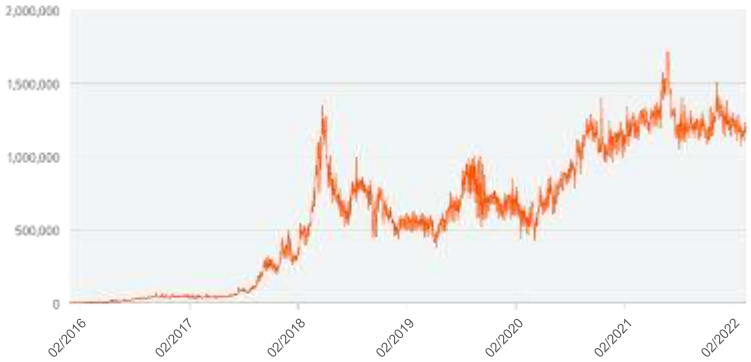
出所：Defillama.com、2022 年 3 月 1 日



さらに、ウォレット数や 1 日の取引件数などのオンチェーンの指標は時間の経過とともに増加しており、イーサリアムエコシステムに対する需要の高さを示しています。取引件数は、支払われる取引手数料と直接的に関係しています。

イーサリアムの 1 日当たりの総取引件数

出所：Etherscan.io、2022 年 3 月 1 日現在



2021 年には、イーサリアムはユーザーが支払った取引手数料により 99 億ドルの収入を計上しました。また、ETH の取引総額は 11.5 兆ドルに達しました [7]。

年率換算ベースの取引収入は依然として増加中

データの出所：Tokenterminal.com、2022 年 3 月 1 日現在

ETH の供給量は、ブロック報酬の形態で流動性に加わるコインに制限がないため、理論上は無限です。EIP-1559 においては、ブロック報酬の発行比率を変動させることが可能になるなど、ETH の金融政策は変更されました。変動比率が可能であるのは、取引高が流通量から除去される ETH の量に影響を及ぼすからです。

バーニングメカニズムが存在することから、ネットワーク需要が増加するにつれ、可変発行率が低下し、取引需要が増加し続けるにつれ、トークンの流通量が減少する傾向にあります。バーニングメカニズムがガス代や年間発行量に及ぼす影響で、需要の高い ETH の希少性に拍車がかかります。

現在、イーサリアムの年間ネットワーク発行量は約 4.5%で、1 ブロック当たり 2 ETH の報酬が支払われています [8]。イーサリアムはスケーラブルな改良型へと移行する段階にあり、今後は時間の経過とともに、ブロック報酬曲線は低下し続ける可能性があります。

なぜ今イーサリアムなのか：価値創造とスケーラビリティを可能にするメカニズムを備えたスマートコントラクトのブロックチェーン

イーサリアムが魅力と価値を高めつつある理由を理解するには、ブテリンがホワイトペーパーで明確にしたこと、つまりブロックチェーンの分散特性はプログラムによって拡張可能であることを認識する必要があります。プログラム可能なブロックチェーンの最初の成功例であるイーサリアムへのエクスポージャーに関心のある投資家は、以下を期待することができると考えられます。

- エコシステム内にロックされた価値、トークンやスマートコントラクトの有用性と相互運用性、そして取引件数の増加と ETH の燃焼に及ぼす影響が引き続き価値を高める
- プルーフ・オブ・ステークへの移行や、イーサリアムコンセンサスレイヤーの展開、レイヤー2 アプリケーションの改善など、オンチェーン・オフチェーンのスケーリングの進化といったアップグレードがイーサリアムにスケーラビリティを与えている。また、こうしたアップグレードは、そのネットワーク効果により、この成長しつつあるエコシステムにこれまで以上に開発者を惹きつけ、ETH の有用性に対する需要をさらに高める

イーサリアムの適応特性も、インターネットの Web 3.0 への進化といった破壊的な動きの中で中心的な役割を果たすのに最も適した立場にあり、その中核的な存在としてユーザーが所有するブロックチェーンエコシステムがあります。こうした動きと、それが喚起するかもしれない ETH に対する需要を踏まえると、このデジタル資産と、それがさらなる拡大を後押しするブロックチェーンネットワークには、大きな成長の可能性があると考えます。

脚注:

1. CoinMarketCap（2022 年 3 月 1 日）。*「Historical snapshot – 01 March 2022.」*
2. Watch the Burn（2022 年 3 月 1 日）。*「Blocks.」*
3. Ultrasound.money（2022 年 3 月 1 日）。*Ultra sound awakening: Track ETH become ultra sound.*
4. Uniswap.（2022 年 3 月 1 日）。*「Ethereum: Overview.」*
5. DeFi Llama.（2022 年 3 月 1 日）。*「DeFi TVL rankings: Ethereum.」*
6. Etherscan（2022 年 3 月 1 日）。*「Contract: 0x00000000219ab540356cBB839Cbe05303d7705Fa.」*
7. Token Terminal（2022 年 3 月 1 日）。*「Projects: Ethereum.」*
8. EthHub. (n.d.) *「Ethereum basics: Monetary policy.」*
9. Hotchkiss, G. I.（2019 年 12 月 19 日）。The 1.x files: The state of stateless Ethereum. *「Ethereum Foundation Blog.」*
10. Agarwal, A.、Smith, C.、Wackerow, P.、Samani, Q.、Joshua, Leung, N. H.、Singh, H.、Richard, S.（2022 年 2 月 4 日）。「Miner extractable value (MEV). Ethereum.」

用語集

用語は、登場する順番に沿って記載されています。

ビットコイン:ビットコイン・ブロックチェーン内の台帳残高上のみに存在するデジタル流通資産。ビットコイン・ネットワークに固有の暗号通貨。

ブロックチェーン:ピア・ツー・ピアを通して共有され、恒常的に残高照合が行われている分散型の台帳。これによって、取引の記録や資産の追跡が、信頼できる仲介者を通すことなく円滑に行われる。

チューリングコンプリート言語:いかなる計算操作も実行できるプログラミング言語。

スマートコントラクト:コードに基づきプログラムで実行される契約。

分散型アプリケーション（DApps）:ブロックチェーン技術に裏打ちされたスマートコントラクトの上に構築された分散型アプリケーション。

分散型金融サービスアプリケーション（DeFi）:仲介者を介さずに金融商品を提供する DApps。DeFi DApps はスマートコントラクトに支えられている。ユーザーは DeFi を介して、分散化された手段により借入・貸付などの金融市場活動に参加することが可能。

非代替性トークン（NFT）:交換不能で唯一無二の識別可能資産。

自律分散型組織（DAO）:スマートコントラクト内にルールと権限を持つ分散型組織。

取引:外部所有のアカウントから送信されるメッセージを格納した署名付きのデータパッケージ。取引は、暗号で署名された命令である。取引とは、手元のデジタル資産を別のアドレスに転送したり、スマートコントラクトを公開または実行することであると見ることができる。

状態:すべてのアカウントと残高に加え、すべてのスマートコントラクトのデータの現在の状態を指す。

ブロック:イーサリアムネットワーク内のデータ構造で、取引の詳細が格納されている。新たに作成されたブロックは、その親ブロック、つまり前のブロックへの参照を含む。

イーサリアム仮想マシン（EVM）：DApps を作成し、アカウントやスマートコントラクトをホストするために開発者が使用するプラットフォーム。EVM はネットワークデータを保存し、ネットワークの状態を常に最新の状態に保持する。

デジタル署名：秘密鍵および取引のハッシュ関数から数学的に割り出される。デジタル署名は、秘密鍵および関連づけられた公開鍵の所有権を、秘密鍵を他人に明かすことなく証明するもの。

公開鍵暗号方式： 非対称暗号とも呼ばれ、暗号化用と復号化用の 2 つの異なる数学的に結びついた鍵を使用する。公開鍵は ETH を受け取る際に、秘密鍵は ETH の支出取引に署名する際に使用する。

ノード：イーサリアムネットワークソフトウェアを実行するコンピュータの分散ネットワークで、ブロックチェーンに入る前に取引やメッセージを検証する。ノードには様々な種類がある。

イーサリアムクライアント：フルノードを実行するために必要なアプリケーション。ノードは基本的に、複数のオープンソースコーディング言語で利用可能なクライアントソフトウェアを実行する。クライアントの目的は、ネットワークの標準に照らし合わせて取引を検証するソフトウェアとして機能することである。

ガス代：イーサリアムネットワークでの取引にはコストがかかる。ガス代は、ブロックチェーン内の取引を検証し、取り入れ、保護するために支払われるイーサの量を指す。ガス代は Gwei 単位で表示され、取引を処理するために必要なガス代は通常、ネットワークの需要に基づいている。

マイニングノード：決済のためにブロックチェーンに記録されるブロックに取引を集約するノードの特別な小集団。マイニングノードは暗号学的ハッシュ関数に基づいて、複雑な数学的パズルを最初に解こうと互いに競争する。マイニングノードは暗号学的ハッシュ関数によりできる限り速く、異なる入力による結果を全力で計算するために、大量の計算リソースを使用する。

暗号学的ハッシュ関数：任意の長さのデータマッピングを、決定論的な固定の長さに変換するのに使用される一方向性関数。暗号学的ハッシュ関数には、以下の 3 つの性質がある。1) 繰り返されること：いかなる入力に対しても、その結果となる出力（ハッシュ値）は同じであるということ。2) 一方向的関数であり、与えられた出力から入力値を割り出すことが不可能であること。3) 入力値を微調整することで出力値が導き出すことが不可能なほど、関数がランダムであるように見えること。マイニングの過程は、何らかの出力値を得るために、暗号学的ハッシュ関数の結果を繰り返し、できるだけ速く算出することに依存している。これらの関数は、公開鍵からアドレスを割り出すためにも使用される。

ハッシュ値：暗号学的ハッシュ関数の出力値。

候補ブロック：マイニングノードが有効なプルーフ・オブ・ワークを見つけ出すことによって、ブロックチェーンに追加しようとしている取引保留中のブロック。プルーフ・オブ・ワークが見つかった後に、候補ブロックは有効なブロックとなり、チェーンに追加される。マイニングノードは、通常、メモリープール内の最も高い取引手数料の取引を選択することによって候補ブロックの形成を行う。

プルーフ・オブ・ワーク：マイニングノードが競って解こうする、暗号学ハッシュ関数に基づいた複雑な数学的パズルの解法。暗号学的ハッシュ関数の特質のため、プルーフ・オブ・ワークは非常に見つけにくいが、マイニングノードがこの解法を見つけるために計算リソースを消費したことを、どのノードもわずかながら検証することができる。プルーフ・オブ・ワークによって、2 つのブロックで同時にマイニングが行われている際の不整合を解決することができる。また、旧来のブロックの改竄を非常に難しく（コストがかかるものに）することによって、ネットワークを保護している。

ブロックタイム：新たなブロックの採掘にかかる時間。

ブロックサイズ：1 ブロック当たりのデータ容量。

ブロック報酬：マイニングノードが、ブロックの解明に対する金銭的なインセンティブとして、固定額の新たに創出された ETH を自身に向けて送金できる特殊な取引。

フロントランニング：メモリプール内の収益性の高い裁定機会を検出すること。その考え方は、フロントランニングすることにより、こうした機会を特定し、任意の機会から利益を得るために、より高額のガス代を得られる取引を送信することにある。

マイナー抽出可能価値または最大抽出可能価値（MEV）：ブロック内の取引を含めたり、除外したり、順序を変えたりすることで、標準的なブロック報酬やガス代を超えてブロックの生成から抽出できる最大の価値 [10]。

オンチェーン：実際のブロックチェーン内で取引が行われていること。

イーサリアム改善提案（EIPs）：イーサリアムネットワークの現在の標準と、合意されたすべてのアップデートについて説明したもの。ネットワーク構築者は、新たなアイデアや既存のネットワークへの変更を提案することができる。

コンファメーション：ブロックに特定の取引が含められた後に、ブロックチェーンに追加されたブロックの数。最初のコンファメーションは、取引がブロック内に含められたときに発生する。新たに有効なブロックがチェーン上でマイニングされる都度、追加のコンファメーションが発生する。

分岐されたチェーン：単一のチェーンから 2 つの異なるチェーンへと枝分かれしているブロックチェーン。これらのチェーンは同一の履歴を共有しているが、新たなブロックが同一性を失うポイントまで到達している。2 つのマイニングノードが同時に 1 つのブロックをマイニングするときに、一時的な分岐が発生するが、プロトコルのルールによりこの分岐は単一のメインチェーンに収束することになる。

メインチェーン：チェーン上にあるブロックの難易度に基づいて、累積的に最大のマイニング作業を行ったブロックチェーン。通常、メインチェーンが最も多くのブロックを有している。

ERC-20：スマートコントラクトに基づく EVM トークンの規格。ERC-20 トークンは、トークン間のコンポーザビリティにインセンティブを与えるため、共通した一連のルールを提供する。

ステーブルコイン：米ドルと 1 対 1 の比率でペッグされるように設計された暗号通貨トークンで、流動性と取引手段を加えることにより市場の安定を意図する。

コンポーザビリティ：他の同種資産と相互作用する機能。

ERC-721：スマートコントラクトに基づいた EVM トークンの規格。ERC-20 と ERC-721 の主な違いは、非代替性トークンをプログラムできるか否かと、その背後にあるルールである。

プルーフ・オブ・ステーク：取引の確認と記録のためには、バリデーターは自らの資産を「担保として預け入れ」なければならないというコンセンサスメカニズム。

バリデーター：プルーフ・オブ・ステークのコンセンサスメカニズムにおいて、取引を検証し、確認するネットワークの参加者。

スラッシング：プルーフ・オブ・ワークのコンセンサスメカニズムにおけるバリデーターに対するペナルティで、担保として預け入れられた資産の全部または一部が差し押さえられること。

プロポーザー：アルゴリズムを使用して選ばれたバリデーターで、新たなブロックを提案する。

アテスター：プロポーザーに選ばれなかったバリデーターは、選ばれたバリデーターのブロックの提案を証明し、その情報が規格に沿ったものであることを確認しなければならない。

Gwei：Giga-wei または Gwei は、イーサリアムネットワーク上のガス代を表すためにしばしば使用される。1 Gwei は 1 Ether の 10 億分の 1。

メインネット：メインブロックチェーンを表す用語。

免責事項

デジタル資産への投資は投機的であり、投資資金の一部または全部を失うなど、高水準のリスクが伴います。こうした投資は、全投資資金の損失を許容できない投資家には適していません。イーサリアム（ETH）は、比較的新しい資産クラスです。それらは特有かつ相当なリスクを有しており、これまでも著しい価格変動下にありました。こうした投資の価値については、何の前触れもなく大幅に下落し、ゼロにまで下がることもあり得ます。投資される場合には、その投資価格が完全に消滅することへの覚悟が必要です。

分散投資は利益を確約するものでなく、損失に対する保証でもありません。この情報は個人または個別の投資アドバイスまたは税務アドバイスを意図するものではありません。この情報を売買のために使用しないでください。投資、納税、税務については、投資顧問、税理士をはじめとする専門家に相談してください。

本資料は特定の一時点における市場環境の評価であり、今後の出来事を予測することを意図しておらず、今後の成果を保証するものでもありません。この情報は個人または個別の投資アドバイスまたは税務アドバイスを意図するものではありません。この情報を取引のために使用しないでください。投資、納税、税務については、投資顧問、税理士をはじめとする専門家に相談してください。

イーサリアム（ETH）については、概ね規制対象外であり、投資は厳格に規制されている投資に比べて詐欺、改ざんなどが発生する余地が大きいといえます。イーサリアム（ETH）は、インフルエンサーやメディアなどの行為・発信等による影響で、急激な価格変動の可能性があります。