

Amundi
Investment Solutions

Trust must be earned

**Investment
Institute**

クリプト・カレンシー（暗号通貨） がメイン・ストリームに躍り出る

ECONOMY AND MARKETS

2025年10月

・機関投資家向けマーケティング資料

規制緩和で暗号通貨が大変貌

デジタル資産の分野は、以前は金融機関の参入を阻んでいた障壁が低くなったこと等の規制緩和で大変貌を遂げつつある。長年、個人投資家や早期採用者に支配されてきたが、**今や機関投資家の暗号資産への関心が顕在化しつつあり、暗号資産エコシステムの成熟化や信頼性の向上に発展する可能性がある。**

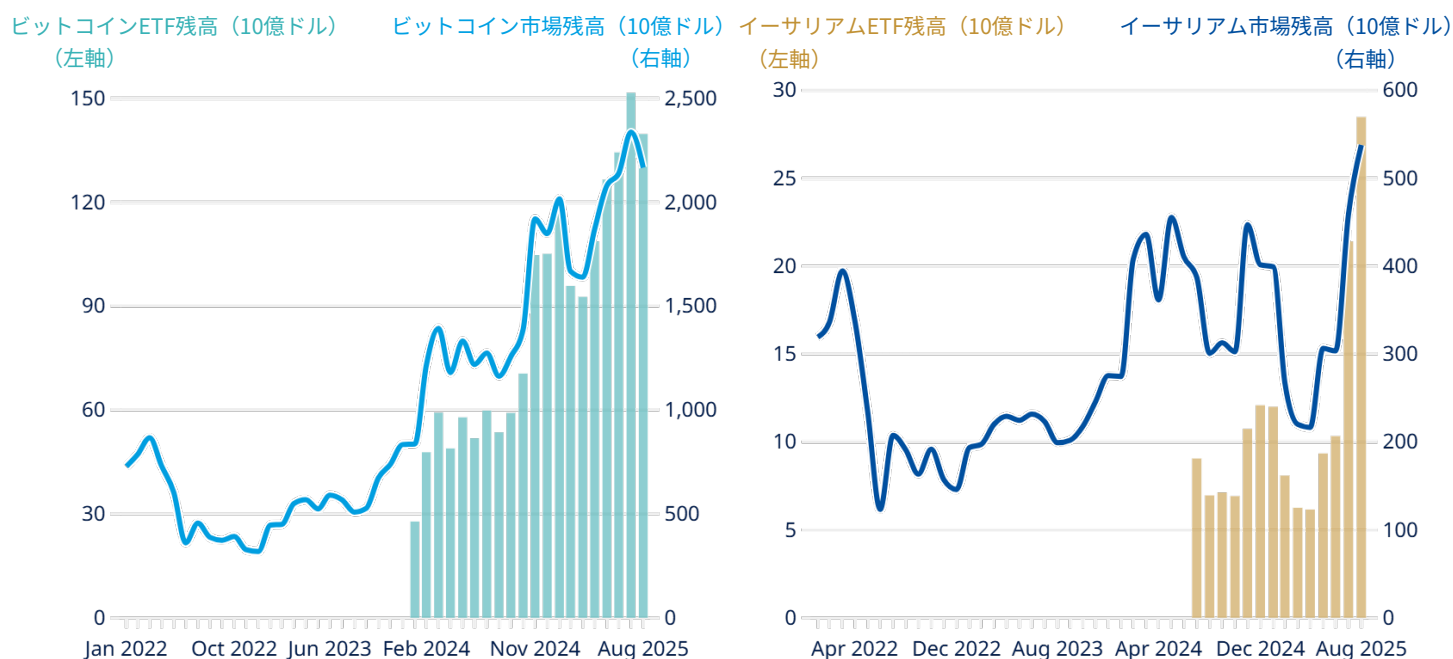
暗号資産は、曖昧な政策や現状優先の対応により、長い間、グレーゾーンで運営されてきた。こうした不確実性が、銀行や資産運用会社など伝統的金融機関の参入を阻んでいた。しかし、現在、政策立案者は、暗号資産を排除するのではなく、広範な金融システムへ安全に統合する方法を模索している。

この動きの主導的役割は米国が果たしている。当初は、強硬に、ほとんどの暗号資産を証券として分類する姿勢だった米国証券取引委員会（SEC）は、2023年と2024年初頭に重要な訴訟で敗訴した後、姿勢を軟化させた。その後、商品ではなく証券を構成する要素について、より明確な定義を示した二つの重要な法案が成立し、規制がより単純化されることになった。例えば、ビットコイン（Bitcoin, BTC）やイーサリアム（Ethereum）は、分散化の主要基準（資産またはガバナンスの5分の1以上を単一の発行者や関連団体が支配していないことなど）を満たすため、商品先物取引委員会（CFTC）の監督下に留まる可能性が高いが、一方、分散化が不十分な基盤で構築されたトークンは個別に審査され、有価証券として扱われ、証券取引委員会の管轄下に入る見込みだ。

また、一般的に、米ドルなどの法定通貨に対して1対1で固定されているデジタルトークンであるステーブルコインについての取り扱いもより明確化しつつある。2025年1月、トランプ米大統領は、米国連邦機関が、中央銀行デジタル通貨（CBDC）の開発や推進を行うことを禁止する大統領令に署名した。このメッセージは、民間発行のドル建てステーブルコインを、自由市場における代替手段として支援する意思の明確な表明となった。デジタルマネーの未来を形作る上で、ネットワークの採用と市場主導のイノベーションは、中央集権的な統制よりも重要になるというものだ。

「政策立案者は、暗号通貨を脇に追いやるのではなく、より広範な金融システムに安全に統合する方法を模索している。」

コインからETFへ：ビットコインとイーサリアムの時価総額は2022年以降急増



出典：AII、ブルームバーグ。2025年8月31日時点のデータ。

出典：AII、ブルームバーグ。2025年8月31日時点のデータ。

この方針は、2025年7月、米国でのジーニアス法（GENIUS法、ステーブルコインの国家イノベーション指導・確立法）の成立により強化された。この法律は、ステーブルコインを、現金や国債などクオリティの高い流動性資産で完全に裏付け、厳格な償還・透明性基準を遵守することを発行者に義務付け、不安定な状況が発生させる可能性のあるアルゴリズム・モデルを禁止するもので、投資家保護の強化に繋がる規制の明確化に向けた重要な一歩である。

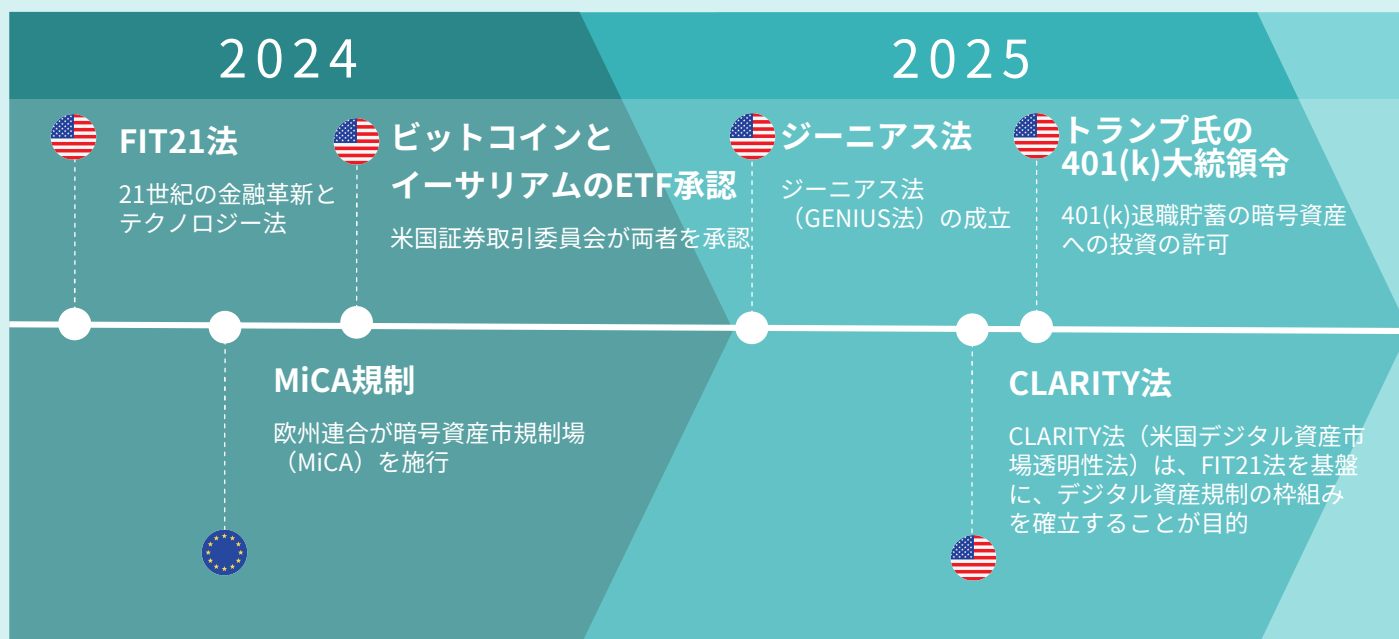
この法の成立は、連邦準備制度理事会が、過去に規制対象銀行の暗号資産活動への関与を事実上抑制していた指針を変更した時期にも重なり、**本法は、これらの金融商品を合法化するとともに、一定の規制を加えることで、ステーブルコインの信頼性を高め、機関投資家の参入に向けた明確な示したものである**。これにより銀行は、トークン化を模索し、デジタル資産を保管・決済システムに統合する可能性を検討できるようになるため、さらなる成長に寄与する可能性がある。さらに、2025年8月の大統領令により、米国の401(k)退職金口座が、暗号資産やその他の代替資産に完全アクセスできるようになり、デジタル資産向けに新たな資金が加わることとなった。

このような変化は米国だけで起きているわけではない。欧州連合（EU）も、加盟国間でのルールを標準化し、この分野で事業を行う企業に法的根拠与える包括的枠組みである「暗号資産市場（MiCA）規制」を施行している。この規制は、各国間での規制の違いを削減し、法的明確性を提供することで、イノベーションを促進し、フィンテックやブロックチェーン企業のEU域内での事業拡大の促進に繋がると期待されている。

英国、アジア、ラテンアメリカの当局も、イノベーションに支援的な政策と消費者保護の強化を組み合わせる方向へ動いている。世界的に規制の枠組みが整備されるにつれ、機関投資家の資金のデジタル資産へ流入は進み、市場に安定性をもたらすと同時に、個人投資家と機関投資家の双方に新たな投資機会を開くことになろう。

「規制の枠組みが世界中で整備されるにつれ、機関投資家の資金のデジタル資産へ流入が進むであろう。」

時系列で見た暗号資産の規制の動き



暗号資産に対する機関投資家の関心の拡大

数年に及ぶ個人投資家主導の熱狂を経て、デジタル資産市場は、漸く新たな段階に入った。機関投資家の戦略的かつ大規模な参入が特徴とするこの動きは、暗号資産エコシステムの成熟化、規模拡大、信頼性向上に寄与し得る。デジタル資産は、現状、世界の流動性市場ポートフォリオのわずか1.5%程度しか占めていないため、今後、インフラ整備が進み、テクノロジーへの信頼度が高まれば、需要のわずかな変化も大きな成長につながる可能性がある。

すでに、JPモルガン、シティ、HSBC、ステート・ストリート、UBSなどの銀行やカストディアンは、カストディ業務、トークン化された預金、決済プラットフォームなど様々な分野で取り組みを開始している。これらはブロックチェーン基盤上のグローバル金融を支える可能性がある。

一方、資産運用会社は、トークン化ファンドや暗号資産上場投資信託（ETF）を立ち上げ、コアポートフォリオへのデジタル資産の組み入れを開始している。これにより伝統的投資家のデジタル市場へのアクセスが容易に可能となるが、この動きは、広範な資産戦略の一環として、カスタム化されたデジタル資産へのエクスポージャーを求めるファミリーオフィスや富裕層からの需要増加とも合致するものと見受けられる。

もう一つの重要な動きは、中央銀行や政府系ファンドの間で、準備資産戦略の分散化の一環として、ビットコインや主要デジタル資産を保有すべきか否かに関する議論が浮上している点だ。この案は、依然、議論の対象ではあるが、各国が金での外貨準備を増やしている対応法に触発されたものだ。これは資産クラスとしての認知度が高まっていることを反映しており、将来の金融インフラにおける戦略的重要性が高まる可能性を示唆している。

機関投資家の採用が進むにつれ、焦点は、いかにデジタル資産の潜在能力を活用するか、どのような役割をポートフォリオ上で果たし得るかに移っている。したがって、こうした資産の価値が、なぜ、どのように変動するのかを理解することが、より重要となろう。暗号通貨は単一の資産クラスと見なされることが多いが、伝統的な金融資産との間の相関は時間とともに変化し、実態は、より複雑であることが明らかになりつつある。

2020年以前、暗号資産関連の主要トークンの間の相関は高かったが、伝統的資産との相関は概して低かった。しかし、過去5年間で見ると、暗号資産は、市場センチメントに、より密接に連動するようになり、短期（数週間～数ヶ月）では、ハイテク株やハイイールド債といったリスク資産との相関性が高まっている。

このため、暗号資産が、投資家のポートフォリオの分散効果に、どの程度寄与できるか疑問視する声も出ている。しかし、こうした相関関係は主に、センチメントと流動性条件が価格変動の大部分を左右する暗号資産の初期段階、かつ投機的な局面の表れと言えよう。また、相関分析によれば、マクロ経済ショック期や市場ストレス期を調整すると、長期的に見て暗号資産とリスク資産の連動性はかなり弱まる傾向にある。例えば、ビットコインと株式の相関は、リスク回避局面以外では弱まる傾向にある。この動きは、資産クラスとしての成熟化が進み、様々な地域で様々なタイプの投資家の採用が進むにつれ、その役割が変化する可能性を示唆している。

「半減期」サイクルでみたビットコイン価格

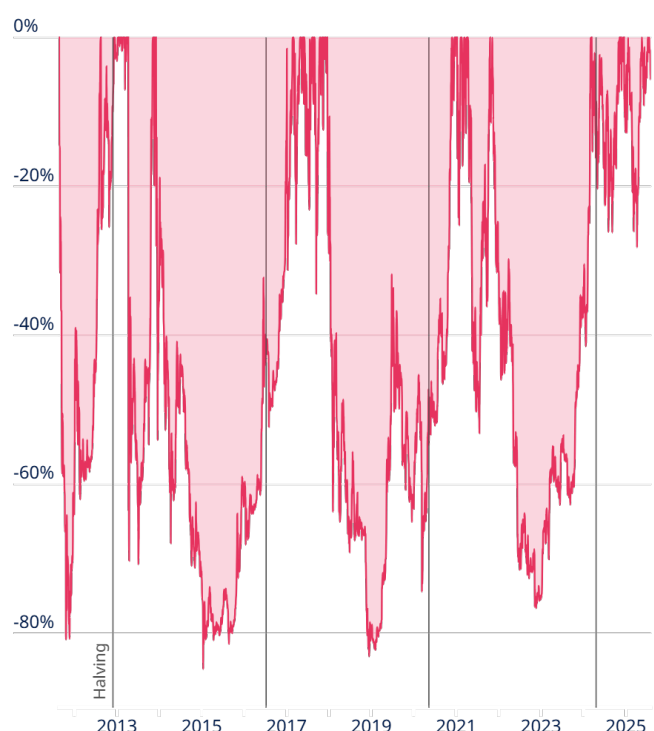
1ビットコインの米ドル価格（対数軸）



出典：All, LSEG DataStream。2025年8月5日時点のデータ。

ETF時代に入ってから下落幅の縮小

直近最高値からの下落率



出典：All, LSEG DataStream。データは2025年8月5日時点。

暗号資産の分散効果



暗号資産は異なる特性を持つ資産グループであり、それを認識して、扱うべきである。異なるトークンは、将来的に使用方法や採用状況に基づいて異なる動きを示す可能性が高い。

- ビットコインは、デジタル価値保存手段として浸透する可能性がある。機関投資家の保有が増加し、発行量は予め定められた半減スケジュールに従って管理されるにつれ、ビットコインのボラティリティは低下し、その動きは、従前からの実物資産に結び付けられてきたマクロヘッジ特性をより反映し始める可能性がある。
- 一方、イーサリアムや大半のアルトコインは、広範なテクノロジー・フィンテック分野のイノベーション・サイクルに依然として連動している。その価値は、ステーブルコイン、分散型金融（DeFi）、トークン化による取引需要が手数料推進型経済を牽引する、ブロックチェーン基盤アプリケーションの成長期待に由来することが多い。結果として、少なくとも、そのプラットフォームの一貫性・拡張性・収益性が証明されるまでは、これらのトークン価格と、情報テクノロジーやベンチャーキャピタル型投資といった成長志向の株式セクターとの相関は継続する可能性がある。したがって、こうした資産はビットコインに比べて高いベータ特性を示す傾向がある。この構造的特性は、リスクオン環境ではアウトパフォームする可能性はあるものの、市場ストレス時にはより急激な下落に見舞われやすいことを意味する。
- ステーブルコインは第三のカテゴリー、つまり、法定通貨（主に米ドル）にペッグされたデジタルトークンであり、主に決済・清算を目的として設計され、伝統的金融とデジタル金融の架け橋となる。担保のクオリティが保証されている限り価格安定性が確保される一方、利回りを生み出さない特性から、投資手段というより、デジタル・キャッシュに近い性質を持つ。暗号資産市場の流動性促進や国際送金の実現に不可欠な役割を果たすが、異なる視点での分析が必要である。

ビットコイン：担保あるいは財務管理ツールとしての可能性

ビットコインは、時価総額が約2.3兆ドルに達し、業界で市場支配率と呼ばれるセクター内での市場シェアが、2025年7月時点で60%以上に上昇するなど、主要な暗号資産としての地位を固めた。この背景として、主にマクロ経済の動向、分散効果を期待しての金融資産としての独自の位置付け、そして特に2024年1月に米国証券取引委員会がビットコイン現物ETFを承認したことを受けての機関投資家からの大規模な資金流入が挙げられる。

ビットコインは、投機的なテクノロジー実験というより、もはやデジタル時代の通貨ツールとして次第に認識されつつある。これは、世界的な債務増加とインフレ上昇に直面する中で、資産の安定性向上に向けた取り組みの一助となり得る可能性がある。例えば、一部の投資家は、ビットコインを金のデジタル版と見なし、担保として長期的に保有する可能性や、法定通貨ベースの金融システムを支える準備資産としての役割（ブレトン・ウッズ体制下で金が米ドルを支えたのと同様）を期待している。

これが実現するかは不透明だが、進行中のマクロ経済的・地政学的変化を通じて、ビットコインに期待されている特性が本質的なものかどうかを試されることになる。世界的な資金調達リスクの高まり、通貨価値の下落、財政赤字の拡大、資本規制、制裁措置といった懸念は、2025年9月に3,500ドル超の史上最高値を記録した金価格の急騰にも反映されている。仮に両者間に何らかの類似性があるとすれば、これらの懸念がビットコインの需要も押し上げることが見込まれる。金は数千年にわたり安全資産・価値保全手段として評価されてきたが、世界経済のデジタル化が進むにつれ、ビットコインのようなデジタル資産への需要は徐々に高まる可能性がある。金もビットコインも、理論上は、どの国の行動にも左右されず、また、供給も制限されているという特性を有する。一方、ビットコインは分割が容易で、最小単位の1Satoshiは0.00000001BTCに相当する。また、このトークンは携帯性に優れ、プログラムが可能で安全かつ完全に分散化されたネットワークに依存している。新規ビットコインはマイニング（採掘）によって生成され、チェーンに追加される各ブロックにおいて採掘者に報酬が与えられる。ブロックは約10分ごとに採掘され、これにより全プロセスの高頻度監査が可能となる。一方、ブロック生成（すなわち新規ビットコイン）に対する報酬は約4年ごと（または21万ブロックごと）に半減する。¹ この「ビットコイン半減期」と呼ばれる仕組みは、報酬が無視できる水準になるまで継続する。これは2140年頃に発生すると推定されており、ビットコインの最大供給量が2100万枚を超えないように設計されている。

マイニングの集中化や量子コンピューティングなどの急速な技術進歩がリスクとなり得る一方で、一部の公的機関・民間企業やその他の機関は、ビットコインを活用した財務戦略（ビットコイン・トレジャリー戦略）を段階的に採用しつつある。2025年7月現在、貸借対照表にビットコインを保有する上場企業は150社以上に上り、これらが所有するビットコインは将来存在する全供給量（2100万枚）の4.5%を超えている。サンプル企業の90%以上が米国上場企業であることから、ビットコイン財務戦略は近い将来、企業流動性管理の新たな手法を切り開く可能性がある。

アルトコインのエコシステム：イーサリアムとプログラム可能なブロックチェーン

アルトコインとは、ビットコイン以外の全ての暗号通貨を指す。これらはビットコインの代替として開発され、拡張可能性（スケーラビリティ）や取引速度、合意形成メカニズムといったビットコインの限界の改善を目的としている²。アルトコインには多様なプロジェクトがあるが、その基盤層を構成するのがプログラム可能なブロックチェーンである。イーサリアムのようなブロックチェーン・ネットワークにおいては、開発者がスマートコントラクトを記述・展開すること可能となる。スマートコントラクトとは、分散型アプリケーション（dApps）の実現には不可欠な、中央集権的な管理を必要とせずに操作をトリガーする自己実行型コードである。

プログラム可能なブロックチェーンの中核をなすのは、ネットワークの「デジタルオイル」として機能する「ユーティリティトークン」で、取引手数料（ガス代）の支払い、スマートコントラクトの展開・操作、ステーキングによるブロックチェーンのセキュリティ確保に不可欠である。例えば、イーサ（ETH）は、ネットワークの稼働に必須となる、イーサリアム・ブロックチェーンのネイティブ・ユーティリティトークンである³。

ユーティリティトークンがプログラム可能なブロックチェーンを支える一方で、分散型アプリケーションやプロトコルを通じて様々なトークンが発行される。この階層構造がアルトコインの世界を特徴付けているが、この階層構造において、基盤層トークン（デジタルオイル）はネットワークに不可欠である一方、アプリケーション層トークンは、それらのネットワーク上で動作する特定の分散型アプリケーションとの相互作用やガバナンスに必要となる。

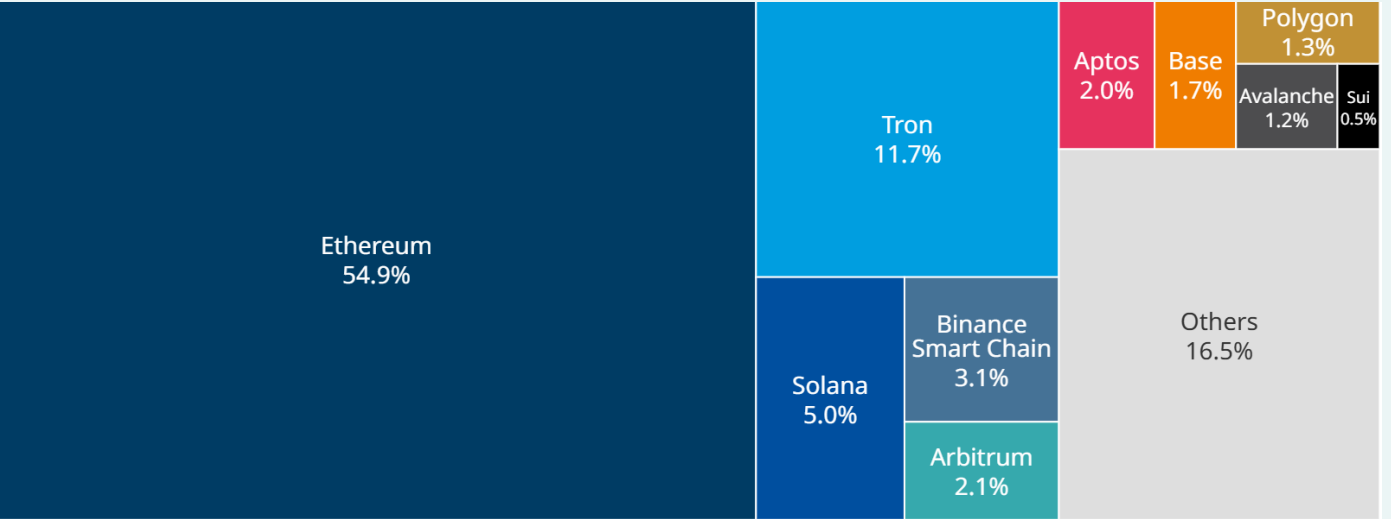
アプリケーションは多様で、現在、分散型貸付・借入・取引（DeFi：分散型金融）、デジタル収集品などの非代替性トークン（NFT）、アイデンティティ・ゲーム・ロイヤリティプログラムで利用されているもの、物流・サプライチェーン管理におけるトレーサビリティなどが含まれる。

また、資産のトークン化⁴も進展している。これによって所有権の分割や移転が容易になるため、資産運用業界における潜在的に重要なトレンドとして台頭しつつある。従来の金融資産を反映するものの、現時点では法的所有権の移転には至らないデジタルトークン（オンチェーン実物資産：RWA）の残高は、2025年7月に250億ドルを超えた⁵。トークン化されたプライベートクレジットと米国財務省資金が大きな割合を占めている。カウンターパーティリスクは残存し、スマートコントラクトには、より厳格な管理が必要だが、暗号資産向けに設計されたプラットフォームとの統合は急速に進んでいる。例えば、トークン化された財務省証券は、暗号資産向けプラットフォームで担保として受け入れられつつあり、現実世界の低リスク資産を裏付けとする借入や売買を可能にする潜在性を有する。利子を生まないステーブルコインや、ビットコインやイーサリアムのような変動性の高い資産とは異なり、トークン化された財務省証券は、運用期間中に収益を生む担保基盤として、安定性と収益性が両立する。

イーサリアムは、依然、先駆者として優位性を享受し、大半のアプリケーションにおいて主要ネットワークとなっている。しかし、その市場シェアは2021年12月の21%から2025年8月には13%まで低下した。今年は、価格の激しい変動も懸念材料となっている。Web3、DeFi、NFTにおける取引量の不足が問題の一因ではあるが、代替ブロックチェーンとの競争も急速に高まっている。Solana、BNB Chain、Ripple、Tron、Avalancheといった挑戦者たちは、手数料の低減やユーザー体験の改善といった革新を進めている。相互運用性の向上と専門化によって、普及と革新が進む中、将来はマルチチェーンエコシステムが主流となる可能性が高い。最終的な勝者は、拡張可能性（スケーラビリティ）、セキュリティ、使いやすさ、そして変化する規制の枠組みへの適応力において最も優れた成果を上げる者たちとなるであろう。

既存のレガシーシステムへのブロックチェーンソリューション統合は依然として複雑であり、多くの企業が技術的・運用上の課題に直面している。しかし、規制の明確化と採用基準の確立により、中核インフラはより強固になり、機関投資家の関心が高まるとアムンディは考えている。

オンチェーン活動を支えるネットワークの世界ではイーサリアム（Ethereum）が支配的



出典：DefiLlama、RWA.xyz、データは2025年8月時点。データはDeFi、ステーブルコイン、オンチェーンのトークン化資産における平均ネットワーク支配率を示す。

ステーブルコイン：決済ネットワークを巡る競争

ステーブルコインは、価格の安定性が維持できるよう、ドルなどの法定通貨と1:1で連動するように設計されており、プログラム可能性、低コスト構造、ブロックチェーン・テクノロジーの高速性が確保されている。

国境越えの決済で利用が拡大し、デジタルエコシステムにおける主要プレイヤーとして台頭している。2025年8月時点でステーブルコインの時価総額は2800億ドルを超え⁽⁶⁾、取引量は前年比で二桁成長を続けている。世界的に新たな金融アーキテクチャーが形成される中、各国において、デジタル決済は戦略的優先事項となりつつある。

現米政権は、前述の通り、中央銀行デジタル通貨（CBDC）の開発ではなく、民間発行のステーブルコインを支援する姿勢を示しており、GENIUS法を通じて、米ドル担保型ソリューションを戦略的に承認している。この法の成立によって、デジタル時代における米ドルの優位性維持と米国債需要の深化という二つの重要な戦略的目標が達成される可能性が高まっている。

なぜなら、第一に、米ドルはデジタル金融アーキテクチャーにおけるデフォルト通貨として設定される。これは、特に中国がSWIFTに代わるシステム構築を推進するなど、加速する地経学的再編への先制的な対応となる。第二に、規制対象となるステーブルコイン発行者は、短期米国債の新たな安定的な買い手となり得る。これにより、長期的に資金調達圧力を緩和できる可能性が高まる。

ステーブルコインは、もはや暗号資産業界だけのゲームではない。



Tetherが発行するUSDTは、時価総額と取引高において最大のステーブルコインである。USDTは取引所や分散型金融（DeFi）プロトコル間で広く統合され、ブロックチェーン間の相互運用性が高く、オフショア市場や新興国市場での高い浸透度を強みとしている。Circleが発行するUSDCは、強力なコンプライアンス体制と透明性の高い準備金証明を通じて機関投資家の採用を推進しているが、少なくとも最近まではUSDTとの差を縮められていない⁷。

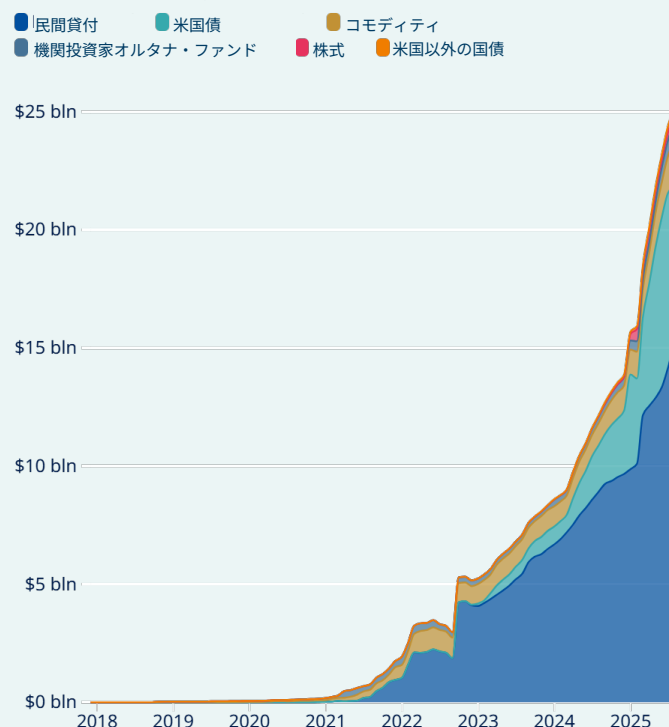
ステーブルコインの利用は、国際送金、小売プリペイド口座管理、実物資産のトークン化において拡大を続けており、2025年8月には残高が2500億ドルを超えた。ビザとマスターカードは、現在、選定パートナーとの間でステーブルコイン決済を処理できる（両社は統合、相互運用性、コンプライアンス枠組みのみに注力している）。一方、PayPalのような新規参入企業は既に自社ステーブルコイン（PYUSD）を提供しており、決済インフラとの連携を活用して市場シェア拡大を図っている。規制の進展により新規発行者が増える可能性が高く、アマゾン、アップル、スターバックスなど既存のユーザー基盤を持つ大規模消費者プラットフォームが米ドル担保型ステーブルコインを発行する道が開かれる可能性がある。

ステーブルコインの時価総額が2500億ドルを突破



出典：AII, RWA.xyz。データは2025年8月3日時点。ステーブルコインの総時価総額はおそらくさらに高く、DefiLlamaによれば約2800億ドルと推定される。

トークン化ファンドの資産額が急増



出典：AII, RWA.xyz。2025年8月3日時点のデータ。

暗号通貨に関連する主なリスク

規制当局が市場の構築と監督を推進する一方で、暗号通貨の設計・運用・普及には、依然、様々な固有の脆弱性が内在している。これらのリスクは暗号通貨ごとに大きく異なり、環境持続可能性や技術的脅威から、ガバナンスの脆弱性、規制リスク、プロジェクト失敗に伴う資本損失リスクまで多岐にわたる。

1

エネルギー消費と二酸化炭素（CO2）排出量

エネルギーと気候変動への懸念は、ビットコインやライトコインのような古いプルーフ・オブ・ワーク（PoW）方式のアルトコインでは、より深刻だが、現代のプルーフ・オブ・ステーク（PoS）方式の⁸プラットフォームやステーブルコインではほぼ無視できる。この違いは、各暗号資産のブロックチェーンを統治するコンセンサス・メカニズムの違いに起因する。ビットコインのようなPoW方式のブロックチェーンでは、採掘業者が強力なハードウェアと膨大な電力を必要とする複雑な数学的パズルを解く競争を行う必要がある。

ケンブリッジ・ビットコイン電力消費指数（CBECI）によれば、ビットコイン・ネットワークの年間電力消費量は約200テラワット時（TWh）⁹に達し、ポーランドやアルゼンチンといった国の年間電力消費量を上回る。したがって、持続可能なエネルギー・ソリューションの導入と化石燃料依存度の低減を求める業界への圧力は高まる見込みだ。

とはいえ、ビットコインのエネルギー消費量は他のエネルギー集約型産業と比べると、依然、低い。ビットコインの採掘は、現在、世界のエネルギー消費量の0.3%未満、世界の電力消費量の0.8%を占めるに過ぎない。金採掘の1.55倍、現在のAIインフラよりわずかに多い電力を消費しているものの、鉄鋼や化学産業に比べれば、ずっと少ない。

2

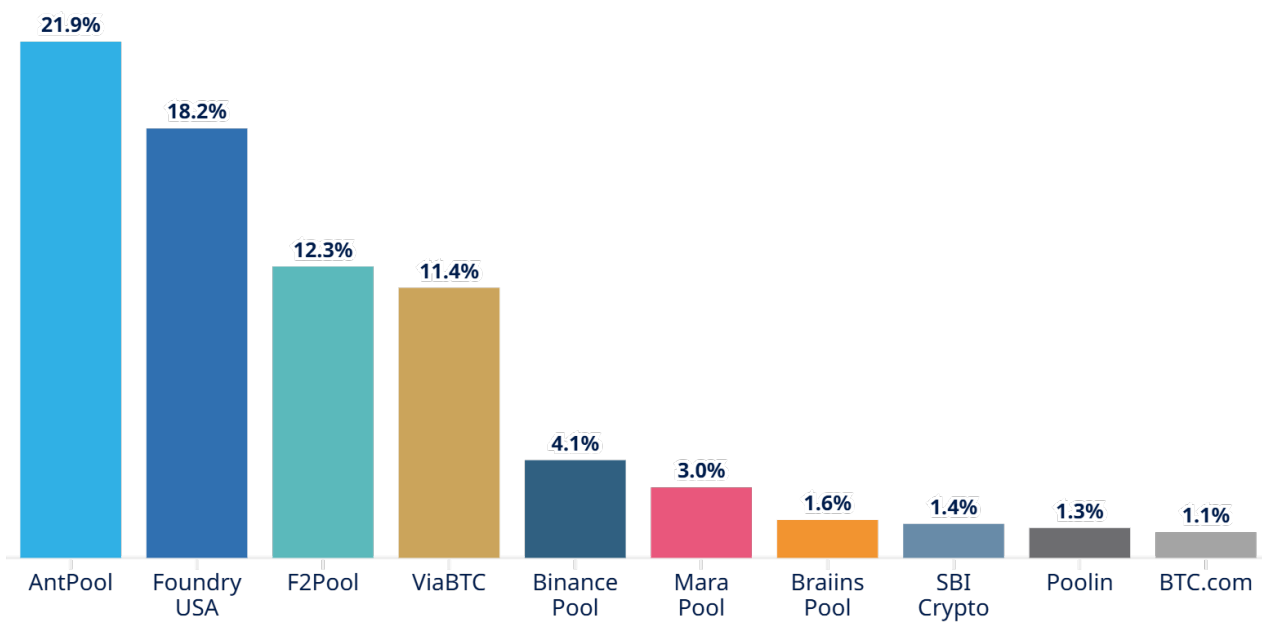
採掘・ステーキングの集中とガバナンス不全のリスク

ビットコイン採掘の電力集中度は高い。米国の月間平均ハッシュレートシェアは約40%に近く、世界トップ2の採掘企業がネットワーク総電力の大部分を支配している。採掘業者が専用インフラに巨額投資していることから、ネットワークの健全性を損なうよりは、維持する方向に強い経済的インセンティブが働くと推測されるものの、このような支配力はシステムの脅威を引き起こす可能性がある。

さらに、イーサリアムやアルトコインなどのPoSネットワークにおいても、ステーキングの集中は同様にガバナンス・コントロールの不均衡につながる。大口流動性供給者（通常は企業や招待パートナーが運営する）はプロトコル決定に影響を与え、活動を検閲できる。中央集権化は従来のウェブ／クラウドアーキテクチャでは一般的であり、アマゾン（AWS）、マイクロソフト（Azure）、グーグル（GCP）といった企業がインターネットインフラの大部分をホストしている。しかし、これらの企業はサービスレベル契約、高いブランド力、規制監督の下で運営されており、現在の暗号プロジェクトの大半には当てはまらない。

ビットコインのマイニングパワー

過去3年間の主要ビットコイン採掘プールの市場シェア（%）



出典：アムンディ・インベストメント・インスティテュート、Blockchain.com。データは2025年8月時点。

3

サイバーリスク

量子コンピューティングは、古典的な公開・秘密鍵暗号テクノロジーに依存するほぼ全ての暗号資産にとって、システムティックで長期的なリスクである。¹⁰ 例えば、ビットコインを所有するとは、秘密鍵を所有することを意味する。秘密鍵は、コインへのアクセス、使用を、その所有者に可能とする秘密のコードである。この秘密鍵は、資金を受け取るために使用される、自動的に生成される公開鍵（ビットコインアドレス）に対応している。取引には、送金先が正当な所有者であることを証明するデジタル署名を作成するために秘密鍵が必要となり、取引中に開示される公開鍵は、ネットワークが取引を受け入れ、ブロックチェーンに追加する前に、受取人の署名を検証するために使用される。この秘密鍵から公開鍵への一方通行の関係こそが、システムの安全性を支えている。

しかし、十分に高度な性能を持つコンピューターが登場すれば、この安全性は保証されなくなる。量子コンピューティングは、鍵を保護する暗号テクノロジーを破り、公開鍵からユーザーの秘密鍵を導出できるようになる可能性がある。2025年半ば時点で、採掘されたビットコインの4分の1以上が、公開鍵が漏洩したアドレスに保管されている可能性がある。この点において、PoSシステムは、引き続き、スマートコントラクトを支えるコードの脆弱性にはさらされるものの、適応性が高く、アップグレードが頻繁に行われ¹¹、開発者間の連携もより活発であることが多いため、量子コンピューティング時代への適応を促進する可能性が高い¹²。一方、ビットコインのようなPoWネットワークは、脅威が現実化しない限り、量子耐性ソリューションへの移行が遅れる可能性がある。

4

ステーブルコインを中央銀行デジタル通貨より優先するリスク：

ガバナンスや担保のクオリティが低下した場合、市場ストレスが流動性危機を引き起こす可能性がある。また、規制の枠組みが機能する銀行システム外でのステーブルコインの広範な利用は、国際的な通貨主権に課題をもたらす恐れがある。こうした課題は担保のクオリティそのものから生じるものではなく、通貨手段の支配権、資本移動の仕組み、日常生活で支配的な通貨の構造的変化に関連している可能性がある。特に、国内機関への信頼が弱い場合には、この最後の点が重要となる。主なリスクは、中央銀行の制御を超えたさらなるドル化、現地銀行システムを不安定化させ、公的外貨準備を脅かす資本逃避の危険性、そして取引主体に関する規制当局や税務当局の情報不足に関連している。

5

マネーロンダリング対策（AML）と規制遵守

暗号資産業界は、2022年以降、本稿で先に述べた規制の影響もあり、大きな進展を遂げたが、マネーロンダリング対策（AML）と顧客確認（KYC）の課題は残っている（トラベルルールの遵守は常に容易ではない）。完全な身元確認なしに 仮名使用で取引が可能で、ピア・ツー・ピア送金や非管理型ウォレットは規制対象外であり、分散型プロトコルではKYC執行の中央管理的枠組みが欠如している場合が多く、制裁回避や資本逃避を許容する恐れがある。デジタル資産業界が成長し、信頼度を高めるには、規制の枠組みとの調和を進め、技術的解決策を活用し、分散化と責任あるコンプライアンスのバランスを取る必要がある。こうした抜け穴を塞ぐ潜在的な解決策として、暗号学で「ゼロ知識証明」と呼ばれる手法の導入が挙げられる。これは一方の当事者（証明者）が、他方の当事者（検証者）に対し、ある主張が真実であることを、その真実性以外の情報を一切伝達せずに納得させるプロトコルである。

オンチェーン分析やオンチェーンID標準¹³も代替案だ。AIの急速な進歩がデジタル体験、コンテンツ制作、意思決定プロセスを形作る中、これらの解決策は特に注目に値する。分散型台帳テクノロジー（DLT）の不変性と透明性は、AIモデルが生成する誤情報や合成データのリスクに対する強力な対策となる。データの発生時刻を証明し、その起源と完全性を暗号的に検証することで、ブロックチェーンはコンテンツの出所を追跡し、それが検証済みの個人または機械によって作成されたかを検証する可能性を秘めている。

6

破綻および類似のリスク

毎年数百の暗号資産プロジェクトが、経営ミスや不正行為により破綻している。ハッキング、盗難、詐欺も、依然、問題だ。取引所が破綻したり、サービス障害が発生したりすると保有資産に影響が出るが、ビットコインはプロジェクトの債務不履行リスクは低い。アルトコインやDeFiは、財務的回復力、監査、透明性のあるガバナンスを欠く小規模プロジェクトが蔓延しているため、より多くのリスクに晒されている。一方、ステーブルコインは信用リスクと準備金リスクに直面している。物理的な担保ではなく合成担保で裏付けられるアルゴリズム型ステーブルコインは、崩壊の危険性が高い。

「毎年数百の暗号資産プロジェクトが、管理不備や不正行為により破綻している。」

結論

暗号資産エコシステムは、過去10年間で劇的な変貌を遂げ、ニッチな実験段階から、金融・テクノロジー・地政学の交差点に位置する複雑で多面的な分野へと進化した。インフラの成熟化と規制の枠組みの整備に支えられ、個人投資家から機関投資家に向けて活用範囲も広がっている。一方で、ビットコインのような基盤テクノロジーとイーサリアムのようなプログラム可能なブロックチェーン、ステーブルコインの間には明確な相違が生じている。両者の間には、設計、活用法、リスクプロファイルに顕著な違いがあり、デジタル資産への投資を検討する投資家は、これらの重要な差異に留意する必要がある。

一方、この進展は摩擦の発生を招くことにもなる。規制当局は監督強化を図っているものの、暗号通貨の設計・運営・普及には、本質的な脆弱性が、依然、内在している。新たなテクノロジー開発とリスクは、部分的には、暗号通貨市場の構造的特徴の一つである高いボラティリティの要因ともなっている。懐疑論や不確実性が、引き続き残されていることも、この資産クラスを通じた高い価格ボラティリティに結びついている。さらに、デジタル資産市場のストラクチャーも、この現象を増幅している。スケジュールが確定され、地理的にセグメント化されていることが多い従来市場とは異なり、暗号資産市場は常にオープンである。流動性が低く、一定の期間毎にしか価格が再評価されないことで、構造上、ボラティリティが低く抑えられているプライベート・アセットと同様、価格発見が連続する公開暗号資産市場は、ボラティリティが急に上昇しやすいという特徴がある。

しかし、こうしたチャレンジは驚くべきものでも、暗号通貨特有のものでもない。過去を振り返ると、すべての主要なイノベーションは、不確実性、落とし穴、混乱を経て、普及・拡大してきている。電子メール、インターネット、スマートフォン、クラウドコンピューティングといったイノベーションの成功事例をみると、その成功は、リスクがなかったからではなく、直面したリスクに対して、時間をかけて理解し、管理し、適応してきた能力を社会が有していたからだとということがわかる。ブロックチェーン・テクノロジーや暗号通貨が、いずれ同等の成功を収めるまでは確認できるものではないが、情報共有に基づく監督、適応に向けた規制、協調的な開発といった必要な対応が進められている可能性が高いことから、現時点では、両者は類似の軌跡をたどっているように見える。

したがって、投資家、開発者、政策立案者には、変化するリスクと構造的特性を正確に理解しながら、イノベーションを受容するという、微妙なバランスを要するアプローチを取ることが求められている。

「成功したイノベーションに共通する特徴は、リスクがなかったということではなく、むしろ、それらのリスクを理解し、管理し、時間をかけて適応する能力を社会が有していたということである。」

Notes

1. Approximately 144 blocks are added to the Bitcoin blockchain daily, while new Bitcoin supply per year is a function of block rewards. In 2009, which is known as Genesis year because that is when the first block was created, the block reward started at 50 BTC, it has halved in 2012, 2016, 2020 and more recently in 2024. The block reward was 3.125 BTC on July 2025.
2. Most altcoins use different consensus algorithms (Proof of Stake, or PoS) relative to Bitcoin (Proof of Work, or PoW). Ethereum, for instance, transitioned from PoW to PoS in September 2022. The event is known as "The Merge" and effectively ended Ethereum's reliance on energy-intensive mining.
3. Similar roles are played, for instance, by SOL on Solana or AVAX on Avalanche.
4. Tokens issued by such protocols are generally referred to as "security tokens" and are digital representations of real-world assets (like equity, debt, real estate and commodities), that are issued and traded on blockchain networks with regulatory compliance features.
5. RWA.xyz
6. DeFiLlama, July 2025
7. Circle Internet Group, commonly known as Circle, has listed on the New York Stock Exchange (NYSE), by launching their initial public offering (IPO) in June 2025. This marked the first major crypto firm to IPO since Coinbase.
8. Proof-of-Work networks (PoW) differ from Proof-of-Stake (PoS) networks in the consensus mechanism that validates token transactions. PoW relies on computational power as miners compete to add new blocks with energy-intensive work. PoS networks, like Ethereum 2.0, select validators based on the amount of cryptocurrency they "stake" or lock up as collateral.
9. As of September 01, 2025, The Cambridge Bitcoin Electricity Consumption Index is updated daily and provides theoretical extreme scenarios to capture minimum/maximum energy consumption.
10. Most blockchains rely on ECDSA (Elliptic Curve Digital Signature Algorithm), which could be broken by quantum computers using Shor's algorithm.
11. Upgrades happen by running "intentional forks" on the network: a technical phenomenon used by developers to implement changes to the protocol of a given network. After the fork, a blockchain splits into two separate branches, which share their transaction history up until the point of the split and go in their own direction from there onward.
12. Many newer platforms (e.g. Algorand with Falcon, QRL using XMSS, Hedera with SHA 384) are employing or investigating quantum-resistant cryptography.
13. Blockchain networks need to encourage adoption of interoperable, reusable digital identity standards (i.e. decentralised identifiers and verifiable credentials) and integrate "zero-knowledge proofs" to allow KYC verification without disclosing personal data. In cryptography, a zero-knowledge proof is a protocol in which one party (the prover) can convince another party (the verifier) that some given statement is true, without conveying to the verifier any information beyond the mere fact of that statement's truth. In light of the fact that one should be able to generate a proof of some statement only when in possession of certain secret information connected to the statement, the verifier, even after having become convinced of the statement's truth, should nonetheless remain unable to prove the statement to further third parties.

IMPORTANT INFORMATION

This document is solely for informational purposes.

This document does not constitute an offer to sell, a solicitation of an offer to buy, or a recommendation of any security or any other product or service. Any securities, products, or services referenced may not be registered for sale with the relevant authority in your jurisdiction and may not be regulated or supervised by any governmental or similar authority in your jurisdiction.

Any information contained in this document may only be used for your internal use, may not be reproduced or disseminated in any form and may not be used as a basis for or a component of any financial instruments or products or indices.

Furthermore, nothing in this document is intended to provide tax, legal, or investment advice.

Unless otherwise stated, all information contained in this document is from Amundi Asset Management SAS and is as of 12 September 2025. Diversification does not guarantee a profit or protect against a loss. This document is provided on an "as is" basis and the user of this information assumes the entire risk of any use made of this information. Historical data and analysis should not be taken as an indication or guarantee of any future performance analysis, forecast or prediction. The views expressed regarding market and economic trends are those of the author and not necessarily Amundi Asset Management SAS and are subject to change at any time based on market and other conditions, and there can be no assurance that countries, markets or sectors will perform as expected. These views should not be relied upon as investment advice, a security recommendation, or as an indication of trading for any Amundi product. Investment involves risks, including market, political, liquidity and currency risks.

Furthermore, in no event shall any person involved in the production of this document have any liability for any direct, indirect, special, incidental, punitive, consequential (including, without limitation, lost profits) or any other damages.

Date of first use: 15 September 2023.

Document ID: 4818876

Document issued by Amundi Asset Management, "société par actions simplifiée"- SAS with a capital of €1,143,615,555 - Portfolio manager regulated by the AMF under number GP04000036 - Head office: 90-93 boulevard Pasteur - 75015 Paris - France - 437 574 452 RCS Paris - www.amundi.com

Photo credit: ©iStock/Getty Images Plus - gremlin

Amundi Investment Institute

In an increasing complex and changing world, investors need to better understand their environment and the evolution of investment practices in order to define their asset allocation and help construct their portfolios.

This environment spans across economic, financial, geopolitical, societal and environmental dimensions. To help meet this need, Amundi has created the Amundi Investment Institute. This independent research platform brings together Amundi's research, market strategy, investment themes and asset allocation advisory activities under one umbrella; the Amundi Investment Institute. Its aim is to produce and disseminate research and Thought Leadership publications which anticipate and innovate for the benefit of investment teams and clients alike.

Get the latest updates on:



- Geopolitics
- Economy and Markets
- Portfolio Strategy
- ESG Insights
- Capital Market Assumptions
- Cross Asset Research

[Visit our Research Center](#)

Visit us on



CHIEF EDITOR

MONICA DEFEND

HEAD OF AMUNDI INVESTMENT INSTITUTE

EDITORS

CLAUDIA BERTINO

HEAD OF AMUNDI INVESTMENT INSIGHTS AND PUBLISHING, AII*

SWAHA PATTANAİK

HEAD OF PUBLISHING AND DIGITAL STRATEGY, AII*

DESIGN EDITORS

VINCENT FLASSEUR

GRAPHICS AND DATA VISUALIZATION MANAGER, AII*

CY CROSBY TREMMEL

INVESTMENT INSIGHTS, AII*

* Amundi Investment Institute

Amundi
Investment Solutions

Trust must be earned

本資料のご利用に当たっての注意事項等

本資料は、アムンディ・インベストメント・インスティテュートが一般・参考情報の提供を目的として作成した資料を弊社が一部翻訳したものです。

本資料は、本資料に含まれるいかなる金融商品の販売や媒介を意図、または購入・売却の勧誘を目的としたものではありません。

本資料は法令に基づく開示資料ではありません。

本資料中に記載したアムンディ・インベストメント・インスティテュートの見通し、予想、予想意見等（以下、見通し等）は、当資料作成日現在のものであり、今後予告なしに変更されることがあります。また、見通し等や過去の運用実績を含むいかなる内容も、将来の投資収益等を示唆または保証するものではありません。

本資料は、信頼できると考えられる情報に基づき作成しておりますが、情報の正確性、完全性について保証するものではありません。

本資料に記載されている内容は、全て本資料作成日以前のものであり、今後予告なしに変更される可能性があります。

本資料に含まれる情報から生じるいかなる責務（直接的、間接的を問わず）を負うものではありません。

弊社の許可なく、本資料を複製または再配布することはできません。

アムンディ・ジャパン株式会社

金融商品取引業者登録番号：関東財務局長（金商）第350号

加入協会：一般社団法人投資信託協会

一般社団法人日本投資顧問業協会

日本証券業協会

一般社団法人第二種金融商品取引業協会