Report 4

ゼロ知識証明で進化するブロックチェーン

ブロックチェーン技術は、過度な期待や幻滅期を越え、実社会への応用が広がる。デジタルアセットを支える基盤として活用が進む一方、世界的なトークン流通（トークンエコノミー）の拡大に対し、処理能力の限界も見えてきた。この課題を克服し、ブロックチェーン活用の新段階を切り開く技術として期待されるのが、ゼロ知識証明だ。

渡邊 大喜　先端技術ラボ エキスパート

ゼロ知識証明技術の概要

ゼロ知識証明（ZKP：Zero-Knowledge Proof）とは、証明したい情報の「中身」を開示することなく、その結論の正しさのみを相手に納得させる暗号技術である。この技術は、主に2つの重要な特徴を持つ（**図表**）。

第1の特徴は、秘匿性の向上だ。データの一部を隠したまま、演算が正しく行われたことを証明できる。例えば、複数の取引を精算する際、個々の送金額や相手先を明かすことなく「収支が正しい」ことを証明できる。暗号資産の普及過程で、プライバシーを重視する開発者コミュニティがゼロ知識証明の実用化を加速させた。ゼロ知識証明を用いることで、規制要件を満たしつつプライバシーを保持した送金を可能にする手法が検討されており、リテール型CBDC（中央銀行デジタル通貨）への応用も議論されている。

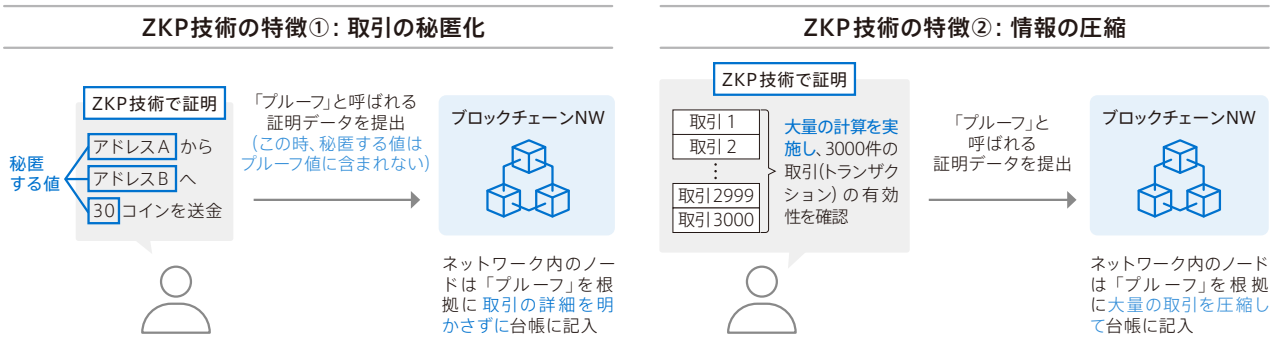
第2の特徴は、情報（計算過程）の圧縮である。ゼロ知識証明では、計算（例えば、取引の正当性の確認など）した証拠を「証明値（Proof）」に変換できる。この証明値は、一度求めれば、その後は検算不要で、計算が正しいことを証明できる。証明値のデータサイズは小さく、検証に要する計算量も少ない。この特徴を活用することで、大量の取引を確認した事実を圧縮し、その証拠のみをブロックチェーンに記録できる。これは、ブロックチェーンのスケーラビリティ問題、すなわち取引の遅延や手数料の高騰などの解決に貢献する。

金融領域で進むパブリックチェーン活用

金融機関でのブロックチェーン活用では、機密性が高く非公開のネットワークであるプライベート・ブロックチェーンの利用が選好されてきた。一方で、昨今のトークンエコノミーの拡大に伴い、金融機関やフィンテック企業でもパブリック・ブロックチェーンの活用事例が増えてきている。この場合、最有力な選択肢はEthereumである。例えば、世界最大の資産運用会社ブラックロックは、2024年3月にトークン化されたMMF（マネー・マーケット・ファンド）をEthereum上で発行し、機関投資家へ提供している。また、米国のサークル社やペイパル社が発行するステーブルコインは、複数のブロックチェーンに対応しているが、その大部分はEthereum上で流通している。さらに、仏銀行大手ソシエテ・ジェネラルが発行した、欧州の暗号資産規制（MiCA）準拠のステーブルコインも、Ethereum上で発行されている。これは、Ethereumが持つセキュリティ、分散性、そして強固なネットワーク効果が信頼されている証拠だ。

しかし、Ethereumは誕生から10年が経ち、より新しいアーキテクチャのブロックチェーンも多数登場するなかで、手数料の高騰や処理の遅さが課題となってきた。ブロックチェーンの外側で大量の取引を処理する「レイヤー2」などの代替策は、一定の成果を上げたものの、エコシステムの分断、流動性の分散、そし

図表　ゼロ知識証明の２つの特徴



出所：日本総研作成

て相互運用性の欠如といった新たな課題を生み出し、根本的な解決には至っていない。

ZKP技術で再構築されるEthereum

25年7月にイーサリアム財団から発表された長期ビジョン「Lean Ethereum」では、プロトコルの根本的な再構築を目指している。ここではゼロ知識証明技術が、単なる暗号学的機能ではなく、よりシンプルで安全、かつ将来にわたって検証可能なアーキテクチャを構築する基盤技術と位置づけられている。

ゼロ知識証明を用いた大きな変化は2つある。1つは、スマートコントラクトの実行環境であるEVM（Ethereum Virtual Machine）を、よりゼロ知識証明と親和性の高いVMに移行することだ。これにより、プライバシー保護型のアプリケーションが容易に構築可能になる。金融機関にとっては、取引内容を開示せずに正当性をパブリックチェーン上で証明できる可能性があり、従来プライベートチェーンを選好してきた理由の一部が解消されうる。

もう1つは、コンセンサス層にゼロ知識証明を取り入れることである。コンセンサスとは、ブロックチェーンに取引を含むブロックを記録するかどうかを決める処理だ。ここにゼロ知識証明の特徴である圧縮性を活用することで検証負荷を軽減し、ファイナリティ（取引の最終確定性）の迅速化を目指している。現在は約15分かかるファイナリティを、数秒に短縮する目標だ。金融機関が求める信頼性と即時性の実現につながると期待される。

2025年は、米国においてステーブルコイン規制が整備されたほか、大手金融機関による預金・債券のトークン化実証が進展するなど、トークンエコノミーが広がる兆しがある。ただし、その規模は伝統的な金融市場に比べるとまだ小さい。グローバル規模でのトークン化を展開するためには、既存の集中型金融システムに匹敵する処理能力が不可欠だ。「Lean Ethereum」は、第1層のブロックチェーン（レイヤー1）で1万TPS[*1]、第2層のネットワーク（レイヤー2）で100万TPSを目標としており、これは、Visaなどの決済ネットワークの処理能力に近づく水準である。今後は、ゼロ知識証明を基盤技術とする新しい設計思想のもとで、ブロックチェーンは長期的な需要に応える形で進化を続けると期待される。X

＊1　Transactions Per Second（トランザクション・パー・セカンド）の略。1秒当たりの取引処理件数。

Profile

渡邊 大喜

（わたなべ・ひろき）

NTT研究所でのR&D業務や事業会社でのシステム開発業務を経て、2022年から日本総研。先端技術ラボにて、先端IT技術に関する動向調査や業務適用に向けた応用研究に従事。