ブロックチェーンエコシステムの安全性，性能，持続可能性を高める

ブロックチェーン技術は，インターネット上に，一定数の計算機が故障したり，悪意を持った行動をしても安全性を保つ新たなタイプの信頼を提供する技術として，大きな注目を浴びています．その理論は革新的である一方で，現在のブロックチェーン技術を支える数学的根拠や実装が，本当に持続的に有効で，私たちがすぐにこの技術を活用できるかというと，未成熟な点が数多くあります．本稿では，ブロックチェーン技術の安全性，持続性への研究課題について紹介します．

松尾（まつお）　真一郎（しんいちろう）

NTT Research, Inc. Cryptography and Informatics Lab

ブロックチェーンの可能性と課題

ブロックチェーンに関心があるかどうかにかかわらず，ブロックチェーンに関与する理由はいくつかあります．暗号通貨，スマートコントラクト，非代替性トークン（NFT）は，このブロックチェーン（分散型台帳）をベースとした技術に依存しており，グローバルなネットワーキングやIT企業，インターネット全体に革命的な影響をもたらす可能性があります．

例えば，初期のインターネットは，単一障害点（SPOF）なしでグローバルなネットワーク構造を実現するために設計されました．しかし，インターネットを介したエコシステムの現在の問題は，影響力のある大手テクノロジ企業がまさにSPOFになっている点です．そのため，こうしたリスキーな弱点のない，拡張可能な信頼の基盤をインターネット上に構築することが求められています．ブロックチェーンは，インターネットの現在のアーキテクチャ上で，障害に耐性のあるシステムや自動的に運営されるシステムの実装に使用されます．障害への耐性を持つメカニズムをプロトコルの設計の一部に組み込むことで，システム全体を良好な状態を保つことをねらっています．

ブロックチェーンには現在のインターネットエコシステム関連の問題を解決できる可能性があるものの，ブロックチェーンエコシステム自体にも対処すべき問題がいくつかあります．例えば，セキュリティ，性能向上と分散化のトレードオフ，持続可能性などです．

セキュリティと暗号化

既存のブロックチェーンのセキュリ

ティ要件と安全性を明らかにする研究のほとんどは，技術全体とシステム全体を考慮していません．これは必ずしもセキュリティの不在を示唆する事実ではありませんが，ブロックチェーンに脆弱性がないことを明言することはできません．

リスクは，ブロックチェーンの仕様だけでなく，その実装にも存在します．分散型自律組織（DAO）に対する2016年の攻撃では，Ethereumブロックチェーンコードの脆弱性が悪用されました．ブロックチェーンは社会的インフラを構成するための基盤技術として幅広い役割を担うことが期待されているため，セキュリティインシデントの影響は大幅に拡大する可能性があります．そのため，コードの品質を確保し，攻撃が発生したときに確実に対処できるように，脆弱性に対する処理手順を導入する必要があります．

同時に，暗号化の使用に関連する標準的な運用モデルも必要です．2004年に暗号学的ハッシュアルゴリズム（SHA）-1の不正アクセスが報じられたことを受けて，IT業界が数年前にSHA-1からSHA-2に移行を完了しましたが，ビットコインをはじめとするほとんどの暗号資産およびブロックチェーンエンジニアリングコミュニティには，そのような移行の経験がなく，また，現在のブロックチェーンのソフトウェアには，移行のためのメカニズムがなく，暗号技術の脆弱性に関連する運用実績もありません．

量子計算機による暗号解読の可能性が，長期的な視点では脅威としてのしかかる中，ブロックチェーン技術で使用されるデジタル署名スキームも，遠い将来安全ではなくなる可能性があります．一方で，量子計算機が登場したとして，安全性を保つ暗号化技術についても開発が進んでいます．例えば，米国国立標準技術研究所（NIST）は，公開鍵の暗号化とデジタル署名を扱う耐量子計算機暗号の最終候補を選出しています．ブロックチェーンアプリケーションは長期的な運用を想定しているため，同様に長期的で安全な暗号化テクニックに移行することが重要です．暗号技術に脆弱性が見つかった際に，より安全な暗号に置き換えられる性質は，基盤となる暗号化の侵害が発生した場合の継続的な安全性に影響します．そのため，この性質をブロックチェーン技術，運用，ガバナンスメカニズムに組み込む必要があります．

性能向上と分散化

ブロックチェーンの台帳は，指定された処理速度のルールに従って処理されます（ビットコインの場合，10分ごとに1 MBのデータブロックが追加されます）．この上限値は，単位時間当りの最大トランザクション数を実質的に決めるため，性能向上の壁となります．ブロックチェーンの場合，この壁は単純に計算機の処理能力を高めて乗り越えることができる，という種類の問題ではありません．

この場合，ブロックの仕様を変更してブロックサイズを大きくするという解決策もあります．一方で，この解決方法では，すべてのユーザノードに保存されるデータ量が増加することになります．その結果，リソースに余裕のある裕福な個人やグループしかノードを運用できなくなり，ノード数は逆に減ります．ノード数が減少するこの解決策は，許可が不要な当初の「分散型」ブロックチェーンの理念とは矛盾するため，ブロックチェーンのセキュリティは低下します．

性能向上と分散化のトレードオフは，元々のブロックチェーン技術の設計理念に関連しています．性能を向上させるために，同じクラウドコンピュータでノード数を減らしたり，複数のノードを設定したりすると，パブリックブロックチェーンの主なメリットの1つである，単一障害点の除去という効果が失われます．そのため，アプリケーションによっては，分散型ブロックチェーンの導入によるコストメリットのバランスを考慮することが重要になります．

持続可能性

環境的な観点では，ビットコインで使用されているプルーフ・オブ・ワーク（POW）ブロックチェーンコンセンサスメカニズムが，こうしたデジタ

ル資産のマイニング（採掘）に投じられる膨大な量のエネルギーに対して持続可能なのかという懸念があります．代替となるプルーフ・オブ・ステーク（POS）メカニズムは，はるかにエネルギー効率に優れていますが，POSは確認遅延など，実装上の課題に直面しています．また，運用条件によっては，POSのメカニズムでは真に分散化したガバナンスと認められないため，規制上有価証券として取り扱われ，より厳しい規制の下での運用を強いられることになります．

ビジネスの観点では，ビットコインなどのパブリックブロックチェーンシステムは障害に対する耐性があるとみなされています．なぜなら，自らが発行する暗号資産を通じて運用手数料を生み出し，ブロックチェーンネットワークを安全に維持するインセンティブを与えるからです．資本成長理論分析では，ブロックチェーンシステムは通常は持続可能ですが，特定の標準ビジネスルール（税金，エネルギーコスト，破産のリスクなど）に制約されない利害関係者がいる場合，チェーンの持続性が損なわれる可能性があります．同様に，POWメカニズムに対するいわゆるセルフィッシュマイニング攻撃は，ブロックチェーンの支え手であるマイナーのインセンティブに影響を与える可能性があり，持続可能性のもう１つの制約になります．また，NFTや自動発効契約などでブロックチェーンを単独で使用しても，公平とみなされる成果は保証されません．公平な成果を得るには，設計を適切に考慮する必要があります．

この分野に何らかの規制が必要になることも考えられます．前述のとおり，障害に強い新たなパブリックインターネットインフラに関心がある場合は，ブロックチェーン自体のアップグレードが必要になるかもしれません．

松尾　真一郎

ブロックチェーン技術は，まだ技術が成熟していない段階で大きな注目を浴びていますが，一方で，その安全性，持続性については，基礎理論においても未解明なところが数多く残されています．NTT Research, Inc. では，誰もがブロックチェーンを安全に使うための理論の研究を進めています．

◆問い合わせ先
NTT Research, Inc.
E-mail　info＠ntt-research.com