ブロックチェーン

渡邊大喜（日本総合研究所）
watanabe.hiroki@jri.co.jp

1. ブロックチェーンとは

ブロックチェーン（Blockchain）は，暗号資産ビットコイン（Bitcoin）を支える中核技術である．ブロックチェーンは，一定量の取引データをブロックとして集約し，それを暗号技術によって連鎖的につなげたデータ構造を取る．ブロックチェーンという用語が示す範囲は文脈によって多義的である．ISO 22739:2020 では，「分散型台帳（Distributed Ledger）」として定義されており，日本ブロックチェーン協会（JBA）では，狭義の意味において「（不特定多数のノードが合意に至るための）プロトコル，またはその実装」と定義している[1]．

ブロックチェーンを用いた最初のピアツーピア支払いシステムであるビットコインに関する論文は，2008 年に匿名の人物 Satoshi Nakamoto によって発表された[2]．Nakamoto は，金融機関をはじめとした中央集権的な第三者機関を通さずに支払いが成立する電子マネーを考案しており，ブロックチェーンはこれを実現するための分散型台帳のデータ構造である（図 1）．ビットコインのブロックチェーンでは全ての送金トランザクションに電子署名が付与され，取引の真正性が保証される．ブロックは前のブロックのハッシュ値を含むことで連結され，データの完全性が保たれる．これだけであれば，改ざんが非常に困難な，頑健な取引履歴を持つ単なる台帳データベースであるが，この技術の肝は，この台帳データを構築する過程，すなわち「プロトコル」にある．トランザクションの送出は，取引の実施者によって行われるが，これらをブロックとして集約し台帳に記録するのは，取引と無関係の第三者である．この第三者は，銀行などの特定の機関ではなく，分散ネットワーク内から選ばれた唯一のノードである．このプロセスは，分散ネットワーク内のノードが全体として一致する値（ブロック）に合意できるかというコンセンサス問題と見なすことができる．

長い歴史を持つ分散システムの研究において，P2P ネットワークのような非同期環境下でのコンセンサス達成は困難であると示されている（FLP 不可能性）[3]．ビザンチン障害耐性を持つ PBFT（Practical Byzantine Fault Tolerance）やクラッシュ障害耐性を持つ Paxos などの古典的な分散合意プロトコルの実装では，メッセージの遅延に対してタイムアウトを導入するなど，弱い同期性を仮定することで FLP 不可能性に対処してきた．対して，ビットコインでは，古典的な分散システムとは異なり，コンセンサスを確率的なものと扱うことで，非同期環境下での FLP 不可能性に対処している．これは，一度受け入れたブロックの合意が覆る可能性がある非決定論的な合意である．Nakamoto は，この確率的なコンセンサスを，シビル攻撃に耐性のある Proof of Work アルゴリズムや経済的なインセンティブ，最長チェーン選択ルールなど一連の手法を組み合わせて実現している．（これらの組合せは「Nakamoto Consensus」と呼ばれる．）

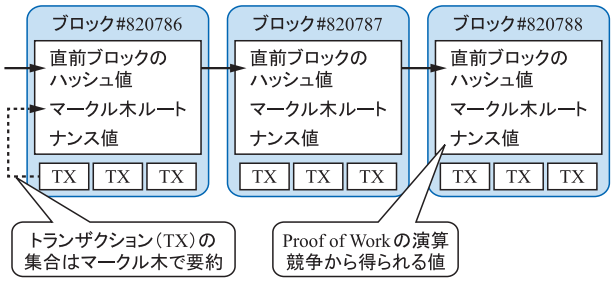

図 1　ブロックチェーンのデータ構造　　ブロックの一部（ブロックヘッダ）を入力としたハッシュ値を計算し，これを次のブロックに含めることでブロック同士を連結する．

このように，ブロックチェーンはデータ構造としてのみならず，プロトコルや分散システムとしての視点からも捉えられる多面的な技術である．なお，Nakamoto の原著においては「ブロックチェーン」という用語は登場しておらず，定義もなされていない．この用語はビットコインの開発初期にコミュニティメンバーによって普及したものと考えられる．

2. ブロックチェーンシステムを構成する要素

ブロックチェーンを用いた台帳システムを構築する技術は，ゼロから発明されたものではなく，コンピュータサイエンスの分野における既知の技術領域を巧みに組み合わせたものである．例えば，表 1 は 6 層に分けて典型的なブロックチェーンシステムの参照モデルを説明している[4]．

（1）　データ層

ブロックチェーンシステムには，ECDSA（だ円曲線 DSA : Elliptic Curve Digital Signature Algorithm）や Schnorr 署名などの電子署名方式や，SHA256 や Keccak-256 などのハッシュ関数といった多様な暗号プリミティブが要素技術として採用されている．また，マークルツリーを用いたトランザクションの圧縮やハッシュチェーンの構築，UTXO（Unspent Transaction Output）などの口座残高を表現するデータモデルといった暗号学的手法を用いたデータアルゴリズムも幅広く利用されている．

本会ハンドブック「知識の森」
https://www.ieice-hbkb.org/portal/doc_index.html

表1　ブロックチェーンシステムの参照モデル
文献（4）を基に作成．

アプリケーション層	暗号資産，存在証明，国際送金，DeFi（Decentralized Finance），NFT（Non-Fungible Token），アイデンティティ管理，など
コントラクト層	Bitcoin スクリプト，EVM（Ethereum Virtual Machine）コントラクト，など
インセンティブ層	コイン総発行量，報酬獲得方法，など
コンセンサス層	PoW（Proof of Work），最長チェーン選択ルール，PoS（Proof of Stake），DPoS（Delegated PoS），PBFT（Practical Byzantine Fault Tolerance），など
ネットワーク層	ネットワークトポロジー，データ転送，データ検証，アクセス制御，など
データ層	ブロックの仕様，タイムスタンプ，ハッシュ関数，マークル木，暗号化，など

（2）　ネットワーク層

ブロックチェーンのネットワークはピアツーピアを基本とした分散型のトポロジーを採用する．理想的には，全ノードが互いに対等に接続されることを目指すが，実際にはネットワークの拡大に伴い，フルノードだけでは運用が困難であり，台帳の一部のみを検証する軽量（ライト）ノードやJSON-RPC 通信を介してノード実行を代行する RPC ノードなど，様々な役割と用途を備えたノードが存在する．更に，不特定多数へ開かれたパブリック型ではなく，コンソーシアム型やプライベート型（または許可型）と呼ばれる閉じたネットワークで運用されるブロックチェーンも存在する．

（3）　コンセンサス層

Nakamoto Consensus で中心的な役割を果たす PoW（Proof of Work）アルゴリズムでは，大量のハッシュ計算によりブロック提案ノードを選出するプロセスを含む．このプロセスは膨大な電力消費を伴うため，環境負荷の観点から批判されてきた．更に，ブロックが覆る確率を低減しながらも，トランザクションの処理性能（スケーラビリティ）を向上させることには困難が伴う．このため，後続に開発されたブロックチェーンは，「電力消費」と「スケーラビリティ問題」を解決することに重きを置いてきた．例えば，PoS（Proof of Stake）アルゴリズムでは，計算能力に基づくノード選出の代わりに，コイン保有量に応じたノード選出が採用されている．また，代表者への選出権委任に基づく DPoS（Delegated PoS）や，ビザンチン障害耐性のアルゴリズム PBFT（Practical Byzantine Fault Tolerance）の改良版など，様々なコンセンサス・アルゴリズムの開発が進められてきた．

（4）　インセンティブ層

経済的インセンティブの設計は，ブロックチェーン維持のための重要な要素である．新しいブロックが作成されると，一定量の暗号資産が報酬として発行され，これはブロックを作成したノードに割り当てられる．ブロックチェーンのネットワークに参加するノードの動機付けのために，発行される暗号資産の総量や報酬額の設計を適切に行う必要がある．

（5）　コントラクト層

「スマートコントラクト」は，イーサリアム（Ethereum）ブロックチェーンへの実装を通じて一般への認知が広まった．スマートコントラクトの概念は，ブロックチェーンが生まれる前の 1990 年代に Nick Szabo によって提案されたものである．Szabo は，契約（コントラクト）が自由市場経済の基本的な構成要素であり，アルゴリズムによって形式化された契約の重要性を説いている[5]．この概念をブロックチェーン上で実行可能な一般化した実装としたものがイーサリアムである[6]．スマートコントラクトの実態は，ブロックチェーン上で展開されるプログラムコードである．ブロックチェーンへのコードの登録や関数の実行などは，電子署名を施したトランザクションを介して行われる．

（6）　アプリケーション層

スマートコントラクトを用いて，様々な分散型アプリケーション（Dapps : Decentralized Applications）が開発されている．多くのユースケースはブロックチェーンで実現される「プログラマブルな送金」または「公証」の機能に帰着する．「プログラマブルな送金」とは，スマートコントラクトを通じて実施される自動化された取引や条件付きの支払いを指す．例えば，クロスボーダー送金や DvP（Delivery versus Payment）決済など，既存金融サービスの効率化に取り組む事例がこれに該当する．更に，ブロックチェーンによって新たに生み出されたサービスとして，DeFi（分散型金融：Decentralized Finance）が挙げられる．DeFi はブロックチェーンシステムを基盤として，金融仲介機関を介さずに分散ネットワーク上でのアルゴリズムによる金融取引を実現したものである．一方，「公証」とはブロックチェーンの改ざん耐性と透明性に基づいて，ブロックチェーン上で事実の証跡を公に記録するものである．この種の公証は必ずしも法的な対抗要件を満たすものではないが，文書やコンテンツなどの存在証明に関する事例や，学歴や資格などのディジタルアイデンティティの証明に関する事例が存在する．ブロックチェーン独自の展開としては，これまで資産として扱われてこなかった概念，例えば，ディジタルアートの保有や不動産を利用する権利などを非代替性トークン（NFT : Non-Fungible Token）として表現することで，経済活動に組み込む事例が活性化している．

3. ブロックチェーン技術の将来展望

ブロックチェーン技術は，これまで様々な企業や組織によって，既存システムの代替としての可能性が探求されてきた．しかし，高まる期待にも関わらず，既存の中央集権型のシステムを置き換えるに足る効率性や利便性を提供できていない．一方で，パブリック型で運用されるブロックチェーンとその周辺で新たに発生したエコシステムは日々拡大を続けている．主にアーリーアダプタによって形成されるこのエコシステムでは，多様なサービスアイデアや技術が試行錯誤されており，開発者コミュニティの熱量も高い．しかし，経済的な利益を優先するあまり，セキュリティや規制への対応が後手に回り，利用者が損害を受けることも少なくない．ブロックチェーン技術の社会への受容は，短期的に進むものではなく，むしろ一進一退を繰り返しながら，長期にわたるプロセスとなるのではないだろうか．

文　　献

（1） 一般社団法人日本ブロックチェーン協会,「ブロックチェーンの定義」を公開しました.
https://jba-web.jp/news/642（2023 年 12 月確認）

（2） S. Nakamoto,“Bitcoin : A peer-to-peer electronic cash system,”2008.

（3） M.J. Fischer, N.A. Lynch, and M.S. Paterson,“Impossibility of distributed consensus with one faulty process,”J. ACM（JACM）, vol. 32, no. 2, pp. 374-382, 1985.

（4） Y. Yuan and F.-Y. Wang,“Blockchain and cryptocurrencies : Model, techniques, and applications,”IEEE Trans. Systems, Man, and Cybernetics : Systems, vol. 48, no. 9, pp. 1421-1428, Sept. 2018.

（5） N. Szabo,“Formalizing and securing relationships on public networks,”First Monday, vol. 2, no. 9, Sept. 1997.

（6） G. Wood,“Ethereum : A secure decentralised generalised transaction ledger,”Ethereum project yellow paper, 2014.

（2023 年 12 月 13 日受付）