ブロックチェーン技術の動向

林 達也 ●株式会社レピダム フェロー／ココン株式会社 技術投資室長

2018年末時点の技術的課題はレイヤリング、標準化、ネットワーク・計算機資源。今後注目の適用分野はID・監査関連で、有効なユースケースの出現が待たれる。

ブロックチェーンは技術領域で注目を集めるキーワードとなって久しいが、2018年末になって、過度な期待を集める状況から、冷静な評価がなされる程度に落ち着いてきた。ここでは、主に技術的な側面から2018年のブロックチェーン動向についてまとめてみたい。

「ブロックチェーン（Blockchain）」は、その実態はさておき、技術分野においてここ数年における「ホット」な単語だったことは間違いない。その一方で、その言及量に対して、多くの人が抱くイメージと実態が一致しない多義的な技術用語は過去に例がなかったのではないだろうか。

ブロックチェーンという単語に対する明確な（厳密な）定義といえるものは2018年末現在存在しておらず、後述する標準化の面でもこの点が大きな課題となっている。ここでは、あくまで筆者個人の観点で見たブロックチェーンと分散型台帳技術（DLT: Distributed Ledger Technology）について、インターネットと技術の観点で動向をまとめた。そのため、ここでは意図的に詳細な使い分けをせず、一括して広く「ブロックチェーン」として表記していることをお許しいただきたい。

なお、仮想通貨・暗号資産に関する領域に関しては岩下直行氏による「1-4-2 仮想通貨（暗号資産）の動きと今後の展望」を、分散型アプリケーション（Dapps: Decentralized Application）に関しては鈴木雄大氏による「2-2-1 Dappsの動向」を、それぞれ参照されたい。

■概況

2018年を終えた段階で、ブロックチェーンはまだビットコインという1つの成功例の延長上から抜け出ていない一方で、ようやく少し冷静な見方がなされるようになってきている。

これらの様々な見方は、1.技術としての評価、2.適用領域としての評価、そしてその2つを合わせた、3.今後の可能性、の3つを混同しがちである。

まず、ビットコインは、現在の状況を作り上げた一大オリジンであり、その影響範囲は非常に広く、多くの人の認識がブロックチェーン≒ビットコインとなっている点に混乱がある。ビットコインをはじめとするブロックチェーンは、すでに確立された技術を起源に、それらを組み合わせて実現されている。ブロックチェーンの根幹ともいえる公開鍵暗号などの近代的暗号アルゴリズムや暗号理論、分散データベース、デジタル・タイムスタンプ（サービス）技術、1990年代に取り組まれたMondexやe-Cashなどの電子マネーの実証実験の歴史的成果を近代的に組み合わせたものがそ

れだ。一方で、その過去の知見が反映されていない側面もあり、ブロックチェーンは「未成熟さ」と「新たな再挑戦」という熱の双方を孕んでいる状況にある。

重要な点として、ブロックチェーンは「技術的には革新的なものではなく」、「銀の弾丸でもない」ということを明記しておきたい。公開タイミングやその状況も含めて、検証済みの要素技術を正しく組み合わせた結果、社会に影響を与えるほどに普及したものがビットコインであり、その一部の特性をビットコインとは独立して表現したのがブロックチェーンだといえる。

■分類

ブロックチェーンには数多くの取り組みがあり、謳われる特徴もその実態も様々である。挑戦的なものもあれば、眉唾のようなものもあり、ひとまとめに語るのは難しいが、ここではその中でも重要だと確実視されるものに触れたい。

全体的な分類の軸として、パブリックかそうでないか（プライベートか）、が挙げられる。ここでの「パブリック」の意味合いは、誰でも参照可能でインターネット上で実際に公開された形で運用されているものといったものである。これに対して、オープンソース実装だが単一の運用がなされていないもの、そもそも参照に条件がある公開されていないものなどがプライベート型、コンソーシアム型などと呼ばれている。

また、データ書き込み・変更の権利を認証・認可なし（Permissionless）、認証・認可あり（Permissioned）に分けることもある。インターネットの文脈ではパブリックかつ認証・認可ありという形態はイメージしにくいが、SNSなど、ログインやユーザー認証（Authentication）を必要とするものを指すケースは十分あり得るだろう。（資料3-5-1）

NECセキュリティ研究所の特別技術主幹である佐古和恵氏は、「データを公開しているかどうかでパブリック／プライベートに分け、(*ノードに）参加するのに許可が必要かどうかでPermissionless／Permissionedに分けるという二軸の分類が自分にはしっくりくる」と説明している[1]（*は佐古氏との議論を踏まえた筆者による補足）。

その特性と社会的影響の大きさも踏まえ、インターネットの文脈では、パブリックブロックチェーンの重要性が現時点では高い。しかし、前述のようにパブリックといっても実態は様々であり、今後もさらに多様化していくだろう。

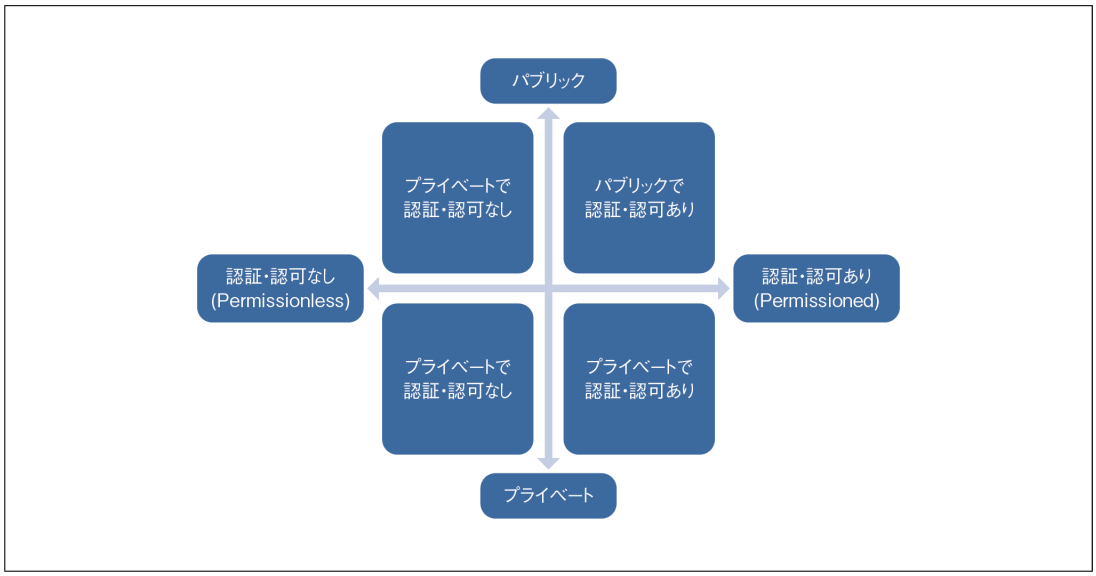
変化の激しい領域であり異論は多くありうるなかで、筆者としても断言ははばかられるのではあるが、ブロックチェーンにおける実装・プロダクトとしては、現時点では以下の3つが「代表的」といっていいだろう（ここでは評価の軸から仮想通貨的な点は外していることをご留意いただきたい）。

●ビットコイン（Bitcoin）

ブロックチェーンを大きなムーブメントにした代表例で、インターネット上で貨幣的な概念を実現する取り組みそのものとオープンソースソフトウェア実装を、そしてその実態を指すこともある。サトシ・ナカモトが公開した論文を元に実装された。

分散型（decentralized）や、コンセンサスアルゴリズム、マイニングの概念などブロックチェーンの基本的な特徴といえるもののほとんどがビットコインに含まれている。継続的に安定して動いており、事実上成功した数少ないブロックチェーンといえる。貨幣・通貨として成立しているかは多くの言説があるが、個人的な意見としては、「人の意識を変えるほど成功した社会実験」だとみな

資料3-5-1　ブロックチェーンの分類



出典：資料をもとに筆者作成

すのが適切だと思っている[2]。

●イーサリアム（Ethereum）

イーサリアムはビットコインよりも汎用性のあるパブリックなブロックチェーンとして普及している。プラットフォーム的な側面もあり、分散型アプリケーションの実装環境としてもよく利用されており、特にスマートコントラクトなどの分野では代表的で、大手クラウドサービスでのSaaSの提供なども行われている[3]。

●ハイパーレッジャーファブリック（Hyperledger Fabric）

オープンソースの基盤技術の中心的存在であるリナックスファウンデーションの下で開発されているハイパーレッジャーの一実装がハイパーレッジャーファブリックである。前述の2つに比べて、パブリックブロックチェーンのように固有のトランザクションを持つのではなくいわゆるプライベートブロックチェーンを実現することを目的としているのが特徴だ。大企業のコミュニティ参加率も高く、ビジネス向け、いわゆるエンタープライズ分野での利用を視野に入れている[4]。

■比較・評価、標準化

ブロックチェーンの有効性を計るにあたって、いくつかの重要な観点がある。簡単にまとめていきたい。

1) 既存の関係データベース（RDB/RDBMS: Relational DataBase）で十分なケースとの比較
2) クラウドサービス上のRDBサービスとの比較
3) 分散データベースとの比較

これらは、ブロックチェーンの技術的な適切さのわかりやすい指標となるだろう。後述のNISTIR 8202も参照されたい。

特に、2018年末にはアマゾンがイーサリアムとハイパーレッジャーファブリックをAWSの上で提供するAmazon Managed Blockchain Service

（アマゾン管理によるブロックチェーンサービス）を発表したことはかなり大きく受け止める必要があるだろう。単にAWS RDSとの差だけでなく、何のためにブロックチェーンが必要なのかを冷静に判断できるようになったといえる。Amazon Managed Blockchain Serviceを使うべきか、Amazon RDS for MySQLサービスでもいいのではないか、といった違いをわかりやすく比較できるだろうし、ビットコインのように自身でビットコインノードを動かす意味は何か、クラウドサービスで「ない」ことの意味は何か、などが多く人に明確になるだろう。

別の判断基準の1つに国際標準化という視点がある。単一の固有の実装ではなく、技術領域の一般化においては「標準化」というプロセスが非常に重要で、特にインターネットの世界では、相互接続性（Interoperability）が重視されている。相互接続性と公開された仕様の2つで、多くの技術が普及している。

国際標準には、大きく分けて国ごとに認められる標準と、国単位ではなく組織や個人が自由に参加可能ないわゆるデファクトスタンダードと呼ばれる標準の2種類がある。インターネットにおいてはデファクトスタンダード、オープンスタンダードの影響が強い。

ブロックチェーンの分野でも、標準化の取り組みは早々と行われている。ISOではTC307 Blockchain and distributed ledger technologies[5]、ITU-TではFocus Group on Application of Distributed Ledger Technology (FG-DLT)[6]、IEEEではBlockchain Initiative[7]が活動をしており、ワールド・ワイド・ウェブ・コンソーシアム（W3C: World Wide Web Consortium）でも、The Web Ledger Protocol[8]やCredentials Community Group[9]でのDecentralized Identifiers[10]の取り組みなどがある。さらに、インターネット標準を策定しているインターネット技術タスクフォース（IETF：Internet Engineering Task Force）でもいくつかの取り組みが始まっている。IETFのリサーチ部門（IRTF: Internet Research Task Force）では分散型インターネットインフラリサーチグループ（DINRG: Decentralized Internet Infrastructure Research Group）[11]の活動が進められているほか、標準化の事前段階としてLedger BoF（Birds of a Feather、関係者の集まり）[12]が過去に実施されている。

筆者自身も上記の標準化の一定量関わっており、私見と明記しつつもだが、標準化の取り組みとしては現時点では時期尚早であるというのが、多くの専門家の見解だといえる。

その証左として、どの標準においてもターミノロジー、いわゆる用語定義の部分すら作るのが難しく、合意形成に至っていない点がある。お互いに話しているものが一致できないほど混沌とした状況が2018年末のブロックチェーン／DLTにおける実態だ。しかし、多くの専門家が長い時間を費やしているのも事実で、結果的に少しずつ共通認識に近づいていることも間違いない。今後の動きに注目されたい。

また、標準化の文脈において、非常に役に立つ資料としてアメリカ国立標準技術研究所（NIST: National Institute of Standards and Technology）が出している内部向けのレポートNISTIR 8202 "Blockchain Technology Overview"[13]がある。特に、NISTIR 8202の8章に引用されているアメリカ国土安全保障省（DHS: United States Department of Homeland Security）作成の”Figure 6 - DHS Science & Technology Directorate Flowchart”は、特にブロックチェーンの幻想を打ち払うのに役に立つだろう。

国際標準化やコミュニティ、コンソーシアムにはほかにも多くの活動がある。ハイパーレッジャーももちろんわかりやすい例であるが、特筆すべき国内関連のものとして2つを挙げておく。

1つは、ビットコインのスケーラビリティを解決することから始まったスケーリングビットコイン・ワークショップ（Scaling Bitcoin Workshop）[14]で、技術的に非常に先進的な取り組みと活動が行われているビットコインに関するトップの活動だ。2018年にはワークショップが日本で開催された。

また、いわゆる仮想通貨交換業者のセキュリティにフォーカスしたクリプトアセットガバナンスタスクフォース（CGTF: Cryptoassets Governance Task Force）[15]というコミュニティが日本で立ち上がっており、IETFやISOなどの標準化団体と連携しつつ、利用者・消費者保護のリスク管理のための安全対策基準の策定やベストプラクティスを提供している。

■課題と期待

ブロックチェーンには、まだまだ未解決の技術的課題が多い。特にネットワークと計算機資源に関しては、かなり冷静に考えなくてはならない課題がある。

変動はあるものの、Bitnodes[16]によると、ビットコインノード数は2018年に遂に1万ノードを超えた。しかし、クラウド時代の1万ノードというのは特に大きな数ではない。ただし、ブロックチェーンの特徴といわれるP2Pネットワーク（Peer to Peer Network）においては、独立したネットワークノードが重要であり、これが多様性を持ったネットワークトポロジーを形成していることで、ピア（peerまたはend）同士の結びつきとして重要性を持つ。

このP2Pネットワークの特性を考えれば、ノード数はそのネットワークの強度につながっていくわけだが、単純にクラウドサービスにインスタンスを増やし続けるだけではブロックチェーンの特色はあまり活かされない。実際に、イーサリアムでは特定のインフラストラクチャに依存していることを問題視する指摘がある。

さらに、ビットコインをはじめとしたブロックチェーン技術において「記録はずっと続けられていく」ため、必要なストレージ量がどんどん大きく増えていくことが避けられない。ブロックチェーンネットワークにおけるノード数が増えれば増えるほど、未来において必要なストレージも拡大していく（これは正確にはフルノードと呼ばれる種別のノードにおける課題であり、ノードの種別分けはすでに行われている）。

資源以外にも、ブロックチェーンの技術視点での大きな課題として、レイヤリングの概念が導入されていない点がある。

プロトコル分野の歴史におけるレイヤリングの論理的な概念としては、ISO OSI参照モデルが挙げられ、そこでは7階層（レイヤー）の分類がなされている。インターネットの世界ではこのモデルから4階層にまとめられており、概念（OSI）と実際の定義（IETF）、さらにその普及の実態・実装はあくまで独立しているが、レイヤーは共通の概念や語彙で整理・分類されている。そして、レイヤリングによって、プロトコルの独立性、疎結合性、相互接続性が担保されることが実際の普及における大きなベネフィットとなっている。

しかし、ブロックチェーンの世界ではこれらが行われておらず、P2Pプロトコルなどのわかりやすい部分ですら相互接続性はもちろん、用語定義すらすり合わせがなされていない。ほかにも、コンセンサスアルゴリズムは、ブロックチェーンでよく話題になる技術的トピックだが、レイヤリングが適切になされていれば、状況・環境に応じた

コンセンサスアルゴリズムを使うなども視野に入ってくる可能性があるものの、現時点ではまだまだそこに至ってはいない。

ブロックチェーンにおいてその初期からすでに大きな課題になっているのが、スケーラビリティの問題である。ビットコインでは端的にトランザクションの確定に10分かかるなどの問題となって顕在化しているが、この問題の主体となるブロックチェーンの外、オフチェーンやサイドチェーンで多段階層を用いて解決するアプローチが「レイヤー2技術」と呼ばれるものである。なお、ここでいうレイヤー2は先に言及したネットワーク視点のレイヤーとはまた別の視点での階層なので注意してほしい（用語の適切さへの配慮の不足はこれらの部分からも透けて見えるだろう）。レイヤー2技術に関して、ビットコインにおいてはライトニングネットワーク[17]が、イーサリアムにおいてはプラズマ／プラズマキャッシュ[18]が、それぞれ実用に非常に近い取り組みとして実装も含めて進んでいる。ただし、議論や研究の余地も残っており、実際にビットコインやイーサリアム上で普及・実用されるまでには、今後も変化があり得る注目領域だ。

そして、これらのオフチェーン、サイドチェーンなどと呼ばれる、主たるチェーン（メインチェーン）そのものではない連携するブロックチェーンの技術は、まだ実装・普及の直前ということも踏まえつつ、今後重要になるといわれている。あわせてこの先は複数のブロックチェーンをつなぐ／アトミックスワップを実現する、クロスチェーンの分野も今後注目の技術トピックになるだろう。すでにある近しい取り組み、参考情報としては、Interledger Protocol（リップル）[19]やNiji（NTT）[20]などが挙げられる。また、Scaling Bitcoin Workshopの発表資料、特に2018年のものは参考になるだろう。

技術的な観点での「トラスト」「トラストレス」という点にも意識を割いておきたい。多くのブロックチェーンではいわゆる「フォーク」と呼ばれるブロックチェーン（トランザクション）の分岐が生じている。事故によるものをアクシデンタルフォーク、互換性の維持された仕様変更によるものをソフトフォーク、互換性のないものをハードフォークと呼ぶことがある。そして、特にハードフォークは、パブリックブロックチェーンにおいて単一で変更不能なはずのトランザクションを、主にソフトウェアの変更により変更（分岐・巻き戻し）してしまうものだ（BitcoinとBitcoin Cashのケース、EthereumとEthereum Classicのケースが有名）。重要なのは、「ハードフォークが可能」な場合、全体向けにその意思決定を行える主体がいるということで、このとき、この主体を「中央」として「トラスト」しているのではないか？という疑問が生じる。そして、これを踏まえてあらためてNISTIR 8202のフローチャートを見てもらうと、ブロックチェーンの幻想と実態をよく理解してもらえるだろう。

最後に、これらを踏まえて今後のブロックチェーンの適用が期待されている分野に触れておきたい。これまでの流れのなかで、元々分散DBで十分、クラウドで十分と思われていた領域に対して、少し温度感が変わってきているのがアイデンティティ（本人確認）分野である。

以前より、難民のような個人としての記録がない（持てない）人々に対してIDを発行する基盤になるのではないかといったユースケースが挙げられていたが、これは「自己証明型身分証明（Self-Sovereign Identity）」のようなアイデンティティ領域での利用として現在注目されている。また、前述したW3Cでも議論されているが、分散ID（Decentralized Identity）も近い領域といえる。

パブリックブロックチェーンの議論では、そもそもいわゆる認証的な「認証する側」「される側」という観点がなかったといえるが、監査済みの記録としてアイデンティティを実現するという流れには一定の価値を感じられる。こうしたなか、マイクロソフトはMicrosoft Decentralized Identity[21]を発表し、注目を集めている。

そのほか、本人確認、ID Proofing、顧客確認（KYC: Know Your Customer）などのID分野がユースケースに挙げられ、それ以外にも監査やサプライチェーンマネジメント（SCM）の分野でも注目を集めている。これらにおいても記録を確認可能にする意味での識別（Identification）が必要であり、結果的にアイデンティティ分野との関連が強い。これは、インターネットという環境とパブリックブロックチェーンの狭間といえる領域であり、DNSのような仕組みを踏まえて今後につながっていくところだと思われる。

私見だが、ブロックチェーン時代とはデータ主体の時代なのではないかと考える。それ以前の時代はソフトウェア、アプリケーションが主であり、そこから生成・管理されるデータがある（従）という世界だったが、ブロックチェーンではブロックチェーンのデータが主、それを維持するためのソフトウェアが従という時代となってくのではないだろうか。

ブロックチェーンは、課題を抱えながらも徐々に正しい評価に近づいていく流れにあり、今後、こういった領域に関連するユースケースが有効になっていく可能性が高いといえるだろう。

1. https://crypto.watch.impress.co.jp/docs/event/1160114.html
2. https://bitcoincore.org/
3. https://www.ethereum.org/
4. https://www.hyperledger.org/https://www.hyperledger.org/projects/fabric
5. https://www.iso.org/committee/6266604.html
6. https://www.itu.int/en/ITU-T/focusgroups/dlt/Pages/default.aspx
7. https://blockchain.ieee.org/
8. https://w3c.github.io/web-ledger/
9. https://github.com/w3c-ccg
10. https://w3c-ccg.github.io/did-spec/
11. https://datatracker.ietf.org/rg/dinrg/about/
12. https://datatracker.ietf.org/wg/ledger/about
13. https://www.nist.gov/publications/blockchain-technology-overview
14. https://scalingbitcoin.org/ja/
15. https://vcgtf.github.io/
16. https://bitnodes.earn.com/
17. https://lightning.network/
18. https://github.com/ethereum-plasma https://plasma.io/
19. https://interledger.org/
20. https://arxiv.org/pdf/1810.10194.pdf
21. https://didproject.azurewebsites.net/

インターネット白書 ARCHIVES

1996,1997,1998,1999,2000....

［インターネット白書ARCHIVES］ご利用上の注意

このファイルは、株式会社インプレスR&Dが1996年～2019年までに発行したインターネットの年鑑『インターネット白書』の誌面をPDF化し、「インターネット白書ARCHIVES」として以下のウェブサイトで公開しているものです。

https://IWParchives.jp/

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、データ、URL、名称など）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真・図の作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は掲載されていない場合があります。
- このファイルの内容を改変したり、商用目的として再利用したりすることはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用される際は、出典として媒体名および年号、該当ページ番号、発行元（株式会社インプレスR&D）などの情報をご明記ください。
- オリジナルの発行時点では、株式会社インプレスR&D（初期は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

お問い合わせ先 | 株式会社インプレスR&D | ✉ iwp-info@impress.co.jp