Web3の技術と未来への課題

斉藤 賢爾 ●早稲田大学 大学院経営管理研究科

Web 1.0とWeb 2.0におけるデータ生産の取り組みを統合しようとするWeb 3.0の試み。しかし、ブロックチェーンによって実現するには課題が多い。技術の進展のために冷静な議論と研究が求められる。

■Webの歴史を振り返る

「Web3」なる用語が何を指し示しているかにはいまだ混乱が見られる。しかし、公開台帳の記録維持作業への参加の報酬として暗号資産を組み込んだ「ブロックチェーン」という仕組みが関係することは、ほぼ共通の認識と言えるだろう。

金融資産が絡むとすれば、議論はポジショントークになりがちで混乱が助長される。そこで本稿では、Web3の技術的要素を抽出することで概念の整理を試みつつ、技術に注目して解説し、将来に向けた課題を問題提起する。

Webと呼ばれる以上、まずはWebの歴史を振り返るところから始めたい（資料1-1-1）。

●いわゆるWeb 1.0

World Wide Web（または単にWeb）は、1989年にティム・バーナーズ＝リー（Tim Berners-Lee）氏らによって発明された[1]。この段階はレトロニム[2]により「Web 1.0」と呼ばれる。Webの当初の目的は、世界中の大学・研究機関の科学者の間で論文をはじめとする情報共有を自動化することだった。論文は基本的にすべての科学者が書くのだから、参加する全員がデータの生産者であり、Webは最初から双方向だったと言える。

しかし、インターネットの商用化を経て参加した一般ユーザーにとっては、サーバーを立てて管理することのハードルが高く、Webは多くの人々にとってもっぱら閲覧する対象となっていった。

●Web 2.0

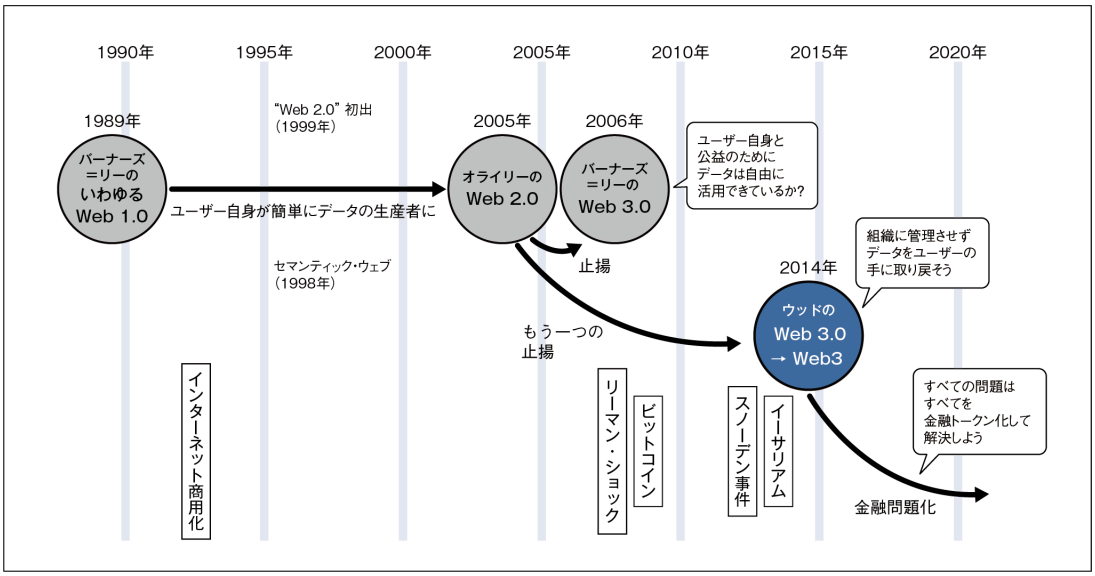
「Web 2.0」という言葉の意味を決定づけたのは、2005年のティム・オライリー（Tim O'Reilly）氏による記事である[3]。Web 2.0は、特定の技術を指すというよりも、Webの新たな応用パターンの総体であり、ブログやソーシャルメディアといったWeb上のサービスを利用することでユーザー自身が簡単にデータの生産者となり、改めてWebが双方向化したことが特徴と言える。

「GAFA（Google, Apple, Facebook, Amazon.com）」はWeb 2.0の時代の象徴であり、それぞれが提供する検索エンジンやWebメール、動画プラットフォーム、センサーの集合体としての端末やOS、社交プラットフォーム、消費プラットフォームなどの利用を通して、ユーザーの生活が生み出すデータが価値の源泉となった。

●Web 3.0とWeb3

メタデータの付加によってデータの自動処理を向上させるセマンティック・ウェブなど、以前からWebの高度化を進めていたバーナーズ＝リー

資料1-1-1　データの生産と活用から見たWebの歴史



出所：筆者

氏は、遅くとも2006年には「Web 3.0」のイメージを持っていたと考えられる[4]。これは、Web 2.0の課題として生じた、データの管理や利用がサービスのプラットフォームの壁で分断されてしまう問題に対抗し、個人や公益のためにデータを自由に活用できるようにすべく、汎用のデータ形式とプロトコルによってWeb上のデータをつなぎ直す試みである。

弁証法的に言えば、Web 3.0は、Web 1.0（フラットな双方向性を持つが難易度が高い）とWeb 2.0（双方向性を簡便に提供するが分断されている）の対立を止揚して統合するものだと言える。

一方、イーサリアム（Ethereum）と呼ばれるブロックチェーンのプロジェクトをヴィタリック・ブテリン（Vitalik Buterin）氏と共に立ち上げたギャビン・ウッド（Gavin Wood）氏は、2014年のブログ記事でWeb 3.0を改めて提唱した[5]。これが、現在Web3と呼ばれるものの原型である。

ウッド氏のWeb 3.0は、2013年に明らかになったスノーデン事件を意識したもので、ユーザーのオンラインでの活動が監視されないことに重きを置き、組織にデータを管理させないことを目指した。

その技術的要素を、ウッド氏による表現に沿って抽出すると①静的な出版②仮名（かめい）での動的なメッセージ③コンセンサス・エンジン④統合されたユーザーインターフェース――の4つとなる。

このうち①はIPFS[6]のような分散ストレージをイメージしており、静的という言葉には変化しない、すなわち投入後に改変されていないことを検証可能という条件も含む。②は、そうした投入も含めて本人がデータを動的にアップデートできることと、そうしたオンラインでの活動を第三者に対して秘匿できることを示している。

①と②はどちらも、広い意味でデータが検閲されない（公開や共有が邪魔されない）ことを示す。そのためには可用性が担保される必要があること

から、①と②を満たす条件の一部として耐障害性がある。耐障害性を保つための常套手段は、ネットワーク上に多数の複製を持つことである。これをユーザーの自律的な参加に任せ、開かれた分散システムとして実現することにより、特定の第三者による検閲を防げる効果も期待できる。

複製間で状態を一致させるためには、それぞれが処理するトランザクションの順序も一致させなければならない。それは計算機科学的な意味でのコンセンサス[7]であり、③の実態となる。しかし、ウッド氏は③を「人々がルールに合意する」というような意味で用いており、技術的な実態と懸け離れている側面がある（その弊害については後述する）。

技術の実態に即しつつ、ウッド氏の言うWeb 3.0の要素を改めて整理し直すと次のようになる。なお、コンセンサスが含まれないのは（a）の一部であるためである。

（a）広い意味で検閲できない公開台帳
（b）ユーザーの活動内容の秘匿
（c）それらを統合するブラウザーとユーザーインターフェース

次項では、これらの実現のために実際に用いられている技術を解説する。

■Web3の技術

●イーサリアムブロックチェーン

ブロックチェーンは、広い意味で検閲できない公開台帳を目指す技術である。イーサリアムブロックチェーンの構造を、資料1-1-2に簡単に示した。

現在のイーサリアムでは、バリデータ（承認者）として記録の維持に参加し、暗号資産であるETH（イーサ）での報酬を得るためには、32ETHのデポジットをシステムに預けなければならない。ブロックはトランザクションの集合であるが、過去にさかのぼってブロックの内容を改ざんしようとすると、ブロックが作成された当時のデポジット総額の大半に相当するバリデータからの証言を取得し直さなければならないため、非常に困難となる。

このブロックチェーンは「スマートコントラクト」と呼ばれる計算オブジェクトを投入しておき、トランザクションによってその機能を呼び出して実行できる。実行結果もブロックチェーンに記録されるため、その実行が真正だったことを参加する全員が確認できる。実行に当たって必要となる計算ステップ数やストレージ容量などの計算機資源の量は「ガス」と呼ばれる。ガス使用料はETHによってしか払えない。

●イーサリアムアドレスとZK-Rollup

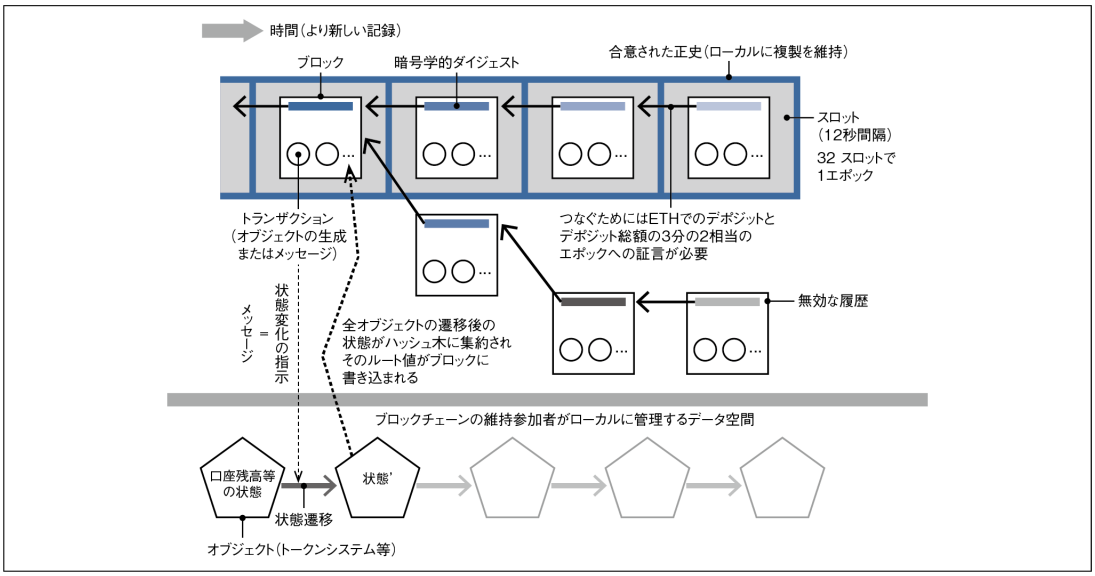
イーサリアムにおけるユーザーの識別子（アドレス）は、おのおのが生成した鍵ペアのうちの公開鍵の暗号学的ダイジェストであるので、仮名（かめい）が実現されている。

Rollupはトランザクションをオフチェーンで、すなわちブロックチェーンの外側で実行する「レイヤー2」の技術である。ZKはゼロ知識を表す。ZK-Rollupでは、多数のトランザクションについて、その内容を秘匿しつつ、実行の真正性の証拠のみを集約して「レイヤー1」のイーサリアムブロックチェーンに書き込める。これにより、ユーザーの活動内容の秘匿とスケーラビリティを同時に実現できる。

●Web3ライブラリ

プログラミング言語ごとにライブラリを用意し、APIを通してイーサリアムの機能を使えるようにすることで、Webプログラミングとイーサリ

資料1-1-2　イーサリアムブロックチェーン



出所：筆者

アムの世界を接続できる。これがWeb3のプログラミング的な側面である。

こうしたライブラリには“web3.js”や“web3.py”などがあり、HTTPやWebSocketを通してWebアプリケーションの中からイーサリアムとその上で動作するスマートコントラクトの機能が利用できる。

■Web3の課題

●よく知られた課題

現在のイーサリアムでは、バリデータは全員が同じ処理を行うため、バリデータ数の増加によっても全体の処理能力が向上しないというスケーラビリティの問題がある。また、人間には秘密鍵の管理が難しく、鍵の漏えいや紛失が後を絶たない。これらへの対策として、シャーディング（水平分散（未実装））やソーシャル・リカバリー・ウォレット[8]などの技術がある。

Web 2.0への回帰的な現象が起きていることも課題である。NFTマーケットであるOpenSea[9]やイーサリアムのノードへAPIを提供するinfura[10]などが巨大プラットフォーム化し、それらへの依存性が高まっている。

●暗号資産の価格低下リスク

スマートコントラクトの実行基盤がもはやイーサリアムだけではない現在、ガス供給量とガス使用料の価格によって複数の実行基盤が競争する市場が生まれている。この競争に伴う価格の均衡化によって暗号資産の市場価格が下がると、バリデータの撤退が起き、ブロックチェーンの安全性が低下する。

●意思決定

ウッド氏はWeb3によって「人々がルールに合意できる」と考えている節があるが、実際には、検閲されずに意思表明を記録することしかできない。それを用いた投票は可能なので、Web3における組織の意思決定は投票に頼りがちである。

しかし、例えば議案がスマートコントラクト

の形式で提出されたとして、投票者が正しく議案を理解できるか、可決した内容を実行するのは誰か[11]といった問題が生じ、それが、人々がだまされたり自律分散しているはずの組織に実質的な支配者が存在したりといったさらなる問題を生んでいる。

■さらなる未来に向けた課題

●ファクトは維持できるか

2022年、機械学習に基づいて画像や文章の生成を対話的に行えるサービスが続々と公開され、我々の知的行為の多くが自動化によって支援される世界の到来がさらに近づいた。

もとより我々はメディアを通してしかニュースに触れておらず、ほとんどの場合に物事の真偽を直接には確かめずに生活している。そんな中に、自動生成されたリアリスティックな画像や文章が大量に組み込まれていくとなれば、我々にはファクトを維持し安全に共有する方法が必要になるだろう。広い意味で検閲できない公開台帳は、概念的にはそのための技術となり得る。

しかし筆者は、ブロックチェーンはそのための適切な技術ではないと考えている。基盤の維持が、暗号資産の市場価格が高まることをインセンティブとする参加者らに依存しており、仮に自動システムが暗号資産を売却するように人々を誘導すれば、価格が操作されることで維持者が退出し記録の安全性が損なわれ得るからである。

●人間は何によって駆動されるのか

資料1-1-1に示したように、最近のWeb3は暗号資産やNFTといったトークンの所持とその市場価格の上昇をインセンティブとして人々を駆動し、すべての問題を解決に導けると考えている節がある。しかし、トークンの市場価格に依拠する考え方の危うさは先に示した通りである。

ユーザー自身と公益のためにデータが自由に活用できることも、ファクトが維持されることも大事である。しかし、Web3はそのために適切な方向に進んでいるのだろうか。本稿がそれを考える一助となれば幸いである。

1. https://home.cern/science/computing/birth-web
2. レトロニムとは、後発の概念の広まりを受け、先発の概念を改めて呼び分ける必要性から生まれた用語。例えば「デジタルカメラ」に対する「フィルムカメラ」。
3. https://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html
4. https://www.nytimes.com/2006/05/23/technology/23iht-web.html
5. https://gavwood.com/dappsweb3.html
6. https://ipfs.tech/
7. 複数の計算プロセスの間で同じ変数の値が等しく共有されること。
8. 秘密鍵の紛失に際して社交関係を利用したリカバリーが可能である。
9. https://opensea.io/
10. https://www.infura.io
11. スマートコントラクトは、ガス使用料を支払う主体が外部から呼び出すことによってしか実行できない。

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および株式会社インプレスが1996年～2023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および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 | インプレス・サステナブルラボ | ✉ iwp-info@impress.co.jp