web3 は金融なのか

斉藤 賢爾｜早稲田大学 大学院経営管理研究科 教授

要　約

「web3」なる言葉が巷を賑わせている。その起源は必ずしも金融と関係しないが、実態としては、DeFi（分散ファイナンス）、NFT（非代替性トークン）, DAO（分散型自律組織）等をその要素として含むとされ、（次世代の）金融に関わる概念であることが示唆される。

本稿では、技術を平易に解説することを通して、web3 が何であるかを考える。ブロックチェーン、スマートコントラクト、DeFi といった基本概念の整理に加え、web3 と特に関係が深いとされる概念のうち、比較的定義が明確な NFT や DAO について詳細に解説し議論する。

結論を述べれば、その金融的側面に注目したとしても、web3 は金融ではないと考える。しかし、金融資産として捉えられがちなデジタルトークンを扱うという意味で、金融が先鋭化したものであることには違いない。私たちは、web3 を考えることを通して、「金融とは何か」という問いに立ち返ることになる。

斉藤 賢爾

早稲田大学大学院経営管理研究科教授

コーネル大学より計算機科学において工学修士号、慶應義塾大学よりデジタル通貨の研究で博士号を取得。日立ソフトウェアエンジニアリング、慶應義塾大学大学院政策・メディア研究科特任講師等を経て現職。

1．はじめに

1．1　web3 との出会い

筆者が「web3」という言葉と初めて出会ったのは、Python プログラミング言語のライブラリ[1]である“web3.py”（2016 ～）の使用を通してである。これは、Javascript 用のライブラリである“web3.js”（2014 ～）から派生したもので、Ethereum[Buterin, 2013] ブロックチェーンとやり取りするソフトウェアを記述するための部品集である。筆者は、Ethereum の応用システムを Python で記述するために、2017 年頃からこれを使用している。“web3.py”は Ethereum 財団によって開発・維持されているので、Ethereum の開発組織自らが、その応用の枠組みを web3 と呼んでいるらしい、と知ったのである。

以上が筆者と web3 との出会いだが、では、世界はどのように web3 と出会ったのだろうか。

web3 と似た言葉に「Web3.0」がある。これは似た言葉というよりも、web3 の起源である。それでは、World Wide Web（WWW または単に Web）の生みの親である Tim Berners-Lee による整理 [Berners-Lee, 2009] に沿って、Web の n.0 バージョン呼称の変遷を見てみよう。

Berners-Lee が 1989 年に発明した、言わば Web1.0 は、その初期の頃から読み書き可能で、全人類が共有するフラットなハイパーテキスト[2]空間だったが、掲示板などの仕組みは作れたものの、書き手としての（データの生産者としての）ユーザの参加は、ハードルが高く、多くはなかった。

1：ソフトウェアの開発を容易にするための部品集。

2：「ハイパーリンク」によって他のテキストを参照し、アクセスできるようなテキスト。

その後、Web2.0[O’Reilly, 2005] という言葉が生まれることになる。これは、データの生産者としてのユーザの参加がより容易になったことを表現したもので、ブログや様々なウェブサービス、そしてソーシャルメディアの台頭により代表される（Web2.0 という概念が生まれたために、遡及的に Web1.0 という言葉が用いられるようになった）。Web2.0 では、Web がアプリケーションサービスのプラットフォームになったが、データがサービスに所有されるため、フラットだった Web の空間に、サービス毎の壁が改めて作られることになった。

その後すぐに Berners-Lee により提唱された Web3.0[Berners-Lee, 2009] では、この「サービス毎の壁」を問題視している。データがリンクされることの復権を叫び、汎用化されたデータ形式とプロトコル（通信規約）を推進し、Wikipedia に代わる DBpedia なるデータ参照の体系化を呼びかけ、オープンデータとビッグデータ解析を促進する、オントロジー（概念体系）を組み込んだ「セマンティック・ウェブ」を提唱した。

一方、Ethereum の共同創設者である Gavin Wood は、同様の問題意識から、独自に Web3.0[Wood, 2014] という言葉を使い始めた。Wood の Web3.0 では、サービスがデータを所有している問題に加え、「スノーデン」[Gidda, 2013] 後の世界においては、個人のデータの管理を組織に任せることは「根本的に壊れたモデル」だとした。

Wood の Web3.0 は、1）検閲できない出版システム、2）仮名（pseudonym）によるメッセージング、3）コンセンサス・エンジン、4）それらを統合するブラウザとユーザインタフェース、の 4 要素から成る。純朴に考えるならば、1）～ 3）は Ethereum により実現されている[3] ので、Ethereum にブラウザを加えたもの、すなわち、Ethereum をブラウザからアクセス可能にしたものが、Web3.0 を実現するソリューションだと Wood らは考えたのだろう。

しかし、Berners-Lee が提唱する Web3.0 と Wood の Web3.0 の混同は避けられない。そうした理由もあって（あるいは単に言葉を省略して[4]）Wood をはじめとする Ethereum 関係者らは web3 という言葉を用いるようになり、Ethereum に接続するためのプログラミング言語ライブラリに “web3.{js¦py}” といった名称が用いられるようになったのだろう（Wood は後に Ethereum を離れ、Web3 財団を共同創設する）。

1．2　web3 概念の変容

ところが、基本的には Ethereum と接続する外部システムを含めたブロックチェーンの応用を指していたこの言葉は、後に変容するに至った。[Kharif, 2021] が述べるように「私たちがオンラインで行うほぼすべてのことの内部に、トークン（代替貨幣）という形で金融資産を組み込む」運動と捉えられるようになったのである。

後述するように、トークンは近代的な所有の概念を実装するからか、このことを Wood の Web3.0 が目指す「個人にデータの所有権を返す動き」と理解する人が多い。つまり、web3 の概念は、今日、「情報管理の分散化」と「あらゆるものの金融トークン化」という 2 つの要素から成っている。

以降では、背景となる技術の解説に続き、web3 を構成する技術の詳細を見ていく。

3：筆者はここに Wood をはじめ多くのブロックチェーン関係者の誤謬があると考えている。本文にて後述するように、ブロックチェーンにおけるコンセンサスは人間の合意ではなく、単に履歴の複製間の整合を取るための機構に過ぎない。web3 に根本的に欠けているのは、人間が合意を形づくることへの洞察ではないだろうか。

4：例えば “web3.0.py” はファイル名としては可能だが、Python のライブラリ名としては扱いが煩雑になる。

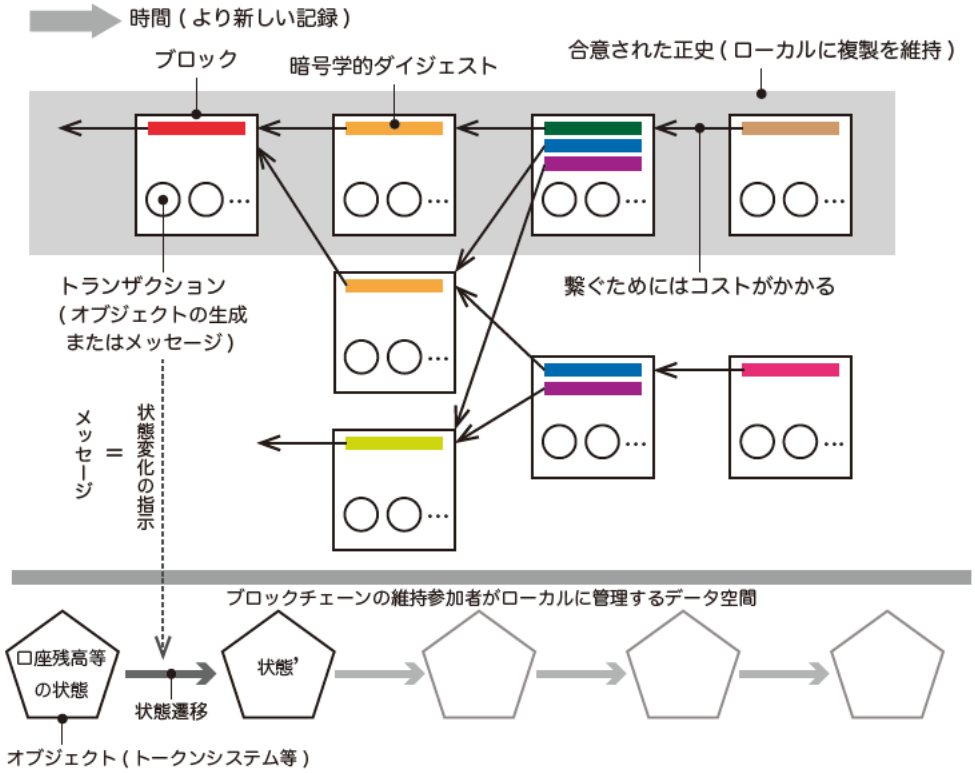
2．背景となる技術

2．1　ブロックチェーン

最初のブロックチェーンシステムである Bitcoin[Nakamoto, 2008] は、もともと銀行による検閲への対策として作られたものである。暗号資産の送金を記録するブロックチェーン技術は、銀行などの仲介者を信頼するのではなく、以下の 4 つの性質を満たし、かつ誰もがそのことを検証できることで、広義の耐検閲性の実現を目指した。

1. 自己主権性 — アカウントを勝手に作れ、本人であることを自ら証明できることを含み、常に自分に決定権がある。
2. （狭義の）耐検閲性 — 誰にも送金記録（取引）の投入・確認を妨げられない。
3. 耐障害性 — 障害の発生によっても送金記録の投入・確認を妨げられない。
4. 耐改ざん性 — 送金記録を改変したり捏造・抹消できない。

図 1　抽象化されたブロックチェーン



資料：筆者作成

ブロックチェーンは、図 1 のように抽象化される。トランザクション（送金記録を一般化したもの）は参加者の間でブロードキャストされ、ブロックチェーンの維持者（Bitcoin 等ではマイナーと呼ばれる）により数百・数千個の単位でブロックに詰められる。ブロックもまたブロードキャストされる。ブロックは、直前のブロックの暗号学的ダイジェスト[5]を含むことで、時間の前後関係の中に位置づけられる。一番最初のブロック（ジェネシスブロックとも呼ばれる）を除き、すべてのブロックは、その直前と見なす（複数の）ブロックをダイジェストにより指し示すので、全体として DAG（Directed Acyclic Graph; 有向非巡回グラフ）を形成する（図における「←」の連なりの構造）。この DAG の各辺（個々の「←」）

5：暗号学的ハッシュ関数により計算される値で、計算の元となるデータ（原像）が同じであれば必ず同じ値になるが、1 ビットでも異なると全然違う値になる。また、どのようなダイジェストになるかは実際に計算するまで分からず、ダイジェストだけを得ても原像を推測できない。

の（再）形成には、Proof of Work（作業証明）[6] や Proof of Stake（ネイティブトークンのデポジット額に応じた権利による投票）など、大きなコストがかかる。もし、悪意のある攻撃者が DAG を遡及的に変更しようとすると、蓄積された膨大なコストを支払わなければならなくなる。一般に、参加者は、ブロックの並びのうち、形成に最も大きな累積コストがかかったもの（すなわち、最も改ざんのためのコストが大きい歴史）に合意し、それを正史として採用する。すなわち、ブロックチェーンは、全体として、参加者各々のローカル環境に正史を複製する過程として動作する。

データに注目すると、参加者のローカル環境で口座残高等の状態が管理される。トランザクションは状態を変化させる指示（メッセージ）だと見なせ、ブロック（の中のトランザクションすべて）が適用されると状態が変化する。このことから、筆者らは、ブロックチェーンを確率的 [7] に進行する状態遷移システム（確率的状態マシン）であると定義づけた [Saito and Yamada, 2016]。

ブロックチェーンの維持に参加すれば、そのシステムにネイティブなトークン（例えば Bitcoin であれば bitcoin, Ethereum であれば Ether）で報われるように設計されているのが普通である。しかし、トークンの市場価値が下がれば、維持者の撤退が増える。すると自動的な調整により維持のためのコストが下がり、改ざんに対する抵抗力が低下する [Iwamura et al., 2019]。それは更なる価格低下と撤退を招きかねない。この正のフィードバックは、ネイティブトークンへの期待が維持されている間は逆に価格の上昇に繋がるが、期待が失われると負のスパイラルに陥り、ブロックチェーンが停止してしまう可能性がある。一旦停止すると、仮に再び開始したとしても、改ざんコストを比較的安価に打ち消せる過剰なハードウェアやトークンが市場に残っているため、新しいチェーンを同様に検閲に強いものにすることは困難だと考えられる。

2．2　スマートコントラクトと DeFi

ブロックチェーンにプログラムコードを書き込んで実行することで、コードやデータについても自己主権性、（狭義の）耐検閲性、耐障害性、耐改ざん性を実現できる。こうしたアプリケーションを「スマートコントラクト」（あるいは単にコントラクト）[Buterin, 2013] と呼び、ユーザはそれを使って本物のプログラムコードが実行されているか、それによって得られた結果が正しく共有されているかを検証することができる。

スマートコントラクトを金融に応用すると、新たなトークンシステムの運用、条件に基づく自動送金、通貨間のスワップ等が可能になる。大まかには、これが DeFi（Decentralized Finance; 分散ファイナンス）である。

3．web3 を構成する技術

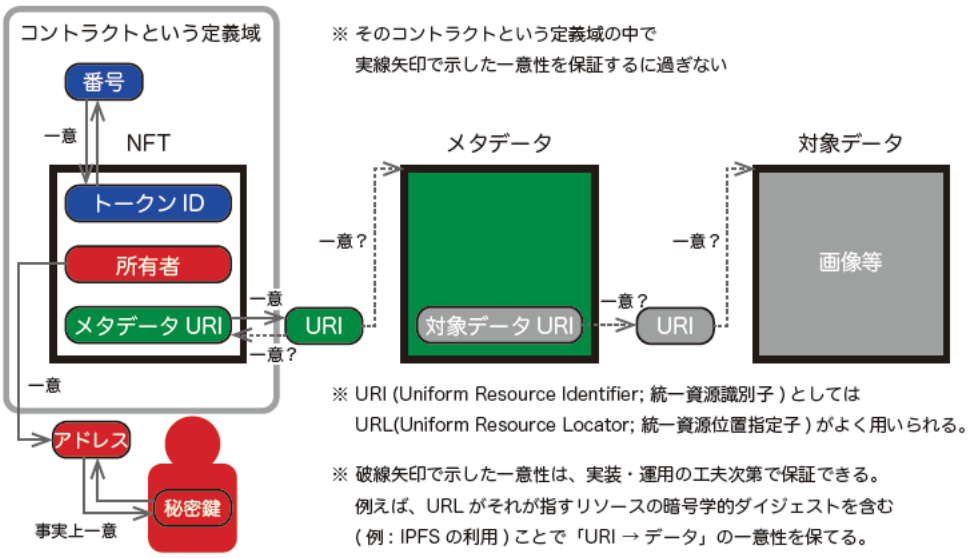
3．1　NFT

スマートコントラクトにより、デジタルな NFT（Non-Fungible Token; 非代替性トークン）の発行も可能になる。ブロックチェーンに書き込まれることで、NFT はその所有者によってのみ他者に譲渡できることが保証される。しかし、物理的かデジタルかに関わらず、ある NFT がブロックチェーンの外にある何かの所有権を表しているかどうか、あるいはある NFT が本物であるかどうかについては、社会的合意に頼らなければならないため、注意が必要である。

6：ブロックのダイジェストが示されたターゲット値以下でなければならないという制約を設け、ブロックの内容を変えながら、当たるまで何度もダイジェストを計算するという「計算機的なくじ引き」を課し、ブロックの生成に多大なコストを生じさせる方式。

7：ブロックチェーンにおいて正史が定まっていく過程は確率的で、時に後戻り（リオルグ；再編成）が起きる。

図2　NFT と一意性



資料：筆者作成

図 2 は、よく使われている ERC-721[8][Entriken et al., 2018] NFT 仕様における一意性を描いたものである。

NFT は、一意に付けられたトークン ID（番号）により区別されるが、コントラクトが定義域となるため、コントラクトの外部ではそもそも一意性は成り立たない。同じ番号の別の NFT は、そのコントラクトの中には存在できないが、他のコントラクトの中には存在できる。

NFT には所有者が割り当てられる。所有者は、その NFT を処分できる（他人に所有を譲ったり、存在しないアドレスに譲渡することで破棄できる）ため、近代的な所有の概念を実装していると言える。だが、その所有は NFT そのものに対してであり、NFT に記されているメタデータ URI が示すメタデータや、更にそのメタデータが示している対象データ（画像等）にまで及ぶものではない。ERC-721 の範囲では、所有者には、メタデータや対象データを処分する権利はない。

また、メタデータや対象データが一意であるかもそもそも定義されない。多くの場合、メタデータや対象データを示すためには URL が使われ、URL が示すリソースはそれを保存しているサーバの都合で置き換えられ得るからである。この問題の解決のために、分散ファイルストレージである IPFS[Benet, 2014] がよく使われている。IPFS における URL はリソースのダイジェストを含むからである（[Wood, 2014] で提案されている通りのことが実現されている）。

8：ERC（Ethereum Request for Comments）は Ethereum における標準を記述した文書のシリーズである。721 は提案番号を示す。

3．2　ガバナンストークンと DAO

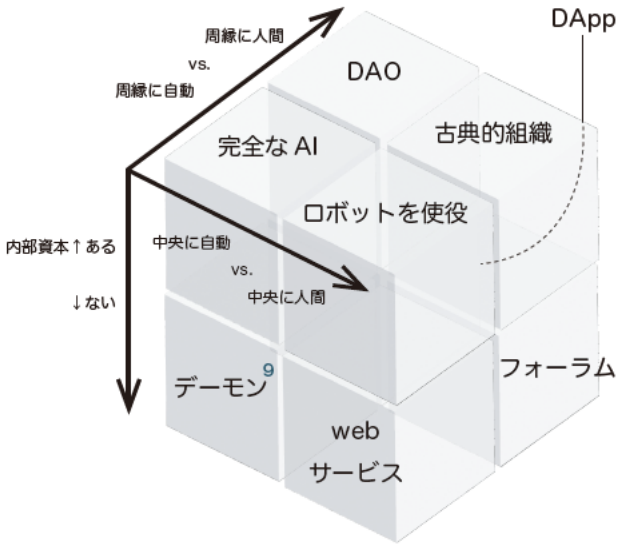
極端な話、事業をプログラムコードとして記述し、ブロックチェーンなどの自己主権的で検閲に強い台帳に書き込み、自動的に実行してその事業をスタートさせることができる。これは、これまで事業を支えてきた金融を、自動システムにより置き換えることを意味し得る。この概念は DAO（Decentralized Autonomous Organization; 分散型自律組織）と呼ぶことができる。

少なくとも、DeFi の世界では、いわゆるガバナンストークンの保有者が投票によってスマートコントラクトの更新やその他の重要な実行を決定するという、中央

機関に依存しない組織運営形態が模索されている。この概念は、上記のような一般化されたものではないが、現在では DAO として一般的に受け入れられている [Buterin, 2013]。

後者の意味での DAO は、株式会社における株式所有のガバナンスをブロックチェーン上に置いたに過ぎないと言っても過言ではない。また、スマートコントラクトは自発的に実行することができず、ブロックチェーンの外部のデジタル署名できる実体がメッセージにより呼び出す必要があるため、投票によってスマートコントラクトを実行する仕組みの有効性には疑問がある。現状では、可決後に管理者が呼び出すか（管理者は呼び出すかどうかを選択でき、DAO の実質的な支配者になる）、可決した提案を誰でも実行できるようにする（悪意のある提案が可決した場合の保護が弱い）という選択肢になる。後者を採用した場合の事故が実際に確認されている [Omniscia, 2022]。また、この事例は、投票者が提案を正しく判断できるという仮定に疑問を投げかけている。

図３　V. Buterin による整理の立体化



資料：[Buterin, 2014] の記述に従い筆者作成

実は Buterin は、ブログ記事 [Buterin, 2014] にて、DAO 等の用語の整理を早期に試みていた。図 3 は、その整理に従い、記事では 2 次元に展開されている分類を（Buterin 本人が本来キューブだと述べているため）立体として表現したものである。このキューブは「内部資本あり vs. 内部資本なし」「中央に自動システム vs. 中央に人間」「周縁に自動システム vs. 周縁に人間」の 3 軸による分類を表している。

この整理によれば、DAO は、中央に自動システムがあり、自動システムだけでは賄えない労働に周縁の人間が従事するものであり、人間を駆動するために内部に資本を蓄えているものだと理解できる。この理解であれば、Bitcoin や Ethereum も DAO の一種だと整理できる。また、中央は自動システムだが投票により意思決定する、現在話題になっている DAO は、[Buterin, 2014] では組織自体が自律的に意思決定しないため単に DO（分散型組織）と呼ばれる。

Buterin が、資本は人間を動かすためのものだと言い切っているのは新鮮である。しかし、自動システムは資本による動機付けを必要としないのだから、完全

9：コンピュータのオペレーティングシステムにおいて、主にバックグラウンドで動作し雑用をこなすプロセス（処理）。別名は「サービス」。

な AI は資本を必要としないし、ロボットを使役する場合も資本は不要なはずである[10]。このキューブには整合性上の問題がある。

4．web3 の意味と課題

4．1　web3 への批判的見方

先に、web3 の概念は以下の 2 つの要素から成ると述べた。

1．情報管理の分散化

2．あらゆるものの金融トークン化

それぞれに批判がある。第 1 の要素については、Web3 は分散型だと言われながら、ブロックチェーンへのアクセスを提供する特定のインフラ事業者や、特定の NFT マーケットプレイスなどが各々の市場で支配的である現実への批判がある [Marlinspike, 2022]。また、第 2 の要素については、[株式会社クニエ , 2022] 等の研究調査が明らかにしているように、投機目的でガバナンストークンを保持しているユーザが多く、実際に投票に参加する人口が少ないため、DAO における投票は一般に定足数が小さく設定されており、少数の有力者によって意思決定が行われがちだという指摘がある。

しかし、あらゆるものを金融トークン化することの問題は、それに留まらない。

4．2　web3 は解決か、問題か

あらゆるものを金融トークン化するという web3 の考え方は、すべてを金融で解決できるとする意思の表れとも言える。

例えば、オープンソースソフトウェア（OSS）開発プロジェクトへの web3 の応用 [Sverdlik, 2021] が取り沙汰されている。私たちの社会の情報空間は、すでに技術インフラの多くの部分を OSS に頼っている。すなわち、ボランティアで働くプログラマにより社会が支えられているのであり、それを心許なく思ったり、危険視する考え方がある。実際、筆者が話をした web3 関係者は、OSS に従事するプログラマに金融トークンで報いることが解決だと語った。

しかし、筆者はそれは解決ではなく、新たな問題を引き起こすと考える。例えば OSS 開発プロジェクトを DAO 化するならば、そのプロジェクトは近代的な意味で特定の集団により所有されることになる。それは、ソフトウェアはフリーであるべきだという OSS の源流となる概念と対立するし、何よりも、投票で意思決定するという現状の DAO の方法に従うならば、技術的な優位性によって技術が選択されるという保証ができなくなる。また、人類共通の文化資産かつ社会基盤としての OSS（の開発プロジェクト）が、誰かの判断で勝手に処分されることにも成りかねない。それは返って心許なく、危険なことではないだろうか。

5．おわりに

貨幣を融通する意味は、人を動機づけ動かすことにある。それが資本の意味だと、筆者は [Buterin, 2014] から改めて学んだ。しかし、だとすれば金融資本だけが資本ではない。

所詮、金融資本による動機付けは、貨幣という移ろいやすい媒体による外的動機付けに過ぎない。簡単には損なわれない、社会関係資本による動機付けの方が強力な場合もあるだろう。暗号資産を内部に溜め込む自動システムだけが DAO ではないということだ。

10：おそらく、中央の人間がロボットを購入したり維持するために資本が必要、あるいはロボットが資本だというロジックなのだろう。
だがそれは周縁に人間「も」いる組織である。また、金融資本以外も資本と捉えるのであれば、フォーラムの内部にも社会関係資本があるのだから、やはり定義と矛盾する。

金融ができることには限界がある。当たり前である。自らの限界を知りつつ、社会の中で役割を果たしてきたのが金融だろう。その意味で、web3 は金融ではない。しかし、web3 は金融の限界を明確な形で可視化することになるのかもしれない。

謝辞

この稿の執筆に当たり議論とインスピレーションをもたらした、早稲田大学 大学院経営管理研究科「ブロックチェーンと分散ファイナンス」ゼミ（2022 年度）の学生諸氏にこの場を借りてお礼を申し上げたい。

参考文献

- [Benet, 2014] Benet, J. (2014). IPFS - Content Addressed, Versioned, P2P File System. https://arxiv.org/abs/1407.3561.
- [Berners-Lee, 2009] Berners-Lee, T. (2009). Web 3.0 and Linked Data. https://www.w3.org/2009/Talks/0427- web30-tbl/.
- [Buterin, 2013] Buterin, V. (2013). A Next-Generation Smart Contract and Decentralized Application Plat- form. https://ethereum.org/en/whitepaper/.
- [Buterin, 2014] Buterin, V. (2014). DAOs, DACs, DAs and More: An Incomplete Terminology Guide. https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/.
- [Entriken et al., 2018] Entriken, W., Shirley, D., Evans, J., and Sachs, N. (2018). Non-Fungible Token Standard. https://github.com/ethereum/EIPs/blob/master/EIPS/eip-721.md.
- [Gidda, 2013] Gidda, M. (2013). Edward Snowden and the NSA files – timeline. https://www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline.
- [Iwamura et al., 2019] Iwamura, M., Kitamura, Y., Matsumoto, T., and Saito, K. (2019). Can We Stabilize the Price of a Cryptocurrency?: Understanding the Design of Bitcoin and Its Potential to Compete with Central Bank Money. Hitotsubashi Journal of Economics, 60(1).
- [Kharif, 2021] Kharif, O. (2021). What You Need to Know About Web3, Crypto’s Attempt to Reinvent the Internet. Bloomberg.
- [Marlinspike, 2022] Marlinspike, M. (2022). My first impressions of web3. https://moxie.org/2022/01/07/web3-first-impressions.html.
- [Nakamoto, 2008] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. http://bitcoin.org/bitcoin.pdf.
- [Omniscia, 2022] Omniscia (2022). Beanstalk Farms Post-Mortem Analysis. https://medium.com/@omniscia.io/beanstalk-farms-post-mortem-analysis-a0667ee0ca9d.
- [O’Reilly, 2005] O’Reilly, T. (2005). What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software. https://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html.
- [Saito and Yamada, 2016] Saito, K. and Yamada, H. (2016). What’s So Different about Blockchain? – Blockchain is a Probabilistic State Machine. In 2016 IEEE 36th International Conference on Distributed Computing Systems Workshops (ICDCSW), pages 168–175.

- [Sverdlik, 2021] Sverdlik, Y. (2021). Web3 Builders Hope to Fix Open Source, 'Broken' by Web 2.0. https://metal.equinix.com/blog/web3-and-open-source/.
- [Wood, 2014] Wood, G. (2014). Dapps: What Web 3.0 Looks Like. https://gavwood.com/dappsweb3.html.
- [株式会社クニエ , 2022] 株式会社クニエ（2022）. 分散型金融システムのトラストチェーンにおける技術リスクに関する研究 研究結果報告書 . https://www.fsa.go.jp/policy/bgin/ResearchPaper_qunie_ja.pdf