



Title	ブロックチェーンELSI（倫理的・法的・社会的課題）の予備的考察：概念の整理・ステークホルダー分析・主要なELSI論点の抽出
Author(s)	金, 信行; 森下, 翔
Citation	ELSI NOTE. 2025, 54, p. 1-31
Version Type	VoR
URL	https://doi.org/10.18910/100255
rights	
Note	

The University of Osaka Institutional Knowledge Archive : OUKA

<https://ir.library.osaka-u.ac.jp/>

The University of Osaka



ブロックチェーンELSI (倫理的・法的・社会的 課題) の予備的考察：

概念の整理・ステークホルダー分析・
主要なELSI論点の抽出

Authors

金 信行

北陸大学 経済経営学部 助教

大阪大学 社会技術共創研究センター 招へい教員 (2025年01月現在)

森下 翔

山梨県立大学 地域人材養成センター 特任助教

大阪大学 社会技術共創研究センター 招へい研究員 (2025年01月現在)

※本ノートの作成は、大阪大学社会技術共創研究センター（ELSI センター）と株式会社メルカリとの共同研究の一環として行ったものである。

目次

1. はじめに	3
2. ブロックチェーンに関連する概念.....	4
2.1. 暗号資産（仮想通貨）	5
2.2. スマートコントラクト.....	7
2.3. NFT.....	8
2.4. DAO	10
2.5. WEB3.....	10
3. ブロックチェーンのステークホルダー.....	12
3.1. マイナー	12
3.2. 開発者.....	14
3.3. 取引所.....	16
3.4. 投資家／起業家	17
4. ブロックチェーンの主な ELSI 論点.....	19
4.1. プライバシー	20
4.2. データの正確性	21
4.3. データの共有財産化.....	21
4.4. アクセス可能性	22
4.5. 開発者の中立性	23
5. おわりに	23
謝辞.....	25
用語集	25
参考文献.....	28

1. はじめに

ブロックチェーンは新たな社会インフラとして大きな注目を集めている先端情報技術である。ブロックチェーンはビットコインを代表例とした暗号資産の基幹技術として脚光を浴び、不動産登記／公文書管理／組織運営／文化コンテンツ売買／金融サービス／科学研究活動といった多様な領域でのユースケースや社会実装構想が発表されている。また日本国内の政策動向でもブロックチェーンの社会実装は重点分野として扱われている。デジタル庁が2022年9月にブロックチェーンを基軸としたWeb3に係る法改正や環境整備を目的として「Web3.0研究会」を発足し、また岸田政権の「新しい資本主義のグランドデザイン及び実行計画 2024年改訂版」ではDX（デジタルトランスフォーメーション）推進の一環としてWeb3の環境整備が重要項目として挙げられている。このように社会の諸領域での幅広い実装可能性が模索され、社会生活のあり方へ大きな影響を及ぼすことが見込まれる先端科学技術については、円滑な社会実装を実現するためにELSI（倫理的・法的・社会的課題）の検討そしてこれに基づくRRI（責任ある研究とイノベーション）の導入が必要とされる。

本稿は今後ブロックチェーンELSIの検討をより本格的に進めるための予備的考察である。本稿では文献調査に依拠して、ブロックチェーンの社会実装に係る諸概念そして社会実装事例に関わるステークホルダーを整理し、ブロックチェーンELSIを考察する上で重要となりうる論点を試論的に提示する。ブロックチェーンの社会実装においては、特定の管理者や組織に依存しない形でネットワークに参加するノードが分散的に管理を行う分散性が特徴として挙げられ、特定のステークホルダーへの信頼を不要とするシステムが構想されている。しかし、とりわけブロックチェーンを活用した社会実装事例やユースケースを観察すると、暗号資産市場の成立によって付随的に発生した規模を拡大した特定のステークホルダーが社会実装事例の運用に大きな影響を及ぼしており、ステークホルダーの利害関心によって権力の不均衡が起きているということがわかる（cf. レードンヴィルタ 2024: 178-212）。本稿では、あたかもその技術仕様において人間が介在しないかのように語られるブロックチェーンが、社会実装事例の運用と維持においては人間の関与に大きく依存していることを本稿に通底する視点として置きつつ、これからブロックチェーンELSIを本格的に検討する上で有用となりうる情報の整理を行う。

本稿は以下の構成から成り立っている。まず第2節では、暗号資産／スマートコントラクト／NFT／DAO／Web3を対象として、ブロックチェーンの社会実装に係る概念を概観しその見取り図を提示する。第3節では、暗号資産を中心としたブロックチェーンの社会実装事例におけるステークホルダーの動向を観察した社会学／文化人類学的研究を基に、ブロックチェーンの社会実装事例の開発と運用に関わる重要なステークホルダーとしてマイナー／開発者／取引所／投資家を取りあげ、これらの動向や利害関心について論じていく。第4節では、ブロックチェーンELSIを技術のミクロレベル／応用のメゾレベル／制度や社会への影響のマクロレベルで包括的に論じ

たレビュー論文に依拠して、ブロックチェーンの技術へ組み込むべきアジェンダを論じたマイクロレベルの論点であるプライバシー／データの正確性／データの共有財産化／アクセス可能性／開発者の中立性を、ブロックチェーン ELSI を検討する上で重要となりうる論点として提示する。第5節「おわりに」では本稿で得られた知見を振り返る。

2. ブロックチェーンに関連する概念

ブロックチェーンは記録されるデータそれ自体とブロックチェーンへの記録に関わる情報をまとめたブロックが数珠つなぎ状に接続されてチェーンを形成しているものであり、端的に言えばデータベースである¹（岡嶋 2022:82）。ブロックチェーンは日本語だと「分散型台帳技術」と紹介される。台帳とは売買や事務記録をまとめた帳簿であり、こうした台帳として会計帳簿／住民基本台帳／登記簿など様々な重要記録が挙げられる。これらの台帳は通常企業あるいは政府や地方自治体など組織が一元的に管理をしているが、ブロックチェーンでは特定の管理者を設けることなく、台帳としての記録のすべてまたは一部をネットワーク参加者全員が共有している。ブロックチェーンでは誰が、いつ、どんな情報を台帳に加えたかに関する情報が公開そして共有されるため記録情報の不正や改ざんが困難になり、台帳の保存と管理を分散的に行うことができる。本節ではブロックチェーン技術によって実現され、社会に影響を及ぼしている新しい概念をとりあげていく。具体的にとりあげる対象は暗号資産／スマートコントラクト／NFT／DAO／Web3であり、概念間の関係を整理した概念図は以下の形でまとめられる（図1）。

¹ <https://coincheck.com/ja/article/320>

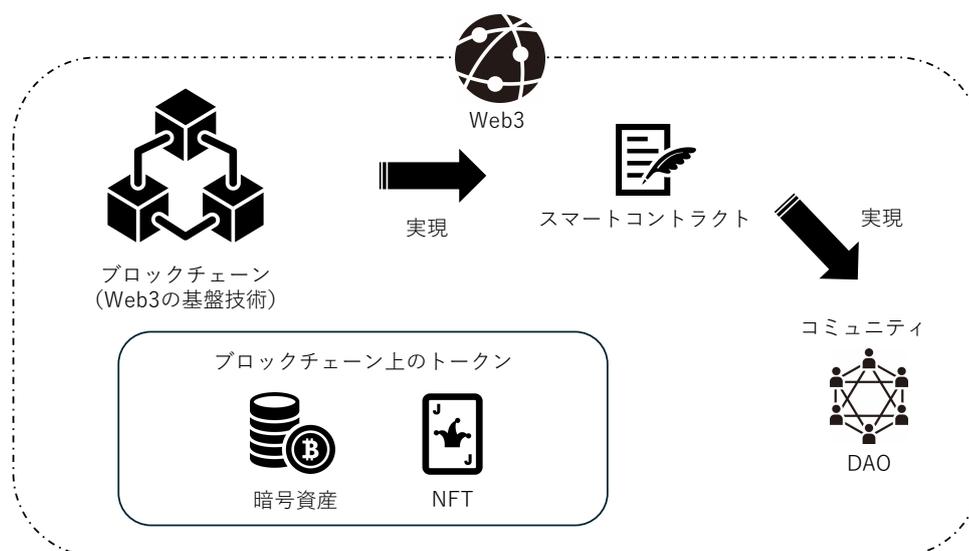


図1 暗号資産／スマートコントラクト／NFT／DAO／Web3 の関係を示す概念

2.1. 暗号資産（仮想通貨）

暗号資産（仮想通貨）はブロックチェーンを基盤として送金記録を分散的に管理する財産的価値（トークン）である（cf. 岡田 2018: 79-96）。「資金決済に関する法律」（資金決済法）によれば、「インターネット上でやりとりできる財産的価値」である暗号資産は以下の3つの性質を備える²。すなわち、①不特定多数に対する代金の支払い等へ活用することができ、かつ法定通貨と相互に交換することができる、②電子的に記録と移転を行うことができる、③法定通貨あるいは法定通貨建て資産ではないことである。これらの性質を踏まえると、暗号資産は日本円や米ドルといった法定通貨そして Suica や PayPay のような電子マネーとは異なる存在である。ここでは暗号資産の代表例であるビットコインを念頭に、暗号資産を支える重要な技術や仕組みについて確認していく³。

まずビットコインを構成する情報技術として P2P という通信技術がある。P2P とは複数の対等な関係（peer）にあるコンピュータ間で通信を行うアーキテクチャを指す。この方式では、サ

² <https://www.boj.or.jp/about/education/oshiete/money/c27.htm>

³ <https://coincheck.com/ja/article/320>

サーバー／クライアント方式とは異なり、1つのコンピュータに接続が集中することなく、分散的なネットワークが実現される。ビットコインでは送金者のウォレットアドレス／暗号資産の送金量／受領者のウォレットアドレスといった支払い記録を含むトランザクションが台帳（ブロックチェーン）へと記録され、この台帳をビットコインの P2P ネットワークに参加するノードが分散的に管理する形となっている。

そしてビットコインではそのセキュリティを高めるために、公開鍵と秘密鍵のペアを用いた公開鍵暗号に基づくデジタル署名やハッシュ関数といった、各種暗号技術が活用されている。ビットコインを送金するには、送金記録のトランザクションを作成し、秘密鍵によるデジタル署名を付してビットコインの P2P ネットワークに送信する。ノードはトランザクションのデジタル署名を通じて、トランザクションの有効性を検証することができる。

有効なトランザクションは、ブロックと呼ばれる単位のデータにまとめられ、台帳に記録される。ノード同士が対等な関係にある P2P ネットワークで各ノードが管理する台帳を同期するには、コンセンサス・プロトコルと呼ばれるノード間で合意を形成する手順が必要となる。

ビットコインにおいて用いられるコンセンサス・プロトコルであるナカモト・コンセンサスは、PoW（プルーフ・オブ・ワーク）というブロック生成のメカニズム、そしてチェーンが分岐した場合により長く計算量が多いチェーンをブロックチェーンの正しい記録として同期する最長チェーンルール（Longest-chain rule）に基づいている。

ビットコインでは、ブロックの追加作業に参加するノード（マイナー）が、互いに競い合う形で暗号学的な計算問題を解く（マイニング）。最初に計算に成功したマイナーによって作成されたブロックが他のノードに受け入れられ、台帳に追加される。ブロックを作成したマイナーにはマイニングの報酬として一定量のビットコインが与えられる。台帳にブロックが追加されると、マイナーは次のブロックを作成するための計算を開始する。

ブロックは直前に台帳へ追加されたブロックのダイジェストとなる値（ハッシュ値）を含んでいる。台帳は、あるブロックには直前のブロックのハッシュ値を含むという数珠つなぎ状の関係のブロックで構成される（このようにブロックがチェーン状に連なるようなデータ構造であることからブロックチェーンと呼ばれる）。完成したブロックが P2P ネットワークを伝播する過程で、もしも同一の直前のブロックに対して、より計算量が大きい問題を解くことに成功したブロックや、すでに後続のブロックまで追加されているブロックが存在することがわかった場合、最長チェーンルールに従ってブロックは置き換えられる。

仮に悪意をもったノードがすでに台帳に取り込まれたブロックに改ざんを加えると、ブロックのハッシュ値が変わってしまう。あるブロックには直前のブロックのハッシュ値を含むという、

台帳を構成するブロック間の関係が壊れてしまうため、改ざんを加えたブロックの後に続くブロックの情報もすべて改ざんする必要が連鎖的に生じる。しかし、ブロックを作り直すには再び計算問題を解く必要がある。さらに、改ざんしたブロックで他のノードが管理している台帳のブロックを置き換えるには、改ざんしたブロック以降の既存のブロックすべてを最長チェーンルールによって置き換えられるだけの計算量の計算問題を解いてブロックを再作成しなければならない。それには、ビットコインの P2P ネットワークに参加している世界中の多くのコンピュータが競い合いながら次のブロックを作成するために投下している計算能力よりも大きな計算能力が必要となる。つまり、ブロックチェーンの不正や改ざんには一つのユーザーでは担うことができない膨大な計算能力が必要になるのである。このように暗号資産は様々な技術や仕組みを活用することで、誰もが自由に参加することができる P2P ネットワークによって台帳情報を不特定多数のノードが共有しながらも、送金記録の改ざんが極めて困難なシステムの上に流通する財となっている。

2.2. スマートコントラクト

スマートコントラクトはブロックチェーンを活用し、人間の介入を最小限に抑えることを目的とした、契約を自動で実行する仕組みである (cf. Szabo 1994)。ブロックチェーンを暗号資産という形で社会実装化したのはビットコインであったが、ブロックチェーンの用途をスマートコントラクトなど暗号資産に限らない形で大幅に拡大したのはイーサリアムである⁴。暗号資産はあくまでその送金に限られたものであったが、スマートコントラクトでは暗号資産に限られない財産情報、そして取引資産の保有者／保有個数／所有情報の移転状況といった非財産的な情報をも、ブロックチェーンに記録することができる。例えば、「買主と売手が一定の条件で合意した場合、買主は対価となる暗号資産を支払い、売主は売買の対象となる暗号資産を移転させる」という契約があった時、スマートコントラクトによってこの内容をブロックチェーンに記録し自動的に実行することができる (cf. 清水／荒巻 2023: 3)。スマートコントラクトでは契約を事前に定義しておけば、トランザクション／所有情報の移行／移転対象の受取を自動化することができる。

イーサリアムにおいてスマートコントラクトを使用する場合、ブロックチェーンには契約の内

⁴ もっとも、ブロックチェーンを暗号資産以外の用途へと応用する動きはイーサリアム登場以前にも存在した (ブテリン [2014] 2023: 432)。一例として、金融資産／コモディティ／固定資産など取引対象となる資産の情報を、ビットコイン・ブロックチェーンのトランザクションデータに追記するカラードコインの取り組みがある (<https://github.com/Colored-Coins/Colored-Coins-Protocol-Specification>)。

容も記録される（清水／荒巻 2023: 7）。前項の暗号資産では、ビットコインのブロックチェーンに書き込まれるのは送金者のウォレットアドレス／暗号資産の送金量／受領者のウォレットアドレスから成る送金記録であった。イーサリアムのスマートコントラクトでは、イーサリアムの暗号資産であるイーサの送金記録に加え、執行したい契約の内容をプログラミング言語で記述したコードをトランザクションに含めることができる⁵。

イーサリアムでスマートコントラクトを実行する際、ビットコインのケースと同様に手数料が発生する（清水／荒巻 2023: 38-39）。ビットコインでは送金記録をブロックに追加するためのマイニングに対して手数料が設定できるが、イーサリアムで送金やスマートコントラクトの実行を行うトランザクションには Gas 代と呼ばれる手数料が必要となる。イーサリアムではブロック生成のやり方として、イーサをステーキング⁶しているバリデーターと呼ばれるノードが確率的に新規ブロックの生成や検証の作業を担う PoS（プルーフ・オブ・ステーク）を採用しており、バリデーターに対してこの手数料が支払われることになる。

スマートコントラクトはブロックチェーンの社会実装を財産的価値の移転にとどまらず、デジタル資産の移転契約の執行という汎用性の高い用途へと広げた事例である。

2.3. NFT

NFT（Non-Fungible Token：非代替性トークン）とは、ブロックチェーンによってデジタルコンテンツの所有情報の移転を記録できる、「代替不可能（Non-Fungible）な」トークンを指す。ビットコインやイーサは通貨としての用途を想定した「代替可能な」トークンである。通常の通貨であれば例えばくたびれた 1 万円札を新札の 1 万円に変えても、1 万円札を 1 千円札 10 枚に両替しても価値の変動はなく、同じ価値をもつという意味で代替可能（Fungible）である。一方で、プロ野球選手がサインした野球ボール、芸人がサインした T シャツ、著名画家が描いたアート作品は、贋作やコピー品には代替できない固有の価値をもつだろう。そのような代替不可能な価値を表現するために、画像／動画／GIF／音声／3D モデル／電子化した書籍や文章といった、それぞれのデジタルデータに固有のトークンを発行する（「ミントする」）ことで、デジタ

⁵ ビットコインのシステムと同様に、スマートコントラクト作成者はこのトランザクションをイーサリアムの P2P ネットワークに送信する。

⁶ 合意メカニズムに誠実に参加することの担保としてイーサをデポジットすること。不適切な振る舞いをした場合はペナルティとしてデポジットしたイーサがバーン（イーサリアムネットワークから削除されること）される。

ルデータの作品情報やトークンの所有者の移転をブロックチェーンに記録する技術が NFT である（フォートノウ／テリー 2022: 33, 39）。

NFT の発行ではイーサリアムのスマートコントラクト規格を採用したものが多く、前項で述べたように、イーサリアムではトランザクションにイーサの送金記録と契約情報のプログラミングコードを組み込むことができる。NFT ではスマートコントラクトを使って、名称／NFT と紐づくメインコンテンツ／コンテンツのプレビュー／コンテンツの説明／任意のウォレットに対するロイヤリティ／NFT の供給量を記述することができる（フォートノウ／テリー 2022: 59）。この仕様によって、ひとつひとつの NFT を識別し、アドレス間での「移転」を行うことが可能になり、個別のデジタルコンテンツの「保有」などを表現することができるのである⁷。メインコンテンツについては、URL のようなメインコンテンツのデータの保存場所に関するメタデータが記録される場合もあれば、メインコンテンツのデータそのものを Data URI⁸ の形で直接記録する形式も採られる。またロイヤリティは NFT の画期的な点として大きな期待が寄せられたものである。ロイヤリティの仕様として最も普及している形式は NFT の売買が成立する際に一定のパーセンテージの額を任意のウォレットアドレスへ支払うよう表明するものであり、NFT の所有者移転が生じる度にこの表明に従い支払いが行われればトークン作成者は継続的に利益を得ることができる⁹。このように NFT は主にイーサリアムのスマートコントラクトを活用して、デジタルコンテンツを表したトークンを売買の対象としつつトークン作成者への一定の利益を確保し、これに関わる台帳記録をブロックチェーンで公開して分散的に管理する試みなのである¹⁰。

⁷ この NFT の特徴によって、アナログ（オリジナル）とデジタル（コピー）の従来的な対立は無効化され、デジタルデータの人工的な希少性に基づいて創作物を扱う新たな巨大市場が形成された（シュタルダー 2022: 44）。

⁸ Data URI スキームとは、通常は別ファイルとして保管・参照されるデータを、URI を用いてテキストに直接埋め込むスキーム。画像のようなバイナリデータであってもエンコードすることでテキストとして表現することができる。

⁹ ロイヤリティの支払いを NFT コントラクトに組み込むことで強制する仕様もあるものの、現実のユースケースではあまり普及していない。

¹⁰ ブロックチェーンの使用用途を幅広く拡張したものとしてイーサリアムは高い知名度を誇るが、ブロックチェーンに基づいたデジタル資産の取引記録の管理については例えば Rare Pepe のような事例がある（http://rarepepedirectory.com/?page_id=25）。インターネットミームとして流行したカエルのイラストである Pepe のなかで、とりわけあまり出回っていない画像が Rare Pepe として名付けられトレーディングカードのように売買されるようになった。Rare Pepe では、Rare Pepe が一定の発行量を定めたトークン化によってブロックチェーンに登録可能なデジタル資産として扱われ、発行量が多い Rare Pepe である Pepe Cash を通貨とした独自の経済圏の構築が構想されていた（https://spotlight.soy/detail?article_id=ut4m7c9nk）。

2.4. DAO

DAO (Decentralized Autonomous Organization: 分散型自律組織) とは、パブリック型ブロックチェーンのスマートコントラクトに基づくルールの記録そしてその自動執行を介して、メンバーによる分散的な管理と自律的なガバナンスがなされる組織構想である (cf. Hassan and De Filippi 2021: 2)。DAO は、管理者をトップとしたヒエラルキー構造によって中央集権的な管理がなされる従来の組織と対比される (福岡/本柳 2023: 5)。中央集権的な組織が持つとされる欠点として、組織構造の変更が経営者または高位の階層に属する組織メンバーの提案で実行され、組織の意思決定や活動は限られたメンバーしか確認することができないなど、透明性の低い組織運営が指摘される。DAO は、組織メンバーによる意思決定への直接的な関与と組織内活動の高い透明性を備えた分散型の組織構造によって、こうした中央集権的な組織が持つ欠点を克服することを志向する。

DAO は類似的な概念やユースケースが極めて多様に展開されておりまだ形成途上の概念であるが、以下の特徴を共通した内容として挙げている例がある (Hassan and De Filippi 2021: 4-5)。
①DAO は人々によるインターネットを通じた協調とガバナンスを可能にするものであり、DAO における組織とは共通目標の達成に向けて行為を行う複数の人々から成る実体だと考えられる。
②DAO のソースコードはスマートコントラクトの機能を備えたパブリック型ブロックチェーンへ記録される。
③DAO のスマートコントラクトでは構成メンバーの行為を規定するルールが定められる。
④DAO のルールはスマートコントラクトで定められているため、当事者の意思とは独立する形で自動的に実行される。
⑤DAO のガバナンスは特定のステークホルダーや組織による中央集権的な管理から独立したものである。
⑥DAO はブロックチェーンを活用することで、透明性/暗号化セキュリティ/分散性といったブロックチェーンの特性を継承している。このように DAO はスマートコントラクトを活用することで分散性と透明性の高い組織運営を志向する発展途上の概念だといえる。

2.5. Web3

Web3はブロックチェーンを基盤として中央集権型ではなく分散型で成立するインターネットのあり方である (城田 2023: 14-16)。ブロックチェーンを基盤とした Web3 のアイデアはイーサリアム共同創設者である Gavin Wood によって広められている¹¹。Wood は Web3 がトラス

¹¹ 名称としては類似しているものの意味内容が異なる概念として、World Wide Web の考案者である Tim Berners-Lee の提唱した Web3.0 (セマンティック・ウェブ) がある。Berners-Lee はブロックチェーンを用いた Web3 の実現という

トレスなモデルに基づくことを強調した。これはクラウドやプラットフォームを管理してビッグデータ分析から莫大な利益を手に入れているビッグテックへ依存することなく、ブロックチェーンのデータとアルゴリズムを誰もが確認し検証できるため特定の中央集権的な組織や機関を信頼する必要がないということである。Web3 の概念に基づく代表的な社会実装事例としては、ブロックチェーンとスマートコントラクトによって金融サービスを自動化する DeFi (Decentralized Finance: 分散型金融)、ゲームのプレイを通じて手に入れたトークン等のゲーム内アイテムを現金化することができる GameFi、運営企業を仲介せずにイーサリアムブロックチェーンで稼働する分散型人材ネットワークの Braintrust、P2P とブロックチェーンを活用して IoT デバイスのための無線ネットワークを構築する分散型ネットワーク構築プロジェクトの Helium、現代の学術業界が研究開発資金の調達方法や知識の共有方法において抱える課題をブロックチェーンと関連技術の活用によって解決することを試みる DeSci (Decentralized Science: 分散型科学) などが挙げられる (cf. 城田 2023: 63-136)。

Web3 は既存のインターネットのあり方である Web1.0 そして Web2.0 と対比する形で示される概念である (城田 2023: 16-21)。Web1.0 はインターネットが社会へと普及した 1990 年頃から SNS が社会に広く定着する 2005 年前後までのタイムスパンに該当した区分である。Web1.0 の時代は、動的なウェブ環境を構築するための技術的基盤が相対的に乏しく、その後比べて静的なウェブサイトによる一方向的な情報発信が行われていた時代である。Web2.0 は 2005 前後年以降の区分であり SNS やプラットフォームの普及を焦点としている。Web2.0 において一般のインターネットユーザーは、Facebook/X (Twitter) /Instagram/YouTube などの SNS を通じて、コンテンツをただ享受するだけでなく発信できるようになった。ただし Web2.0 で主役となるのはこうした消費者でありクリエイターでもある一般ユーザーではなく、SNS やプラットフォームを作り管理する世界的な大手 IT 企業であるビッグテックだ。ビッグテックは一般ユーザーが SNS やプラットフォームを使った履歴データへのアクセスを独占し、ユーザーに関するデータ分析をサービス改善に活用することでユーザーを囲い込み、サービス拡大で巨万の富を得た。ブロックチェーンに支えられた新しいインターネットのあり方である Web3 では、コンテンツを読みそして生み出すユーザーのデータを排他的に独占する主体はなく、一般ユーザーはこうしたデータを共有財産とすることができるとみられている。また Web3 のトークンエコノミーにおいては、サービスに貢献した利用者トークンを配布することでユーザーへ利益を還元する仕組みが構想されている (cf. 城田 2023: 138-139)。ブロックチェーンに基づく Web3 のインターネ

理念に懐疑的な見解を述べており、みずからはブロックチェーンを用いない Solid という独自のウェブ分散化プロジェクトを運用している (<https://solidproject.org/>)。

ットサービスでは中央集権的な仲介者の排除によって、共有台帳としてのブロックチェーンに記録されたデータは誰もが活用できる公開データとなりうる。

3. ブロックチェーンのステークホルダー

前節ではブロックチェーンに関連する概念を整理したが、これらの社会実装においては開発と運用を担うステークホルダーが大きな役割を果たしている。ブロックチェーンの技術仕様では想定されていないものを含んだこれらのステークホルダーは、社会実装事例の開発と運用のインフラを維持し、暗号資産コミュニティにおいて権力の中心点として機能し、社会実装事例のプロジェクトの成否を大きく左右する。本節ではこうしたステークホルダーとしてマイナー／開発者／取引所／投資家に焦点を当て、ブロックチェーンの社会実装事例をとりあげた社会学／文化人類学的研究を基に、社会実装事例の開発と運用におけるステークホルダーの動向や役割を整理する。

3.1. マイナー

本稿でとりあげる第一のステークホルダーはマイナーである。2.1 で述べたように、マイナーはビットコインのような PoW 方式をとる暗号資産において、ブロックチェーンへ新たなブロックを追加・検証するプロセスに参加し、競争に勝利することでマイニング報酬として一定量の暗号資産を手に入れる存在である。すなわちマイナーには二つの役割がある。それはブロックチェーンの不正や改ざんの有無を検証する極めて重要な作業を担うと同時に、競争をつうじて暗号資産を新しく獲得することを試みる存在なのである。特に後者の競争はマイニング使用機器や参加形態の面でマイナーの変容を促した。

Hayes の研究によればビットコインが社会に定着して以降、マイニングに用いられる機器は CPU (Central Processing Unit : 中央演算処理装置) → GPU (Graphics Processing Unit : 画像処理装置) → ASIC (Application Specific Integrated Circuit : 特定用途向け集積回路) へと、そしてマイニング主体は個人 → マイニングプール → マイニング専門業者へと変化していった (Hayes 2023: 5-7)。ビットコインのマイニングが開始した 2009 年から 2010 年中頃にかけては、投資ではなく脱中央集権的な金融システムの維持に関心をもつ個人のマイナーが PC の CPU によってマイニングを行い、2010 年 11 月には世界初のマイニングプールである Slush Pool が形成される。しかし、2010 年後半にはマイニングの計算作業をより効率的に行う機器として GPU が使われるようになり、マイニングに参加するノードがもつ計算能力の向上に伴いマイニングの難易度も急速に上昇したため、個人の CPU でマイニングに成功することは難しくなった。2010 年後半から 2013 年にかけては、マイニングによって利益を得ることを目的とした投資家や起業家が参入してマイニング機器へ多額の投資を行い、またマイニングプール間の競争でマイニングプー

ルの統合が進んだことで、マイニングの難易度はさらに上昇した。2013年にマイニングのハッシュ関数の計算に特化したASICであるBlock Erupterがリリースされると、2013年以降から現在に至るまで、ASICをはじめとしたマイニングのインフラへの設備投資とマイニング機器の利用に係る膨大な電気使用料を賄うことができるマイニング専門業者が、マイニングにおいて支配的な地位を占めるようになる¹²。

こうしたマイニング専門業者は大量のマイニング機器を安価な電気料金で運用する大規模なマイニング施設を世界各地で建設している。中央アジアのジョージア共和国におけるBitfury Group社のマイニング事業を分析したWyethらによれば、Bitfury Group社は電気使用料/人件費/土地代/人的ネットワークの観点からジョージアでのマイニング事業を開始そして拡大し、Bitfury Group社とジョージアの規制当局および政府関係者との人的ネットワークはBitfury Group社と国家の結びつきを極めて強固なものとした(Wyeth et al. 2023: 824-827)。ジョージア政府はBitfury Group社がジョージアの首都トビリシ西部に構えるマイニング施設の土地の大部分を、所得税/固定資産税/付加価値税が非課税となるFIZ(自由工業地区)に指定した。また暗号資産取引に関して海外投資家を優遇する法律が制定されたことで、暗号資産の売却益やジョージアから海外へのハッシュパワーの販売益については付加価値税の対象外となった。ジョージアの投資関係者/法律関係者/元規制当局関係者は、Bitfury Group社のマイニング施設をジョージアへ誘致するにあたってファンド投資や法整備など様々な支援を行い、彼らの多くはBitfury Group社に雇用され要職に就いている。例えばビットコイン取引において違法性が疑われる取引や取引主体を発見する捜査ツールである、Crystal Blockchainの提供を通じて世界各地の規制当局や法執行機関と協力するなど、Bitfury Group社はジョージアに限らず政府機関へのロビー活動や相互交流を促進することで、国家や規制当局と協力して自社に有利な規制状況を作り出している。

上述した研究からわかるように、とりわけマイニング専門業者のようなマイナーはマイニング施設を稼働してハッシュパワーの寡占状況を担っており、暗号資産の重要な意思決定において大きな影響力を有するステークホルダーである¹³。マイナーが暗号資産自体そして国家や暗号資産

¹² マイニングプールか専門業者かを問わず一部のマイナーが突出した計算能力を保有することは、検証を多数決に依存している暗号資産のネットワークに深刻な懸念をもたらす。一つのマイナーもしくはマイニンググループの計算能力がマイニングの計算能力全体の51%を超えると、不正や改ざんのあるトランザクションをブロックチェーンの記録として承認することが可能になってしまう。この問題は51%攻撃として知られている。

¹³ 一例として、ビットコインのコア開発者を務めたGavin Andresenが決済処理の効率化のためにビットコインのブロックサイズを大幅に拡大する提案を2015年に行った際に、ブロックサイズの拡大によってマイニングコストが増大し、またトランザクション承認の混雑状況によって得る手数料が低下することを危惧した大手のマイニング専門業者が反対したため、両者の間で深刻な対立が起きた(レードンヴィルタ 2024: 201-203)。

の規制においていかなる影響力を行使しているのかを調査することは、ブロックチェーン ELSI を考察する上で重要な作業となるだろう。

3.2. 開発者

本稿が注目する第二のステークホルダーは開発者である。開発者やエンジニアはブロックチェーンの基礎的な技術の発展や暗号資産を活用したサービス開発において基幹的な役割を果たす。ブロックチェーンの社会実装を志向するプロジェクトではユーザー間の相互交流を促進し、プロジェクト内容への意見やコミットメントを募るためのオンラインコミュニティが立ち上げられる。そして、開発者やエンジニアはその専門性からこうしたオンラインコミュニティのリーダーシップやマネジメントにおいて、中心的な役割を果たす集団に属して活動していく。

ビットコインの技術構想を発表した Satoshi Nakamoto やイーサリアムを考案した Vitalik Buterin といった先駆的な開発者の存在は、ブロックチェーンコミュニティや人々によってどのように受け止められているのだろうか。Humayun と Belk の研究によれば社会そしてブロックチェーンコミュニティにおける Nakamoto の神話化は複雑な様相を呈している (Humayun and Belk 2018: 24-30)。ビットコインの運営を Gavin Andresen へ引き渡した 2010 年以降表舞台に現れずその素性が明かされていない、Nakamoto の正体へと迫る試みは熱狂的に繰り返されてきた¹⁴。Humayun と Belk のインタビュー対象者であるビットコイン愛好家や企業関係者は、革新的な社会実装事例の構想とプロトコルを提示した天才的な人物として Nakamoto を称賛しつつ、Nakamoto の正体や素性を明かすことがブロックチェーンコミュニティへもたらしうる影響を懸念している。Nakamoto の正体が明かされれば、かつてのスノーデン事件や Nakamoto をめぐるこれまでの報道のように、暗号資産の革新性や利便性といった論点よりも Nakamoto のプライベートな生活や交友関係といったゴシップへと注目が集まる可能性がある。また、Nakamoto の経歴／人柄／価値観といったプライベートな情報の内容次第では、企業投資の中止や暗号資産市場の暴落のような形で、ビットコインあるいはブロックチェーンの社会的な評価や信頼が毀損されることもありうる。Nakamoto が革新的な技術を提起した正体不明でミステリアスな存在としてカリスマ的な人気を誇るように、ブロックチェーンの社会実装の新たな可能性を開く開発者は象

¹⁴ 例えば、2014 年には Newsweek 誌が Nakamoto の正体は日系米国人のエンジニアで Satoshi の出生名をもつ Dorian Nakamoto だと報じ、Dorian Nakamoto 自身は強く否定したにもかかわらず、Dorian Nakamoto に対するマスメディアの取材そして報道が加熱する事態が生じた (<https://wired.jp/2014/03/07/bitcoin-creator-satoshi-nakamoto-revealed-after-years-of-mystery/>)。

徹的な存在として大きな影響力を有している。

暗号資産である Electra の運営コミュニティを分析した Çalışkan の研究によれば、Electra コミュニティにおける権力の中心は運営における技術的なメンテナンスを担うコアチームにある (Çalışkan 2022a: 15-16; Çalışkan 2022b: 7-9)。Electra の Discord コミュニティでは取引所への上場やホワイトペーパーの作成といったコミュニティに関する重要な意思決定が、コアチームを中心として下される。Discord のチャットだけでなく毎週日曜日に専用チャンネルでコミュニティの意思決定に関するミーティングを行うコアチームは、Electra コミュニティの管理において非常に大きな力をもっている。コアチームは、Electra の取引に用いるウォレットのセキュリティ強化やアップデート、Electra の送金情報を記録するブロックチェーンのプログラミングコードにおけるバグの処理など、プロダクトに関わるあらゆる不具合へ対処する。またコミュニティ運営の面でも、こうした不具合に伴うコミュニティメンバーからのクレーム対応、コミュニティの規約や秩序に従わないメンバーに対するメンバーシップの制限など、Discord コミュニティを維持するワークも担っている。Electra 創設者とコアチームの対立が起きた際に、新たな暗号資産である Electra Protocol を発表し Electra のコミュニティを移行させたのも、このコアチームであった。

このようにブロックチェーンを実装したプロダクトやサービスにおいて、プロジェクト運営層に属する開発者はしばしば権力の中心点として機能していく。ブロックチェーンにおける理想としての分散性と現実に生じた中央集権制の歪みを覆い隠す開発者のレトリック戦略を明らかにした Vidan と Lehdonvirta の研究によれば、このようなレトリック戦略は①人間と装置の混同／②合理的なエージェントの仮定／③技術的な専門知識の強調／④問題を一時的なバグとして同定する置き換えである (Vidan and Lehdonvirta 2019: 54-55)。

まず①人間と装置の混同では、上述したような開発者と一般ユーザーの間にある権力の不均衡から成るブロックチェーンの世界が、同じ力をもつノードの集合体である P2P として描き直される。②合理的なエージェントの仮定では、例えばマイニングプールの形成によって、ブロックチェーンに参加する他のノードの計算能力を圧倒的に凌駕し単独でブロックチェーンの記録に不正や改ざんを加えられるような主体が現れた際、不正や改ざんを行うことは暗号資産の交換価値を損なうため、こうした主体がブロックチェーンに悪意ある不正や改ざんを働くことは非合理的であり従ってその実行は非現実的であると説明される。③技術的な専門知識の強調では、ブロックチェーンの社会実装プロジェクトの運営においてソフトウェアのメンテナンスやプログラミングコードのバグへの対処など不安定性が可視化されることで、情報工学の高度な専門性を備えた開発者こそが管理に適した存在として受け入れられる。④問題を一時的なバグとして等置する置き換えでは、ブロックチェーンのプログラミングコードには本来何も問題が無く、ブロックチェーンの社会実装事例の運用において生じている矛盾や問題はあくまで一時的に生じているバグな

のだという解釈が示される。

以上で概観した研究から、特定の管理者や組織を置かず各ノードが記録を管理する分散性がブロックチェーン最大の特色として喧伝されているが、ブロックチェーンの実際の運用においてはブロックチェーンの技術的内容に習熟した開発者とユーザーの間に権力の不均衡が生じていることがわかる。ブロックチェーン固有の文脈ではないものの、アルゴリズムの社会学的研究では行政機構におけるAIの利活用やビッグテックの巨大化を背景に、社会変革の旗手となる先端情報技術のアルゴリズムについて高度な専門知識を有した人材層が、「コーディング・エリート」という現代社会の支配階層として存立していることが指摘されている(Burrell and Fourcade 2021: 216-218)。ブロックチェーン ELSI を考える上では、プラットフォームを活用した実際の運用プロジェクトのなかで開発者コミュニティがいかなる役割を果たしているかを考察することも重要になるだろう。

3.3. 取引所

ブロックチェーンに関して本稿がとりあげる第三のステークホルダーは取引所である。取引所はブロックチェーンの技術仕様で構想されていたものではなく、暗号資産が社会実装された後に投機目的のユーザーが暗号資産市場へ参入するための窓口として作られた。数多くの顧客から資産を預かる取引所は一体どのような業務を行い、また運営されているのだろうか。取引所を調査した Çalişkan の研究によれば、取引所では六種類の経済的实践——市場交換／物々交換／贈与／銀行業務／仲裁／ソフトウェアとデータサービス——が行われている(Çalişkan 2022c: 5-7)。まず①市場交換について、これは取引所が一定のレートで顧客が送金した法定通貨と引き換えに暗号資産を販売することを指している。②物々交換について、顧客は自身の暗号資産と他の顧客がもつ異なる種類の暗号資産を物々交換することができる。取引所はこの物々交換に手数料を課し、また手数料の減額と引き換えに取引所独自の暗号資産の購入を提案するなど利益を得ている。そして③贈与については、取引所は独自の暗号資産を顧客へギフトとして配布することで取引所の利用と独自の暗号資産の活用にインセンティブを与えたり、新規顧客を誘致するキャンペーンとして少額の暗号資産を無料配布したりする。このようなインセンティブは「リワード」や「エアドロップ」として知られている。④銀行業務。取引所は顧客の資産管理と運用を行う。多くの取引所は顧客から預かった暗号資産をブロックチェーンに登録せずに取引所内の保有資産として取引所独自の会計システムで管理する。取引所は顧客の取引行為に応じて、スポット取引手数料／先物取引手数料／入金手数料／出金手数料といった多くの手数料を顧客に課す。取引所は顧客から預かった暗号資産を取引所自身が独自に行う取引に活用する場合もある。取引所は顧客の資産をもとに、他の顧客のレバレッジ取引に対して暗号資産の貸付を行い、借りた顧客から金利を得る。また、先に述べたように取引所は独自の暗号資産を発行するが、これは必ずしも

パブリック型ブロックチェーンを活用したものであるとは限らず、取引所の複式簿記帳簿で管理されていることもある。

⑤仲裁について、取引所は顧客間のトラブルを仲裁する機能を果たす。取引所の仲裁機能は多くの場合ユーザに加入が義務づけられる有料サービスであるが、しばしば顧客は取引所の仲裁内容に不服の申し立てができず、取引所との関係が悪化している顧客へのサービス提供を打ち切る手段としての恣意的な運用も行われる。暗号資産の価格が変動する時にこうした顧客間のトラブルが増え、取引所が顧客による暗号資産の取引停止を執行するが、顧客が取引所のトラブル対応や仲裁判断の是非を問えるかどうかは取引所の一存に委ねられておりほとんどのケースで受け付けられない。

⑥ソフトウェアとデータサービスについて、取引所は暗号資産取引に有用なソフトウェアやデータを有料で顧客に提供している。顧客は様々な種類の取引を組み合わせる暗号資産の運用を通じて大きな収益を得たいので、暗号資産の価格形成や変動を分析するためのソフトウェアやデータへ大きな関心を持っている。取引所はこうしたソフトウェア開発やデータ収集を注力して行い、ソフトウェアとデータへのアクセス権ならびにサポートサービスを販売もしくはサブスクリプションの形で顧客に提供する。

Çalışkanはこのように単なる商品の交換にとどまらないプラットフォームでの多様な経済実践を「堆積」(stack)として捉え、取引所において多様に展開されている経済実践の様態に対する入念な調査研究を基に規制を行う必要性を論じている(Çalışkan 2022c: 11)。規制を考える上では、まず取引所やプラットフォームにおいていかなる経済実践が生じているかを調査し可視化する必要があるだろう。

3.4. 投資家／起業家

本稿で最後にとりあげる第四のステークホルダーは投資家および起業家である。暗号資産というまったく新しい投資商品について投資家は一体どのような価格予測を行い取引へと参加するのだろうか。韓国の暗号資産投資家コミュニティを分析したLeeの研究によれば、韓国のビットコイン投資家は金融市場の相場分析として知られるファンダメンタルズ分析とテクニカル分析を暗号資産に応用して、ビットコインの値動きを予測し取引へと活用している(Lee 2022: 10-14)。ファンダメンタルズ分析は金融や経済に関するマクロな経済指標に基づき金融商品の本来的な価値を推定する手法であり、投資家は推定価格と現在の市場価格を比較して売買の判断を下す。またテクニカル分析は市場の価格チャートを観察して周期的なパターンや法則を発見する手法で、投資家はこれらのパターンや法則に則った予測で売買を判断する。韓国におけるビットコイン取引のオンラインコミュニティではテクニカル分析でビットコインの将来価格を予測する投稿が毎

日数多く投稿され、価格チャートの読みとり方を学ぶ勉強会がオンラインとオフラインを問わず頻繁に開催される。そもそもこうした分析手法は既存の金融商品を対象とした分析手法であり暗号資産の価格予測へ活用できる可能性は極めて不透明だが、こうしたことはビットコイン投資家の間で概ね共有されている。暗号資産の価格を予測する合理的な手法など何も存在しない中で、ビットコイン投資家は様々な出来事が連関して偶然的に生じる価格変動に意味や法則性を見出す、ある種のゲームへと没入したギャンブラーとして取引に参加している。

暗号資産や NFT への投資におけるこうしたギャンブラー的熱狂を、暗号資産を活用したサービスの開発者や管理者がコントロールすることは容易ではない。NBA の試合における選手のプレー動画を NFT 化したトレーディングカードゲームである NBA Top Shot のオンラインコミュニティを分析した Zaucha と Agur の研究によれば、Discord コミュニティにおいて NBA Top Shot のサービス提供者の期待とコミュニティユーザーの意図の間には著しい相違があった (Zaucha and Agur 2024: 2245-2248)。NBA Top Shot の運営に携わるサーバー管理者が NBA Top Shot に参加するユーザー像としていたのは、カードゲームの駆け引きを楽しむゲーマーや、選手のプレー動画を収集し他のファンとコレクションについて意見を交わすコレクターなどであった。しかし、Discord サーバーにおいてこうした期待に合致するユーザーは少数で、大多数は購入するカードパックやカード売却のタイミングについて投稿を重ねる投資家のユーザーであった。投資家のユーザーはポートフォリオ/ボラティリティ/リスクといった金融取引の用語に加え、「命懸けで持ちこたえる」という意味の HODL や「価値の急上昇」を意味する mooning といった俗語を自身の投稿の中で使い、NBA Top Shot を投資市場とのアナロジーで捉えていた。Discord サーバーの各チャンネルにおいてこうした投稿や、投資家のユーザーと投機的な関心を嫌厭するユーザーとの間で諍いが絶えなかったため、チャンネルと関係のない投稿を減らすためにコミュニティリーダーのチームへの質問を募る #help チャンネルを一時的にロックするなど、Discord サーバーのモデレーターはコミュニティへ介入せざるをえない事態が生じた。管理者はファンの交流促進を目的としたプラットフォームを構築したものの、投機や投資を目的としたユーザーの市場的な関心がプラットフォームを席卷したのである。

また投資あるいは投機的な関心はブロックチェーンを活用したプロジェクトやビジネスの成否を左右する。2017 年の ICO (Initial Coin Offering) バブル¹⁵の生成と崩壊プロセスを分析した Swartz の研究によれば、ICO バブルにおいてトークンを発行した数多くのブロックチェーンブ

¹⁵ ブロックチェーンを活用したトークンやサービスの開発事業に対する投資が加熱したことで生じた 2017 年の投資バブル。ICO バブルにおいてこれら開発事業に対する投資は推定 50 億米ドル以上に上ったとされるが、開発事業の相次ぐ中止やトークン価格の暴落によって 2018 年 1 月までに ICO バブルは崩壊した (cf. Schwartz 2022: 1700-1701)。

プロジェクトは起業家の失踪やトークン価格の暴落に終わる形で失敗した (Swartz 2022: 1705-1707)。ICO のブロックチェーンプロジェクトは、様々なトークンが法定通貨を代替する経済圏を構築し、トークンを介して財のオンライン取引を加速するトークンエコノミーに関するプロダクトやサービスであった。このトークンエコノミーは暗号資産が十分に普及した上で実現するかもしれない未来社会であり、ICO を発表する起業家やプロジェクト責任者はこうした未来社会がいつどのように到来するかの見通しが不確かであることを承知した上で、プロダクトやサービスのビジョンを語るしかない。一定数の投資家が ICO への投資のポジションを保持し続けたこうした未来社会が到来すれば投資家は莫大な投資リターンを得られるが、トークン価格の下落やプロジェクトに対する懸念が生じた時に投資家は不透明な未来社会の到来に賭けてポジションを保持するよりも、トークン価格の暴落によって自身の手元に無価値なトークンだけが残るリスクの回避を重視してトークンを売却する。ICO バブルは、ブロックチェーンプロジェクトの未来に対する期待と猜疑心が入り混じる中で、起業家と投資家が状況合理的に行為した結果生じた熱狂現象だったのである。

ブロックチェーンの実際的な運用では、サービスの利活用ではなく暗号資産の取引による利益の最大化を目的とした投資家や、暗号資産による事業を展開しようとする起業家の動向が大きな影響力をもつ。投資家がいかなる認識をもっておりまた他の投資家やステークホルダーとどのようなコミュニケーションを行っているかを調査することは、ブロックチェーンの ELSI 論点を検討する一助となるだろう。

4. ブロックチェーンの主な ELSI 論点

前節では、ブロックチェーンの実際の運用のなかでステークホルダーの動向や利害関心によって生じるブロックチェーンの理想と現実のギャップを論じた。本節では、ブロックチェーンの理想的な社会実装として構想される概念に内在する ELSI に着目する。ブロックチェーン ELSI については実際のプロダクトおよびサービス開発と並行してその検討が行われており (cf. Akar and Akar 2020; Hyrynsalmi et al. 2020)、とりわけ Tang et al. (2020) はブロックチェーンの倫理的課題を包括的に提示し具体的に論じている。本節では紙数の都合からブロックチェーンの技術に内在する技術スタックレベルの倫理的課題に絞り、Tang らの議論に依拠して¹⁶ (Tang et al. 2020: 610-613)、ブロックチェーン ELSI で重要になりうる論点としてプライバシー／データの

¹⁶ 本節での ELSI 論点の名称については、Tang et al. (2020) における原語表記を踏襲しつつ論点の内容を加味した名称を設定している。

正確性／データの共有財産化／アクセス可能性／開発者の中立性の五つを抽出し、その内容を整理していく。

4.1. プライバシー

ブロックチェーンの第一の ELSI 論点はプライバシーである (Tang et al. 2020: 610-611)。このプライバシーに関する論点は、さらに二つに分けられる。一つ目の観点はブロックチェーンの擬似的な匿名性である。ブロックチェーンの特徴の一つは記録されるデータを誰でも参照可能であることにあり、トランザクションに関わるすべてのデータがそのまま公開されるわけではない。暗号資産を用いたトランザクションではウォレットが使われるが、トランザクションを行う当事者に関してブロックチェーンで公開される情報はウォレットアドレスのみであり、名前／性別／年齢／国籍といった当事者の身元情報を含まない。こうした身元情報はウォレットを発行する暗号資産取引所やウォレットプロバイダーが保有している¹⁷。そのため、悪意がある第三者がトランザクションに関するウォレットアドレスの情報を収集し、これら暗号資産取引所やウォレットプロバイダーにサイバー攻撃をしかけてトランザクション当事者の身元情報を手に入れると、トランザクション当事者は危険にさらされることになる。

二つ目の論点は「忘れられる権利」である。「忘れられる権利」は EU の GDPR (General Data Protection Regulation: 一般データ保護規則) において第 17 条に規定があり¹⁸、一定期間の後に記録すべき正当な条件なくして個人の過去に関するプライバシーに関する情報がインターネット上に残っている場合、管理者がこれを削除することと検索結果で表示されないことを個人の権利とする考え方である。ブロックチェーンではトランザクションの検証作業に必要なデータが、過去から現在に至るまでインターネット上に保存そして公開されており、すべての人がこの情報にアクセスすることができる。一つ目の観点で述べたようにウォレットアドレスの形で一定の匿名化はなされているものの、暗号資産の送金記録や NFT の作成者など経済活動の記録は誰もが参照可能な形でブロックチェーン上に残り続ける。ブロックチェーンに記録されるデータは「忘れられる権利」の行使対象となりうるが、例えばブロックチェーンにおいて削除義務を負う管理者に相当する主体が不明確であるなど、権利行使と義務履行に係る法的課題が指摘されている

¹⁷ ウォレットプロバイダー等を介さず、ユーザーが自分で秘密鍵を生成し暗号資産を管理するウォレット (セルフ・カस्टоди・ウォレット) の場合、ユーザーの情報が第三者に保有されることはない。

¹⁸ <https://www.jipdec.or.jp/library/word/csm0kn0000006pe.html>

(Hofman 2019: 250-251)。なお、日本には「忘れられる権利」について明文化された法律上の規定は存在せず、司法においても独立した権利として認められないという見解が示されている¹⁹。

4.2. データの正確性

ブロックチェーンの第二の ELSI 論点はデータの正確性である (Tang et al. 2020: 611)。ブロックチェーンが将来的に生活やビジネスにおいて様々な記録を分散的に管理する社会インフラとなった場合、記録されたデータの正確性は極めて重要である。ブロックチェーンの記録データは組織や個人による意思決定の基盤となるため、データに瑕疵や誤りがある場合これが及ぼす影響は深刻なものとなる。ブロックチェーンのシステムは信頼できるデータ管理主体を必要とせず、データ管理の分散性と透明性に優れた情報技術となっている。しかし、ブロックチェーンは記録されたデータ自体の信頼性や正確性を保証するわけではないため、データの信頼性は従来のデータベースと同様に非技術的な仕方で担保されなければならないという問題がある。Tang らはこの特徴を「すべてのデータが…認証されたこと、また変更不可能であることを保証する、信頼を欠いたオープンな分散型台帳 (trustless distributed open ledger that ensures that all data… are authenticated and immutable)」 (Tang et al. 2020: 611) と表現する。ブロックチェーンにおけるデータの記録や保存は、不審な改ざんがなされたかどうかの検証がマイナーによって行われたことを表している。データ自体に欠損や瑕疵のあるデータが持ち込まれた場合であっても、マイナーによって承認されればそのデータはブロックチェーンの正当な記録として扱われてしまうのである²⁰。

4.3. データの共有財産化

ブロックチェーンに関わる第三の ELSI 論点はデータの共有財産化である (Tang et al. 2020: 611-612)。2.5 で述べたように、Web2.0 以前ではユーザーが過去から現在に至るまでプラットフォームを利用した履歴であるビッグデータへのアクセスをビッグテックが独占し、これを排他的に管理する中央集権的な組織となっている。一方でブロックチェーンの場合、記録された情報

¹⁹ <https://www.sankei.com/article/20160713-FL7I4SKUQZIH5NCV5HZMNYVCAY/>

²⁰ 関連する問題として「オラクル問題」と呼ばれているものがある。スマートコントラクトにおいてチェーンの外部の情報が必要となるとき、この情報をチェーンに提供するサードパーティないしそのサービスを「オラクル」と呼ぶ。「オラクル問題」とは、外部データの信頼性がこのオラクルの信頼性や脆弱性に依存してしまうという問題を指す。

を保管し管理する中央集権的な組織は存在しない。ブロックチェーンに記録されるデータには誰もが平等にアクセスし、ブロックチェーンの記録データから付加価値を出すことも同じ条件で自由に行うことができる。ブロックチェーンのデータは蓄積したデータに対して排他的なアクセスをもつ中央集権的な組織による支配から解放された、民主化された財となる。データに対する排他的なアクセスを独占する機関がないブロックチェーンのデータは共有財産であり、不均衡なデータ管理から自由になった形でサービス開発やイノベーションが生じる契機となる。しかし、データを管理するプラットフォーマーの介入による再中央集権化を懸念する論者もいるように²¹、データの寡占による構造的な不均衡や不公正が生じる可能性が原理的に排除されているわけではない点には注意が必要である。

4.4. アクセス可能性

ブロックチェーンに関する第四のELSI論点はアクセス可能性である(Tang et al. 2020: 612)。ブロックチェーンの特色は記録検証作業が不特定多数のノードへ開かれていることや、ブロックチェーンの記録情報へステークホルダーが自由にアクセスできることにある。しかし、ブロックチェーンの種類によっては検証作業へ参加できるノードや記録情報の公開の範囲は制限される。この問題に関わるブロックチェーンの種類として、パブリック型／プライベート型／コンソーシアム型の三つがある。パブリック型はブロックチェーンのノードとして特定の管理者の許可など取ることなく誰でも参加可能で、データへのアクセス可能性は万人に開かれている。プライベート型では単一の管理者が、コンソーシアム型では複数の管理者がおり、管理者の許可を得たノードのみが記録検証作業へ参加することができる。またプライベート型とコンソーシアム型では、ブロックチェーンの記録情報の公開範囲は無制限とは限らず特定のユーザーに限定されることもある。プライベート型とコンソーシアム型については、記録情報へのアクセスが管理者の決定によって閉ざされてしまう可能性があり、また記録情報が不特定多数へ公開された場合でも管理者が許可を出した少数のノードによってブロック内のデータに不正や改ざんが行われる懸念がある。この許可型ブロックチェーンにおいては、不特定多数のノードの検証によってブロックのデータに不正や改ざんがないことを保証する、ブロックチェーンの重要な特色である分散性が損なわれていることには注意せねばならない(岡嶋 2022: 136-140)。

²¹ <https://markets.businessinsider.com/news/currencies/crypto-isnt-decentralized-nft-bored-ape-yacht-club-buys-cryptopunks-2022-3>

4.5. 開発者の中立性

ブロックチェーンに関わる第五の ELSI 論点は開発者の中立性である (Tang et al. 2020: 612-613)。ブロックチェーンでは開発の基礎となるプロトコルやエンドユーザーに関わるソフトウェアはしばしばオープンソースとして公開されているが、ブロックチェーンの基礎となる通信技術や暗号技術の発展に貢献するエンジニアは多くない。多くのエンジニアは既存のブロックチェーンを活用し社会実装化したプロダクトやサービスの開発に注力しており、企業からのバックアップを受けている。この場合、ブロックチェーン開発に関わるエンジニアがブロックチェーンのエコシステム全体ではなく、自身に支援を行う企業の利益を優先することは極めて自然である。ブロックチェーンの倫理性を担保するためには、ブロックチェーン開発においてブロックチェーンのエコシステム全体の利益が確保されるような技術の中立性を維持する必要がある。より優れた社会実装を可能にするために、オープンソース化されたブロックチェーンの基礎技術の改善を活発に行う開発コミュニティが必要なのである。

5. おわりに

最後に本稿での議論を改めて振り返り、課題や展望について論じていく。第2節では、ブロックチェーンに関連する諸概念として、暗号資産/スマートコントラクト/NFT/DAO/Web3の内容とそれぞれの関係を整理した。第3節では、ブロックチェーンの社会学/文化人類学的研究のレビューを通じて、ブロックチェーンの運用を支えるステークホルダーとしてマイナー/開発者/取引所/投資家を取りあげ、それらの動向や利害関心を論じた。第4節では、Tang et al. (2020) を参照することで、プライバシー/データの正確性/データの共有財産化/アクセス可能性/開発者の中立性というブロックチェーンの ELSI 論点を挙示した。

ブロックチェーン ELSI の探索および RRI の実現を志向する本稿の課題として、本稿が示した ELSI 論点は第1節で概観したブロックチェーンの社会実装に係る諸概念の構想に留まっていることが挙げられる。例えば 4.3 で言及した「データの共有財産化」など本稿が試論的に抽出した ELSI 論点は、ブロックチェーンの実際上の運用において生じる状況や問題ではなく、ブロックチェーンの諸概念における形成途上の構想に依拠したものである。第3節で萌芽的に論じたように、ブロックチェーンの実際的な運用にあたってはその理想や構想とは異なる現実が生じうるのであり、この状況に紐づく形でブロックチェーンの ELSI 論点を明確化そして提示することが今後の研究の課題となるだろう。

そしてこの課題へと取り組むための展望として、ブロックチェーンの社会実装事例の開発と運用に関係するステークホルダーが集まるプラットフォームの調査は有用となりうる。ブロックチ

チェーンは信頼すべき中央集権的な管理者や管理組織を介さずに、ユーザー自身の手で分散的な記録管理を行うことができる新技術として世に出た。しかし本稿で抽出した ELSI 論点やステークホルダーの動向を踏まえると、社会実装事例の開発や運用において生じたのは、一部のステークホルダーが非常に大きな影響力を備え信頼せざるをえない中央集権的な存在と化してしまう事態であった。ブロックチェーンの ELSI を深く探る上では、ブロックチェーンの社会実装事例の開発や運用を推進するコミュニティに着目し、コミュニティの活動基盤となる Discord のようなプラットフォームにおいていかなるステークホルダーがどのような役割や活動を担っているかを調査する必要があるだろう。そしてこうしたプラットフォームにおけるステークホルダーの実践をリアルタイムで観察し、調査結果を開発現場へと継続的にフィードバックすることは、ブロックチェーン ELSI に対処しブロックチェーンの円滑な社会実装を実現する RRI の一つの方向性となりうる (cf. Fisher et al. 2006)。

謝辞

本稿の加筆修正にあたり、株式会社メルカリの栗田青陽氏および荒川貴将氏からは主にブロックチェーンの技術的内容について、大阪大学社会技術共創研究センターの岸本充生氏および赤坂亮太氏からは主に ELSI 論点の明確化について、有益なコメントとフィードバックをいただきました。この場を借りて深謝申し上げます。

用語集

DAO (Decentralized Autonomous Organization) : 分散型自律組織。従来型の中央集権的組織と対比される、パブリック型ブロックチェーンとスマートコントラクトの利用によって実現される組織形態とされる。厳密な定義があるわけではなく、ヴィタリック・ブテリンによる定義（「伝統的な企業や NPO の法的外観を模倣しつつもその執行にはブロックチェーン技術のみを使用するエンティティ」）をはじめ、さまざまな定義がある（Hassan and De Filippi 2021）。2.4 節を参照のこと。

DeFi (Decentralized Finance) : 分散型金融。ブロックチェーンとスマートコントラクトによって自動化された金融サービスを指す概念。

DeSci (Decentralized Science) : 分散型科学。研究開発資金の調達方法や知識の共有方法など現代の学術業界が抱える課題を、ブロックチェーンと関連技術の活用によって解決する構想。

GameFi : ゲームと分散型金融 (DeFi) の融合を表す概念。ゲーム・プレイを通じて暗号資産を報酬として獲得したり、ゲーム内で手に入れたアイテムを暗号資産に交換したりできる仕組み (Play to Earn; P2E) を持つブロックチェーン・ゲームの開発が進んでいる。

NFT (Non-Fungible Token) : ブロックチェーンによってデジタルコンテンツひとつひとつの保有情報やその移転を記録できるトークン。2.3 節を参照のこと。

P2P (Peer to Peer) : サーバによる中央管理を用いず、複数の対等な関係にあるコンピュータ間で通信を行うアーキテクチャ。

PoS (Proof of Stake) : ブロックチェーンに新しいブロックを追加するメカニズム (コンセンサス・メカニズム) のひとつ。イーサリアムなどで採用されている。一定量の暗号資産をブロックチェーン上にロック (ステーキング) しているノードが、ステーキング量に基づいて設定された確率で、ランダムにブロックの検証者 (バリデータ) を割り当てられる方式。PoW よりもエネルギー効率が良いとされるが、検証の権利が暗号資産の保有の多寡に依存することへの懸念も指摘さ

れる。

PoW (Proof of Work) : ブロックチェーンに新しいブロックを追加するメカニズム (コンセンサス・メカニズム) のひとつ。ビットコインなどで採用されている。ブロックの追加作業に参加するノードが互いに競い合う形で計算問題を解き、最初に条件を満たす解を発見したノードの解答が検証されると新たなブロックがチェーンへと追加される方式。計算に伴うエネルギー消費の高さが懸念されている。

Web3 : ブロックチェーンを基盤として中央集権型ではなく分散型で成立するインターネットの構想。2.5 節を参照のこと。

暗号通貨ウォレット : 単にウォレットとも呼ばれる。ユーザがブロックチェーンにおいて暗号資産をやり取り・管理するためのツール。トランザクションの作成に必要なユーザーの秘密鍵／公開鍵を格納する。形態はさまざまで、ソフトウェアの形を取ることもあればハードウェアの形を取ることもある。

イーサリアム : Vitalik Buterin によって 2013 年に考案された、特定の管理者を置くことなく分散的に機能するアプリケーションを開発しまた運用するためのブロックチェーン・プラットフォーム。2.2 節を参照のこと。

公開鍵暗号方式 : 電子署名に用いられる暗号方式。秘密鍵 (署名鍵) と公開鍵 (検証鍵) と呼ばれる鍵データ (いずれも整数値の形をとる) のペアを用いる。秘密鍵でデジタル署名を作成し、対になる公開鍵でデジタル署名の検証を行う。ブロックチェーンでは、公開鍵からウォレットのアドレスを生成する。アドレスから暗号資産残高を移転するトランザクションには、秘密鍵を使ったデジタル署名を付与する必要がある。秘密鍵の管理者のみがアドレスにある暗号資産を移転できる。

コンセンサス・アルゴリズム : コンセンサス・プロトコルを構成し、ノード間で合意を形成するために用いられるアルゴリズム。新たなブロックを作成するノードを決定するアルゴリズムや、ブロックチェーンが分岐した場合に正しいとみなすブロックチェーンを決定するアルゴリズム等がある。2.1 節を参照のこと。

コンセンサス・プロトコル : ノード間で共有するブロックチェーンデータの整合性を取るために合意 (コンセンサス) を形成する一連の手順。

スマートコントラクト : 人間の介入を最小限に抑えることを目的に、ブロックチェーンを活用して契約を自動で実行する仕組み。2.2 節を参照のこと。

ナカモト・コンセンサス：ビットコインにおいて用いられるコンセンサス・プロトコル。2.1 節を参照のこと。

ノード：P2P 型ネットワークに接続するコンピュータ端末のことで、ブロックチェーンにおいてはトランザクションデータやブロックチェーンデータの共有・保管、ブロックの追加・検証・マイニングなどを行う主体を指す。

ハッシュ関数：任意のデータから固定長のデータを生成するための関数。出力から入力が入力が復元困難であるという性質を持つ。ブロックチェーンにおけるブロック間の前後関係を保証し、改ざんを防ぐことで、セキュアなトランザクションの構築に貢献している。

ビットコイン：Satoshi Nakamoto によって 2008 年に考案された、ブロックチェーンを基盤として送金記録を分散的に管理する暗号資産。

ブロックチェーン：データをブロックと呼ばれる単位にまとめ、数珠つなぎ状につなげて記録する仕組み。

マイニング：PoW に基づく暗号資産においてブロックの追加作業に参加するノードが互いに競い合う形で計算問題を解くこと。2.1 節を参照のこと。

参考文献

- Akar, S, and Akar E., 2020, Is it a new tulip mania age?: A comprehensive literature review beyond cryptocurrencies, bitcoin, and blockchain technology, *Journal of Information Technology Research*, 13(1): 44-67.
- Burrell, J., and Fourcade, M., 2021, The society of algorithms, *Annual Review of Sociology*, 47(1): 213-237.
- Çalışkan, K., 2020, Platform works as stack economization: Cryptocurrency markets and exchanges in perspective, *Sociologica: International Journal for Sociological Debate*, 14(3): 115-142.
- , 2022a, Data money makers: An ethnographic analysis of a global cryptocurrency community, *The British Journal of Sociology*, 73(1): 168-187.
- , 2022b, The rise and fall of Electra: Emergence and transformation of a global cryptocurrency community, *Review of Social Economy*, 1-25.
- , 2022c, The elephant in the dark: A new framework for cryptocurrency taxation and exchange platform regulation in the US, *Journal of Risk and Financial Management*, 15(3): 1-18.
- Fisher, E., Mahajan, R., and Mitcham C., 2006, Midstream modulation of technology: Governance from within, *Bulletin of Science, Technology & Society*, 26(6): 485-496.
- Hassan, S., and De Filippi, P., 2021, Decentralized autonomous organization, *Internet Policy Review*, 10(2): 1-10.
- Hayes, A., 2023, Competing imaginaries: Crypto-utopianism and the material forces of Bitcoin mining, *Anthropology Today*, 39(4): 4-8.
- Hofman, D., Lemieux, V. L., Joo, A., and Batista, D. A., 2019, The margin between the edge of the world and infinite possibility: Blockchain, GDPR and information governance, *Records Management Journal*, 29(1/2): 240-257.
- Humayun, M., and Belk, R. W., 2018, “Satoshi is dead. Long live Satoshi”: The curious case of Bitcoin’s creator, *Consumer Culture Theory*, 19: 19-35.
- Hyrnsalmi, S., Hyrnsalmi S. M., and Kimppa, K. Blockchain ethics: A systematic literature

review of blockchain research, *Well-Being in the Information Society. Fruits of Respect: 8th International Conference, Proceedings 8*, 145-155.

Lee, S. C., 2022, Magical capitalism, gambler subjects: South Korea's bitcoin investment frenzy, *Cultural Studies*, 36(1): 96-119.

Swartz, L., 2022, Theorizing the 2017 blockchain ICO bubble as a network scam, *New Media & Society*, 24(7): 1695-1713.

Szabo, N., 1994, Smart contracts. (<https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html>)

Tang, Y., et al., 2020, Ethics of blockchain: A framework of technology, applications, impacts, and research directions, *Information Technology & People*, 33(2): 602-632.

Vidan, G., and Lehdonvirta V., 2019, Mine the gap: Bitcoin and the maintenance of trustlessness, *New Media & Society*, 21(1): 42-59.

Wyeth, R., Rella, L., and Atkins, E., 2024, The material geographies of Bitfury in Georgia: Integrating cryptoasset firms into global financial networks, *Environment and Planning A: Economy and Space*, 56(3): 816-832.

Zaucha, T., and Agur C., 2024, Newly minted: Non-fungible tokens and the commodification of fandom, *New Media & Society*, 26(4): 2234-2255.

ヴィタリック・ブテリン, [2014] 2023, 「イーサリアムホワイトペーパー——次世代のスマートコントラクトと分散型アプリケーションのプラットフォーム」『イーサリアム——若き天才が示す暗号資産の真実と未来』(高橋聡訳), 374-432, 日経 BP.

ヴィリ・レドンヴィルタ, [2022] 2024, 『デジタルの皇帝たち——プラットフォームが国家を超えるとき』(濱浦奈緒子訳), みすず書房.

岡嶋裕史, 2019, 『ブロックチェーン——相互不信が実現する新しいセキュリティ』, 講談社.

——, 2022, 『Web3 とは何か——NFT、ブロックチェーン、メタバース』, 光文社.

岡田仁志, 2018, 『決定版 ビットコイン&ブロックチェーン』, 東洋経済新報社.

清水音輝／荒巻陽佑，2023，『スマートコントラクトの仕組みと法律』，中央経済社。

城田真琴，2023，『決定版 Web3』，東洋経済新報社。

フェリックス・シュタルダー，[2022] 2022，「コモンズから NFT へ——デジタルオブジェクトとラディカルな想像力」（秋吉康晴／増田展大／松谷容作訳）『メディウム』，3: 39-51.

福岡真之介／本柳祐介，2023，『DAO の仕組みと法律』，商事法務。

マット・フォートナウ／キューハリソン・テリー，[2021] 2022，『NFT のすべて——歴史・仕組み・テクノロジーから発行・販売まで』（Pivot Tokyo 訳），翔泳社。

ELSI NOTE No. 54

令和7年2月7日

ブロックチェーン ELSI（倫理的・法的・社会的課題）の予備的考察：

概念の整理・ステークホルダー分析・主要な ELSI 論点の抽出

金 信行	北陸大学 経済経営学部 助教 大阪大学 社会技術共創研究センター 招へい教員（2025年1月現在）
森下 翔	山梨県立大学 地域人材養成センター 特任助教 大阪大学 社会技術共創研究センター 招へい研究員（2025年1月現在）

A Preliminary Research on the Ethical, Legal, and Social Issues (ELSI) of Blockchain:

Conceptual Clarification, Stakeholder Analysis, and Identification of the Key Issues

Nobuyuki Kim	Hokuriku University Osaka University
Sho Morishita	Yamanashi Prefectural University Osaka University



大阪大学 社会技術共創研究センター
Research Center on Ethical, Legal and Social Issues

〒565-0871 大阪府吹田市山田丘 2-8
大阪大学吹田キャンパステクノアライアンス C 棟 6 階
TEL 06-6105-6084
<https://elsi.osaka-u.ac.jp>



大阪大学

Osaka University
Research Center on
Ethical, Legal and
Social Issues