WIDE Technical-Report in 2017

分散レッジャー技術と来たるべき社会変容

wide-tr-ideon-dlt2017-00.pdf

WIDE Project : http://www.wide.ad.jp/

If you have any comments on WIDE documents, please contact to board@wide.ad.jp

Title: 分散レッジャー技術と来たるべき社会変容
Author(s): 斉藤 賢爾 (ks91@wide.ad.jp)
Date: 2017-01-18

分散レッジャー技術と来たるべき社会変容

斉藤 賢爾
ks91@sfc.wide.ad.jp

2017 年 1 月 18 日

概 要

2008 年, 匿名の開発者サトシ・ナカモトにより, デジタル通貨システム「ビットコイン」を実現するための分散タイムスタンプサービスとして提案されたブロックチェーンは, 言わば空中に約束を固定する装置 (空中約束固定装置) として機能し, 今やデジタル通貨のみならず, 契約や企業の自動経営まで, 新たな社会基盤としての様々な応用可能性が取り沙汰されている.

本稿では, ビットコインのような第 1 世代のブロックチェーンが抱える課題と, 2017 年 1 月時点での分散レッジャー (分散台帳) 技術の動向に鑑みて, そうした技術に対する社会のニーズと社会が求める同技術の将来像を改めて明らかにし, 逆に同技術が投入・展開された未来における社会の変容を論じる.

本稿は [23] に加筆修正したものである.

1 ブロックチェーンとは何か

まずはじめに, ブロックチェーンとは何か, 改めて振り返るとともに, 本稿がブロックチェーンという用語で指し示す範囲を明確にしたい.

1.1 分散タイムスタンプサービス

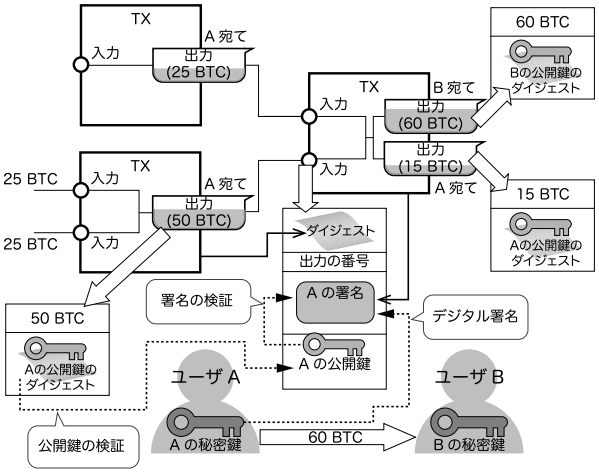
ブロックチェーンは, 2008 年, 匿名の開発者サトシ・ナカモトにより, デジタル通貨システム「ビットコイン」を実現するための分散タイムスタンプサービスとして提案された [14].

ビットコインは, 管理者のいない環境下で「電子的に表現されたコインの制御権[1] の移転」, すなわち電子コインによる「送金」を実現することを目標に設計されている. 送金の取引は入金 (入力) と出金 (出力) の間の関係を記述するが, ビットコインでは, 未使用の取引出力がコインであるとするいわゆる UTXO (Unspent TX[2] Output) 構造 (図 1) を用いて電子コインのデジタルデータ形式を定義している.

この構造は, 適切な秘密鍵を用いて取引にデジタル署名できる主体だけが送金できることを保証するが, 署名の検証に必要な情報 (公開鍵) をデータ構造の中に埋め込み, 公開鍵のメッセージダイジェスト (ハッシュ値) をコインの送金の宛先とすることで, まったく関係のない第三者でも公開鍵の正当性を確認でき, 取引の形式的な正しさを検証可能にした点で画期的である.

ところが, デジタル署名だけでは同じコインが 2 度使われるような不正があっても検出できない. 「二重消費 (double spending)」と呼ばれるこの問題を解決するための方法は色々あるが, 1 度使われたコインを使用済みと

[1] 一般に貨幣は公共財であり, 私的に所有されないが, 持ち主は次にそれをいつ誰に渡すかを制御できる.
[2] TX はトランザクション (transaction) の略.



- ユーザ A から B へ 60BTC を送金する例.

図 1: ビットコインのいわゆる UTXO データ構造

して記録するべく, 全取引を時間軸で一列になるように固定し, その順序関係が参加する全員にとって一致して観測されるようなタイムスタンプサービスを使うという単純な発想も可能である. この発想がビットコインと同時に発明されたブロックチェーンの基本である (図 2).

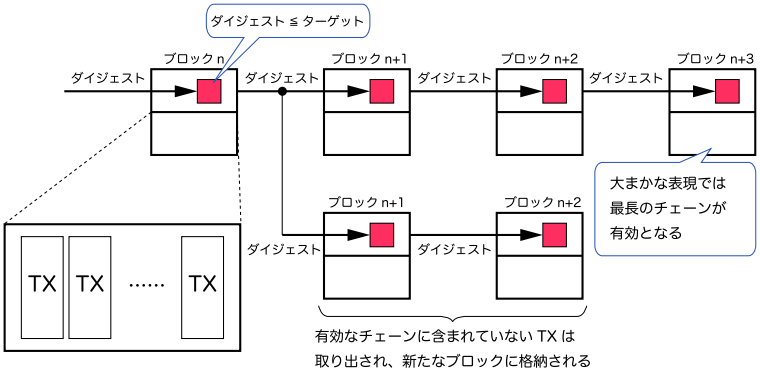


図 2: 第 1 世代のブロックチェーン

この言わば第 1 世代のブロックチェーンでは, 取引群を格納する各ブロックのヘッダ部に直前のブロックのダイジェストを置くことにより, ブロックの前後の関係を明確に表現する[3]. あるブロック (番号 n) を作る際に, すでに直前のブロック (番号 $n-1$) が存在していない限り, 番号 $n-1$ のブロックのダイジェストを計算することはできないのだから, この構造は論理的にブロックの作成時刻の相対的な前後関係を表すものと言える. こうしたブロックチェーンでは, 前のブロックから受け継がれるターゲット値[4]以下のダイジェストが得られるようにブロックの

[3] この構造をハッシュチェーンと呼ぶ.
[4] ビットコインでは, ブロック間の間隔が平均して 10 分間になるように 2016 ブロック毎にターゲット値を調整している.

データを構成しなければならないという,「作業証明 (proof of work)」の仕組みによって改ざんを抑止している. ブロックの作成 (や作り直し) にはコストがかかり, 古いブロックの改ざんを試みる場合ほど, それ以降のブロックのデータを次々に改ざんしなければならず, 改ざんにかかるコストが累積的に増えるようになっているのである.

ただし, ネットワークに対するブロックの提案は自律分散的に行われるため, 条件を満たす別々のブロックが複数の参加者から同時に提案され, 参加者がそれぞれ独自の判断でそれらに続くブロックを繋げていき, 結果としてチェーンが分岐していくことがある. 順序が一意に定まらなければ二重消費の問題を解決することにならないので, ビットコインでは, 作業証明のコストがより多く支払われてきたチェーン (大まかには, より長く延びているチェーン) を全員が採用するというコンセンサス機構「ナカモト・コンセンサス」を備えている. ナカモト・コンセンサスは, 覆すためのコストがより大きい歴史を正史として採用するという意味で, 設計の意図に整合的である.

本稿における「ブロックチェーン」は, こうした第 1 世代のブロックチェーンの特徴を踏襲しているものを指す.

1.2 ブロックチェーンを理解する

あらゆる技術は, 特定の問い (要求) に対する答えである. したがって, ある技術を理解するためには, まずその問いを理解する必要がある. ビットコインの問いは,「自分が持っているお金をいつでも自分の好きに送金することを誰にも止めさせないためには？」というもの[5]であり, その他のブロックチェーンや, より一般化した概念であり後述する分散レッジャー (distributed ledger; 分散台帳) 技術にも適用可能なように汎用化すると,「アセット (資産) の制御の権限を中央ではなくエンド (端点) が持つには？」となる.

図 3は, そうした問いに応える技術としてのブロックチェーンや分散レッジャーを理解するために, その機能を階層構造として整理したものである.

図 3: ブロックチェーン/分散レッジャーの機能の階層構造

1.2.1 正当性 (validity)

正当性 (の保証) は, システムに投入されたトランザクションやレコードがルールに基づいて記述されており, 過去の記録と矛盾しないことを保証する機能である.

[5]サトシ・ナカモトの論文では明記されていないが, 後述する R3 Corda の開発者の整理 [17] による.

一般に, デジタル署名により, 本人性 (すなわち, 権限を持つ本人であるか) の確認と記述内容の否認不可能性が提供される. 署名の検証を第三者が行う場合は, 記録の中に公開鍵を埋め込んだり, あるいは何らかの PKI を用いる必要がある.

1.2.2 存在証明 (proof of existence)

存在証明は, トランザクションやレコードの存在の否認不可能性を提供する機能である. 内容の否認不可能性は前述のようにデジタル署名によってもたらされるが, それでも「この時刻に存在した」あるいは「このイベントの前/後に存在した」ということは, 原理的に否認できる. デジタル署名には時刻の概念がないからである. デジタル署名の対象を (相対) 時間の中に位置づけるこの機能は, タイムスタンプサービスと関係が深い.

取引の当事者であれば, メッセージのやり取りの履歴の中にトランザクションやレコードの受信を位置づけることができるため, この機能を明示的に必要としない場合を考えることもできる (不要ではない).

1.2.3 唯一性 (uniqueness)

唯一性 (の保証) は, トランザクションやレコードがユニークである (アセットの歴史が分岐せず, 単一のタイムラインを刻んでいる) ことを保証する機能である.

自律分散環境では, アセットの歴史のビューがノードにより異なる場合も発生し得るため, 二重消費が起きていないことを保証する等の目的でこの機能が必要になる.

ただし, 例えばクリエイティブコモンズのライセンスにもとづくデータの頒布の記録など, この機能の必要がない場合を考えることもできる.

1.2.4 ルール (rules)

ルール (の管理) は, 正当性を確認するためのルールや自動処理の記述・エンフォースメントおよび実行を提供する機能である.

こうしたルール記述を「スマートコントラクト (smart contract)」と呼ぶことがある.

ブロックチェーン/分散レッジャーが実世界とどうリンクできるかについて課題が山積している現状, スマートコントラクトでできることは, デジタルに表現されるアセットをあらかじめ定められたルールに従って移転することくらいであるが, 言わばアプリケーション層となるこの層は社会への影響と直接繋がる部分であり, 今後特に重要になると考えられる.

1.3 空中約束固定装置

こうした構造を持つことで, ブロックチェーンや分散レッジャーは, 言わば「空中に約束を固定する装置」として機能する. ビットコインで言えば, 約束とはコインの宛先だけがそのコインを送金できるというものである. 約束がどの主体にも属さず, 空中で維持されていることにより, エンドが権限を持つことを保証でき, かつ, 常時ネットワークに接続しているわけではなく間欠的にシステムに参加するような主体にも対応できる.

以降, ブロックチェーンや分散レッジャーのこの性質に言及する際は, 「空中約束固定装置」という用語を用いる.

日本銀行総裁は, 2016 年 8 月の第 1 回 FinTech フォーラムの冒頭での挨拶 [20] で, 『「ブロックチェーン」や「分散型元帳」は, 「帳簿は特定の主体が管理するもの」という従来の考え方を大きく変えるものです. 金融の発展自体が帳簿というインフラに支えられてきたことを踏まえれば, 帳簿の革新は, 金融の形態にも大きな変化をもたらす可能性があります』と述べている. しかし, その監査可能性や, 権限を持つ主体による運用の自律性を考えるなら, 帳簿は本来的に空中に置かれるべきものである.

空中約束固定装置は, 特に公共財に関して, その制御権を公正に運用することに適している. 社会に影響力を持ちうるその最初の実装 (ビットコインブロックチェーン) が, 貨幣という公共財の分野に登場したことは象徴的だと言える.

2 ブロックチェーンへの期待と課題

ここで, ブロックチェーンの期待される応用について述べ, ブロックチェーンが抱える技術とガバナンスの諸問題を明らかにしたい.

2.1 期待されている応用

後述するハイパーレッジャープロジェクト [13] での整理 [7] の仕方に倣って, ブロックチェーンについて期待されている応用を列挙する.

2.1.1 金融アセット管理

仲介を不要とする直接アクセス, 合意された実時間内の決済, ビジネスルールの記述・埋め込み, 秘匿性の制御等が期待されている. このうち, 実時間性や秘匿性については第 1 世代のブロックチェーンでは対応できない.

2.1.2 企業行動 (特に財務上の意思決定) の自動化

株式分割, 減資・併合, 株式移転・交換, 合併, 第三者割当増資等の実時間での実行と秘匿性の制御が期待されている. 同様に, 実時間性や秘匿性については第 1 世代のブロックチェーンでは対応できない.

2.1.3 サプライチェーン管理

材料のトレースバックや, 生産・貯蔵から販売までの記録と検索機能の提供が期待されている. 厳しい実時間性が要求されなければ第 1 世代のブロックチェーンでも対応でき, ダイヤモンドやワインにおける応用事例が存在する [5].

2.1.4 マスターデータ管理

権限を持つ者のみが更新でき, 指定された検証者がそれを承認する仕組みが期待されている. 厳しい実時間性が要求されなければ第 1 世代のブロックチェーンでも対応可能である.

2.1.5 シェアリングエコノミーと IoT(Internet of Things)

信用が必ずしも確立していない状況下でのスマートシティ, 交通, ヘルスケア, リテール, 建築, 教育等への応用が期待されている. 公共財の公正な運用のために適しているという空中約束固定装置としての性質上, 最も高い期待が持たれる応用のひとつであるが, 暗に実時間性や秘匿性についての要求があり, 第 1 世代のブロックチェーンでは対応できない.

2.2 スケーラビリティの課題

実時間性や秘匿性の欠如に次ぐ技術的な課題の代表例として, システムがスケールアウトしない, すなわち, ノードを追加することでは性能上の問題を解決できないという課題がある.

ブロックチェーンでは, 全機能を有するノードの各々がブロックチェーンのデータ全体を処理するため, 取引の増加に伴い, データ構造を維持するためのコストが直線的に上昇する (図 4).

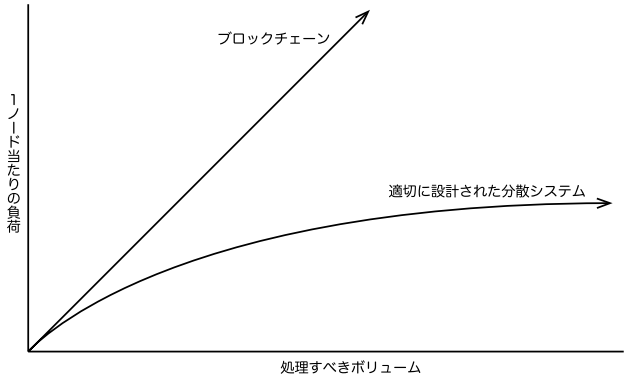


図 4: スケーラビリティの課題

ただし, ブロックチェーンを実装するためには, ハッシュ値をキーとするブロックや取引の検索機構を備える必要があるので, それを KVS(Key-Value Store) だと捉えれば, 既存の分散 KVS の手法を用いた改良の余地があると考えられる.

2.3 ワンネスの罠

ブロックチェーンは, 大規模災害や政変などによりネットワークが分断されると, チェーンが安定的に分岐することになり, 唯一の正しい歴史が保たれるという大前提が崩れ, 正しく動作しない. 「世界がひとつ」でなければ動作しないというこの性質を, 以降は「ワンネス (oneness)」と呼称する.

「分散」の考え方と真っ向から対立するかたちとなる「ワンネス」がもたらす重要な帰結は, 技術を進化させるガバナンスが利きにくいということである. ブロックチェーンでは, インターネットのその他のアプリケーションでは普通に行われている, 「一部で違うことを試して, うまくいったら全体で採用する」ということができない. 一部が異なる仕様で動くとチェーンが分岐してしまうからである. すると, 現実への適用性を実地で評価しながら技術を進化させていくことが困難になる. めまぐるしく変化する技術的・社会的状況の中で, 実際に使われていく技術を維持していくためには, この困難性は致命的となる.

この困難性は, 例えば, 一度ブロックチェーンにデプロイされたスマートコントラクトのコードを修正できないというかたちでも浮上しうる (もちろん, そのように設計しないことも可能である). ソフトウェアは, 改善が可能な状態に置かれるべきであり, 開発者の権限を不当に制限するそのような設計は決して望ましくはない.

2.4 インセンティブ不整合性

ブロックチェーンはマイナーにより維持されるため, マイナーが大規模に撤退することにより停止するおそれがある. マイナーは, ブロックを生成することにより報酬を得ている. ブロックの生成にはコストがかかるため, 報酬として得られる通貨の価格が下落し, 投入するコストに見合わなくなると, 撤退という選択肢が現実的となる.

このことがもたらす帰結は, ビットコインの場合, 「ビットコインの価格が下落する $\Rightarrow$ ビットコインブロックチェーンが停止する」である. したがって, この設計は素のビットコインに関してはインセンティブ整合的と言える.

しかし, ブロックチェーンの上で様々なアプリケーションが動作している場合はこの限りではなく, 「ブロックチェーンのネイティブ通貨の価格が下落する $\Rightarrow$ その上のアプリケーションすべてが停止する」となるため, このインセンティブ設計はブロックチェーンを汎用のアプリケーション基盤として見た場合に不整合的である.

3 分散レッジャー技術の動向

ここで, ブロックチェーンを分散レッジャーの一種として捉え直し, 現在開発途上にある一連の技術について動向を見た上で, さまざまな課題の解決・解消に向けた設計の提案を行いたい.

3.1 問いの立て直し

前述のように, あらゆる技術は特定の問いに対する答えであるので, 問いを立て直すことにより, それを解くための技術を改めて考え直すことができる. 分散レッジャーを「空中約束固定装置」として捉えるならば, その技術への問いは以下である.

Q1: 空中とはどんな範囲か.

Q2: 約束とはどんな種類か.

Q3: その空中にどうやってそうした種類の約束を固定するか.

分散レッジャーの設計では, これらを各々のアプリケーションの文脈の中で問うことになるし, それに伴い, 「正当性」「存在証明」「唯一性」「ルール」のそれぞれについて, 要求を満たすための設計上の選択をすることになる.

3.2 様々な分散レッジャー技術

3.2.1 ハイパーレッジャー (Hyperledger)

ハイパーレッジャーはリナックスファウンデーション (Linux Foundation) におけるプロジェクトであり, 多くの企業による貢献で成り立ち, 複数の汎用の分散レッジャーをオープンソースで開発している.

ハイパーレッジャーは「ビジネスのためのブロックチェーン技術」を謳っており, 「約束」は汎用的であるが, 「空中」は, 特に明記しない限り特定の事業のステークホルダーからなる空間となる.

3.2.2 ハイパーレッジャー・ファブリック (Fabric)

「ファブリック」[10] は, IBM と Digital Asset Holdings により貢献されたコードのマージから始まった分散レッジャーである.

ファブリックでは, コンセンサス機構について, 既存の耐ビザンチン障害[6]プロトコル (BFT; Byzantine Fault Tolerance)[11][3][4] の応用を基調に置いているが, BFT ではノードの総数 n が既知である必要がある. その意味で「空中」を完全なるパブリックかつオープンな空間にはできない. しかし, ビジネス応用の多くにおいては, それはむしろ望ましい性質と言えるかも知れない.

表 1に, ファブリックにおける設計上の選択をまとめた.

表 1: Fabric における設計上の選択

ルール	ドッカー (Docker) コンテナで実行する「チェーンコード (chaincode)」
唯一性	PBFT (Practical BFT) またはナカモト・コンセンサス チェーンコードの結果に対するコンセンサスが必要
存在証明	ハッシュチェーン
正当性	RocksDB 上の構造と軽量 CA による PKI

3.2.3 ハイパーレッジャー・ソウトゥースレイク (Sawtooth Lake)

「ソウトゥースレイク」[9] は, インテルにより貢献されたコードにもとづく分散レッジャーである.

この分散レッジャーでは, 「空中」をパブリックかつオープンな空間とすることも念頭に置き, PoET (Proof of Elapsed Time; 経過証明) と呼ばれる, 存在証明および唯一性のための機構を持つ. これは proof of work の作業のコストを実際には投入せずに (電力を浪費せずに), 指定された難易度に基づく時間を単に確率的に経過させるものだと考えられる. ビットコインブロックチェーンにおける作業証明は確率的過程であり, 本質的な意味で「くじ引き」であることを考えると, このアイデア自体は妥当と言えるが, 現時点では標準とは言えないハードウェアによるサポートを必要とする.

表 2に, ソウトゥースレイクにおける設計上の選択をまとめた.

表 2: Sawtooth Lake における設計上の選択

ルール	「トランザクション・ファミリー (transaction families)」
唯一性	ナカモト・コンセンサス (PoET ベース)
存在証明	ハッシュチェーンと PoET (ハードウェアサポートが必要)
正当性	「トランザクション・ファミリー (transaction families)」

[6] ビザンチン障害は, プロトコルからの任意の逸脱であり, 共謀なども含み障害の種類について前提を置かない.

3.2.4 ハイパーレッジャー・いろは (Iroha)

「いろは」[8] は, 日本のスタートアップであるソラミツにより貢献されたコードにもとづく分散レッジャーである.

この分散レッジャーはシンプルな構造を持ち, かつモバイルアプリケーションの開発を前提に設計されている. また, 独自の BFT 系コンセンサスアルゴリズム, およびピアを評価する評判システムをもつ.

表 3に, 「いろは」における設計上の選択をまとめた.

表 3: Iroha における設計上の選択

ルール	サンドボックス JVM 上での「チェーンコード (chaincode)」
唯一性	Sumeragi (BFT)
存在証明	マークル木
正当性	公開鍵を埋め込む構造

3.2.5 コーダ (Corda)

「コーダ」[16] は金融系の分散レッジャーとして R3 コンソーシアムにより開発されている.

その他の分散レッジャーと異なり, コーダは, その技術が解となるべき「問い」を明確にしている. その問いとは, 金融上の契約に関し, 「私が見ているものはあなたが見ているものと一致しており, 我々はどちらもそのことを知っていて, かつ監査にも同じものが見えていると知っているという状態をいかに作り出すか」というものである. その意味で「空中」とは契約の当事者たちおよび監督者が関わる範囲であり, コーダでは全体のコンセンサスという概念を捨てていると考えられる (すなわち分権化の余地がある).

分散システムには CAP 定理 [6] にもとづく不可能性[7]があり, ブロックチェーンは可用性のために一貫性を犠牲にする設計になっているが, コーダでは, 逆に一貫性のために可用性を犠牲にするかたちでも動作できるように設計されていることが表明されている (金融の応用では一般に後者が望ましく, そうした応用を視野に入れた各分散レッジャーでも同様な設計が採られているはずだが, 設計の意図が明白に伝わってこない).

表 4に, コーダにおける設計上の選択をまとめた.

表 4: Corda における設計上の選択

ルール	サンドボックス JVM 上での実行 法的文書 (契約書) とのバインディング
唯一性	プラガブル
存在証明	契約の相手および監査と共有されることによる実現か
正当性	UTXO 構造および X.509 PKI

[7]一貫性 (Consistency), 可用性 (Availability), 分断耐性 (Partition-tolerance) は 3 つ同時に実現できないという不可能性. 論理的に正しいが, ウェブアプリケーションではネットワークの分断を事実上無視できるような構成も可能である. しかし, P2P システムでは全体を統一的に制御できないため, 分断の可能性を無視できない.

コーダのコードは公開されており, 今後はハイパーレッジャーの一部となる見込みである.

3.2.6 タングル (tangle)

「タングル」[15] は IoT への適用を見据えた分散レッジャーであり, ブロックという概念を捨て, 取引が個別に過去の幾つかの取引を承認する有向非巡回グラフの形態を採る. すなわち, ブロックチェーンが取引の全順序を形成・維持しようとするのに対し, タングルでは半順序を形成することになる. 「空中」は単一の空間ではなく, 枝分かれし, 分権のための構造をもち得る.

表 5に, タングルにおける設計上の選択をまとめた.

表 5: tangle における設計上の選択

ルール	IoT 向けマイクロペイメント「イオタ (IOTA)」
唯一性	トランザクション間の署名関係の DAG (有向非巡回グラフ) による確率的保証
存在証明	トランザクション間の署名関係の DAG による
正当性	独自構造と考えられる

3.3 将来の分散レッジャーに向けた提案 — 課題の解決・解消に向けて

ここで, これまでに得られた知識をもとに, 今後新たに分散レッジャーを設計する場合, どのようなものにすべきかという提案を行いたい.

公共財の公正な運用のために適しているという, 空中約束固定装置としての性質を活かすためには, オープンでパブリックな分散レッジャーにこそ意義があると考える. そのような新たな分散レッジャーの設計では, 同様にオープンでパブリックな仕組みであるブロックチェーンの持つ課題を一通り解決または解消することが期待される.

実時間性の課題 :

ブロックチェーンは現実と同期して動作できないが, それはナカモト・コンセンサスに大きな理由がある. 作成にあたって最もコストが投入された履歴が正史として採用されるというこの仕組みでは, トランザクションやレコードを後追いでしか認められない.

ナカモト・コンセンサスは唯一性の保証のための機構であるので, これを即時性のある仕組みで置き換える必要がある. ひとつの考え方は, レッジャー上で取り扱われる各々のアセットに責任をもつ主体が当該アセットの状態遷移の唯一性を保証するという方式である.

秘匿性の課題 :

ブロックチェーンの内容が秘匿されないのは, トランザクションやレコードの正当性の検証を無関係な第三者に委ねているためである. コーダで提案されているように, 当事者が正当性を検証するのであれば, その内容は当事者以外に対して秘匿できる.

ただし, コーダでは X.509 証明書を用いる PKI を採用しており, これは現行の商慣習に照らして妥当と言えるものの, より自律分散的な公開鍵証明の採用が望ましい. かといって, ビットコインで採用されている

ような, 公開鍵のダイジェストを識別子とする方法では, 対応する秘密鍵が失われたときにアセットの制御権が永久に失われることになる. 公開鍵と識別子は何らかの方法で分離しておく必要がある.

スケーラビリティの課題およびワンネスの罠：

ブロックチェーンのスケールアウトの困難性とワンネスがもたらす問題には共通の要因がある. それは, 分権できない構造による欠点だということである. 逆に, 分権できるかたちで同様の技術を実現することには, 大きな期待と可能性がある.

スケールアウトできる仕組みとしては, 前述のよう分散 KVS, もしくは DHT(分散ハッシュテーブル) の採用を考えることができる. また, レコードの実体として大きなデータを扱う場合にはそうしたデータを保存するストレージも必要となるが, それも KVS に保存することを考えることができる.

分権を実現するためには, 近傍性を考慮できる設計が望ましく, DHT に関する既存の一連の研究 [25] を参考にできる.

インセンティブ不整合性：

インセンティブ不整合性の課題については, 通貨ではなく, アプリケーションのレベルでインセンティブが提供される必要がある. すなわち, システムの維持に資することで, その貢献を行った者に対し, すべてのアプリケーションに共通するような価値が得られるようにインセンティブを設計することが肝要である. そのためには「正当性」「存在証明」「唯一性」「ルール」のレベルで考える必要がある.

自分が投入するトランザクションやレコードでこれらの機能が必要な場合は, 他者が投入するトランザクションやレコードについて, 同じ機能を提供しなければならない (提供しない場合は自分のトランザクションやレコードが放棄される), といった, tit-for-tat (しっぺ返し) の機構を考えることができる.

表 6に, 提案する設計上の選択をまとめた.

表 6: 提案する設計上の選択

唯一性	アセットを負債と捉える場合の債務者が保証 (i-WAT 方式)[18]
存在証明	トランザクション間の署名関係による DAG の形態をとるヒステリシス署名 [26]
正当性	UTXO 構造 + 識別子と公開鍵を分離してレッジャー上に PKI を形成する [24]

4 来たるべき社会変容

ここで, ブロックチェーンや分散レッジャー技術が社会にどんなインパクトをもたらしつつあるか, そして未来においてどう発展するかを考えたい.

4.1 人類史における転機

「約束」は人間社会の基礎であり, 「空中約束固定装置」により, 人が約束を結びそれを実行に移していくやり方が変わっていくとするならば, そうした, 社会を下支える基盤の変化による影響を受けるのは, 何も金融機関だ

けに限らない．一般化するならば，人々が共同で何かをしたり業を起こす (起業する) 方法が変わっていくことになる．

現在，起業と言えば会社づくりであるが，人類史に残る会社の代表格は「東インド会社」だろう．これは初の株式会社と言われる．すなわち今，人類史に残っているのは，現在の会社の仕組みの起点となる会社なのである．とすれば，次に人類史に残る会社は，近代的な株式会社を終焉させる形態を採ることになるだろう．

そのような会社のかたちとして有力だと筆者が考えるのが「自律分散組織 (DAO; Distributed Autonomous Organization)」，すなわち，経営が自動化された組織である．実は，例えばビットコインは DAO の具体例だと言われる．ユーザを株主，コインを株式，ブロックチェーンを維持する参加者であるいわゆるマイナー (採掘者) たちを従業員と考えれば，ビットコインのプロトコルは，株式の移転を業とするその組織の経営の仕方を記述していると見なすこともできるからである．

DAO のような考え方を一般化すると，「法」を技術の提供者が定義するということになる．ただし，Lawrence Lessig (サイバー法学者) がかねてから指摘している [12] 通り，コンピュータソフトウェアには元々そういう力があると考えられる．

4.2 地球規模 OS

筆者は，2007 年頃，仲間らとともに「地球規模オペレーティングシステム」[21] の概念を提唱した (図 5)．これは，地球上の資源と人間との関係をコンピュータとユーザとの関係になぞらえ，現在は OS に当たる金融・貨幣経済システムを時代遅れにし，人類が真っ当に資源の共有・共用を行うための基盤である．地球規模 OS は，人々が

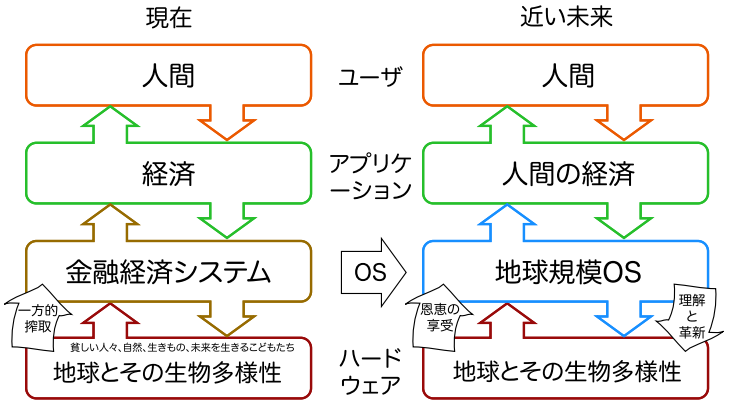


図 5: 地球規模 OS

アプリケーションとして新たな業を起こすための基盤として，何らかの決済システムを内包し，かつ，プログラミング言語・プログラミング環境を内包することになる．そして，人的資源を含む地球上の資源の会計システムを提供し，人々はその上で新たな「法」を定義できることになる．

こうした基盤づくりへの道は，地球規模 OS という言葉で呼ばれるかは別として，すでに始まっているようにも思える．

現在は未だ，社会を変えたい，と考えたときに人々が起こす行動として，「選挙に立候補するなどして政治を志す」「公務員になって行政に参加する」「起業する」あるいは「非営利活動を立ち上げる」といった方法がばらばらに存在している．すなわち，政府，営利企業，非政府/非営利 (NGO/NPO) というセクターが独立している．と

ころが, 各種のハッカソンに代表されるように, これらの方法やセクターを統合するかのように, 「アプリをデザインして社会に投入すると, そのエージェントとして人々が働くことで社会の課題が解決される」という道筋ができ始めている.

この道筋は, ブロックチェーンの動向とも無縁ではなく, オープンソースで開発が進められている「イーサリアム (Ethereum)」[2] は, 第 1 世代のブロックチェーンの課題に対しある程度の取り組みを見せると同時に, そこにプログラミング言語を載せ, 分散アプリケーション, 特に履行が自動化された契約としてのスマートコントラクトを開発・実行するためのオープンな基盤として作られている.

4.3 貨幣経済の衰退がはじまる

スマートコントラクトをオープンでパブリックな空間に登録・実行できるならば, 任意の約束を空中に固定できるのであるから, 地球という, 現代の人類にとっては究極的な公共財を公正に取り扱うための新たな基盤として用いることができることになる. イーサリアム自体にはビットコイン同様に課題が山積しているとしても, こうした基盤が現れることで, 旧来の金融貨幣経済における仕組みは時代遅れになっていくと考えられる.

一方, 例えば通貨への応用に限ってみても, こうした基盤により様々なコミュニティや用途に向けたデジタル通貨システムの作成が容易となり, 利用可能な通貨が乱立することになると, 人間が平易に取り扱える選択肢の数を上回るおそれがあり, 一見, 私たちの不利益になるようにも見える.

しかし, 例えば Amazon Go[1] のような店舗が一般化していき, 人々が支払いという行為を意識せず, 各店舗で利用できるクーポン, ポイント, 地域通貨といったものがその人に (スマートフォンのようなかたちで) 随行するソフトウェアエージェントにより, その人のポリシーに従って適切に利用されていくのであれば, 人間にとっては貨幣は見えなくなり, 気にしなくてもよいものとなる. おそらく, ポリシーに従って, ソフトウェアエージェントからは行動の提案も行われるだろう. 例えば, 「今日のお昼は, ここから少し歩くけど, あのケーキ屋に行ったら？今あなたが食べたいだろうメニューがあるし, お得だから」といったようにである. さらに, そこにシェアリングエコノミーが加われば, ソフトウェアエージェントの提案に従って見知らぬ人にコーヒーを一杯ごちそうすることで, 後に自分も見知らぬ人から助けられるといった, SF 作家 Bruce Sterling による短編小説「招き猫」([19] に収録) と区別がつかない世界が出現する. 本人は助け合いに参加しているだけなのだが, 裏側でアカウンティングが行われ, 善行が報われるように調整されるのである.

かくして, 貨幣は見えなくなり, 背後でのシェアリングエコノミーの拡大により, 貨幣経済の衰退が本格的にはじまる. このことは貨幣経済自身のロジックに照らして極めて整合的である [22]. 貨幣経済の中では, 貨幣を使わない行動こそが, 最も望ましいからである.

4.4 サイバーフィジカル社会

本当に社会のインフラとしてスマートコントラクトが使われていくためには, 物理的な世界との接続はどうしても必要である. 例えば, 遺言を自動的に実行するためには, システムが「人の死」という契機を正しく捉えることが必須となる. カーシェアリングで用いられるためには, 運転免許証や乗用車のキーとシステムが接続される必要がある. Amazon Go のような店舗であれば, 利用者が商品を店外に持ち出すということが正しく認識されなければならない.

これは, スマートコントラクトの実用化には, 「サイバーフィジカル (cyberphysical)」な環境が前提になるということを意味する. サイバーフィジカルとは, 広く捉えれば, 様々な (人工知能によりアシストされた) センサー (検

知器)/アクチュエーター (駆動装置) や, スマートフォンなどの携帯デバイスや, あるいは法制度などによって, 人間の生活環境を支える社会インフラとコンピュータネットワークとが互いに密接に繋がり合っていることを指す.

そして , ひとりひとりがスマートフォン等を持ち歩き, 情報環境と常に密接に繋がりながら生きている現在, 我々は, すでにサイバーフィジカル時代への入口に立っていると言えるのである.

スマートコントラクトは, 生活空間におけるプロセッサの数ほどもあるかもしれない. エアコンや電子レンジといった世の中に存在するすべての家電や, 乗用車, 時計, ロボット, 電車, 航空機, あるいはエレベータなど , コンピュータを内蔵するありとあらゆるものが, 将来的にはスマートコントラクトに基づいて挙動を決めるかもしれない.

「空中約束固定装置」としてのプラットフォームは, そうしたサイバーフィジカルな世界を前提にすると同時に, サイバーフィジカルな世界のための基盤になり得るのである.

5 分散レッジャー技術と社会の未来

まとめとして, 今後我々が課題とどのように向き合い, どのような社会の変化を目撃することになるのか考えたい.

5.1 露見したガバナンスの課題

2016 年 6 月 17 日, イーサリアム上に作られた自律分散投資ファンド The DAO のコードの脆弱性が突かれ, 360 万 ETH(50~60 億円相当) というデジタルコインが盗難に遭った. イーサリアムの開発・運用コミュニティがこの事件に対処するための選択肢としては, チェーンの互換性を維持して窃盗犯のアドレスのみを凍結する (ただし盗難された資金は戻らない) といった手段もあったが, 結果として「盗難が無かったことにする歴史の書き換え」が選択され, 7 月 20 日に実行された. これは強権発動とも言え, それを支持しないユーザたちが書き換え以前のチェーンの継続使用を固持する分裂騒ぎが起きる等, ブロックチェーンにおけるガバナンスの課題を浮き彫りにする結果となった.

5.2 自動化される未来へ

そのように, 技術が実際に社会で使われていく中で, 課題を明らかにする様々な事件が起きていく一方で, 約束は本来的に空中に置かれる必要があるし, ブロックチェーンが可能にするとされる世界には, やはりインパクトがある.

自動化は, 今後発展する人工知能の助けを得て, 社会のあらゆる場面に浸透していくと思うが, 知力の面で人間を凌駕し得る人工知能は, いつどのように人間の社会が定めたプロトコルを逸脱するかも分からず, 社会という分散システムにおける潜在的なビザンチン障害ノードであるとも言える. そうした相手との約束をどう結んでいくかということも, 今後は考えていかなければならないだろう.

ブロックチェーンや分散レッジャー技術とそのガバナンスには課題が山積しており, 現在のかたちからの変化は免れない. しかし, 空中に約束を固定するための何らかのプラットフォームが, 未来社会における自動化, そして地球という公共財を私たちが公正に使っていくための基盤として, 大きな役割を果たしているだろうことは間違いないと考える.

参考文献

[1] Amazon.com, Inc. Amazon.com:: Amazon go. https://www.amazon.com/b?node=16008589011.

[2] Vitalik Buterin. A Next-Generation Smart Contract and Decentralized Application Platform, 2014. https://github.com/ethereum/wiki/wiki/White-Paper.

[3] Miguel Castro and Barbara Liskov. Practical Byzantine Fault Tolerance and Proactive Recovery. *ACM Transactions on Computer Systems (TOCS)*, Vol. 20, No. 4, November 2002.

[4] Allen Clement, Edmund Wong, Lorenzo Alvisi, Mike Dahlin, and Mirco Marchetti. Making Byzantine Fault Tolerant Systems Tolerate Byzantine Faults. In *Proceedings of the 6th USENIX Symposium on Networked Systems Design and Implementation (NSDI '09)*. USENIX Association, 2009.

[5] Everledger.io. Everledger - beta. https://www.everledger.io.

[6] Seth Gilbert and Nancy Lynch. Brewer's Conjecture and the Feasibility of Consistent, Available, Partition-tolerant Web Services. *ACM SIGACT News*, Vol. 33, No. 2, June 2002.

[7] Hyperledger Project. Hyperledger Whitepaper. Available electronically at https://docs.google.com/document/d/1Z4M_qwILLRehPbVRUsJ3OF8Iir-gqS-ZYe7W-LE9gnE/pub.

[8] Hyperledger Project. iroha. https://github.com/hyperledger/iroha.

[9] Hyperledger Project. sawtooth-core. https://github.com/hyperledger/sawtooth-core.

[10] IBM Corp. Hyperledger fabric. http://hyperledger-fabric.readthedocs.io/en/latest/.

[11] Leslie Lamport, Robert Shostak, and Marshall Pease. The Byzantine Generals Problem. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, Vol. 4, No. 3, July 1982.

[12] Lawrence Lessig. *Code: And Other Laws of Cyberspace, Version 2.0*. Basic Books, 2006.

[13] Linux Foundation. Hyperledger – blockchain technologies for business. https://www.hyperledger.org.

[14] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. Available electronically at http://bitcoin.org/bitcoin.pdf.

[15] Serguei Popov. The tangle. Available electronically at http://iotatoken.com/IOTA_Whitepaper.pdf.

[16] R3. corda. https://github.com/corda/corda.

[17] R3. Introducing R3 Corda^{TM}: A Distributed Ledger Designed for Financial Services. http://www.r3cev.com/blog/2016/4/4/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services.

[18] Kenji Saito. *i-WAT: The Internet WAT System – An Architecture for Maintaining Trust and Facilitating Peer-to-Peer Barter Relationships –*. PhD thesis, Graduate School of Media and Governance, Keio University, February 2006.

[19] Bruce Sterling. *A Good Old-Fashioned Future*. Spectra, 1999. (小川 隆 訳, 「タクラマカン」, ハヤカワ文庫 SF, 2001).

[20] 黒田東彦. 【挨拶】情報技術と金融—中央銀行の視点—. 日本銀行 第 1 回 FinTech フォーラム, 2016. https://www.boj.or.jp/announcements/press/koen_2016/ko160823a.htm/.

[21] 斉藤賢爾. 地球規模 os の実現に向けて ～ ポスト石油・石炭ピーク時代における情報ネットワーク ～. 信学技報 IN2010-132(2011-1), pp. 79–84, 2011.

[22] 斉藤賢爾. インターネットと金融 — 弱体化する貨幣経済 (角川インターネット講座 10 第三の産業革命 経済と労働の変化 第 9 章). 角川学芸出版, 2015 年 2 月.

[23] 斉藤賢爾. ブロックチェーン，分散レジャー技術と社会の未来 – 空中約束固定装置のある暮らし –. 情報処理 2016 年 12 月号「特集 社会を変えるブロックチェーン技術」, pp. 1210–1215, 2016.

[24] 斉藤賢爾. ブロックチェーンにおける識別子と鍵管理. 日本銀行 第 1 回 FinTech フォーラム, 2016. https://www.boj.or.jp/announcements/release_2016/data/rel160831b5.pdf.

[25] 斉藤賢爾, 高野祐輝. 現実世界の条件に適応する分散ハッシュテーブル. 電子情報通信学会論文誌, Vol. J96-D, No. 6, pp. 1433–1446, 2013.

[26] 洲崎誠一, 松本勉. 電子署名アリバイ実現機構 — ヒステリシス署名と履歴交差. 情報処理学会論文誌, Vol. 43, No. 8, pp. 2381–2393, 2002.