ブロックチェーン研究

領　内　　修*

The Study Of Blockchain

Osamu RYONAI

要　旨

「ビットコイン」の背景には、「ブロックチェーン」と言う画期的なインターネット技術がある。ブロックチェーンは、『「情報の移動」から「価値の移動」のインターネット』を成立させ、新時代を開いた。本稿では、この「ブロックチェーン」を考察する。テーマは「帳簿の世界での不正がブロックチェーンで防げるか」だ。その考察方法として、アナログとデジタルの両世代での不正防止を考えたい。帳簿への記録と言う観点から、人が長い間築き上げてきた不正防止の工夫に焦点を当て、その様々な工夫が電子データの新時代においても通用するのか？　システム上では不正防止万能的な役割を期待されているブロックチェーンだが、真に万能なのか？　万能とすれば、どんな役割で、金融や経済・社会の近未来にどんな影響を与えるのかをも検討しよう。

【キーワード】　＊価値のインターネット　　＊デジタル・ネット公証人
＊帳簿を背負った初の通貨　　＊スマートコントラクト

Ⅰ　はじめに

ここ 30 年の社会の変遷を振返る時、我々人類は 1981 年／パソコン、1995 年／インターネット、2009 年／仮想通貨　2015 ／仮想現実・人工知能　と言う画期的な技術を得てきたことに気付く。

中でも、世界を国境無く、瞬時に結ぶインターネットの普及には情報の受発信で、大きな恩恵を受けた。また、仮想通貨ビットコインを誕生させた、新インターネット「ブロックチェーン」と言う重要技術もある。ブロックチェーンは【「情報伝達」から「価値移動」のインターネット】を成立させた画期的なデータベースで、本稿では、この「ブロックチェーン」を考察する。

テーマは「帳簿の世界での不正がブロックチェーンで防げるか」だ。

その考察方法として、アナログとデジタルの両世代での不正防止の流れと方法を考えよう。

そこでは、銀行業務と企業経営経験に基づき「紙ベース」と「電子データベース」の不正行為の具体的事例の検討から、問題点抽出と解決方法を見てみよう。一方、ブロックチェーンと言う

2018 年 9 月 12 日受理　*社会学部総合社会学科教授

新データベースの技術を検証し、それが持つ「分散台帳技術」効果が、次世代の不正防止に役立つかを考えよう。この論文は、人類が築いてきたアナログ世代の不正防止の工夫や技術が、デジタル世代にも通用するかを検証し、顕現化して来る問題点が解決出来るかを検討することを目的とする。更に、今後の社会や経済・金融にどのような影響を与えるのかを検討するものである。

Ⅱ　帳簿の不正を考える

＊不正の種類

昨年から本年央（2018）にかけて、モリカケ問題や財務省高官による下記の（1）～（5）の問題が表出し、政治問題化して記録への不正行為が浮き彫りにされた。その前後にも、国内外の大企業による「粉飾決算」「不正データ」「不正会計」等、数字の改竄・偽造が多く顕現化した。

IT バブル崩壊時の米国エンロンやワールドコムの巨額粉飾決算、6 年前からの東芝買収案件の減損処理での不正決算処理も意図的な数字改竄に当たる。これらは法的観点から、どのような犯罪になるのか？　法律上、刑法第 17 章「文書偽造の罪」には、次の条文が規定されている。

詔書偽造等の罪	（154 条）	公文書偽造等の罪	（155 条）
虚偽公文書作成等の罪	（156 条）	公正証書原本不実記載等の罪	（157 条）
偽造公文書行使等の罪	（158 条）	私文書偽造等の罪	（159 条）
虚偽診断書等作成罪	（160 条）	偽造私文書等行使罪	（161 条）

電磁的記録不正作出及び供用の罪（161 条の 2）

「改竄」「捏造」「隠蔽」等は、「特定不正行為」と言う言葉でまとめられるが、それにしても不正行為の種類・分類がこんなに多いとは驚きだ。（以下「文部科学省のガイドラインより」）

（1）捏造　：　存在しないデータ、研究結果等を作成すること
（2）改竄　：　研究資料・機器・過程を変更する操作を行い、データ、研究活動によって得られた結果等を真正でないものに加工すること
（3）盗用　：　他の研究者のアイデア、分析・解析方法、データ、研究結果、論文又は用語を当該研究者の了解又は適切な表示なく流用すること
（4）隠蔽　：　真実の情報を隠すこと
（5）偽装　：　隠すのではなく、偽りの情報を真実情報であるかのように伝えること

上に言う「記録する」「記録した」ものを「不正に処理する」とは、どのような処理をすることで産まれてくるのであろうか？　　以下の具体的な事例で検証してみよう。

＊事例検証

「不正に処理された」に該当する実際の 4 事例から、問題点や解決の可能性を考えよう。

①伝票間引きによる使い込み

事　象・・・伝票処理を一手に行っていた会計担当者による入金伝票処理中のごまかし。伝票をズタ袋に入れて個別の綴じや整理を行わず。作業途中、入金伝票 10 枚中 2 ～ 3 枚を入金処理せず、その分を捨て、該当資金を自分のポケットに入れ、長年にわたり、数千万円を横領。カネの出入りを担当一人に任せて、長期間、監査も行わず、放置されたため、多額となった。損害金は未回収。

問題点・・・処理伝票の間引き。間引き伝票はズタ袋に入れておき、ばれない時点でゴミとして伝票を処理。入金帳への記帳の前段階の不正であり、記帳していないため、営業担当の集金帳との整合チェックが無ければ、露見しない。

解決可能性 ･･･ 意図的な伝票未作成による不正　　入金処理（伝票作成）前不正

②他人印押印による伝票作成

事　象・・・昭和 55 年銀行 A 支店での事件。女子行員と男性主任による 2 千万円の横領上下関係にあった男女二人が、新人女子行員の印鑑を残業時に勝手に使用、作成者・再鑑者・主任者の 3 者欄に押印、偽伝票を作成、出金伝票作成の上、新設の口座に入金し、横領したもの。

問題点・・・別人の印鑑を勝手に流用して何度も押印した伝票偽造、元帳にウソの記載をした。取引そのものが詐欺。新人行員が監査の折、『この伝票に覚えがない』と言ったことから発覚。二人は懲戒解雇。資金は回収。

解決可能性 ･･･ 伝票偽造、取引不存在の詐欺行為。　　伝票作成時不正

③類似の案件になるが、昭和 59 年 M 銀行 L 支店「支店長による 24 百万ドル横領事件」。その手口は、②と同様、2 年間一度の休暇取得もなく、数人の部下の休暇時に印鑑を勝手に流用し、偽造伝票で出金を重ね、ラスベガスで放蕩した。監査による発覚。　　伝票作成時の不正

④旅費搾取

事　象・・・月に 2 ～ 3 度の同一地へのカラ出張による偽装伝票作成。これを部下に正式処理させ、1 千万円の横領。出張に疑問を抱いた隣席の内部告発で発覚

問題点・・・伝票に対するデータの正確さや整然性に問題は無いが、伝票作成自体が詐欺。問題は、内部告発無しで発覚したかによる。全く露見しなかった可能性も。

解決可能性 ･･･「電子データ帳簿」においても、内部告発的なことは可能なのだろうか？

伝票作成前・中・後の連続不正に相当

＊各帳簿の不正

各帳簿とは、「紙の帳簿・電子データの帳簿」を指し、「記録されたもの」の意であるが、ここでは主として、カネを扱う伝票類をさす。カネの出入りを記録するデータがアナログ（紙の帳簿）であれ、デジタル（電子データの帳簿）であれ、それを正確に記帳・記録し、記憶化させてきた

ものが、帳簿である。本項で言う「各帳簿の不正」の検討は、ブロックチェーン登場以前を言う。

【取引記録の流れ『取引→仕訳→補助簿→総勘定元帳』】から帳簿上の不正を考えよう。

補助簿は取引を日付順に記帳する帳簿のことだが、総勘定元帳はそれらの取引を勘定科目ごとに総て記帳する帳簿を指す。各勘定科目の残高の確認帳簿であり、期末にはこの帳簿をベースに決算書を作成する。記帳の手順は①仕訳し、②補助簿に記入、③総勘定元帳に転記の流れになる。

1975 年外国為替専門銀行の東京銀行に入行、初任店は大阪支店計理課（経理･計算課）だった。計理課には、その日の大阪支店各課の取引伝票がすべて集結する。朝 9 時から 13 時までの午前の分と 13 時から 17 時までの午後の取引分に 2 分して整理し、それらを一枚の総勘定元帳に転記する。各課伝票は、課名が識別できるように番号の色が赤・青・緑等と異なり、取引番号順に印刷済みの順番号のものを使うので、二重番号や偽造番号が入り込む余地や偽伝票は混じらない。営業カウンターの預金課や外国送金課は、現金の受け渡しが行われる場所であり、ここでの出入金伝票は非常に大事に扱われた。実務での伝票記入は「入金」･「出金」･「振替」の 3 種類が用いられ、「入金伝票」は現金が入る取引に使用し、「出金伝票」は現金が出る取引に使用する。

一方、「振替伝票」は　出入伝票以外に使用するすべての伝票を言い、各取引課で使用する。簿記では、振替伝票（入金伝票・出金伝票まで含めて）の中に全ての情報があり、振替伝票を正しく記載すれば、あらゆる帳簿や財務諸表（貸借対照表・損益計算書など）は作成出来る。

伝票・補助簿や総勘定元帳の各作成時点前後で起こる不正は、先の事例検証で見た通り、

⑷伝票作成前の不正（預かった金の詐称や入出金の金額誤魔化し等を指す）
⑹伝票作成中の不正
⑹伝票作成後の不正（伝票を束ねる時点）

の 3 つになる。

伝票・補助簿の転記済み票・帳は、各課の手を離れて、総務課や庶務課の手に委ねられる。

各課分を地下 2 階の庶務課別室に持ち込み、職員が各課別に各伝票の左端上を一枚ずつ糊付けし、100 枚ごとに「和綴じ」していく。ここでは伝票の束への「改竄や抜取り、追加差し込み」が起こらぬ工夫がされていた。前述の個々の取引伝票を各課毎に識別し、伝票の偽造や取引の順に応じた不正不可の工夫を「不正防止第 1 弾」とすれば、それに続く伝票を「束」として閉じる時点での同様の工夫は、「不正防止第 2 弾」と言える。

これらの伝票に基づいて作成された各課別の総勘定元帳は、大阪支店一日の取引結果を示す報告書となり、これが深夜便で東京本部に運ばれ、東京の経理部が丸 2 日遅れで、「某月某日の銀行総勘定元帳」を作成する。これを作成することで、銀行本体の資金繰状態も把握出来た。

この総勘定元帳作成は、昭和 50 年当時の話であり、既に電子計算機が導入されており、オフラインからオンラインになる段階だった。私には、得難い経験になったが、コンピュータ導入に伴う電子データ総勘定元帳と時期的に最後に当たる紙ベース総勘定元帳が併用されていた場に居合わせたことになる。

「紙➔オフライン（電子）➔オンライン」の流れを　総て経験できたことは、良い経験だった。

上記のような(a)(b)(c)と言う 3 時点での不正を認識し、それを防ぐ努力をしても、銀行・企業の勘定系を取り巻く事故や事件は残念ながら、昔から減ることなく、逆に昨今は増加傾向にある。

これらの事件・事故は、伝票や総勘定元帳の作成段階での操作で起こるものも数多くあるが、

(d)伝票作成前の取引交渉時（企業の談合）やコミュニケーション時（インサイダー等）
(e)財務諸表完成前後の役員による故意の不正

も、昔に較べ、増加している。

(e)については、「財務諸表の利益処分➔剰余金の処分」が、経営者判断に基づく記載であり、「引当金の作成➔計上」は、『将来発生する費用・損失の見積計上』であるため、記載の是非は当事者判断となり、恣意的な不正行為が目立ってきている現状を踏まえての指摘である。

上記の通り、一伝票から財務諸表完成時（a）～（e）まで、不正時点を指摘できるが、それらに対しては、厳重に改竄や偽造が起こらぬよう種々工夫がされてきた。

しかし、現実は先の事例に見るように、より巧妙に、より大胆に不正行為が行われている。

紙ベース帳簿の不正は、防止の取組も様々あったが、容易くは防げないことが確認できた。

では、コンピュータ導入後の電子データ（電磁的記録）帳簿の不正防止はどうだろうか？

電子データベースでは、不正は防げ、改竄や偽造は起こらないか？　起こらなかったか？

残念なことではあるが、紙もデジタルも不正（a）（b）（c）は、同様に起こり、事務処理過程での不正は防げなかった。伝票作成前(d)や(e)故意(e)の不正は、紙であれ、電子であれ、同様である。

それでは、帳簿を離れた「簿外世界」では不正はどんな状況にあるのだろうか？

＊簿外不正

簿外不正を考える材料は、平成 19 年（2007）に発覚した社会保険庁の「失われた年金」記録問題が相応しい。これは、金融機関では考えられない事件で、納付された資金、集めた金がどこに行ったか　不明で分からない？と言う事件である。帳簿上での不正分類（a）の範囲外に属し、伝票作成云々の前に「集めたはずのカネが存在しない」と言うものになる。

社会保険庁には、正確な帳簿記録（事務処理や管理）体制が存在しなかったのだろうか？

一旦、集めたカネの入金記録が確認出来ず、消えて無くなってから、調査・追跡して分かるものではないだろう。　「年金が失われる」や「消えて無くなる」って、どこかおかしくないか？！

この時世に「カネの神隠し」は通用しない。誰かが盗ったものだろうが、集めてきた段階での手間暇のかかる最初の「カネ集め」➔「帳簿つけ」をおろそかにしたのだろうか？

帳簿に関する私見を述べれば、帳簿は「カネの存在のみなもと」で「カネを扱う基本」である。

この事件はその基本を外したものと言わざるを得ない。この事件の教訓は、帳簿そのものが不正の温床にもなり得るのだが、取扱う側の人間にはもっと多くの問題があると言うことだろう。

民間金融機関では、現金を扱う部署と、バックオフィスたる管理、監督する場所は明確に分け、

大蔵検査や日銀考査の第三者の目も入れて、取扱い・管理・検査が個別機能する形をとっていた。

最近話題の商工中金問題もそうだが、各省庁が大蔵の向こうを張って作った省庁金融機関は、機能のどこかに欠陥があったか　機関能力が低いまま発進したと言えるのだろう。

そもそも集めた資金の行方が分からないことは通常の銀行では絶対に無い。

集めた金を悪意ある行員が横領する事件は数多くあったが、公的機関が集めた資金の存在そのものが不明と言うのは考えられない。処理方法を銀行に真似ても、根底に流れる「絶対的な記録＝帳簿付け」の姿勢が無ければ、カネを取り扱う資格は無い。記録が消えるはずがなく、ただ記録しなかっただけとしか考えられない。「意図してか」（政治資金に消えたか､流用されたか)､「意図せず」かは不明だが、残念ながら、この問題は、特定不正行為の（1）～（5）の罰則に該当しないし、帳簿付け以前の不正（a）の枠外で、不正行為に何ら変わりはないのだが、この様な簿外不正が存在することを改めて認識させられた大事件だった。

＊その他の不正

間違いを起こすはずの無いコンピュータによるデータ処理においても、新たな不正の出現があった。紙ベースでは存在しなかった「プログラムバグ」や「システムへの攻撃」「ハッキング」「コンピュータウィルス問題」がそれである。コンピュータ利用で、処理が簡便かつスピードアップしたが、不正が減少し、無くなった訳ではなく、逆に複雑で難解な組織犯罪不正の芽が産みだされた。世界の多くの金融機関はこれへの対処に多額のカネを使い、解決に苦心している。

平成 8 年 4 月 1 日　当時の三菱銀行と東京銀行が合併した。その約 1 年前から銀行のシステムをどちらの銀行コンピュータシステムに片寄せするかの検討を開始した。当然の事ながら、合併は対等であっても、人事はルールとシステムを握った方が覇者となる。優劣の結論を決めたのは法人・個人の取引口座数であった。6000 万以上の口座数を誇る「少品種大量処理」得意の旧三菱銀行の単機能型コンピュータ　VS　外国為替専門銀行として＄・£・ＤＭ等、多種多様な通貨処理をシステムに組み込んだ「多品種少量処理」を標榜する旧東京銀行の多機能型システムとの登用争い。貿易金融を必要とする大企業を中心とした 500 万口座数に留まる東京銀行のシステムは新設置の最新型だったが、採用結果は明らかだった。当然の事ながら、6000 万口座が稼働できないシステムは新銀行としては採用不可で、旧三菱銀行のシステムの採用になった。

ただ、この判断を行った時点では、処理数能力の優位性のみの判断であり、伝票処理の仕方や考え方（哲学）の違いに目が行かず、のちに種々の問題が出てくることに気付かなかった。

それは、単純な処理能力の質的量的の優劣ではなく、伝票処理法 or 処理哲学に大きな差異があり、次世代の銀行業務を担うには、採用システムはあまりに古いコンテンツであったことだ。

具体的には、①一枚の取引伝票が二つに分かれ、②左右の「入り払い伝票」が個別に対象振替相手伝票を求めて飛び交い、③入り払いの片側ずつの伝票集計が同時処理され、④その後、見つけられた振替伝票を集計、先の集計数字と整合する　と言う分割大量処理方法を指す。

片側ずつと振替伝票の 3 集計が合わないと、勘定元帳に記載できず、3 つが揃うまでには処理時間がかかるシステムだった。一方､旧東京の二頭立て馬車と称されたタンデムコンピュータは、伝票が分れず、一つの取引の右・左（資産項目・負債項目の　┬　この形をトンボと称する）が

同時に揃って一枚で動くため、片割れ伝票の相手方を探す必要なく、時間もかからず、高速処理が可能だった。逆にコンピュータシステム全体の容量が小さく、処理件数が少なかったことが難点だった。この容量を増やすには新設同様の多額の金を必要とした。同じような銀行コンピュータシステムと言っても、能力だけで比べられない大きな差異があり、簡単なシステム統合は出来ない。様々な金融機関の合併話が起こる中で、いずれの統合も、より大きな不正の懸念（バグ狙いと集計時間差を狙った外部からの不正アクセス等）を内包し、異質のコンピュータ同士を繋ぐことの困難さ、統合翌日から通常業務をスタートさせる危険性を認識する必要がある。

この状態に事務屋として携わる当事者の不安や懸念には大きいものがあると言わざるを得ない。

Ⅲ　ブロックチェーン登場

＊ブロックチェーンによる不正防止

「データ」を如何に瞬時に他者に送信出来るか？の命題に回答を出したのはインターネットだ。

現代社会は、インターネットの恩恵には種々浴してきたが、特徴は以下の通りだろう。

その良さは、①情報が瞬時に国境を超え、②情報発信者が個人でも可能で、③安価なコストで、大量情報の受発信が可能な点にあり、その欠点は、①匿名性・プライバシーが保てない②データ複製が簡単で、③流出情報は回収不可な事だろう。欠点は、コピペ全盛を可能にしてしまった。

長い人類の歴史で、瞬時にデータが行渡るという事は、インターネットがほんの 20 数年前に実現したばかりのものだが、同時に欠点も世界に拡散した。これを少しでも改善する手段があるのか？　との問いに応えたのが、サトシナカモトが発明した「ブロックチェーン」であった。

まず、最初に BTC に応用された「ブロックチェーン」は、旧のインターネットの持つ 3 つの欠点を防ぎ、欠点の代表である「コピーし放題・改竄自由・発信者の勝手自由」と言う厄介者を封じ込め、放逐する役目を負っていた。（論文完成 2008 年 10 月 28 日、BTC2009 年 1 月 3 日）

金が絡む話（通貨は当然）で、帳簿利用となると、全く旧インターネットは使えなかった。

このインターネットに「一大革命」を起こし、劇的に信頼を与えたのはブロックチェーンである。

ブロックチェーンは、「P 2 P ネットワークをベースに、ネット上の取引情報のすべてがブロックでつながって記録され、共有される仕組み」と定義される。この定義の中で、単なる仮想通貨のベース技術に留まらない「取引分散台帳」が実現されたことに注目しよう。

取引分散台帳は、二重譲渡を防ぐ元となる取引記録台帳の一つである。二重台帳は、一参加者が複数参加者に対し、同じ取引を何度も行うことを指し、コピーそのものである。そのコピー防止を可能にしたのは、P 2 P（Peer-to-Peer）で、中央集権でない分散型の通信アーキテクチュアを指し、参加者の対等通信に特徴がある。「P 2 P」と「コンセンサスアルゴリズム」（全体の合意形成によって承認された取引のみをブロックとして記録し、溜め、認められるため、二重台帳が起こらない工夫をみんなの合意を得て行った合意形成の仕組み）と「ハッシュ」[1)]（ハッシュ関数という計算方法を実行することにより、任意のデータを一定長の値に変換したもの）の 3 技術でブ

ロックチェーンは成立している。

更に、インターネットにおける「ブロックチェーンの位置づけ」も確認しておこう。

情報伝達の3つの良さをキープし、不正の3つの欠点を無くす　とはどういう意味か。

帳簿の改竄や偽造の不正行為をどう防ごうとしているのか？　4年前からの自分の研究ノートから、この分野で集めた言葉への疑問・言語の定義・造語　等の抜粋を拾うと以下のようになる。

・取引記録台帳　＝　ブロックチェーン　　・ネット上の仮想大福帳（デジタル台帳）
・記号化した情報をブロック（箱）に詰める　・正当性を担保（価値の鎖）
・デジタル・ネット公証人　　・価値の移動がネットで可能
・メリット：真正性・コスト削減　　・デメリット：容量・多数決問題（51％）
・金のみならず、物権・債権等の「資産」をネット上で動かすことを可能にする
・「信頼性」は「公的機関仲介不要」の可能性を持つ
・「いつでも　どこでも」場所を選ばず、スマホ・携帯等で接続出来る

「仮想大福帳」や「デジタル･ネット公証人」は、この技術をより理解し易く考えた私の造語だ。

今日、ブロックチェーンは、信頼のネットワークと位置付けられて、改竄や偽造が入り込む余地がない。「紙」や「電子」の帳簿作成前・作成中・作成後の各時点での検討では、いずれのデータも、現時点では、不正排除が可能になる。しかし、将来はどうだろうか？　3ベース技術に基づいて作成されたブロックに帳簿が乗り、システムに守られれば、将来も対応可能か？

と問われれば、一概にそうは言えないことを記しておこう。

昨今では、ハードとソフトの進化の速度が尋常ではなく「今日出来ない事も明日出来るようになる」時代だ。ハード面では､従来のコンピュータのハッシュ値の計算能力をはるかに上回る「量子コンピュータ」の出現がその懸念である。スーパーコンピュータをはるかに上回る能力があれば、想定外のことが起こり、ブロックチェーンが成立しなくなる惧れもあり得る。

ソフト面では、昨夏から何度も起こっているBTC分裂騒動のポイントである「ハードディスク容量」と「処理時間」の問題がある。それは、10分間で2,000の情報データの現行処理能力に対するマイナー（採掘者）らの不満が原因で、もっと容量を大きくし、時間短縮を諮りたいグループがそれぞれ個別に既存に仕掛けたものだ。10分間を秒単位に縮め､2,000を20,000等の10倍、20倍にアップスケールする模索をしたのが分裂要因だ。取引数が激増することで、拡張性懸念が顕著になった。ブロックチェーンの長大化が参加者の個別PCの容量を上回り、P2Pネットワークの現状利用では、大量取引に対応出来なくなりつつある。又、10分ごとのブロック作成時間は、即時性が必要とされる金融取引決済には全く向かない。プログラムから言えば、合意形成を築くには6ブロックが必要なため、10分×6＝60分かかることになる。各ブロック完結に1時間は待てない。又、改竄は可能だと言う説も浮上してきた。株式会社のM＆A同様、全取引の51％を取得すれば、取引の改竄は可能になる。世界中に存在するBTC取引者を確認し、持ち分を高値で買い取り、過半を占めて取引チェーンを改竄し我が物にする。そうまでする値打ちがあるかどうか疑わしいが、先々、BTCの高値予想からの説で、無視出来ないらしい。

カネにまつわる世界では、次から次へと様々な不正の種がつきないものだ　と感心も得心もする。

＊ビットコイン（＝ BTC）誕生

2011 年会社の IR（インベスター・リレーションズ＝投資家対応）担当として、ニューヨークで初めて知った BTC の存在。　最初は、単なる米国内での流通の電子通貨だと考えていた。

周りで、使っている人もおらず、『国境を越える電子通貨』って、又　米国人はバブルの素材を創生したのか！と言う程度の認識だったが、来日する金融アナリストたちの説明の影響もあって、ギリシャ経済危機（2012 年）辺りから、このコインの動向をフォローするようになった。

「価値の移動」「カネの移動」がネット上で初めて可能となったその歴史と技術を振り返ろう。

2008 年 9 月 16 日のリーマンショックを契機にサトシナカモトの「A Peer-to-Peer Electronic Cash System」（P 2 P 電子マネーシステム）に関する 8 ページの論文骨子は、同年 10 月頃には完成し、インターネットを通じて、世界中のプログラマーたちがこの論文のプログラム化に取組んだ。2009 年 1 月 3 日、プログラマーらの苦心作が完成、BTC がネット上に公表された。

既存の通貨や経済システムへの疑念や不信から､新時代の通貨や経済の仕組みを模索した｢P 2 P 電子暗号通貨」（デジタルクリプトンカレンシー＝ BTC）が誕生した日になった。

この電子データが、価値を持ち、人々が通貨として実際に流通させるには「ビットコイン・ピザ・デイ」と称される 2010 年 5 月 22 日（ピザ 2 枚を 1 万 BTC で購入した取引成立日）まで、およそ 1 年半を要することになる。最新の仮想暗号通貨といえども、過去の様々な通貨同様、簡単には人々から「通貨としての認知」を得ることが出来なかったわけだ。

通貨の三大要素である 1 ）交換可能（支払）2 ）価値保存（蓄蔵）3 ）価値測定（尺度）は、簡単には整わない。権限を取得し、流通し、通貨としての地位を獲得していくには、時間と人々の選択が必要である。国家や中央権力の強制力下でも、それは同様で、悪貨や地域通貨の藩札の如きは満足な流通すらしなかった歴史もある。最新時代の最新通貨の誕生は苦労の連続だった。

新通貨がカネの役割を果たすようになるには多くの労と時間がかかった。2011 年頃には、悪徳集団「シルクロード」が、BTC の普及流通に麻薬やマネーロンダリングで、量の拡大と言う点で寄与？し、同主催者ロス・ウルブリヒトはあまりの悪徳ぶりから、2013 年投獄された。

同様に中国やロシアの自国通貨を信用しない人々によっても BTC 取引は盛んに行われ、自国の通貨からの逃避者によって使われ、広まった経緯を持っている。これらは、通貨が通貨としての認識を得るには、どの時代にあっても普及のための苦労と時間がかかるという証左でもある。

日本では、2014 年当時、殆どの人が知ることなく、東京六本木の怪しげな外人バー数軒でその取引実績があった程度で、同年 2 月に Mt. Gox 事件で一躍ニュースとなり、人々の認知を得た程度だった。勿論、政府も官庁も時の副首相も「何それ、通貨？モノでしょう」と言う態度だったことは記憶に新しい。しかし、昨年の 4 月 1 日に成立施行された「改正資金決済法」により、日本人にも「仮想通貨ブーム」が到来、昨冬の BTC 高騰の原因は日本人の取引参加者激増によるものと判明している。

それでは、October 31, 2008　作成の　Satoshi Nakamoto による　ビットコイン論文

「A Peer-to-Peer Electronic Cash System」の一部（3.4.5.6の4項目抜粋）の説明を見よう。
（字数制限から8頁全文掲載を断念、論文本文はネット上で公開されている。和訳は領内）

3．タイムスタンプ・サーバー「そのデータがタイムスタンプ[2)]された時点で、ハッシュとなるために存在していたことが証明される。各タイムスタンプはそのハッシュの中に前のタイムスタンプを含んでいくことでチェーンを形成し、タイムスタンプが増えるたびに直前のタイムスタンプを補強」

4．プルーフ・オブ・ワーク「データブロックをハッシュとして処理し、そのハッシュを広範囲に公開するハッシュ化の際に要求される0ビットを与える値が見つかるまでの間、データブロックにワンタイムパスワードを足すことでプルーフ・オブ・ワークを実現している。
この作業をやり直さない限りそのデータブロックを変更することはできない。
その後のデータブロックもチェーン化されて後に連なるため、該当ブロックを書き換えようとするならば、それ以降の全てのブロックを書き換えなくてはならない。」

5．ネットワーク「プルーフ・オブ・ワークを見つけ次第、参加者はブロックを全参加者に告知する。参加者は、ブロックに含まれる全ての取引が有効であり、以前に使われていない場合にのみ、それを承認する。参加者は、承認されたブロックのハッシュを直前のハッシュとして用いて、チェーンの次のブロックの作成を開始することで、ブロック承認を表明する。
参加者は常に最長のチェーンを正しいものと判断する」

6．インセンティブ「新しいコインを一定量安定して追加していくことは、金鉱労働者がリソースを消費して採金し、金の流通量を増やすことと似ている。この場合、消費しているのはCPU時間と電力である。インセンティブは、取引手数料によっても得ることができる。
もしある取引でアウトプットされた価値がインプットされた価値よりも少ない場合、
その差は取引手数料としてその取引を含むブロックのインセンティブに加算される。」

これらの記述は、プログラム化されたBTCに在る「その思想・哲学の肝」に当たる。

上記の詳細説明は省くが、大まかに言えば、『相互管理してデータのやりとりを行い、定期的に同期処理し、1ブロックに2,000前後の情報データを記録、ハッシュで暗号化、ブロックを封緘。ブロックは10分毎に新規作成され、通貨としての機能を発揮する』が要約になろう。

『Ⅲの不正防止』で3項目の一つと書いた「合意形成」（コンセンサスアルゴリズム）については、論文の「4．Proof of Work（4.プルーフ・オブ・ワーク）」があるが、文字通り、「労力をかけた証明」で、仕事量が大きい人ほどブロック承認の成功率が高いとされている。これに対し、第2の仮想通貨流通量のEthereum（イーサリアム）が採用した「Proof of Stake」（資産保有の証明）では、「労力」より「資産量」（コインを持っている量と保有期間）で、ブロック承認の成功率を決める合意形成がされ、早さ・速さも余計な手間がかからないため、計算も短くて済み、1分以内での作成で、電気代も安く済むメリットがある。この部分での改善の余地はまだまだあるのだろう。今や1,500種類を超える仮想通貨はBTC亜種とも言えるのだが、BTCの弱点や欠点をカバーすべく、各種の工夫がされ、「幸せの通貨」として、通貨に哲学を持たせたリップルコイン

も産まれており、通貨そのものが過渡期と言えるのかもしれない。

＊帳簿履歴を背負う通貨

2018 年 1 月 26 日ＮＥＭ（New Economy Movement）流出盗難コインチェック事件が発生、社会はその流出金額 580 億円という金額に驚き、その具体的な盗難事件の概要が明らかになるにつれ、この会社の管理の杜撰さに呆れた。その時のショックもあって、1 BTC の価格は 2 か月前のピーク時 220 万円の 4 分の 1 に急落した。この事件では、仮想通貨の技術やシステムに欠陥が無いにも拘わらず、人的な資金管理体制の不備が原因で、人災であることが判明した。

故意か他意かは別にして、4 年前の Mt. GoX 事件と同じく、扱う人による行為の結果だった。その後の数か月で金融庁や関係機関が種々の規制やルール制定に動き、取扱業者の選択選別が行われているのは周知の通り。事件を起こしたコインチェック自体もマネックス証券に買収され、業者選別はこの 8 月末時点でも、登録業者やみなし業者の淘汰が行われている最中だ。

この事件での TV コメンテーターとして出演した折、ディレクター・プロデューサーへの事件説明の際に「仮想通貨」の帳簿上における大きな発見をした。

それは、『失われた NEM は追跡できるのか？』と言う質問に『泥棒の背中にカラーボールを投げて識別できるように、それぞれの盗難 NEM も識別出来、追跡可能』と答え、放送時にもその説明をした。紙幣は「通し番号」から盗難紙幣の識別は可能だが、仮想通貨はどうだろう。

仮想通貨＝電子データは、通し番号は打てないのにどのように追跡可能なのか？　を考えると、仮想通貨は、それが産まれた時からの「取引記録＝帳簿歴を背負っている」から、どの取引の何時のどの分が盗まれたのかが判ると気付いた。履歴を遡れること自体が画期的なことだとも。

仮想通貨は、「通貨としては、初めて帳簿を背中に背負ってる。」カラーボールで印が可能と言うことと同じだ。「データが通貨」と言うこと以上に「記録＝履歴そのものが通貨」と言う人類がかつて手にした通貨の中で、「取引歴が分る」全く新しい通貨　と言う新認識が出来た。

2015 年 6 月刊行の自著「3 つの近未来」の 119 頁に『その採掘作業はブロックという単位で管理されている・・・ブロックがチェーンで繋がり、纏めて管理され破れない。これが複製不可ということの特徴』と書いたが、「帳簿＝通貨」の認識には当時至っておらず、不明だった。

どの BTC であっても、2009 年 1 月 3 日の誕生から、全ての採掘（マイニング）を経て、今日までの BTC 取引すべての「過去記録＝全帳簿の全閲覧」が可能で、10 年間の過去履歴が検証出来る。過去だけでなく、将来もチェック可能で、BTC の通貨としての理論上の最終年度は 2142 年、本 8 月での流通量は約 1700 万／ 2100 万 BTC（全発行数 693 万ブロック・2100 万 BTC の 80％に相当）で、今後産まれる新たな 400 万 BTC も対象で、全て管理されるという真実。

仮想通貨全体への理解が深まる中でも、この「帳簿を背負う通貨」は画期的な指摘だろう。

Ⅳ　結論　と　今後の課題

ブロックチェーンが今後様々な作用をもたらす可能性のある近未来社会を考えてみたい。

BTC に代表される仮想通貨は一角に過ぎず、社会を大きく変える動きとして徐々に認められつ

つあるのは、「簿記・新会計の世界」と「契約世界」である。更に「公証の世界」とでも言うべき三つ目の世界もある。自分が経験したブロックチェーンに欠けていると思える「人への説得力」や「絆への介入」をどう扱うべきかを問題提起して、論文の最終としよう。

「複式＋ブロックチェーン」が普及すれば、帳簿付けが財務諸表作成に直結するため、仕訳後の不正行為は大きく減る要因にもなろう。Ⅱの事例で診た4事例は、このブロックチェーンを導入した新複式簿記ではどのようになるかを考えてみよう。

①帳簿作成前の不正・・・仕訳が同時帳簿作成になるので、仕訳以前の不正には対処できないが、仕訳が出来れば、それは同時に帳簿作成となり、不正が入り込めない。

②帳簿そのものがウソ・・・うその仕訳、虚偽偽造伝票への対処だが、うその仕訳が成り立つか？を考えるとき、紙ベースよりは成り立ち難いが、ウソを見抜く機能や能力がブロックチェーンそのものには無いので、完璧な対応は出来難い。AIとの併用等、仕訳前の対応が不可欠。

③他人とのコミュニケーション内容をブロックチェーンに挿入することは可能か？・・・
②と同様、ブロックチェーン単独での見破りや告発には無理がある。ブロックチェーンは信頼の絆の連続性がその取引の担保となっているが、信頼の無い絆の連続性を「おかしい」と感じ、自ら見破ってはくれない。このような感性を人工知能で代替（内部告発が仲間の日常の異常を感じ取っての行動であるように、人工知能にも、対象者の普段の仕事ぶりやメールのやりとり等から異常性を感知して、取引仲間・上司・同僚に警告を発し、未然に不正防止を行うような仕組み）が可能かを考えておく必要がある。

②③対応の実現は近いだろう。スマホやモバイルでの位置情報での検索や、出張の実際の有無の確認、交通切符の提出、出張時間割等の分析を人工知能（機械・深層学習付きAI）が検証、監査そのものをシステムが、自ら要求する電子告発を可能にしていけば、実現出来るだろう。

「単式簿記⇒複式簿記⇒新複式簿記」と言う従来の複式簿記にブロックチェーンを伴った新会計方式的な簿記が出現すれば、不正防止の強い味方になるだろう。

これは、製品販売やサービス或は費用の処理などを通常の仕訳で行うが、タイムスタンプ（電子的時刻証明）を併ない、ブロックチェーンに記録する。仕訳は、売方は貸方に売上金計上・借方に売掛金を記載、一方購入者側は、貸方に買掛金・借方に仕入計上する。この両側の仕訳がリアルタイムにブロックチェーンに記録され、ウオッチする必要のある監査法人、会計事務所、経営者など限定対象者がこれらの記録を同時に見ることが可能になる点がミソである。

これが、従来の複式と異なる簿記の特徴になる。

この簿記により、監査法人は財務情報を仕訳と同時に把握でき、不正行為の有無等の都度確認が容易になる。この事で、監査業務のより迅速な処理と不必要な人員・コスト削減が実現可能となり、依頼者たる経営者には逆の意味で費用削減となり、現場の立場からは、不正行為の確認や通常で気付かなかった事柄が確認でき、より透明な経営になるだろう。[3)]

＊スマートコントラクト

仮想通貨の二重払い回避や信頼の基礎になっているブロックチェーンが、インターネット社会の契約社会を牽引するシステムになり得るとして、『ありとあらゆる取引の世界に応用可能な信頼のネットワーク』と注目を浴びる事態になっている。ブロックチェーンがその汎用性の高さから様々なサービスへの更なる応用が期待されるのは当然だろう。

先に見たように「分散台帳」を実現する技術、ブロックチェーンを応用したものは様々あり、「貨幣」に使われたのがビットコインだったが、今や、ブロックチェーンを巡る応用は、産官学あげて行われており、なかでも、契約条件の確認や履行を自動的に行い、仲介者無しで価値取引を実現するスマートコントラクト技術が注目点されている。

スマートコントラクトの注目領域は・医療へのシームレスな適用・デジタル著作権・低価額資産向けの新信用市場・成果に応じた自動支払適用　・インダストリアル・マッシュアップ（企業同士が流動的に協業する全く新しい世界）　・インダストリアル IoT（あらゆるモノを、リアルタイムのデジタル市場に接続し、機材が稼働していない遊休時間を企業間で売買できるようにする）と幅広い。

ますます、これらの領域は拡大しているが、中国ではその領域プロジェクトの過半が実現不可という情報も出ており、玉石混交状態で混乱し始めてもいる。[4)]

ブロックチェーンの進展を 3 段階で考えると問題点も見えてくる。

① 低コストで記録を残す機能として、ベルギーで、すべてのダイヤモンド取引記録に使用され始めた。音楽の著作権管理や不動産登記にも使えると各団体がこの導入に動き始めている。
② IoT で得られた情報をベースに、ブロックチェーンで書かれた契約内容と一致したならば、様々な自動処理を行う。スマートコントラクトで執行、その記録をブロックチェーンで残す方法で、試行錯誤の段階だ。
③ スマートコントラクトにより、組織がなくても契約を実行できる。組織の代替としてブロックチェーンを使うケースが考えられるが、世の中で起きる全てのことを契約書に書けるか？
と言う本質的な疑問があり、現時点での目標は「相応部分を自動化可能に」と言う程度だろう。全ての記録が繋がり、出来事が自動契約になり、スマートコントラクトになるかは何とも言えない。

＊「絆」へのブロックチェーン介入は可能か。

『「公証の世界」で、自分の経験したブロックチェーンに欠けている「人への説得力」や「絆への介入」をどうするのか』とⅣの冒頭で書いたが、それは自らの任意後見人登録時のことだった。

この時、公証人はどう振舞い、どう我々を助けたか？を述べて、その違和感の説明の一助にしよう。今から 5 年前、87 歳の母が倒れた。病院に運び込まれた母は、どこかで倒れて頭を打ったらしく、「硬膜下血種」で、脳手術を受けた。この折、母を自宅介護することを決め、24 時間ヘルパー体制で臨むこととした。同時に恢復した母と妹に「母の財産管理を自ら行う」任意後見人制度を説明し、万一の時の為に、自分が就くことの説明をした。

事　象・・・平成 25 年 11 月 14 日に高齢の母の為に「委任契約と任意後見人」登録を奈良地方法務局所属の酒井公証人立ち合いの下、行った。

問題点・・・この時、母と私との契約席に、妹にも陪席させ、法的な目的や効果、任意後見人に関する知識を酒井公証人から事細かく、説明頂いた。法学士の私は別として、説明や相互の理解に 1 時間半近くを要したが、第 3 者たる酒井公証人の懇切丁寧な解説で、3 人が納得して公証手続きを行えた。これについては、今 92 歳の母も妹も『懇切に教えて頂き、理解出来て』良かったとしている。

将　来・・・本年 6 月 7 日付「ダイヤモンドオンライン」[5)] に野口悠紀雄氏の公証人に関する関連コメントがあった。「公証人はブロックチェーンに置き換えよ」と。

野口氏は文中で、アナログ時代の公証制度に関して非常に重要な指摘をしている。

1．定款認証だけでなく、公証人が行なっている仕事の殆どは、ブロックチェーンを用いれば、簡単に安く処理できるようになる。様々な対象について広範囲に見直しを行なうべきだ。
2．公証人をブロックチェーン利用で代替することである。
　真正性の証明はブロックチェーンで代替できる。
3．定款だけでなく、ブロックチェーンによる真正性の証明を、さまざまな対象について認めるような制度改正を行なうべき　　と。

野口氏意見に全く賛成だ。ブロックチェーンシステムの持つ真正性やコスト削減は大いに役立つし、その普及が社会をより進化させるだろう。法務局 OB の天下り先になっている各地の公証人選任にもメスが入るだろう。ブロックチェーンによる公証人代替案は、良い事尽くめのように思える。しかし、ここで浮き彫りになるのは、法的知識に乏しい母と妹を充分に納得させた酒井公証人の「3 者同時説得力」や当事者への配慮の利いた「コミュニケーション能力」がブロックチェーン導入で代替可能かと言う点だろう。信頼性や真正性では、完璧に見えるブロックチェーンだが、データ記録の各時点（前中後）は信頼出来るだろう。ただ、そのシステムに乗っかる前段階での「人と人」「コミュニケーション領域」にまで、システムだけで信頼出来ると割り切るにはまだ時間がかかる気がする。特に我が実例では、母と妹の信頼を勝ち得たのは「デジタル公証人」ではなく、「人間公証人」だったから。無味乾燥なロボアドバイザー的な代替システムでは無理があったろう。酒井氏が居なくては、説得にならなかった。冷静に説明しても、カネや損得がまつわる話では機械やシステムだけでは、事が片付くには今少し人間側にも慣れや訓練が必要で、人工知能に頼るにしても、相応の時間と経験が必要だろう。

最後は人間同士が関わる「心と心のつながり＝絆の領域」にブロックチェーンをどのようにスムーズに関与させ得るかが問題点となろう。真正性を記録する時点より前では、安直にその「絆」を省略し、無視することは出来ず、この段階の「絆」を如何にシステム化し、記録段階に結び付けるかを考えることが、今後のブロックチェーンのより良い普及に繋がると考える。
それが本論文の結論でもある。

注

1）ハッシュ

・元のデータに戻せない（不可逆性）・・・重要な特徴

・元のデータが少しでも変わると変換後のハッシュが全く異なる値になる

・ハッシュ技術によって取引情報は暗号化され、ハッシュは不可逆性を持つ。

2）タイムスタンプ

タイムスタンプ、発行 1 億件 電子文書に打刻、非改ざん証明　　日経新聞記事　　2018/9/3

日本データ通信協会によると、2018 年 1 ～ 6 月の発行件数は 1 億 700 万件で前年同期より 28％増えた。文書と時刻を一体で暗号化するタイムスタンプがあれば、後から内容が変更されていないと証明できる。財務省の文書改ざん問題などを受け、データの信用を担保する技術として注目されているようだ。タイムスタンプは、日本の標準時を決めている情報通信研究機構が配信する時刻をもとに NTT データなどの認定事業者が発行する。事業者は総務省の指針に基づき、日本データ通信協会が認定する。件数集計は 17 年からだが、同協会によると、半期で 1 億件を超えるのは初めてとみられる。タイムスタンプは現在、国税庁が電子帳簿の要件として求めている。行政手続きを原則として電子化するデジタル・ガバメント（電子政府）などの取り組みが官民で進めば、タイムスタンプを含む電子証明の技術はニーズが一段と高まる。

3）この発想を暗号作成者のイアン・グリッグは「三式簿記」と称した。

又、日本では、「井尻雄士氏の三式簿記」があるが、同概念には、未来の財産を表す予算や儲ける加速度をあらわす利力などの時間概念を通じた展開があるようで、本稿ではそれらのような深い考えに基づく記述でではなく、単純な会計上の指摘にとどめるもの。

4）「ブロックチェーン・プロジェクトの 92％が失敗 平均寿命は 1.22 年」

https://coinchoice.net/92-blockchain-projects-1-22-years/　　2018 年 6 月 23 日

ブロックチェーン技術はこれまで、世界で 8 万件余りのプロジェクトが実施されたが、今日まで生き残っているのは僅かに 8 %、640 件ほどに過ぎず、その平均寿命も約 1.22 年という、将来的に余り喜べない意外な事実が明らかになった。これは中国・工業情報化省の情報通信研究院（CAICT）が調査した結果で、2018 年 5 月末に中国・貴陽で開かれた「2018 年中国国際ビッグデータ産業展覧会」で報告された。

5）「起業促進の決め手、公証人はブロックチェーンに置き換えよ」

https://web.smartnews.com/articles/2Lqhk9YhFBF　　DIAMOND　ONLINE　2018.6.7

野口悠紀雄：（早稲田大学ビジネス・ファイナンス研究センター顧問）

参考文献

東京銀行職員研修所（1972）『現行外為経理入門』 東京銀行計理部

佐々木良一（1993）『インターネットセキュリティ入門』 岩波新書

日立総合計画研究所編（1993）『エレクトロニック決済と金融革新』 東洋経済新報社

岩崎和雄／佐藤元則共著（1995）『電子マネーウオーズ』 産能大学出版部

山川　裕（1996）『エレクトロニック・コマース革命』 BP 社

（インターネット時代の電子決済システム）

河崎貴一（2001）『インターネット犯罪』 文春新書

サイモンシン著　青木薫訳（2001）『The　Code　Book　暗号解読』 新潮社

梅田望夫（2006）『ウエブ進化論』 ちくま新書

吉本佳生／西田宗千佳共著（2014）『「ビットコイン」のからくり』 講談社ブルーバックス

川上量生（2015）『鈴木さんにもわかるネットの未来』 岩波新書
アレック・ロス（2016）『THE INDUSTRIES OF THE FUTURE』
（邦訳 未来化する社会）（株）ハーバー・コリンズ・ジャパン
A・M・アントノプロス（2016）『Mastering Bitcoin』
（邦訳 ビットコインとブロックチェーン）NTT 出版
ナサニエル・ポッパー（2016）『DIGITAL GOLD』
（邦訳 デジタル ゴールド）日本経済新聞出版社
ドン＆アレックス タプスコット（2016）『BLOCKCHAIN REVOLUTION
（邦訳 ブロックチェーン レボリューション） ダイヤモンド社
神永正博（2017）『現代暗号入門』 講談社ブルーバックス
中島真志（2017）『After Bitcoin （アフター・ビットコイン）』 新潮社
中島明日香（2018）『サイバー攻撃』 講談社ブルーバックス
伊藤穣一／アンドレー・ウール（2018）『教養としてのテクノロジー』 NHK 出版新書
ジェイコブ・ソール（2018）『帳簿の世界史』 文春文庫
デイビッド・バーチ（2018）『ビットコインはチグリス川を漂う』 みすず書房
ビジネス研究会（2018）『60 分でわかる！ブロックチェーン最前線』 技術評論社

Summary

In the background of “bit coin,” revolutionary internet technology called “block chain” exists. Block chain opened up a new technology by establishing the internet from “information transfer” to “value transfer.” This paper discusses this “block chain.” Theme is “whether block chain can prevent unjust activities in the world of bookkeeping.” It will discuss the comparison of the unjust prevention in the world of both analog and digital. Over the years, people have established methods to prevent unjust activities in the world of analog bookkeeping. Would such methods work in the digital era? System-wise, blockchain is said to be an absolute solution to prevent universal unjust activities, but is it truly effective to all kinds of unjust activities? This paper also discuss the effect or impact that it would have on the financial economy and society.

【Key words】 ＊ internet from value transfer ＊ notary public in the internet
＊ currency accompanying bookkeeping ＊ smart contract