

サプライチェーンマネジメントにおけるブロックチェーンの応用システムモデルの考察

Study of Blockchain Application Model for Supply Chain

川口 夏輝/Natsuki KAWAGUCHI

中央大学総合政策学部

[Abstract]

It has been ten years since Satoshi Nakamoto published "White Paper" for Blockchain. The paper aims to propose a solution to the double-spending problem using a peer-to-peer network. Blockchain is powerful, disruptive innovations. Actually, the technology is applied to many services. There will be challenges as Blockchain matures. To get over these difficulties, what we can do is only to do much experimentation. So, I propose Blockchain for supply chain in this paper. First, I will introduce related technologies such as blockchain and supply chain. Then, I will advocate the theory of a system and experiment it.

[キーワード]

ブロックチェーン、サプライチェーンマネジメント

1. はじめに

サトシ・ナカモト氏がブロックチェーンの原論文であるホワイト・ペーパーを発表してから約10年が経過した。ブロックチェーンは主に暗号通貨に使用されてきた。しかし、その目的を超えて、この技術は様々な分野に応用されようとしている。特に証券、土地登記、文書の管理などの効率化が期待されている。ブロックチェーンが発達し、成熟していく過程で様々な課題が生まれることが予想される。処理速度など技術的な問題や、そもそも、この技術をどう应用するかという議論も活発になるであろう。ブロックチェーンがそのような課題を克服し、その技術が最大限生かされるためには、実験を通してその応用のあり方について理解を深めることが必要である。本研究の目的は、サプライチェーンにおけるブロックチェーンの応用システムモデルを提示、考察、実験することである。

2. ブロックチェーン

サプライチェーンマネジメントにおけるブロックチェーンの応用システムモデルを考察する前に、まず、ブロックチェーンの定義と仕組み、メリット・デメリットについて概観する。

2.1. ブロックチェーンとは

日本ブロックチェーン協会(Japan Blockchain Association, JBA)はブロックチェーンの定義を以下のように定めている。¹

- (1)「ビザンチン障害を含む不特定多数のノードを用い、時間の経過とともにその時点の合意が覆る確率が0へ収束するプロトコル、またはその実装をブロックチェーンと呼ぶ。」
- (2)「電子署名とハッシュポインタを使用し改竄検出が容易なデータ構造を持ち、且つ、当該データをネットワーク上に分散する多数のノードに保持させることで、高可用性及びデータ同一性等を実現する技術を広義のブロックチェーンと呼ぶ。」

定義上のビザンチン障害について説明を加える。2014年にチューリング賞を受賞した数学者レスリー・ランポート博士らが考案した「ビザンチン将軍問題」は、分散システム上の信頼性に関わる問題である。ビザンチン将軍問題で想定する場面は、ビザンチン帝国の将軍達がそれぞれ部隊を率いて敵を包囲している戦場である。各部隊はそれぞれ離れた場所において、伝令を相互に送ることでしか連絡できない。戦局は、将軍達が一斉に指令を出して攻撃を仕掛ければ勝てるが、一部の部隊だけで攻撃を仕掛けると負けるという状態である。つまり、攻撃が撤退かのどちらかを、全将軍が一致して同意しなければならない。しかし、将軍達の中には裏切り者がいる可能

¹ 日本ブロックチェーン協会 (<https://jba-web.jp/>) (2019/2/28 アクセス)

性がある。裏切り者の将軍は、他の将軍から攻撃の提案を受けると、撤退の提案にすり替えて別の将軍に伝達するかもしれない。そうなると、一部の将軍は攻撃指令と撤退指令の両方を受け取ることも想定される。最悪、一部の部隊だけが攻撃を開始してしまい、負ける可能性もある。ビザンチン将軍問題とは、誠実な将軍達が全員一致で攻撃または撤退に同意できる場合、つまり、正しい判断に将軍達の判断を全員一致へと導く方法を考えることである。ランポート博士は、このビザンチン将軍問題を、耐故障性のある分散システムにおける同意問題として考えた。ここでいう分散システムは複数のコンピュータが協調することで1台のコンピュータではできないような処理を実現するものとする。また、同意とは複数のコンピュータで同じ値を持つことである。同意したい値を通信で他のコンピュータへ送ればよいという意見もあるかもしれないが、コンピュータは壊れることがあり、複数のコンピュータがあればそれだけ壊れるコンピュータも増える。故障しても、そのまま止まれば対処できるが、動き続け、しかも間違った通信や処理を始めると非常に問題である。つまり、ビザンチン将軍問題では、故障しても止まらずに、間違った動作を行うコンピュータを裏切り者の将軍、他の正常なコンピュータを誠実な将軍に見立てることで、複数の正常コンピュータが同じ値を持つ方法やその条件を扱ったということである。

ノードとは、ネットワークに能動的に接続されている電子デバイス、コンピュータなどを指す。

プロトコルとは、データ通信を行うために、あらかじめ決めておく規約を指す。

日本情報処理開発協会は電子署名、及び、ハッシュ関数を以下のように定義している。²

電子署名とは、電磁的記録に記録することができる情報について行われる措置であって、次の要件のいずれにも該当するものをいう。

- (1)「当該情報が当該措置を行ったものの作成に係るものであることを示すためのものであること。」
- (2)「当該情報について変更が行われていないかどうかを確認することができるものであること。」

ハッシュ関数とは、文字や数字などのデータ(入力値)を一定の長さのデータ(出力値)に変換するための手順(関数)のことをいい、ハッシュ関数を用いて出力された値をハッシュ値と呼ぶ。ハッシュ関数は、異なる2つの入力値から同じ出力値を算出することが困難な特徴をもち、また、出力値から入力値を逆算することも困難である。

2.2. ブロックチェーンの仕組み

ブロックチェーンの文脈でトランザクションは取引を意味する。トランザクションには送信者によって正しく作られたことを証明するために、作成日時のタイムスタンプと電子署名が施されている。一定数のトランザクションを格納したものをブロックという。取引が新規に生成されたブロックやそれに続くブロックに取り込まれる流れを承認といい、ブロックが新しく追加されて鎖状、すなわちブロックチェーンになる。

タイムスタンプとは、電子データがある時刻に確実に存在していたことを証明する電子的な時刻証明書である。

ブロックチェーンの文脈でのスマートコントラクトを、一般社団法人ブロックチェーン推進協会(Blockchain Collaborative Consortium, BCCC)副代表理事である杉井靖典氏は、「契約成立のために必要な条件が記された取引内容が、ブロックチェーン上に改ざん困難な状態で記録されており、そこに書かれた条件が満たされると、自動的に成立するトランザクション」と説明している。³

2.3. ブロックチェーンのメリット・デメリット

一般社団法人ブロックチェーン推進協会(Blockchain Collaborative Consortium, BCCC)副代表理事である杉井靖典氏はブロックチェーンのメリットを以下のように説明している。

- (1)システムが壊れることなく永続的に稼働し、続けられること
- (2)一度書き込まれたデータをあとから改ざんすることが不可能なこと

これは、サービス事業者やシステムの管理者ですら、データを改竄、変更することができないことを示す。ブロックチェーンは数学的な理論や情報技術を組み合わせることで、事業者が何者であろうが関係なく、そこに記録されたデータが真正であることを保証できるようになった。これは、お互いに信用できない者同士であっても、不正があることを心配することなく取引が行えるようになることを意味する。

しかし、このメリットはデメリットにもなり得る。ブロックチェーンに一旦記録されたデータは、仮に正当な理由があったとしても編集も削除もできない。このような改竄防止の仕組みが実現しているのは、多くのノードが同じデータをコピーしあって共有しているからである。

このようなメリットとデメリットを踏まえ、杉井氏はブロックチェーンを一般的なデータベースや分散ストレ

² 日本情報処理開発協会『電子署名・認証関連 用語・技術標準集』、Ver. 1.3

³ 杉井靖典『いちばんやさしいブロックチェーンの教本』株式会社インプレス、2017年

ージなどといった外部システムとうまく連携しながら利用していく必要があると指摘している。⁴

2.4. ブロックチェーンの種類

ネットワークの管理者、参加者の特徴に応じ、ブロックチェーンは大きく「パブリック型」、「プライベート型」、「コンソーシアム型」の3種類に分けられる。

(1)パブリック型

パブリック型ブロックチェーンではネットワークに管理者が存在せず、誰でもネットワークに参加し、取引台帳の記録と承認ができる。

(2)プライベート型

プライベート型ブロックチェーンではネットワークに管理者が存在し、管理者、参加者共に単一の組織、グループに限定される。

(3)コンソーシアム型

コンソーシアム型ブロックチェーンではネットワークに管理者が存在し、管理者の許可により複数のグループ、組織が参加可能である。

パブリック型ブロックチェーンの場合、ネットワークが分散されているため、参加者が増えれば増えるほど取引の改竄が困難になり、システム障害に強いという特徴がある。完全分散型というブロックチェーンの理念としてもパブリック型は理想的と言える。しかし、参加者のコンセンサスが取りにくく、取引の承認スピードが遅くなるというデメリットもある。それを改善するのがプライベート型、コンソーシアム型ブロックチェーンである。特に、コンソーシアム型ブロックチェーンは信頼できる参加者によって取引の承認が行われるため、記録、承認の安全性もある程度担保され、スピードと効率が両立できる点から有力視されている。

3. サプライチェーン

次にサプライチェーンについて戦略的サプライチェーンマネジメントの点から概観する。

3.1. サプライチェーンにおける原則

ショシャナ・コーエン、ジョセフ・ルーセルは『戦略的サプライチェーンマネジメント』で、他社をしのぐ卓越したサプライチェーンマネジメントの実現に向けて守るべき原則について以下のように分類、論じている。

3.2. 戦略基盤

企業はイノベーション、顧客体験、品質、コストという4つの側面で競い合っている。いずれも大切だが、リーディング企業ではその中の1つを特に重要な競争基盤と位置づけ、その他の要素は競争上のポジショニングを強化するものとして活用している。

(1)イノベーション

イノベーションを競争基盤とする企業は、顧客の心理を把握し、競争を勝ち抜くヒット製品を生み出し続けている。そこで重要となるのは市場投入までの時間である。ここで成功を左右するのは、サプライチェーンとエンジニアリングチェーンの統合、つまり、新たな製品、サービスの設計に関わる社内外の全ての活動を統合できるかどうかという点である。このレベルの統合を実現するには、プロセス、データを一貫した方針の下で管理することが求められる。

(2)顧客体験

顧客体験を競争基盤とする企業は、個々の顧客のニーズを満たす体験を提供する。そのような企業は顧客の好みを深く理解し、関連するサプライチェーンもそれに合わせて調節している。優れた顧客体験の提供は顕著な業績

⁴ 杉井靖典『いちばんやさしいブロックチェーンの教本』株式会社インプレス、2017年

の差につながる。顧客体験の分野に秀でた企業はサービスのコストと収益性も相関関係を理解しているため、顧客ごとにカスタマイズしたサービスを提供するコストを評価できる。そのような企業は顧客に豊富な選択肢を提供すべき状況を把握しているだけでなく、そうすべきでない場合も心得ている。製品、サービスを顧客が欲しいと思ったその時に欲しい場所に届けることで、無理に生産を急ぐことによるコストも、顧客離れ引き起こすコストも、ともに回避できる。そのため、顧客体験で戦う企業は顧客離反率や顧客維持コストが比較的安く、優れた業績を達成できるという訳である。

(3) 品質

品質を競争基盤とする企業はプレミアムな製品やサービスで知られ、いつも変わらぬ信頼感を提供する。品質の高さは製品開発が大きく影響する他、生産、調達、品質保証、返品対応といったサプライチェーンの主要プロセスが極めて重要な意味を持つ。また、壊れやすい、傷みやすい製品を扱う場合は、輸送や保管のプロセスも欠かせない。品質で戦う企業は、製品の生産過程の始まりまでさかのぼって追跡できるトレーサビリティの能力が競争上の差別化要因になっている。トレーサビリティを確保するために、企業は製品が顧客にわたるまでの流れを厳密に管理しており、さらに、荷印やトラック・アンド・トレース技術を用いて、顧客が購入した製品が正しく出荷されたものであることを保証している。

(4) コスト

コストを競争基盤とする企業は、コストに敏感な買い手を引きつける価格や、コモディティ市場でシェアを維持できる価格を提示する。この競争基盤で戦う企業には、極めて効率的なオペレーションが求められる。その土台となるのは製品やプロセスの標準化である。同様に、サプライヤー、生産品質、在庫の管理も重要である。サプライチェーンのパフォーマンスは、効率性に関するメトリクス、すなわち、資産稼働率、在庫日数、製品コスト、サプライチェーン総コストなどに基づいて評価される。

3.3. サプライチェーン戦略の主要素

サプライチェーン戦略には、関連する大小様々な活動や意思決定が含まれる。これは一連の活動が全体として1つの競争戦略を支えているということの意味する。ここで基本となるのは、顧客サービス、販売チャネル、バリューシステム、オペレーションモデル、資産配置の5つの要素、及び、各要素に対する企業の選択である。企業がこれらの要素について決断する際、1つの要素だけに注目し、ほかの要素を検討しない場合がある。しかし、サプライチェーンから戦略的メリットを最大限に引き出すには、全体への影響を踏まえて各要素を慎重に検討することが重要である。

(1) 顧客サービス

サプライチェーン戦略を策定するための最初の一步は、顧客サービスの目標を定義することである。顧客のタイプに合わせてデリバリーのスピード、正確さ、柔軟性のレベルを多様に検討することは、顧客体験を決定する上で大切である。こうした検討の答えは各企業のビジネス戦略によって決まり、その企業のターゲット顧客にも関わってくる。

(2) 販売チャネル

企業が製品、サービスを買手に届ける方法は多数存在する。ここでの意思決定は、ターゲットとする市場セグメントや地理的条件を踏まえて行われることになる。使用するチャネルによって利益率が大きく変わるため、チャネルの適切な組み合わせを判断しなければならない。また、製品が不足したり、需要が高まったりした場合に、誰に優先的に製品を供給するのかという点も決める必要がある。

(3) バリューシステム

効率的なサプライチェーン戦略を策定するためには、企業のバリューシステムを確実に理解している必要がある。これを理解すれば、このサプライチェーン活動について、自社とパートナー会社のどちらが担当するかを決める時に役立つ。このことに関連し、サプライチェーン活動には2種類あることを念頭に置かなければならない。すなわち、意思決定に関するものと実行に関するものである。企業はしばしば、意思決定の活動を自社でコントロールし、実行の活動をアウトソーシングすることを選択する。

(4) オペレーションモデル

製品、サービスをどのように生産するかという1つ1つの意思決定を総合したものがオペレーションモデルである。こうした意思決定の影響は製造工程だけでなく計画、オーダー管理、調達、納入の進め方にも波及する。オペレーションモデルには次の4種類がある。

- ・見込生産：大量販売される規格品を生産する際に、最も広く採用されるモデルである。工場では顧客から受注する前に生産を開始し、注文が来るまで完成品を保管する。大量生産によって生産コストを抑えられ、すぐに出荷可能な在庫を維持することで顧客の需要に素早く対応できる。
- ・受注生産：カスタマイズが必要な製品や、受注頻度が低い製品の生産に適したモデルである。顧客の注文が発生してから製品、サービスを生産する。在庫が膨らむことを防ぎつつ、多様な製品を提供できる。
- ・受注仕様生産：製品の汎用部分だけ事前に見込生産し、受注してから完成させるハイブリッドモデルである。最終製品のバリエーションが多く、受注生産よりも顧客リードタイムを短縮しなければならない場合に適している。受注仕様生産と似たものに、受注組立て生産がある。このアプローチでは売上予測に基づいて事前に部品を生産し、顧客の注文を受けてから製品を組み立てて、完成させる。
- ・受注設計生産：個々の顧客によって仕様が異なる複雑な製品やサービスを提供する業界に適したモデルで、その特徴は受注生産と多くの点で共通する。顧客の発注プロセスの最終段階で企業的设计部門が仕様を定義し、その顧客の注文に必要な原材料のリストを作成する。

(5) 資材配置

サプライチェーン戦略を定義する際に検討すべき最後の要素は、物理的な資産の配置である。ここでいう資産には、有形資産だけではなく無形資産も含まれる。これらの資産の場所、規模はサプライチェーンのパフォーマンスを大きく左右する。生産、計画、調達、オーダー管理、倉庫保管、物流のプロセスごとに最適な資産配置は異なる可能性がある。

3.4. 優れたサプライチェーン戦略のテスト

また、優れたサプライチェーン戦略の主要素に対するテストとして、シヨシャナ・コーエン、ジョセフ・ルーセルは『戦略的サプライチェーンマネジメント』で、以下の条件を提示している。

(1) 市場優位性

優れたサプライチェーン戦略を立てるには、顧客やサプライヤーに対するその企業の影響力を理解していることが求められる。なぜなら、戦略目標を満たすためにサプライチェーンを再構築できるかどうかは、その企業の相対的な力によってかなり左右されるからである。大切なのは企業の市場におけるパワーポジションを最大限に生かすことである。

(2) 複雑性調整

サプライチェーンが複雑化すると、オペレーションのコストがかさみ、運転資本が増加し、需要の変化への対応は遅くなる。大切なのは複雑性の適切なレベルを決定してパフォーマンスを管理することである。

(3) 障害回復力

回復力は安定したサプライチェーン戦略が持つ重要な特徴の1つである。一般的にサプライチェーンの回復力は冗長性、柔軟性を高める手法を組み合わせることで確立できる。

(4) 社会的責任

企業は自社のバリューシステム全体の活動が、持続可能性、労働条件、倫理、環境の面で基準を満たすものであることを目指し、社会的な責任を果たさなくてはならない。

(5) 環境適応性

変化が止むことがない以上、適応力を保ち続けることが重要である。サプライチェーン戦略に常に目を配っていなければ、すぐに市場のニーズとずれてしまうことになりかねない。サプライチェーンは内外の様々な要因を踏まえて調節する必要がある。

4. サプライチェーンマネジメントにおけるブロックチェーンの応用

ブロックチェーンとサプライチェーンマネジメントについて概観してきたが、その応用システムモデルについて考察をする。

4.1. サプライチェーンにおけるブロックチェーンの応用システムモデル

以下はサプライチェーンにおけるブロックチェーンの応用システムモデルの全体図である。

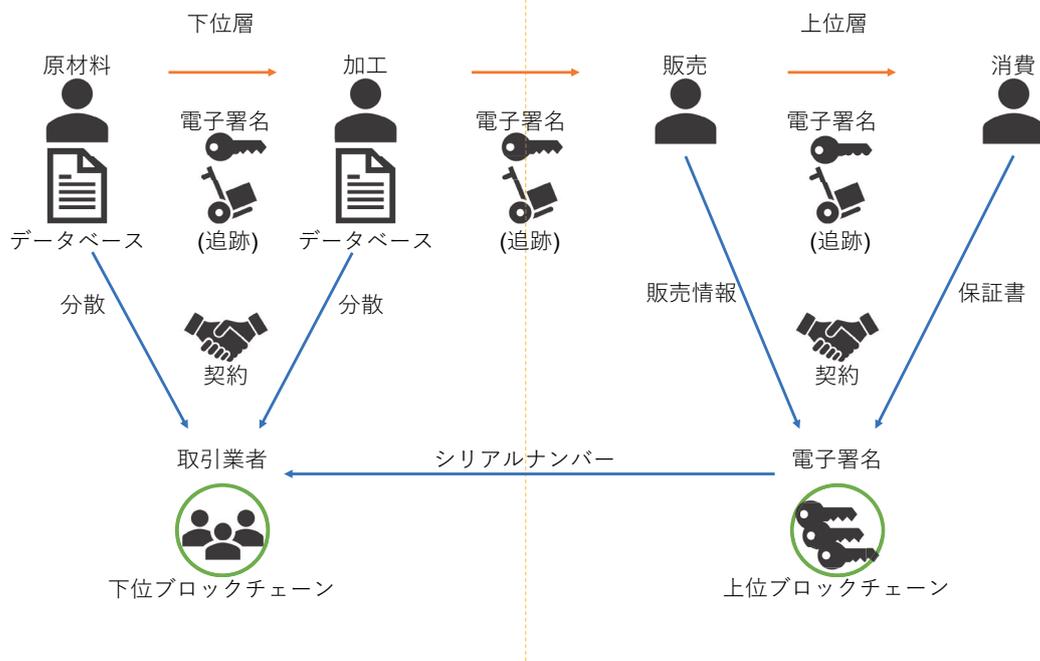


図1. サプライチェーンにおけるブロックチェーンの応用システムモデル

このシステムにおける用語を以下のように定義する。

- ・下位層： 原材料、加工段階での取引
- ・上位層： 販売、消費段階での取引
- ・下位ブロックチェーン： 下位層での契約を記録
- ・上位ブロックチェーン： 上位層での契約を記録

このシステムの取引の流れは以下の通りである。

(1) 原材料段階

(1-1) 原材料にシリアルナンバーを振る

-この段階でシリアルナンバーを振ることによって、サプライチェーンの始点から終点まで一貫した ID で検索することが可能になる。

(1-2) 原材料の情報を下位ブロックチェーンへ流す

-原材料の情報をネットワークに周知させることで取引相手を募集する。

(1-3) 取引相手が決定したら下位ブロックチェーンが生成される

-この時点で原材料段階と加工段階の契約は成立したとみなす

(1-4) 原材料に関するデータベースを書く

(1-5) 原材料データベースを下位ブロックチェーンに分散させる

-この項目については本章の第2項で詳しく説明する。

(1-6) 原材料段階の電子署名を生成する

(1-7) 必要に応じて原材料を追跡する

(2) 加工段階

- (2-1) 原材料段階の電子署名を認証する
- (2-2) 加工に関するデータベースを書く
- (2-3) 加工データベースを下位ブロックチェーンに分散させる
- (2-4) 加工段階の電子署名を生成する
- (2-5) 必要に応じて商品を追跡する

(3) 販売段階

- (3-1) 加工段階の電子署名を認証する
- (3-2) 販売に関するデータベースを書く
- (3-3) 販売段階の電子署名を生成する
- (3-4) 必要に応じて商品を追跡する

(4) 消費段階

- (4-1) 販売段階の電子署名を認証する
-顧客による電子署名の認証により、全体の取引での契約が成立したとみなす。
- (4-2) 契約が成立したら上位ブロックチェーンが生成される
- (4-3) 商品をシリアルナンバーで検索する
-上位ブロックチェーンと下位ブロックチェーンはシリアルナンバーによって接続されているため、両ブロックチェーン共に検索が可能である。

4.2. サプライチェーンにおけるブロックチェーンの応用システムモデルの特性

次に、本システムモデルの特性について考察をする。

(1) 包括的・同時的な記録

商流、金流、物流、情報ネットワークが全て、即時、記録されている。

(2) 多層防御

このシステムでは多層防御が用いられている。情報セキュリティにおける多層制御とは、攻撃者によってネットワークやシステムのセキュリティが侵害されないように複数の防御を設置するアプローチを指す。ここでは上位層と下位層を分けることによって、セキュリティが侵害されてもその原因を特定することが容易になり、被害を最小限に食い止めることに効果的と想定する。

システムの規模を大きくしたい場合、下位層と上位層の間に中位層を単数、または複数設けることができる。中位層を多くすればするほどシステムの規模は大きくなる。しかし、このシステム構造自体が単純なので、中位層を増やしても複雑度は飛躍的に上がることはない。

(3) 下位ブロックチェーンネットワーク

下位ブロックチェーンネットワークにおける情報の周知の流れは以下のパターンが考えられる。

- ・原材料の情報を周知: これがものの製造順序からして基本である。
- ・加工段階から取引相手を募集
- ・販売段階から取引相手を募集
- ・消費段階(すなわち顧客自身)が取引相手を募集: 顧客ニーズが最大限に反映される

このように、ビジネスの出発点は多種多様である。これによって、今までにない新しいビジネスが生まれる可能性がある。また、各段階の個人や組織が情報を周知した場合、全ての計画に取引が成立するわけではない。計画によっては取引相手の立候補がない場合も考えられる。つまり、良い計画には取引相手の立候補が複数あり、そこから最善の取引相手を選ぶことができる。しかし、逆に悪い計画には取引相手の立候補がなく、その計画が無理に実行されることはない。

(4) 電子署名

原材料、加工、販売の各段階でそれぞれ電子署名を生成する。それらの電子署名は1段階あとの段階で認証される。そうすることによって、同じ組織、企業での不当な認証は起こりにくくなる。また、正当な認証を迅速にす

る経済的なインセンティブが生まれる。これは、承認をしなければ自身のビジネスが滞るが、不当な承認をすれば、それもまた結果として自身のビジネスに悪影響を及ぼすことになるためである。上位ブロックチェーンを生成するためには電子署名を、消費者段階を除く全ての段階の数だけ揃える必要がある。消費者が販売段階の電子署名を認証したことでその契約は成立したとみなす。これは前述のスマートコントラクトに当たる。

(5) 追跡

追跡は、その商品を次の段階へ輸送する時に小包番号を振るなどして可能である。しかし、完全な記録を取ろうとするあまり、現実的ではないコストがかかる可能性もある。このシステムでは適切なレベルでの記録を可能にするために、追跡は任意に設計してある。

(6) データベース

このシステムではブロックチェーンとデータベースを併用している。書き換えるべきではない契約情報をブロックチェーンに、変更の可能性のある情報をデータベースに記録している。このように、柔軟性を保ちながらブロックチェーンを利用している。しかし、ブロックチェーンを使用してセキュリティを高めていても、データベースが弱点になってしまえば意味がない。この問題を解決するために、このシステムでは、データベースを下位ブロックチェーンネットワークに分散させている。前述の通り、ブロックチェーンはたくさんのノードが同じデータをコピーしあって共有することで、改竄防止の仕組みを実現している。データベースの分散という手法はこの理論と同様である。しかし、この場合、分散といっても完全分散ではない。そのデータを保有することが適切であり、且つ、そのデータを保有することでその組織、企業自身そしてシステム全体に利益があるノードに分散させる。

(7) 上位ブロックチェーン

このシステムでは上位ブロックチェーン上のブロックを保証書として使用している。これにより、販売店は顧客に商品のみを手渡すことが可能になる。また、顧客は保証書の保管をする必要がなく、紛失の可能性はなくなる。

4.3. サプライチェーン戦略の観点からの考察

第3項で触れた、他社をしのごう卓越したサプライチェーンマネジメントの実現に向けて守るべき原則の観点からこのシステムの考察を行う。以下の表は戦略基盤、サプライチェーン戦略の主要素、サプライチェーン戦略のテストにおける各項目に、どのシステム特性が解決策となり得るかを分析したものである。

	システム特性	注釈
戦略基盤	-	-
(A) イノベーション	(0)	プロセス・データを一貫した方針のもとで管理
(B) 顧客体験	(3)	顧客のニーズに適切に対応
(C) 品質	(1)	包括的・同時的な記録でトレーサビリティを確保
(D) コスト	(0)	効率的なオペレーションを実現
サプライチェーン戦略の主要素	-	-
(a) 顧客サービス	(3)	顧客に合わせてプロセスを多様に検討可能
(b) 販売チャネル	(0)	チャネルの適切な組み合わせを判断可能
(c) バリューシステム	(0)	企業のバリューシステムを確実に理解可能
(d) オペレーションモデル	(3)	4種類のオペレーションモデルに対応
(e) 資材配置	(0)	最適な資産配置を判断可能
サプライチェーン戦略のテスト	-	-
(あ) 市場優位性	(0)	企業の市場におけるパワーポジションを理解可能
(い) 複雑性調整	(0)	シンプルなシステム設計により複雑性調整可能
(う) 障害回復力	(2)	ブロックチェーンの冗長性・データベースの柔軟性 多層防御による障害回復力の実現
(え) 社会的責任	(0)	システム全体の活動が社会的な責任を果たしているか分析可能

(お)環境適応性	(1)	サプライチェーン全体の様々な要因を解析可能
----------	-----	-----------------------

表1. サプライチェーン戦略とシステム特性

(システム特性)

- (0) システム全体として該当
- (1) 包括的・同時的な記録
- (2) 多層防御
- (3) 下位ブロックチェーンネットワーク
- (4) 電子署名
- (5) 追跡
- (6) データベース
- (7) 上位ブロックチェーン

4.4. 実験

サプライチェーンにおけるブロックチェーンの応用システムモデルをサンプルコードで実験した。今回はダイヤモンドのサプライチェーンを想定している。以下の表と画像はそのサンプルコードの一部と実行画面である。

```

from Crypto.PublicKey import RSA
from Crypto.Signature import PKCS1_v1_5
from Crypto.Hash import SHA256
from base64 import b64decode, b64encode
import sys
import socket
from contextlib import closing
import hashlib
import datetime
from collections import defaultdict
from pymongo import MongoClient

class Diamond:
    def __init__(self, serial_number):
        self.serial_number = serial_number

class Contributor(Diamond):
    def __init__(self, serial_number):
        super().__init__(serial_number)
        self.name = input("Name: ")
        self.carat = input("Carat: ")
        self.price = input("Price: ")
        self.message = input("Message: ")
    
```

表2. サンプルコード

```

Serial Number: 20000501054
-----
Name: Bob Smith
Carat: 1.0
Price: $1000
Message: DEADLINE 2000/12/31/24:00:00
-----
b'Buy!'
-----
[<_main__.LowerBlock object at 0x103a83a90>, <_main__.LowerBlock object at 0x103e81668>]
-----
Country: South Africa
Province: Southern Cape
Trader: State Diamond Trader
Parcel Code: 123456789
-----
Verified
-----
Carat: 0.25
Color: F
Clarity: SI1
Cut: Excellent
-----
Verified
-----
Retailer: Tiffany & Co.
Purchaser: Alice Brown
Date: 2012/12/25
-----
Formation of Contract!
-----
[<_main__.HigherBlock object at 0x10482b0b8>, <_main__.HigherBlock object at 0x10482ba58>]
-----
Do you want to search your diamond?
[0]Yes! [1]No
0
Input your serial number
20000501054
-----
<Information of Lower Blockchain>
Contributor: Bob Smith
Raw Carat: 1.0
Raw Price: $1000
-----
<Information of Higher Blockchain>
Retailer: Tiffany & Co.
Purchaser: Alice Brown
Date: 2012/12/25

```

図2. 実行画面

5. 結論

本論文ではサプライチェーンマネジメントにおけるブロックチェーンの応用システムモデルの構築、実証実験を行った。ブロックチェーンとデータベースを併用し、セキュリティを保ちつつデータ活用の利便性に配慮した柔軟なシステムモデルを提示することによりビジネスモデルに組み込みが容易なモデルを示した。これらのモデル構築では、電子署名の期限が短いことなどによるデータの長期保存・利活用にも配慮したシステムとなっている。また、データベースが単一障害点になることを避けるため分散管理措置をとった。しかしながら、データベ

ースのセキュリティを向上させるにはただ単に分散させるだけでは不十分である。データベース上の個人情報の管理やデータ量の増加、長期間の利活用と保存などの問題が予想される。本モデルは、これらブロックチェーン単独での問題点の解決もしくは、ブロックチェーンとデータベースの併用に関する新たな方法を提案し実証した。

[参考文献]

- [1] 日本ブロックチェーン協会 (<https://jba-web.jp/>) (2019/2/28 アクセス)
- [2] 杉井靖典 『いちばんやさしいブロックチェーンの教本』 株式会社インプレス、2017年
- [3] 国立情報学研究所 『国立情報学研究所ニュース』 Vol. 69、2015年9月、ISSN 1883-1966(Print)
- [4] ショシャナ・コーエン、ジョセフ・ルーセル 『戦略的サプライチェーンマネジメント』 英治出版、2015年
- [5] 日本情報処理開発協会 『電子署名・認証関連 用語・技術標準集』、Ver. 1.3
- [6] N. Kawaguchi, “Blockchain for Supply Chain: Flexible and Secure Blockchain, Journal of Transformation of human behavior under the influence of The Infosociconomics Society Vol. 4, 2019年2月, ISSN 2423-9607
- [7] UK Government Office for Science 『分散型元帳技術：ブロックチェーンを超えた応用の可能性』、2016年 (2019年3月14日受理)