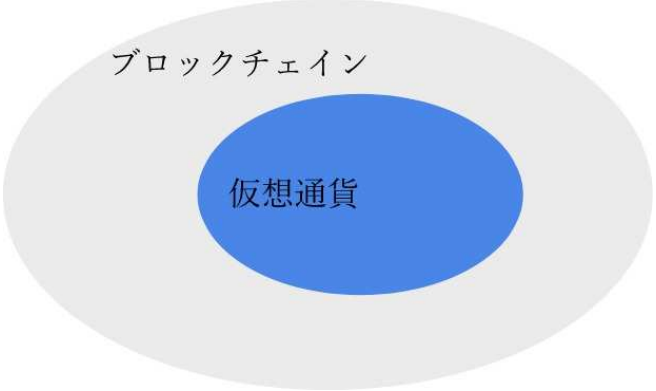
WHY BLOCK CHAIN

2020年3月9日

WGメンバー　岡田誠司
（株式会社オーシス代表取締役　ＩＴコーディネータ）

「ブロックチェイン」とは

- 「ブロックチェイン」は技術を切り出して語られることが多いですが、本質はその思想にある
- ブロックチェーンの成功例としてビットコインが語られることが多いが、
  あくまでビットコインはブロックチェーンを使った成功例であり「仮想通貨＝ブロックチェーン」ではない



ブロックチェーンの技術

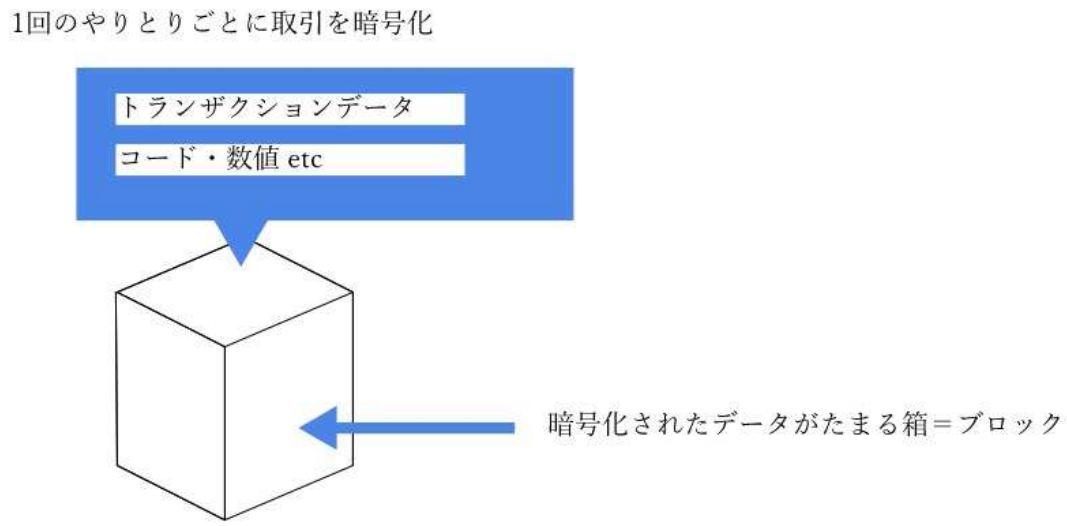
ブロックチェインの技術の中身は

- １．暗号化技術
- ２．コンセンサスアルゴリズム
- ３．ピァ・トゥ・ピァ（P2P）
- ４．ＤＬＴ（分散型台帳技術）

の４つの技術を組み合わせたものの総称となっている

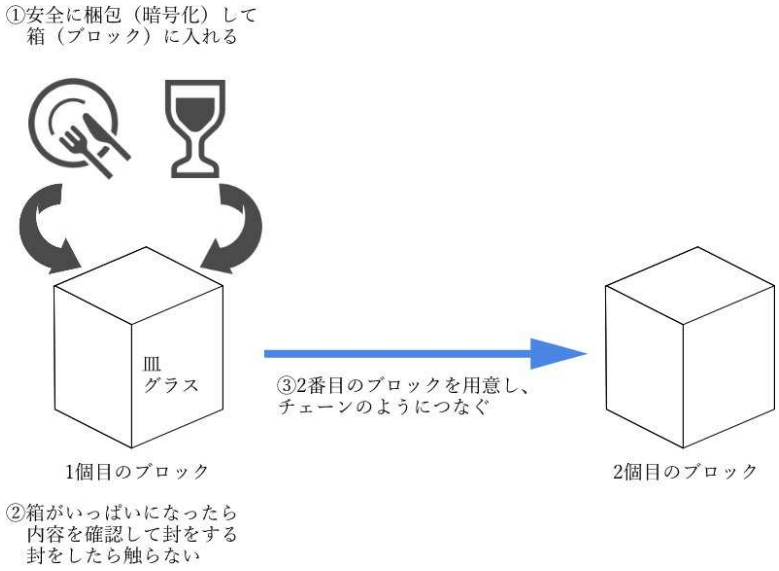
暗号化技術1

- １体１のトランザクション、１回のやり取りごとにその取引が暗号化されていることを意味している技術である



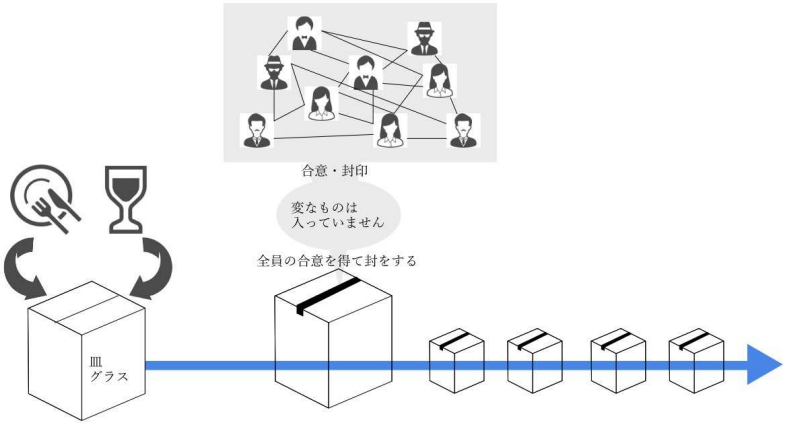
暗号化技術2

- 同時に暗号化技術と関連する技術としてブロックチェーンの名前の由来になっているブロック管理という手法がある



コンセンサスアルゴリズム

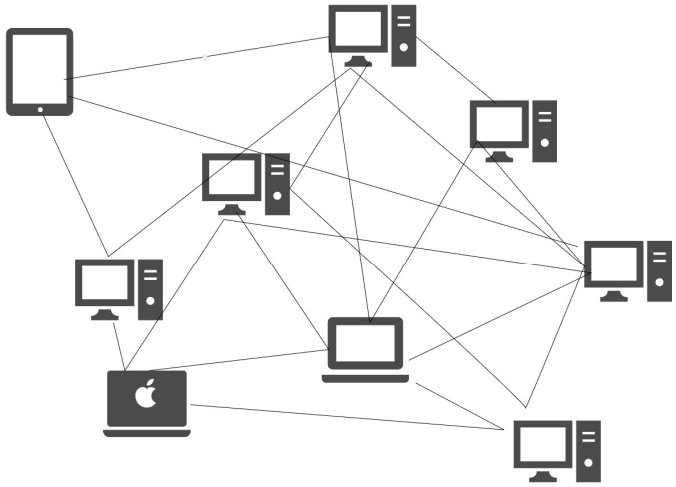
- 暗号化されたデータをブロックにするとき、本当にこのブロックには正しい情報か言っているか？と全員に確認してからブロックの封をするのがブロックチェーンのやりかたである
- この全員からOKをもらう「合意形成」の作業。この作業をコンセンサスアルゴリズムという



取引の連続性を保ち、過去データの改ざんを防ぐ

ピア・トゥ・ピア（P2P）1

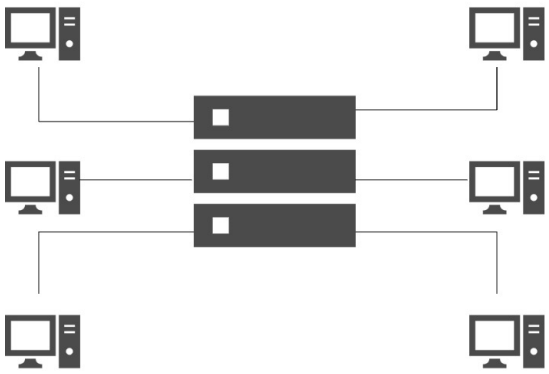
- 全参加者に対して、「みなさん、これで大丈夫ですよね？」という合意形成を取るために個々の参加者同士が通信するピア・トゥ・ピア（P2P）技術を使用して行われる



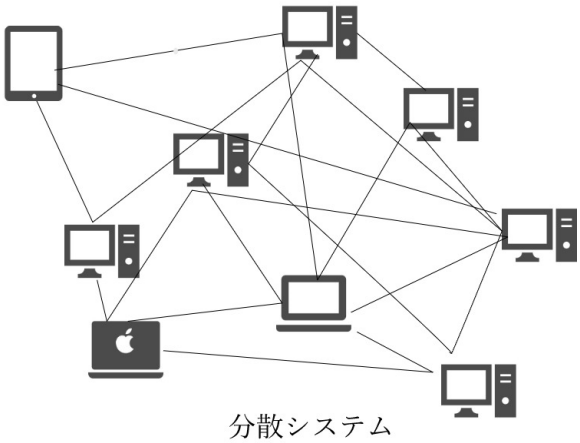
P2Pネットワーク

ピア・トゥ・ピア（P2P）2

- １か所が機能を失うと全体が機能しなくなる集中システム方式（クライアントサーバ方式）ではなく、Ｐ２Ｐを使用することによる分散システム方式（P2P方式）を採用することによりシステムの堅牢性を安価に構築している



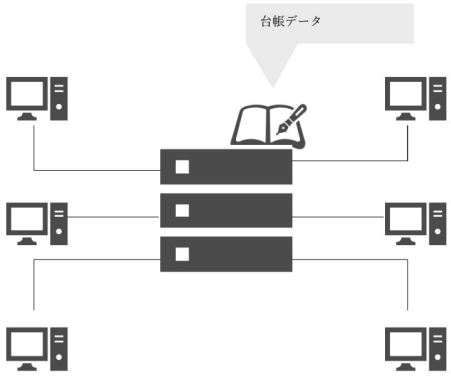
集中システム



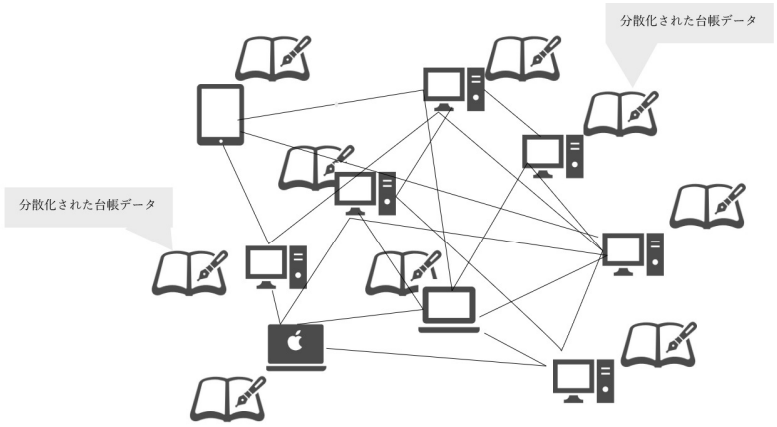
分散システム

ＤＬＴ（分散型台帳技術）

- Ｐ２Ｐで作る分散型システムの中の参加者１台１台の中に台帳を持っている状態である
- デメリットにもつながるが、だれでもこの台帳内部のデータを見ることができる。ただしプライバシーに直結しないデータを入れることで見られても問題ない状態を作っていることがブロックチェーンの特徴である



中央型台帳「セントラルレジャー」



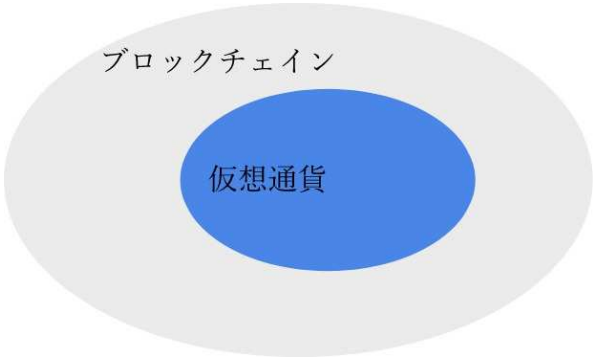
分散型台帳「ディストリビューテッドレジャー」

ブロックチェーン技術総合

- １件のトランザクションに対して、でセキュリティ対策をとる。さらにその１件１件をまとめたブロックについてもセキュリティ対策をとる。（暗号化技術）
- そしてブロックにまとめる際にそのセキュリティ対策を取ったこと自体に対してみんな大丈夫だよね？という確認を取る。（コンセンサスアルゴリズム）
- そもそもその合意形成を取るネットワークも分散型システムで構築するピァ・トゥ・ピァ（P2P）
- 最後にそのデータがある台帳も分散する（ＤＬＴ（分散型台帳技術）
- この４つの技術を組み合わせることでブロックチェーンを安価かつ堅牢に構築している

ブロックチェーンの最大の運用例「ビットコイン」

- 現在ブロックチェーンの最大のユースケースはビットコインである。
- ただ最大のユースケースではあるが、仮想通貨とブロックチェーンは同じものではなく、あくまでブロックチェーンは仮想通貨を実現させているテクノロジーであり、仮想通貨はブロックチェーンという手段を使ったサービスの一つである
- ブロックチェーンを手段としていても仮想通貨ではない別のサービスというものも今後当然出てくる



ビットコインの発行主体は？

- 発行主体は一般的な通貨と違い発行主体はない。しいて言えばブロックチェーンの技術が発行しているといえる
- 特定の誰かが発行しているわけではなく、ブロックチェーンに参加している全員が発行主体だといえる
- そしてその参加者全員がプログラム自体や取引履歴を検証できるようになっていることで、透明性・信頼性が高い仕組みとなっている
- まずビットコインウォレットという専用の財布を持つ。
  そのウォレットIDで管理するため、ビットコインの仕組み上個人情報を管理しない

２種類の鍵で暗号化

- 前述のビットコインウォレットが働くのは個人のデバイス上である
- そしてビットコインウォレットに紐づいた秘密鍵と公開鍵を使ってビットコイン取引の注文がウォレットにある秘密鍵と公開鍵を使って暗号化される
- この暗号化された文字列をビットコインアドレスと呼び、その独自のビットコインアドレスが生成されると注文情報としてインターネットの世界へと飛ぶ。
  この送付先はビットコインネットワーク参加者全員に届く必要がある。
  そして、インターネットを介して参加者全員に向けて不正がないかと確認を依頼する

全ノードが確認

- この参加者をノードと呼びます。
  全ノードがビットコインアドレスが正当なものかを確認し、すべてノードからの承認を得る必要がある
- このノードをつなぐ技術として、ピァ・トゥ・ピァ（Ｐ２Ｐ）が使用されている
- 全ノードから有効確認を受けたビットコインアドレスはビットコインネットワーク内にあるトランザクションプールという場所にためられる。
  ただしこのためられた時点では、注文としては承認されていない。
  「確認済みだが未承認」という中途半端な状態でプールにためられている
- この「確認済みだが未承認」というトランザクションプールにたまった検証済みビットコインアドレスをブロックに詰めていくその作業を競い合い、競い合うことで不正を避ける
- その競争に勝ってブロックを詰めた人が報酬として新規発行されたビットコインを取得できるという流れになる

連携とセキュリティ

- このブロックに詰める競争が１レース終了するとすぐに次のレースが始まる。
  その過程で一つ前にできた最新のブロックの内容を部分的に反映させるような作り方をする。
  このブロックがチェーン上になっているためブロックチェーンという名前がついている

- このつながりを何らかの手段で改ざんした場合、ブロック間で不整合が起きすぐに不正が発覚することになる。
  それを逃れるにはすべてのブロックを改ざんするしかない、
  しかしそのブロックすべては無数のブロック詰め競争が常時行われている。
  そのため普通にブロックができるよりもはやい速度で改ざんしていかなければ改ざんは成功しない、
  スピード競争そのものが改ざんを難しくしているということになる

ブロックチェーンの普及を阻むもの

- ブロックチェーンは考え方がオープンになった後も普及しずらい状況が続いている
- その状況は以下の３つの要素があるためと考えている
  １．ブロックチェーンはビジネスになっていない
  ２．**法律を超えることはできない**
  ３．ブロックチェーンに技術的に向かないこと

ブロックチェーンはビジネスになっていない

- ブロックチェーンは安くシステムを構築できるという諸説があるが、
  あくまでブロックチェーンを利用してサービス運営をする側にとってであって、
  基盤となるブロックチェーンのオープン　ソースを開発することそのものには結構なお金がかかる

- さらに既存技術で問題なく動いてきたシステムをブロックチェーンで作り直すメリットがない。
  あくまでブロックチェーンならではの新しいシステムを構築するビジネスを作る必要がある

法律を超えることはできない

- ブロックチェーンは国の法規を超えて機能することはない。
  既存のやり方で法的に管理されているものはいくら利用者側がブロックチェーンを導入し、
  データ上いくら変更しても、実際の法律上の書類が書き変わらないためどうにもならない

例：不動産登記など
ブロックチェーンで建物や土地の売買そのものは可能かもしれないが、
国が保存している登記簿のデータが書き変わらない限り、登記は移転しない

ブロックチェーンに技術的に向かないこと

- 技術的にブロックチェーンを採用するのに不適切な案件がある
  1. 大きなデータ
  2. 特定のデータのみを検索してすぐ取り出したい場合
  3. 管理対象が、個体管理に向かない場合

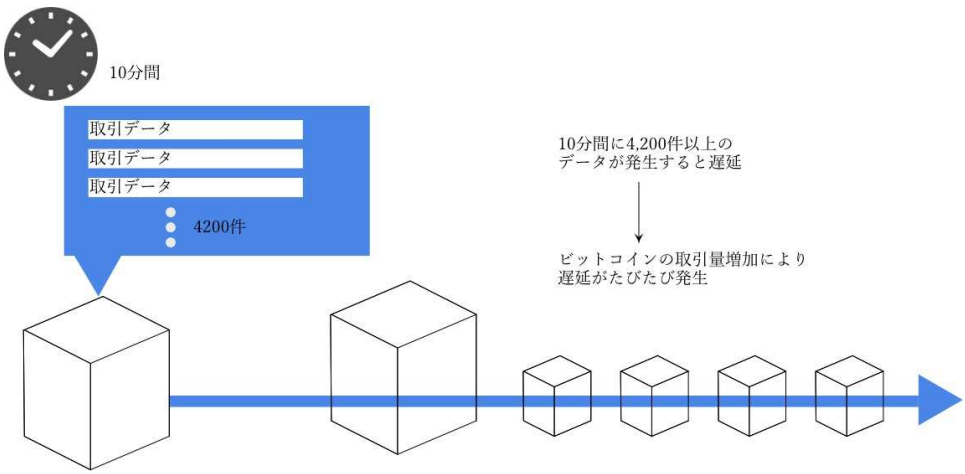
  上記の３つである。

- それぞれブロックチェーンに使用されている技術との相性が非常に悪いものばかりである

大きなデータ1

- 大きなデータは、１件当たりのデータが大きい場合や１日に処理する件数が多い場合両方があげられる。

- 巨大な画像データが何百万件とあって、それをすべてブロックチェーンで保存するとなるとこれは非常に困難である。



大きなデータ

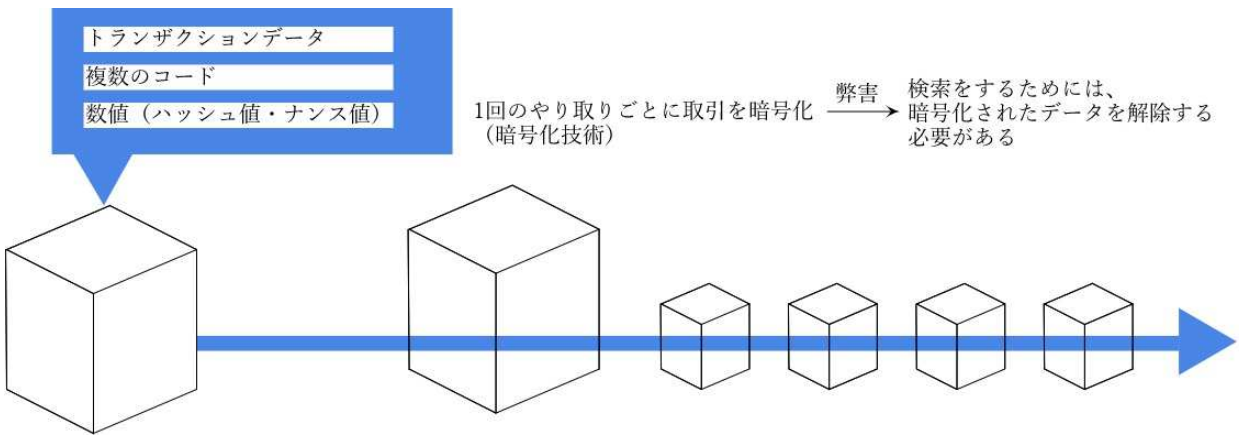
- そもそもブロックチェーンは取引を記録していくものであって、取引される商品自体を保存する技術ではない。

- そのため既存技術でデータそのものはデータベースに保存し、ブロックチェーンはあくまでコンテンツの目録と利用履歴の管理に特化するという分業方式で対応は可能である

特定のデータのみを検索して すぐ取り出したい場合

- まずブロックチェーンでは台帳として過去から今に至るまでのすべての記録が暗号化されて保存されている

- そのため特定の情報だけを参照しようとした場合、すべてのデータを複合化して探す必要がある

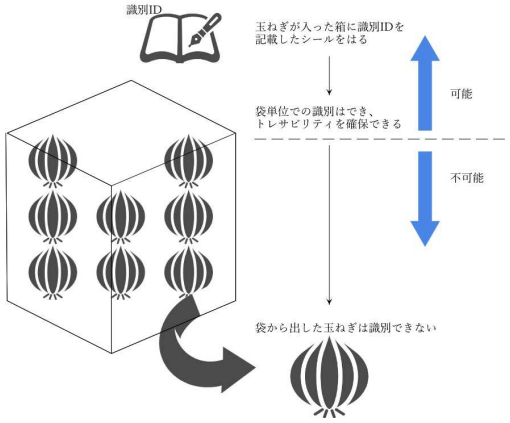


特定のデータのみを検索して すぐ取り出したい場合

- こちらもまた解決策として、新しい手法も出始めているようだが、そもそもその手法自体がブロックチェーンの原則から考えると例外に当たる。
  そのため一般的にはテキスト検索は不得意だと認識したほうが良いと思う
- 過去の変化の履歴を追う場合は非常に適しているが、特定の条件を抽出するという場合は不適切である
- 今回としては解決策というより、要件とブロックチェーン技術がアンマッチである

管理対象が、個体管理に向かない場合

- これはブロックチェーン技術で可能か不可能かというより、物理的に可能か不可能かという話になる
- ブロックチェーンでは一つ一つの箱に識別ＩＤ（以下、シリアルナンバー）をつけるイメージである
- そのため箱単位で出荷するもののさらに中身を判別したい場合、一つ一つの中身にシリアルナンバーをつけて、
  その一つずつを箱に入れる必要がある



管理対象が、個体管理に向かない場合

- 現実問題として、中身一つ一つにシリアルナンバーをつけることがコスト的に可能かどうか、
  そしてそのコストをブロックチェーン導入のメリットで吸収できるほど小さいものなのか？
  という物理的な問題が立ちはだかる。

- 実際の要件の粒度が現実的に可能かどうかということで先ほど同じく要件に対して不適切である

参考

- IPAから以下の報告書が発表されています。
- 「非金融分野におけるブロックチェーンの活用動向調査」の報告書を公開
  https://www.ipa.go.jp/ikc/reports/20191223.html
- 文献調査、ヒアリング調査を実施しています。文献調査ではより実用に近い先進的な取り組みを行っている事例から海外事例23件、国内事例10件を対象として調査を行い、その中から更に海外11社、国内5社へヒアリングを行い、ブロックチェーンの活用における現状、課題、対策を分析しています。


(5) コンビニにおけるサプライチェーンシステム

前提

主な対象業種	サプライチェーン	用途	トレーサビリティ
プロジェクト名	コンビニにおけるサプライチェーンシステム	国	日本

プロジェクト概要

本プロジェクトは、コンビニエンスストアで扱う食品の原材料の調達から店舗に至るまでの一連の流れ（サプライチェーン）に関する情報を、ブロックチェーン技術で集約することで、信頼基盤プラットフォームの構築を目指し、本プロジェクトである、本プラットフォームの構築で、消費者をはじめ、メーカー、卸・物流事業者、小売業など、コンビニエンスストアのサプライチェーンに関わる全てのステークホルダーは、商品がどこで作られ、どこに運ばれ、どの店舗で売られたのか、消費期限はいつかなど、食品の品質に関する情報を、安全かつ手軽に確認できるようになり、扱いやすいサプライを確保することができる。

本プロジェクトでは、メーカー以降のサプライチェーンシステムをスコープとしており、ブロックチェーン適用の可能性や技術的な課題について検証することを目指したものである。なお、個品管理に必要な個品識別技術（RFIDやQRコード）については、解決方法が確立している。

サービスのシステムイメージ

出典）https://www.mizuho-ir.co.jp/company/release/2018/lawson0926.html

組織

プロジェクトオーナー	名称	ローソン	分類	大企業/ユーザ
主な共同、連携先	名称	みずほ情報総研	分類	大企業/アプリケーション開発
			国	日本

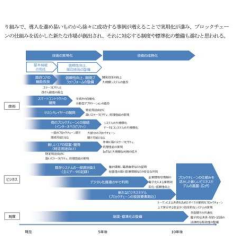


図 5-14 非金融分野におけるブロックチェーン実現化の流れ

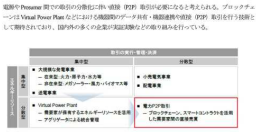


図 5-8 電力事業の管理体制・リソースごとの概況と発展の方向性

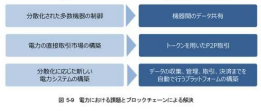


図 5-9 電力における課題とブロックチェーンによる解決

考察

- ブロックチェーンを学習してみて改めて分かったこととしては、ブロックチェーンは仕組みであると感じた。

- ブロックチェーンを導入するためには、国や業界内の有力なプレーヤーが足並みをそろえて導入するのが理想的ではあるが、日本はすでに経済成長を支えてきたかなりの精度で出来上がった社会の仕組みそのものがあり、その社会の仕組みを捨てて新しくブロックチェーンを導入するメリットがあまりない。

- そのため既存の仕組みがない発展途上国のほうがほぼゼロの状態から仕組みを構築することが可能な分、普及のハードルが低いと思われる。

- 同時にブロックチェーンはビジネスモデルでもあるため、導入するに最適な環境が把握できるということはすでにビジネスとして成立しているということでもあると考えている