



平成29年度 第2回関東テレコム講演会

# ブロックチェーン概要とユースケース

2018年2月15日（木）

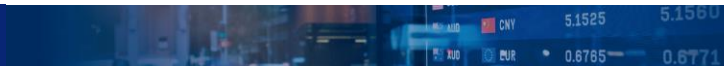
貝塚元彦

日本証券アナリスト協会検定会員  
インダストリー・コンサルタント

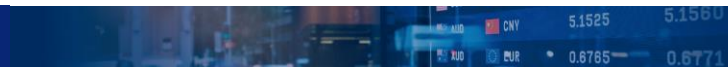
ブロックチェーン・ソリューション部長  
インダストリー・ソリューション事業開発  
日本アイ・ビー・エム株式会社

# 目次

1. FinTechのトレンド
2. ブロックチェーン概要
3. IBMの取り組みとHyperledger Fabric
4. ブロックチェーンの適用領域と事例



# 1. FinTechのトレンド



# AI Watson 適用領域と事例

## 人とシステムが共存し、共に思考する銀行業務を実現

### 対話

#### ①自然言語でコンピューターと応対ができるようになった

- ・ タブレットやPC等の端末に“自然言語”で入力し、その内容をWatsonが解釈し、情報を探り当てることができる

#### Automatic response of chat BOT

Web、スマホアプリ、SNSなどをIFとして顧客からの照会対応をチャットBOTで実現

### 認知

#### ②組織知・蓄積された声・画像からの示唆を得られるようになった

- ・ 組織で蓄積されたマニュアルや規定、規約、または、コールセンターで蓄積された声といったデータからより、実用的な気付き・示唆を得られること

#### Call Center operator support

コールセンターで照会された内容に応じて自動的に最適な回答を作成するオペレーター支援機能

### 学習

#### ③起こりうるパターンを全てルール化しなくても学習した結果を活かせるようになった

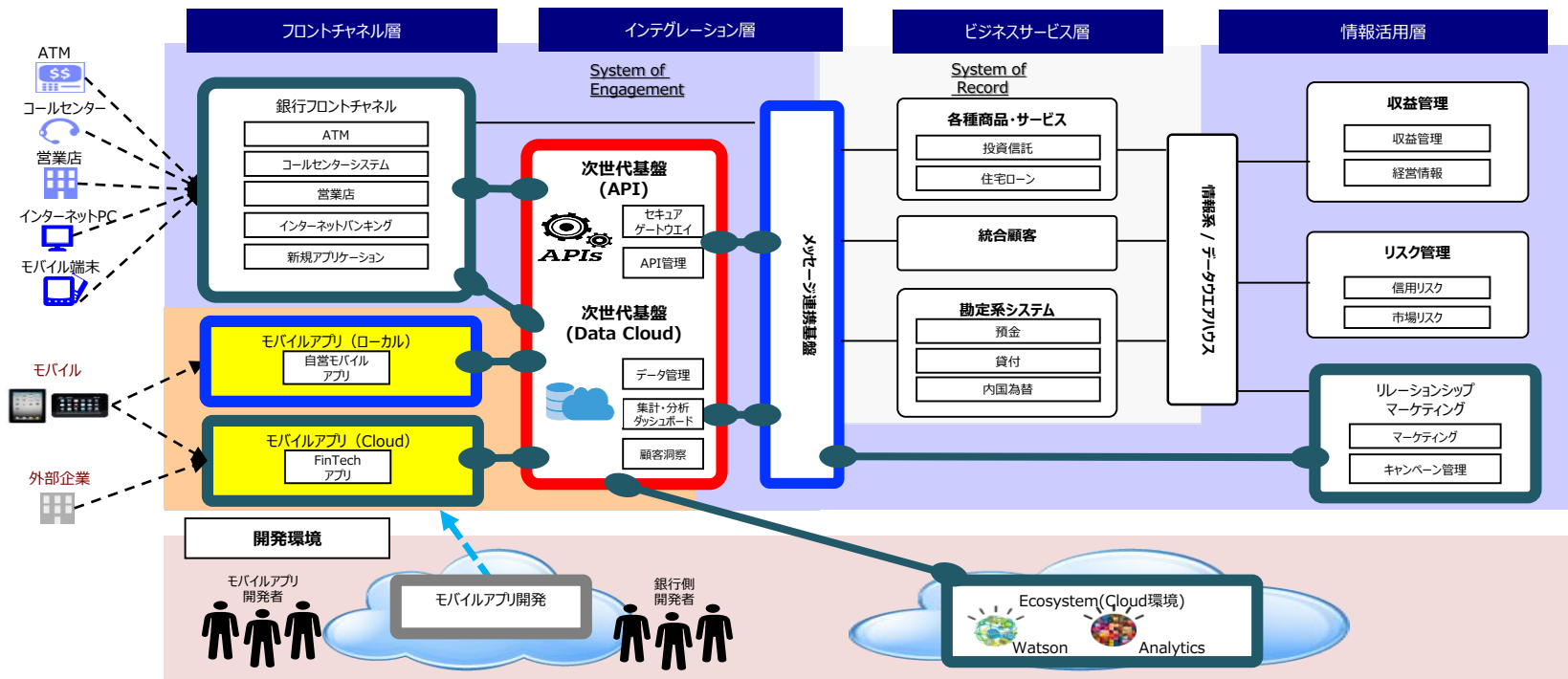
- ・ 想定されるケースや事後で発生した事象・結果をもとに学習し、その後の処理に活かすことができる

#### Insurance payment assessment work support

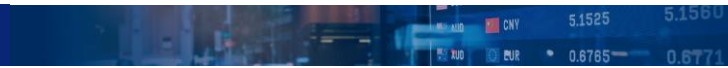
過去査定事例をシステムが学習し、経験の浅い社員でも高品質な査定が実現可能となった

# API バンキング

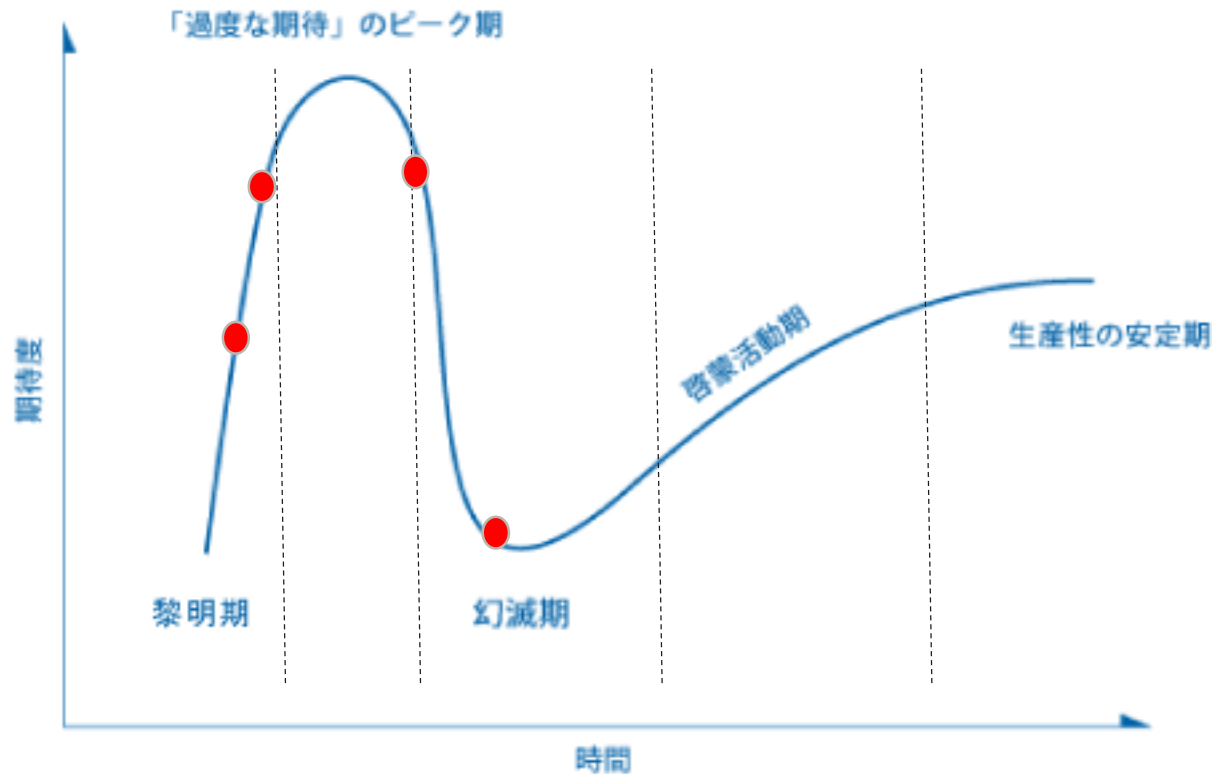
既存システムとの連携および、外部企業との接続にオープンAPIを活用し、今まで以上に接続範囲の拡大が可能になり新しいビジネスを創出します



## 2. ブロックチェーン概要



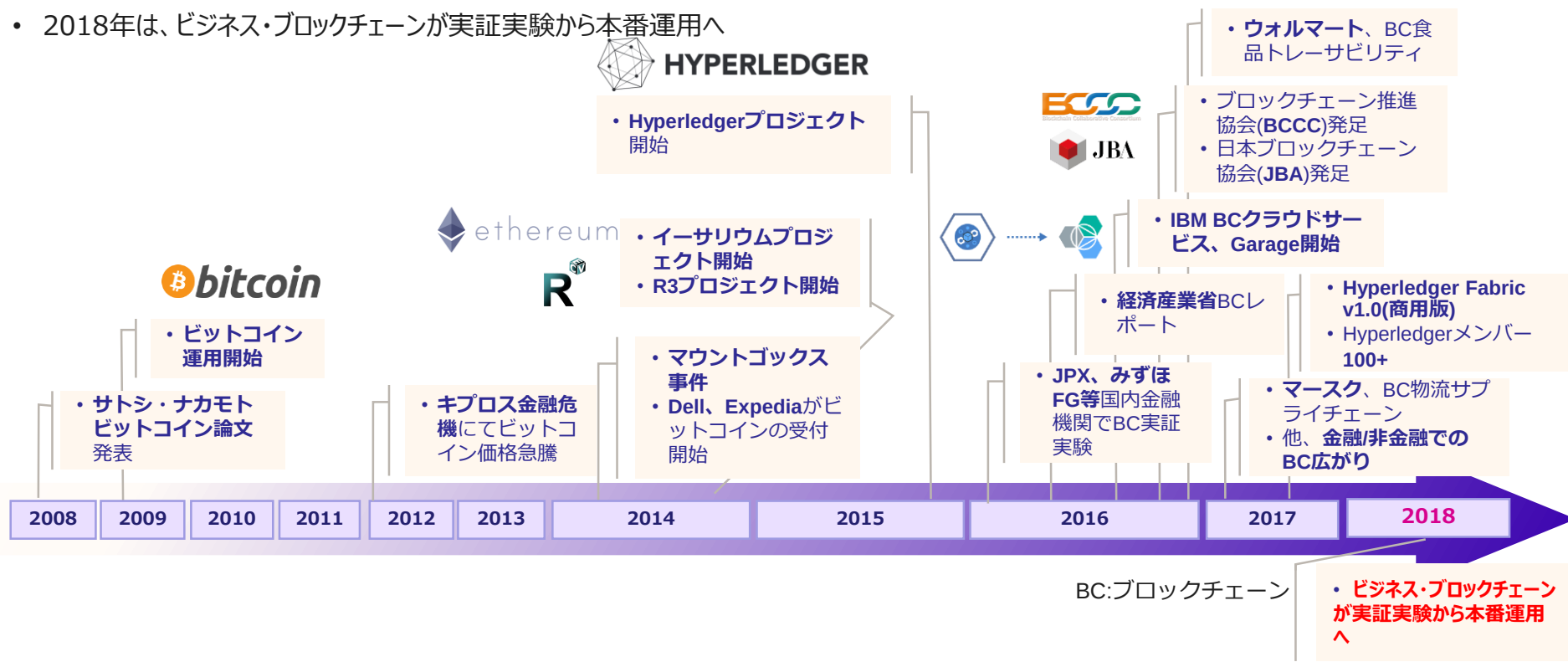
# ガートナー「先進テクノロジーのハイプ・サイクル」



出典： [http://www.gartner.co.jp/research/methodologies/hype\\_cycle.php](http://www.gartner.co.jp/research/methodologies/hype_cycle.php)

# ブロックチェーンの歴史：仮想通貨からビジネス・ブロックチェーンへ

- ・ 暗号(仮想通貨)：ビットコインへの注目の高まりから、特に昨年、国内で金融機関を中心にブロックチェーン(あるいは「分散台帳技術」)の活用検討、検証が活発に。
- ・ 2017年は、基盤技術の成熟化とともに、金融/非金融でビジネスへのブロックチェーンの適用検討が本格化。
- ・ 2018年は、ビジネス・ブロックチェーンが実証実験から本番運用へ



BC:ブロックチェーン

・ ビジネス・ブロックチェーンが実証実験から本番運用へ



# ブロックチェーン適用が検討されている業務

ブロックチェーン技術は、各種デジタル資産の保管、資産の所有権移転を安全かつ確実に実施できる技術であると考えられています。以下のように各業界で適用が検討され効果が見込まれています。

## 仮想通貨



「ビットコインの国内取引高は2016年1-6月期に4300億円、7月は単月で2000億円を突破」した(2016/8/16日本経済新聞 電子版)。日本国内では、改正資金決済法も整備され、仮想通貨の両替所市場は今後も規模の拡大が予想される。

## 国際送金



ブロックチェーンによる非集中型の送金サービスにより、透明性やスピードの向上、コストの削減が可能になる。仮想通貨の両替所を使った海外送金サービスなども可能である。

## 証券取引



多くの証券取引所で、ブロックチェーンによるポスト・トレーディング処理の効率化など、証券市場の改革が検討されている。

IBMはJPXと共同に低トランザクション市場を想定したブロックチェーン技術の実証実験を行った。

## 資産管理



不動産登記簿など、ブロックチェーンを資産台帳として使用することで、資産に関するすべてのステークホルダーが、直接その資産の情報を見たり、取引をすることが可能になる。

## 契約管理



ブロックチェーンによって契約管理ができれば、契約が進行するに連れ最新状態が記録され、改ざん不可能な監査証跡が保存される。ただし、スマートコントラクトを契約書として利用するには、電子署名法など関連法について当局への確認が必要であらう。

## 保険



保険加入者は、仲介者を介さずにダイレクトに契約を結ぶことができ、保険市場の透明性および正確性が向上する可能性がある。例えば、ロンドン保険市場をブロックチェーンによって改革しようとしている企業もある。

## 貿易金融



貿易金融には平均12社が関与し、27の文書がやりとりされる複雑なプロセス。

スマートコントラクトによる自動化により、効率性、スピード、正確さが向上し、リスクを低下させる可能性がある。

## サプライチェーン マネージメント



複雑なサプライチェーン・ネットワークにまたがる取引をブロックチェーン上に記録することで、プロセスのエンド・ツー・エンドでの可視化・効率化が可能になり、製品の来歴管理が可能になる。



IBMが提唱する「デバイス・デモクラシー」では、「ブロックチェーンはIoTの世界において相互に連携するデバイス間のトランザクションを管理・調整する枠組みとして非常に有用である。」と謳っている。

## 本人確認



個人認証の重要性が高まっているが、いまだ運転免許証のコピーを利用するといった方法が行われている。ブロックチェーンを使えば、低コストで安全に本人確認情報を共同所有するしくみが構築できると期待されている。

## 自立分散型組織



ブロックチェーンは、社会貢献を目的としたソーシャルビジネスのための持続可能なプラットフォームとして利用できる。これにより、全ての人の公平なサービスの提供が期待される。

## スマートグリッド



中央集権型のシステム構成では、柔軟な分散エネルギー市場の構築は難しい。小売・送電網自由化のもとでは、ブロックチェーン技術を使った分散エネルギーの市場の構築が期待される。

# 弊社ブロックチェーン・プロジェクト事例

海外400件,国内40件以上のプロジェクト実績に基づく経験、アセット、高品質な開発手法をご提供可能です。

## 主な海外実績（公開済のみ）

|                                |                   |
|--------------------------------|-------------------|
| HSBC, Bank of America, IDA     | 貿易金融・信用状          |
| ABN AMRO                       | 経営再建・回復           |
| Crédit Mutuel Arkéa            | 合併共有台帳            |
| Kouvola Innovation             | サプライ・チェーン・ロジ      |
| London Stock Exchange          | 市場革新              |
| IBM Global Financing           | 争議解決のためのシャドー・チェーン |
| Everledger                     | ダイヤモンドの来歴         |
| China UnionPay                 | ロイヤルティ・ポイント管理     |
| CLS                            | バイラテラル・ネットティング    |
| UBS                            | 貿易金融              |
| Walmart                        | サプライ・チェーン         |
| Postal Savings Bank of China   | カストディ業務           |
| Dubai Government Agencies      | 貿易金融と物流トラッキング     |
| Maersk                         | クロスボーダー・サプライチェーン  |
| AIG / Standard Chartered       | 多国間保険             |
| Deutsche, HSBC, Rabobank, etc. | デジタル・トレード・チェーン    |

## 国内実績（公開済のみ、公開日順）

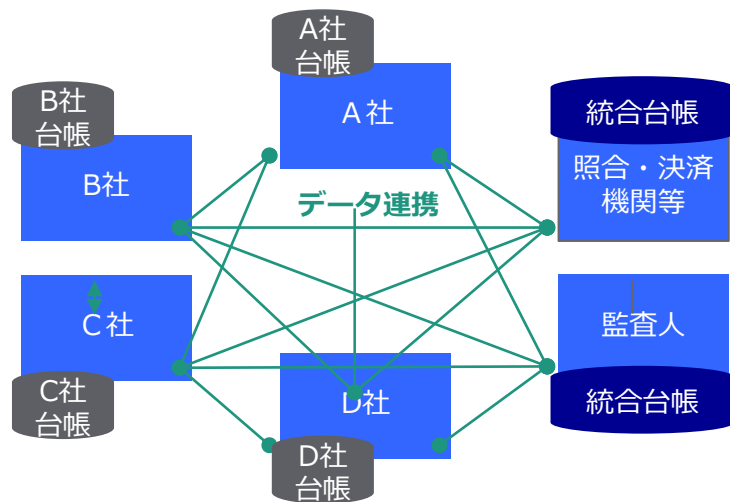
|                             |                  |
|-----------------------------|------------------|
| 日本取引所グループ (JPX)             | ポスト・トレード         |
| みずほフィナンシャルグループ              | デジタル通貨           |
| 三菱東京UFJ銀行                   | 契約管理             |
| SBI証券                       | 債券取引             |
| 三井住友信託銀行                    | グローバル・カストディ業務    |
| 三井住友銀行                      | 貿易関連書類の電子化       |
| みずほフィナンシャルグループ              | 貿易金融基盤           |
| 岩手銀行他                       | 法人顧客との収納業務       |
| 沖縄銀行                        | 食券販売・管理システム      |
| デジタル・アドバタイジング・コンソーシアム (DAC) | デジタル広告効果透明化      |
| イオンフィナンシャルサービス              | アジア圏金融プラットフォーム構築 |
| ソニー                         | グローバル教育情報の共有基盤構築 |

IBMはBlockchainテクノロジー・リーダーにおけるNo.1の評価を受けました。（2位 Microsoft社, 3位 Accenture社）

※2017/9/18 Juniper Research社 "IBM Ranked No1 Blockchain Technology Leader"

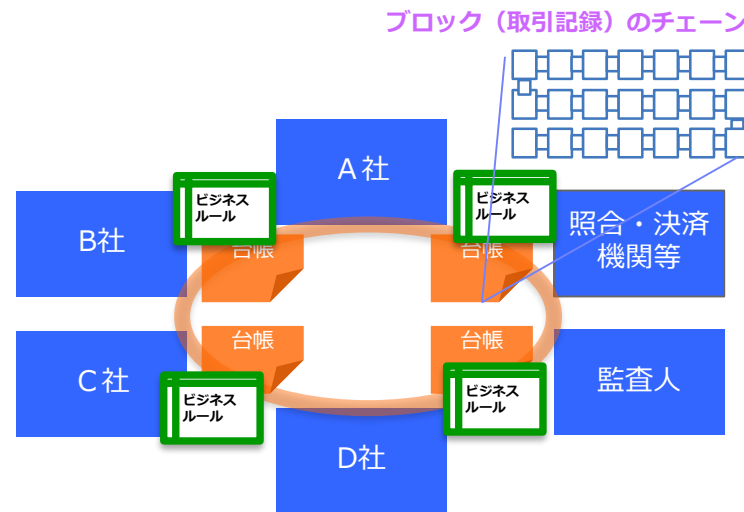
# ブロックチェーンとは：分散台帳技術 (DLT: Distributed Ledger Technology)

- ネットワークの全取引の履歴を記録する台帳を、それぞれの参加者がもちます。
- ブロックチェーン技術を用いて台帳管理を非集中化することにより、各種取引の**期間・コスト・脆弱性**を改善することが期待されています。



従来台帳管理

- 各参加者が個別内容の台帳を保有
- 決済機関等による集中データ管理
- 各社システム間での個別のデータ連携



ブロックチェーンでの台帳管理

- すべての参加者が同一内容の台帳を保有
- 管理主体を持たない非集中・分散データ管理
- ブロックチェーン機能による統一されたデータ連携

# ブロックチェーンの技術構成 (Hyperledger)

- 参加者間でやりとりされる各種（資産）取引を記帳する

分散台帳

スマート  
コントラクト

- ビジネスロジックによる処理の自動化や、柔軟な台帳の活用を実現する為の仕組み

- 分散ノード間で、台帳の同一性を確保するための仕組み

コンセンサス  
（合意形成）

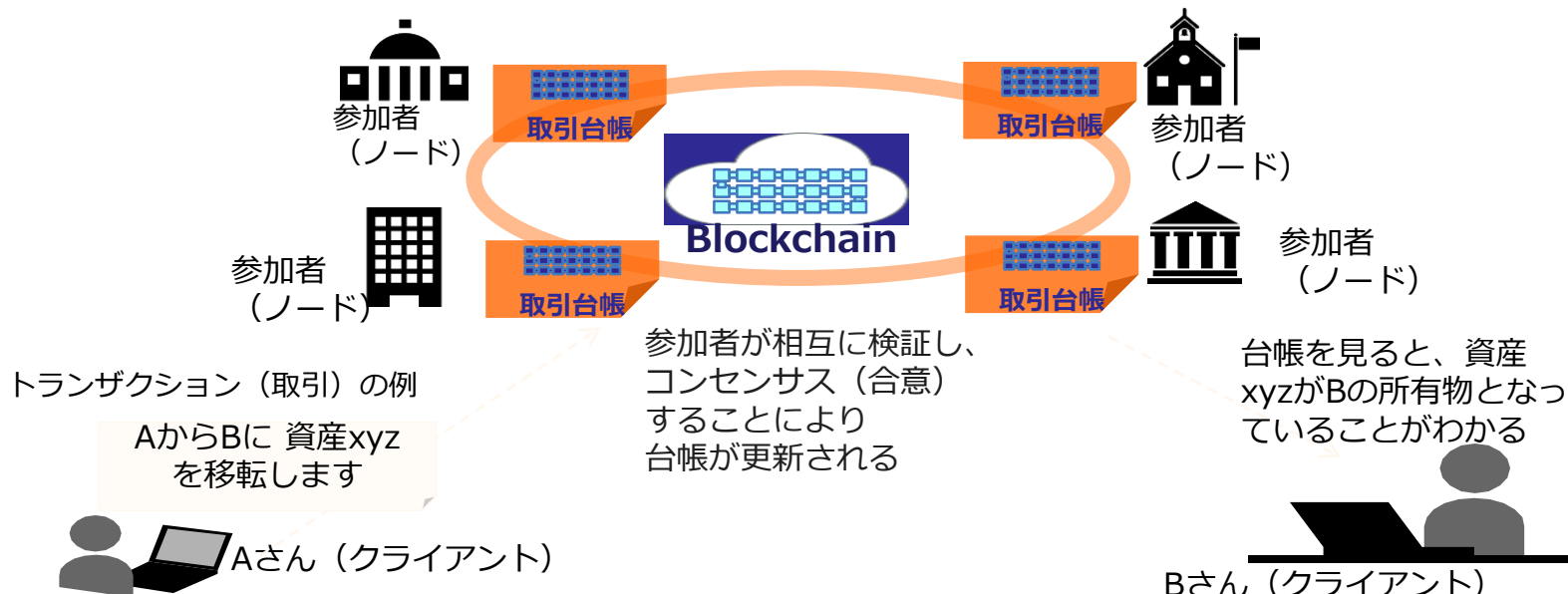
セキュリティ

- 参加者間の匿名性を確保したり、取引内容のプライバシーを保護する為の仕組み

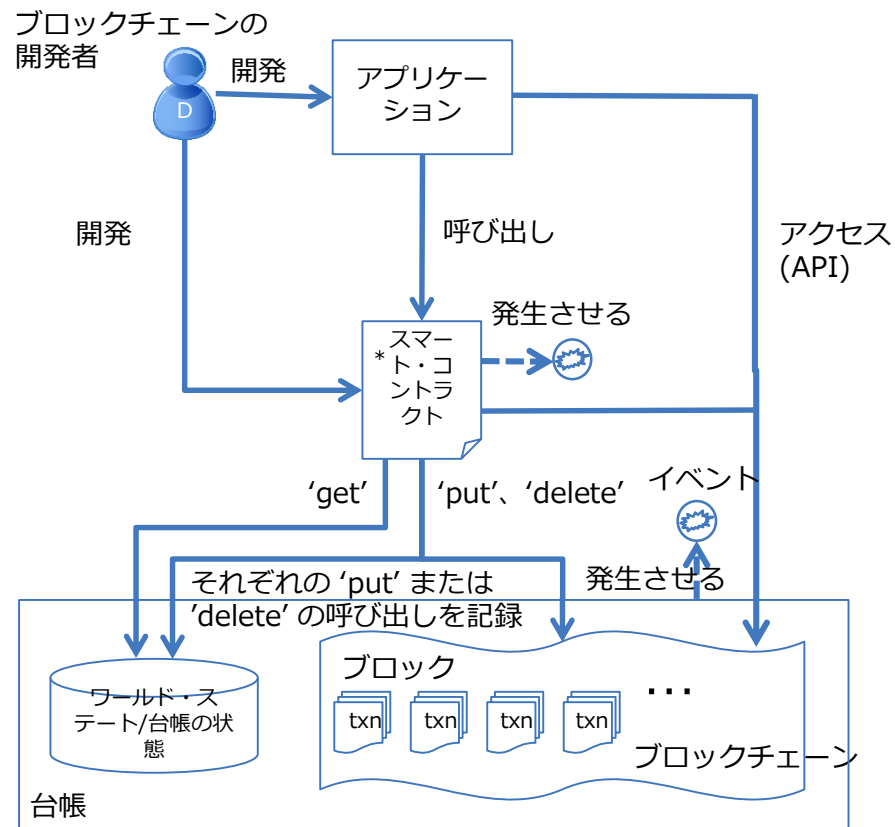
# ブロックチェーンの基本構造

|            |                    |
|------------|--------------------|
| 分散台帳       | スマート<br>コントラ<br>クト |
| コンセン<br>サス | セキュリ<br>ティ         |

- **トランザクション（取引）**の情報が、すべての参加者に送られます。
- 全ての参加者が、**同じ台帳の複製**を持っています。
- 台帳は、過去の記録が改竄できないような、**特殊な構造**を持っています。
- 台帳は参加者の**コンセンサス（合意）**によって、**更新**されます。



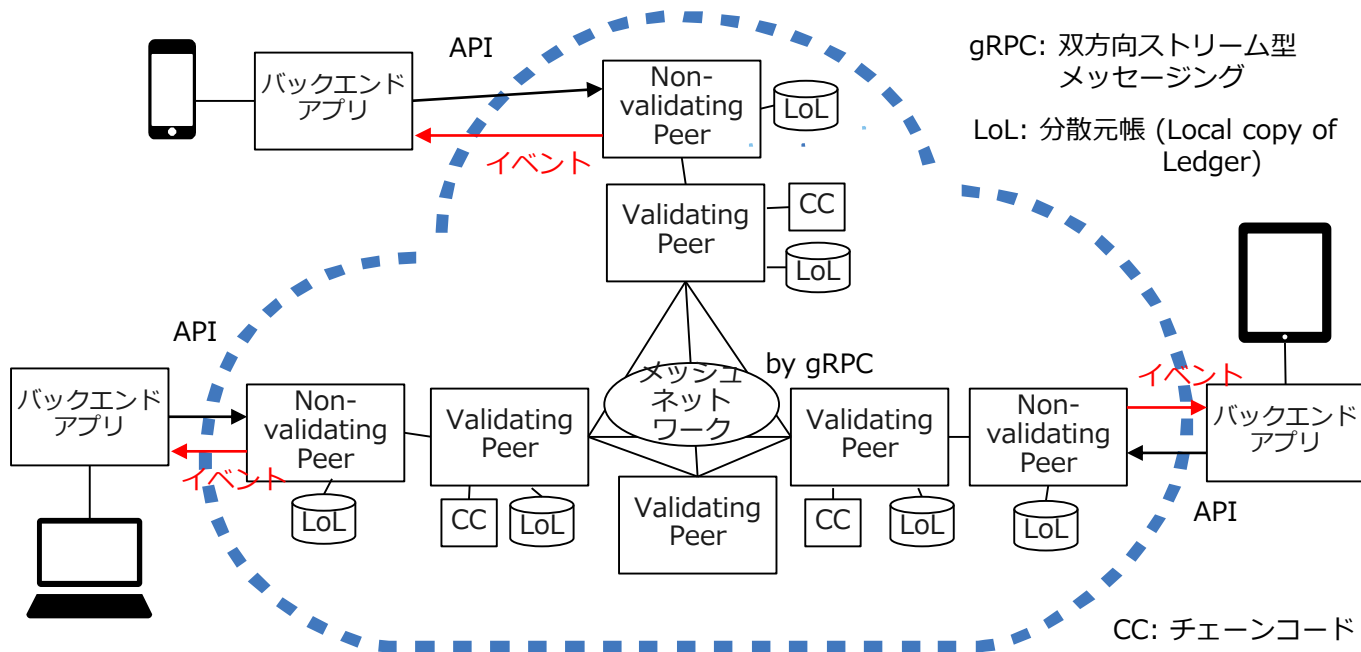
# ブロックチェーン・アプリケーションと分散台帳



\* スマート・コントラクトは、チェーンコードを使用して実装

## 2種類のアプリケーション

- Blockchain API をコールするクライアント・アプリを開発
- Blockchain チェーンコード（スマート・コントラクト）を開発



# 分散台帳

- 参加者間でやりとりされる各種（資産）取引を記帳する為の仕組み
  - 証券（株・債券）
  - 証書（貿易・保険）
  - 登記（不動産）
- 全ての参加者が同じ台帳の複製を持つ
- 追記のみ可能、改竄不可能
- ビジネスでは各種資産を管理する為、複数の台帳を管理

トランザクション  
= 1回の取引記録



|      |  |
|------|--|
| 分散台帳 |  |
|      |  |

台帳  
= 過去の全てのトランザクションの記録





# コンセンサス

|            |  |
|------------|--|
|            |  |
| コンセン<br>サス |  |

- ブロックチェーンは、分散したノードが同一の情報を保持するための技術
- 分散したノードが同一の情報を保持するためには、
  - 更新する情報が正しい事
  - 更新後に、それぞれのノードのデータが同一になることを確認する必要がある
- この確認を行う仕組みを「コンセンサス」と呼ぶ
- コンセンサスには様々な仕組みを使うことが可能
  - ビットコインにおける「マイニング」
  - 多数決
  - 分散コンセンサス形成アルゴリズム
  - etc.



# ビザンチン将軍問題

- ビザンチン帝国の将軍たちはお互いに離れた場所において、伝令で他の将軍たちと連絡を取っている
- 作戦成功のためには、一斉に攻撃を仕掛ける必要がある
- 万が一、裏切った将軍がいて、嘘の指令を伝達すると、統一した行動がとれずに敗北する可能性がある
- 裏切った将軍がN人のとき、忠実な将軍が $2N+1$ 人以上であれば、正しい統一行動をとることができる
- 出典: 国立情報科学研究所ニュース NII Today Vol. 69, Sep. 2015.  
[http://www.nii.ac.jp/userdata/results/pr\\_data/NII\\_To\\_day/69/all.pdf](http://www.nii.ac.jp/userdata/results/pr_data/NII_To_day/69/all.pdf)
- レスリー・ランポート博士の考案した分散システムの信頼性にかかわる問題

図2 | 3人のビザンチン将軍(裏切り者1名を含む)

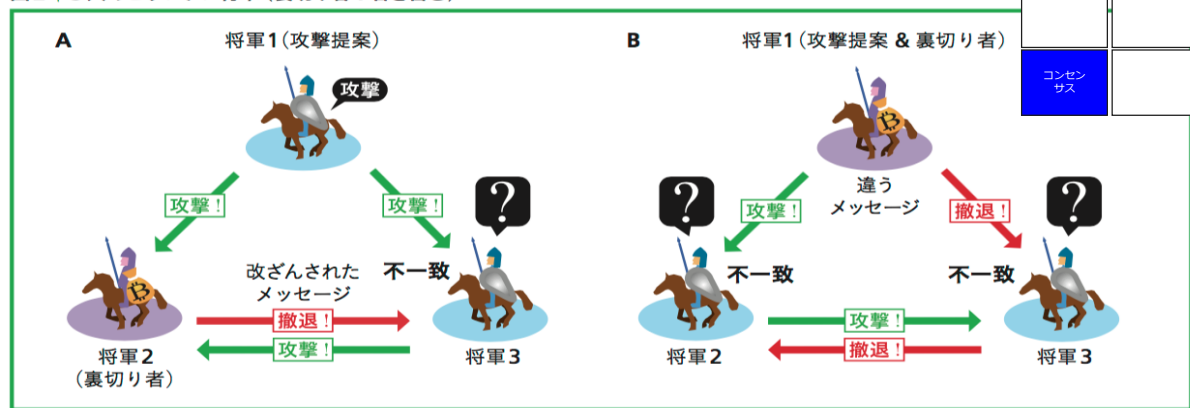
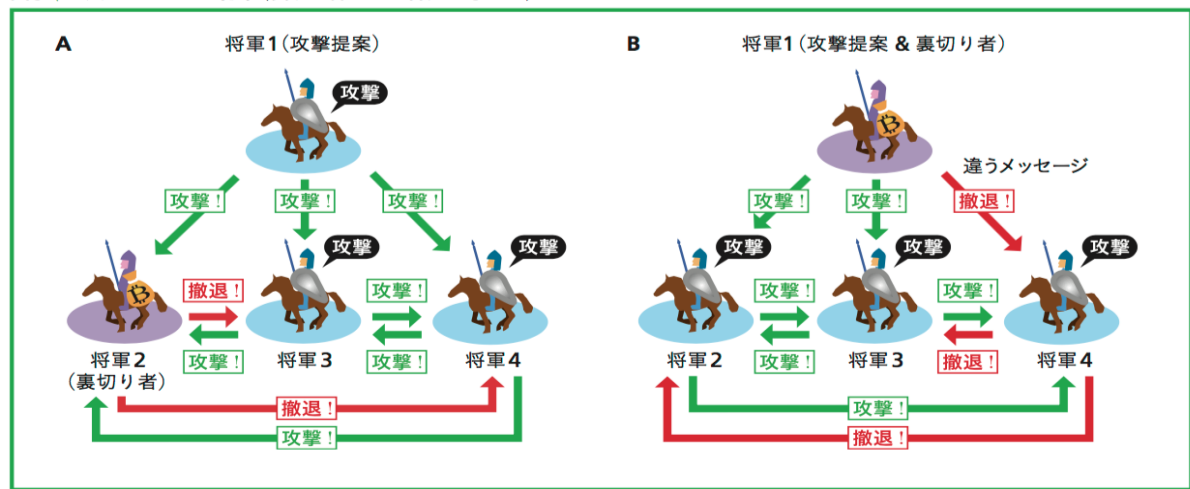
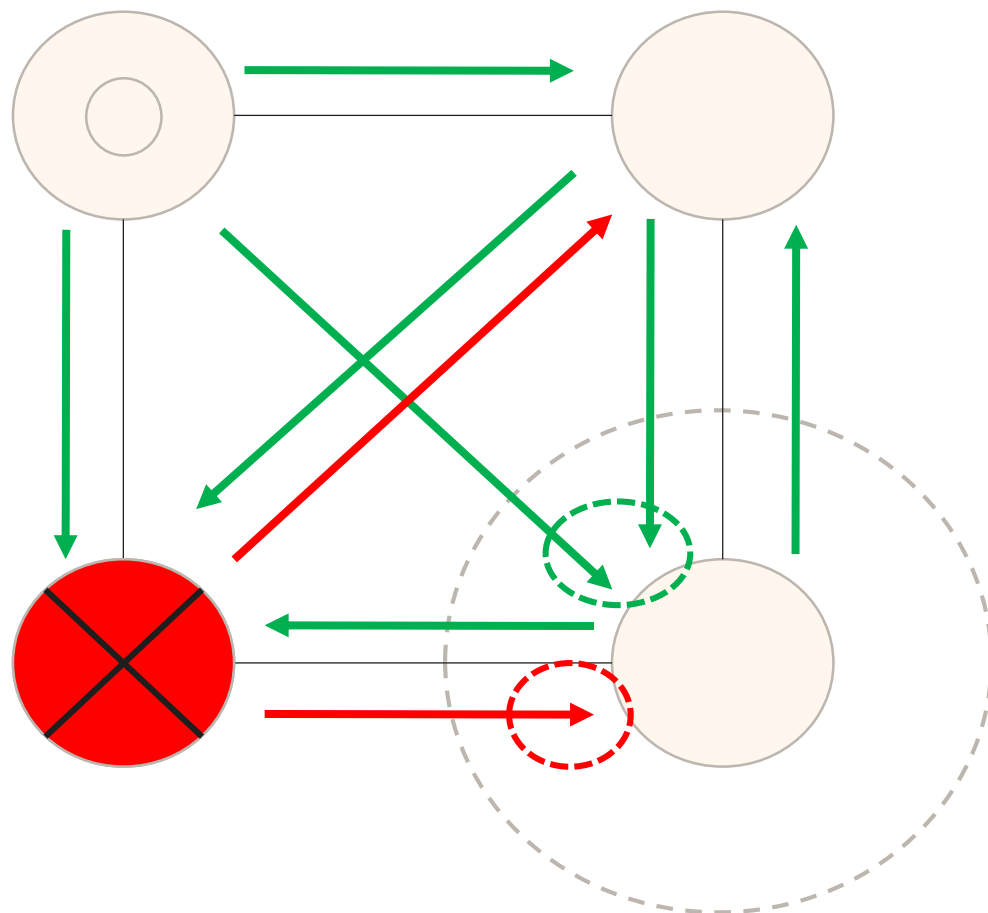


図3 | 4人のビザンチン将軍(裏切り者N=1名、 $4 \geq 3N+1$ )





# コンセンサス方式のいろいろ

|        |  |
|--------|--|
|        |  |
| コンセンサス |  |

| 管理者          | 無し                                                                                             | 複数企業                           | 単一企業    |
|--------------|------------------------------------------------------------------------------------------------|--------------------------------|---------|
| ネットワーク形態     | パブリック型                                                                                         | コンソーシアム型                       | プライベート型 |
| P2Pへの参加      | 自由                                                                                             | 許可制                            |         |
|              | 不特定、悪意のある参加者を含む可能性がある                                                                          | 参加者の身元が判明しており、信頼できる            |         |
| コンセンサス方式     | Proof-of-Work (mining)                                                                         | 分散コンセンサス形成アルゴリズム               |         |
|              | <ul style="list-style-type: none"> <li>電力消費が多い</li> <li>ファイナリティがない</li> <li>51%攻撃問題</li> </ul> |                                |         |
| トランザクション処理時間 | 長い(例:10分)                                                                                      | 短い(例:数秒)                       |         |
| 代表的なユースケース   | 仮想通貨                                                                                           | 銀行間送金、証券取引など<br>ビジネスネットワークでの使用 |         |
| 実装例          | Bitcoin, Ethereum                                                                              | Ripple, DAH, Hyperledger       |         |

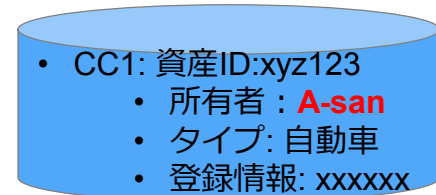
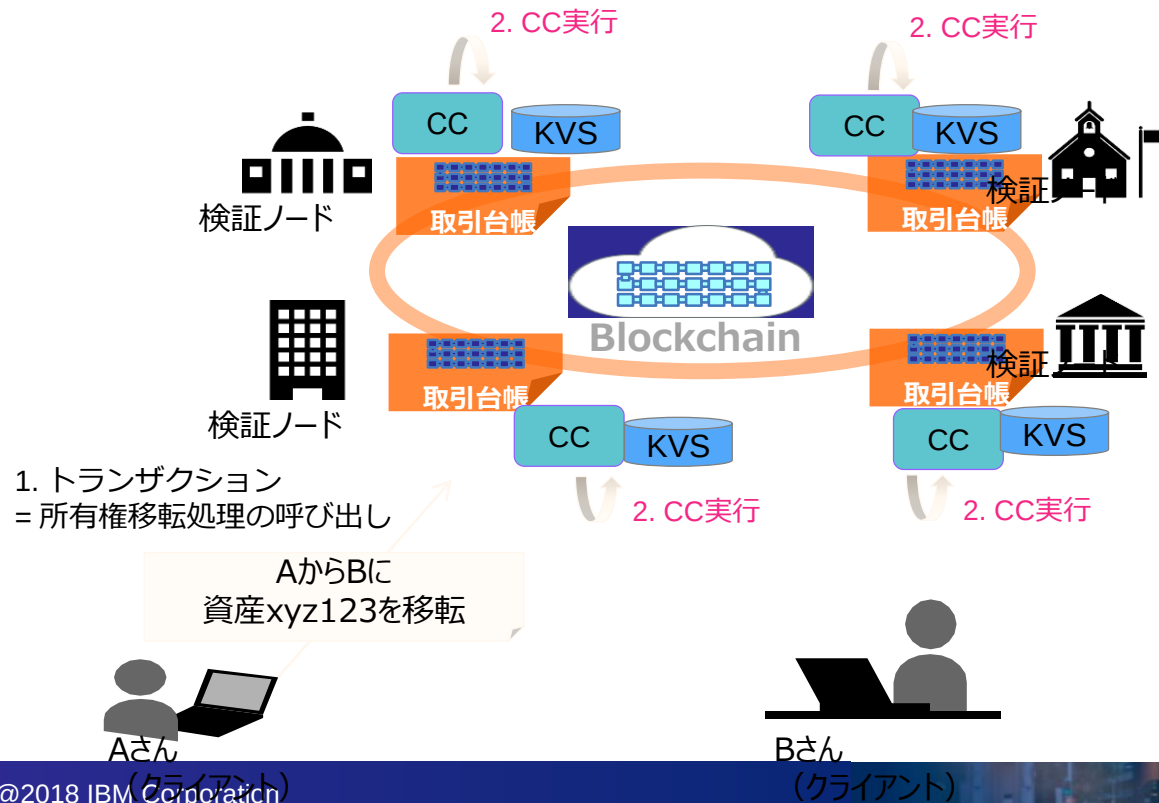
Hyperledger: 業務使用における重要性

→ ユースケースに応じて、異なるコンセンサス方式を利用できる

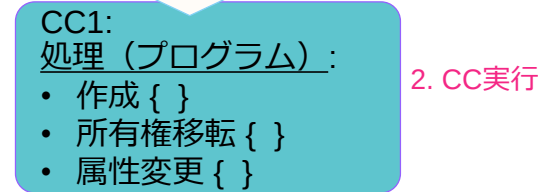
# スマートコントラクト

チェーンコードにより、プログラムを分散ノード上で実行し、複雑なトランザクション処理の自動化が可能になる

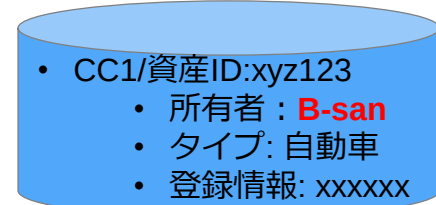
## 0. トランザクション実行前



## 1. トランザクション発生



## 3. トランザクション実行後



# ブロックチェーンで検討すべきセキュリティ要件



## Hyperledger Fabricが 提供する機能

アクセス制御

アイデンティティ  
管理

データ流出の防止

鍵の不正利用の防止

アプリケーション

ブロックチェーン  
プラットフォーム

基盤レイヤー

プライバシー管理

マルウェアの  
侵入防止

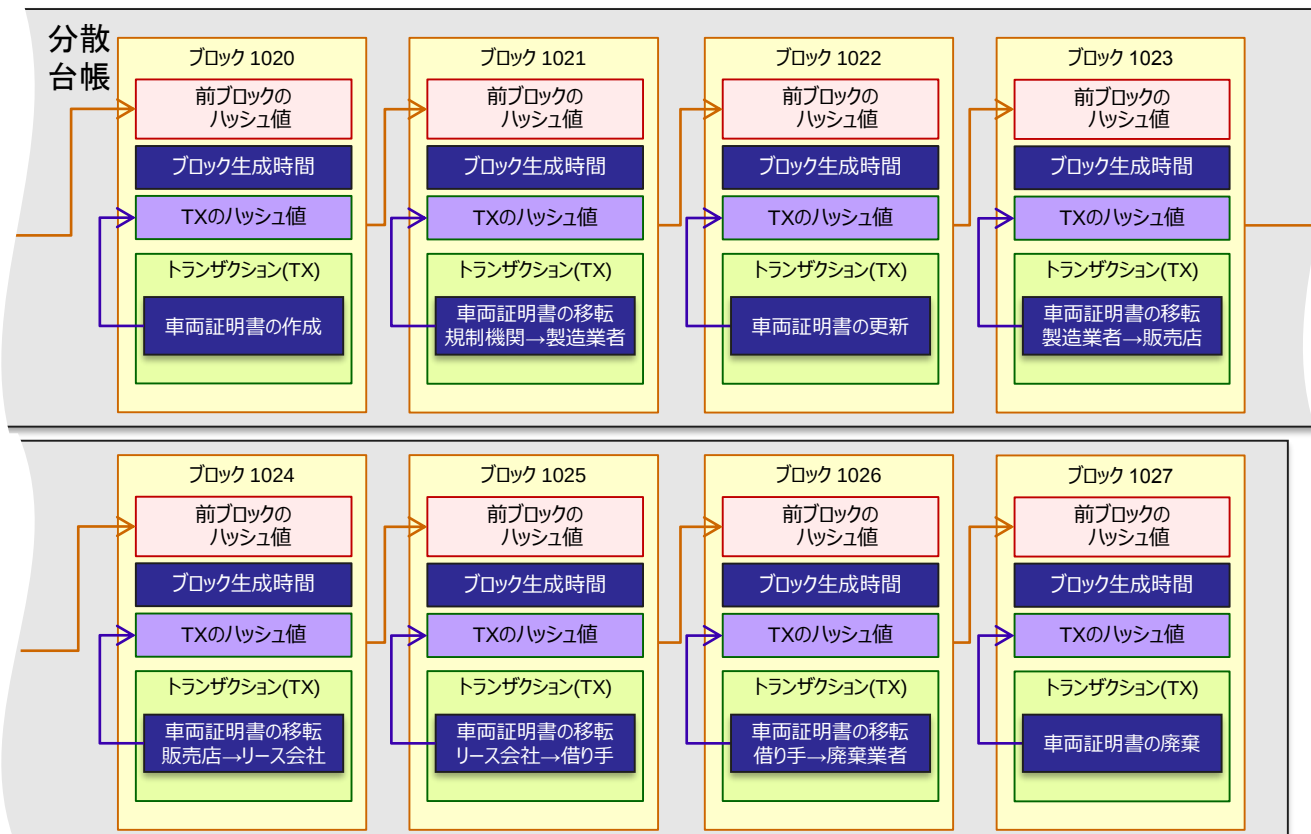
# Hyperledgerのセキュリティ機能



| セキュリティ要件   | 実現方法                                                                                                                                         |
|------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| ユーザー認証     | ユーザーIDとログインによりユーザー認証を行う。                                                                                                                     |
| トランザクション認証 | Hyperledger の電子証明書 の仕組みにより、トランザクションを認証する。<br>アプリケーションにログイン中のユーザーIDごとに、Hyperledger の電子証明書を紐づけ、それぞれのトランザクションをどのユーザーが発行したかを、電子署名によって確認することができる。 |
| プライバシー保護   | 匿名証明書により、トランザクション実行者を匿名化できる                                                                                                                  |
| データの暗号化    | Hyperledger のセキュリティ機能により、トランザクションの内容を暗号化する。                                                                                                  |
| アクセス制御     | チェーンコードの中でアクセス制御を行い、ユーザーごとに実行できるトランザクションを制限する。また、データへのアクセス（read/write）も、チェーンコード内でアクセス制御を行う。                                                  |
| 監査対応       | トランザクションのデータがブロックチェーン上に記録されるため、監査証跡として利用できる。                                                                                                 |
| 可用性        | 一部のノードの障害発生時も他のノードでの実行が継続できる。                                                                                                                |

# 耐改竄性：台帳の仕組み (HyperLedger Fabricの例)

- 分散台帳は、前のブロックのハッシュ値とトランザクション、トランザクションのハッシュ値とタイムスタンプからなるブロックのつながりでできています。



## ハッシュ関数（要約関数）：

- あるデータが与えられた場合にそのデータを代表する数値（ハッシュ値）を得るための関数のこと。
- 元データが少しでも変更されると、全く異なる結果（代表値）が返される。
- 代表値から元データを類推刷ることは不可能。



# IBM Blockchain Platformが解決します

## インダストリー・プラットフォームを実現する基幹テクノロジー



ビジネス・ネットワークを迅速に立ち上げ、  
本格運用できる 統合ブロックチェーン基盤

- Hyperledger Fabric V1をベースとした  
IBM Cloud 上のPaaS
- アイデアをすぐ形にできる開発環境  
(Hyperledger Composer)
- ライフサイクル全般を支援するツール群
- 異次元のセキュリティ、性能、連続稼働
- 24時間365日のサポート

### Develop - 開発

ブロックチェーン・アプリケーション開発  
を加速するクラウド・サンドボックスと  
「遊び場(プレイグラウンド)」

### Govern - ガバナンス

コンソーシアム型のブロックチェーン・  
ネットワークの立上げと民主的な運営を  
支援するツール群

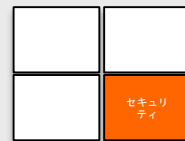
### Operate - 運用

本番利用を想定した性能とセキュリティを  
備えるIBM Cloud上の常時稼働システムと  
IBMによるフルマネージド・サービス

# IBM Blockchain Platform :

実証実験から本格展開まで支える3つのプラン

国内含む全世界のデータセンターからサービス提供中



| プラン | 1 Starter※                                                                                | 2 Enterprise                                                                                        | 3 Enterprise Plus※                                                                                  |
|-----|-------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| 目的  | 実証実験向けプラン                                                                                 | 本番業務向けプラン                                                                                           | セキュリティや性能要件が<br>厳しい業界向けプラン                                                                          |
| 特徴  | <ul style="list-style-type: none"><li>分散ネットワーク</li><li>管理されたピア</li><li>モニター・ツール</li></ul> | <ul style="list-style-type: none"><li>共有セキュア・コンテナ</li><li>ガバナンス・ツール</li><li>高可用性</li></ul>          | <ul style="list-style-type: none"><li>専有セキュア・コンテナ</li><li>ガバナンス・ツール</li><li>高可用性</li></ul>          |
| 課金  | <ul style="list-style-type: none"><li>ピア時間単位</li><li>51円/時間～<br/>(最小構成)</li></ul>         | <ul style="list-style-type: none"><li>参加メンバー単位</li><li>ピア・インスタンス単位</li><li>約20万円/月～(最小構成)</li></ul> | <ul style="list-style-type: none"><li>参加メンバー単位</li><li>ピア・インスタンス単位</li><li>約41万円/月～(最小構成)</li></ul> |

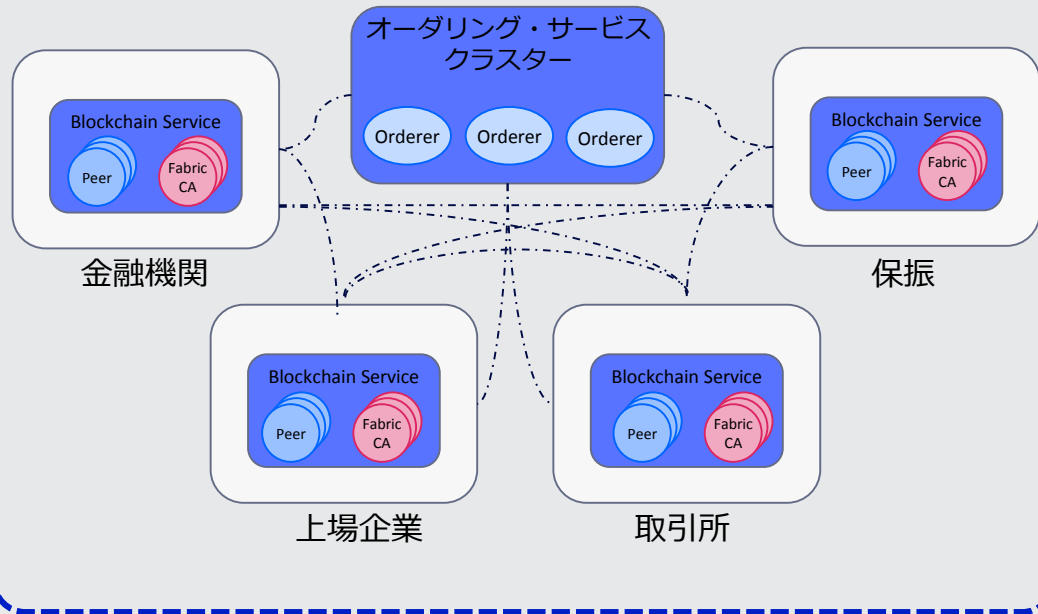
※ StarterおよびEnterprise Plusプランは近日リリース予定(価格に変更する可能性があります)

# IBM Blockchain Platformのネットワーク構造



## IBM Blockchain Platform

### 分散ビジネス・ネットワーク



- コンソーシアム型ネットワークを容易に構築
- メンバーは各IBM Cloudアカウントに紐付けてネットワークに参加
  - ✓ メンバー単位の課金
  - ✓ ピア数はメンバー毎に決定
  - ✓ メンバーの役割やポリシー定義を支援するツール群
- トランザクション順を決定するオードリング・サービスは、メンバー間で共有

# IBM Blockchain Platformの今後の拡張計画



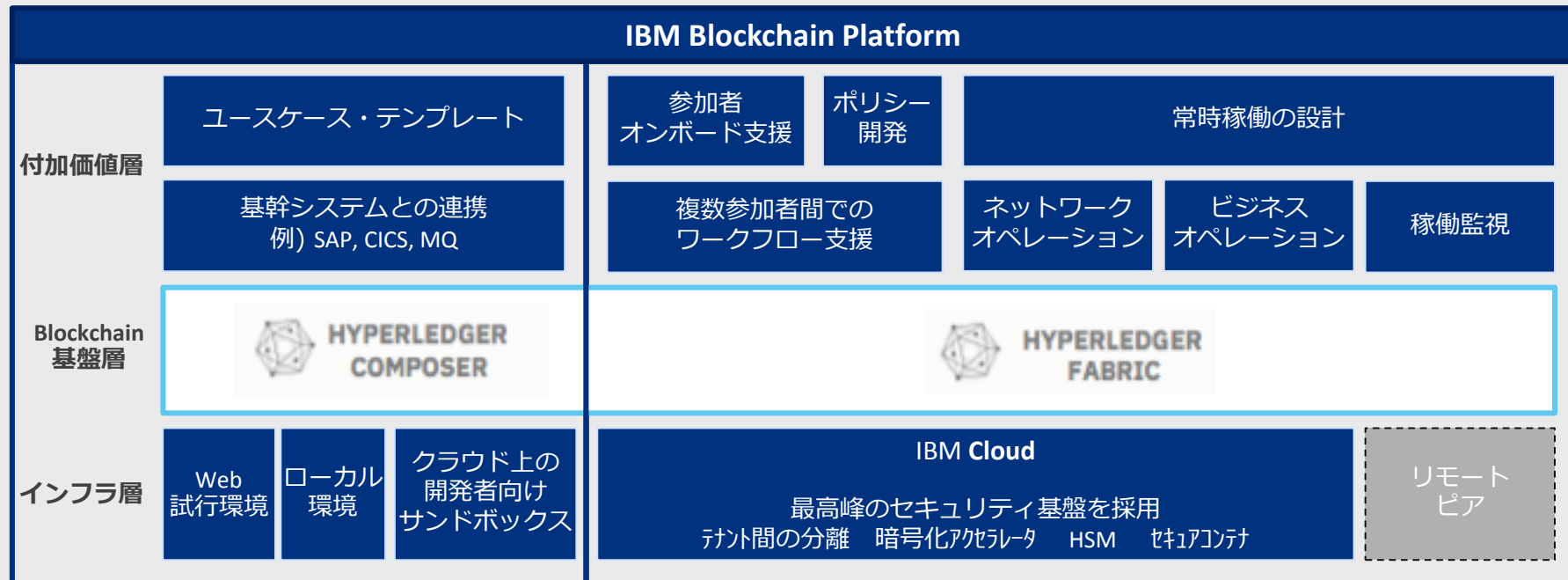
|                             | Q1                                                                                                                                                  | Q2                                                                                                                                                                                                                                                                 | 2H18                                                                                                                                                                                                                                                                                                                               |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>1 Starter Plan</b>       | <ul style="list-style-type: none"> <li>• <b>Beta (Think)</b></li> </ul>                                                                             | <ul style="list-style-type: none"> <li>• <b>Generally Available</b></li> </ul>                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                    |
| <b>2 Enterprise Plan</b>    | <ul style="list-style-type: none"> <li>• HSM for Enrollment Certs</li> </ul>                                                                        | <ul style="list-style-type: none"> <li>• Fabric V1.1, CouchDB and full HSM</li> </ul>                                                                                                                                                                              | <ul style="list-style-type: none"> <li>• Resource usage reporting</li> <li>• Blockchain analytics</li> <li>• Advanced governance</li> <li>• Hybrid networks / ICP support</li> <li>• Advanced HA/DR</li> <li>• Storage offering</li> <li>• Integrated documentation across Fabric, Composer and IBM Blockchain Platform</li> </ul> |
| <b>3 Enterprise+ Plan</b>   | <ul style="list-style-type: none"> <li>• Contact Offering for Pricing/Ordering</li> <li>• HSM for Enrollment Certs</li> </ul>                       | <ul style="list-style-type: none"> <li>• <b>Generally Available</b> <ul style="list-style-type: none"> <li>• Fabric V1.1, CouchDB, full HSM</li> <li>• Multi-site DR with sponsor user (recover network &lt; 48 hrs)</li> </ul> </li> <li>• <b>GDPR</b></li> </ul> |                                                                                                                                                                                                                                                                                                                                    |
| <b>Compliance</b>           |                                                                                                                                                     |                                                                                                                                                                                                                                                                    | <ul style="list-style-type: none"> <li>• FedRAMP , SOC2</li> </ul>                                                                                                                                                                                                                                                                 |
| <b>Hyperledger Fabric</b>   | <ul style="list-style-type: none"> <li>• <b>Fabric 1.1 GA</b></li> <li>• Query (CouchDB), perf. Improvements</li> <li>• NodeJS Chaincode</li> </ul> | <ul style="list-style-type: none"> <li>• <b>Fabric 1.2 GA</b></li> <li>• Ledger Archive</li> </ul>                                                                                                                                                                 | <ul style="list-style-type: none"> <li>• Auditability and Pruning</li> <li>• Byzantine Fault Tolerance</li> <li>• Zero Knowledge Proof</li> </ul>                                                                                                                                                                                  |
| <b>Hyperledger Composer</b> | <ul style="list-style-type: none"> <li>• Enhanced Starter Plan Experience</li> </ul>                                                                | <ul style="list-style-type: none"> <li>• <b>Composer 1.0 GA</b></li> <li>• Ease of deployment</li> <li>• VisualStudio Support</li> </ul>                                                                                                                           | <ul style="list-style-type: none"> <li>• Ops Console, Analytics</li> </ul>                                                                                                                                                                                                                                                         |

# IBM Blockchain Platformの全体像



**ソリューション** 国際貿易, 地方創生, 食の安全, 国際送金, デジタルID, プライベート・エクイティ ...

**他システム連携** Watson, IoT, API管理, メッセージング, ワークフロー, 資産管理 ...

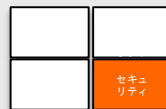


# IBM Blockchain Platform : "Managed" Blockchainサービス



| 1/2           |                            | 通常のクラウドサービス(IaaS)                                | IBM Blockchain Platform                     |
|---------------|----------------------------|--------------------------------------------------|---------------------------------------------|
| システム環境 (サーバー) |                            | ○<br>クラウドとして提供                                   | ○<br>クラウドとして提供                              |
| 環境構築          | 設計                         | X<br>ノード配置や可用性設計含め、1から設計する必要あり                   | ○<br>設計は不要 (可用性を考慮した設計済)                    |
|               | 初期構築                       | X<br>CA, Order, Peerやネットワークの導入、構築が必要             | ○<br>構築済。管理画面(GUI)での操作で起動                   |
|               | 構成変更                       | X<br>PeerやChannel等の追加や変更はやや複雑なコマンド操作により実施する必要あり。 | ○<br>管理画面(GUI)での操作で追加、変更可能。                 |
| 運用管理          | 稼働確認                       | X<br>別途、機能を実装する必要あり                              | ○<br>管理画面(GUI)からの確認が可能                      |
|               | 起動・停止操作                    | X<br>別途、機能を実装する必要あり                              | ○<br>管理画面(GUI)からの起動・停止が可能                   |
|               | ログの監視                      | X<br>別途、機能を実装する必要あり                              | ○<br>管理画面(GUI)からの監視が可能                      |
|               | ブロックチェーンの状況確認              | X<br>別途、機能を実装する必要あり                              | ○<br>管理画面(GUI)からのブロックの状況 (ブロックの高さなど) の確認が可能 |
|               | スマートコントラクト (チェーンコード) の状況確認 | X<br>別途、機能を実装する必要あり                              | ○<br>管理画面(GUI)からのチェーンコードの配置・稼働状況の確認が可能      |
|               | バックアップ                     | X<br>別途、運用する必要あり                                 | ○<br>Managedサービスとして、標準でバックアップ取得 (日次)        |

# IBM Blockchain Platform : "Managed" Blockchainサービス



| 2/2              |                          | 通常のクラウドサービス(IaaS)                     | IBM Blockchain Platform                                |
|------------------|--------------------------|---------------------------------------|--------------------------------------------------------|
| 障害対応             | 障害検知                     | X<br>別途、障害検知の仕組みづくりと障害監視体制が必要         | ○<br>ManagedサービスとしてIBM運用チームで対応                         |
|                  | 障害回復                     | X<br>障害検知とあわせて、別途、障害回復の仕組みづくりと運用体制が必要 | ○<br>ManagedサービスとしてIBM運用チームで対応                         |
| メンテナンス (パッチ適用など) |                          | X<br>別途、運用の仕組みと体制が必要                  | ○<br>ManagedサービスとしてIBM運用チームで対応                         |
| セキュリティ           | ネットワーク暗号化                | ○<br>Hyperledger Fabricの機能として提供 (TLS) | ○<br>Hyperledger Fabricの機能として提供 (TLS)                  |
|                  | システム・アクセスの制限 (管理者ログインなど) | X<br>個別に設計と仕組みづくりが必要                  | ○<br>Managedサービスとして仕組みを実装。管理者ログイン不可                    |
|                  | データ暗号化                   | X<br>暗号化の実装が必要                        | ○<br>Managedサービスにて標準的に実装 (蓄積データを暗号化)                   |
| コンソーシアム対応        | 複数組織の参加の仕組み              | X<br>複数組織 (メンバー) 間での調整と、接続など手動で行う必要あり | ○<br>複数組織 (メンバー) によるネットワーク構成を基本機能としてサポート               |
|                  | ガバナンスツール                 | X<br>提供されていない                         | ○<br>ガバナンスツールは組み込み済                                    |
| サポート             |                          | △<br>基盤 (HW) 部分のみ                     | ○<br>ブロックチェーンネットワーク (ピアを含む) について対応 (ユーザー開発のチェーンコードを除く) |

# まとめ

## Blockchain Solutions

世界中のお客様との協業でビジネスを変革するプラットフォーム  
(GTD, Food Trust, Universal Payment など)

## Blockchain Services

全世界で約500のプロジェクトをリードし、国内実績も豊富

## IBM Blockchain Platform

- *Starter*
- *Enterprise*
- *Enterprise Plus*

**コンソーシアム型ネットワークに必要な全ての要件を兼ね備える  
業界唯一のフルマネージのブロックチェーン・プラットフォーム**

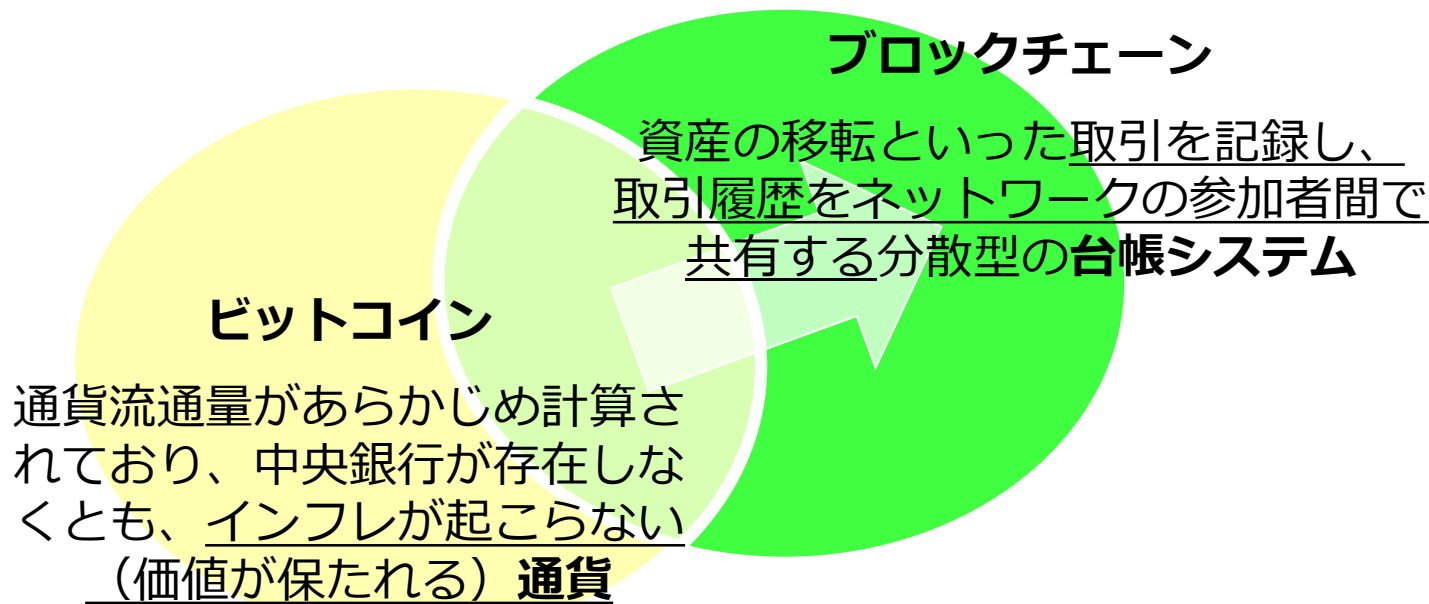


進化を続けるエンタープライズ向けブロックチェーン技術



# (参考) 「ビットコイン」と「ブロックチェーン」の関係整理

- ブロックチェーンは、ビットコインを実現するための基盤技術として発明された技術。即ち、本来はビットコインを構成する一部分になります。
- 現在は、様々なビジネスシーンで活用可能であるとの期待の下、全世界的な検討が行われています。その過程で概念が拡張されています。



# (参考) ブロックチェーン=暗号通貨(ビットコイン)?

## A1 : No

- ファイナリティーが無い
- コンセンサスに時間がかかる(10分等)
- PoWに莫大なエネルギーが必要

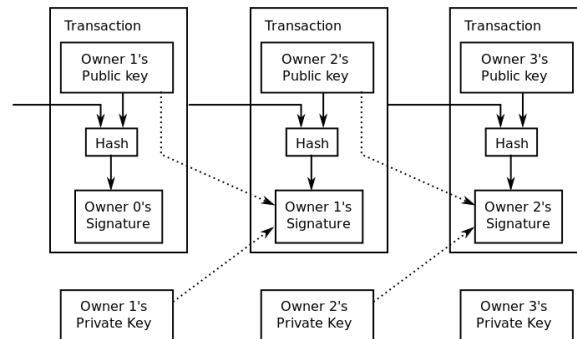
- ビットコインによって、その基盤技術であるブロックチェーンは有名になりましたが、ブロックチェーンは通貨だけでなく、資産や権利の移転を含む、様々な業務に適用することができます。

### 1. bitcoinは規制されていない通貨

- 中央機関を必要としない
- 転々流通可能

### 2. ブロックチェーン技術を用いて、現金相当の「コイン」を流通させることも可能です

### 3. ブロックチェーン≠ bitcoin



# (参考) Bitcoinの合意形成の仕組み：Proof of Work



## (参考) ハッシュ値・ハッシュ関数とは

「明日の天気は晴れです。」

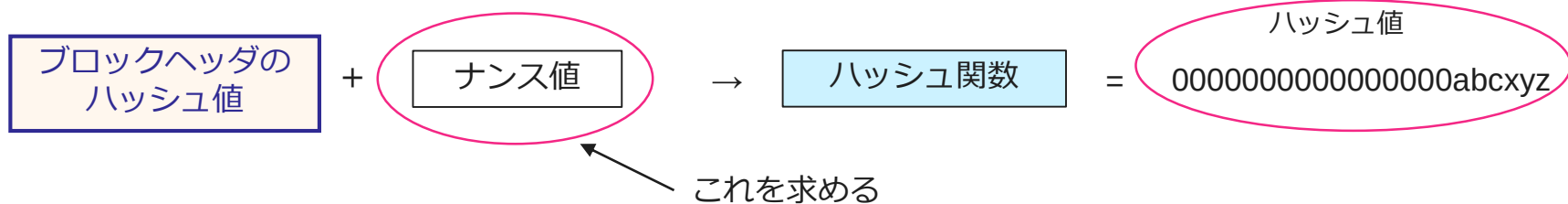
この文章を[ハッシュ関数(ある計算式)]を通すと

d5a4508fdc93cac73a5eb91ab96c020e

のような文字列に変換される

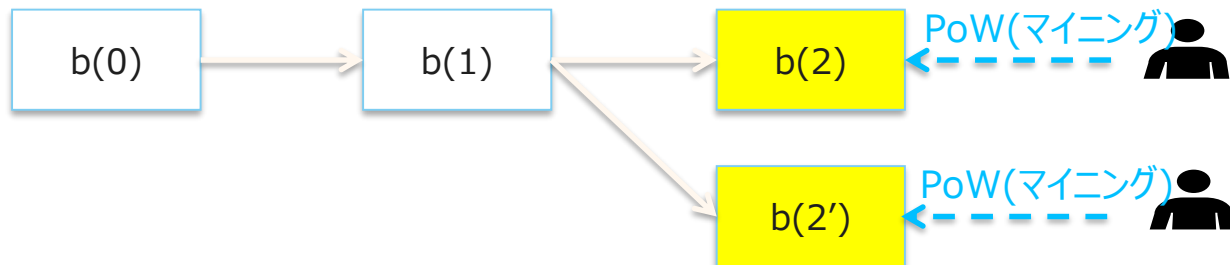
この文字列を**ハッシュ値**または、単に**ハッシュ** という  
ハッシュとは、データを投入して生成される文字列

ビットコインのマイニングはハッシュ関数にある値(ナンス値)を入力して先頭に0が16桁となるハッシュ値を求める作業を行います。このナンス値を求めることをProof of Workと呼ぶ。

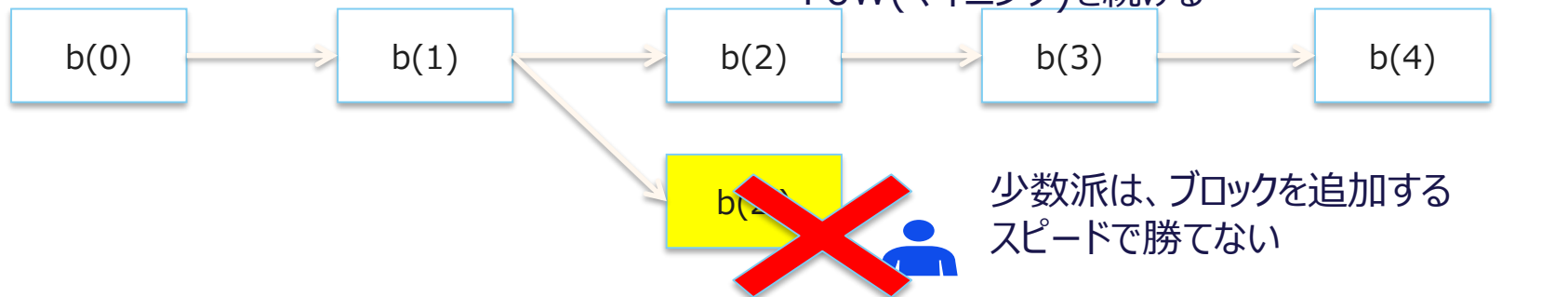


## (参考) PoWでのファイナリティの問題

タイミングによって、複数のPoW(マイニング)がほぼ同時に成功し、ブロックが分岐する場合がある



長く延びたブロックが正当と認められる



棄却されたブロック内のトランザクションは無効になる可能性がある  
分散コンセンサス形成アルゴリズムでは、このような問題はない

# 進化を続けるHyperledger Fabric

V0.6での多くのお客様との実証実験の経験を通じて、改善を継続

| 目的              | V1での拡張内容             |
|-----------------|----------------------|
| トランザクション処理量の増加  | 並行処理可能な合意手法の採用       |
| トランザクションの機密性の向上 | 特定ノード間でのデータ共有がより容易に  |
| データをより活用しやすく    | データストアを変更可能に         |
| 運用の改善           | 稼働中でのチェーンコード入れ替えが可能に |
| 認証の柔軟性の向上       | お客様固有の認証管理を使用可能に     |
| 単一障害ポイントをなくす    | 複数の認証局をサポート          |

# ブロックチェーンの利点と不向きなこと : システム目線

## ○ ブロックチェーンの利点

1. 分散台帳・処理により中央機関を必要としないことで、低コストにシステムが構築・運用できることが期待される
2. 一部のノードが停止していても処理が継続できるため、1台あたりは低コストで信頼性が低い基盤でも構築できる
3. 各ノード（各参加者）間で同じビジネスロジック、データが共有され、改ざんしにくい状態で取引記録が保持されるため、可監査性に優れている

## × ブロックチェーンに不向きなこと

1. 分散台帳をコンセンサスを取りながら更新していくため、パフォーマンス（高TPS、高レスポンス）は出にくい
2. 複数の組織・会社で構成されず、1組織だけで構成される場合（通常のシステムで対応可能）

# まとめ: Hyperledgerの特徴

| 特徴         | 説明                                                              |
|------------|-----------------------------------------------------------------|
| 用途         | コンソーシアム型やプライベート型などでの業務使用を意識                                     |
| 台帳         | 一般的なブロックチェーンの他に、台帳の最新状態を表すデータストア (KVS) を持つ                      |
| スマートコントラクト | チェーンコードにプログラムすることで、複雑な業務ロジックをブロックチェーン上で実行し自動化することができる           |
| コンセンサス     | 高速・軽量かつファイナリティのあるコンセンサスアルゴリズムをサポート<br>任意のコンセンサスの仕組みをプラグインして導入可能 |
| セキュリティ     | トランザクション認証、暗号化、匿名化など高いセキュリティを実現                                 |
| 拡張性・柔軟性    | 様々なトランザクションやコンセンサスのモデルを組み込むことができ、さまざまなブロックチェーン利用においての基盤として利用できる |
| 高可用性       | 一部のノードに障害が起きても、他のノードで業務継続可能                                     |



# ブロックチェーンの利点 : ビジネス目線



## 時間の短縮

数日かかっていた業務  
処理を一瞬で  
完了できる



## コスト削減

処理の自動化や  
仲介機関の排除  
オーバーヘッド削減



## リスク低減

改ざん、不正の防止、  
単一障害点の排除



## 信頼を向上

プロセスと記録を共有することにより、信頼を向上し、ビジネスの運営を円滑に

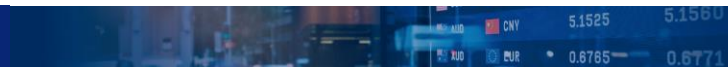
# ブロックチェーンに向いていない処理

## 弱み



1. スピードが求められる取引 (ミリ秒)
2. 小規模組織  
(ビジネスネットワークなし)
3. データベースの代替
4. メッセージングミドルウェアの代替
5. トランザクション処理システムの代替

### 3. IBMの取り組みとHyperledger Fabric



# IBMの目指すブロックチェーン

## IBMの目指す企業向けブロックチェーン

Bitcoin



- 政府などにより規制されない、転々流通可能な仮想通貨
- 誰でもビットコインネットワークに参加可能 (Public Network)
- Proof of Work(マイニング)による合意形成



- コンソーシアムなどのビジネスネットワークの中で会社/組織をまたがる業務に適用
  - スマートコントラクト
- 許可制 ネットワーク
  - セキュリティとプライバシー
- 高い処理性能 (スループットとレスポンス)

# エンタープライズ向けブロックチェーンにむけて IBMの取り組み：Hyperledger Project



- 2015年12月にアナウンスメント
  - 2017年6月現在 +130社
- 標準化の中で、先進的なブロックチェーン技術を推進
- IBM：発足メンバー
  - 44,000行に及ぶコードを寄贈
  - 技術ステアリング・コミッティーの初代議長（Chris Ferris）

## プレミア会員



## 一般会員



# IBMの取り組み：オープン・コミュニティ Hyperledger Fabric

- エンタープライズ向け許可制ブロックチェーン基盤技術

ブロックチェーン構造

アプリケーション  
レイヤー

ブロックチェーン  
プラットフォーム

基盤レイヤー

ブロックチェーン基盤 (Hyperledger Fabric)

複数種類の台帳が  
共存可能

参加者認証

各種取引データ  
の活用を志向

分散台帳

セキュリティ  
/ プライバシー

IBM研究所開発  
暗号技術

業務特性に応じて  
合意ルールを選択

合意形成

スマート・  
コントラクト

高度な権限設定  
でのデータ秘匿

システム拡張性  
への考慮

複雑な業務処理  
の実現

オープン環境

稼働環境に依存しない  
可搬性技術

オープン

- Hyperledgerプロジェクト  
100+ メンバー
- オープンソース(GitHub)

汎用

- スマート・コントラクト

許可制・セキュリティ

- 認証・認可、プライバシー

# エンタープライズ向けブロックチェーンの要件

IBMの研究によると、エンタープライズ向けのブロックチェーンには、**許可制ブロックチェーン**が唯一の方法だという結論に達しました。

[https://www.ibm.com/developerworks/community/blogs/gcuomo/entry/A\\_Case\\_for\\_Permissioned\\_Blockchains?lang=ja](https://www.ibm.com/developerworks/community/blogs/gcuomo/entry/A_Case_for_Permissioned_Blockchains?lang=ja)

## アイデンティティ管理

- 参加者の身元確認
- 参加者の認証
- 参加者のロール管理

## プライバシー管理

- トランザクションの暗号化
- 同じユーザーが発行した複数のトランザクションを関連付け（匿名化）

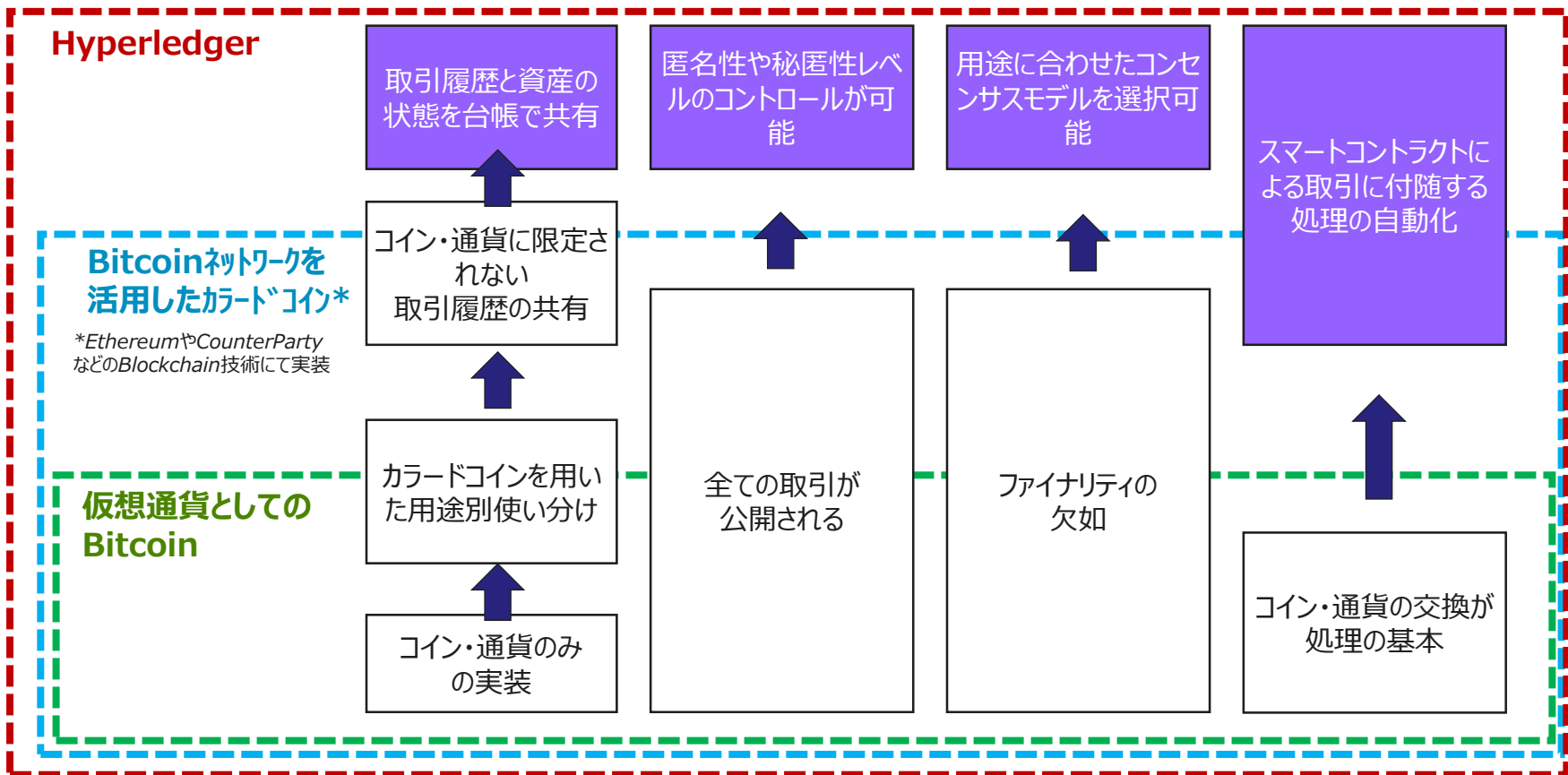
## アクセス制御

- スマートコントラクトに対するACL制御

## コンセンサス手法

- 認可制の特性を活かした軽量なコンセンサスの手法の採用
- 要件に合わせて選択可能

# 「資産移転」の仕組みづくりBitcoin, Blockchain, Hyperledger



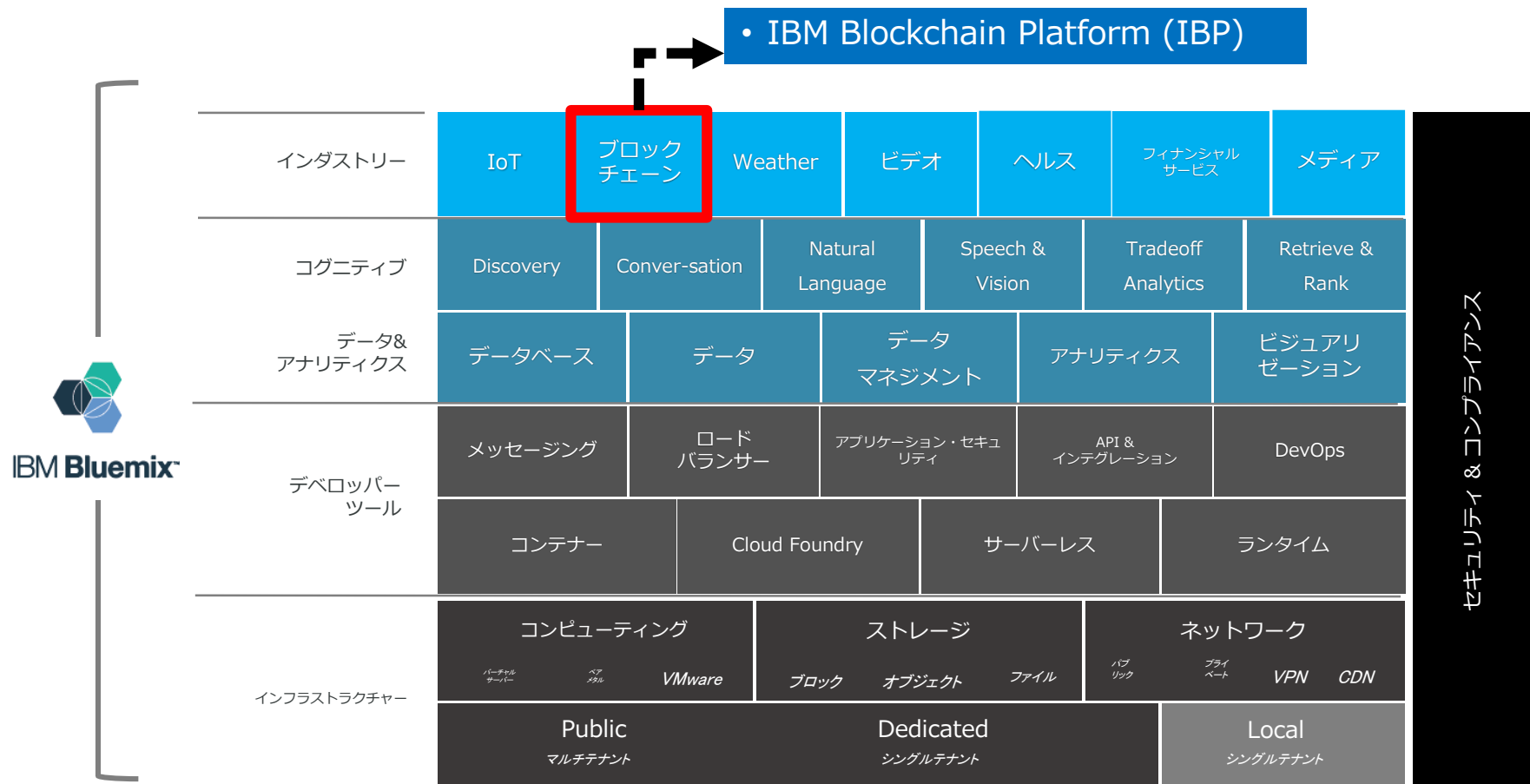


# IBMの取り組み：Hyperledger Fabricの特徴

①さまざまなユースケースに対応（汎用的）で、②エンタープライズ向けにセキュリティを強化（許可制。エンタープライズ向け）がポイントです。

|                   | Hyperledger Fabric  | Ethereum                   | Ripple            | Bitcoin         |
|-------------------|---------------------|----------------------------|-------------------|-----------------|
| 説明                | 汎用<br>ブロックチェーン      | 汎用<br>ブロックチェーン             | 決済用<br>ブロックチェーン   | 決済用<br>ブロックチェーン |
| ガバナンス             | Linux Foundation    | Ethereum 開発者               | Ripple Labs       | Bitcoin 開発者     |
| 通貨                | なし                  | Ether                      | XRP               | BTC             |
| マイニングの報酬          | 該当なし<br>（マイニングなし）   | あり                         | 該当なし<br>（マイニングなし） | あり              |
| データ最新断面           | Key-Value<br>データベース | ブロック中にステー<br>トを保管          | なし                | なし              |
| コンセンサス・<br>ネットワーク | 変更可能                | マイニング                      | Ripple プロトコル      | マイニング           |
| ネットワーク            | プライベート、<br>パブリック    | プライベート、<br>パブリック           | パブリック             | パブリック           |
| プライバシー            | 限定された参加者に<br>公開     | 参加者全員に公開                   | 参加者全員に公開          | 参加者全員に公開        |
| スマート・コントラクト       | 複数のプログラミング<br>言語に対応 | 「Solidity」という<br>プログラミング言語 | なし                | なし              |

# IBMの取り組み : Blockchain-as-a-Service



# IBMの取り組み：プロジェクトの進め方（例）



1. ブロックチェーン技術の紹介・議論
2. ビジネス・モデルの議論
3. ブロックチェーン適用事例のデモ



1. ブロックチェーンの構成要素を深く理解
2. Bluemix上でのハンズオン
3. 既存プロトタイプをカスタマイズ



1. デザイン・シンキングワークショップでビジネス課題を定義
2. アジャイル手法で、段階的に開発
3. 既存システムとの統合を検討



1. プロジェクトを発展させパイロットを実施または、新しいプロジェクトを開始
2. ビジネス・プロセスの再設計
3. 実運用に向けた開発

## 概要セッション

- ・ 概要
- ・ 技術
- ・ ユースケース

## スキル習得 支援サービスなど

- ・ 技術詳細
- ・ ハンズオン

Bluemix Garage

Blockchain-as-a Service

High Security Business Network

# IBMの取り組み：お客様との取り組み

## Blockchain Garage

お客様のアイデアを、ブロックチェーンを活用した  
ビジネス・アプリケーションとして設計・開発する  
IBM Bluemix Garage for Blockchainを日本でも提供開始。

ブロックチェーン・テクノロジー活用の専門知識と、  
デザイン・シンキングとアジャイル開発といった手法を  
組み合わせ、実践的なビジネス・ソリューションの開発を支援します。



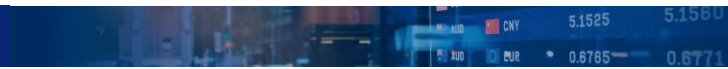
## Bluemix Garageとは？

1. イノベティブなアプリ開発を大企業から  
スタートアップまで幅広く支援
2. ユーザー視点でモバイル系アプリ、新規アプリ  
を短期開発支援  
(Design Thinking、Lean start up)

活用例：大手金融機関、大手航空会社、その他



## 4. ブロックチェーンの適用領域と事例



# 各インダストリーでの適用が検討されている業務

各インダストリーにて、ブロックチェーンへの適性が認められている業務エリアで、実用化に向けた検討が進んでいます。



## 金融

## 公共

## 小売・流通

## 保険

## 製造・物流

貿易金融  
多通貨同時決済  
不動産融資

公的な台帳管理  
住民ID管理  
診療記録  
薬品サプライチェーン管理

サプライチェーン  
ポイントプログラム  
小売／供給者間の情報共有

保険請求支払記録  
リスク定量化

サプライチェーン  
部品の出処証明  
保守記録／  
トラッキング

# 共有リファレンスデータ

ネットワーク上でリファレンスデータを共有する場合、その情報更新や配布は通常ファイルベースでのバッチ転送にて対応されています。更新までの時間を要すること、また、参加者間での情報不一致になるケースもあります。

## 現状業務

- ネットワーク上の参加者は、リファレンスデータ共有が必要（例えば、銀行・支店コード）
- 個々に関するデータを更新する場合、更新データを中央管理機関へ連携し、各参加者に配布してもらう必要がある。

## 活用方法

- ネットワーク参加者は個々に関するデータをブロックチェーン上の台帳を更新
- ブロックチェーンは、すべてのデータを単一ビューで提供

## 導入効果

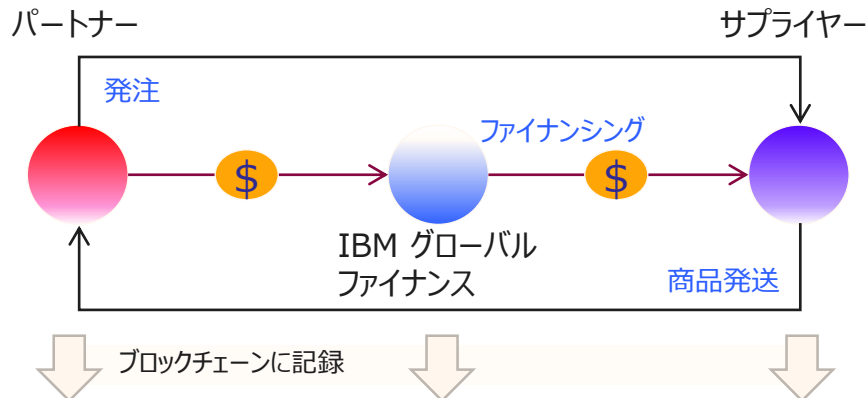
- 統合され整合性が取れたデータにより、エラー減少
- 準リアルタイムでのリファレンスデータ更新





# 事例：サプライチェーンファイナンス

サプライチェーン参加者間のすべてのやりとりを不変性／不否認な情報としてブロックチェーン上に記録し、プロセスを可視化し、参加者間の情報不整合からくる争議を回避し、取引プロセス時間の短縮します。



- IBMグローバル・ファイナンス (IGF) は世界中の 4,000 以上のサプライヤーやパートナーにまたがるサプライチェーン・ファイナンスを提供しています。
- パートナーは、サプライヤーから購入をするときに、融資を受けます。
- 2014年には290万件以上の取引があり、IBMは450億ドル（約5兆4千億円）の融資を行っています。
- 一方で、年間25,000件以上の争議が発生しています。（金額の不一致、商品が届かない、など）



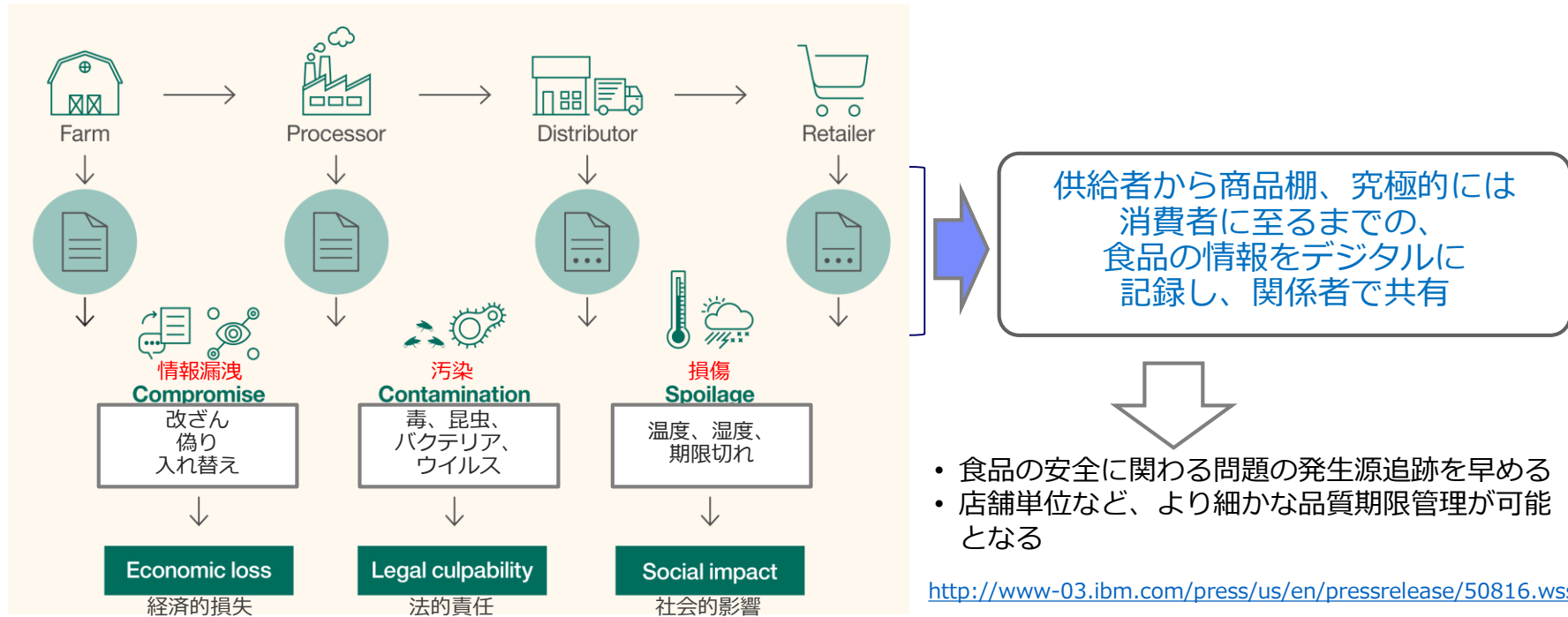
- 包括的に事務処理全体の可視化が可能
  - ✓ 課税ステータスに疑問？ → 取引先の結果をすぐ参照
  - ✓ 商品未到着？ → 処理状況確認
- 関係者間の資本移動・決済にかかる時間を短縮
- 争議の件数を削減、解決までの時間を短縮



# サプライチェーン：食の安全（トレーサビリティ）

ウォルマート、清華大学、IBMは共同で、豚肉の生産・流通経路の記録・追跡にブロックチェーンの利用の検討・検証を開始しました。

台帳がそれぞれで管理され、透明性が確保されていない状態と、それによるリスクを回避



# 食品安全確保のための大規模ブロックチェーンの発表 (2017/08/22)

中国における実証実験を経て、IBMとWalmartは、食の安全を可視化するFood Safety Platformの開発に踏み切りました。

2018年初頭の限定的なリリースを目指して、現在、主要食料品関連企業10社と、プラットフォームの開発を推進しています。



## IBM Announces Blockchain Collaboration with Major Retailers and Food Companies to Address Food Safety Worldwide

Date added: 22 Aug 2017

A group of the world's leading retailers and food companies are working with IBM to explore how blockchain technology can be used to make the food supply chain safer. Blockchain technology can be used to improve food traceability by providing trusted information on the origin and state of food. Pictured is a crate of oranges being scanned as part of a food safety blockchain. (Connie Zhou for IBM)

[Download hi-res version \(image/jpeg, 1 MB\)](#)

[→ View the associated news release](#)

## Engage IBM

[→ Contact a media relations representative](#)

[→ Site feedback](#)

## Share

[Facebook](#)

[Twitter](#)

[LinkedIn](#)

## 参加企業

**Dole** (米)、**Kroger** (小売 : 米)、**Nestle** (スイス)、**Unilever** (蘭)、**Walmart** (米) **Driscoll's**(果物 : 米)、**Golden State Foods**(卸売 : 米)、**McCormick**(スパイス : 米)  
**McLane Company** (SCMサービスプロバイダー : 米)、**Tyson Foods** (食品加工 : 米)

# 貿易金融 (Trade Finance)

関連する多くの企業間で煩雑な書類のやり取りが発生している貿易金融は、ブロックチェーンの適用により、大幅なプロセス改善が期待される典型的なユースケースのひとつです。

## 現状業務

貿易金融では、銀行、輸出企業、運輸会社、輸入企業等の多数の参加者の間で、大量の貿易書類をやりとりする必要があり文書の処理に多くの手間と時間を要する

## 活用方法

参加者の間での貿易書類をブロックチェーン上に保管し連携処理を実施

決済指示や貿易書類の業務処理をブロックチェーン上の処理にて実行し、ワークフローを自動化

## 導入効果

迅速かつ安全な貿易書類の交換

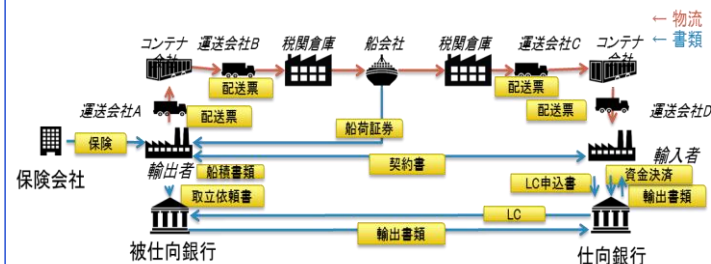
情報連携効率化によるプロセス時間の迅速化とコスト削減

電子化参入コスト軽減による小規模企業の利用促進

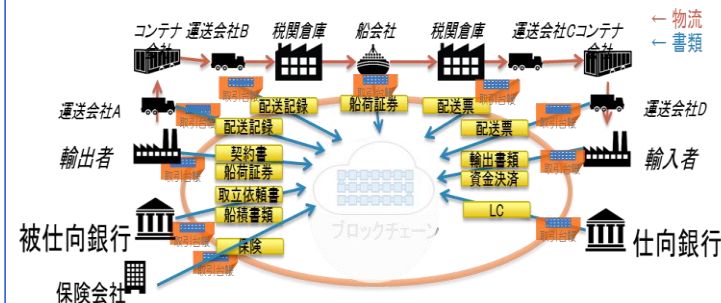
IoT活用による物流情報の把握による金融サービス提供

タイミングの把握とビジネス機会の増加

## Before



## After



# 物流サプライチェーン

IBMとデンマークの海運大手のMaerskは米国時間2017年3月5日、物流サプライチェーンにおけるトランザクションの運用と管理、追跡にブロックチェーン技術を利用することを発表しました。船荷主や海貨業者、貨物船業者、港湾関係者、税関と協力し、国境をまたがるトランザクション向けのブロックチェーンツールの開発を行います。

## ■ 共同プラットフォームの稼働

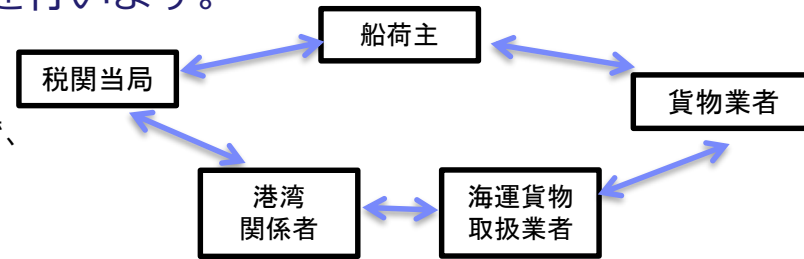
- IBMとMaerskは、物流のサプライチェーンと協力していくことで、2017年中にブロックチェーンによるデジタルプラットフォームの実働に入ることを目指します。

## ■ ブロッチェーンによる期待効果

- ブロックチェーンソリューションによって、紙ベースの書類による手作業が大半を占める処理をブロックチェーン技術で置き換え、透明性とデータ共有の安全性の向上が見込まれます。

## ■ HSBN:稼働環境

- IBMはこのソリューションをHyperledger Fabricをベースにして自社のクラウドとハイセキュリティビジネスネットワーク(HSBN)にホストし、クラウド基盤IBM Bluemixから提供します。

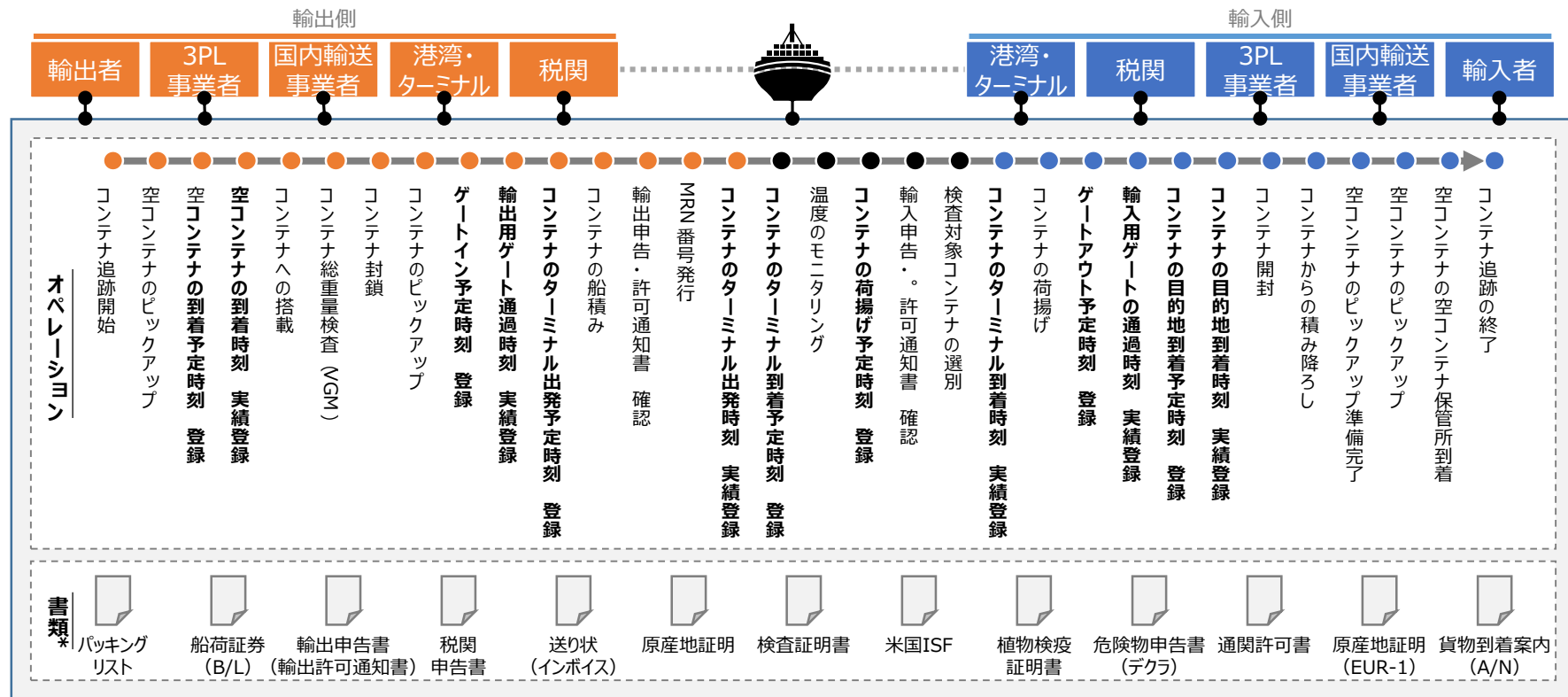


<http://www-03.ibm.com/press/us/en/pressrelease/51712.wss>

# ソリューション構想 全体像

・ 輸出入に関する書類、オペレーションの進捗情報を、電子化の上、関係者で共有できる仕組みを構築する。

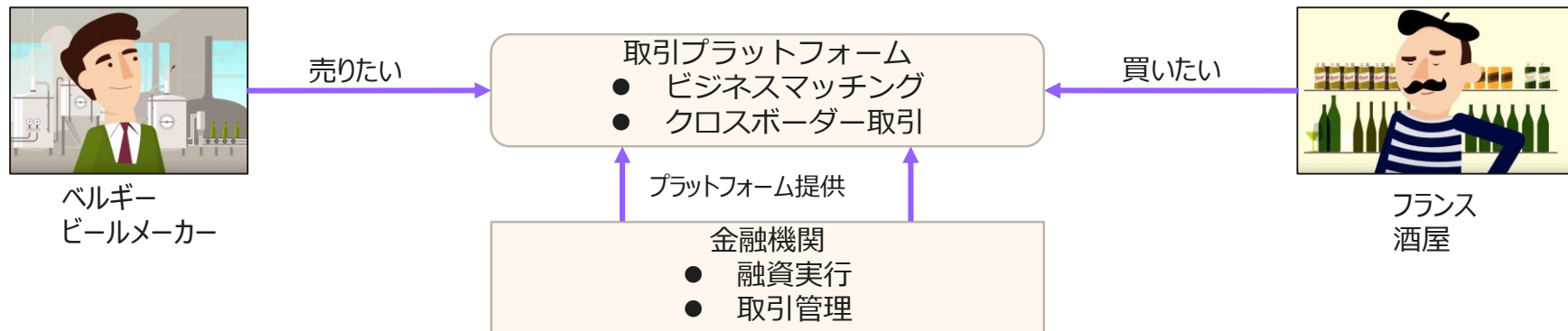
1. 書類の電子化・共有により、関係者の事務負担の軽減が期待可能。
2. 輸出入オペレーションの進捗情報の共有により、輸出者／輸入者のリスク・安全在庫量の削減が期待可能。



\*ここに記載した書類のリストは、輸出入に関わる代表的な書類を列挙したものです。ここに記載した以外の書類についても本ソリューションで電子化可能なものは存在し、一方ここに記載した全ての書類が電子化可能な訳でもない。

# 事例：デジタル・トレード・チェーン（中小企業向け貸付）

ブロックチェーンを活用し、クロスボーダー取引を簡素化することで新しい取引先とのビジネスで収益源を切り開き、貿易の拡大を促進します



## 中小企業のメリット

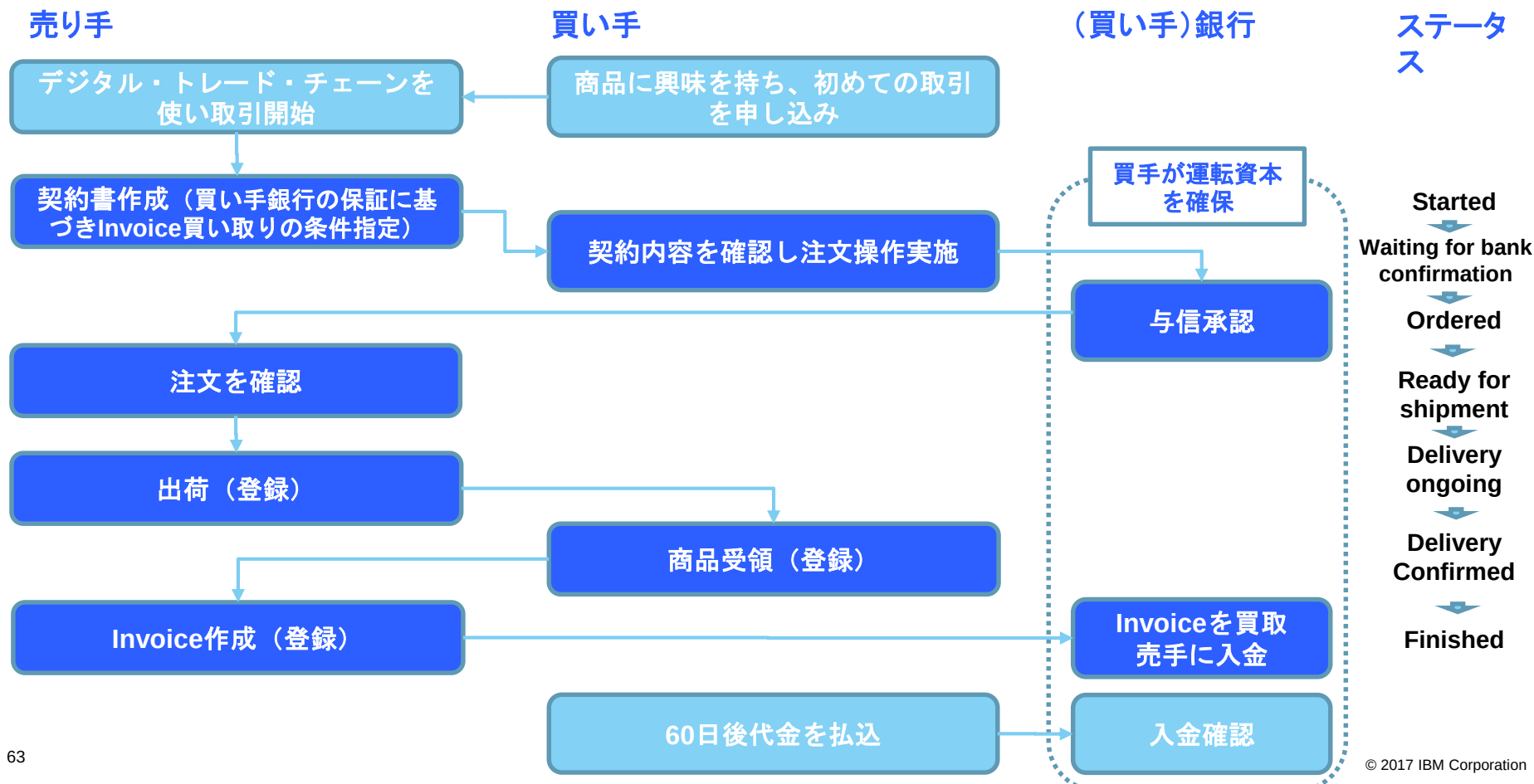
- ✓ 資金調達へのアクセスを高める
- ✓ 国内外または他の欧州市場で新規パートナーとの取引を開始するのに役立つ

## 銀行のメリット

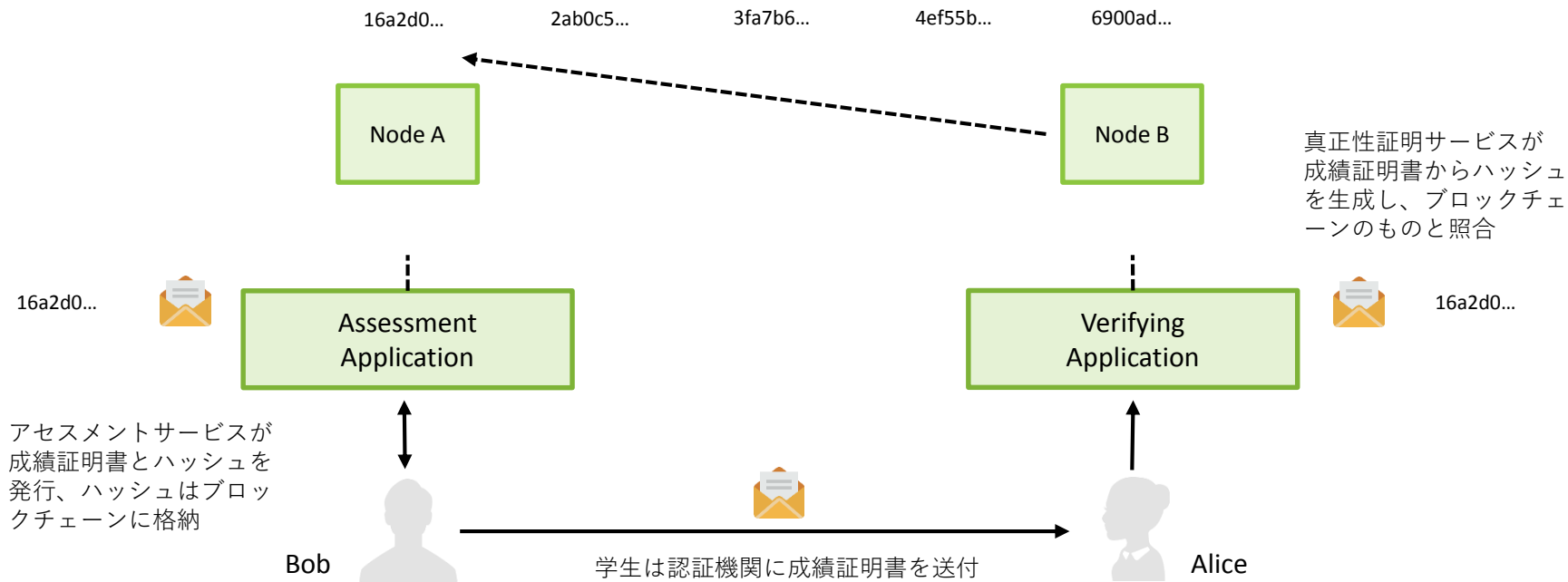
- ✓ 貿易金融プロセスを簡素化
- ✓ 新しい収益源を開拓し、新たな取引関係を開始し、貿易拡大を促進
- ✓ 貿易取引に説明責任と透明性を与える
- ✓ 迅速で簡単かつ低コストの貿易取引を可能
- ✓ 中小企業(SME)の顧客管理を最適化

## コンソーシアム参加銀行

- ドイツ銀行
- HSBC（イギリス）
- KBC（ベルギー）
- ソシエテジェネラル（フランス）
- ラボバンク（オランダ）
- Natixis（フランス）
- ウニクレディト（イタリア）

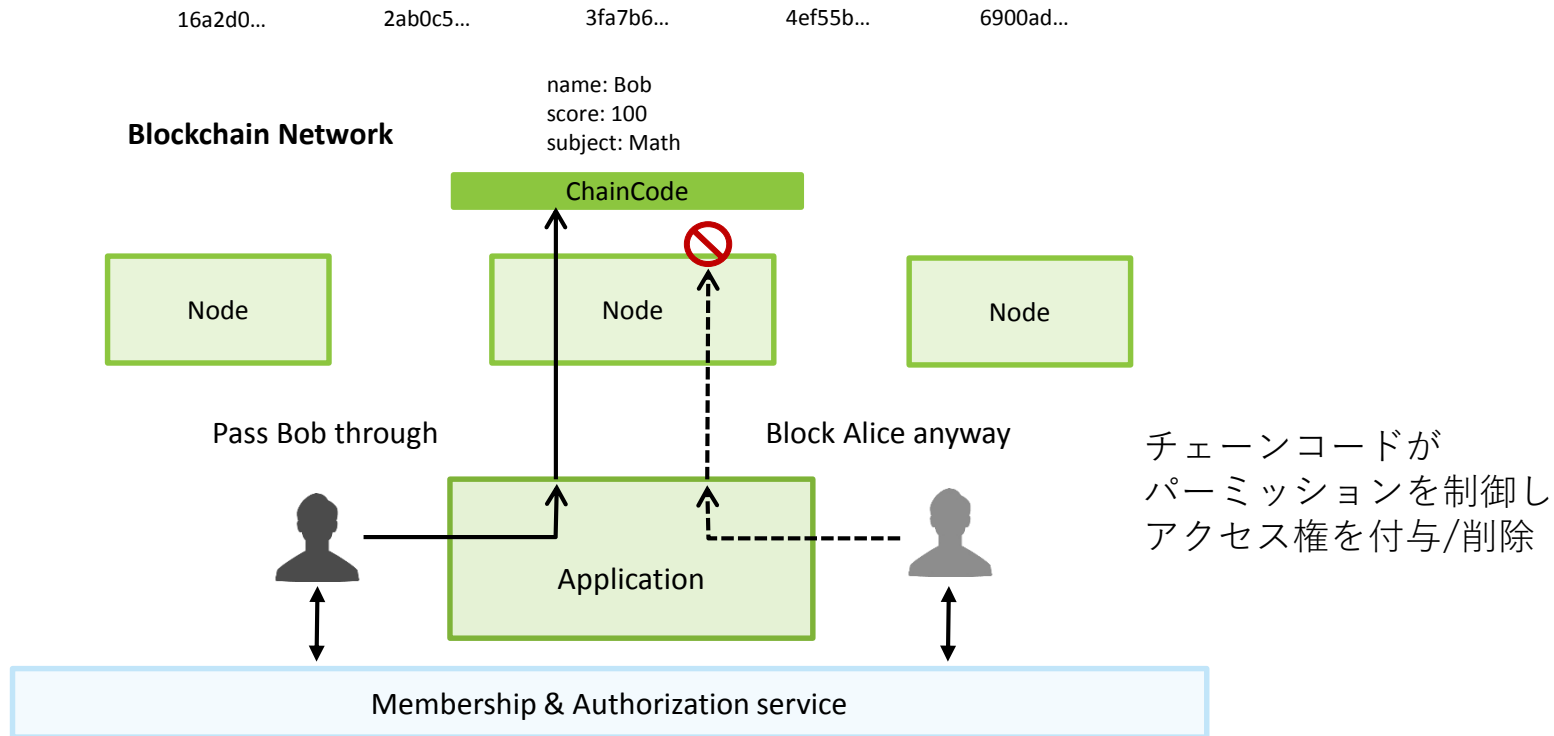


# 事例：成績証明書の真正性確認





# データアクセス権限制御



# IBM Blockchainの情報

## 弊社ブロックチェーン ポータル・サイト

<http://www.ibm.com/industries/jp/ja/blockchain/>



## 弊社技術情報誌 ProVISION

<https://www.ibm.com/blogs/pro-vision/>



[No.91] FinTechの共創戦略が金融サービスを変える  
- Fintech及びBlockchainを特集しております

# ビジネスを変える！ IBMブロックチェーン解説セミナー(連載シリーズ)



## 第1回目

2月15日(木)17時-18時

これから始める  
ブロックチェーン

## 第2回目

2月27日(火)17時-18時

Hyperledger Fabric  
とIBM Cloudで  
始める  
ブロックチェーン

## 第3回目

3月1日(木)17時-18時

「ビジネス向け」  
IBMブロックチェーン  
・サービス

- IBM Blockchain Platformの  
特徴と活用方法 -

申込サイト <http://ibm.biz/BCwebinar>

# ご清聴ありがとうございました。

貝塚 元彦

日本証券アナリスト協会検定会員

インダストリー・コンサルタント

ブロックチェーン・ソリューションズ部長

インダストリー・ソリューションズ事業開発

日本アイ・ビー・エム（株）

Mobile: +81 80-5915-4396

Mail: mkaizuka@jp.ibm.com

IBM Blockchain Link: [ibm.com/industries/jp/ja/blockchain](https://ibm.com/industries/jp/ja/blockchain)