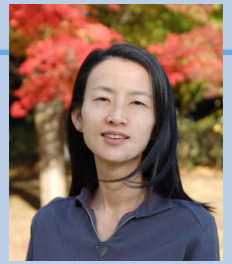
ブロックチェーンの最近の動向

吉濱佐知子, Ph.D
日本アイ・ビー・エム株式会社
東京基礎研究所
ブロックチェーン・テクノロジー担当部長

IBM Research について



IBM基礎研究部門: 世界13拠点/3,000人
全ての研究所が、何らかの形でブロックチェーンに関与

- Hyperledger Fabric基盤の技術開発
- 実証実験、技術支援、ソリューション開発

ブロックチェーンへの意識の変化

2016年２月

- ブロックチェーンとは何か？
- ビットコイン？
- どう動くのか？
- 何に使えるのか？

2017年２月

- ブロックチェーンについておおむね理解した。
- 自社の業務の中で、どのように使えば大きな価値が出るのか？
- 様々なプラットフォームが乱立しているが、何を使えばいいのか？

ブロックチェーンのユースケースは多様化

金融 ← → 非金融

契約やプロセスの自動実行

情報共有基盤

価値の取引

金融市場

Nasdaq

ASX

JPX JAPAN EXCHANGE GROUP

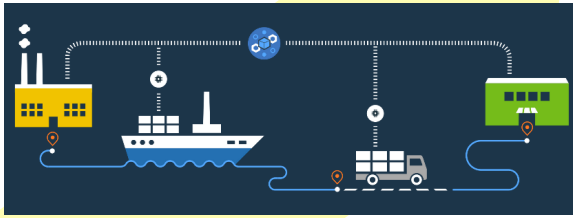
London Stock Exchange

再保険

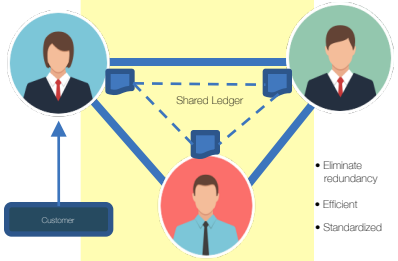
LLOYD'S laboration

B3i

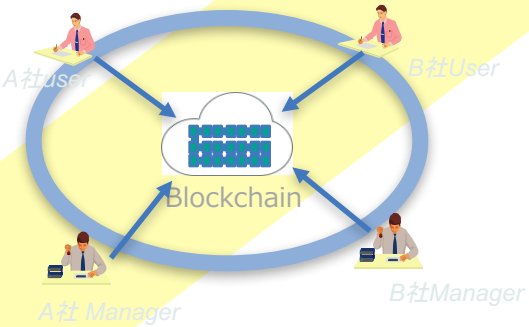
貿易（物流・金融）



KYC/AML

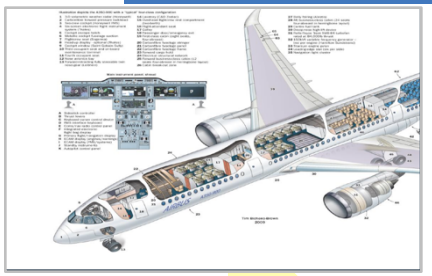


契約管理



食品トレーサビリティ

部品の来歴管理



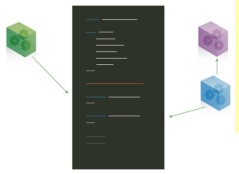
送金・国際送金

仮想通貨

ダイヤモンドの来歴管理

everledger

資産管理



Hyperledger Fabric の変遷

黎明期
(2015末～)

- 金融インフラ等として使用する上での要件を取り込み、従来の分散DB/コンピューティング技術を取り入れた新たなブロックチェーンを基盤を開発
  - 分散データベース (key-value store)
  - スマートコントラクト
  - ファイナリティのあるコンセンサス・アルゴリズム
  - セキュリティ＆プライバシー（認証、匿名化、暗号化等）

v0.5～0.6
(2016.03～)

- 様々な業務を想定した実証実験で検証し、課題を抽出
  - パフォーマンス
  - スケーラビリティ
  - より高いセキュリティ＆プライバシー
  - 単一障害点の排除

V1.0
(2017.03)

- 新しいアーキテクチャに刷新し、課題を改善

Hyperledger Fabric V0.6からV1.0へ: 業務使用可能な基盤への進化

カテゴリ	**V0.6** (2016.09)	**V1.0** (2017.03)
コンセンサス	トランザクション実行前にコンセンサスを取るため、実行結果について合意していない。結果として、非決定的チェーンコードにより実行結果が異なっても、ブロックに書き込まれてしまう。	トランザクション実行結果についてコンセンサスを取る。
パフォーマンス	チェーンコードが逐次実行されるため、ボトルネックとなる。	チェーンコードの並列実行を可能とする。
メンバーシップサービス（認証局）	認証局が１つしかないので、単一障害点となる。また、パフォーマンス上のボトルネックとなる。	分散化された認証局をサポートする。
プライバシー	すべてのノードが同じデータを持ち、同じチェーンコードを実行するため、個別のプライバシーを設定できない。	プライベートチャネルの導入により、ネットワーク内の一部のノード間に閉じたデータ共有が可能になる。
スケーラビリティ	ノード数の上限が低い・動的にノードを追加できない（PBFTの特性）。	より多くのノードをサポートし、動的なノード追加も可能になる。
データベース	KVSのみ。クエリー機能などが不十分で不便。	プラッガブルに様々なデータベースをサポート。
アップグレード	チェーンコードをアップグレードすると、過去のデータにアクセスできなくなる	チェーンコードのアップグレード後のデータの移行が可能になる。