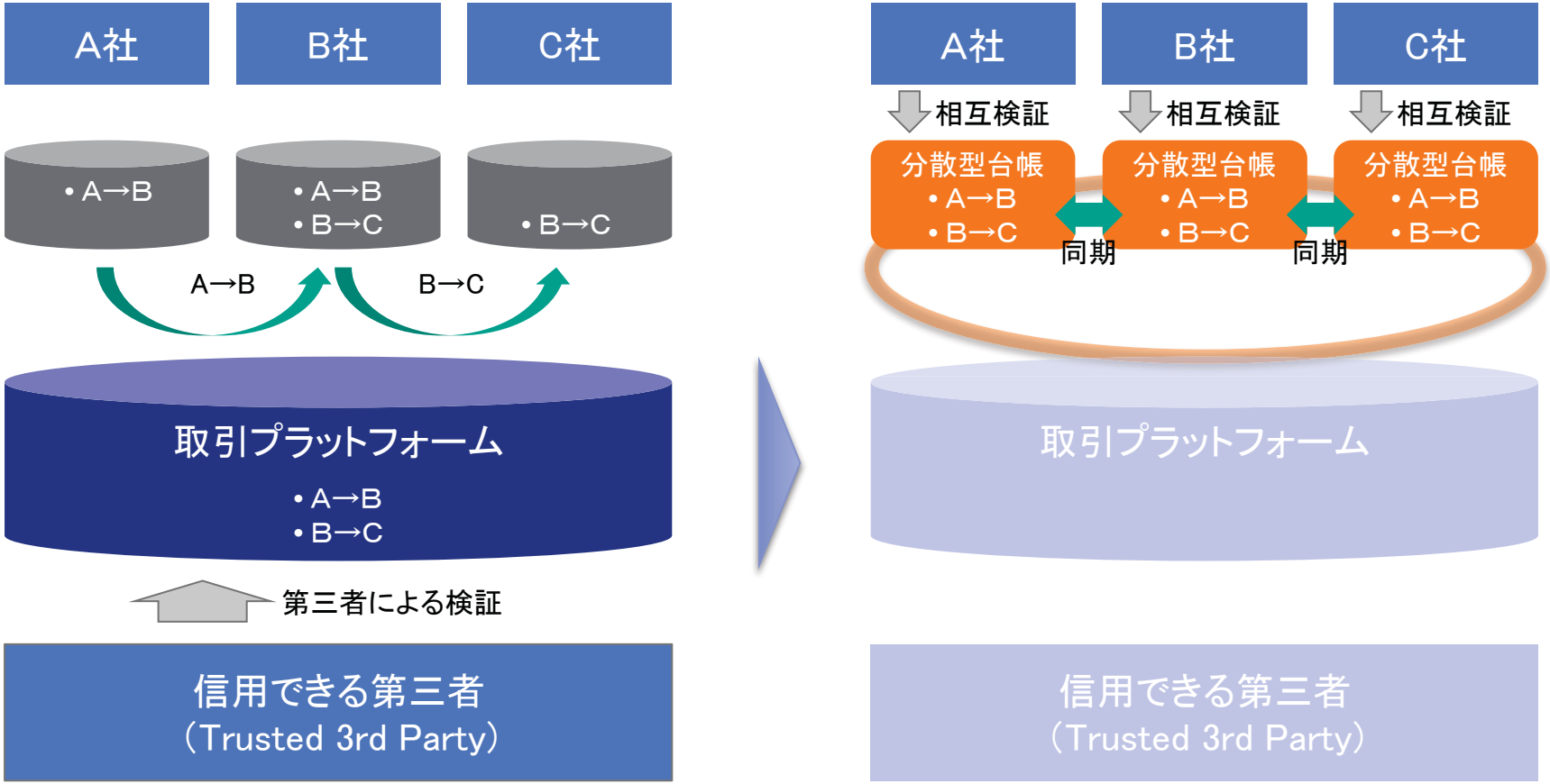
ブロックチェーン技術を金融業務に適用する際の留意点

2016年3月17日
日本アイ･ビー･エム株式会社

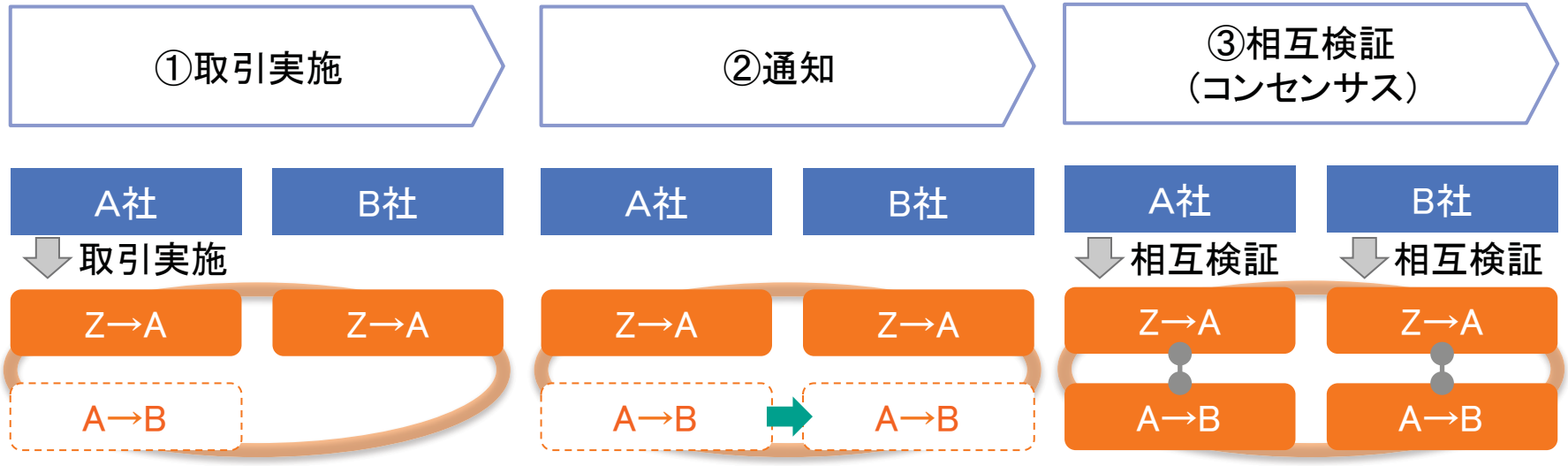
ブロックチェーンとは

- Satoshi Nakamotoがビットコイン向けに開発したP2P(Peer-to-Peer)技術
- 信用できる第三者を(基本)必要とすることなく取引等を行うことが可能
- ビットコイン以外のユースケースでの活用が期待されている



取引の流れ

・ ①取引実施、②通知、③相互検証の3段階で取引を処理



- A社がB社に送金
- 取引を他に通知
- 取引を相互検証（コンセンサス）

ビットコイン版ブロックチェーンの主な課題

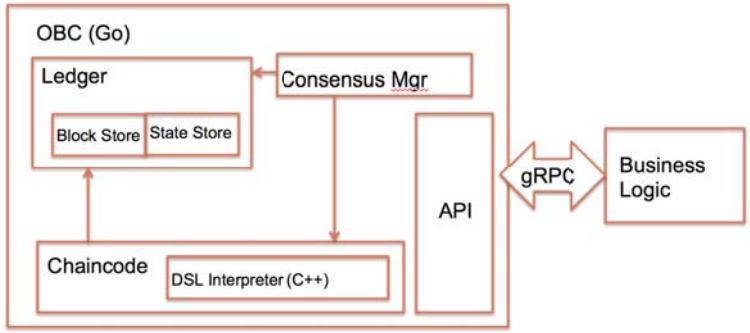
ビットコインの特性	ビットコイン版ブロックチェーンの主な課題
• 匿名性 (Anonymity)	• ビットコインの場合はpermissionless/trustless • 参加者が匿名の為、AML/CFT対応が困難
• 透明性 (Transparency)	• ビットコインの場合は取引が平文で流通 • 利益情報を含む金融取引等、秘匿性(Privacy)を必要とするユースケースには向かない
• ブロックチェーンの分岐 (Fork)	• ビットコインの場合は分散型台帳がフォーク(分岐)する等の理由により、厳密な”ファイナリティ”がない
• マイニング (Proof of Work)	• ビットコインの場合は相互検証に多大なシステムリソースを必要とする • トランザクション処理性能の限界(7取引/秒) • インセンティブが無くなった後はどうするのか

あるべきブロックチェーン基盤整備に向けた取組み

取組み	取組み概要
• あるべきブロックチェーン基盤の整備（Hyperledger Project）	• 多くのオープン技術を確立してきたLinux Foundationのもと、各企業とのコラボレーションを通じ、あるべきブロックチェーン基盤を整備
• コンソーシアム・プライベート型ブロックチェーン（Permissioned/trusted）	• Permissioned/trusted（主体の顕名性確保） • 参加者のidentity保証（認証局の設置） • ブロックチェーンの良さでもある『信用できる第三者を必要としない仕組み』とのバランスも考慮
• 透明性と匿名性・秘匿性のバランス	• AML/CFTや相互検証に必要な透明性を確保しつつ取引の匿名性・秘匿性を実現
• “ファイナリティ”を確立するコンセンサスモデル（PBFT/PBFT-Sieve）	• “ファイナリティ”のある相互検証 • 多くのシステムリソースを前提としない相互検証

Linux Foundation Hyperledger Project

- Ripple・IBM・DAH・Blockstream4社（順不同）がHyperledger Projectにコード提供
- 今後IntelやJPMC等からも提供予定
- 2/25 TSC (Technical Steering Committee)にてDAH/IBM Proposalに従い進めることを確認

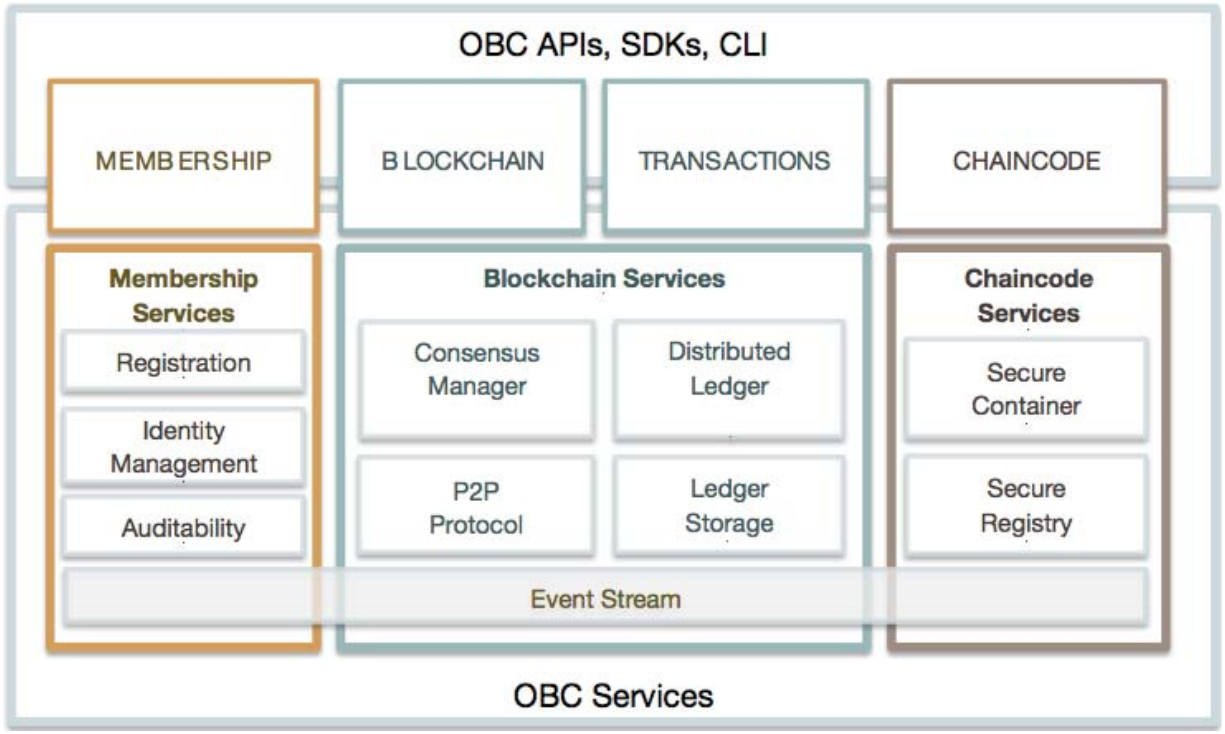
第一段階: Two Initial Code Bases	第二段階: Single Code Base
• Bitcoin (UTXO) モデルの検証 • DAH Java + Blockstream libconcensus	• 汎用性のあるFlexibleなIBM OBC (Open Block Chain)にBitcoin (UTXO)モデル等を統合
• Alternate モデルの検証 （汎用性のあるモデル） • IBM OBC (Open Block Chain)	

※DAH-IBM Hyperledger Project Proposal – 20160223v2.docxより作成

“ファイナリティ”を確立するコンセンサスモデル

コンセンサス モデル	①取引実施	②通知	③相互検証
マイニング (Proof of Work)	• 取引実施	• **取引を各ノード (マイナー)**に通知	• **各マイナー**が取引をパッケージング(仮ブロック)の上、検証 • 最も早く検証が完了したマイナーのブロックが正 • 場合によってはフォークが発生(分散型台帳の複数バージョン)
PBFT PBFT-Sieve	• 取引実施	• **取引をLead Validator(のみ)**に通知	• Lead Validator**(のみ)**が取引をパッケージング(仮ブロック) • **共通の取引パッケージ**(仮ブロック)をValidatorが検証し、ブロックを確定(ファイナル)

IBM OBC (Open Block Chain)



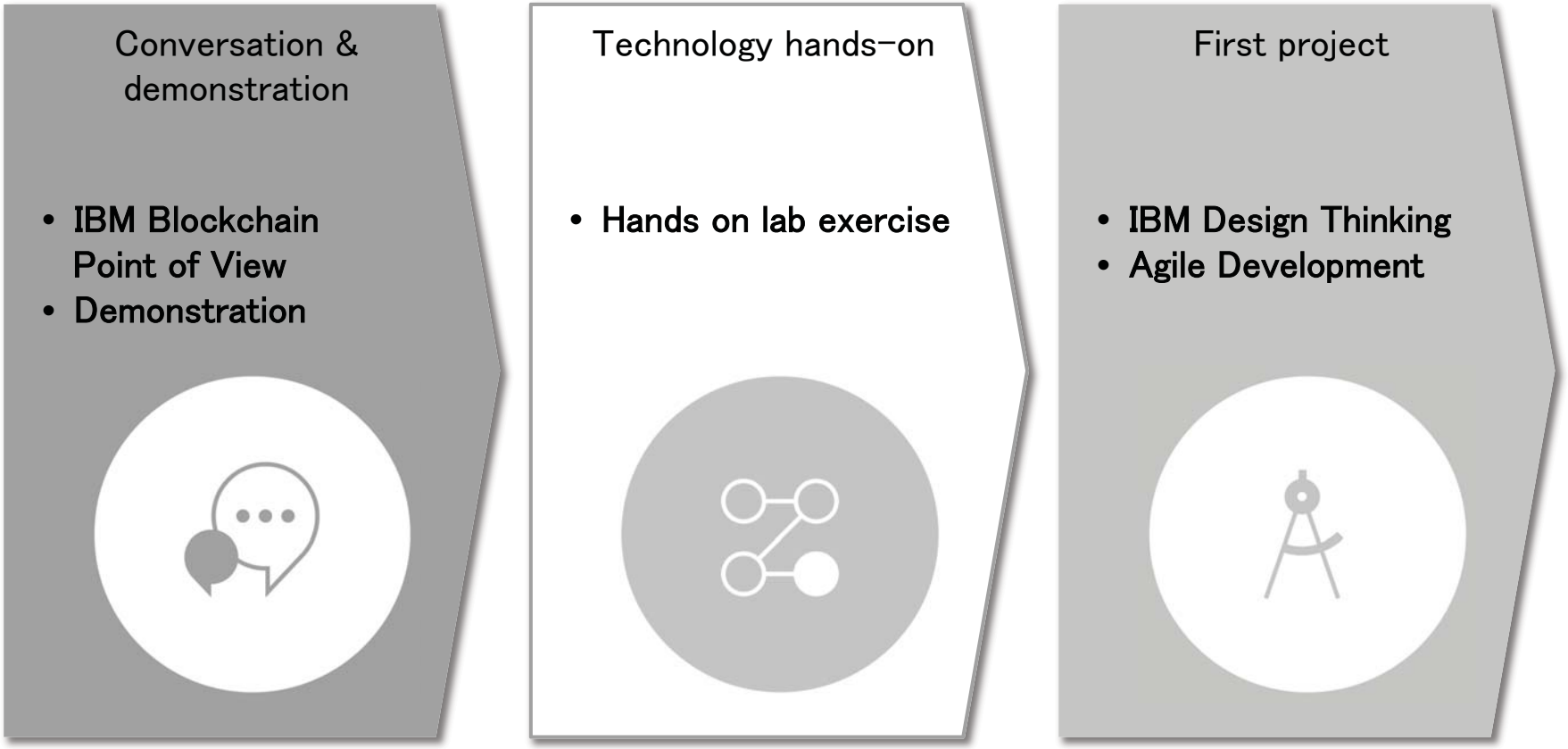
IBM OBCの特徴

- 仮想通貨等、金融取引ユースケースのみでの利用を前提としない、汎用性のあるアーキテクチャー
- Permissioned/trusted ネットワーク（Membership）
- 匿名性・秘匿性対応
- 多くのシステムリソースを前提としない、効率的なコンセンサスモデル（& Pluggable）

一方、インセンティブ課題等、あるべきブロックチェーン基盤に向けた検討は今後も必要
（システム外での対応含め）

IBM Bluemix for blockchain garage

・ ニューヨーク、ロンドン、シンガポール、東京にIBM Bluemix for blockchain garageを開設予定



参考：日本取引所グループとの実証実験

ニュースルーム > ニュースリリース >

日本取引所とブロックチェーン技術の実証実験で合意

Select a topic or year

↓ ニュースリリース　　↓ 関連する XML feeds

TOKYO - 16 2 2016:

2016年2月16日

日本IBMは、株式会社日本取引所グループ（以下、JPX）と共同で低トランザクション市場を想定したブロックチェーン※1技術に関する実証実験を、3月より支援することで合意しました。

ブロックチェーンはより多くの取引参加者に対し、低コストで効率的な取引の仕組みを実現できる可能性があり、海外においても実証実験が行われるなど、高い関心を集めています。

今回、日本IBMはJPXと共同で、ブロックチェーン技術の特性を長短所の両面から早期に把握し、ブロックチェーン技術の評価と低コストでの運営可能性を検証します。

本実証実験では、業界標準として広く普及する可能性や、各種認証方式やプライバシー要件、複数資産カテゴリー、複雑な業務処理への適用を勘案し、多くのオープン技術を確立してきたオープンソース・コミュニティであるLinux Foundationが提唱するハイパーレジャー（Hyperledger）プロジェクトのフレームワークを利用予定です 。

ハイパーレジャーの開発には、グローバルのIBM リサーチが貢献しています。今回の実証実験で日本IBMは、IBM東京基礎研究所を含むIBMリサーチとの連携や、金融機関を含む60社を超えるグローバルでのお客様との検討実績といったグローバルのネットワークを活かした支援を推進していきます。

※1: 分散型台帳技術。取引記録や資産登録簿などのデータを分散型ネットワーク上の参加者にて安全に共有し管理する技術。低コストでの構築運用が可能と考えられている。

- 低トランザクション市場を想定した場合の、技術的な限界や可能性についての評価を実施
- 精算・決済といった『ポストトレード処理』の効率化に寄与する可能性がある
- **Hyperledger ProjectはLinux Foundationが主導することから業界標準に成長する可能性がある**