日本銀行 第3回 FinTechフォーラム

# 証券ポストトレードへのブロックチェーン技術検証と今後の課題

2017年 2月28日

株式会社 みずほ銀行
富士通 株式会社

本プレゼンテーションには、出願中の特許（２件）の内容が含まれております。

# 目次



## 1．これまでの取組み

・証券ポストトレードでのフェイルを低減
・証券ポストトレードの実証実験の流れ

## 2．今回の取組み

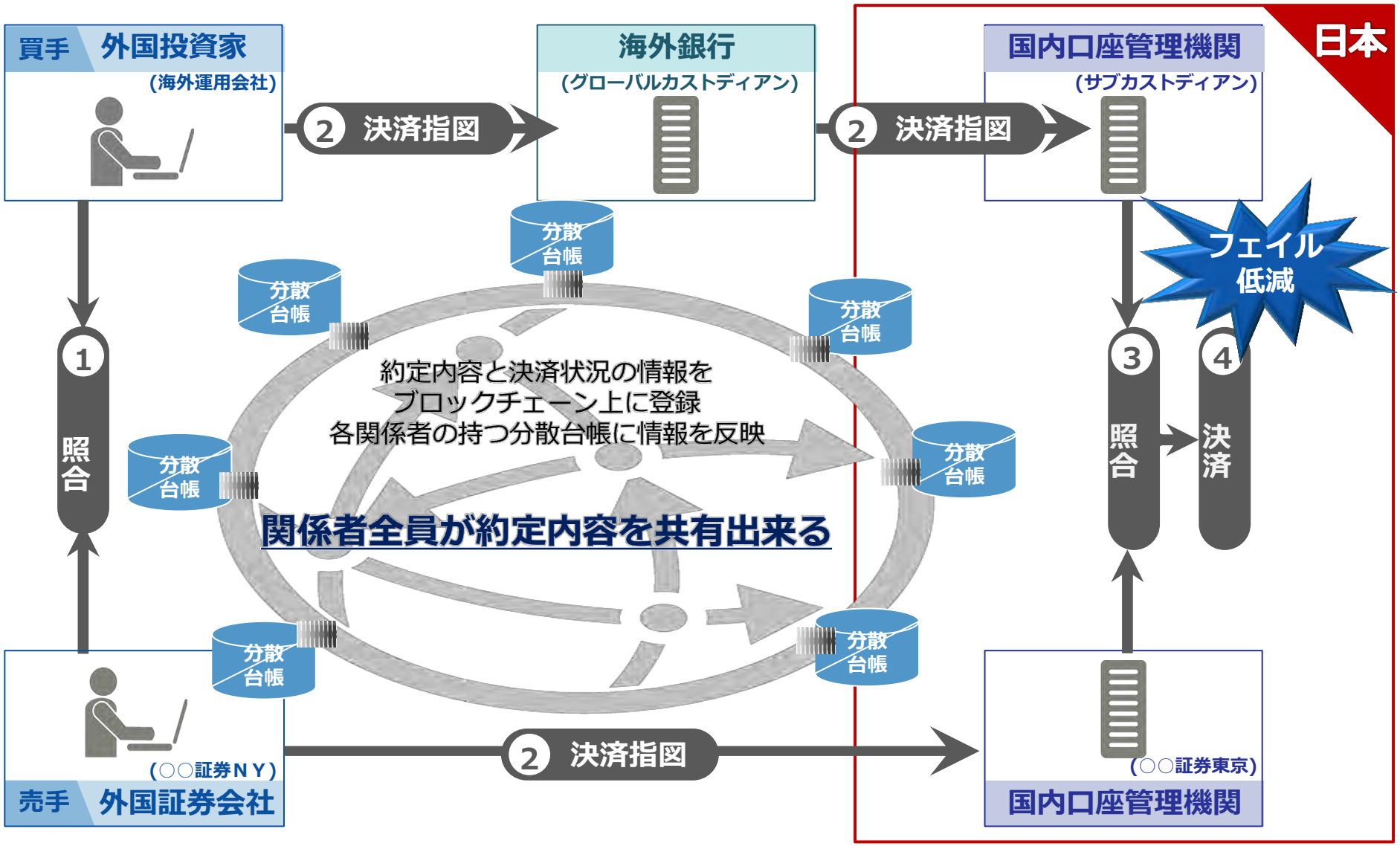
・BitcoinとHyperledger Fabricの違い
・アプリケーション開発における課題
・参加者管理、認証局における課題

## 3．今後の取組み

# これまでの取り組み

# 【振り返り】
# Blockchainで約定内容を共有し、フェイルを低減。

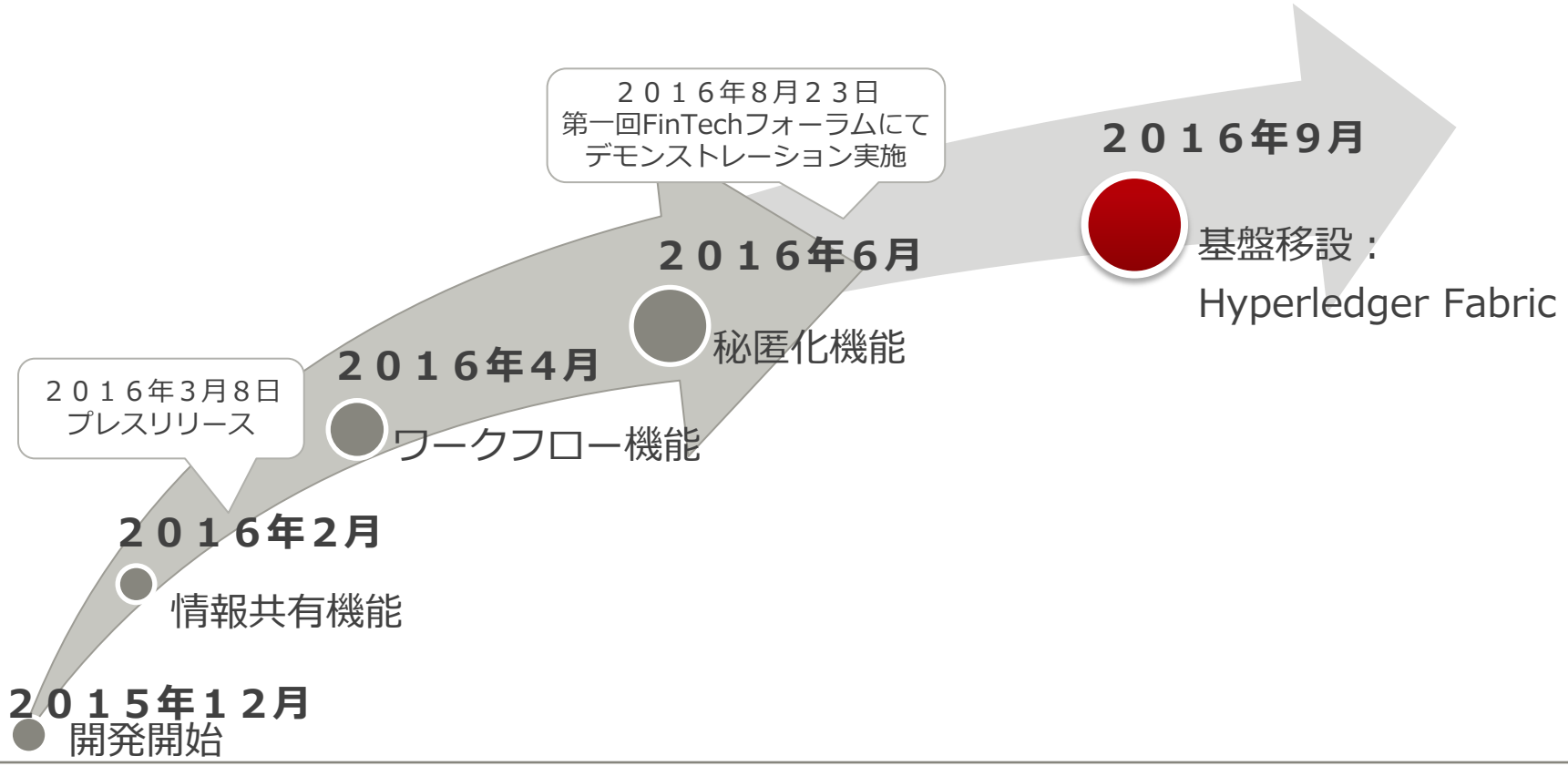




# 証券ポストトレードの実証実験の流れ



- 多くの実証実験が行われているコンソーシアムチェーンを用いて、業務課題を見出す
- 汎用性の高いHyperledger Fabricに注目



# 今回の取り組み

# BitcoinとHyperledger Fabricの違い



■ 証券ポストトレードシステムをBitcoin(ColoredCoin)、Hyperledger Fabric v0.6.1に実装して比較

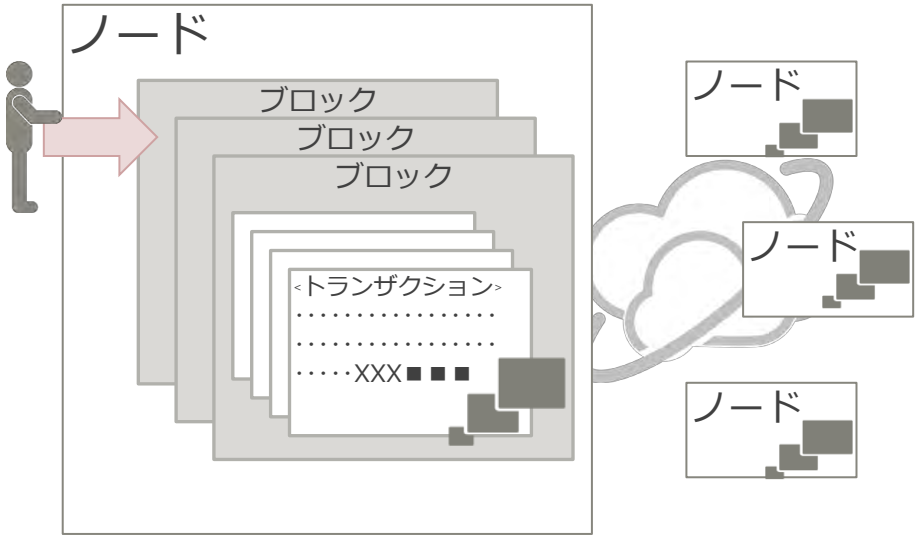
| 項目 | Bitcoin | Hyperledger Fabric |
|---|---|---|
| 種別 | • パブリック | • プライベート/コンソーシアム |
| 基盤の特性 | • 仮想通貨基盤 | • 汎用基盤 |
| 合意形成 | • Proof of Work<br>全ノードによる競争 | • PBFT<br>検証ノードによる合議 |
| データの公開範囲 | • すべての参加者に公開<br>Bitcoin基盤には制御機能はなく<br>アプリケーションに制御機能を実装 | • 公開範囲の制御が可能<br>Fabricの機能を使って実装 |
| アプリケーション開発 | • データサイズに制約あり、工夫必要 | • いわゆる”スマートコントラクト”となるアプリケーション(“チェーンコード”)を汎用言語で実装可能 |
| 参加方法 | • 誰もが参加可能 | • 認証局に許可されたノードのみ参加可能 |

# アプリケーション開発



## Bitcoin

- データの格納サイズや利用方法など、制約が大きい

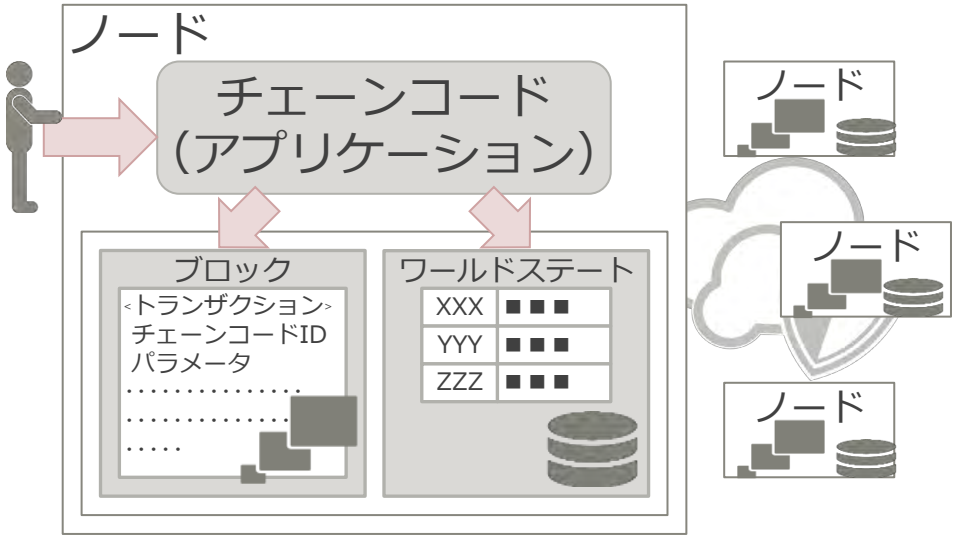



トランザクション情報の余白(OP_RETURN)に
約定情報・承認情報を追記

約定情報・承認情報は
複数のトランザクションを分割して登録

## Hyperledger Fabric

- スマートコントラクトを実現する
  チェーンコード（アプリケーション）を
  汎用言語（Java、Go）で実装可能
- ワールドステート（KVS）にデータ保管




トランザクション情報とは別に
ワールドステートに約定情報・承認情報を保持

約定情報・承認情報はワールドステートに登録

# アプリケーション開発における課題（Fabricの場合）



## ■ アプリケーション（チェーンコード）は汎用的、自由度が高い

- 様々なアプリケーションを実現可能
- ソフトウェア技術者のハードルが低く、ブロックチェーン活用を促進

## ■ 一方で、アプリケーションの品質担保が課題

- 各ノードで実行されるアプリケーションの実行結果は必ず同じになるように注意必要（時刻や乱数等、ノードごとに異なる情報を利用しない）
- Fabric V1.0に向けて“Next Consensus Architecture”でノード間の整合性は保たれるが、アプリケーションの実行結果が正しいことを証明できるか

**従来のシステム開発と同じく、品質確認の仕組みや制度が必要**

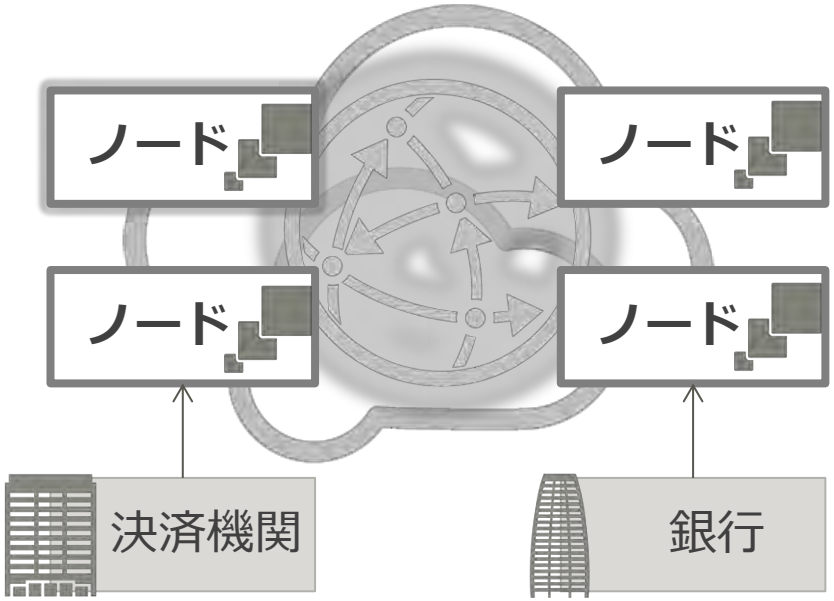
- **アプリケーションの品質検証と担保**
- **アプリケーションの配備を承認する制度**

# 参加者の管理



## Bitcoin

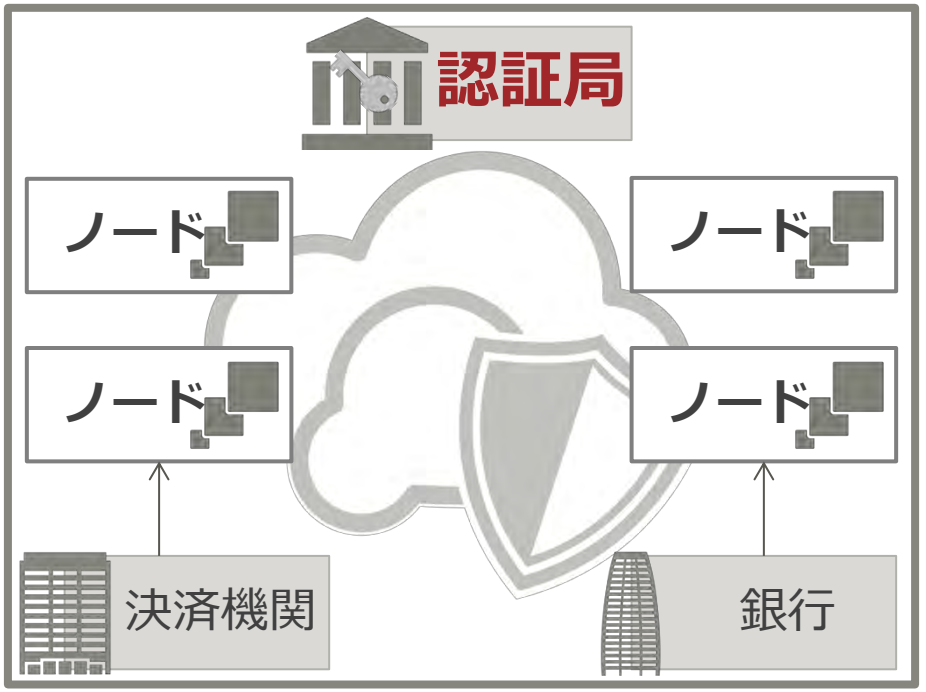
- オープンな環境
- 誰でも参加可能
- 接続さえすれば全員が情報共有可能




Bitcoinネットワークにより、誰もが情報共有可能

## Hyperledger Fabric

- クローズドな環境
- 限定されたメンバーのみ参加可能
- 認証局から承認されたメンバーのみ情報共有可能




限定されたメンバーだけで安全に情報共有可能

# 認証局に関する課題（Fabricの場合）

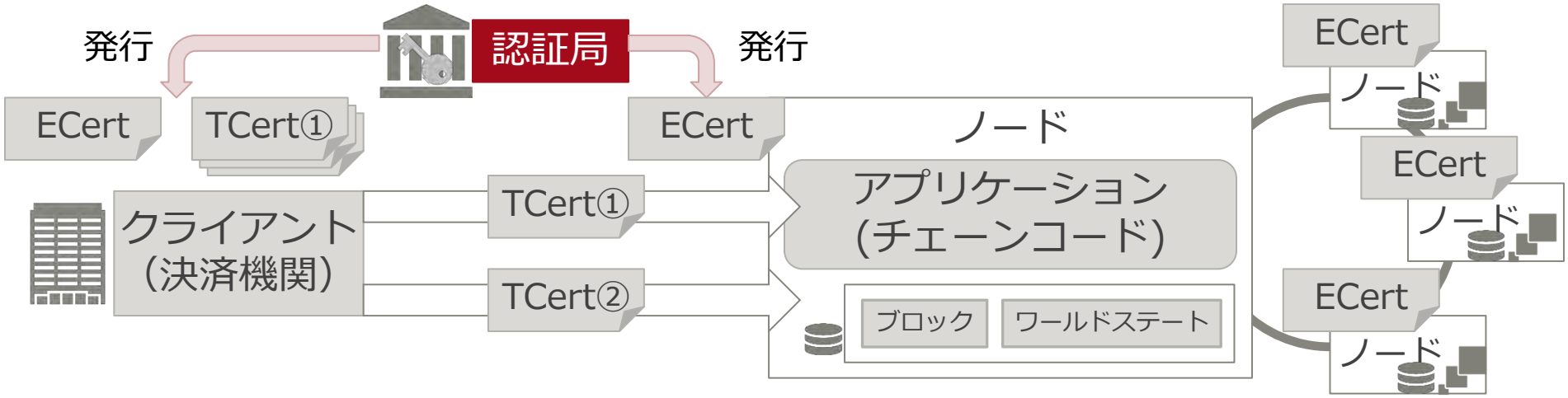


## ■ 公開鍵基盤（PKI）の仕組みにより、高いセキュリティを実現

- 鍵管理をＨＳＭ(ハードウェア・セキュリティ・モジュール)を利用する等、高い安全性が確立された従来技術を適用

## ■ 運用上、認証局が重要な位置づけを担っている

- コンソーシアムへ参加する時
  認証局の許可（ECert）なくして、コンソーシアムチェーンに参加できない
  コンソーシアムの中でも、認証局の運営主体が重要になる
- 個々のトランザクションを発行する時
  認証局が発行するトランザクション証明書（TCert）を付加する必要あり
  使い方によっては、認証局がシングルポイントとなってしまう
  （Hyperledger Fabric V1.0では認証局を二重化できる予定）

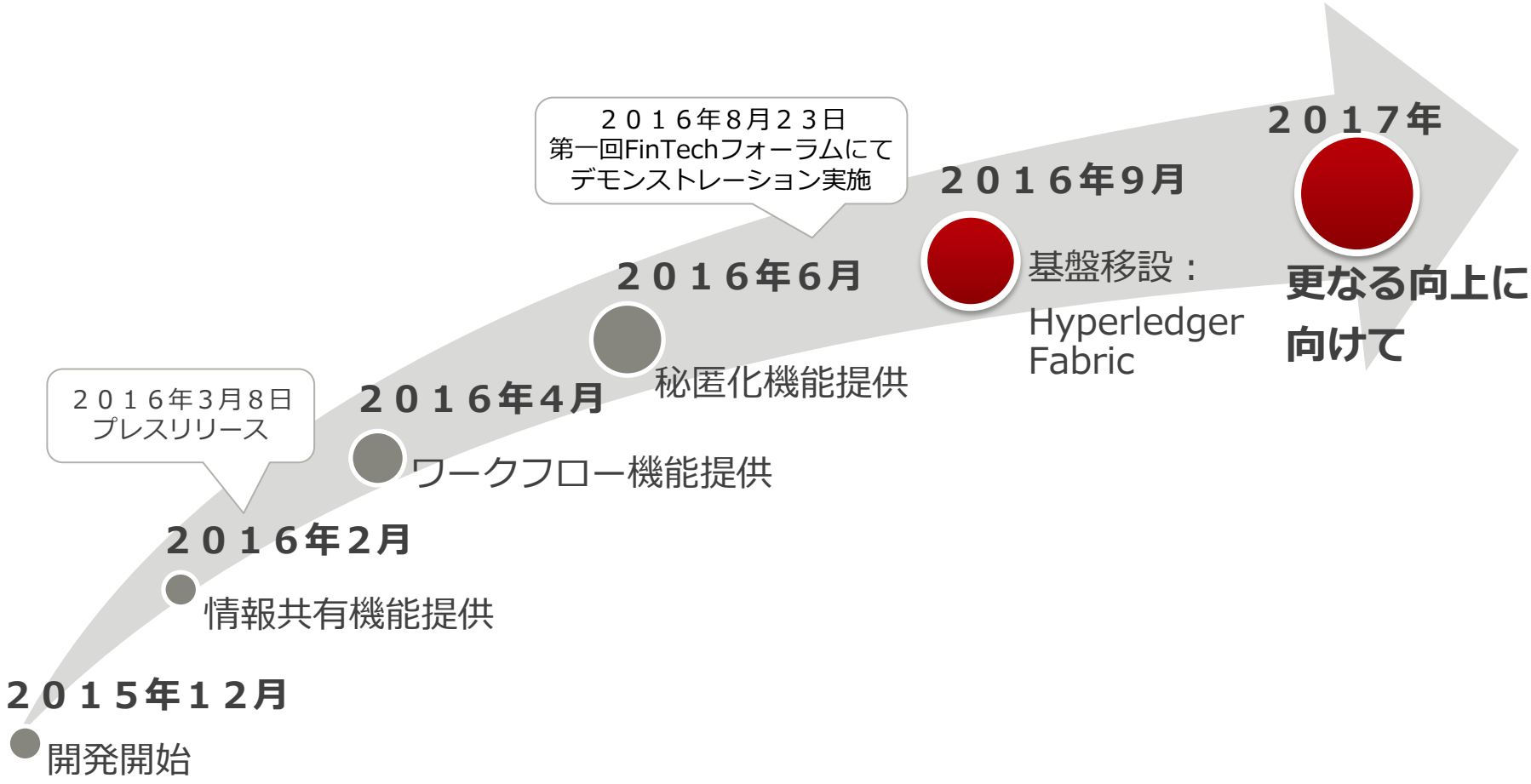


# 今後の取り組み

# 今後に向けて



- ブロックチェーン基盤の特徴に応じて、使い分けていく必要あり
- 今後も、他のブロックチェーン基盤での実証を進めることにより実用化に向けた見識を深めていく



MIZUHO FUJITSU