東京短資株式会社
THE TOKYO TANSHI CO.,LTD.
×
@HAW
International Inc.

ビットコイン・ブロックチェーンの資金貸借市場への応用可能性

PoC experiment for a lending market on Bitcoin Blockchain

2017年2月28日
第3回FinTechフォーラム

東京短資株式会社　仲宗根 豊
株式会社ハウインターナショナル　取締役CTO 高橋 剛

Background info.　Who?

東京短資株式会社
THE TOKYO TANSHI CO.,LTD.

Founded 1909

Interbank
Money Market Broker

HAW International Inc.

Founded 1999

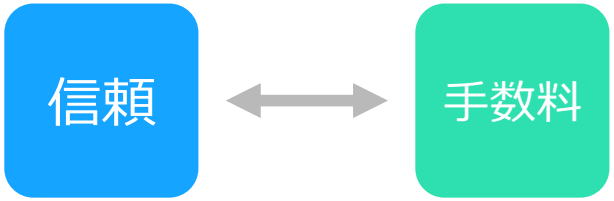
クラウドをベースとした
システム開発企業

2015年初頭からブロック
チェーンの研究開発を開始

東京短資株式会社 THE TOKYO TANSHI CO.,LTD. × HAW International Inc.

Background info. Why Totan?

仲介ビジネスの抽象化



様々な形態の信頼

仲介者としての信頼
最適な相対者を見つける信頼
…

信頼できる第三者が不必要
「送金」の実験

bitcoin

<u>貸借取引において“信頼できる第三者”である我々は？</u>

Background info.
Why lending without TTP(Trusted Third Party)?

東京短資株式会社 THE TOKYO TANSHI CO.,LTD. × @HAW International Inc.

自らをDisruptするモデルからの検証

<u>現在の置き換えではなく、
新しい可能性を見たい</u>

Background info. Bitcoin?

bitcoin

“**トラストレス**なクロニクル”

（信頼できる第三者を必要としないセキュアな歴史的記録）

*ここでいうセキュアとは改ざんが困難である、また、ビザンチン障害に耐性があること

Background info. Bitcoin?

bitcoin

実験的なデジタル通貨システム
”世界中どこの誰にでも送金できる“*

* github.com/bitcoin/bitcoin

Background info. Bitcoin’s preconditions

bitcoin

◆ 前提条件(Satoshi Nakamoto論文より)
- P2P、分散 DB
- 暗号学的証明を信頼（離散対数問題等）
- 相対取引かつ直接取引
- 51%攻撃がない限りにおいてセキュア

◆ 機能的な制限、特徴
- スケーラビリティ
- 秘匿性
- 取引記録の透明性

Background info. Ledger technologies.

世の中、数多のblockchainと呼ばれるものがあるが…

ethereum

bitcoin

HYPERLEDGER

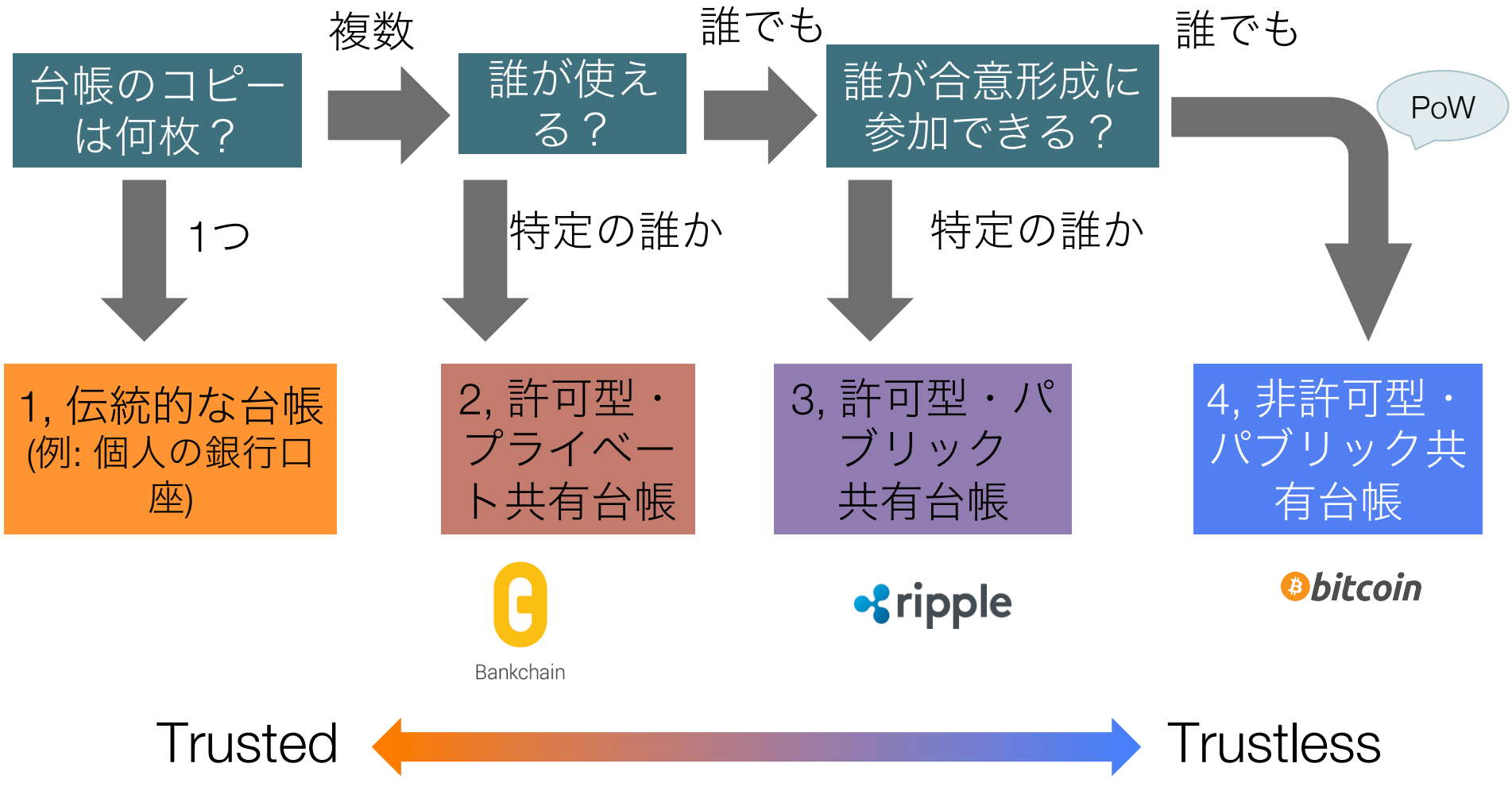
ripple

東京短資株式会社 THE TOKYO TANSHI CO.,LTD. × HAW International Inc.

Background info. Ledger technologies.

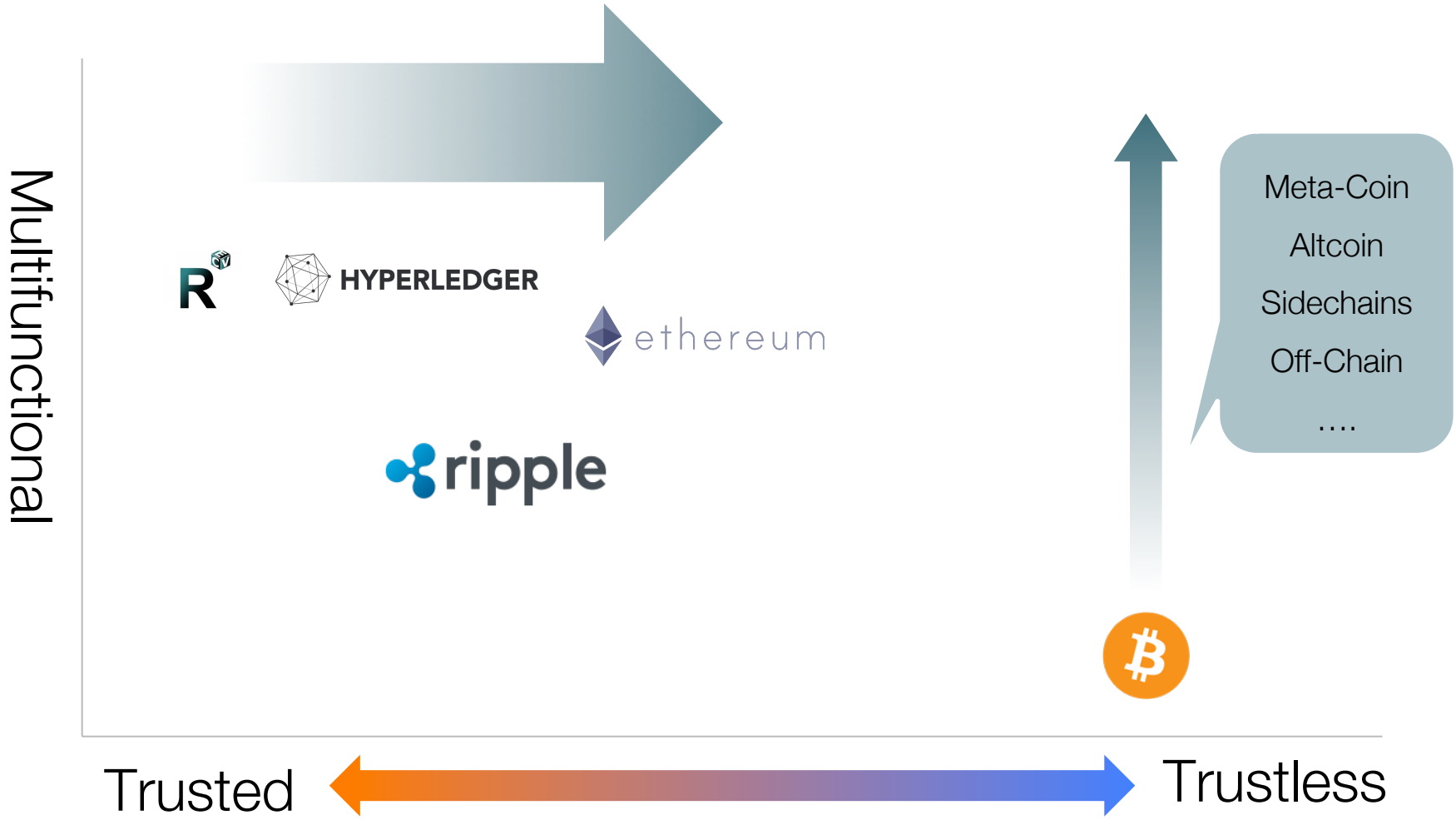
最も“信頼点”が分散されセキュアな
Ledgerを基盤にしたい。

Background info. Ledger technologies.



*Dave Birch (Consult Hyperion) の図を改変して引用

Background info. Ledger technologies.



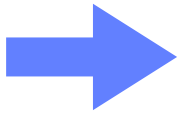
*DG Labの図を改変して引用
*ポイントはイメージ

Why Bitcoin Blockchain ?

◆TTP less

◆hash power (secure)

◆オープンで盛んな研究



bitcoin

基盤として採用

PoC概要

◆目的
金融市場インフラに対するパブリックなブロックチェーンを適用する実証実験の実例が現時点では乏しいため、知見や技術を獲得すべく、実証実験を行っている。

◆ステータス
現時点では概念を実証すべく、プロトタイプ構築の最中にある。
検証・評価する段階にはない。

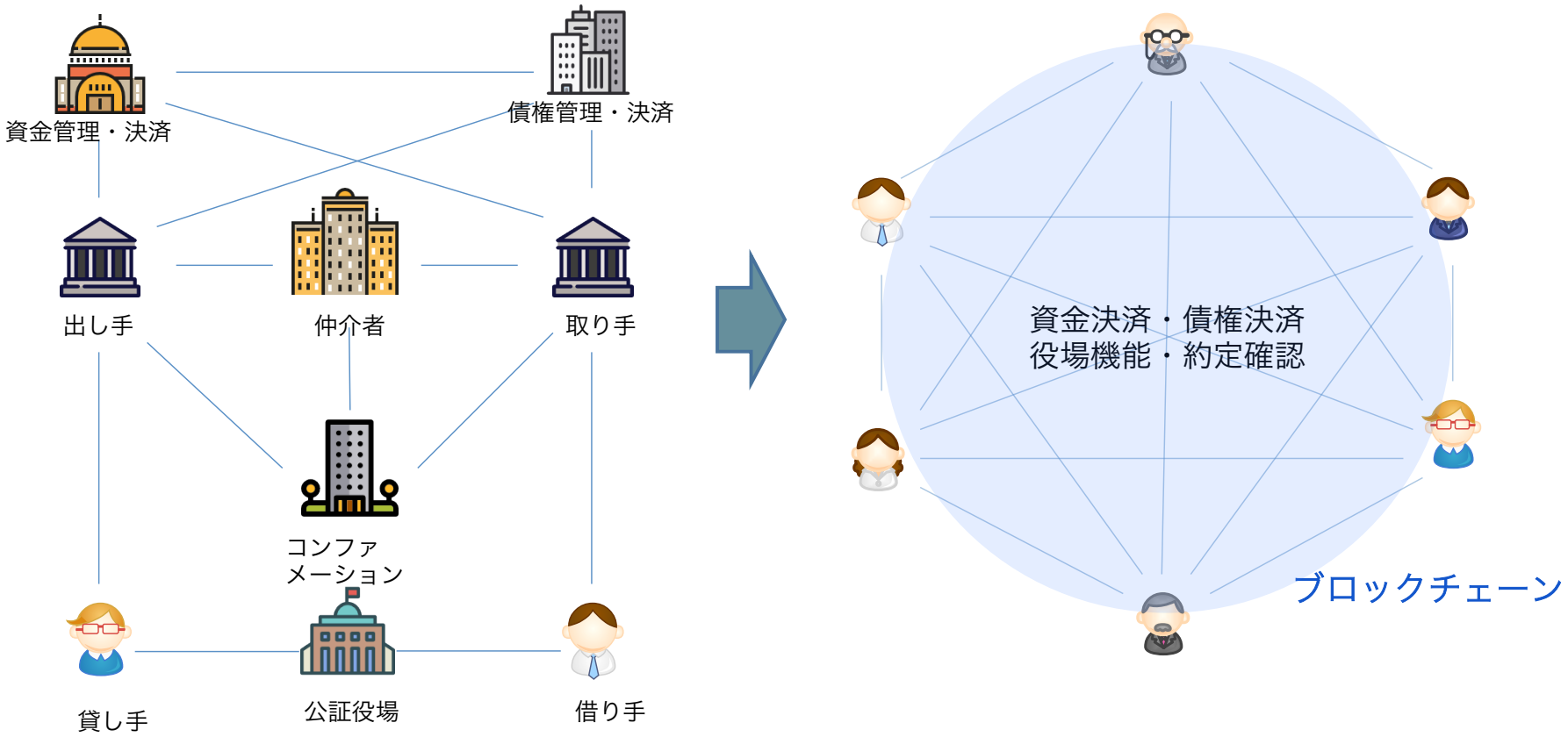
◆採用した規格
Bitcoin protocol、Overlay protocol on Bitcoin (OAP, PoE)

◆その他研究対象の規格
Other Meta-Coin, Altcoins, Side-chain, Off-chain, DLT(PBFT)

◆対象としたこと
商品性を削ぎ落とし、抽象化した“資金貸借”
資金と権利の移転
Bitcoin protocolに基づく、金融取引要件の表現
クローズドな取引参加者ネットワーク

◆今後の対象
処理性能やコンセンサスアルゴリズム等の検証・評価
ブロックチェーン実装の比較
特定の市場、商品への適用

PoC概要


資金管理・決済
債権管理・決済
出し手
仲介者
取り手
コンファ
メーション
貸し手
公証役場
借り手
資金決済・債権決済
役場機能・約定確認
ブロックチェーン

PoC概要

より抽象的

資金貸借取引の抽象化/要件のBC化								
			①現状	②コンファメーションのBC化	③債権のBC化	④債権と資金決済方法のBC化	⑤預金通貨にて暗号通貨を併用	⑥預金通貨の暗号通貨化	**⑦現金通貨の廃止・暗号通貨のみ**
DVP			**現DVP**	現DVP	現DVP	疑似DVP	仮想DVP	BC DVP	**BC DVP**
資金決済	決済手段	現金通貨	**JPY**	JPY	JPY	JPY	JPY	JPY	Blockchain
		預金通貨						Blockchain	
	決済方法	日銀ネット口座振替				Blockchain	Blockchain		
債権		発生・譲渡・消滅	**現行**	現行	Blockchain				
コンファメーション			約定確認仲介	Blockchain コンファメーション不要					
通貨・決済の信頼性			日本政府、日本銀行、PoW						PoW
Gateway (参加者の本人確認)			日銀、保振、短資会社、電債記録機関、取引所等						ネットワーク

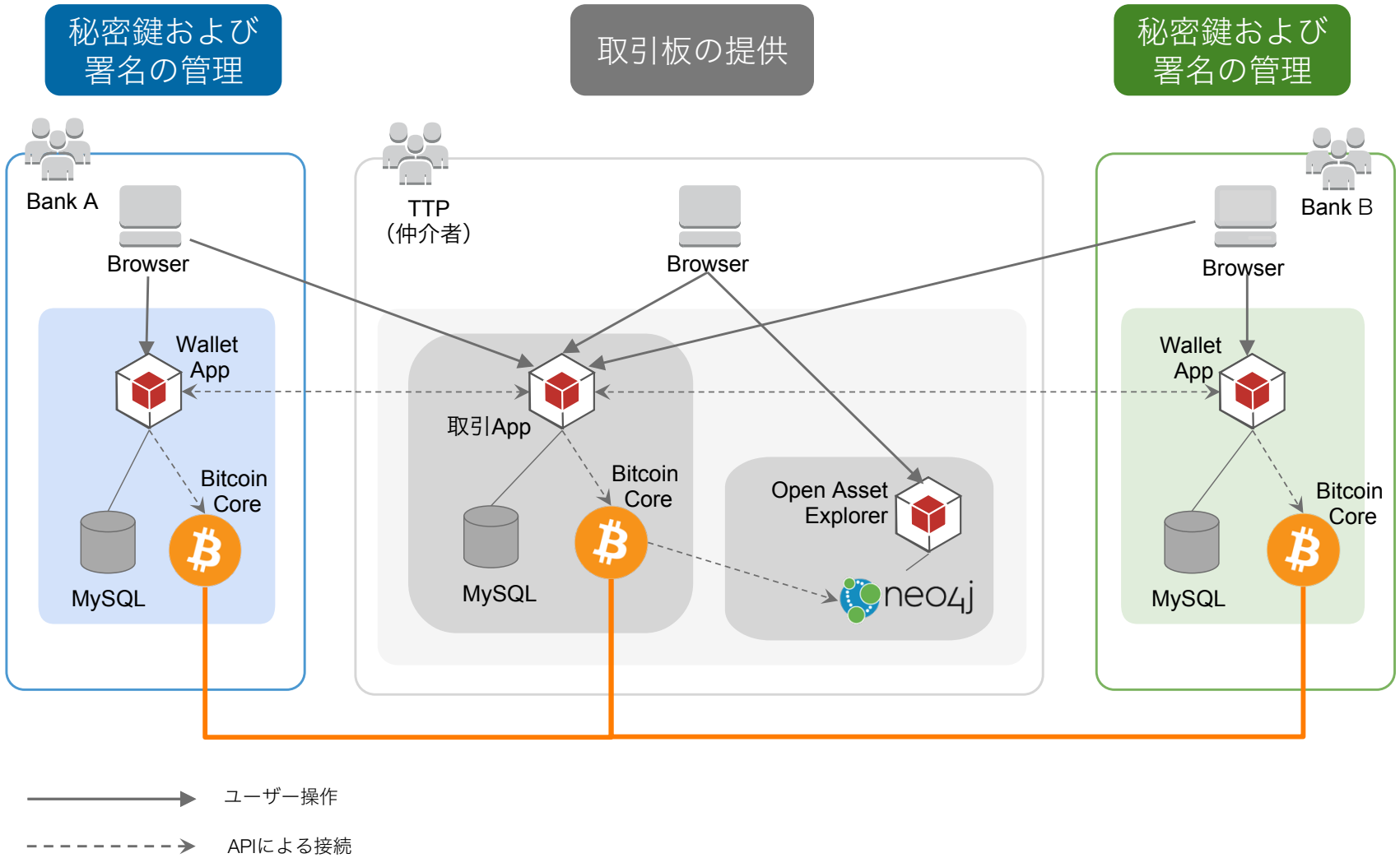
現DVP…資金決済と債権決済の物理的場所が異なる。※例外あり ex, JGB
擬似DVP…債権決済と資金決済方法が同一トランザクション
仮想DVP…債権決済と法定通貨とペッグされた仮想通貨が同一トランザクション
BC DVP…債権決済と預金通貨（仮想通貨）決済が同一トランザクション

PoC概要

PoC機能別分類

機能 ＼ 信頼点(記録媒体)		現状	PoC				
		中央管理者/仲介者	参加者自身	中央管理者/仲介者	コンソーシアムDLT	パブリックBlockchain	パブリックBlockchain上のOverlay
前提	通貨の信頼性	中央管理者/仲介者				Bitcoin NW	
	口座管理	中央管理者/仲介者	参加者				
	債権の移転 (発生/分割/譲渡/償還)	中央管理者/仲介者					Open Assets Protocol / PoE
	OnBoarding	中央管理者/仲介者		中央管理者/仲介者			
Pre trade	注文	中央管理者/仲介者		中央管理者/仲介者	コンソーシアム型DLT	→	Overlay
	取引板	中央管理者/仲介者		中央管理者/仲介者	コンソーシアム型DLT	→	Overlay
	マッチング	中央管理者/仲介者		中央管理者/仲介者	コンソーシアム型DLT	→	Overlay
Trade	約定	中央管理者/仲介者		中央管理者/仲介者	コンソーシアム型DLT	→	Overlay
	コンファーメーション	中央管理者/仲介者					
	支払い指図	中央管理者/仲介者				Bitcoin NW	
	資金決済	中央管理者/仲介者				Bitcoin NW	
Post trade	債権決済	中央管理者/仲介者				Bitcoin NW	

システム構成


秘密鍵および
署名の管理
取引板の提供
秘密鍵および
署名の管理
Bank A
Browser
Wallet
App
Bitcoin
Core
MySQL
TTP
（仲介者）
Browser
取引App
Bitcoin
Core
MySQL
Open Asset
Explorer
neo4j
Bank B
Browser
Wallet
App
Bitcoin
Core
MySQL
ユーザー操作
APIによる接続

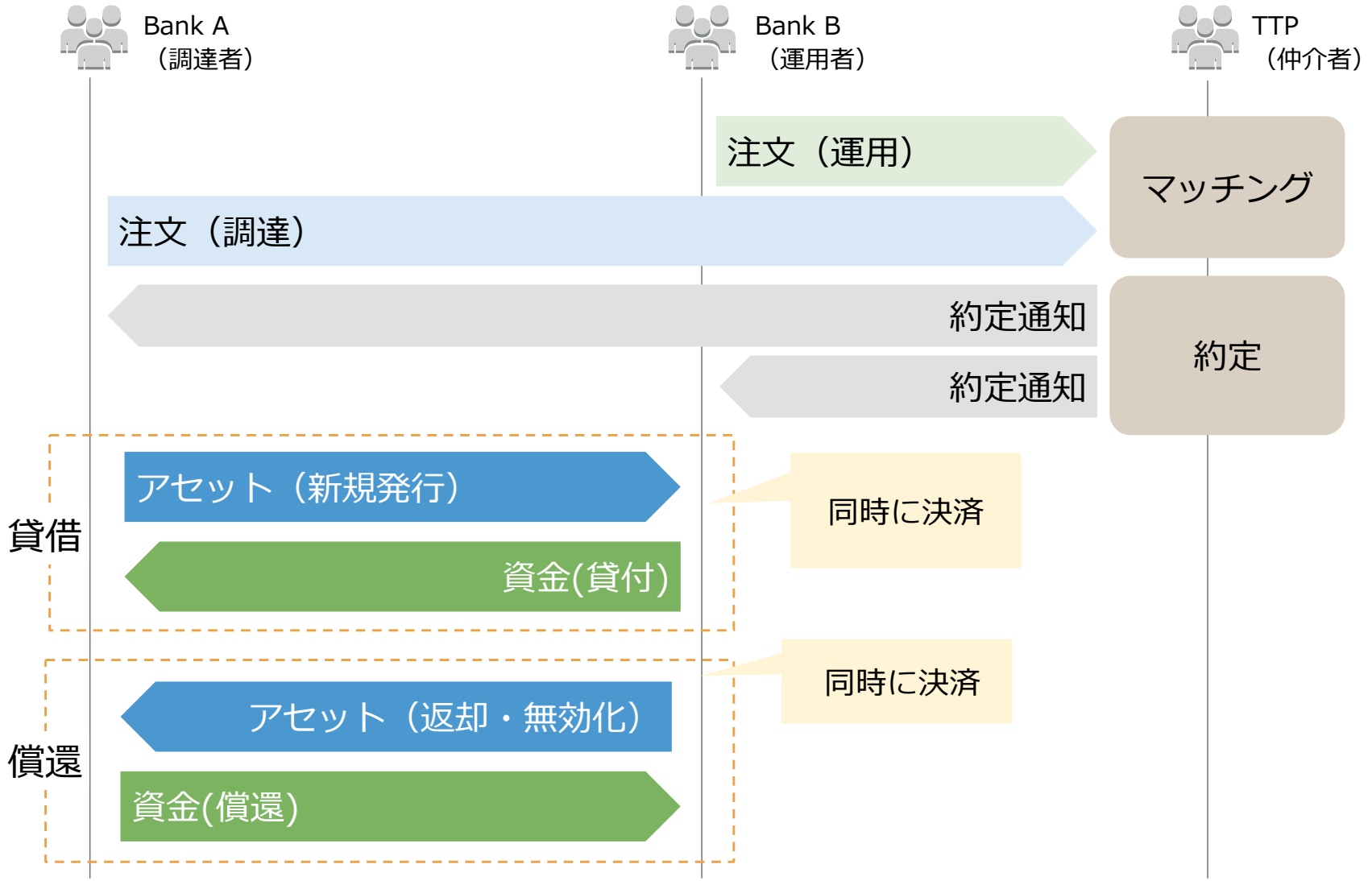
資金貸借の表現方法

- Open Assets Protocolに基づいたアセットを利用
- 貸借を以下の交換と考える
  - 運用者が保有する暗号通貨（Bitcoin）
  - 調達者が発行した（もしくは保有する）アセット
- アセット化によるメリットや課題を検討

Open Assets Protocol

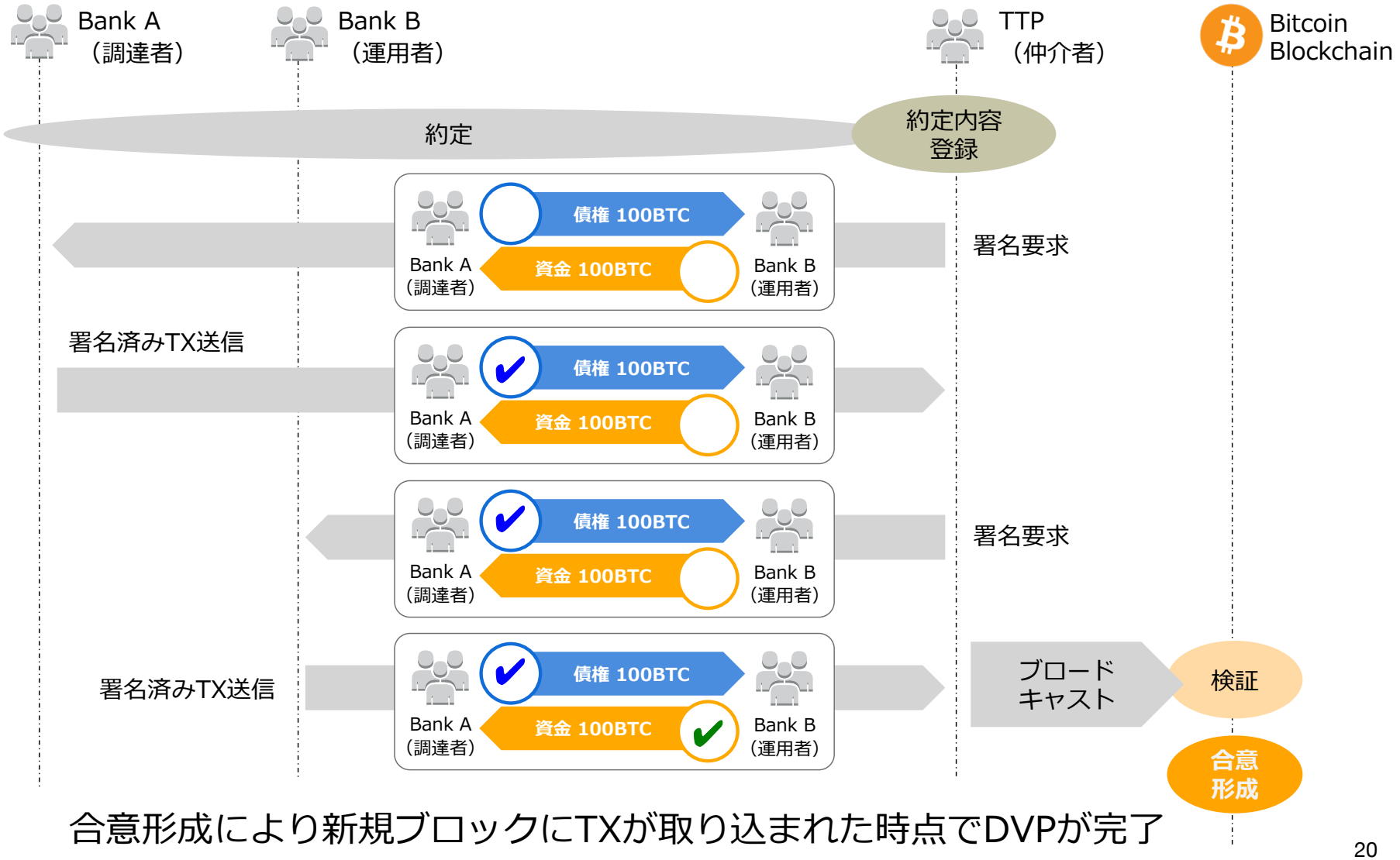
- Bitcoinブロックチェーン上で独自の価値を発行・流通させることができる、Colored Coinと呼ばれる技術の一つ
- ブロックチェーン上には価値の数量的な取引のみを記録し、その価値の定義等については外部に記録
- Ruby言語での実装についてはハウ社が提供している（オープンソース）

アセットの流れ


Bank A
（調達者）
Bank B
（運用者）
TTP
（仲介者）
注文（運用）
マッチング
注文（調達）
約定通知
約定
約定通知
貸借
アセット（新規発行）
同時に決済
資金(貸付)
償還
同時に決済
アセット（返却・無効化）
資金(償還)

東京短資株式会社 THE TOKYO TANSHI CO.,LTD. × HAW International Inc.

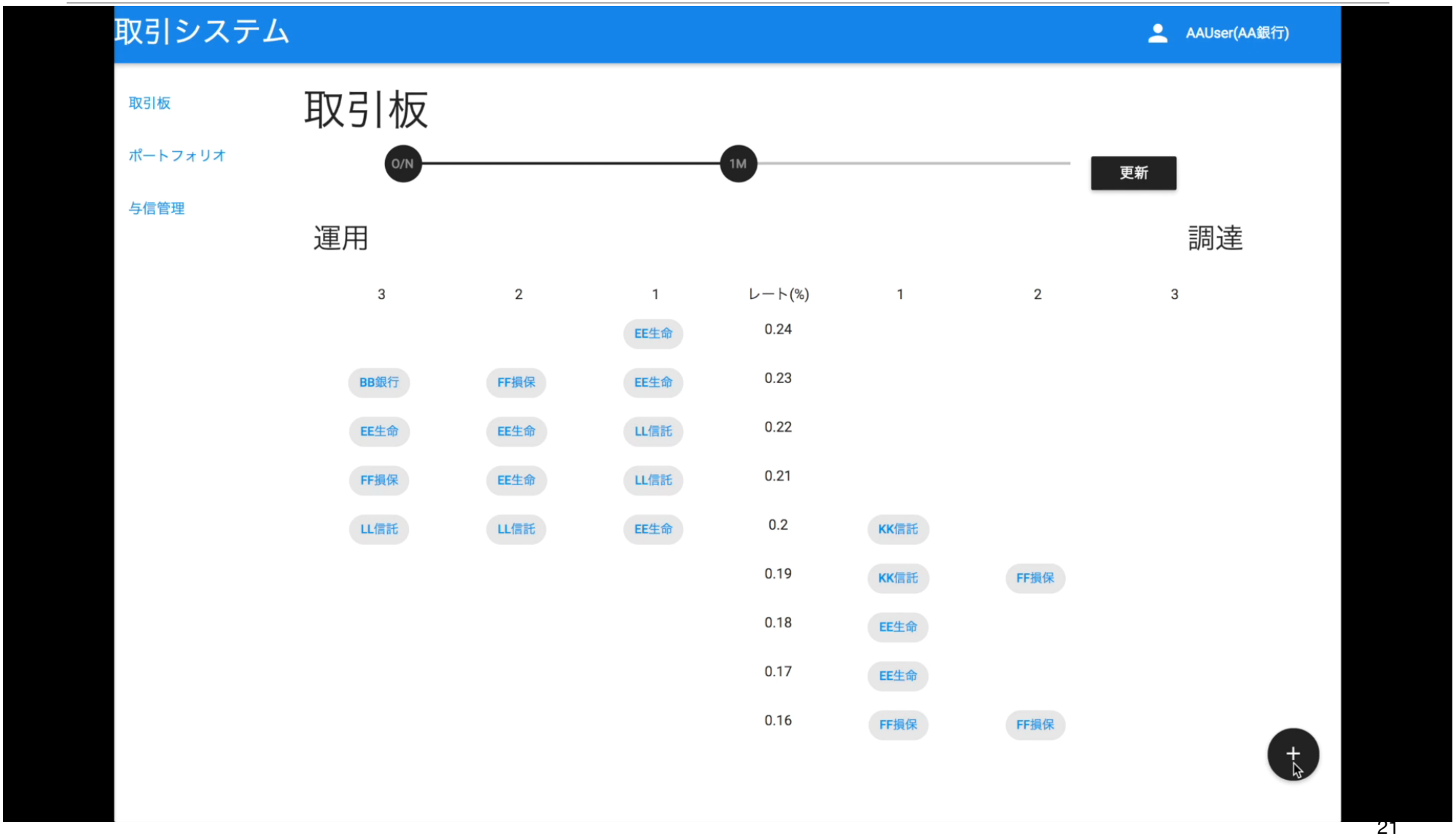
DVPの実現



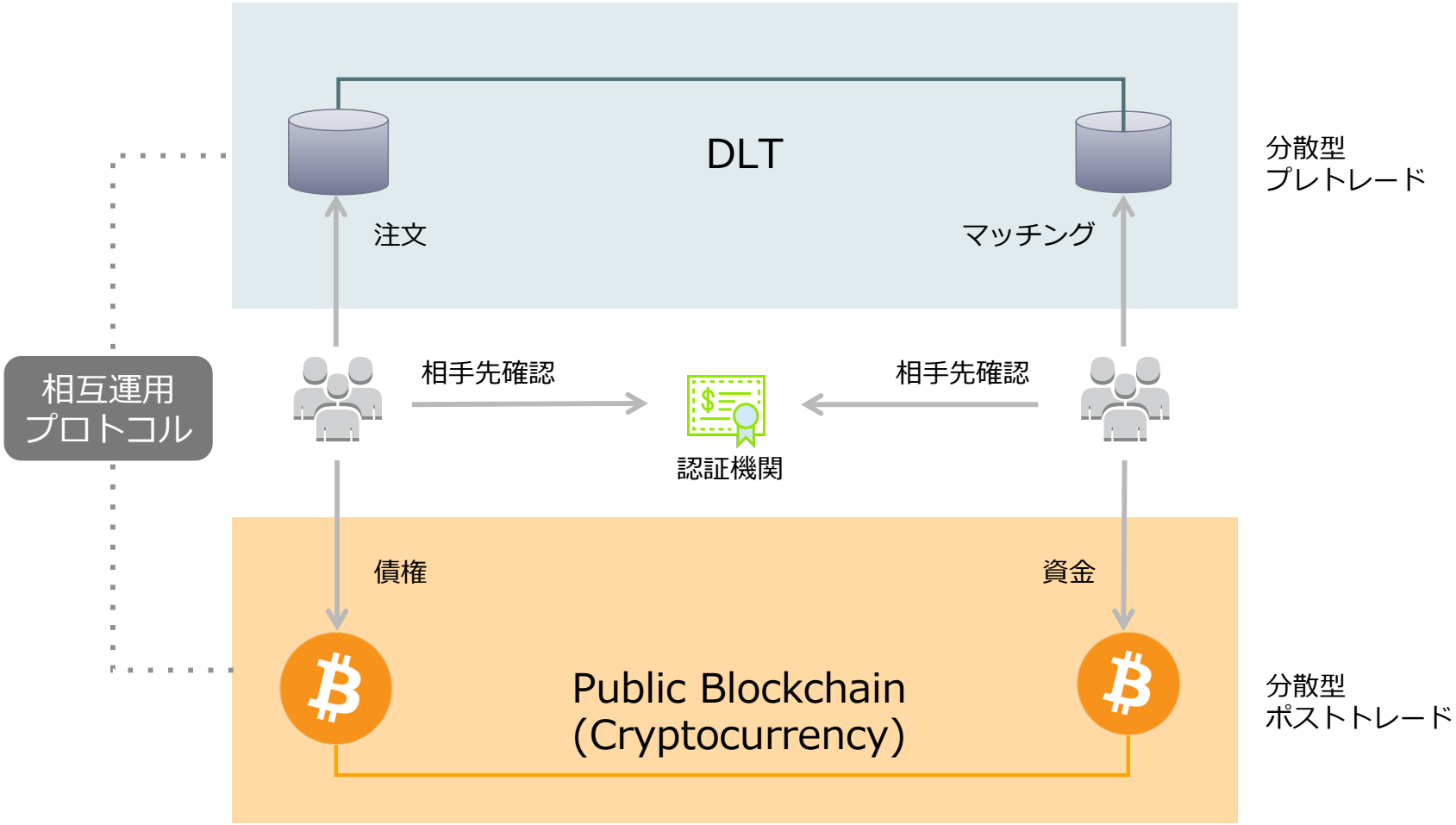
合意形成により新規ブロックにTXが取り込まれた時点でDVPが完了

東京短資株式会社 THE TOKYO TANSHI CO.,LTD. × HAW International Inc.

デモ



分散型市場の可能性


DLT
注文
マッチング
分散型
プレトレード
相互運用
プロトコル
相手先確認
相手先確認
認証機関
債権
資金
Public Blockchain
(Cryptocurrency)
分散型
ポストトレード

今後目指す姿

信頼点 / 行動主体	参加者自身	中央管理者	コンソーシアム型 分散台帳	パブリック Blockchain	パブリック Blockchain上のLayer
管理者/仲介者		OnBoarding			
参加者	口座維持管理	注文 →	注文	約定 支払い指図	債権の移転(発生/分割/償還)
		取引板 →	取引板		
		マッチング →	マッチング		
Bitcoinマイナー (PoW)				通貨の信頼性 資金・債権決済 (DVP)	

まとめ

**Bitcoinのプロトコルに沿うことで、現状において最もトラストレス
かつセキュアな権利の移転（発生・譲渡・償還）を実現**

- 可能性の示唆
  - 世界中のマネーマーケットが繋がる
- 今後の論点
  - 法定通貨とのリンク
  - Bitcoinの機能を補完するプロトコルやサービス
    - Altcoin, Off-chain, Side-chain, Overlay（Layer 2） etc.
  - Bitcoinのコンセプトを補完するモデル
    - 信頼できる第三者モデル、プライベートチェーン etc.
  - オープンな研究開発