日本銀行 CBDC Forum WG4 プレゼンテーション

UTXOモデルの特徴理解

SBI R3 Japan 株式会社

前半

生永 雄輔

2024/1/30

Exective Summery

- このプレゼンテーションでは、日本銀行 CBDCフォーラムの参加者の皆様に向けて、UTXOモデルに対する弊社の理解をご紹介します。プレゼンテーションは以下のような構成です。
- まず、他のモデルと対比した形で、UTXOモデルのご紹介をいたします。対比するデータモデルとしてバランスモデルとトークンモデルを紹介いたします。お金の所有を表現する際に、これまで、「持ち主を主語にする（バランスモデル）」のか、はたまた硬貨や紙幣と同様に「お金を主語にする（トークンモデル）」の２択だったのですが、UTXOモデルはそこに新しい考え方を導入したデータモデルであるということを説明します。
- つづいて、UTXOモデルの具体的な特徴である、同時実行の容易さとプライバシー確保の容易さを説明します。特徴理解のための簡素な例を示すと同時に、実例を紹介いたします。
- 最後に、弊社が販売している分散型台帳基盤Cordaを例に、UTXOモデルを決済領域に活用した時に必要なコンセンサスモデルについて説明させていただきます。この議論は次回に続くものとなります。

SBI R3 Japan

SBI R3 Japanからのアジェンダ

前半（本日）＝技術的なSession

✓**UTXOに対する弊社理解**を共有

後半＝将来に向けたSession

✓決済の長期的変化に対する弊社仮説

✓**将来ビジョンの中で、UTXOの適用可能性**をマッピング

SBI R3 Japan

前半アジェンダ

1. 自己紹介
2. SBI R3Japanからのアジェンダ
3. UTXOモデルに対する弊社の理解
   1. 他モデルとの比較
   2. 同時実行／シャーディング
   3. プライバシー
4. UTXOを前提とした決済コンセンサス

SBI R3 Japan

SBI r3 Japan

他モデルとの対比

バランス／トークン／UTXO

お金の所有を表す三つのモデル

1.バランスモデル

2.トークンモデル

3.UTXOモデル

SBI R3 Japan

典型的なお金のデータ

持ち主	金額
Aさんが	100円持っている
Bさんが	1000円持っている
Cさんが	10000円持っている
Dさんが	100000円持っている

SBI R3 Japan

バランスモデル

持ち主＝主語	金額
Aさん	100円持っている
Bさん	1000円持っている
Cさん	10000円持っている
Dさん	100000円持っている

バランスモデル

持ち主＝主語	金額
Aさん	100円持っている
Bさん	1000円持っている
Cさん	10000円持っている
Dさん	100000円持っている
～	
Aさん	200円持っている

典型的なお金のデータ

持ち主	金額
Aさんが	100円持っている
Bさんが	1000円持っている
Cさんが	10000円持っている
Dさんが	100000円持っている

トークンモデル

持ち主	金額＝主語
Aさんの持ち物	100円**玉**（100-1）は,
Bさんの持ち物	1000円**札**（1000-1）は,
Cさんの持ち物	10000円**札**（10000-1)は,
Dさんの持ち物	100000円**札**（100000-1)は,

現実のお札に似ていて、**全てのお金にシリアル番号が振られている必要**がある。

SBI R3 Japan

トークンモデル

持ち主が述語	金額＝主語
Aさんの持ち物	100円玉（100-1）
Aさんの持ち物	100円玉（100-2）
Aさんの持ち物	10000円札（10000-2)
Aさんの持ち物	10000円札（100000-3)

→ Aさんは20200円持っていることを表現

SBI R3 Japan

トークンモデル

持ち主が述語	金額＝主語
Aさんの持ち物	100円玉（100-1）
Aさんの持ち物	100円玉（100-2）
Aさんの持ち物	10000円札（10000-2)
Aさんの持ち物	10000円札（100000-3)
～	
Bさんの持ち物	100円玉（100-1）

同じシリアルのついたお金が二つあるのはNG

典型的なお金のデータ

持ち主	金額
Aさんが	100円持っている
Bさんが	1000円持っている
Cさんが	10000円持っている
Dさんが	100000円持っている

SBI R3 Japan

UTXOモデル

持ち主	金額
Aさんが	100円持っている
Bさんが	1000円持っている
Cさんが	10000円持っている
Dさんが	100000円持っている

UTXOモデル

持ち主	金額
Aさんが	100円持っている
Bさんが	1000円持っている
Cさんが	10000円持っている
Dさんが	100000円持っている
Aさんが	1000円持っている
Bさんが	100円持っている

→ 主語を指定しない※ので一番柔軟

※個別の取引を主語（主キー）とし、ブロック間の順序性を取引単位でチェックするのがUTXOモデルという理解

UTXOモデル

持ち主	金額
Aさんが	100円持っている
Bさんが	1000円持っている
Cさんが	10000円持っている
Dさんが	100000円持っている
Aさんが	1000円持っている
Bさんが	100円持っている

これでAさんが1100円持っていることを表現
（100+1000）

SBI R3 Japan

まとめー３モデル対比

モデル名	長所	短所
バランスモデル 	• **金額によってデータ量が増えない** • 主体別残高を計算する必要がない • エンジニアにとって理解が容易	• 二人と同時に取引できない • 取引相手に残高が見える
トークンモデル 	• 複数の人と同時に取引できる • 取引相手に自分の残高が見えない • ユーザーにとって理解が容易	• **金額が増えるとデータ量が増える** • 主体別残高計算が大変
UTXOモデル 	• **設計次第でバランスモデルにもトークンモデルにも変化可能** • データ量の圧縮可能 • 主体別残高の秘匿可能 • 複数人の同時取引可能	• 柔軟な為、理解が難しい

SBI R3 Japan

同時実行とシャーディング

パフォーマンス実現に対する取組

①同時実行　Pt. 1/4

持ち主	金額
Aさんが 	100円持っている → Bさんへ渡す
Bさんが	1000円持っている
Cさんが 	10000円持っている → Dさんへ渡す
Dさんが	100000円持っている
Aさんが	1000円持っている
Bさんが	100円持っている

SBI R3 Japan

①同時実行　Pt. 2/4

持ち主	金額
Aさんが	100円持っている
Bさんが	1000円持っている
Cさんが	10000円持っている
Dさんが	100000円持っている
Aさんが	1000円持っている
Bさんが	100円持っている

Bさんへ渡す

Dさんへ渡す

SBI R3 Japan

①同時実行 Pt. 3/4

持ち主	金額
Aさんが 	100円持っている
Bさんが	1000円持っている
Cさんが 	10000円持っている
Dさんが	100000円持っている
Aさんが	1000円持っている
Bさんが	100円持っている

①同時実行 Pt. 4/4

持ち主	金額
Aさんが	100円持っている
Bさんが	1000円持っている
Cさんが	10000円持っている
Dさんが	100000円持っている
Aさんが	1000円持っている
Bさんが	100円持っている

Bさんへ300円

Dさんへ渡す

SBI R3 Japan

【参考】Project Hamiltonに対する当社理解

- Phase1 
  - ✓ **UTXOモデル**による移転取引の高速化
  - ✓ Phase2を見据えて2フェーズコミット実装

- Phase2   
  - ✓ スマートコントラクト分散実行
  - ✓ **データモデル依存は無い**
    - ➢ UTXO／トークンモデルに基づく価値の移転をPhase2実装上で実現するには2フェーズコミットが必要

SBI R3 Japan

②シャーディング

持ち主	金額	使える地域
Aさんが	100円持っている	大阪市
Bさんが	1000円持っている	東京都中央区
Cさんが	10000円持っている	大阪市
Dさんが	100000円持っている	大阪市
Aさんが	1000円持っている	東京都中央区
Bさんが	100円持っている	大阪市

②シャーディング

持ち主	金額	使える地域
Aさんが	100円持っている	大阪市
Bさんが	1000円持っている	東京都中央区
Cさんが	10000円持っている	大阪市
Dさんが	100000円持っている	大阪市
Aさんが	1000円持っている	東京都中央区
Bさんが	100円持っている	大阪市

大阪市内の取引と、中央区内の取引は**独立して管理**可能
但し、ネットワーク側管理の工夫は必要

SBI R3 Japan

金融DXによる侵食①株のT+1決済

DTCC　Project Ion

段階	POC　Pilot　Production
ソリューション名	PROJECT ION
ユースケース	公開株の決済期間短縮
開発会社	DTCC（米国証券保管振替機構）
ユーザー	証券会社、銀行、清算機関等
国	米国
背景、課題	• DTCCは2020年に2.3兆ドルの証券決済処理を実施。 • 大量の証券決済(1億件/日、6500件/秒)を分散台帳上で処理することで、**証券決済期間の短縮**を目指している
特徴、利点	• 実証実験にて上記大量決済を**分散台帳上で処理可能なことを確認済** • 既存の株式決済基盤と並行運用中(2022年8月時点で1日平均10万件、ピーク時は16万件)

サービス概要

ASSET DIGITIZATION
顧客がシステム間で資産をシームレスに移動させて決済する
NETTING
リアルタイムネッティングにより、顧客持高を最適化する
INTERFACES
後方互換性を確保し、簡単に採用可能にする

市場のニーズ
機関投資家向けに、決済リスク削減による米国市場競争力強化
・ 2021年1月にゲームストップ株問題
・ 2008年9月 リーマンショック（株ではないが同種の事例）

Next Step	• 証券の決済期間短縮（T+2 ⇒ T+1、T+0）、決済リスクの低減 • 金融機関の現行決済システムとの接続 • **中央清算機関との連携**も含めた機能拡張を予定

SBI R3 Japan

⇒ 株の銘柄ごとに独立して管理（ネットワークは単一）

SBI R3 Japan

プライバシー

プライバシーの定義

人	行動／性質
Aさんが	アイドルの大ファン
Bさんが	日本国籍
Cさんが	院卒
Dさんが	阪神ファン
Aさんが	熱心な仏教徒
Bさんが	宝くじに当たった

SBI R3 Japan

プライバシーの定義

人	行動／属性
Aさんが	アイドルの大ファン
Bさんが	日本国籍
Cさんが	院卒
Dさんが	阪神ファン
Aさんが	熱心な仏教徒
Bさんが	宝くじに当たった

人が特定できても、
行動／属性が判別できない

SBI R3 Japan

UTXOモデルによるプライバシー

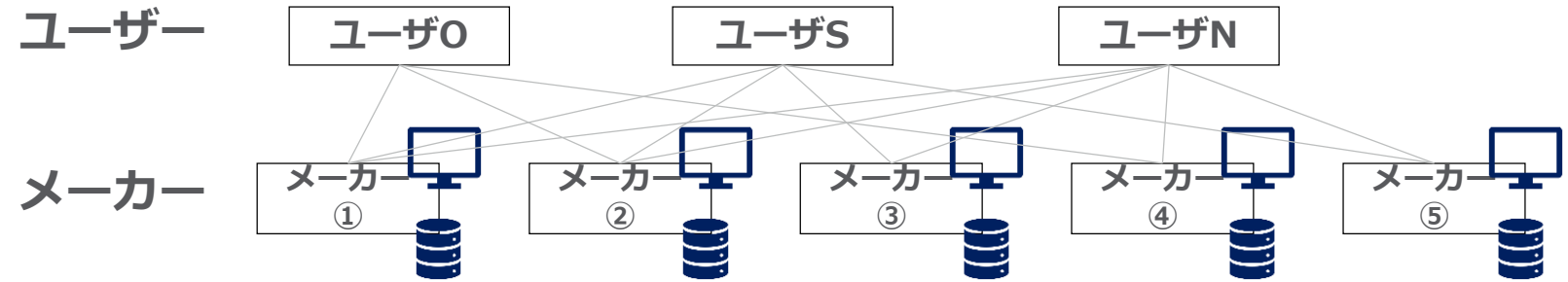
持ち主	金額
Aさんが	100円持っている
Bさんが	1000円持っている
Cさんが	10000円持っている
Dさんが	100000円持っている
Aさんが	1000円持っている
Bさんが	100円持っている

- Aさんが「全部でいくら持っている」という情報は隠蔽可能＝プライバシーの確保が容易

SBI R3 Japan

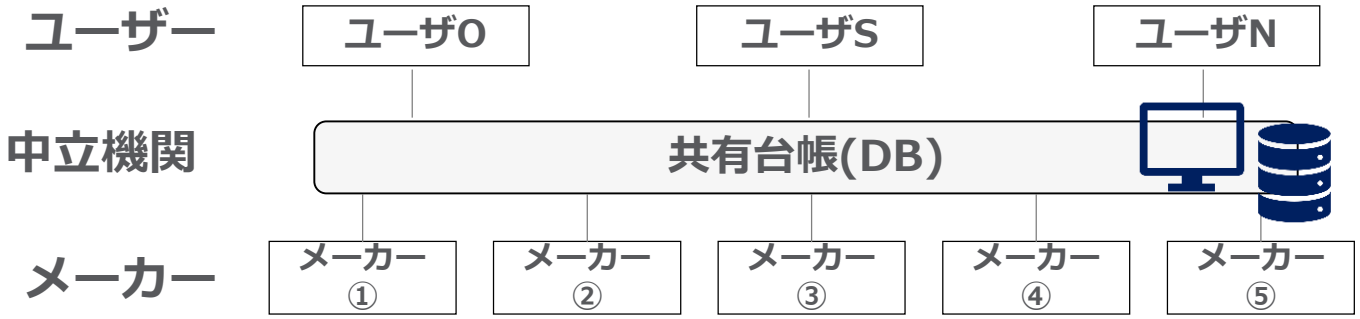
【匿名事例】実業系の要求

サイロ化



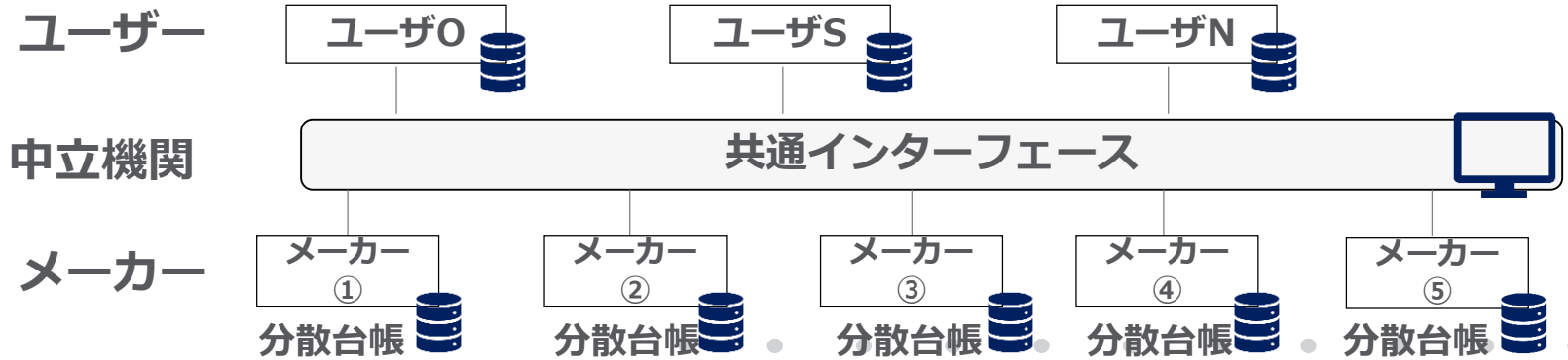
- × ユーザー視点で煩雑
- × 接続多、高コスト
- × メーカー側協調難

一元化



- ○ ユーザー視点で簡易
- × メーカーは今まで集めたデータの所有権を放棄
- × メーカー側合意形成難

分散台帳化



- ○ ユーザー視点で簡易
- ○ メーカーは今まで集めたデータの所有権を維持
- ○ 業界合意形成容易

【参考】匿名性

人	行動／性質
Aさんが	アイドルの大ファン
Bさんが	日本国籍
Cさんが	院卒
Dさんが	阪神ファン
Aさんが	熱心な仏教徒
Bさんが	宝くじに当たった

SBI R3 Japan

SBI R3 Japan

コンセンサス

分散システムにおけるコンセンサス

- システムの状態変化を何らかのルールに基づいてネットワーク全体で承認する行為

（Ex）

① ルールベース：特定の条件を満たすと承認したとみなす。（PoW、PoS）
② 主体ベース　：特定者が承認することで承認したとみなす。（PoA）
③ ①×□②の組み合わせ

決済にコンセンサスが必要？

・当事者がOKと言っているのになぜ第三者の認証が必要なの？

・当事者がOKと言っている取引を第三者がNGを出せるということ？

SBI R3 Japan

決済に必要なコンセンサスの分離

関係者コンセンサス

・決済内容の確認

ユニークネスコンセンサス

・決済通貨の複製が無い事の確認
（偽札NG / 通貨量不変）

※総流通量に対するコンセンサスも必要だが、この議論は後半で

SBI R3 Japan

関係者コンセンサス＝決済内容合意

- 電子署名技術（公開鍵暗号技術）だけで実現可能。

- 電子署名技術におけるRoot Of Trust課題に対する事前合意が必要

  ☑☐ビジネス：KYC／取引時確認

  ☑☐技術：X509／VC

- 合意の「存在証明」はユニークネスコンセンサスの役割

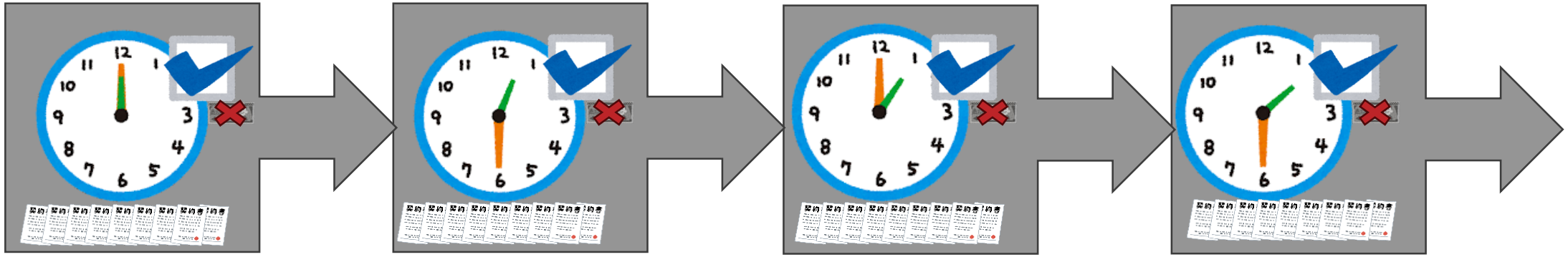
SBI R3 Japan

ユニークネスコンセンサス＝複製防止

- ネットワーク（エコシステム）参加者全体で偽札を許容しない仕組み。
  - ✓ 解決策①**離散的な時点ごとの整合性**を確認する。
  - ✓ 解決策②**取引毎に整合性**を確認する

時点整合性：ユニークネスコンセンサス

✓解決策①離散的な時点（ブロック）を設定し、**時点ごとの整合性**を確認する。



いいところ○

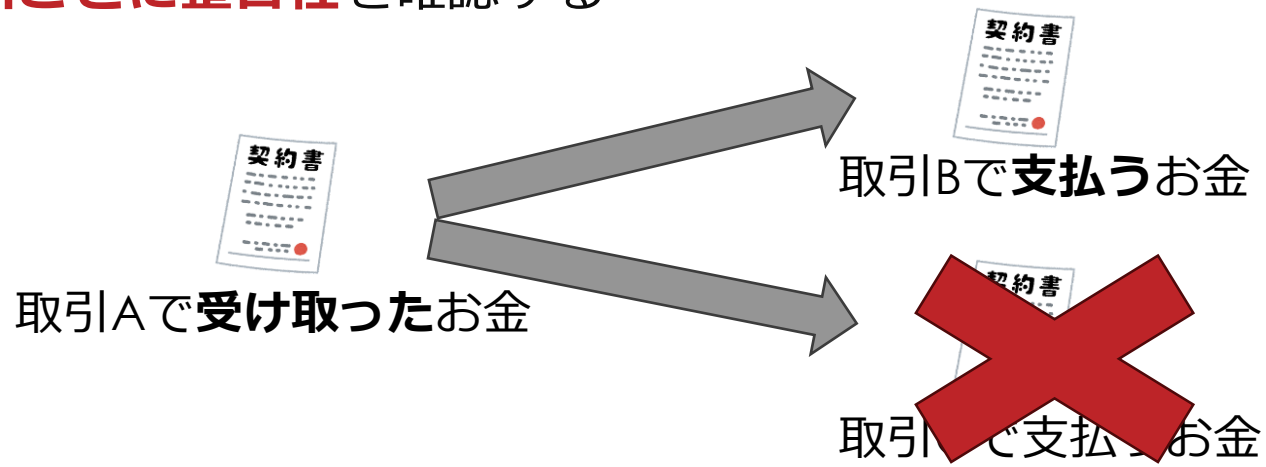
・ブロックが単位となるので、分散系の複雑さに制約を持たせることができる。

悪いところ✕

・ブロック内に無関係な決済データを複数含めるため、実現可能な要件に制約がかかる。

取引毎整合性：ユニークネスコンセンサス

✓解決策②**取引ごとに整合性**を確認する




いいところ○

・柔軟性が高く多様な要件（プライバシー、可用性、パフォーマンス）を実現可能

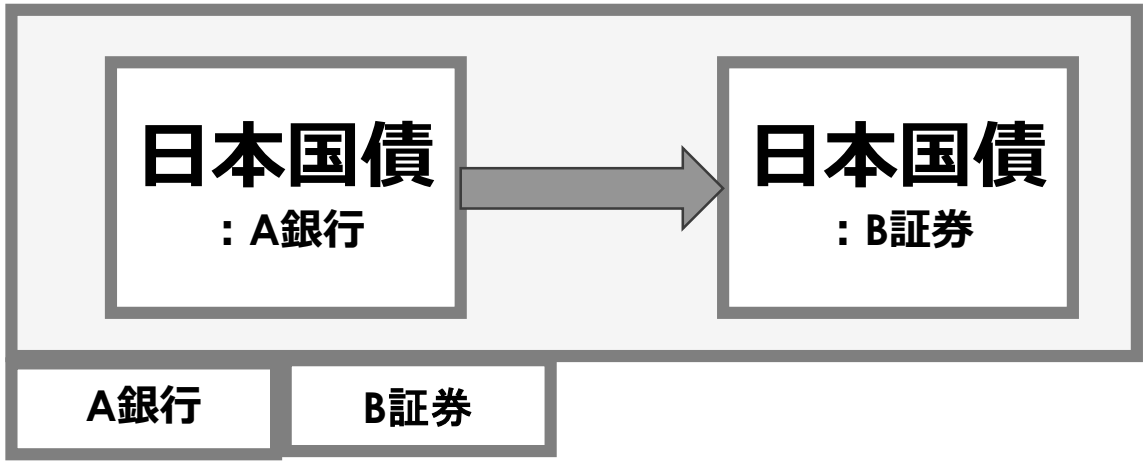

悪いところ✕

・分散系の複雑さに制約がない為、分散度のコントロールが難しい。

SBI R3 Japan

UTXO ×□ 関係者コンセンサス

in Corda

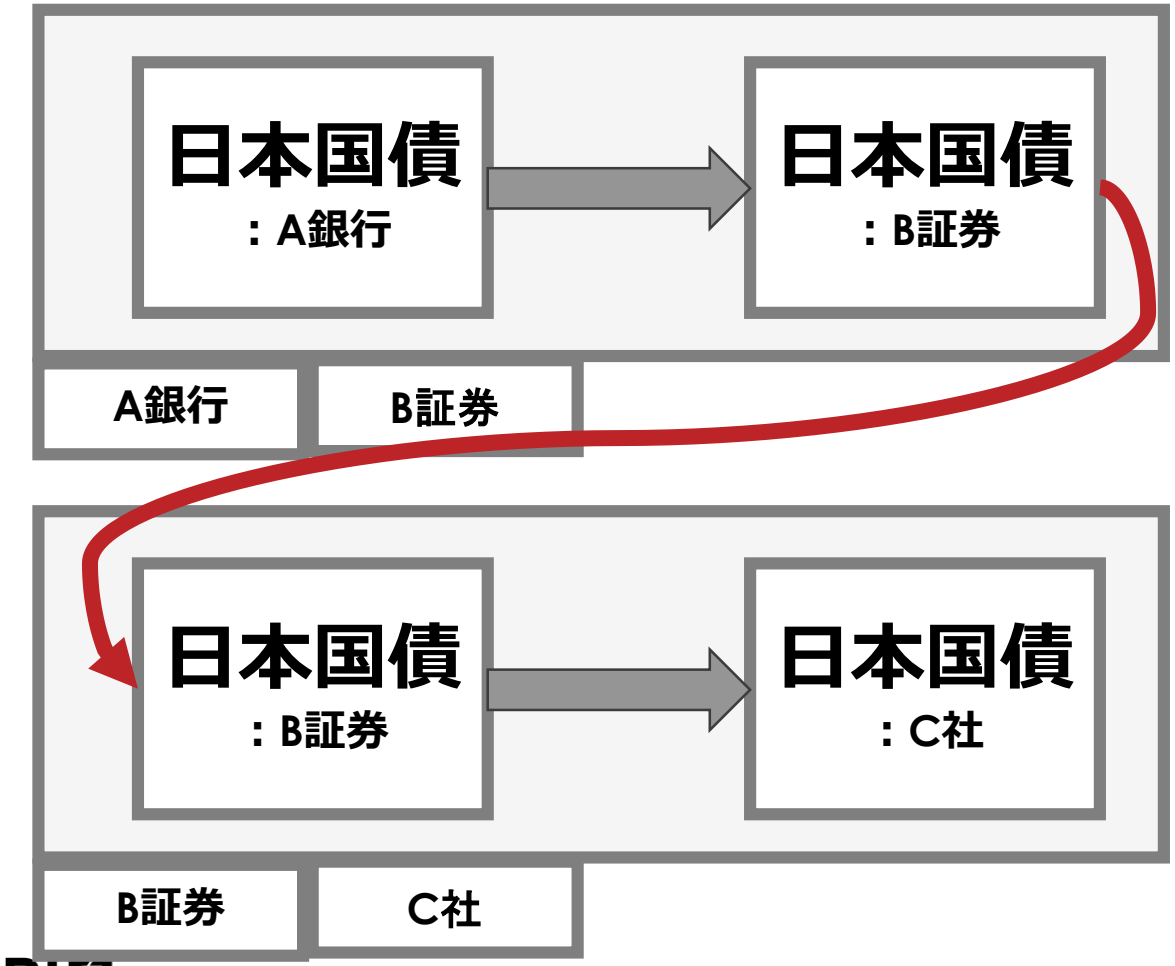


決済内容
「日本国債をA銀行からB証券に渡す」
に対して
「A銀行とB証券の署名をつける」
ことでコンセンサスを確認する。

SBI R3 Japan

UTXO ×□ 関係者コンセンサス（pt1）

in Corda



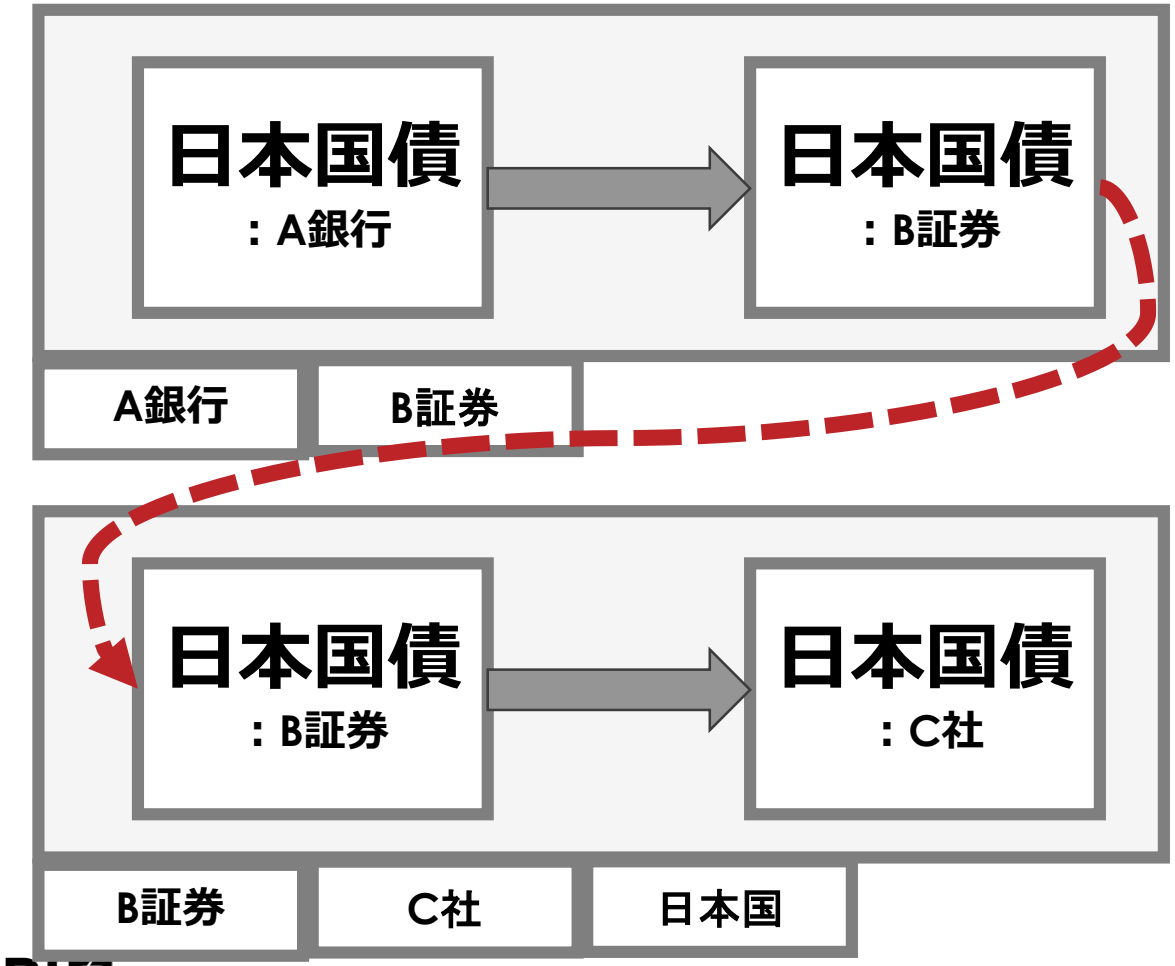
決済内容
「日本国債をA銀行からB証券に渡す」
に対して
「A銀行とB証券の署名をつける」
ことでコンセンサスを確認する。

決済内容
「日本国債をB証券からC社に渡す」
に対して
「B証券とC社の署名をつける」
ことでコンセンサスを確認する。
＋
B/Cは、A→Bのやりとりも確認する必要がある。

SBI R3 Japan

UTXO ×□ 関係者コンセンサス（pt2）

in Corda



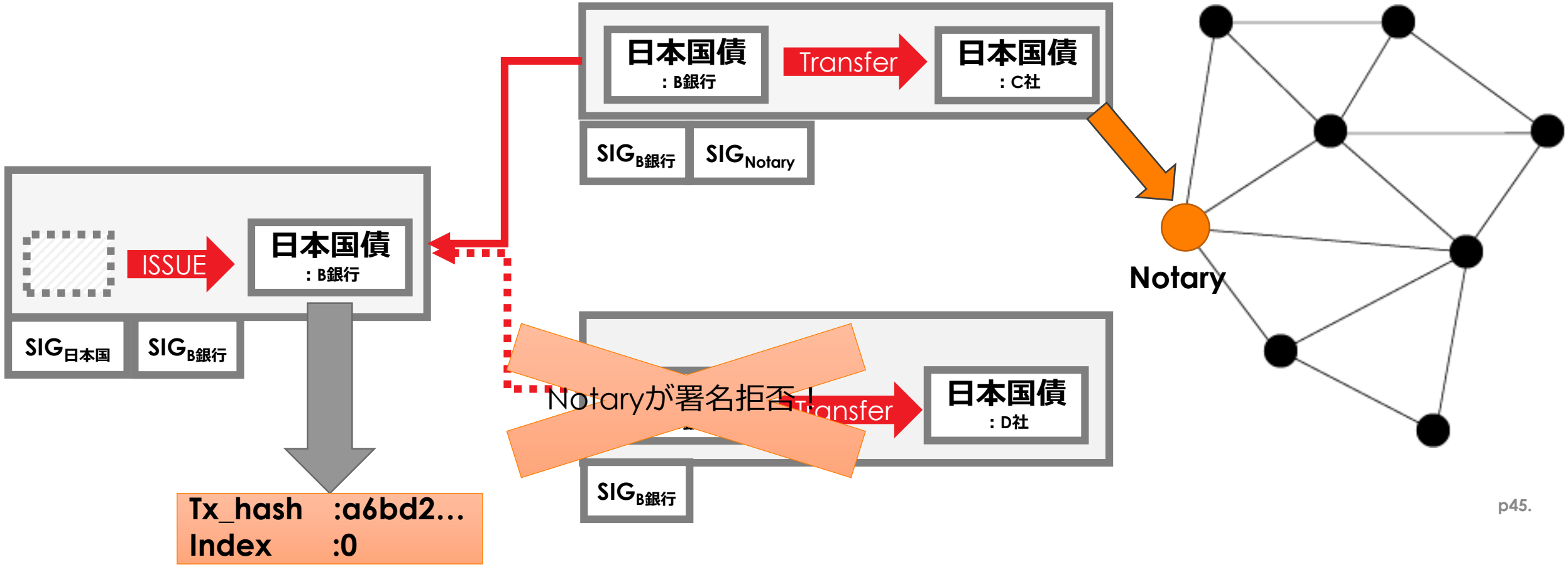
決済内容
「日本国債をA銀行からB証券に渡す」
に対して
「A銀行とB証券の署名をつける」
ことでコンセンサスを確認する。

決済内容
「日本国債をB証券からC社に渡す」
に対して
「B証券とC社の署名をつける」
ことでコンセンサスを確認する。
＋
~~B/Cは、A→Bのやりとりも確認する必要がある。~~
日本国が署名するというやり方もある。

SBI R3 Japan

UTXO ×□ ユニークネスコンセンサス

in Corda

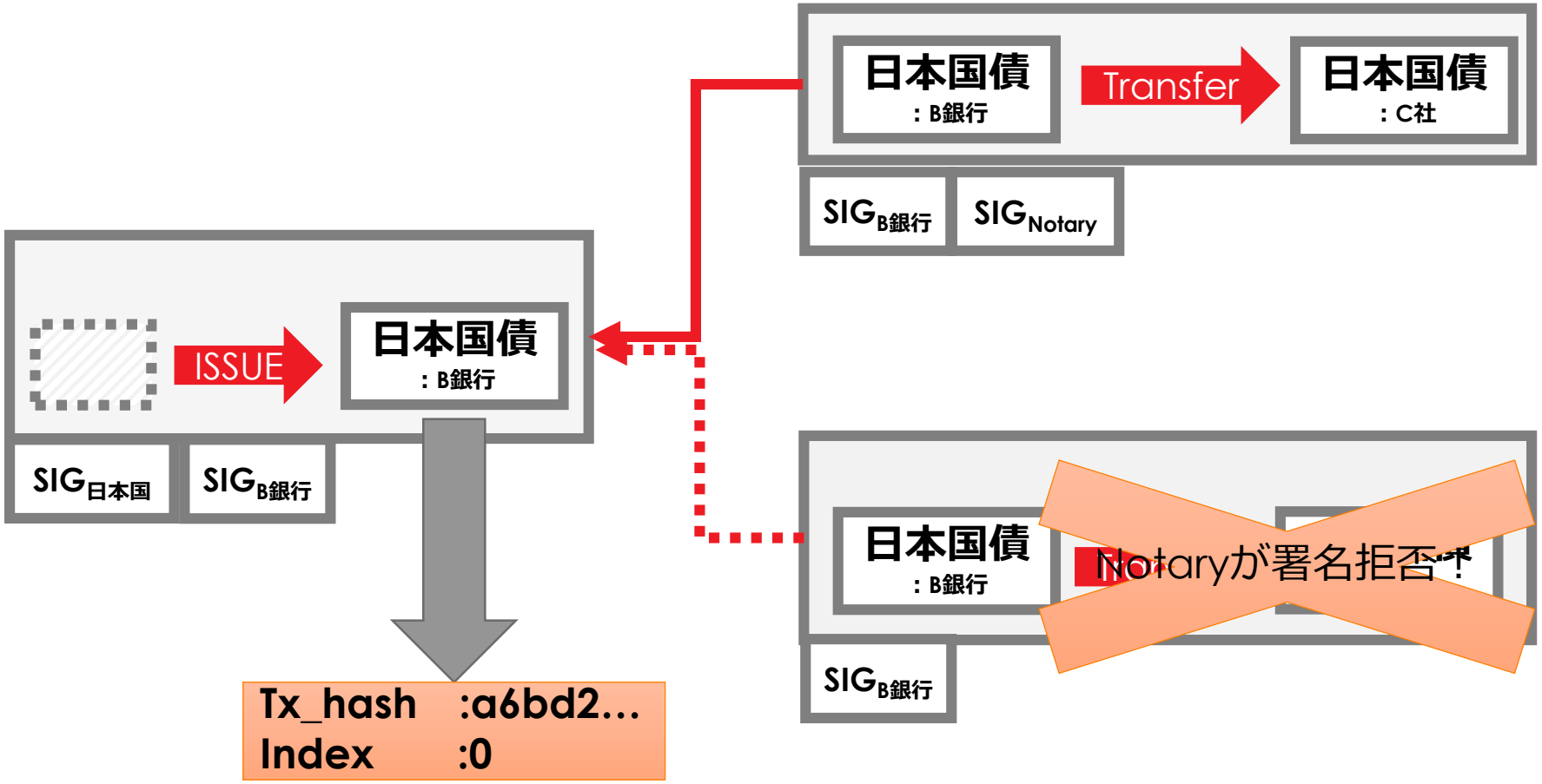


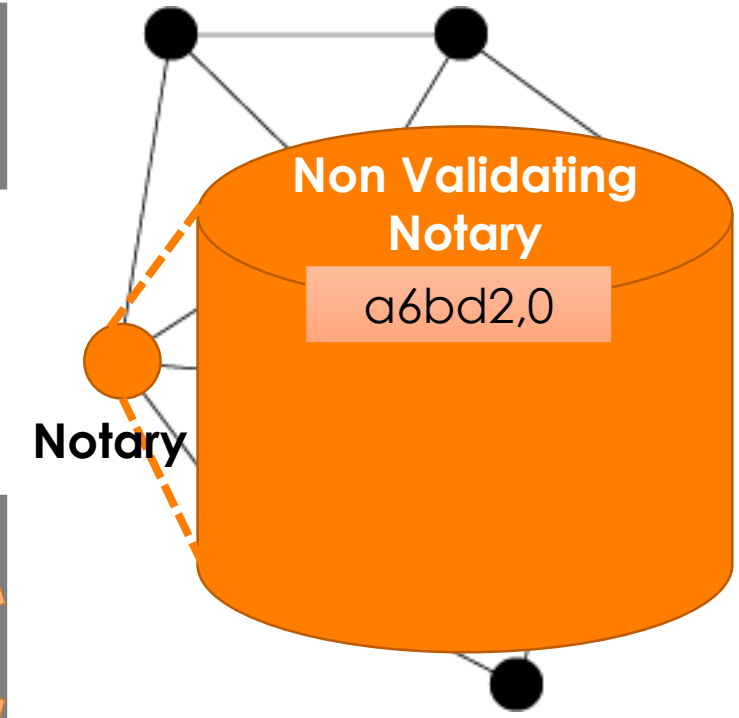
SBI R3 Japan

p45.

UTXO ×□ ユニークネスコンセンサス

in Corda





SBI R3 Japan

p46.

まとめ（前半）

- 弊社の理解するUTXO
  - ✓同時実行
  - ✓プライバシー
  - ✓コンセンサス
    - ➢決済に必要なコンセンサス

※Hashチェーン技術は限定的活用

SBI R3 Japan

後半アジェンダ（仮）

変更の可能性が（大いに）あります

- CBDCに必要なコンセンサス
- CBDCを中心とした二十年後の決済
- UTXOモデル活用領域の検討

SBI R3 Japan

SBI R3 Japan

【参考】匿名性とプライバシーの定義

匿名性とプライバシーの定義

人	行動／性質
Aさんが	100円持っている
Bさんが	1000円持っている
Cさんが	10000円持っている
Dさんが	100000円持っている
Aさんが	1000円持っている
Bさんが	100円持っている

SBI R3 Japan

匿名性とプライバシーの定義

人	行動／性質
Aさんが	アイドルの大ファン
Bさんが	日本国籍
Cさんが	院卒
Dさんが	阪神ファン
Aさんが	熱心な仏教徒
Bさんが	宝くじに当たった

SBI R3 Japan

プライバシー

人	行動／性質
Aさんが	アイドルの大ファン
Bさんが	日本国籍
Cさんが	院卒
Dさんが	阪神ファン
Aさんが	熱心な仏教徒
Bさんが	宝くじに当たった

どんな人か
わからない

SBI R3 Japan

プライバシー

人	行動／性質
Aさんが	アイドルの大ファン
Bさんが	日本国籍
Cさんが	院卒
Dさんが	阪神ファン
Aさんが	熱心な仏教徒
Bさんが	宝くじに当たった

どんな人か
わからない

SBI R3 Japan

匿名性

人	行動／性質
Aさんが	アイドルの大ファン
Bさんが	日本国籍
Cさんが	院卒
Dさんが	阪神ファン
Aさんが	熱心な仏教徒
Bさんが	宝くじに当たった

行動主体がわからない。

SBI R3 Japan

匿名性

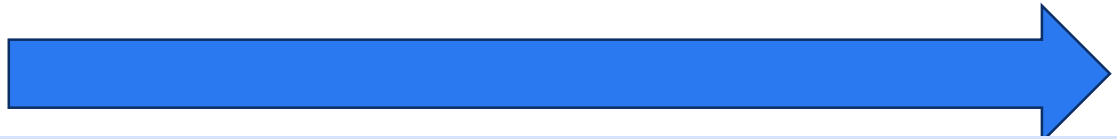
人	行動／性質
Aさんが	アイドルの大ファン
Bさんが	日本国籍
Cさんが	院卒
Dさんが	阪神ファン
Aさんが	熱心な仏教徒
Bさんが	宝くじに当たった

行動主体がわからない。

SBI R3 Japan

匿名性・プライバシー

人	行動／性質
Bさんが	日本国籍
Bさんが	宝くじに当たった
Bさんが	X銀行に口座を持っている



プライバシーの実現は法人／個人いずれに対しても必要な要件

匿名性が高いことは規制当局としてはUnfavor

SBI R3 Japan