# 2 日本のFinTechでの活用

## コインチェック社の概要

**ライセンスの状況**：２０１７年９月末までに仮想通貨交換業ライセンスを申請済み（審査中）　みなし業者として運営中

**会員数**　：推定２００万ユーザー超
**月間取扱高**　：約４兆円（公称）（2018年12月現物取引高として国内最大）

**取扱い仮想通貨銘柄数**　：　国内最多（13コイン）


**特徴**
- ✓ ユーザーフレンドリー
- ✓ ライトユーザーが多い
- ✓ スマートフォンから取引できる
- ✓ 即時入出金に対応など利便性が高いところが人気

**今回の「ＮＥＭ」に限らず、**
**すべての仮想通貨はその特性上、秘密鍵が流出してしまうと**
**システムに侵入する必要なく送金ができてしまいます！**

▼

# 秘密鍵をいかに厳重に
# 管理することに問題は集約される

## 秘密鍵の保管場所は適切であったか？

- ✓ **PCやスマートフォンのファイルシステム上**
  - ⇒ インターネットに接続された環境のホットウォレット
  - ⇒ ファイヤーウォール設置の有無により安全評価は異なる
  - ⇒ インターネットから隔離されたコールドウォレット
- ✓ **PCやスマートフォン内のセキュアエレメント**
  - ⇒ OSの堅牢性に依存
- ✓ **USBに記録して保管**
  - ⇒ 安全性に疑問
- ✓ **紙に印刷して保管（ペーパーウォレット）**
  - ⇒ 印刷機のメモリ内からの漏洩、印刷機の動作周波数等からの解析可能性
- ✓ **仮想通貨専用のハードウェアウォレット**
  - ⇒ 一般には安全と考えられるが、耐タンパ性に関する認証等、安全基準は未確定
  - ⇒ **比較的新しい暗号・署名アルゴリズムへの対応は遅くなる**
- ✓ **業務用のハードウェアセキュリティモジュール（HSM）**
  - ⇒ 認証基準があるが
    **最新技術を利用する一部仮想通貨の暗号や署名の各アルゴリズムには対応していない**

技術的困難性の一要因

## 秘密鍵の保管場所は適切であったか？

Ed25519 SHA-3

- ✓ **仮想通貨専用のハードウェアウォレット**
  - ⇒ 一般には安全と考えられるが、耐タンパ性に関する認証等、安全基準は未確定
  - ⇒ **比較的新しい暗号・署名アルゴリズムへの対応は遅くなる**




**個人ユースを想定しているため、**
**複数人で署名を行うマルチシグネチャ業務を想定していない**

※NEMに対応したハードウェアウォレットは１２月下旬に登場したばかり

## 秘密鍵の保管場所は適切であったか？

**FIPS (Federal Information Processing Standard) 140-2**
暗号モジュールに関するセキュリティ要件の仕様を規定する米国連邦標準規格に準拠するHSM(Hardware Security Module) の採用はされているか？

**レベル１**
個人使用レベルで考えられる高度なセキュリティ
（スマートフォン内のセキュアエレメント・ICカード）

**レベル２**
商用・実用レベルに耐える高度なセキュリティ
（クラウドベンダーが提供する水準のHSM）

**レベル３**
商用・実用レベルで考えられる最高のセキュリティ
（銀行・カード会社等の専用データセンターで運用される水準のHSM）

**レベル４**
国家機密・軍事レベルで要求されるセキュリティ
（レベル３に加えて、HSM建物レベルの堅牢性基準、所在地の不特定性を含む）

## コールドウォレットをマルチシグネチャで運用する際に敬遠されがちな点

特に仮想通貨の送信オペレーションに影響

即日出金等の対応ができない等ユーザーの不満とトレードオフ

- ✓ **トランザクションコストが2～3倍に増加する**
  - ⇒シグネチャが複数ある分だけトランザクションサイズが肥大化
  - ⇒価格競争力の低下（入出金に掛かる手数料等に影響）
- ✓ **ネットワーク越しの遠隔制御が不可能**
  - ⇒ネットワークに繋がっていれば、それはホットウォレットになってしまう
- ✓ **運用手順が煩雑で構築コストも高い**
  - ⇒ 同一のコンピュータ上、同一の個室内で交互の署名を施すのは安全対策にはならない
  - ⇒ 物理的に分離された別々の個室（コールドウォレット取扱室）を複数準備する必要がある
  - ⇒ コールドウォレット取扱室に対する常時監視と入退出管理が要求される
- ✓ **オペレーション人件費の高騰**
  - ⇒ 少なくとも署名者を複数人雇う必要がある
  - ⇒ 署名者不在の際、業務を滞らせないようにするためには、少なくともオペレーター3名マネージャ3名程度が必要となる。24時間対応を考えるとその2.5倍も

**乱数を作る**
↓
**公開鍵暗号ペアを作る**
↓
**ウォレットアドレスを作る**
↓
**トランザクションを作る**
↓
**トランザクション署名を行う**
**（マルチシグネチャなら署名を複数繰り返す）**
↓
**トランザクションをブロックチェーンのネットワークに放送する**
↓
**ブロックチェーンに取り込まれる**

オフラインで実施可能

↑この部分をインターネットにつないだまま運用するウォレットが**「ホットウォレット」**

**ネットから分離して実施するウォレットが「コールドウォレット」**

## 仮想通貨のウォレット管理

- ✓ 究極的には秘密鍵を厳重に管理することに集約される
- ✓ 秘密鍵はオンラインに置かない（ネットワークから隔離する）

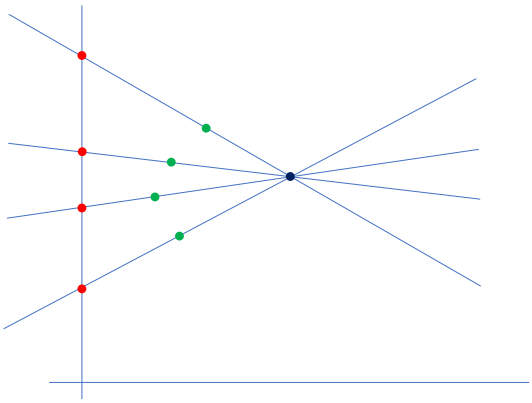
⇒ **コールドウォレット**

- ✓ 管理する秘密鍵は少ない方が安全
- ✓ ただし、１つだと盗難された際に取り返しがつかない
- ✓ 同じく、１か所に管理を集約しては意味がなくなる
- ✓ ３～５つ程度の秘密鍵を分散管理し、通常２～３つを運用に利用する

⇒ **マルチシグネチャ**

併用によりセキュリティは向上する

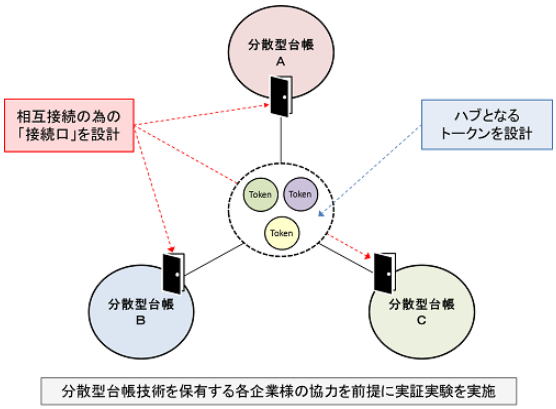
秘密分散法による鍵管理

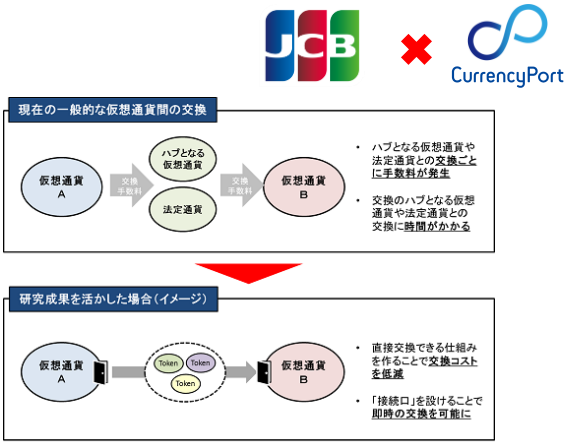


## 私たちが関与した実証実験・事例

CurrencyPort

### JCBと当社共同よる、異種分散台帳間の相互運用性に関する研究開発を開始




**ブロックチェーンコア開発ベンダー10社程度による共同研究コンソーシアム化を想定**





## 前提：ブロックチェーンのスケーラビリティ問題

CurrencyPort

**単体のブロックチェーンにおける処理性能問題**

例）ビットコイン

**オンチェーン・スケーリング**（BCH）

⇒ BigBlocks

**オフチェーン・スケーリング**（BTC）

⇒ SegWit

✓**セカンドレイヤー技術** … 層を重ねる方向性

（マイクロペイメントチャネル、ライトニングネットワーク等）

✓**サイドチェーン技術** … 横に広げる方向性

## 例）Ethereumのスケーラビリティ向上対策（「Raiden」プロジェクト）

CurrencyPort

**オフチェーン処理技術によりペイメント機能の能力を大幅に拡張する**

- ✓ **µRaiden**
  - Raiden Networkを利用しトラストレスな当事者間支払い機能の拡張（1:n）
  - 1秒以内の取引完了と手数料の圧縮（1/100以下）
- ✓ **Raiden Network**
  - Ethereum版のセカンドレイヤー技術
  - µRaidenを相互接続してネットワーク化、複数の第三者を経由してルーティング
  - ペイメントチャンネルを開く際に利用者の資金をデポジット（ロック）する
- ✓ **raidEX**
  - Raiden Networkを利用した分散型取引所
  - 複数トークン間アトミックスワップの実現(DVP)

※課題：最新のステートを保持している参加者の誰かがオンラインである必要がある
インフラ維持のためのインセンティブモデル設計が難しい





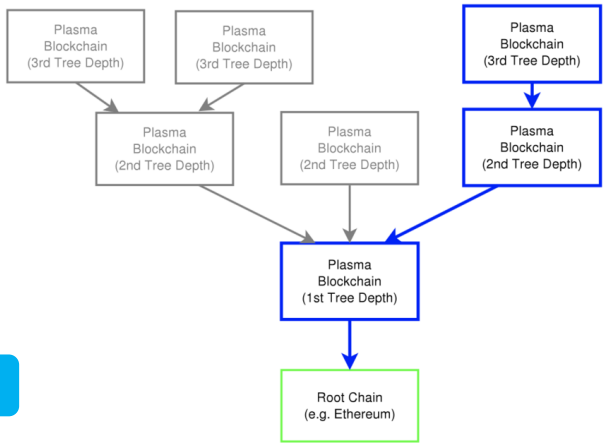
## 例）Ethereumのスケーラビリティ向上対策（「Plasma」プロジェクト）

CurrencyPort

**ブロックチェーンネットワークの階層化によりトランザクション処理能力を大幅に拡張する**

- ✓ オフチェーン処理ではなくブロックチェーンを階層化して並列処理を行うアプローチ
- ✓ Ethereumのルート・ブロックチェーンに保存されるデータサイズは減少する
- ✓ トランザクション手数料が減少
- ✓ トランザクションの実行速度が向上
- ✓ スマートコントラクト実行速度の向上

**1秒間に数十億のトランザクション実行を目指す**

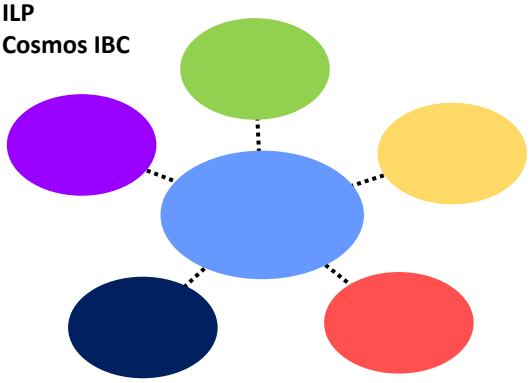



課題：withholding attack（Plazmaのブロックをわざと承認しない攻撃）

出典：https://plasma.io/plasma.pdf

## 異種ブロックチェーン間相互接続のアプローチ

例）
- ILP
- Cosmos IBC



スター接続型

直接接続型

## 価値は概念

# 価値 ⇒ 概念

## 価値は概念

# 台帳　⇒　概念



## 価値は概念

# 価値を台帳に記録する
# ⇒　概念

## 価値は概念

CurrencyPort

# ブロックチェーンやDLTの種類がが変わっても

# 概念を共有できる

 19

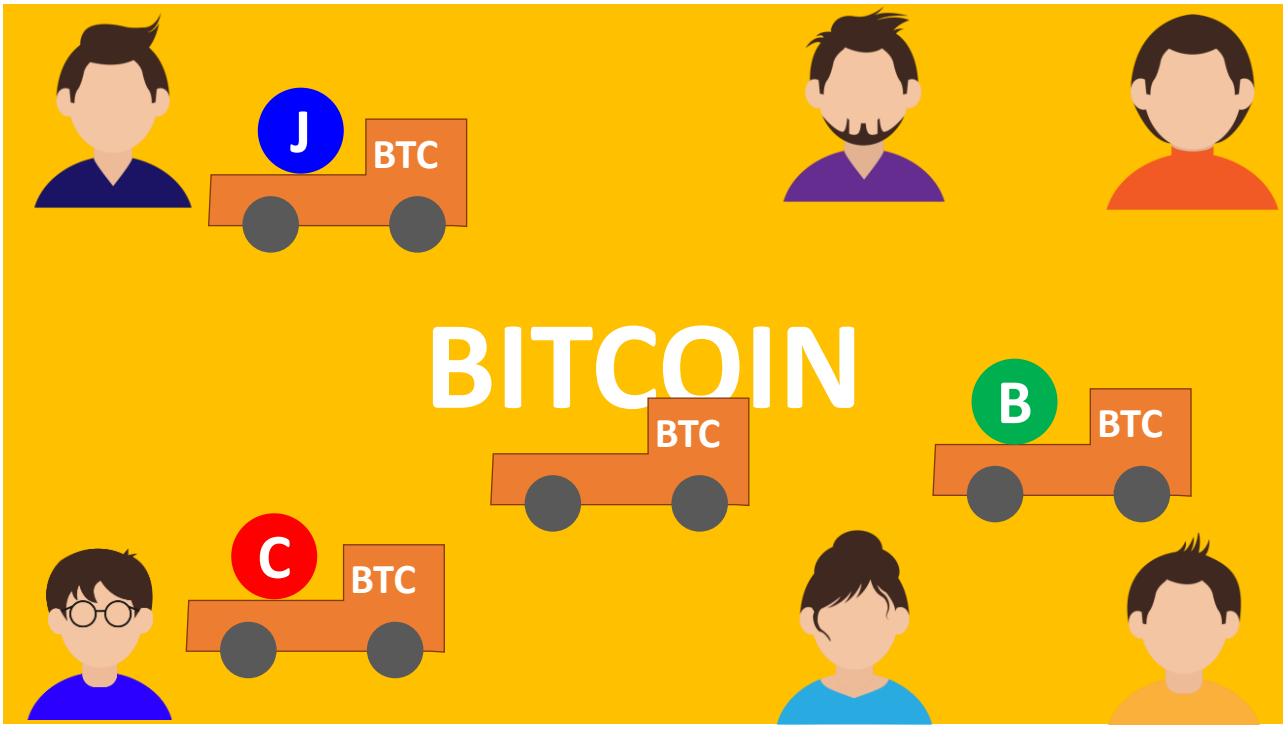
## 価値は概念

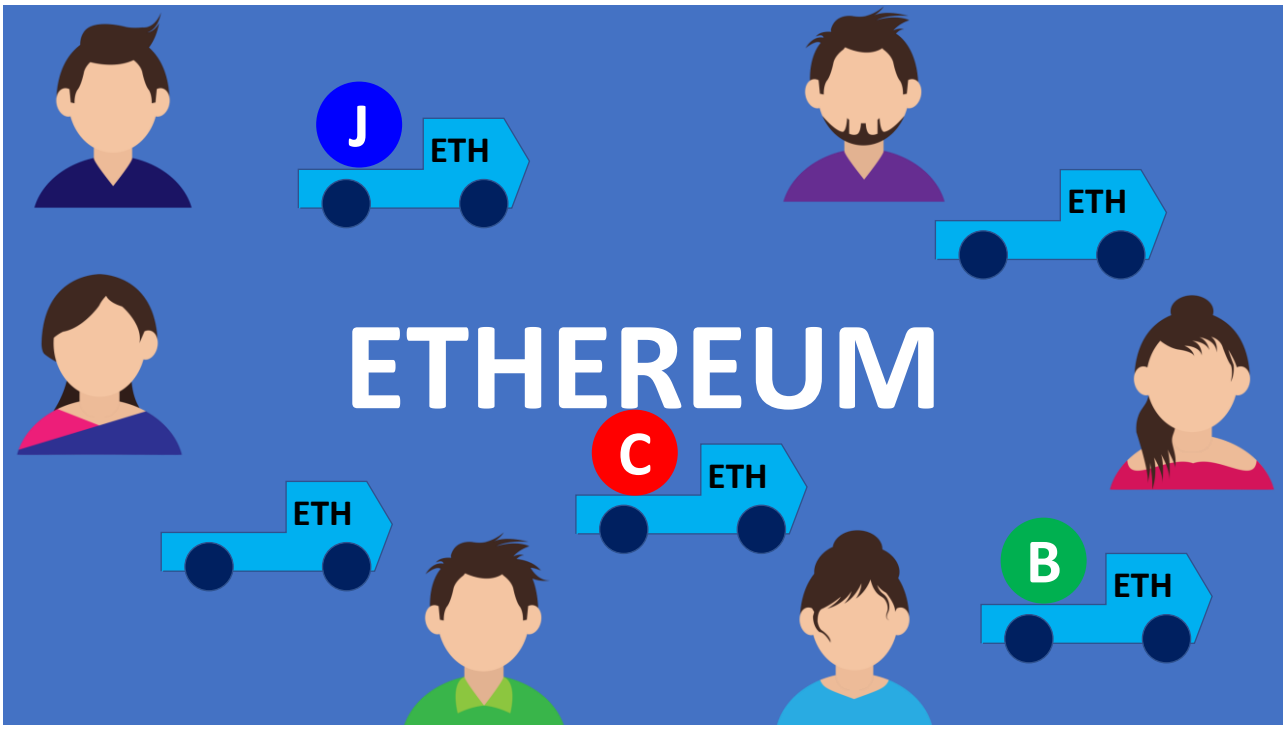
CurrencyPort

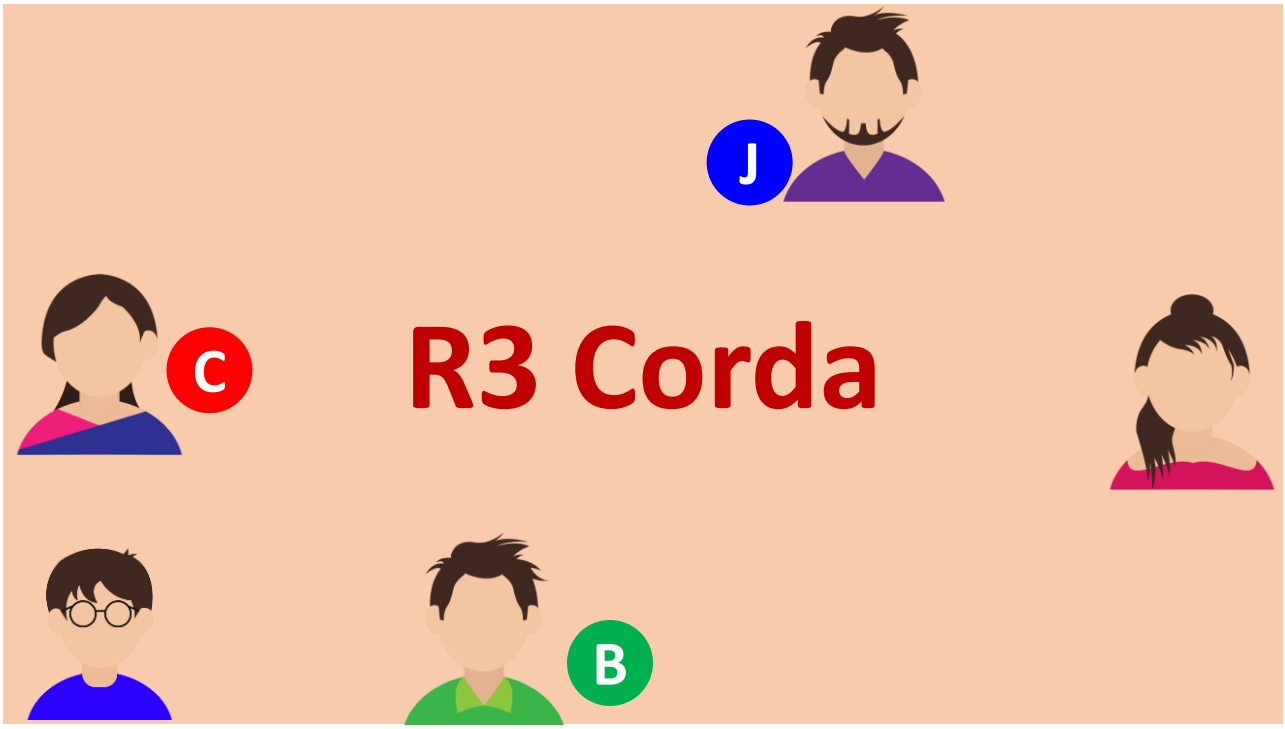
# ブロックチェーンやDLTの種類がが変わっても

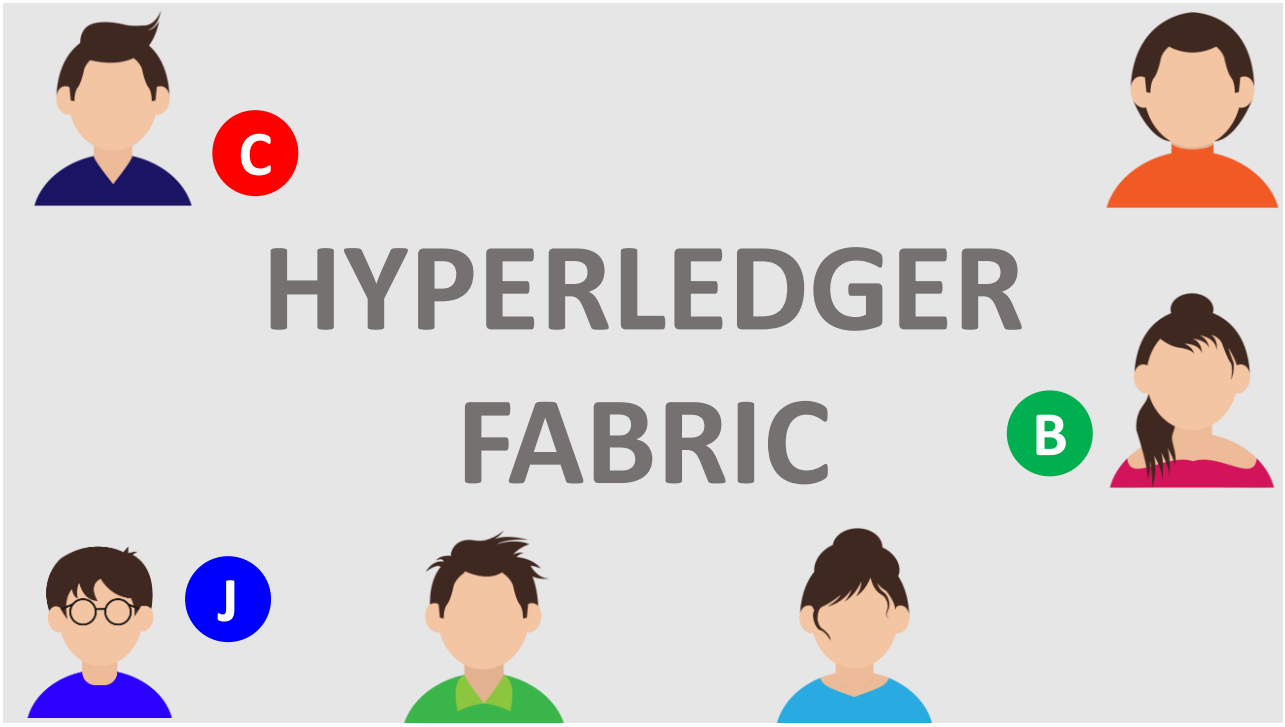
# 価値を共有できる

 20

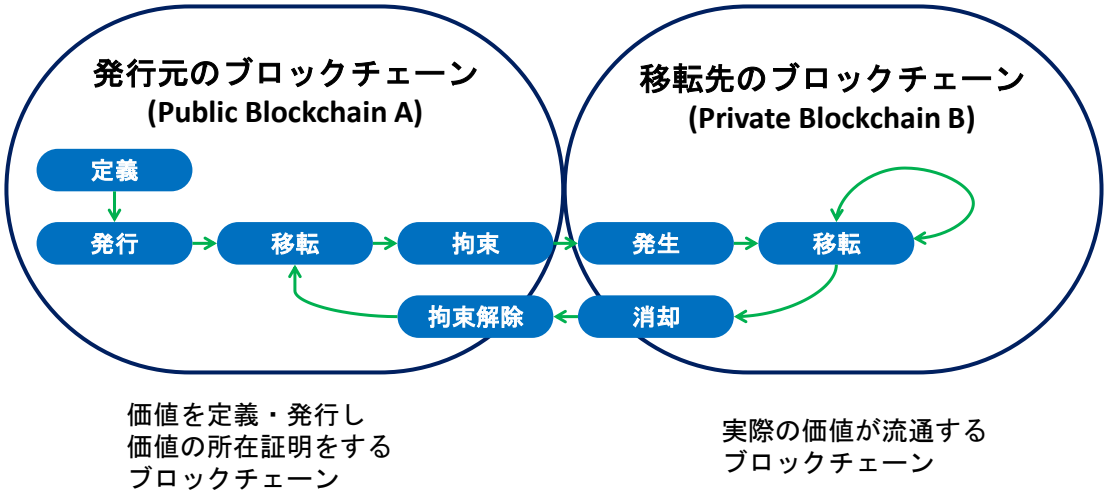

J
BTC
BITCOIN
BTC
B
BTC
C
BTC


J
ETH
ETH
ETHEREUM
C
ETH
ETH
B
ETH


J
C
R3 Corda
B


C
HYPERLEDGER
FABRIC
B
J

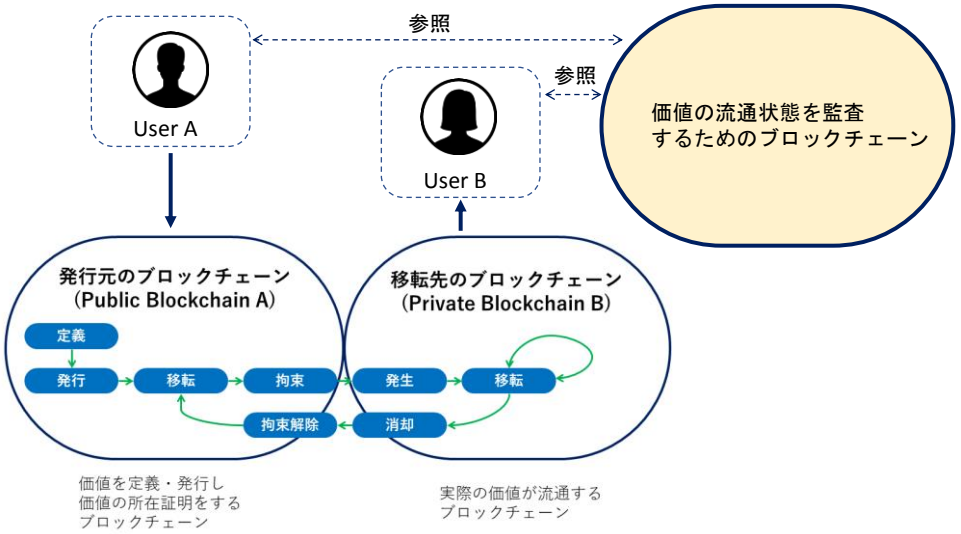
## 異種ブロックチェーン間相互接続に必要な機能





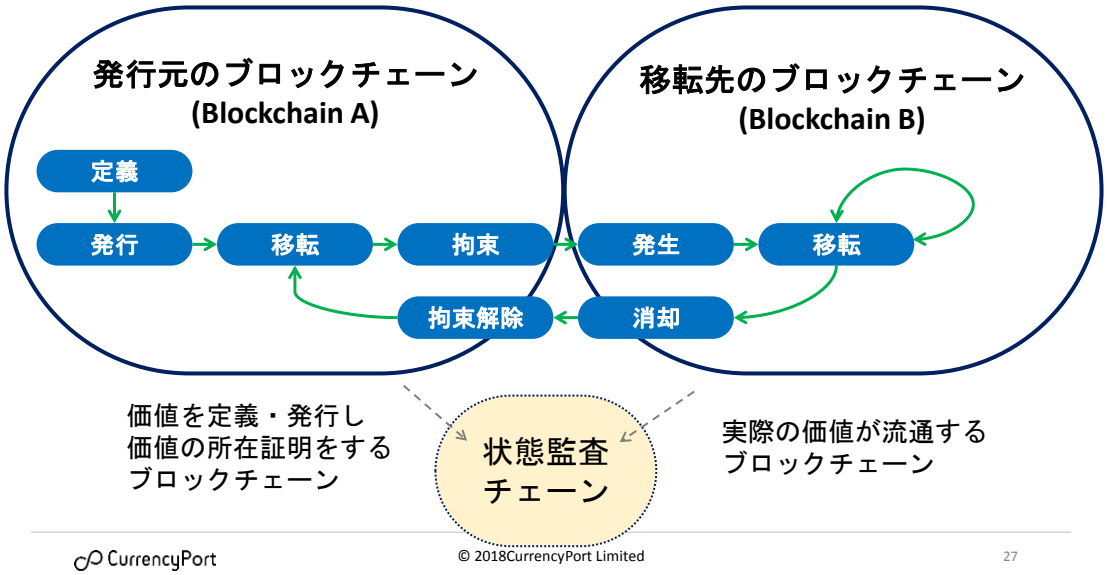


## 異種ブロックチェーン間相互接続の基本



## 異種ブロックチェーン間相互接続に必要な機能

CurrencyPort



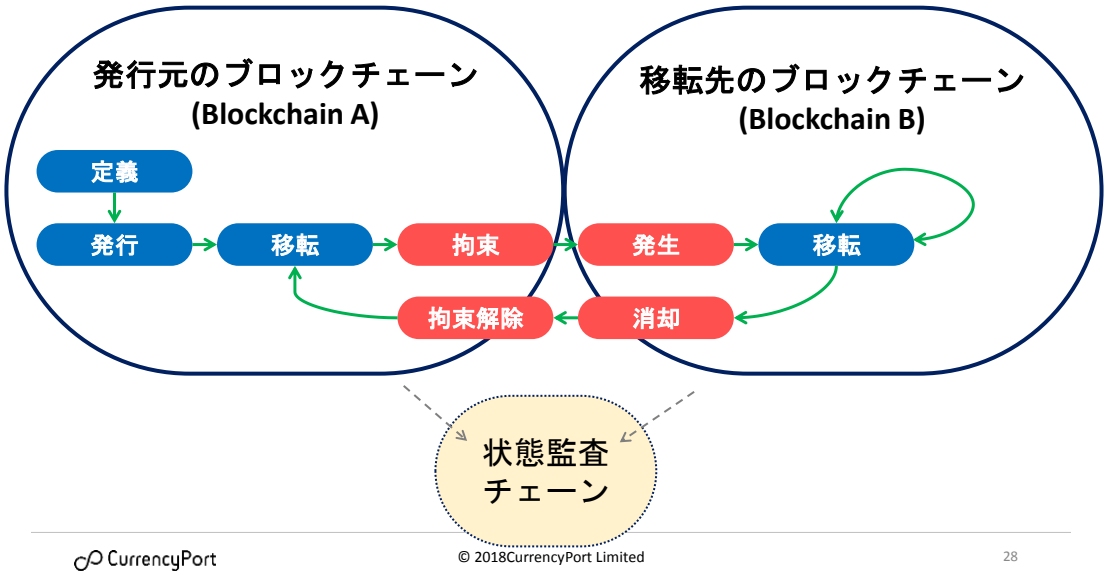

CurrencyPort



27

## 異種ブロックチェーン間相互接続に必要な機能

CurrencyPort

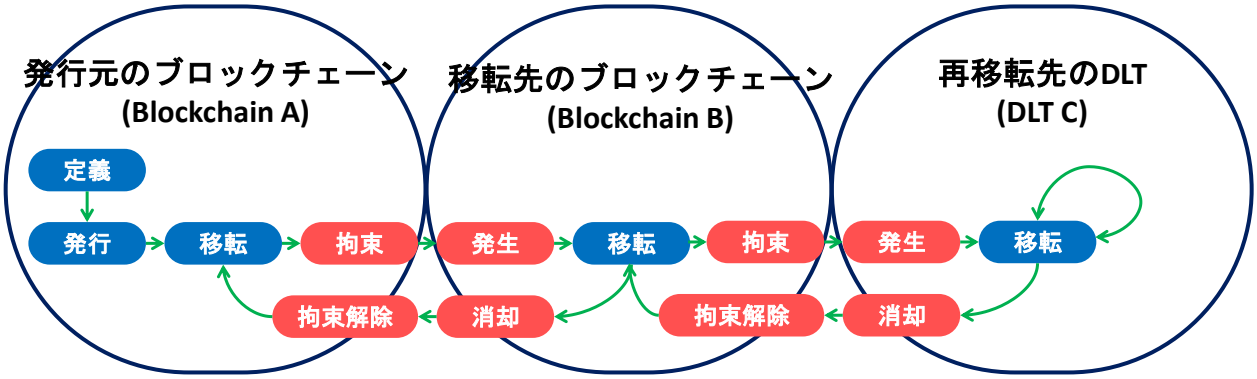



CurrencyPort



28

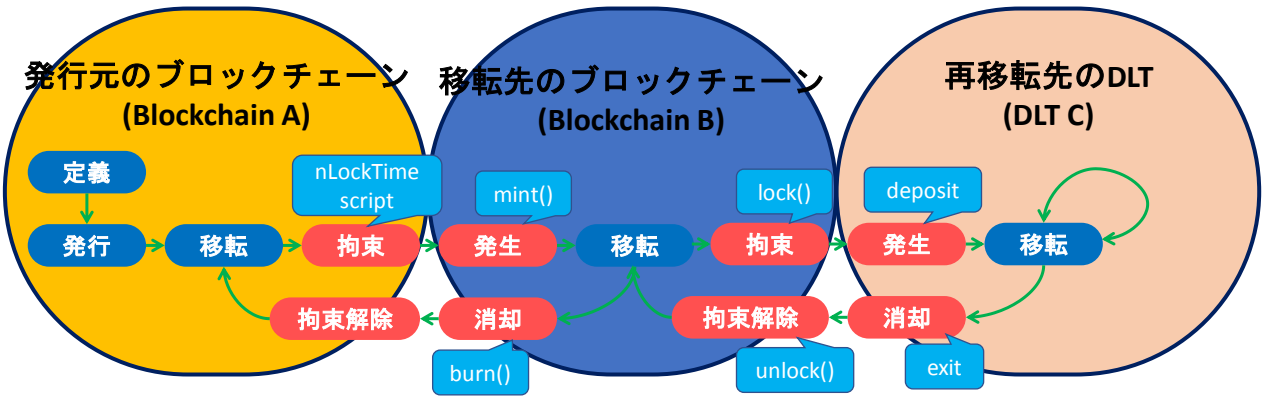
## 異種ブロックチェーン間相互接続に必要な機能







## 課題：名称の違い ⇒ 割当て・平準化の提案等も必要




**Bitcoin**
（スクリプト）

**Ethereum**
(スマートコントラクト)

**Corda**
(スマートコントラクト)

## コンソーシアム結成（近日予定）

CurrencyPort

bitcoin ethereum HYPERLEDGER corda

mijin miyabi orb IROHA

beyond-blockchain.org Keychain