CurrencyPort

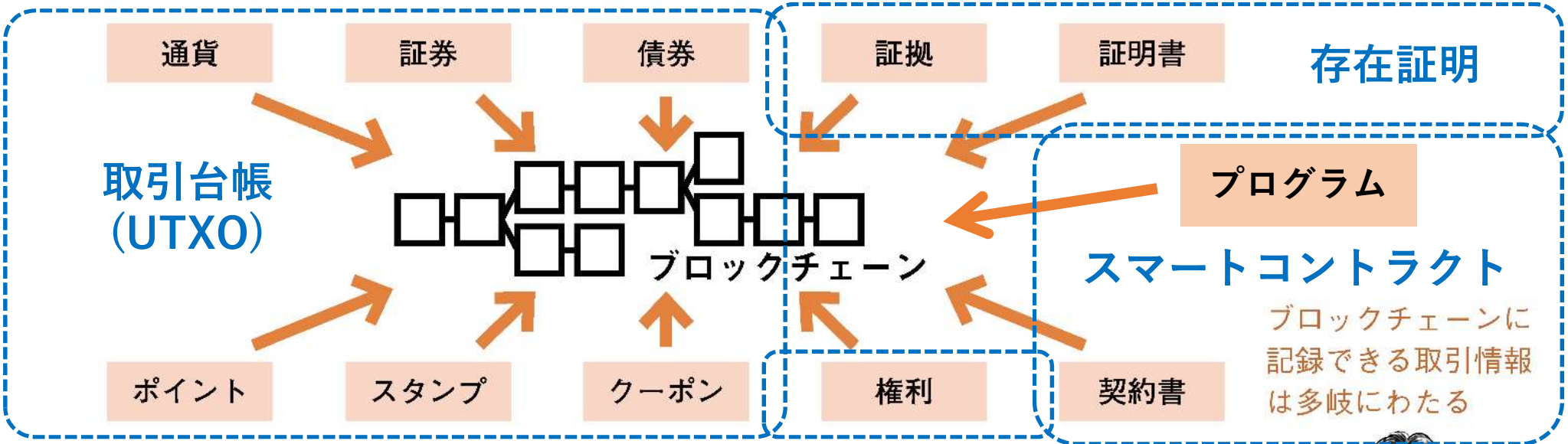
スマートコントラクトで
契約を執行する仕組みを知ろう

- ✓ 送金の目的以外のものをブロックチェーンに記録する方法
- ✓ 契約を自動的に執行する仕組み
- ✓ コンピューターによる合意形成とは？
- ✓ 外部環境の情報を基にする合意形成
- ✓ 機械同士が能動的に合意形成をする未来

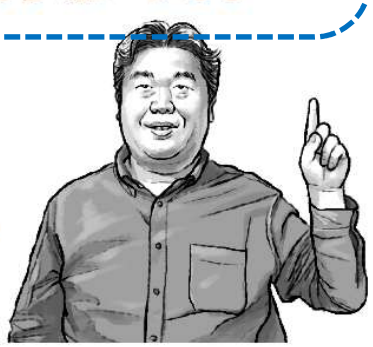
ブロックチェーンに
なにを記録するかがカギ

CurrencyPort

▶ブロックチェーンにはさまざまな取引情報が記録できる 図表01-3



ブロックチェーンの生みの親といわれている「サトシ・ナカモト」氏は、誰にも止められず、誰にも邪魔されない「送金取引」をこのような仕組みに記録できれば仮想通貨が実現できると考えました。それが「ビットコイン」です。



帳簿の連続性を保証する仕組み 未使用残高「UTXO」

Unspent Transaction Output

CurrencyPort

デジタルマネー

▶ UTXOの概念図 図表40-1

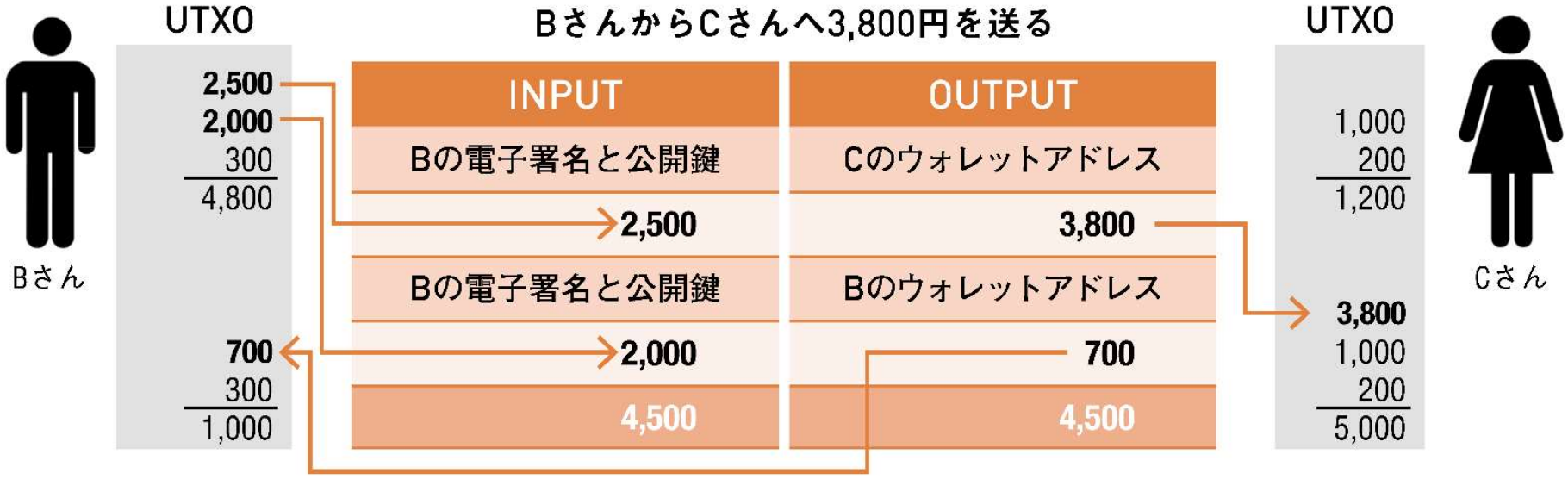
ブロックチェーンが「台帳技術」といわれるゆえん

帳簿の連続性を保証する仕組み 未使用残高「UTXO」

Unspent Transaction Output

CurrencyPort

デジタルマネー



送金するときは、送金額を満たすUTXOから送金する。足りない場合は、複数のUTXOをInputに配置する。
InputとOutputの合計は常に同じ額となる

ブロックチェーンが「台帳技術」といわれるゆえん

送金以外を目的とするトランザクション

CurrencyPort

ファイルの存在証明

▶送金以外を目的とするトランザクションの例 図表39-2

Aさんがある文書の存在証明をしようとした

INPUT	OUTPUT
Aの電子署名と公開鍵	Aのウォレットアドレス
3,000	3,000
	OP_RETURN
	文書のハッシュ値
3,000	3,000

送金の取引

存在証明したい文章

Hash((文章))

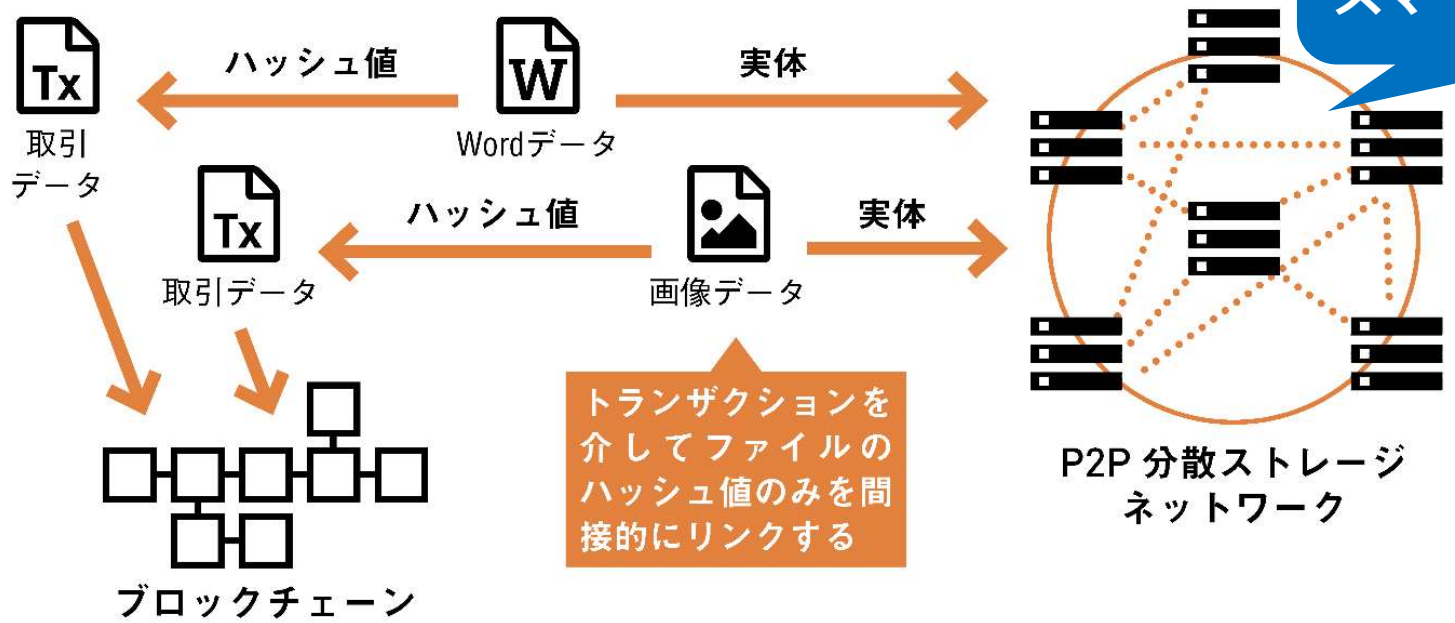
送金を目的としなくても、必ず送金の取引は行う必要がある。その場合、自分宛に送金する形をとる

送金以外の拡張機能を利用する目的で作られるトランザクションであっても「送金」の取引は必ず記載されています。

ファイルのハッシュ値と実態をつなげる「コンテンツアドレス」

CurrencyPort

▶ファイルの実体はP2P分散ストレージへ ファイルのハッシュ値のみブロックチェーンへ 図表28-2



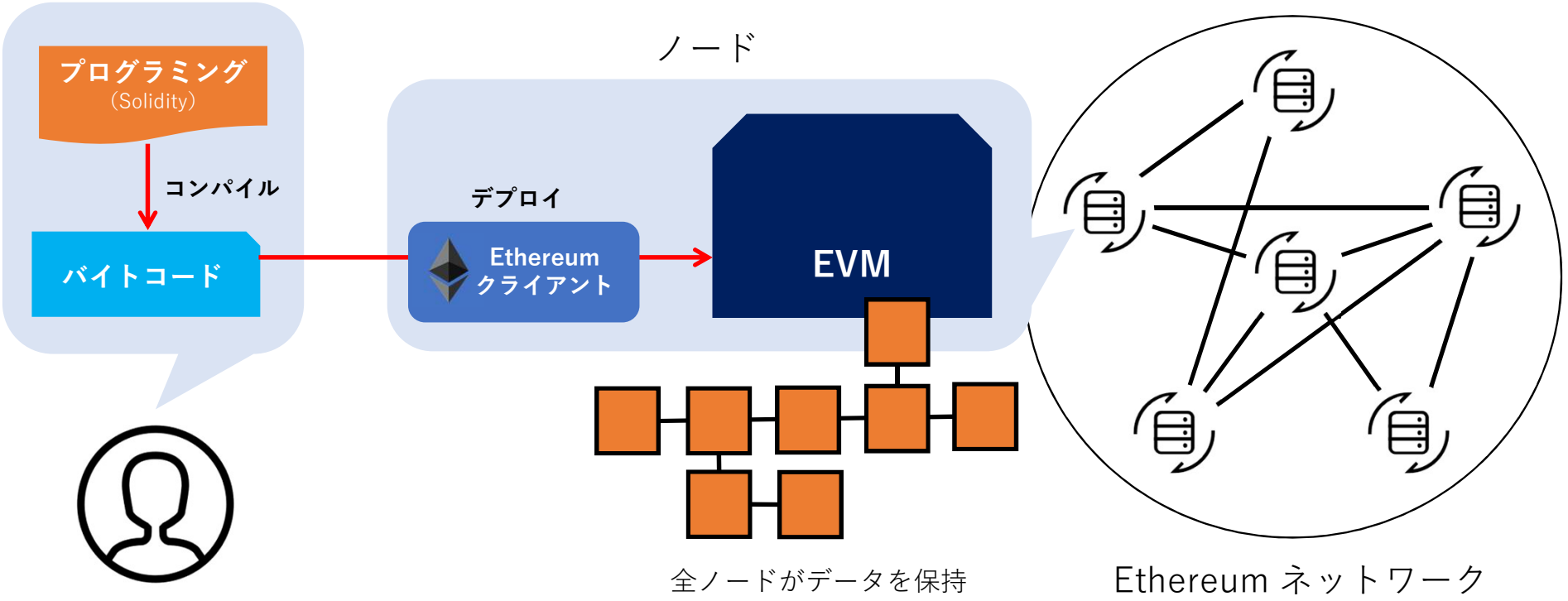
契約とプログラムを結合することができればスマートコントラクトに

ブロックチェーンに記録したデータは、変更や削除ができないという点に注意が必要です。

ハッシュ値をアドレスとして利用することで、ファイルの特定が可能になる

○「改ざんされては困るもの」の保存に適している

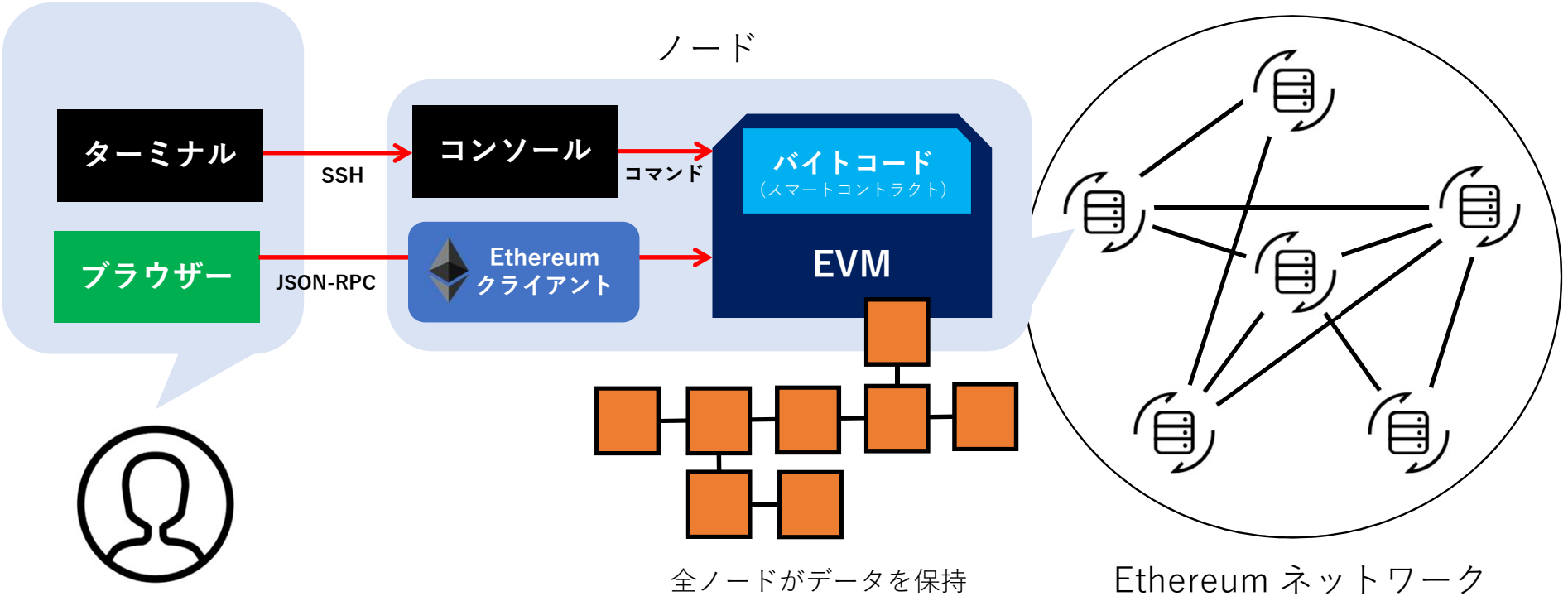
Ethereum スマートコントラクトデプロイのイメージ



- ✓データの検証や計算は各ノードで一斉に実行
- ✓データの更新は更新内容をネットワークに投かん

UTXOモデルではなく
状態遷移モデルを採用

Ethereum スマートコントラクト実行のイメージ



- ✓データの検証や計算は各ノードで一斉に実行
- ✓データの更新は更新内容をネットワークに投かん

UTXOモデルではなく
状態遷移モデルを採用

複雑な条件分岐を含む高度なスマートコントラクト

CurrencyPort

▶スマートコントラクトをプログラミングできるブロックチェーン 図表48-1

Ethereum（イーサリアム）

スマートコントラクト開発言語：
Solidity（専用言語）、Python

Hyperledger Fabric（ハイパーレジャー・ファブリック）

スマートコントラクト（チェーンコード）開発言語：
Go、Java

R3 Corda

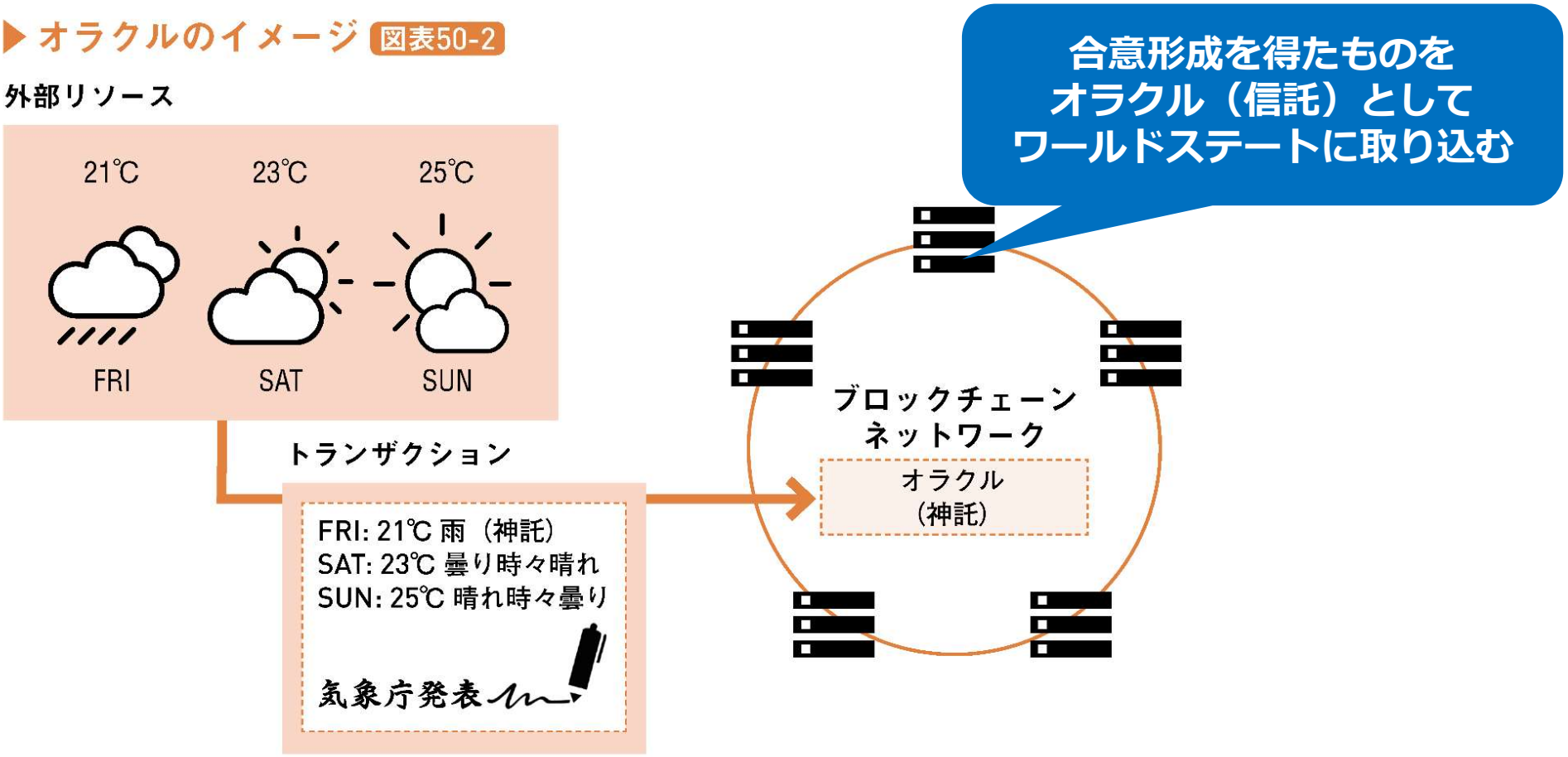
スマートコントラクト開発言語：
Kotlin（Javaから派生）

スマートコントラクトでは、使用される言語に関わらず、バイトコード化され仮想マシン上で実行されるため、合意に影響するような環境依存性はなくなります。

第三者提供の情報リソースを「オラクル」（信託）と考える

CurrencyPort

▶オラクルのイメージ 図表50-2



外部リソースはトランザクションから登録して、合意を得たものを「オラクル」とする

ワールドステート（世界の状態）

CurrencyPort

▶ワールドステートはすべてのスマートコントラクトから参照できる情報 図表48-2

ブロックチェーンのネットワークに参加しているノードが一斉に計算して合意

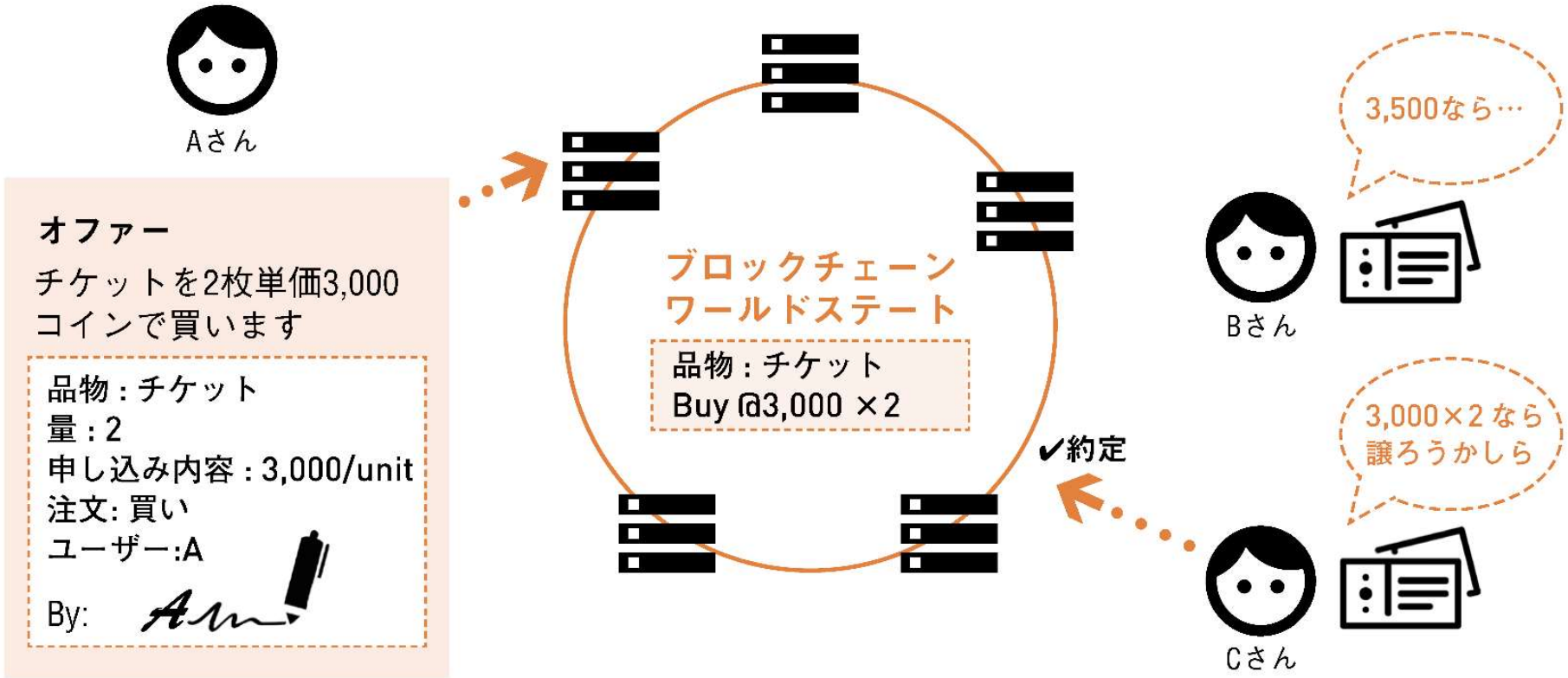
スマートコントラクトにおける合意結果は、「ワールドステート」と呼ばれ、ブロックチェーンに記録されると、ほかのスマートコントラクトと共有されます。

ワールドステートの合意で中央集権的組織が不要となる取引の例

CurrencyPort

DEX

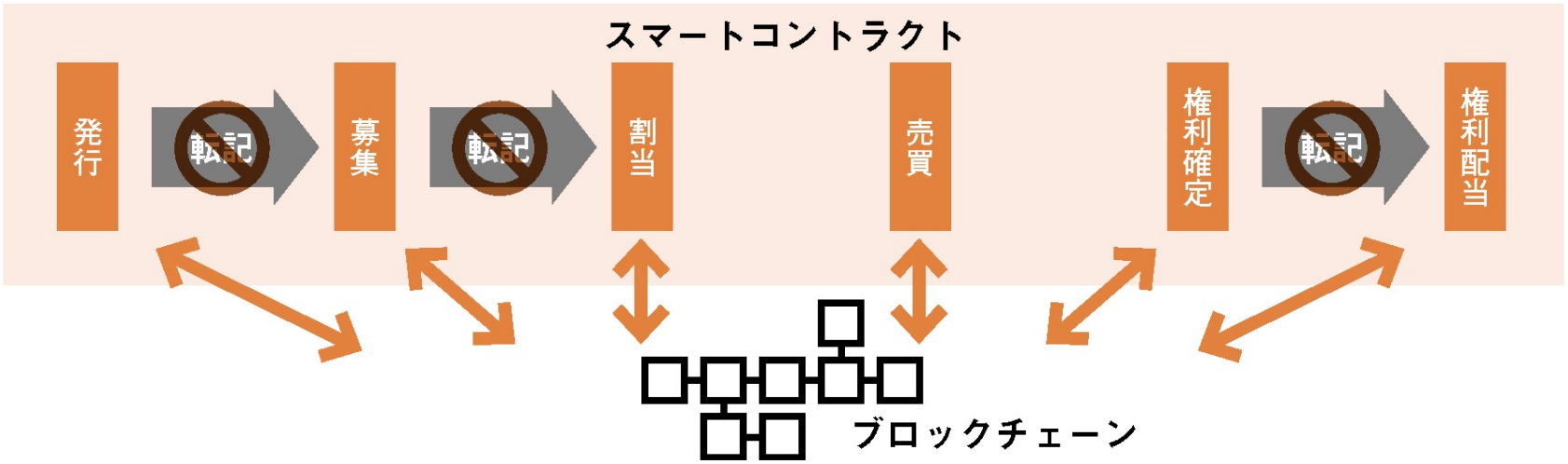
▶ワールドステートを応用したチケット取引所の例 図表48-3



トランザクションにオファーを書き込んでワールドステートに投かん。ほかの参加者が契約を自動的に約定

スマートコントラクトとの相性が良い証券分野での活用

▶ブロックチェーン技術の台頭によって消える「リコンサイル（転記）業務」 図表56-1



証券業務では、発行から配当までを1つの分散システムで構築できる。
そうなるとリコンサイル（転記）業務は事実上なくなる

証券としての価値の一生、つまり、証券が生まれて死ぬまでのいっさいを、ブロックチェーンを使って記録管理できるため、従来分断されていた各業務は１つのスマートコントラクトによって置き換えが可能になってしまいました。

Ethereumの開発コミュニティ

EIP (Ethereum Improvement Proposal)とERC (Ethereum Request for Comment)

「EIP」と「ERC」は、ともに、GitHubでチケット管理されている技術提案
https://github.com/ethereum/EIPs/issues

「EIP」は、Ethereumのシステム全体に関わる様々な改善提案全般
「ERC」は、Ethereum上で動作するスマートコントラクトにより実現される機能の実装に関する標準仕様の提案（プロジェクトの自由意思で採択可能な技術提案）

EIP ⊇ ERC（ERCはEIPの部分集合）

コアデベロッパー同士によるオンライン会議「Core Devs Meeting」が定期的に開催されており、議題とされた提案の承認を得る。この模様はYouTube上でライブ放送され、世界中のだれもが自由に視聴・参加できるオープンな場となっている
https://www.youtube.com/channel/UCNOfzGXD_C9YMYmnefmPH0g

Ethereum上に発行するトークンの標準仕様提案

ERC20

Ethereum Token Standard（現時点で最もシェアの高いトークンの表現仕様）
EOA（Externally Owned Account）と呼ばれる、利用者アカウント（≠コントラクト）宛にのみ送信可能

ERC223

ERC20の改良提案。誤ってトークンを取扱えないスマートコントラクトのアドレス宛にトークンを送信してしまうと、トークン移動ができなくなってしまう不具合（ゾンビトークン）の問題を解決する提案
トークンを受取れないコントラクトアドレスに送ってしまった時、送り主にトークンを戻す機能を追加

ERC777

ERC20として振舞いながら、トークンを送受信できるスマートコントラクト用のインターフェイスを定義

ERC721

ERC20、ERC223、ERC777 がそれぞれFungible Token（代替可能なトークン）を定義した規格であるのに対し、ERC721は、Non-Fungible Token（代替不可能なトークン）を定義するために提案された規格

※トークン様式に関する標準提案は、これら以外にもいくつか存在します

代替可能なトークンと代替不可能なトークン

代替可能なトークン（Fungible Token） ERC20、ERC223、ERC777

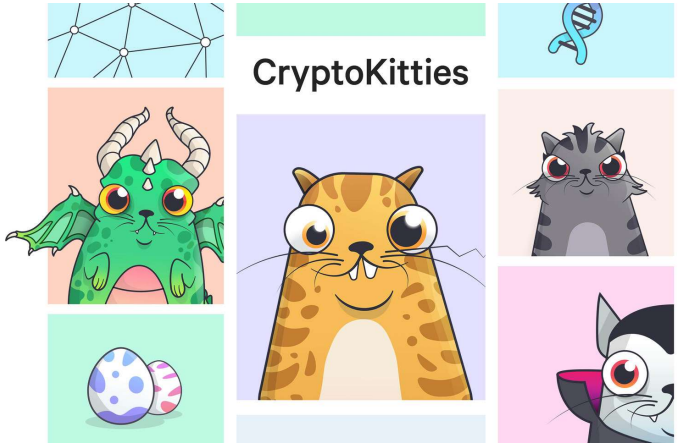
通貨、証券、ポイント、スタンプ、クーポン等
保有している数量のみで、価値の評価が可能なトークン

代替不可能なトークン（Non-Fungible Token） ERC721

不動産の権利、座席の予約券、ゲームのアイテム、くじ引き抽選券等
他のリソースと代替不可能で、個別に価値の評価をすべきトークン

IPSF等、外部のP2P分散ストレージに配置したドキュメントと連携して
個別の価値を表現可能

事例）CryptoKitties
⇒ 人気でEthereumのトラフィックを占有してしまったため
現在では、専用のブロックチェーンに移行



識別可能な資産の登記（Distinguishable Asset Registries）EIP821

ブロックチェーン上の物理的またはデジタルの識別可能なアイテムの所有権を追跡する仕組み

代替不可能なトークン（NFT: Non-Fungible Token） ERC721 に対する所有者とその資産を参照するスマートコントラクト

例）不動産の権利登記、美術品のオーナー確認、ゲームアイテムの所有者確認

- ✓ NFT（ブロックチェーン上の資産の表現）… 265bits ハッシュ値
- ✓ DAR（その資産を登録するコントラクト）… 160bits アドレス

URIの表現様式

```
nft://<chain's common name>/<DAR's address>/<NFT's ID>
```

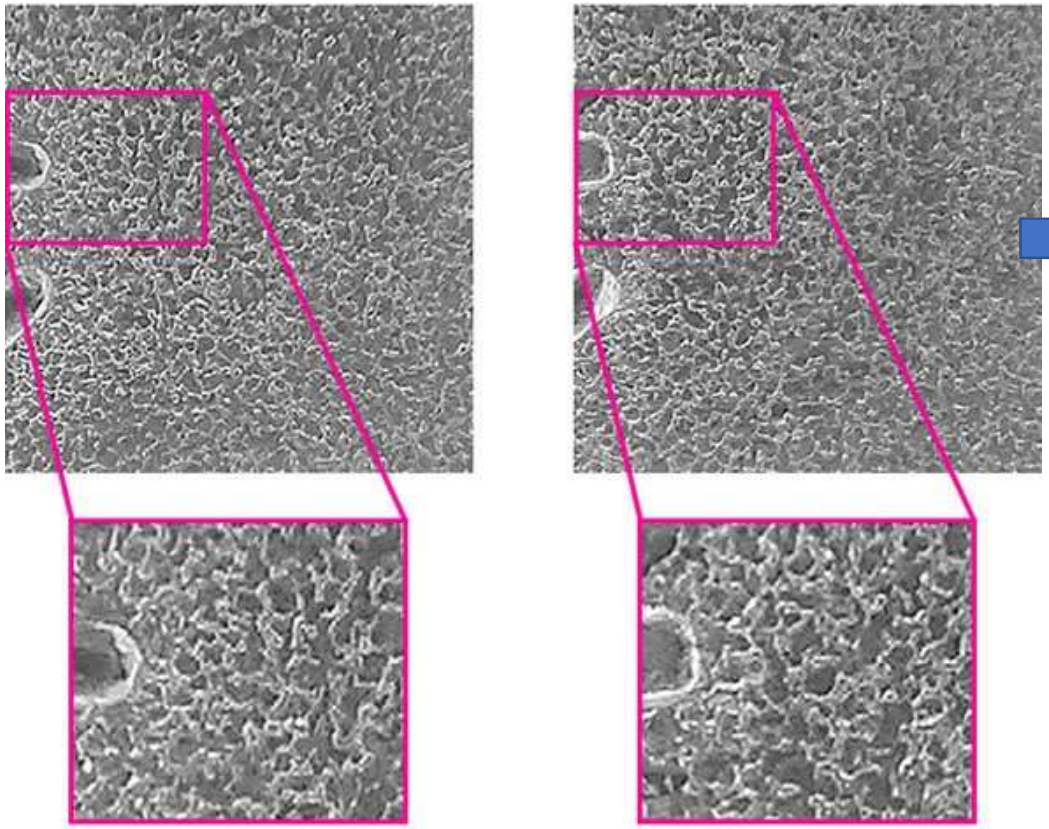
URIの表現例

```
nft://ethereum/0xF87E31492Faf9A91B02Ee0dEAAd50d51d56D5d4d/0xfaa5be24e996feadf4c96b905af2c77c456e2debd075bab4d8fd5f70f209de44
```

参照：**ERC721** … Identify （人間、グループ、オブジェクト、およびマシンに対する一意のID付け）

モノを譲渡可能なトークンにする仕組み

製品個別情報をブロックチェーン上で流通可能な状態にトークン化



NEC、富士ゼロックス等

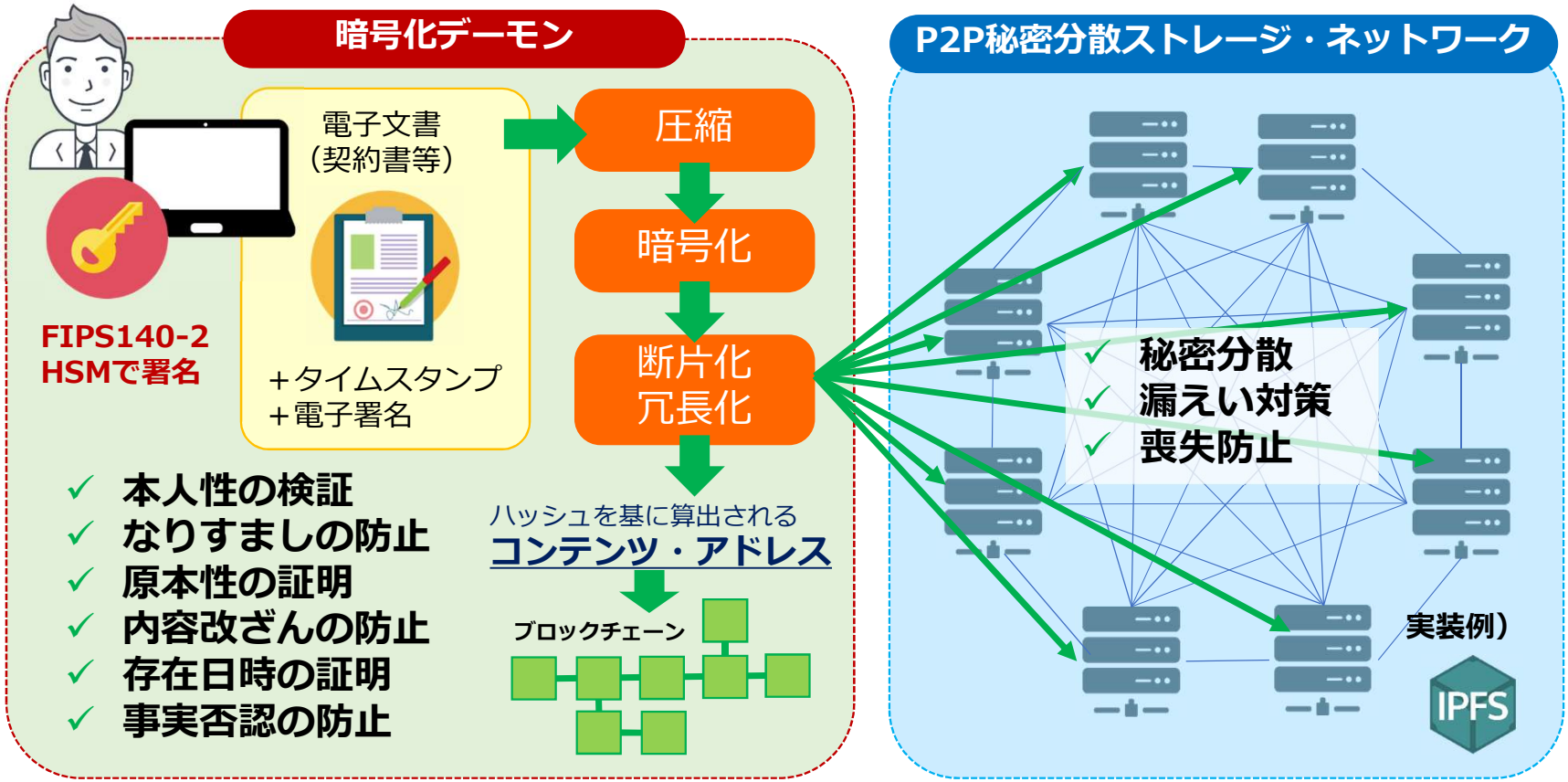
- ✓ 物体指紋
- ✓ 製品指紋
- ✓ 個体識別情報

1. データを秘密分散ストレージに保管
2. ハッシュベースのアドレスを取得
3. ハッシュベースのアドレスと、
4. メタデータを併せてトークン化
5. 上記トークンをブロックチェーン上で発行する
   （代替不可能なトークンとして）

参考）Digital Arts Chain
http://digitalartchain.com/publish.html

P2P秘密分散ストレージ

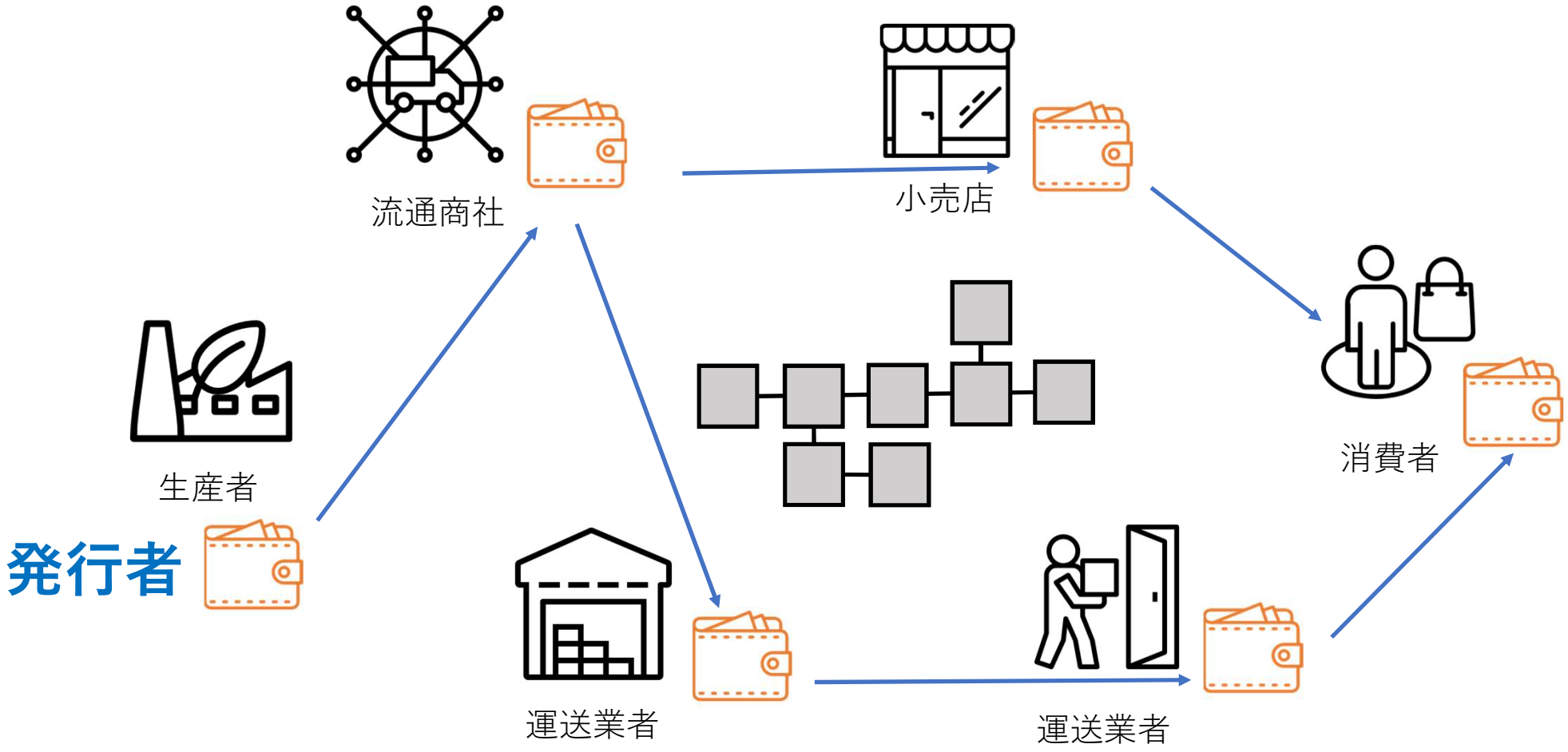
商取引で日々取り交わされる、あらゆる電子文書の真正性を担保する基盤



ブロックチェーンを用いた流通トレーサビリティに必要なシステム

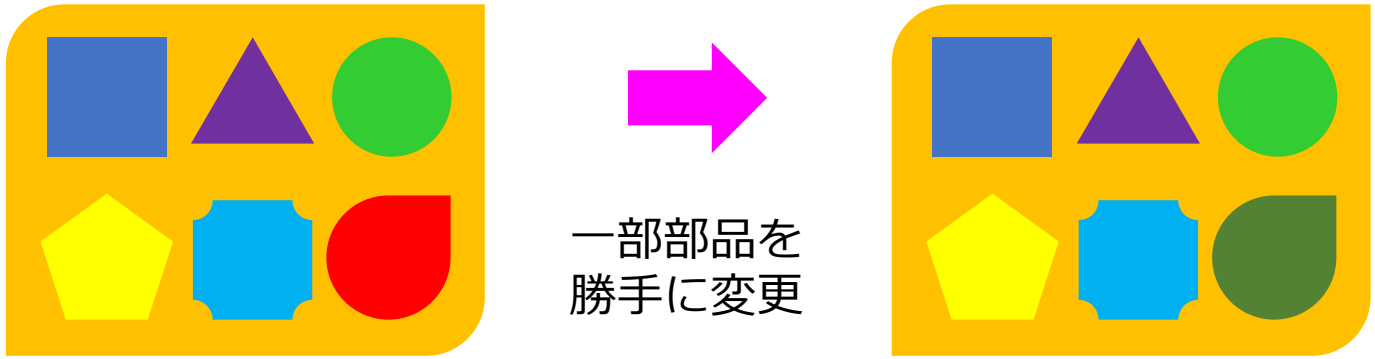
CurrencyPort

商品追跡の基本は、NFT（代替不可能なトークン）を移転するだけ



流通トレーサビリティ（サイレントチェンジ防止対策）

部品供給元が、発注メーカーの指定とは異なる（が、気づかない程度の）
安価な模造品に変えてしまう事によるトラブル（クレームやリコール）の防止



発注メーカーが
指定する**正規部品**

部品サプライヤーが
納品した**模造部品**

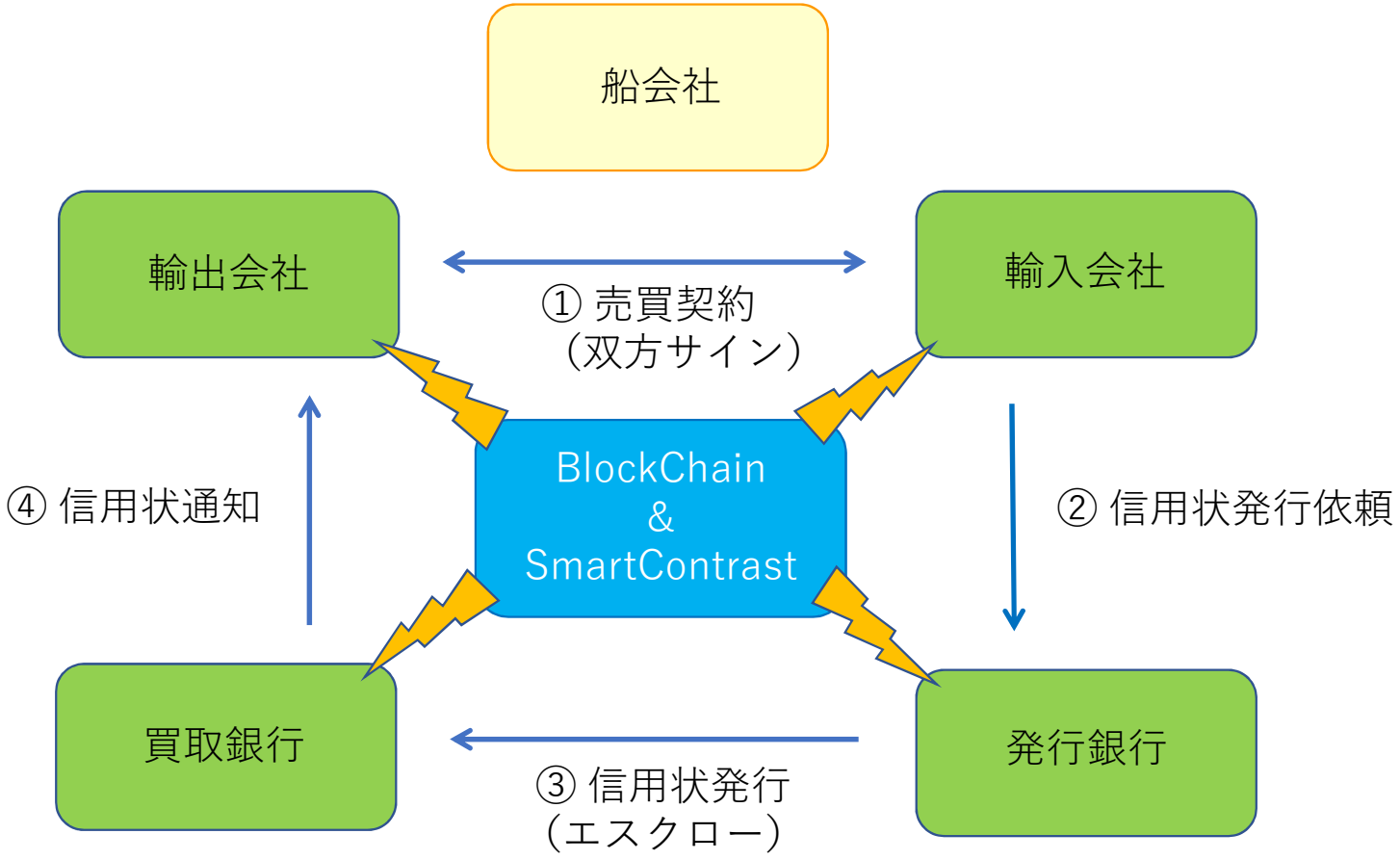
正規の部品メーカーのみが発行できる電子署名を含む納品書の
ハッシュ値をブロックチェーンに記載する事を納品基準とする。

流通トレーサビリティ（クロスドッキング・SKU管理）

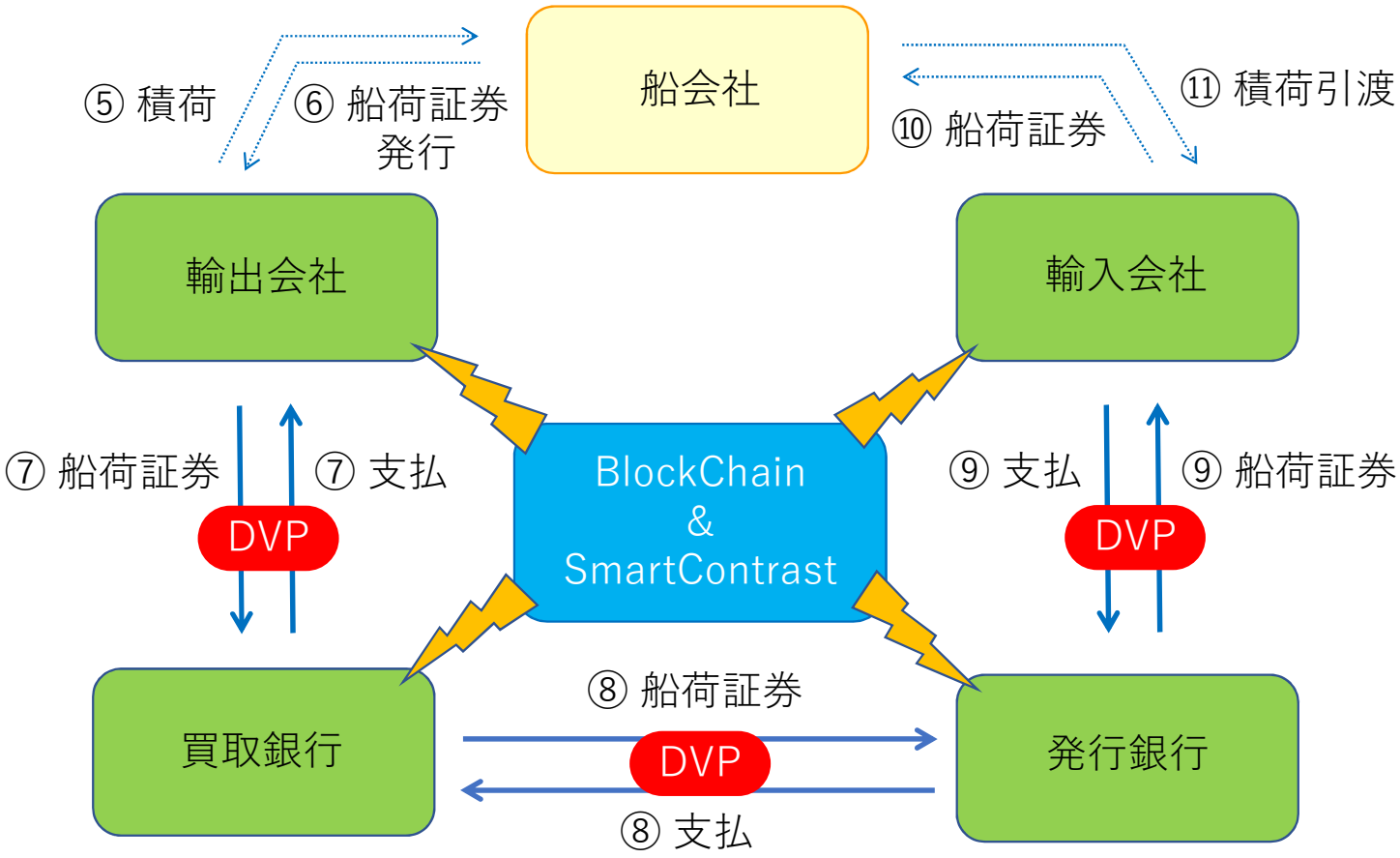
物のトークン化 ⇒ ロケーション／荷役業務／所有権の移転ステータス管理
入庫、検品、保管、受注、引当、ピッキング、梱包、出荷、輸送等の追跡

【出荷】**発注店舗の在庫**　【消化仕入】**流通商社の滞留在庫**　【入庫】**各メーカーの在庫**

貿易取引業務／信用状（L/C）発行～通知



貿易取引業務／船荷証券の引渡しと支払い



Ethereumのスケーラビリティ向上対策（「Raiden」プロジェクト）

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)

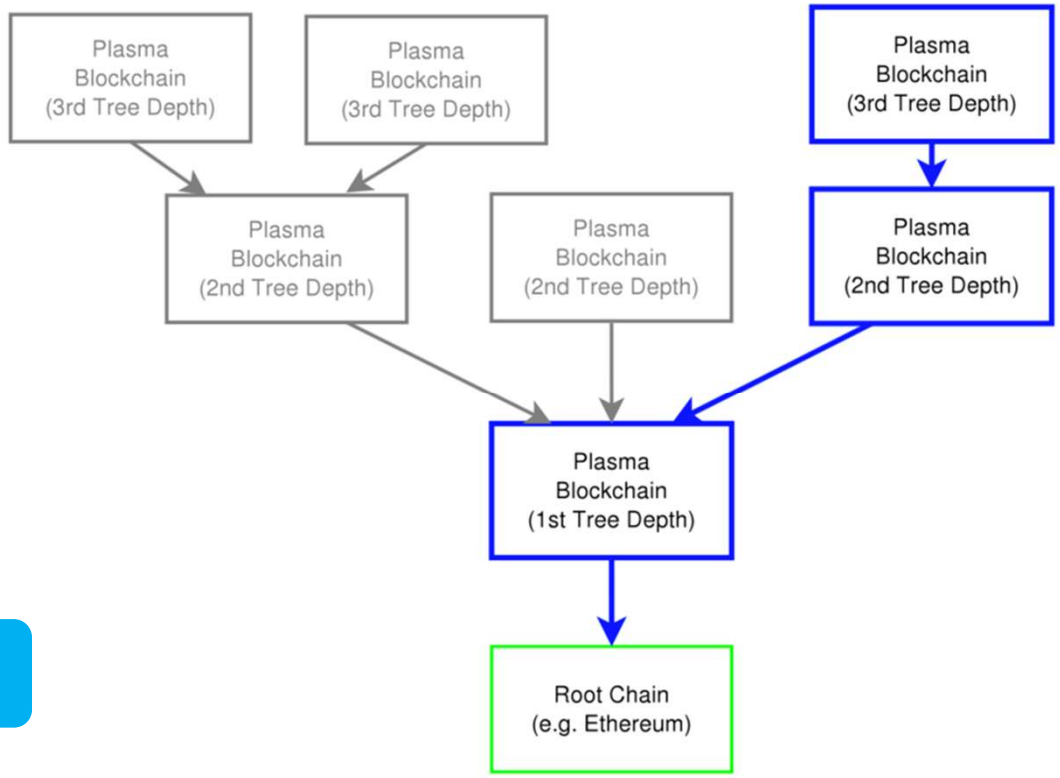
※課題：最新のステートを保持している参加者の誰かがオンラインである必要がある
インフラ維持のためのインセンティブモデル設計が難しい

Ethereumのスケーラビリティ向上対策（「Plasma」プロジェクト）

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

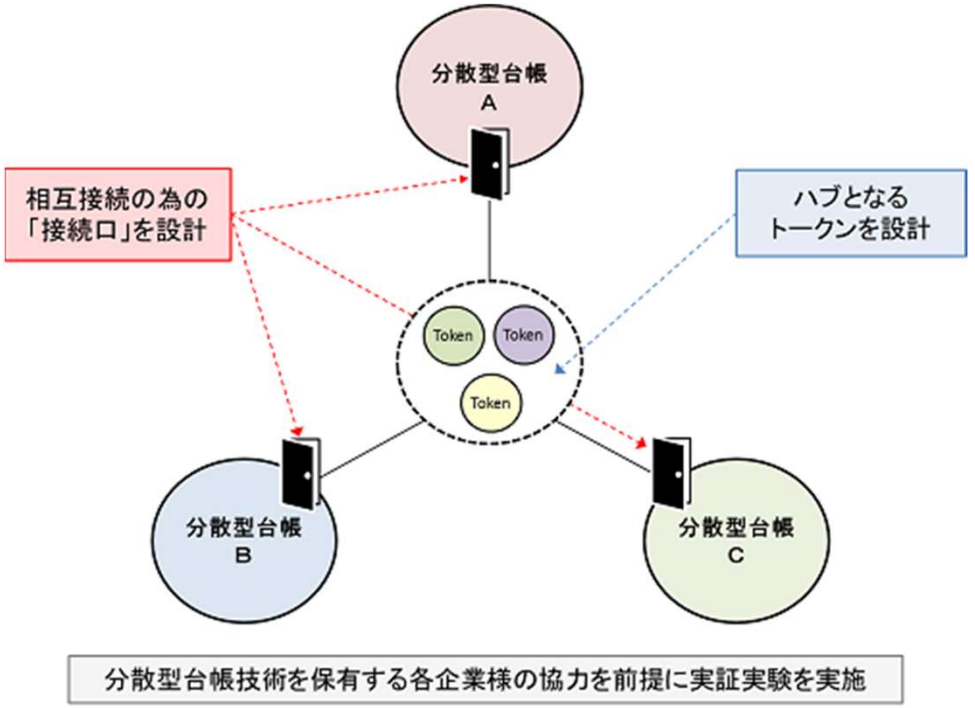


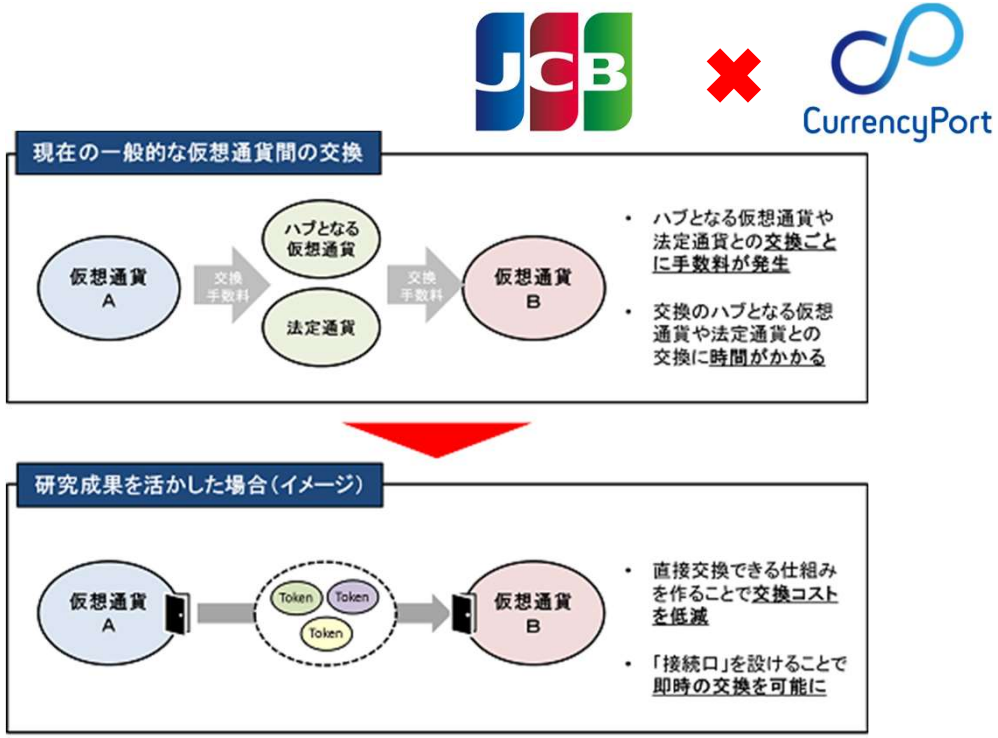
課題：withholding attack（Plazmaのブロックをわざと承認しない攻撃）

出典：https://plasma.io/plasma.pdf

異種ブロックチェーン間のインターオペラビリティとスケーラビリティ

ブロックチェーンネットワークの相互接続により運用柔軟性の高いネットワークを構築する



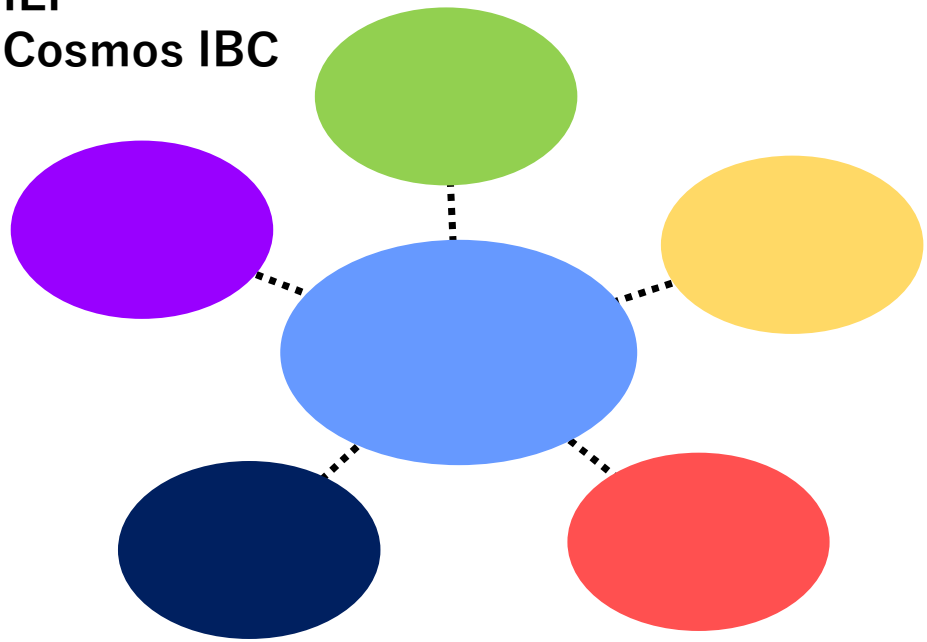


国内のブロックチェーン・コア開発ベンダー10社程度による共同研究コンソーシアム化を想定

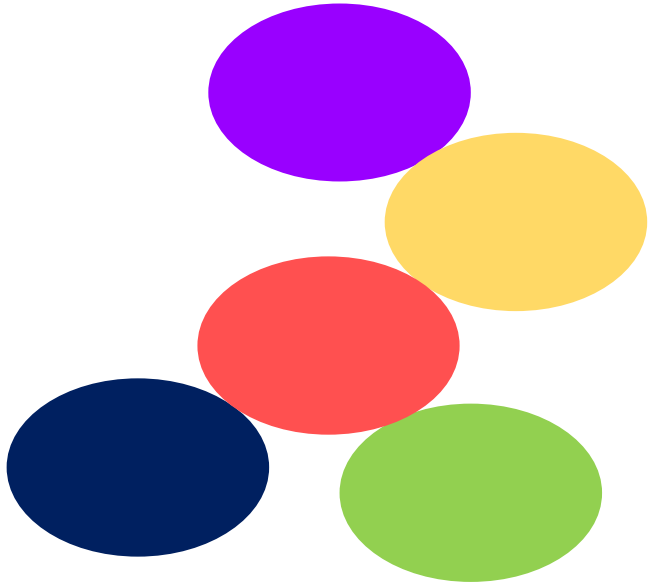
異種ブロックチェーン間相互接続のアプローチ

例）

- **ILP**
- **Cosmos IBC**



スター接続型



直接接続型

価値は概念

CurrencyPort

価値　⇒　概念

価値は概念

台帳　⇒　概念

CurrencyPort

価値を台帳に記録する
⇒　概念

CurrencyPort

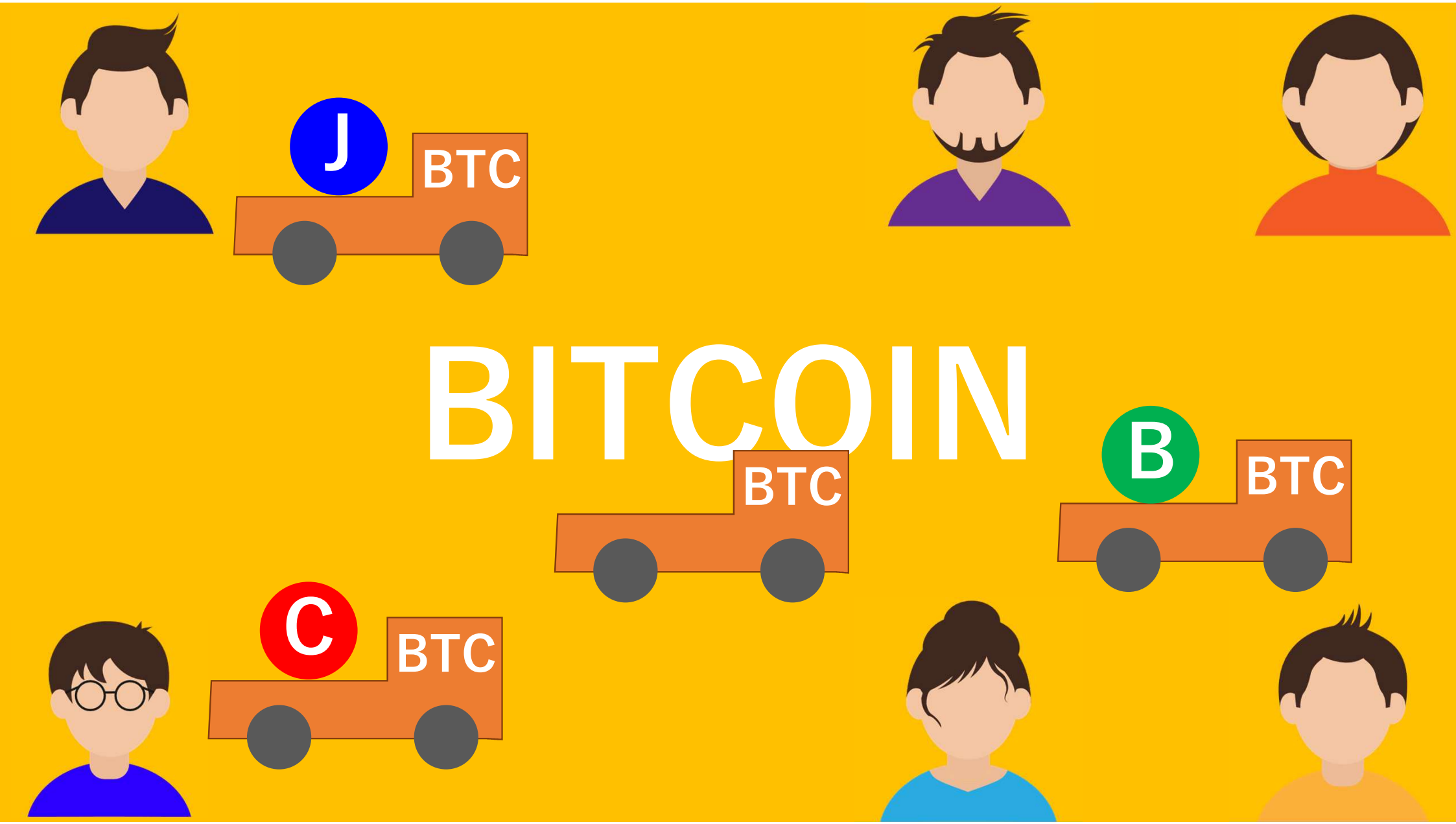
ブロックチェーンやDLTの種類がが変わっても

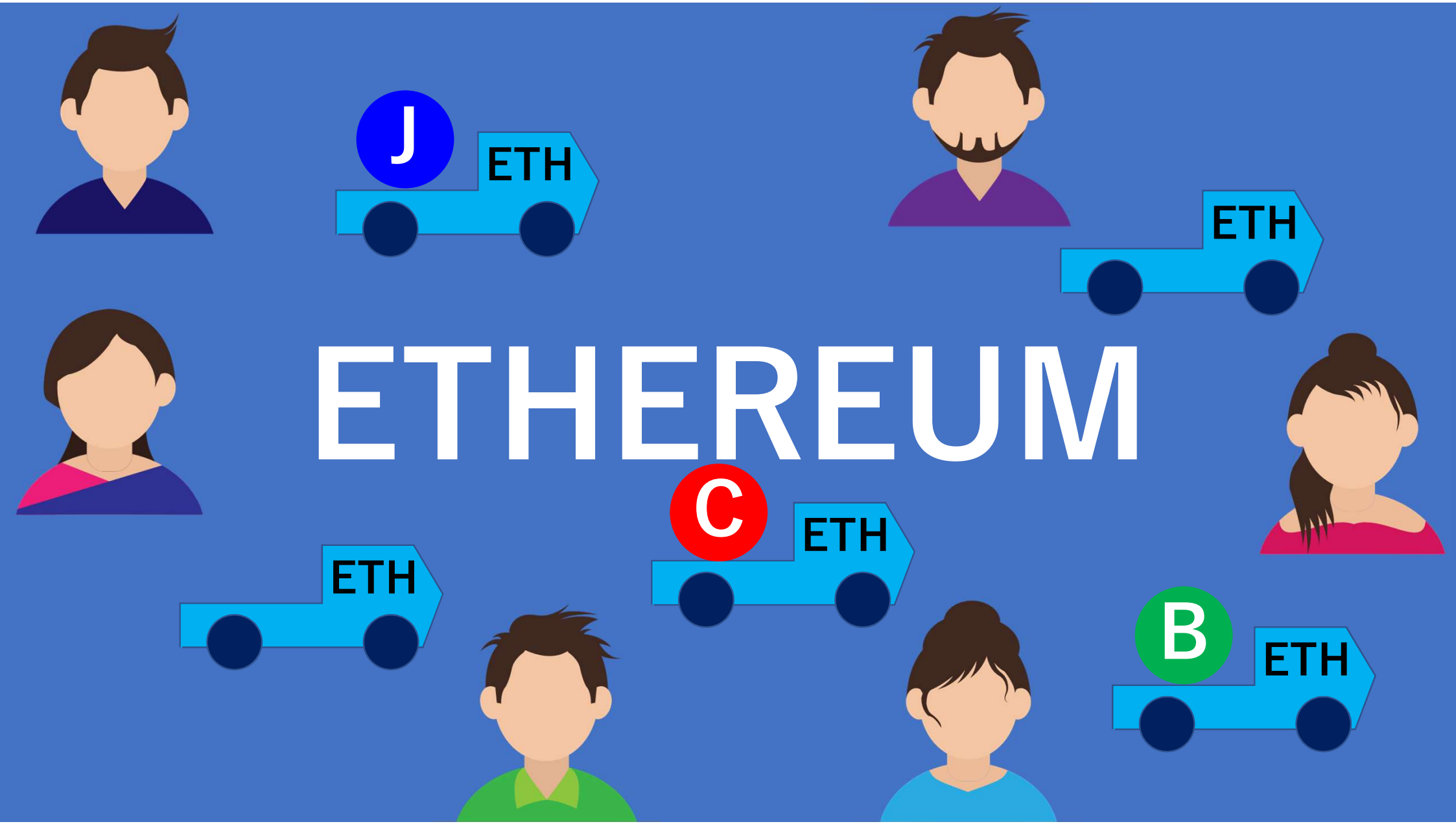
概念を共有できる

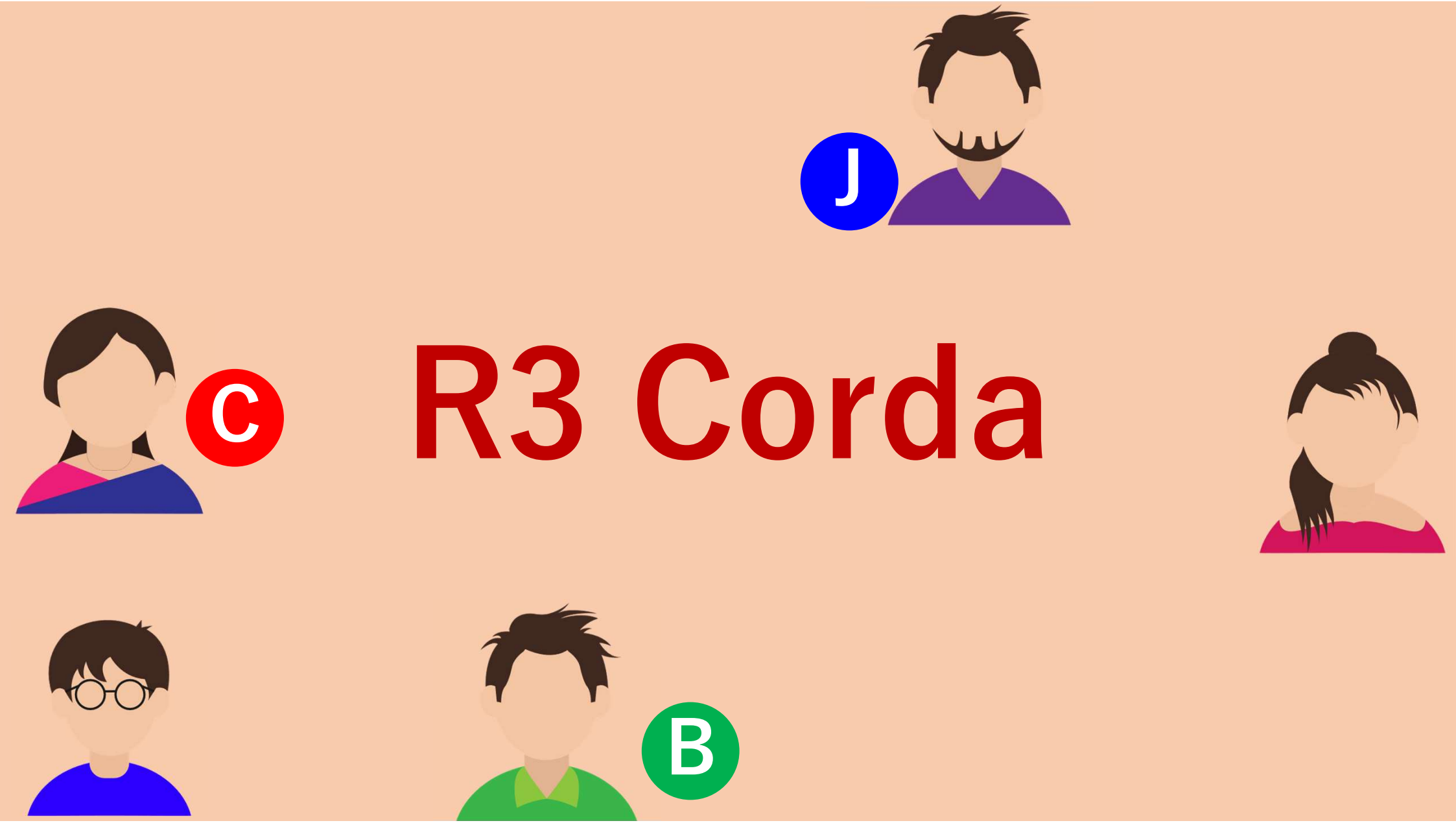
CurrencyPort

ブロックチェーンやDLTの種類がが変わっても

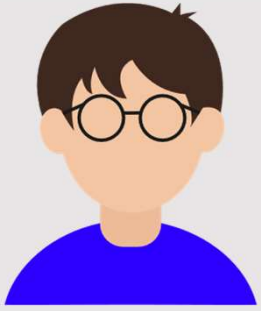
価値を共有できる


J
BTC
BITCOIN
BTC
B
BTC
C
BTC

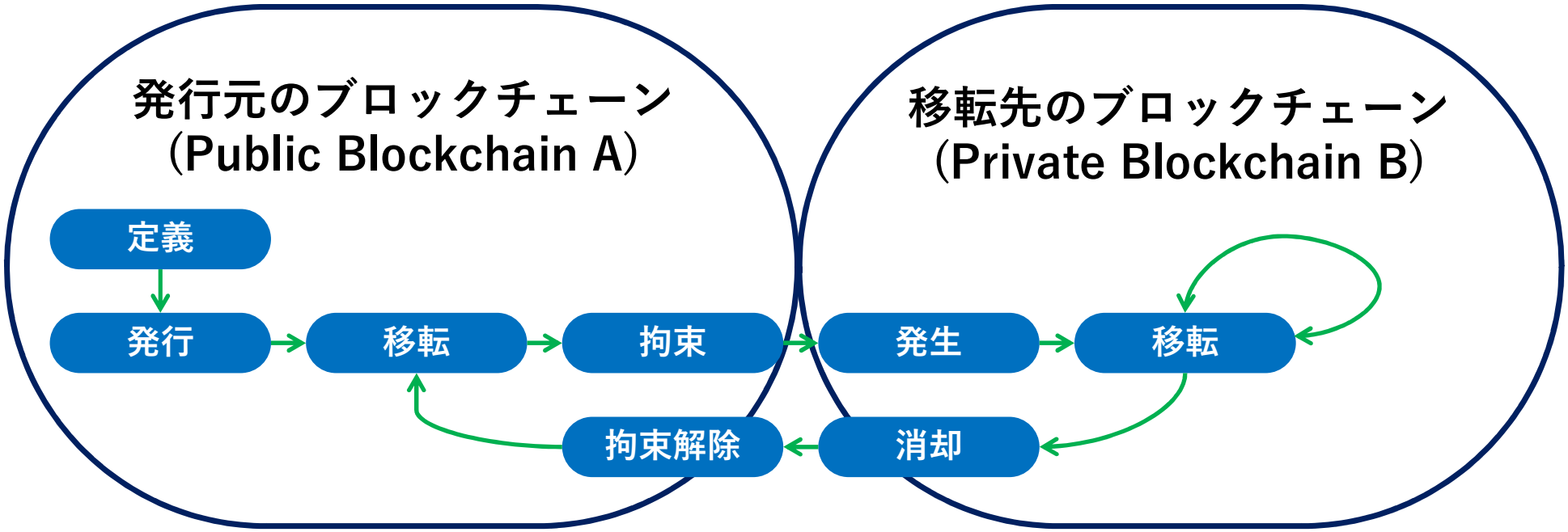

ETHEREUM
J
ETH
ETH
C
ETH
ETH
B
ETH


J
C
R3 Corda
B

HYPERLEDGER FABRIC



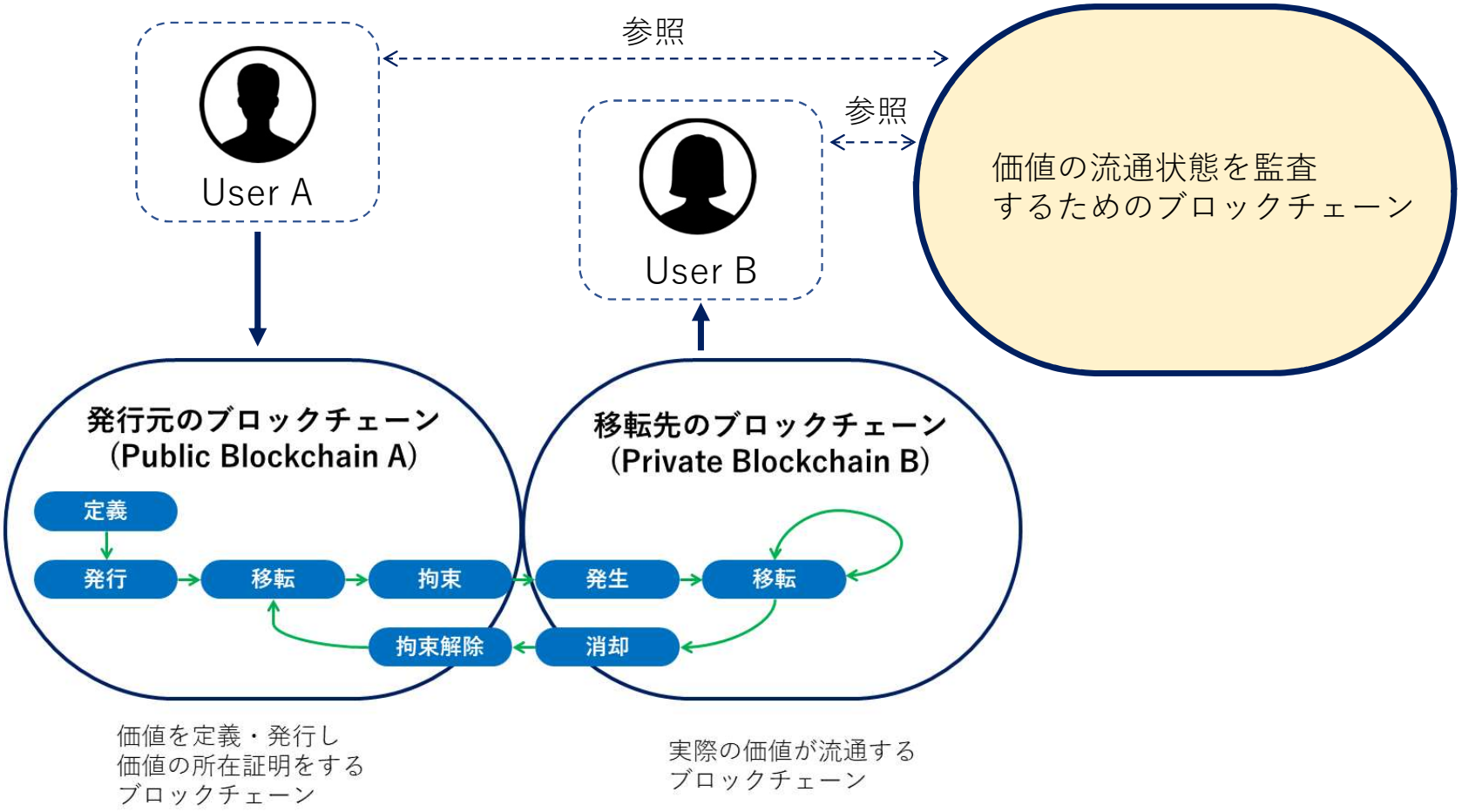
異種ブロックチェーン間相互接続に必要な機能



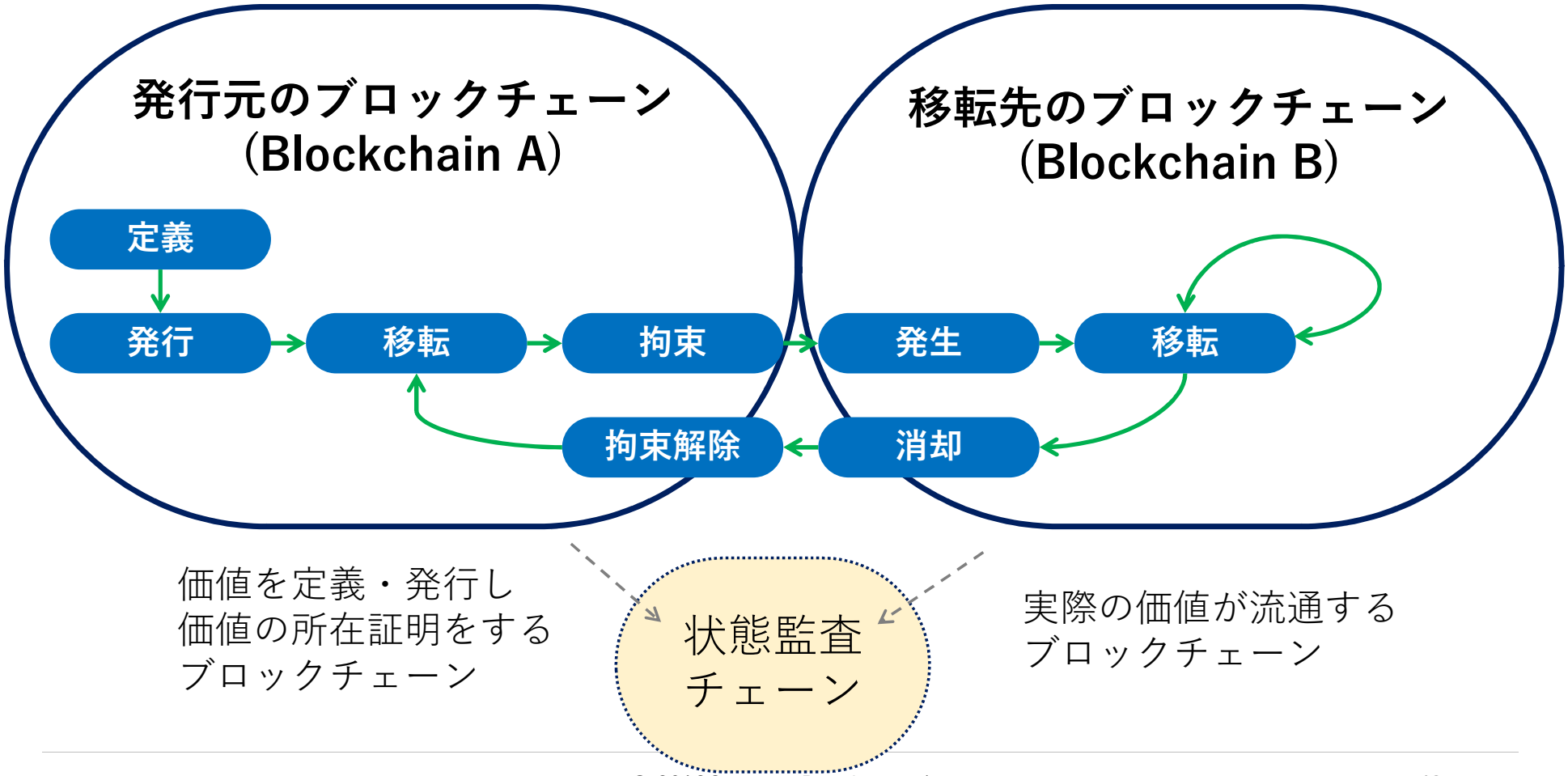
価値を定義・発行し
価値の所在証明をする
ブロックチェーン

実際の価値が流通する
ブロックチェーン

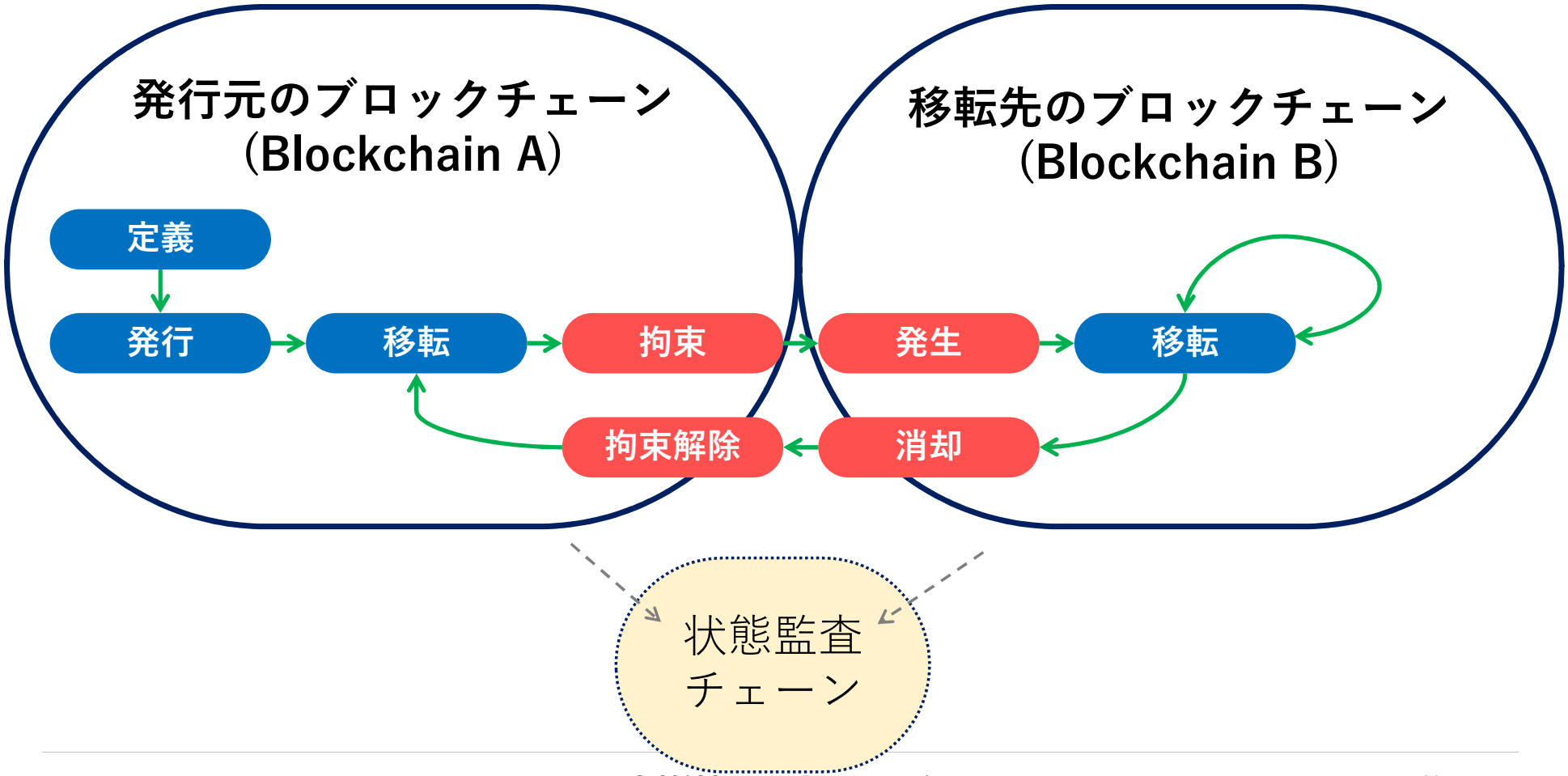
異種ブロックチェーン間相互接続の基本



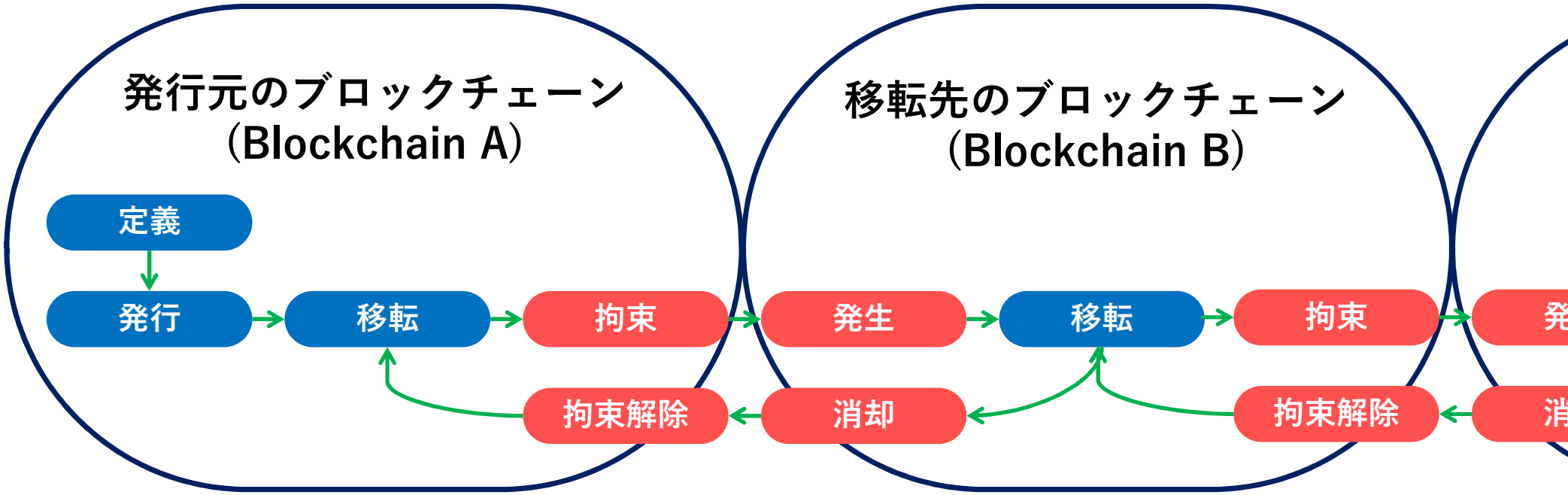
異種ブロックチェーン間相互接続に必要な機能



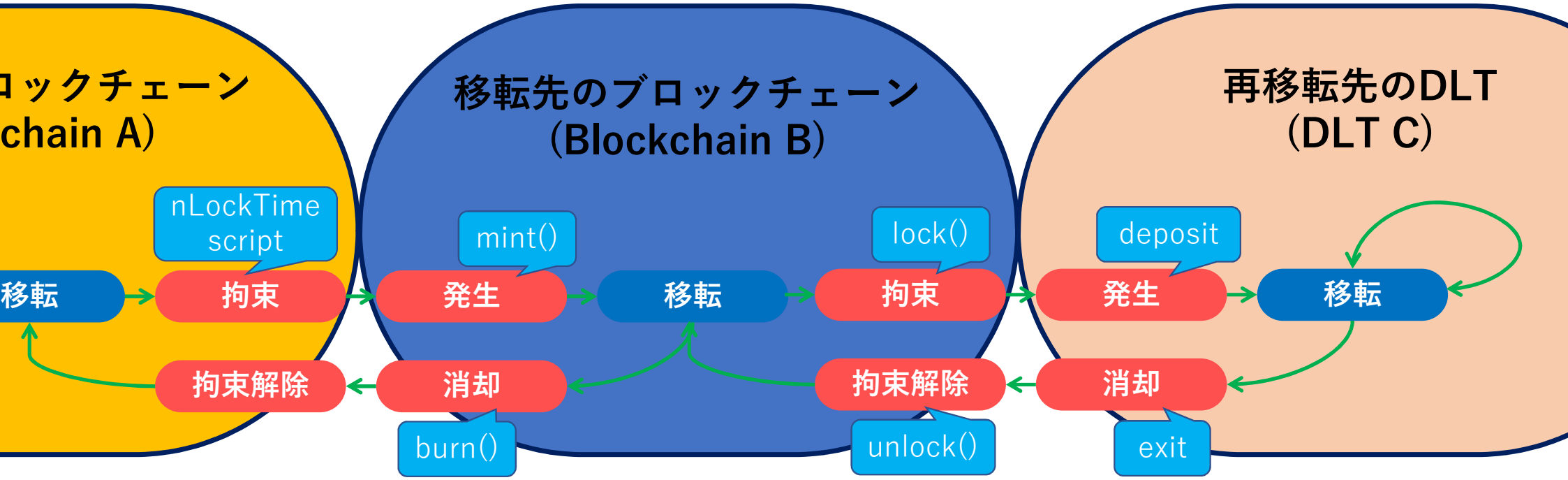
異種ブロックチェーン間相互接続に必要な機能



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

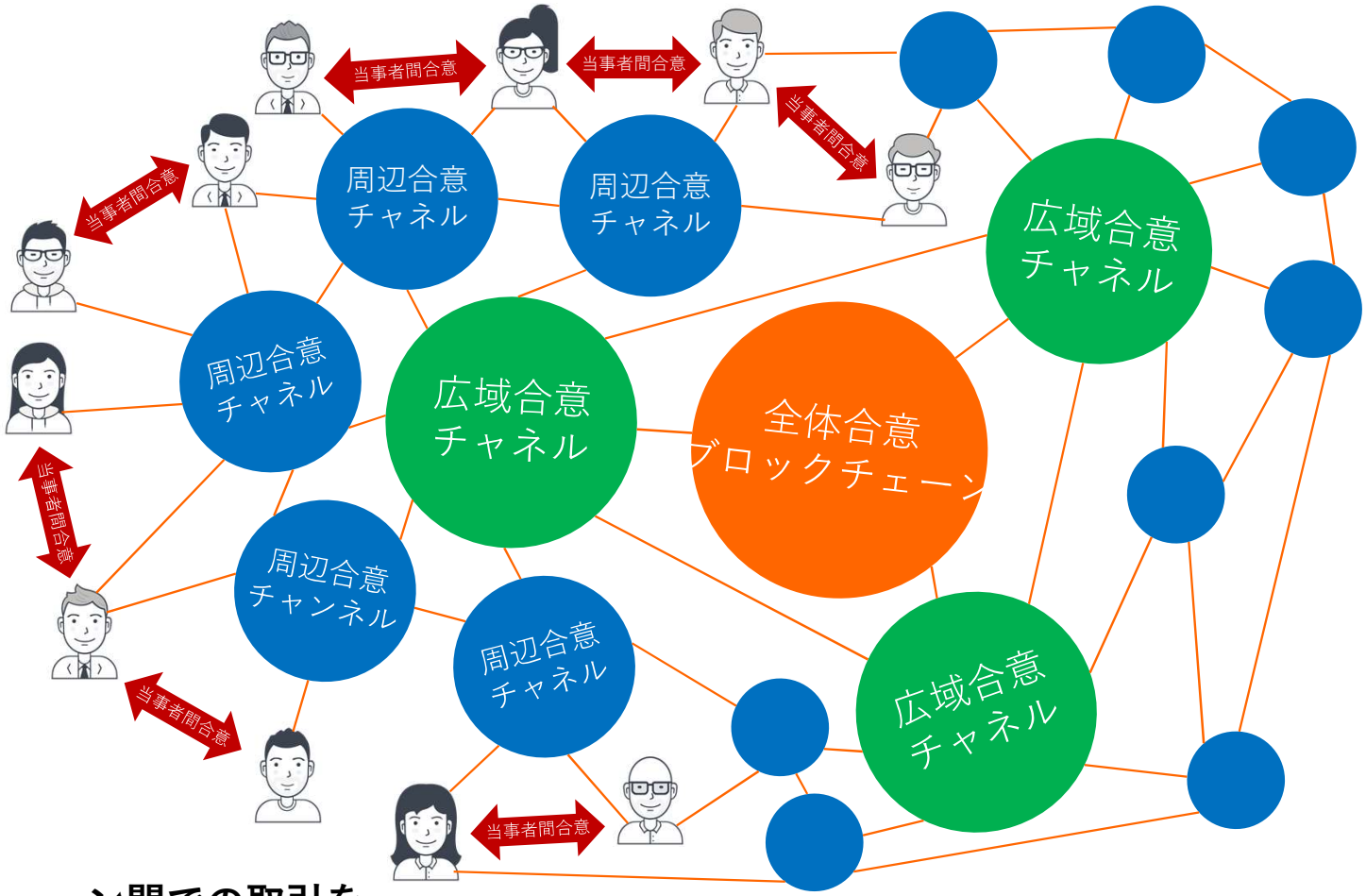


Bitcoin
(スクリプト)

Ethereum
(スマートコントラクト)

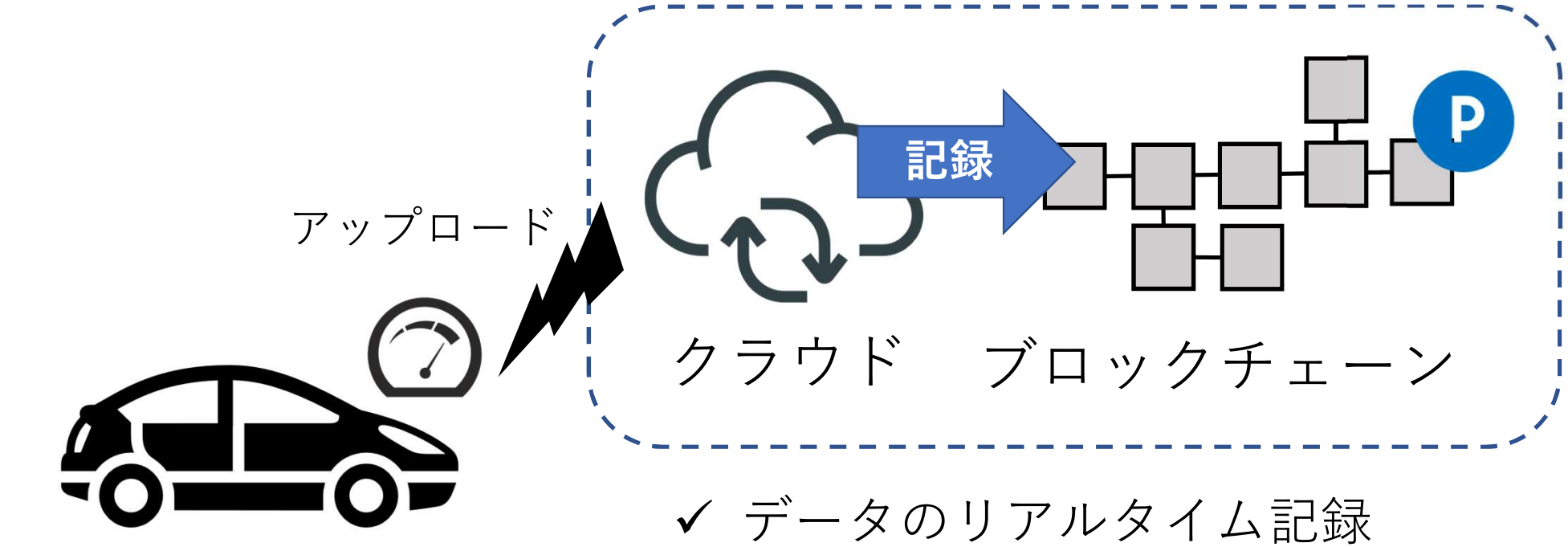
Corda
(スマートコントラクト)

多層合意ネットワークによるスループット向上効果



異種ブロックチェーン間での取引を
理論上、無限大のスループットで行う

8-6-1. 車の走行データを随時ブロックチェーン上に記録



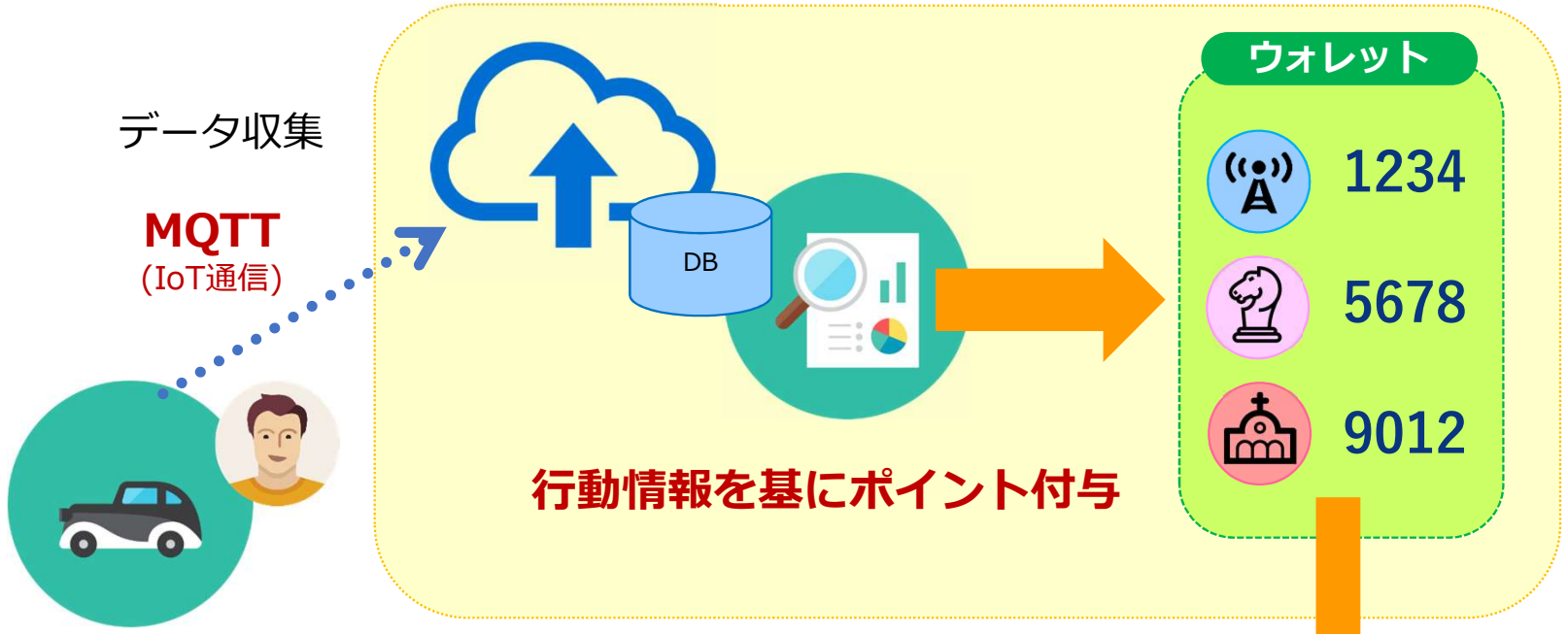
✓ データのリアルタイム記録
✓ エビデンスの真正性証明

Blockchain Collaborative Consortium

IoTを用いた行動ログ収集に基づくインセンティブ付与

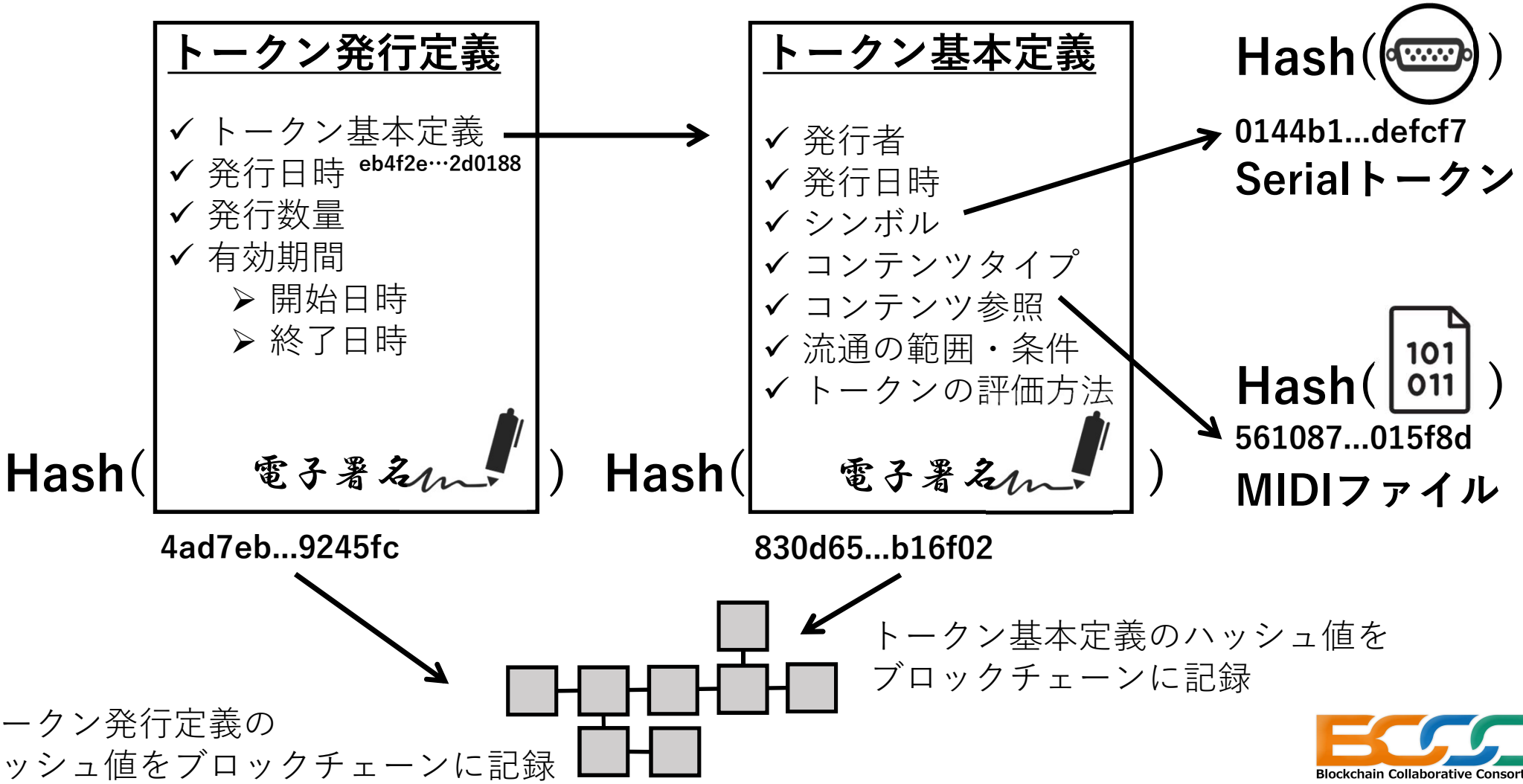
CurrencyPort

ブロックチェーンの特性を利用した「新トークンエコノミー」の創出



8-13. IoT・スマートシティ分野への応用 [a]

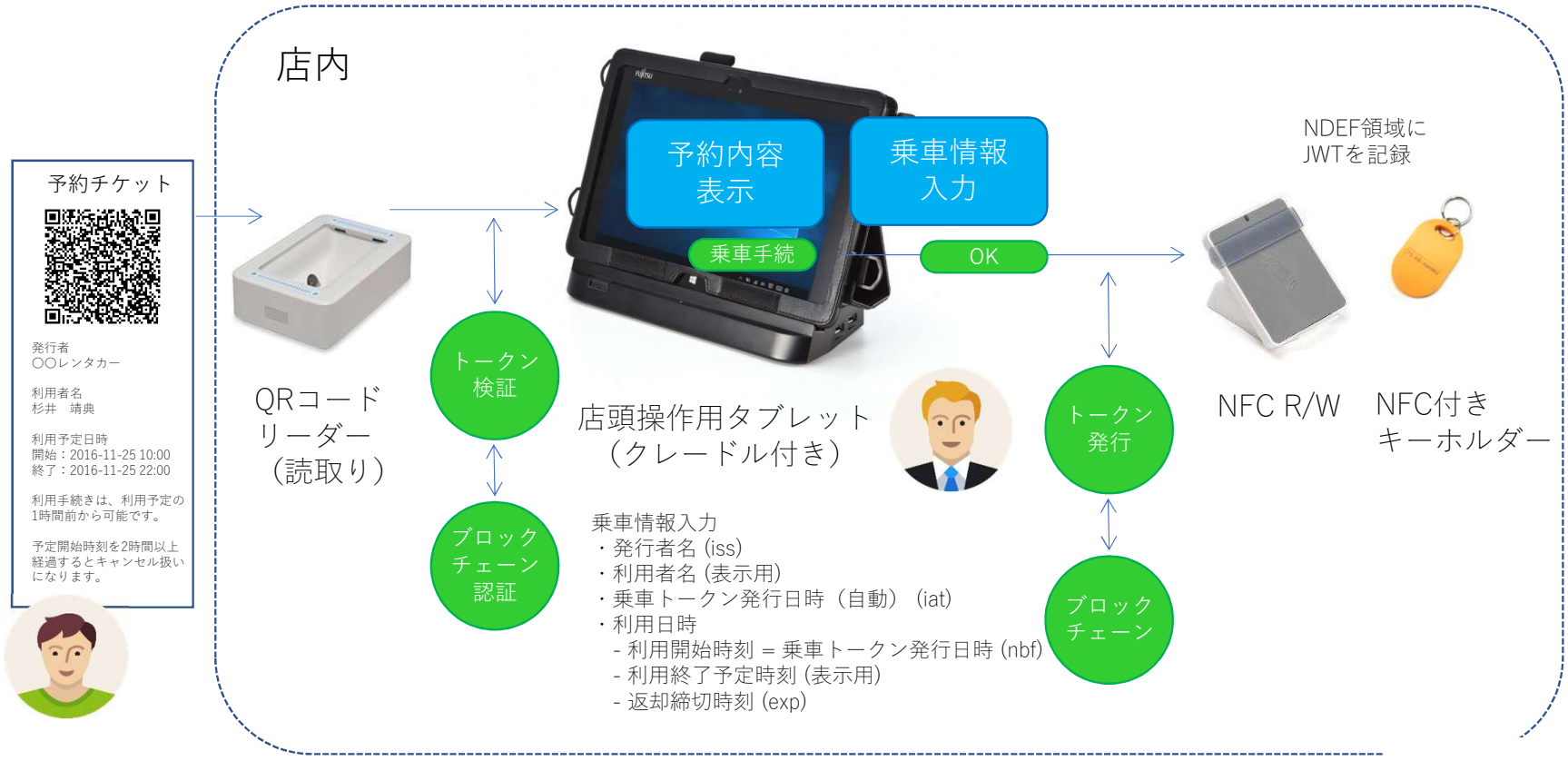
デバイス使用権をトークンでコントロールする技術



Blockchain Collaborative Consortium

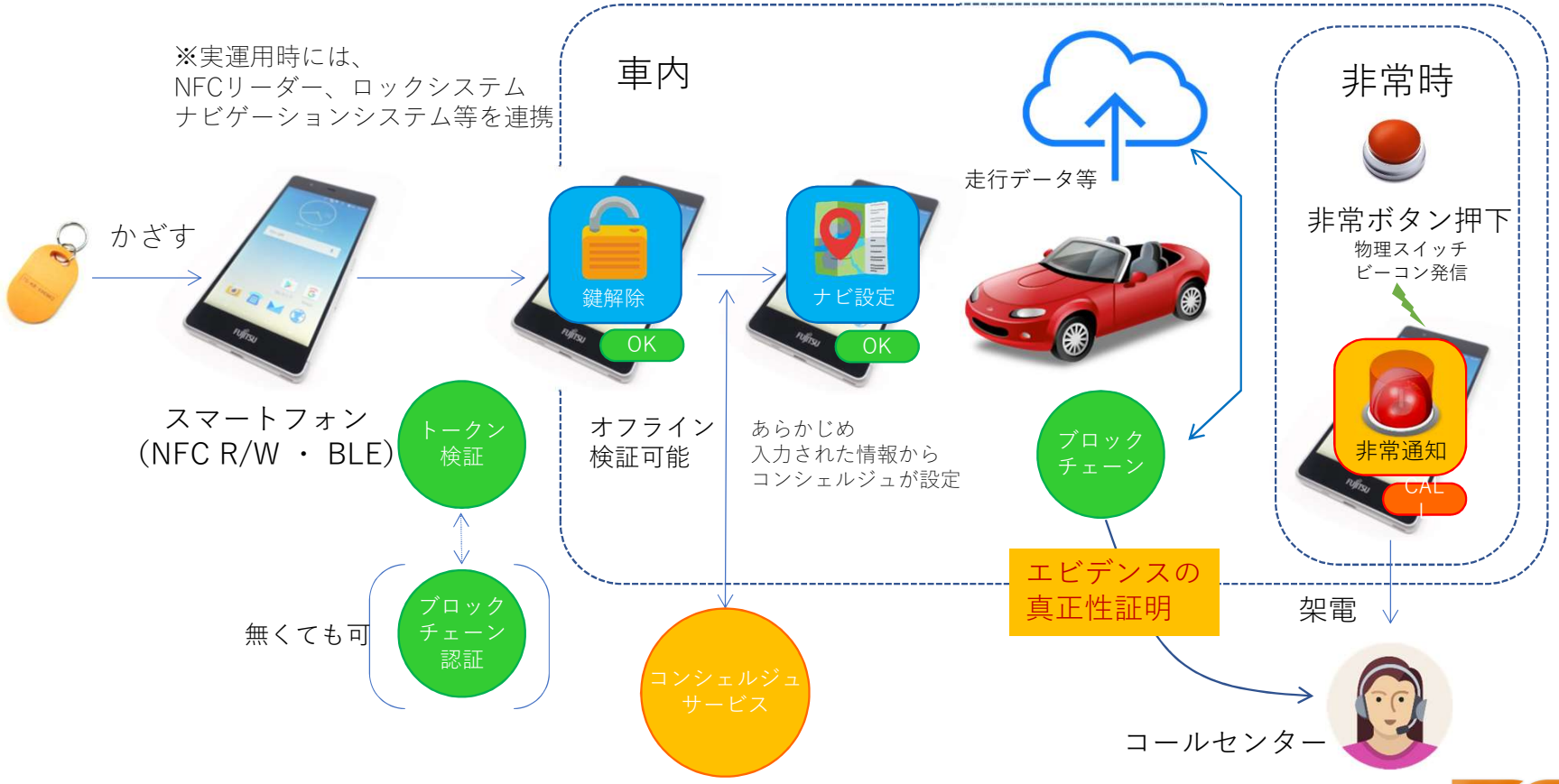
レンタカー利用時の認証、キー発行（制御）

店頭での乗車手続き。乗車トークン入りのキーを発行する



レンタカー乗車中(走行データエビデンス)・損害保険

3.車のロック解除・ルート自動登録・走行中・非常時通知（架電・エビデンス証明）

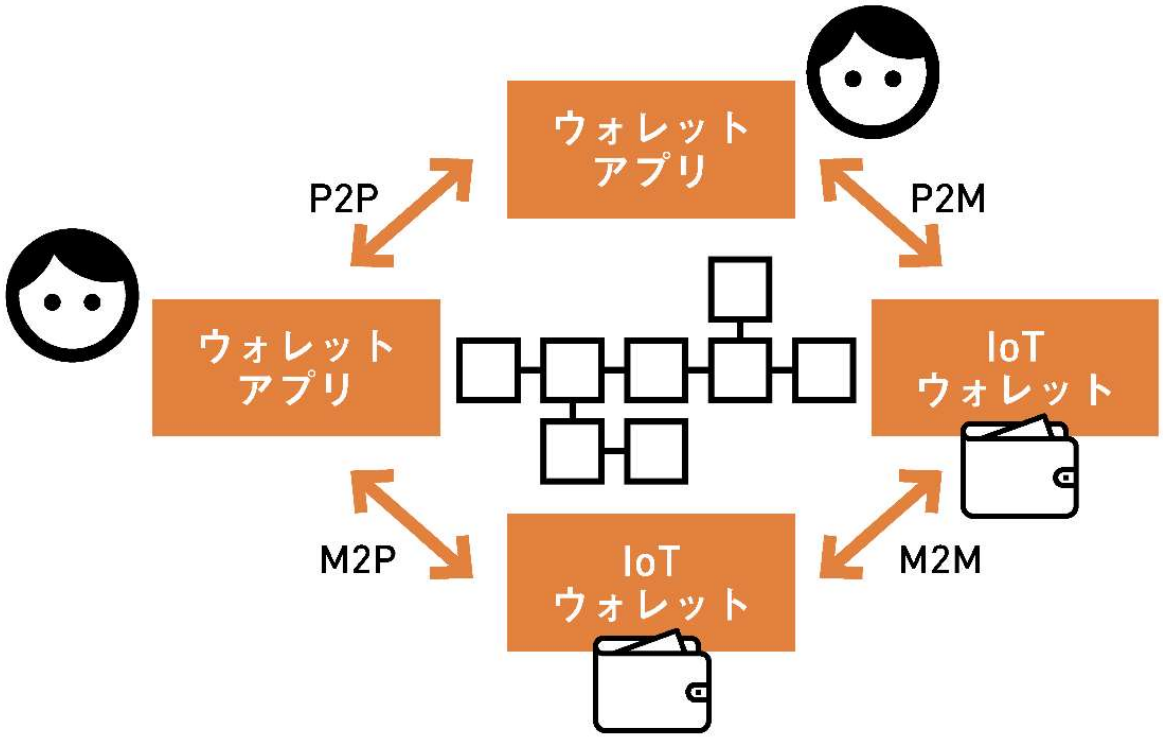


マシンがスマートコントラクトを利用するとどうなるか？

CurrencyPort

機械間自動取引

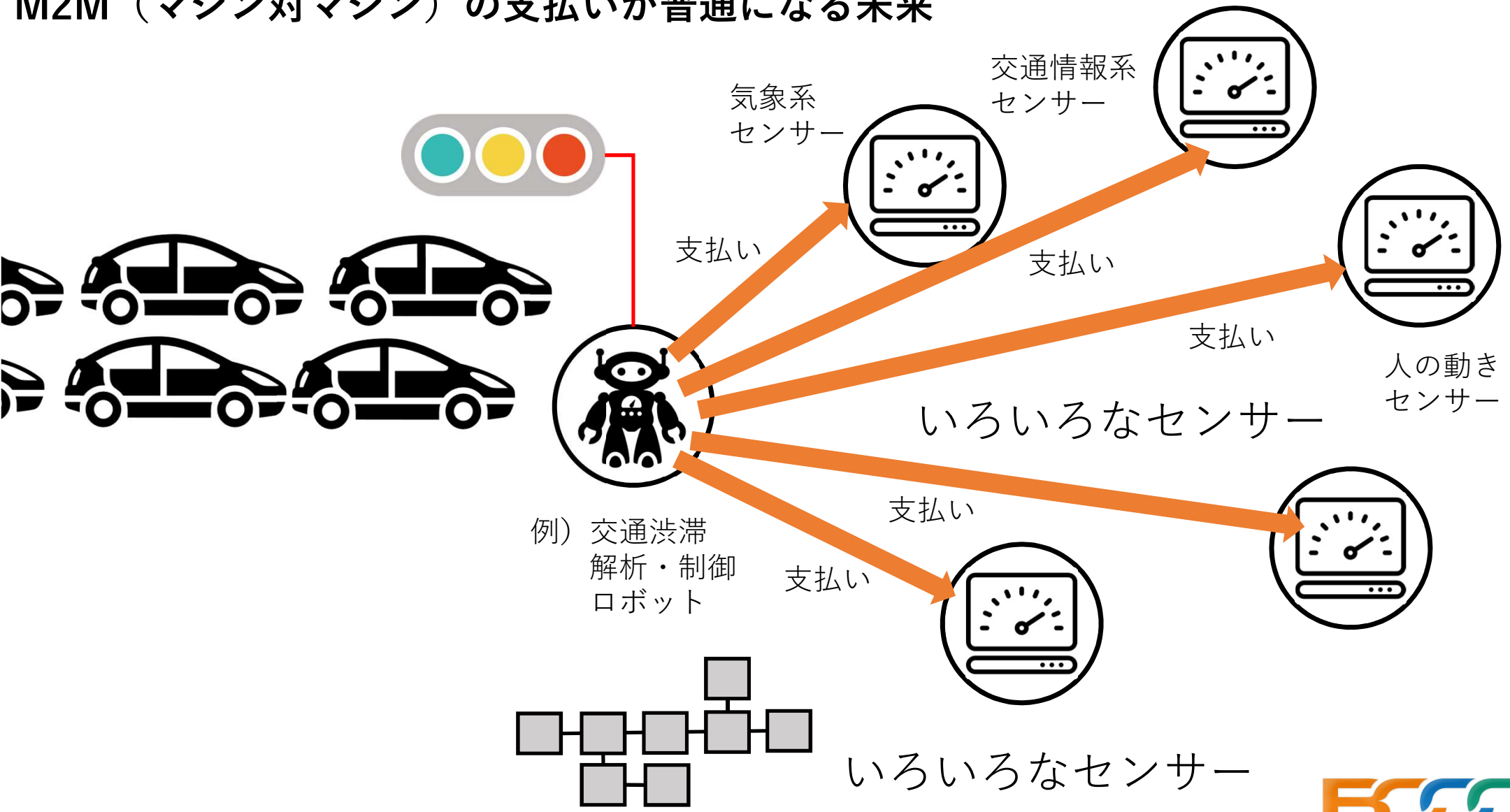
▶マシンが自律的にサービスを提供する 図表51-1



スマートコントラクトによって、P2P（People to People：人と人）だけでなく、P2M（People to Machine：人と機械）、M2M（Machine to Machine：機械と機械）の取引が当たり前になる

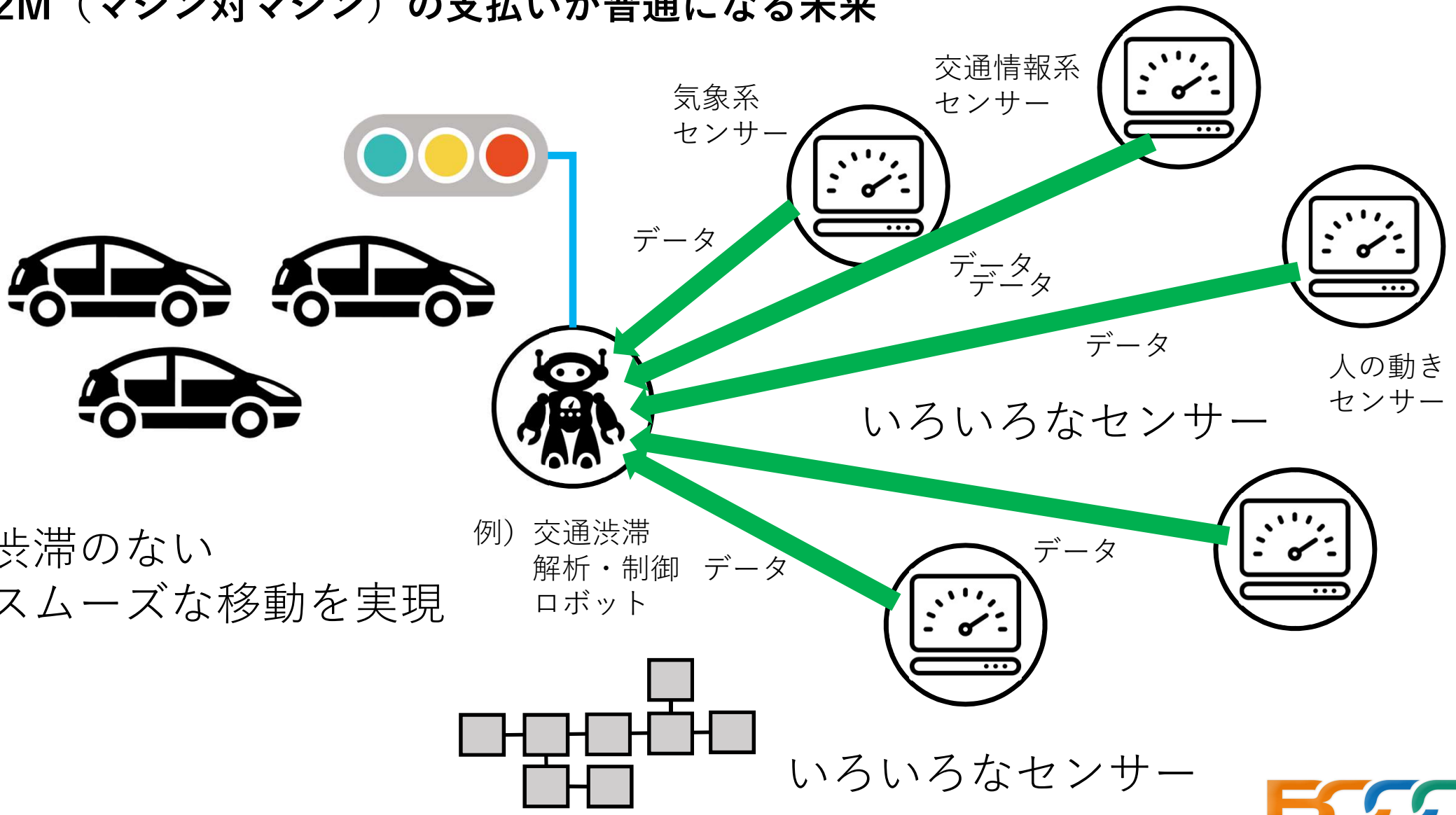
近い将来スマートコントラクトを利用する主役は、マシンになるかもしれません。

M2M（マシン対マシン）の支払いが普通になる未来



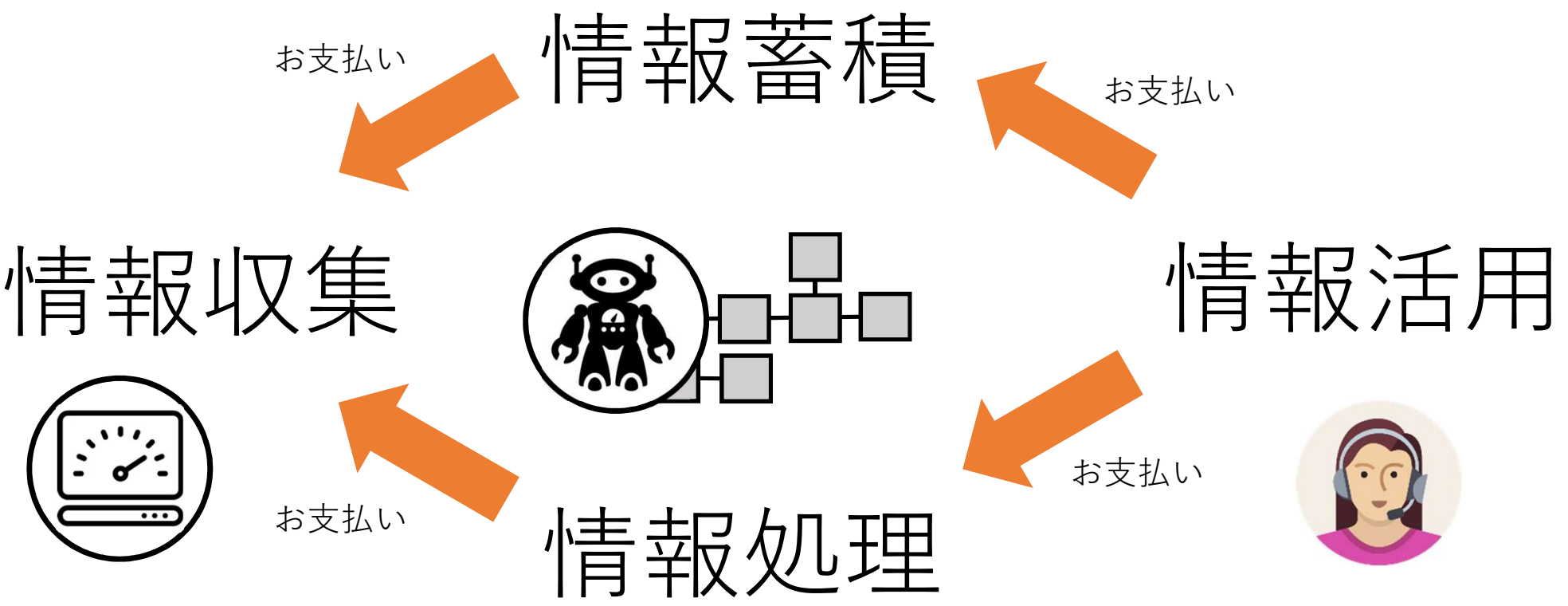
Blockchain Collaborative Consortium

M2M（マシン対マシン）の支払いが普通になる未来



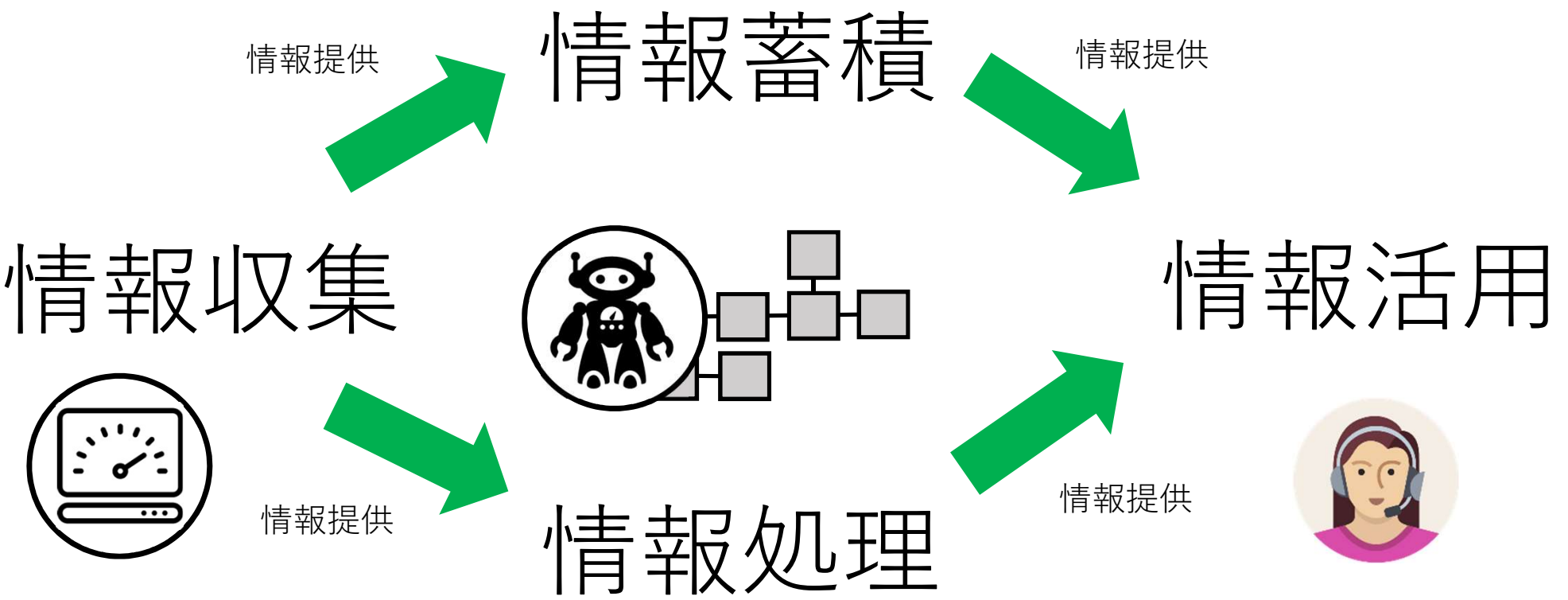
Blockchain Collaborative Consortium

スマートシティ・IoT「自律分散差社会」のエコシステム



Blockchain Collaborative Consortium

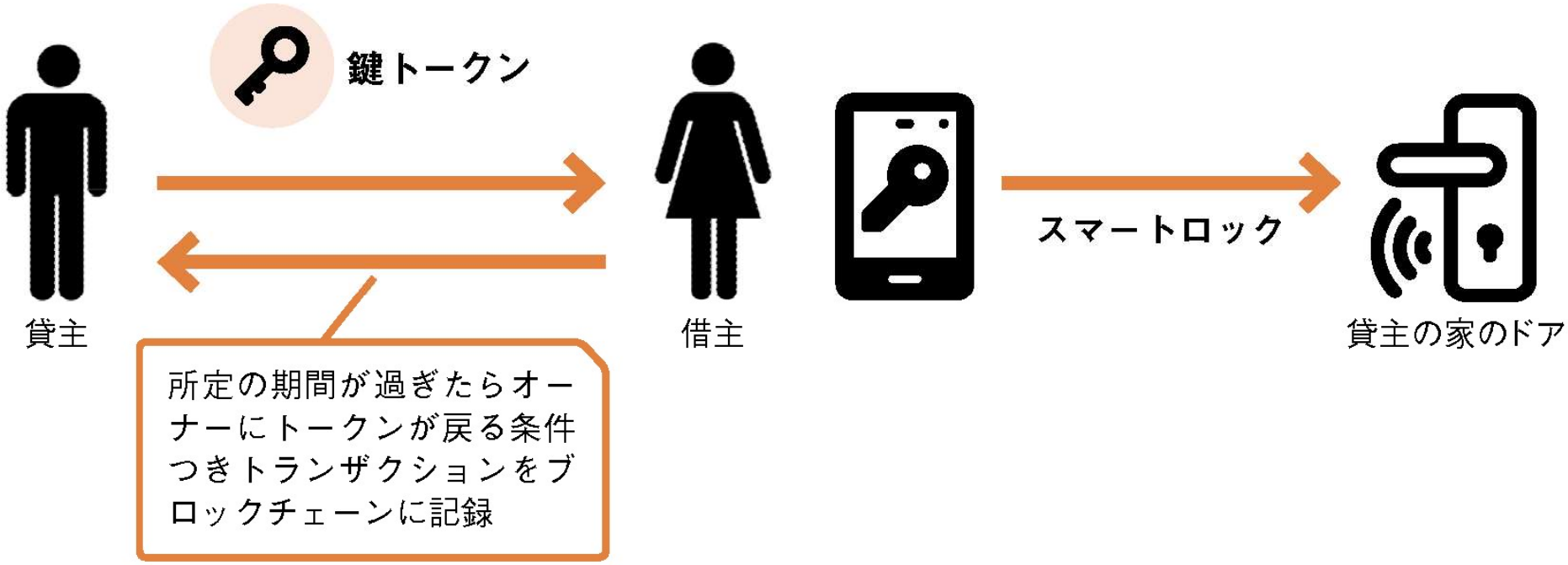
スマートシティ・IoT「自律分散差社会」のエコシステム



Blockchain Collaborative Consortium

スマートコントラクトを
シェアリングエコノミーに応用する

▶シェアリングエコノミーへの応用イメージ 図表65-1



たとえば民泊の場合、「部屋の鍵を開ける権利」をトークンに持たせることができる

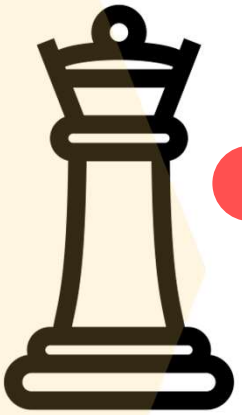
広告・販売促進への応用

モノに情報を付与できるLED照明技術（富士通）＋ 電子通貨配布技術（当社）

現地に行かないともらえないコイン

光に埋め込まれた
（人の目に見えない）

モニュメントID情報



モニュメント

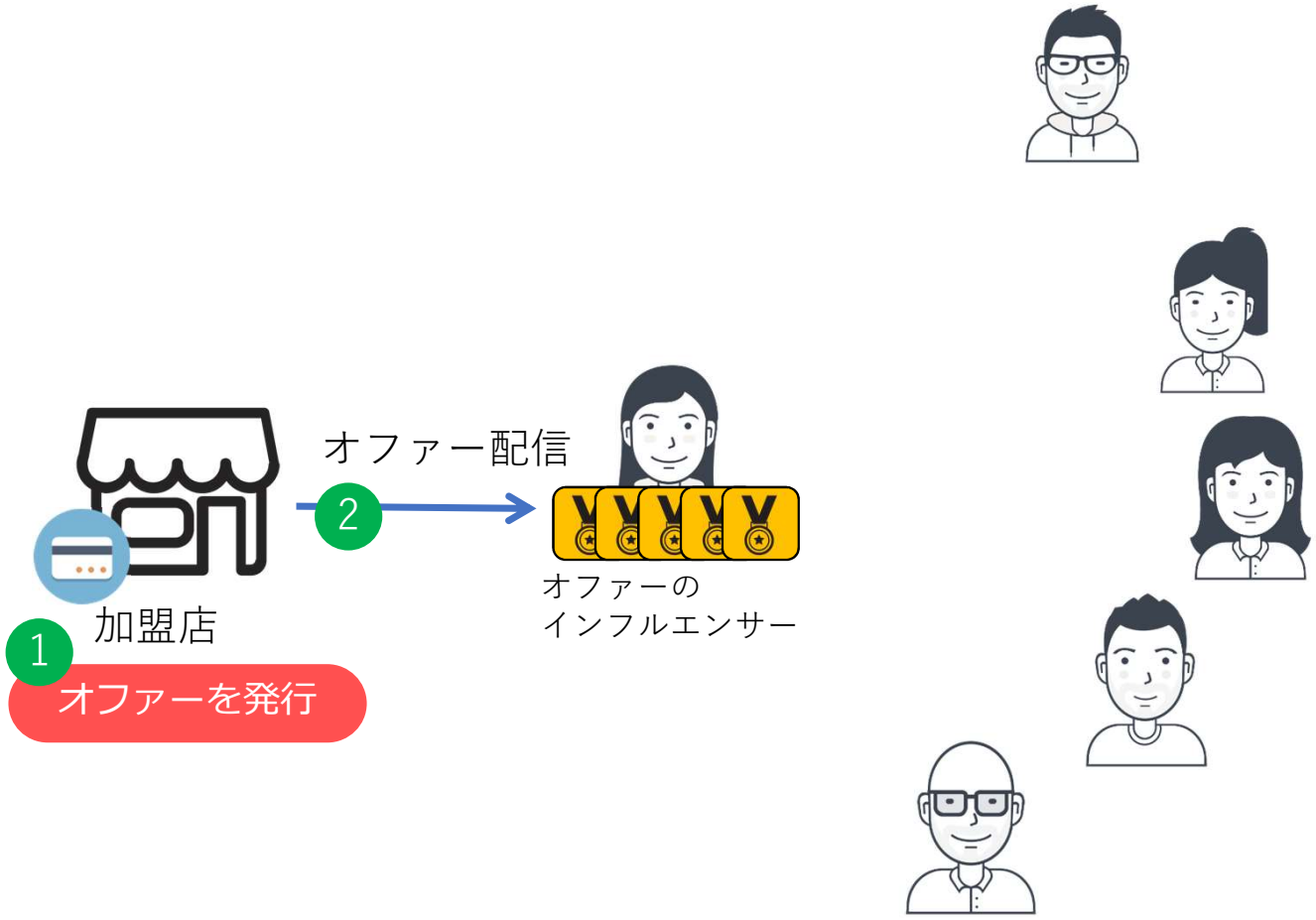
不思議感

FUJITSU ✖ CurrencyPort

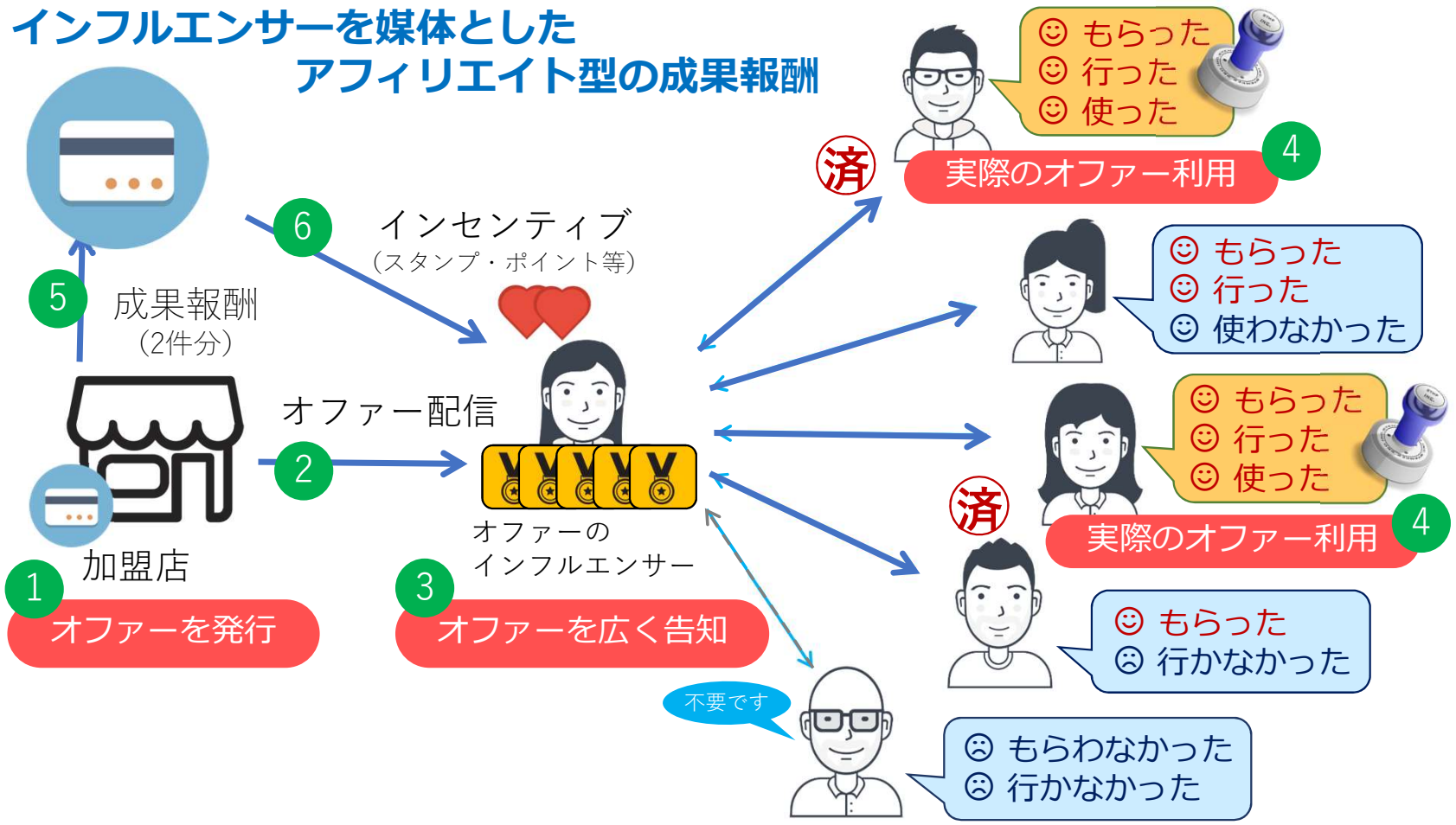
ID（アドレス）
入力方式の改善

モニュメントを撮影するだけで

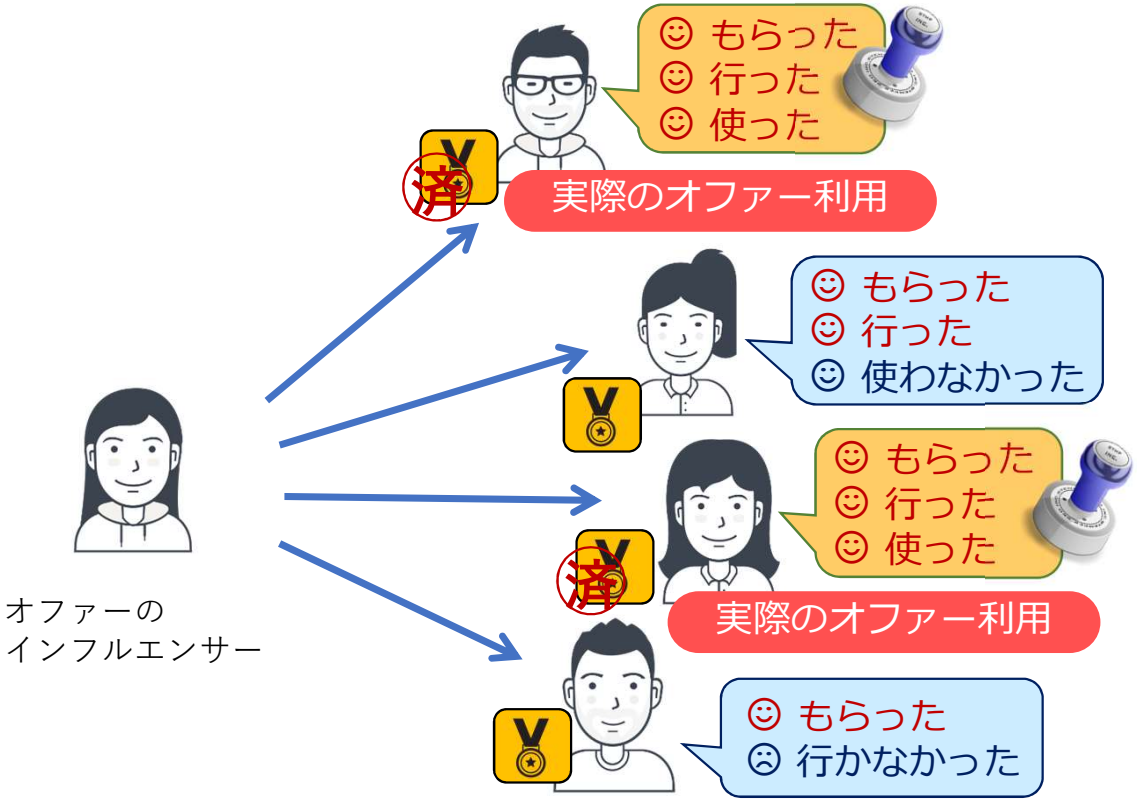
オファーの拡散方法とインセンティブ



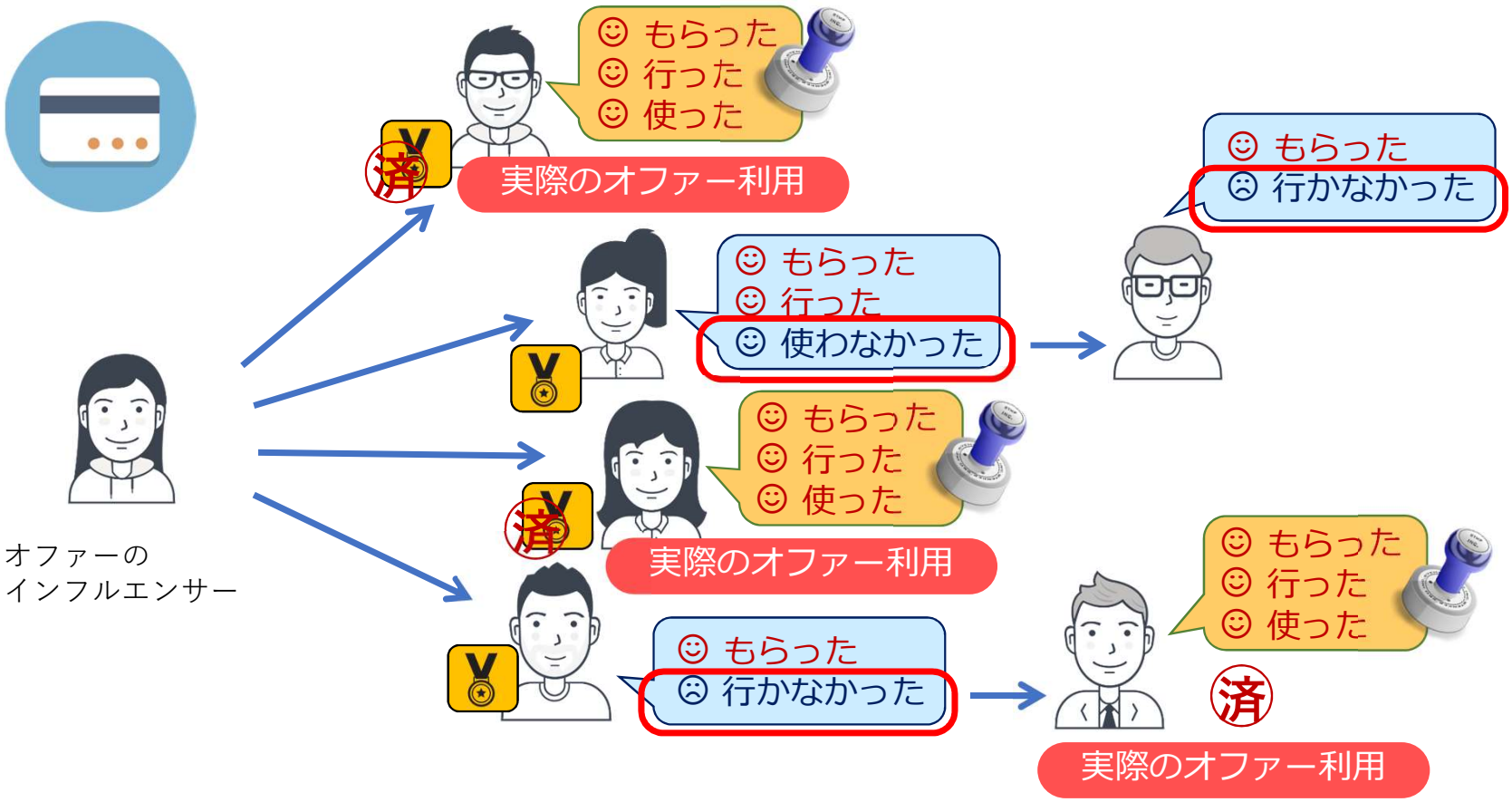
オファーの拡散方法とインセンティブ



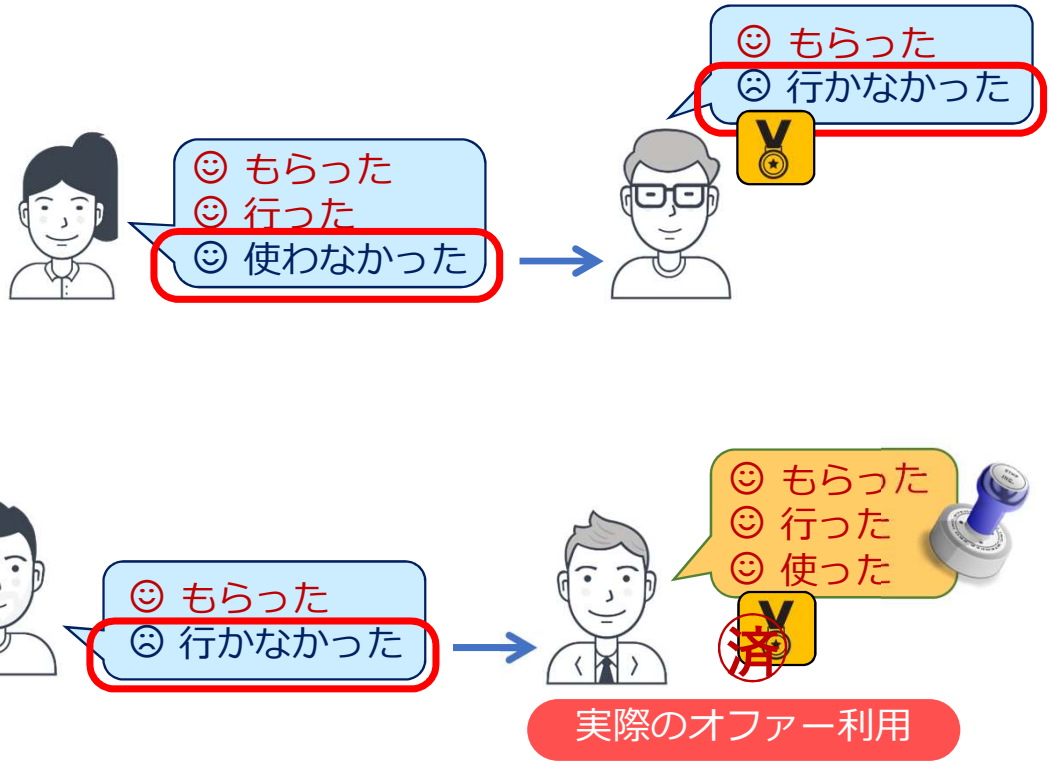
未使用のオファーは転々流通させることができる



未使用のオファーは転々流通させることができる

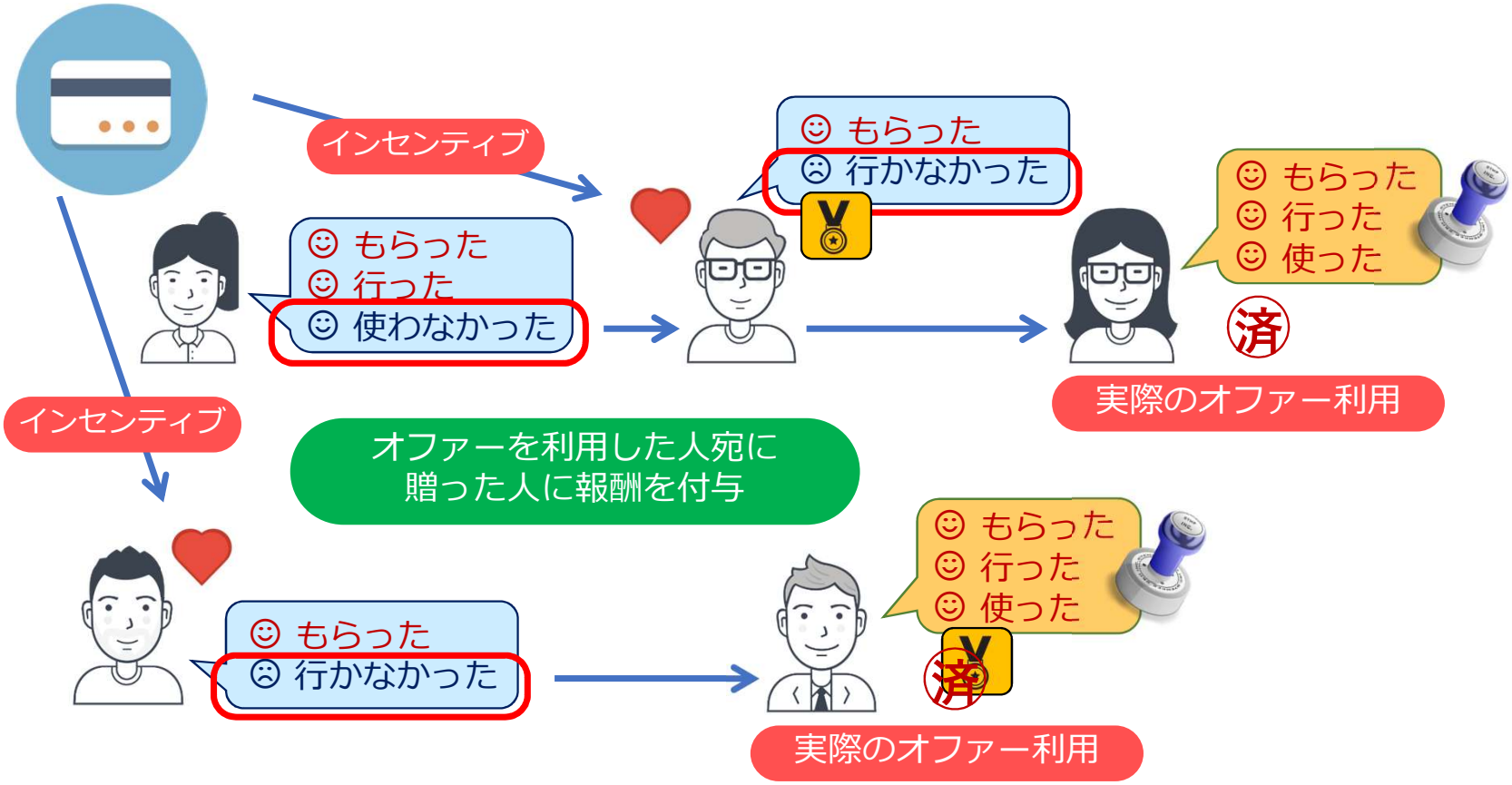


未使用のオファーは転々流通させることができる



オファーの転々流通を促す追跡型インセンティブ

自分で利用しないオファーは、使ってもらえそうな人に贈るとお得に！



期待できる効果

仮想通貨技術を応用したオファー転送によって

- ✓ 本当にクーポンを利用したい人にオファーが到達する
- ✓ オファーの利用率向上が見込める
- ✓ オファーの転々流通ぐあいを可視化して追跡できる

  ⇒ **マーケティング施策に利用可能**

- ✓ JCBカードを持っていない潜在層にもリーチする

見方を替えれば、仮想通貨技術をそのまま使っていろいろできる。

CurrencyPort

ブロックチェーンの特性を利用した「新トークンエコノミー」の創出