CurrencyPort

ブロックチェーンの社会実装における課題と対策

2018年7月25日

カレンシーポート株式会社
代表取締役・CEO　杉井　靖典

講演者プロフィール

カレンシーポート株式会社 - CurrencyPort Limited

◆有識者委員等

・経済産業省	ブロックチェーン検討会	委員
	システム評価軸整備検討委員会	委員
・特許庁	特許出願技術動向調査	委員
・日本銀行	決済システムフォーラム	プレゼンター
	FinTechフォーラム	プレゼンター
・全国銀行協会	ブロックチェーン活用可能性検討会	委員
	ブロックチェーン研究会	メンバー

その他、各省庁内にて「ブロックチェーン」「分散台帳技術」関連の勉強会に招聘

◆業界団体

ブロックチェーン推進協会（BCCC）副代表理事

日本ブロックチェーン協会（JBA）理事

FinTech協会　会員

◆執筆

「いちばんやさしいブロックチェーンの教本」

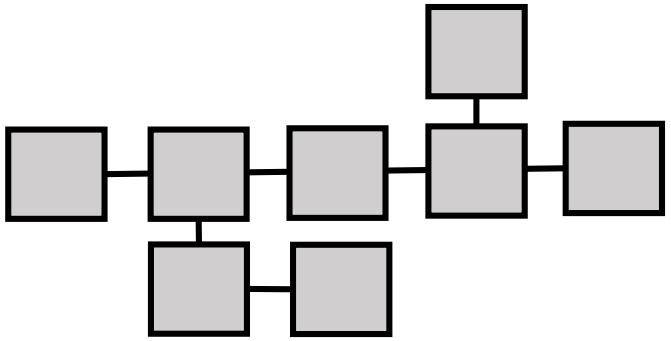
「ブロックチェーンの衝撃」（4章）

「ブロックチェーン＆ビットコイン入門編」（寄稿）　その他、メディア掲載実績多数

ブロックチェーンとは

CurrencyPort

少し前の事実（概ね１時間程度以上）を未来永劫保証するサービス



実は、Paymentサービスはブロックチェーン向きではない
逆に言えば、１時間未満の取引リスクを保証する保険や、
オフチェーンレイヤーのサブシステムなどと組合わせる。

１時間程度待っても構わない取引には、非常に強力な
取引事実証明、存在証明（契約書や特許の期日）
事実否認防止、情報追跡が可能。

トレーサビリティを実現するトランザクション

トレーサビリティ

複数圃場から獲れた北海道産たまねぎを
出荷センターに集約して同梱するUTXOモデル

INPUT	OUTPUT
圃場A（北見）のたまねぎ	北海道産たまねぎ
60Kg	**100kg**
圃場B（富良野）のたまねぎ	
30Kg	
圃場C（札幌）のたまねぎ	
10Kg	

北海道産たまねぎを仕入れして
チェーン店各小売店舗宛てに振分ける

INPUT	OUTPUT
北海道産たまねぎ	スーパー〇×世田谷店
100Kg	**30Kg**
	スーパー〇×杉並店
	20kg
	スーパー〇×渋谷店
	20kg
	スーパー〇×目黒店
	10Kg
	スーパー〇×倉庫保管
	20kg

トレーサビリティを実現するトランザクション

トレーサビリティ

スーパー〇×世田谷店で北海道産玉ねぎを
5個入り（約1Kg）のパックにするUTXOモデル

INPUT	OUTPUT
北海道産のたまねぎ	北海道産たまねぎ5個入り
30Kg	**30袋**

店頭にならんだ、30袋の売れ行きに関する
UTXOモデル

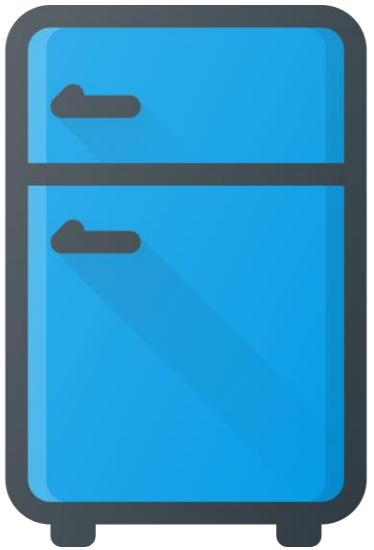
INPUT	OUTPUT
北海道産たまねぎ5個入り	安藤さん
30袋	**2袋**
	伊藤さん
	1袋
	宇藤さん
	1袋
	江藤さん
	1袋
	売れ残り在庫
	15袋

トレーサビリティを実現するトランザクション

トレーサビリティ

伊藤さんのお買い物品を冷蔵庫に入れるUTXO

INPUT	OUTPUT
北海道産たまねぎ	野菜室へたまねぎ
1袋（5個入り）	**5個**
千葉県産のにんじん	野菜室へにんじん
1袋（3本入り）	**3本**
鹿児島県産じゃがいも	野菜室へじゃがいも
1袋（6個入り）	**6個**
カナダ産のぶたにく	冷凍庫へぶたにく
800g	**800g**
△□のカレールー	食品庫へカレールー
1つ（8ブロック）	**1つ**



トレーサビリティを実現するトランザクション

トレーサビリティ

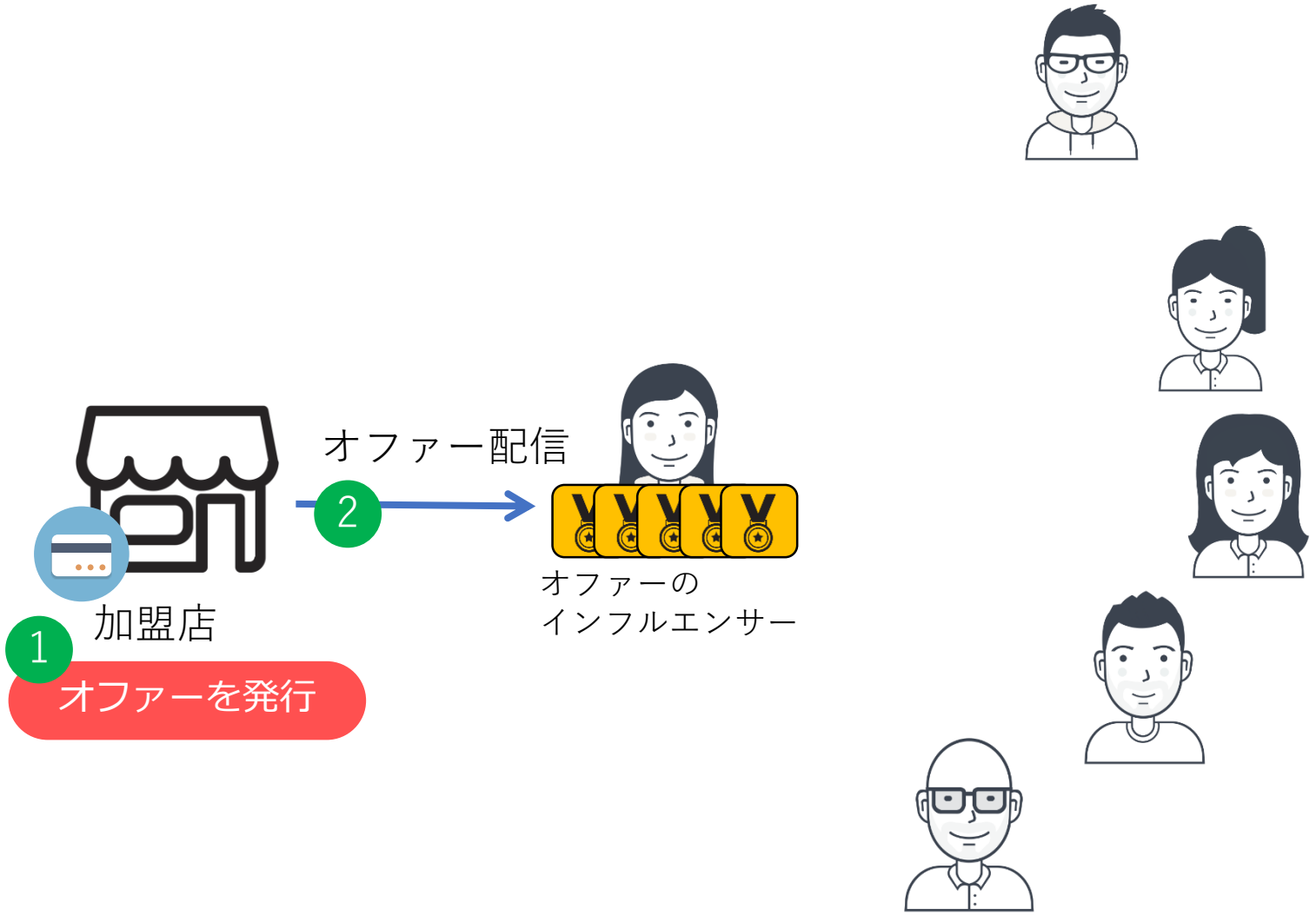
カレーを5人前つくるUTXOモデル

INPUT	OUTPUT
野菜室の たまねぎ	鍋の カレー
1個	**5人前**
野菜室の にんじん	野菜室の にんじん
1本	**0.5本**
野菜室の じゃがいも	冷蔵庫の ぶたにく
2個	**200g**
冷蔵庫の ぶたにく	食品庫の カレールー
400g	**4ブロック**
食品庫の カレールー	空中の 水蒸気
8ブロック	**50cc**
水道の 水	
500cc	

カレーを2人分をよそるUTXOモデル

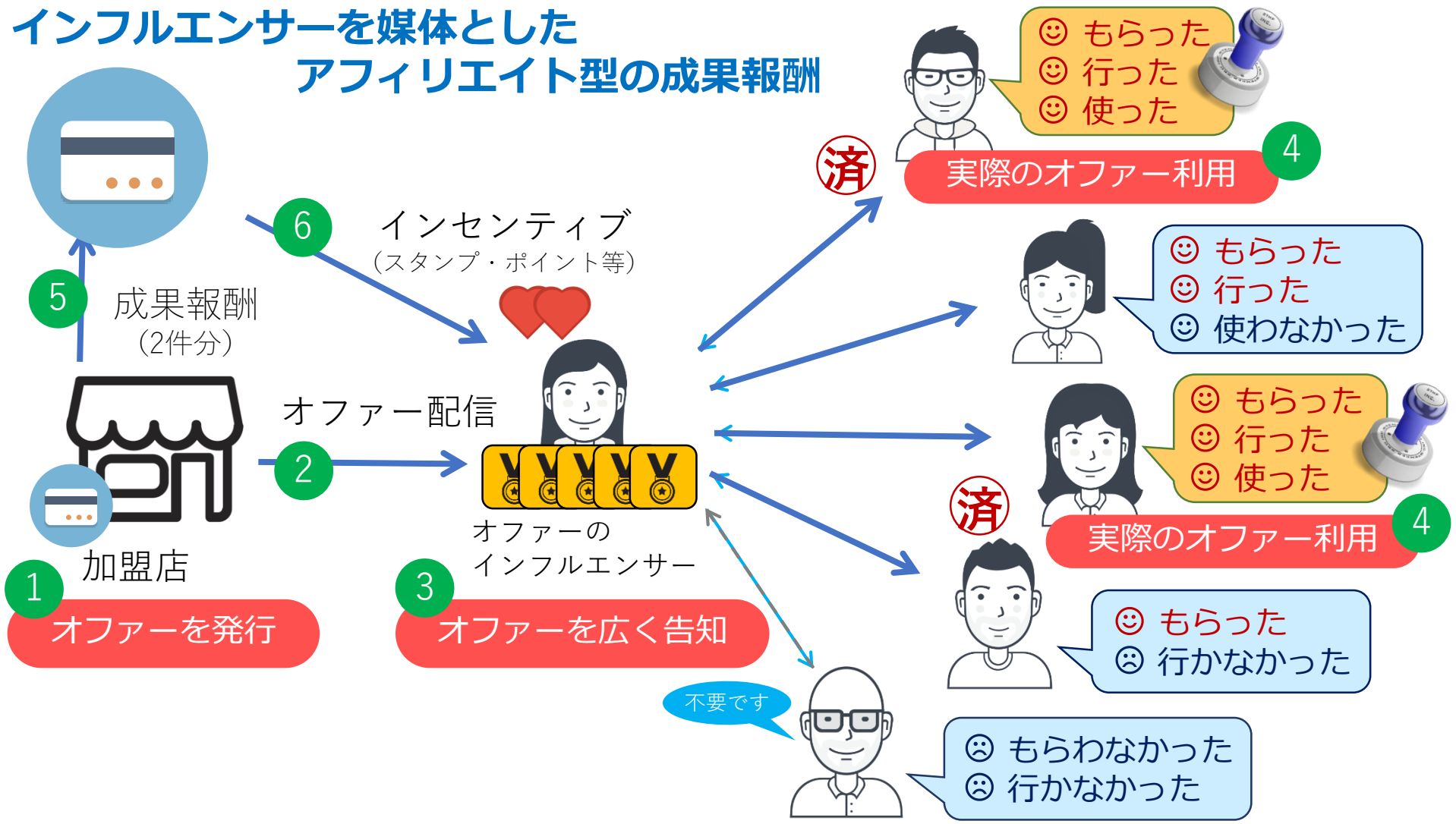
INPUT	OUTPUT
鍋の カレー	皿1の カレー
5人前	**1人前**
炊飯器の ごはん	皿2の カレー
1000g	**1人前**
	鍋の カレー
	3人前
	皿1の ごはん
	200g
	皿2の ごはん
	200g
	炊飯器の ごはん
	600g

追跡広告とインセンティブモデル

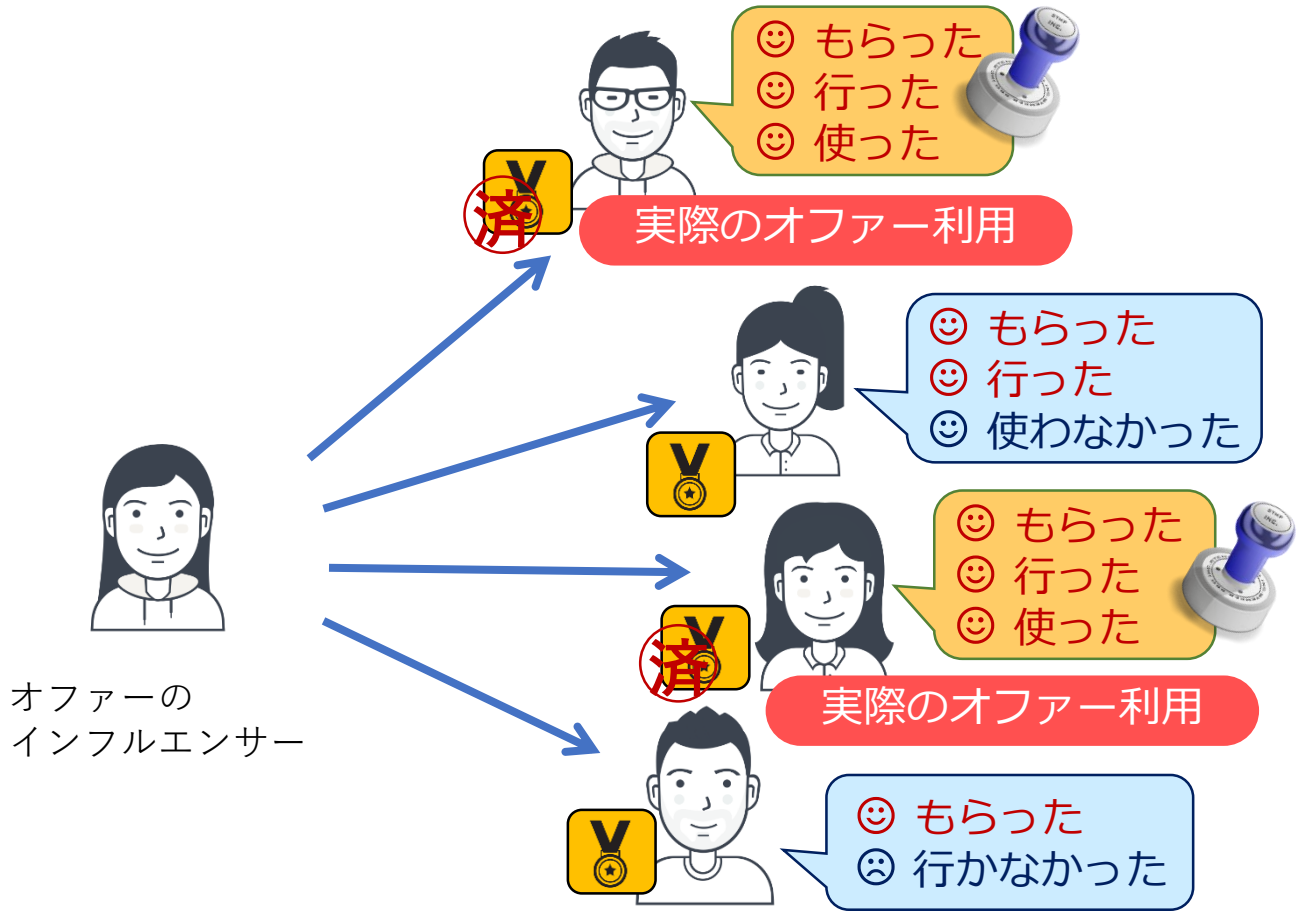


追跡広告とインセンティブモデル

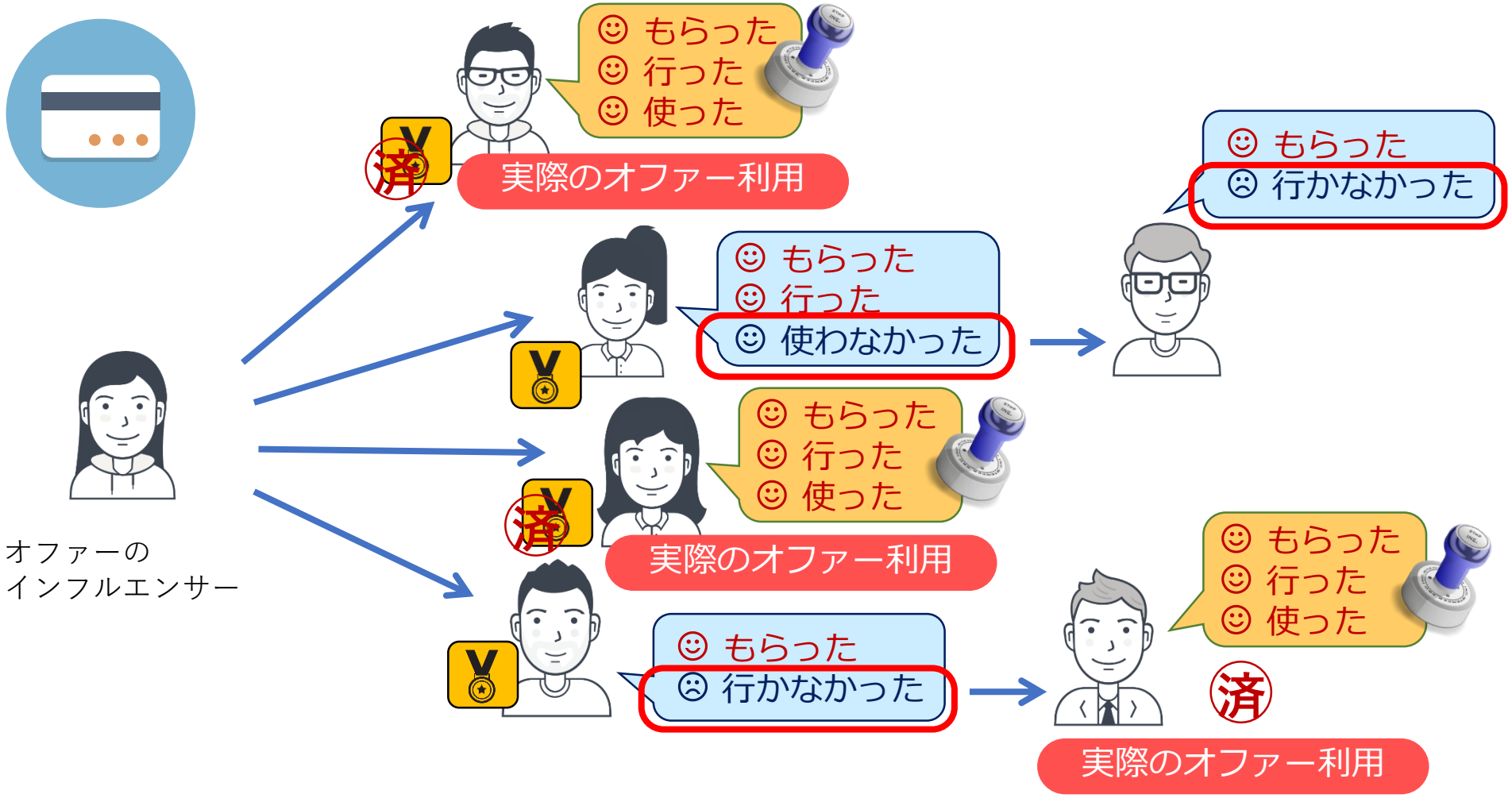
CurrencyPort



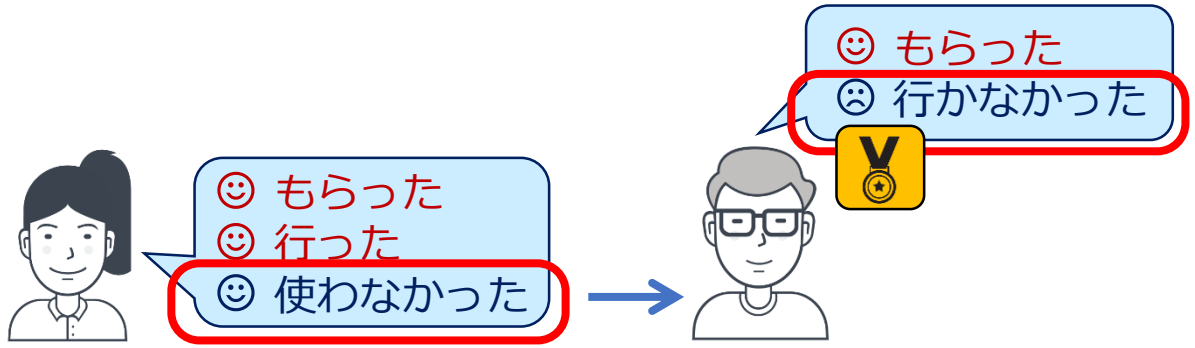
追跡広告とインセンティブモデル（オファーの転々流通）

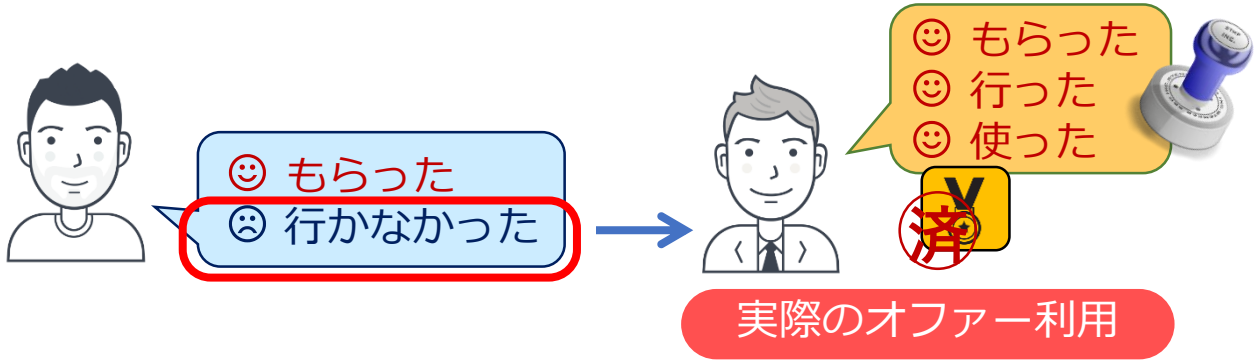


追跡広告とインセンティブモデル（オファーの転々流通）



追跡広告とインセンティブモデル（オファーの転々流通）

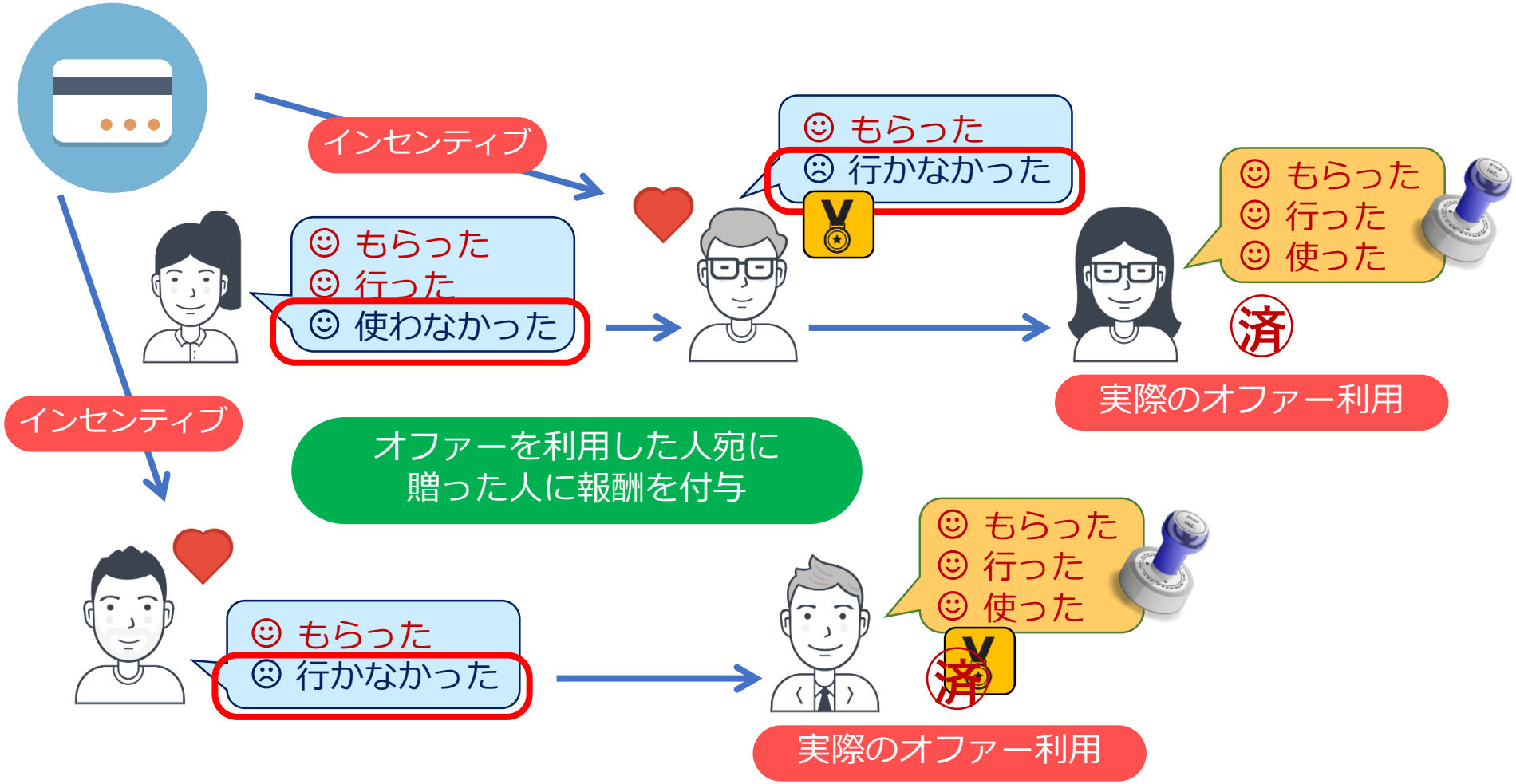




追跡広告とインセンティブモデル（オファーの転々流通）

CurrencyPort

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！



ブロックチェーンの社会実装における課題

CurrencyPort

1．世界規模取引に向けた拡張性

2．異種ブロックチェーン間の相互運用性

3．ルーズな運用にも耐えるセキュリティ

スケーラビリティ

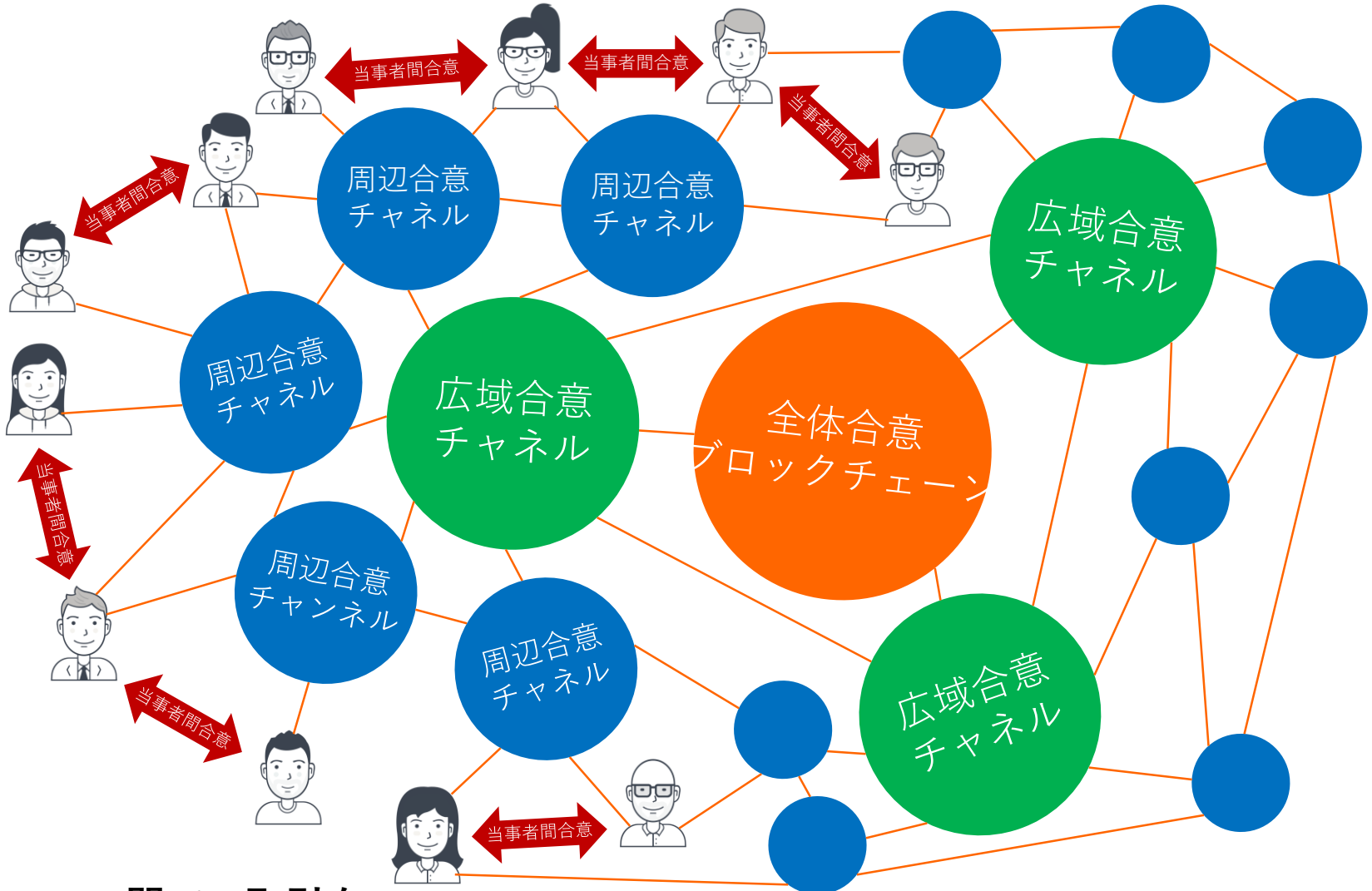
世界規模取引に向けた拡張性

CurrencyPort

ブロックチェーンのスケーラビリティ議論の方向性

1. ブロックサイズを拡大する（ビッグブロック）
2. 層を重ねる（セカンドレイヤー）
3. 横に広げる（サイドチェーン、インターオペラビリティ）

多層合意ネットワークによるスループット向上効果



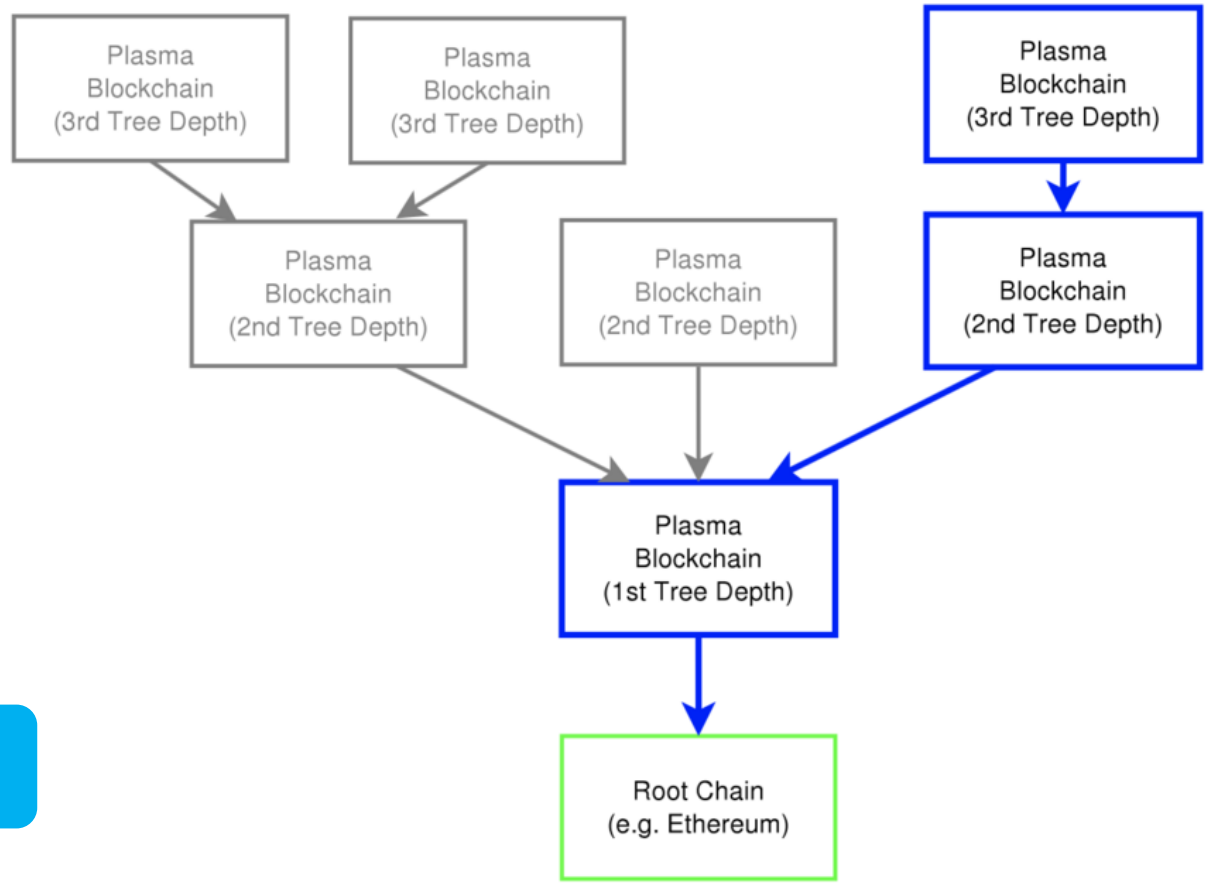
異種ブロックチェーン間での取引を
理論上、無限大のスループットで行う

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

ブロックチェーンの社会実装における課題

CurrencyPort

1．世界規模取引に向けた拡張性

2．異種ブロックチェーン間の相互運用性

3．ルーズな運用にも耐えるセキュリティ

異種ブロックチェーン間の相互運用性（インターオペラビリティ）

CurrencyPort

ブロックチェーン　⇒　価値取引の台帳技術

価値　⇒　概念
台帳　⇒　概念

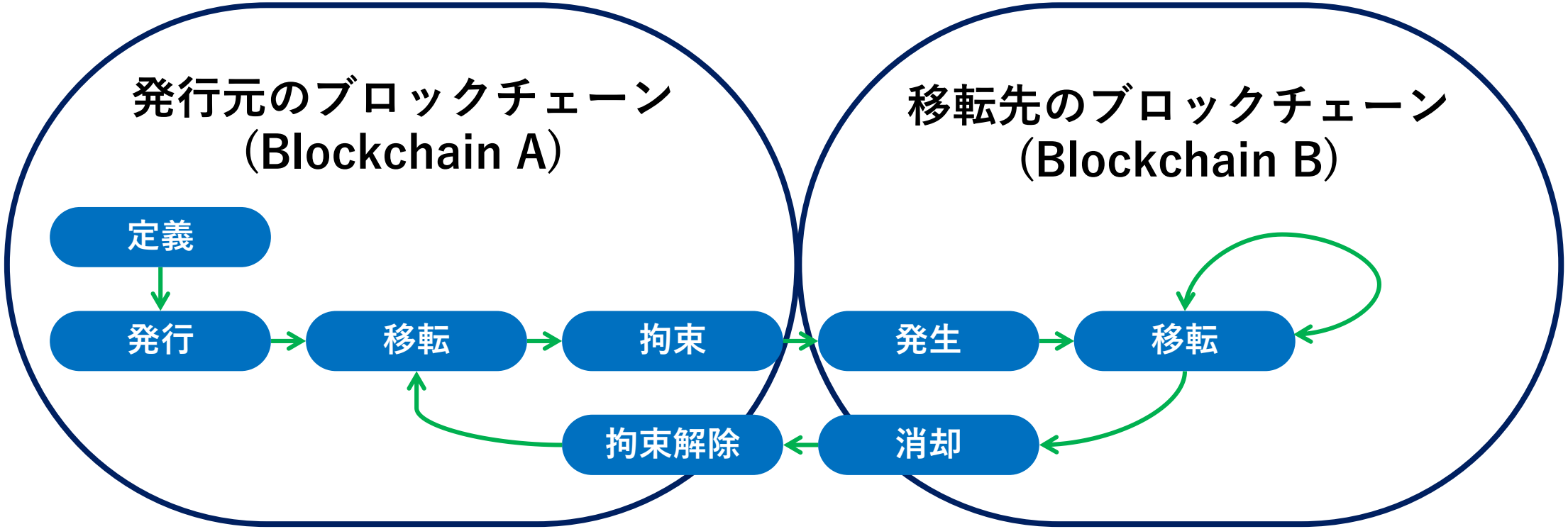
概念　⇒　共有可能　⇒　相互乗り入れが可能

異種台帳間でも価値取引の相互運用が可能

インターオペラビリティ

異種ブロックチェーン間の相互運用性

CurrencyPort



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

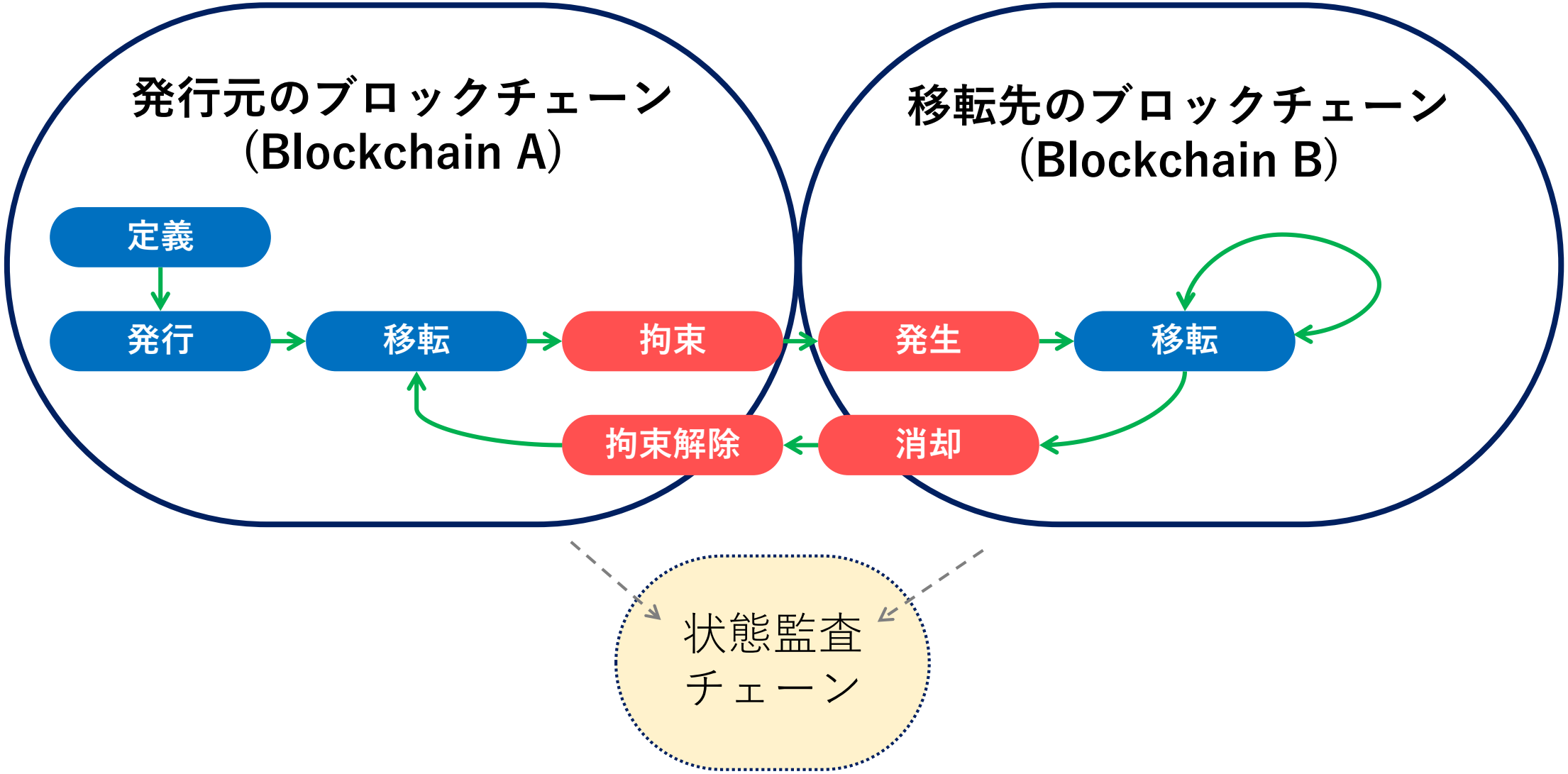
状態監査
チェーン

実際の価値が流通する
ブロックチェーン

インターオペラビリティ

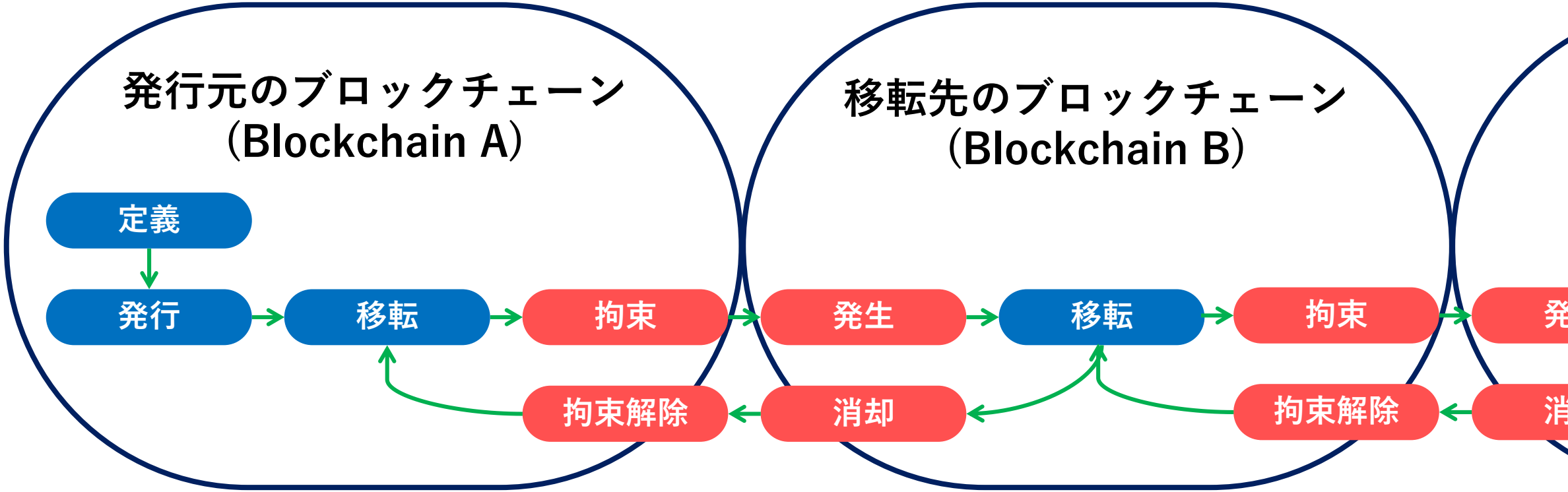
異種ブロックチェーン間の相互運用性

CurrencyPort



インターオペラビリティ

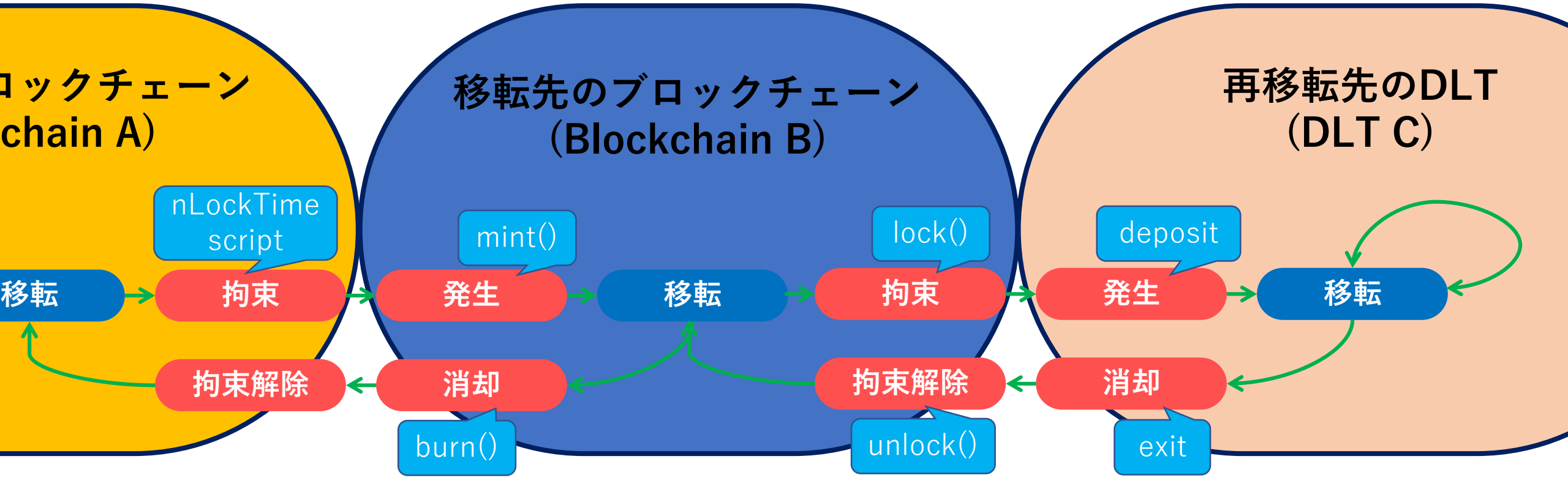
異種ブロックチェーン間の相互運用性



インターオペラビリティ

異種ブロックチェーン間の相互運用性

CurrencyPort



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)

ベンダーロックインを生まない姿勢が重要

ブロックチェーンの社会実装における課題

CurrencyPort

1．世界規模取引に向けた拡張性

2．異種ブロックチェーン間の相互運用性

3．ルーズな運用にも耐えるセキュリティ

ルーズな運用にも耐えるセキュリティ

ブロックチェーンに記録するトランザクションには

必ず電子署名を施す必要がある

▼

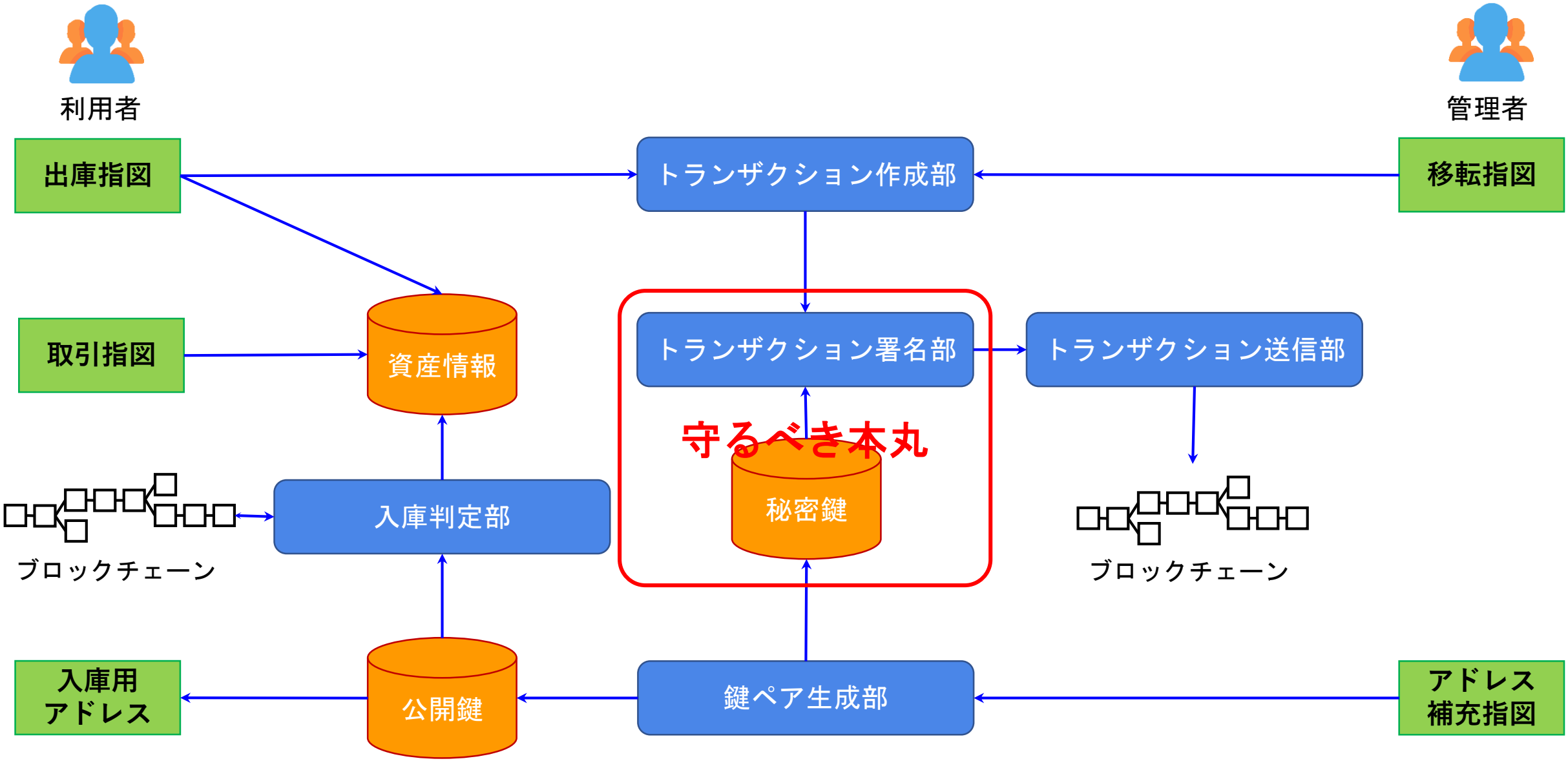
署名鍵の管理が必須

- 署名鍵の盗難・盗聴　⇒　資産の流出に直結
- 他人に署名鍵を見られてしまうだけでダメ
- 署名鍵を紛失してしまうとリカバーが不可能
- サービス事業者も責任が取れない
- 利用者が自らで適正に管理する必要がある

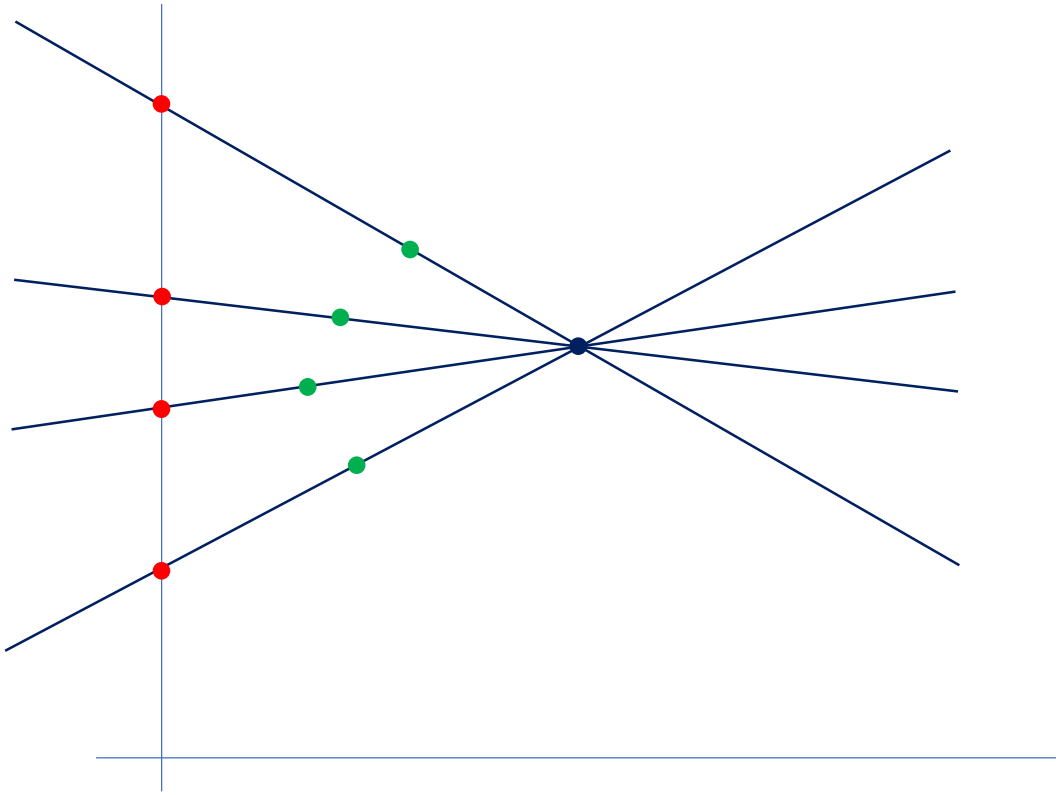
実用性に疑問符
本当に流行るのか？

ブロックチェーン・ウォレットの概念図

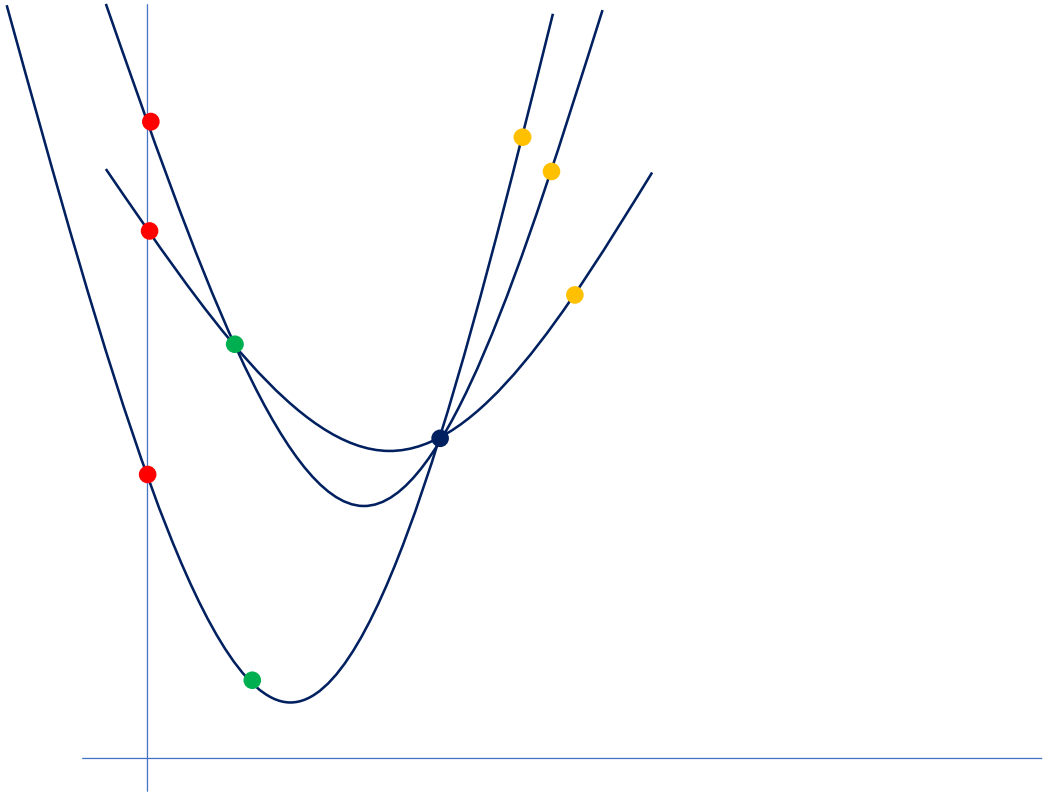
CurrencyPort



秘密分散法の原理



閾値２の秘密分散
1次関数



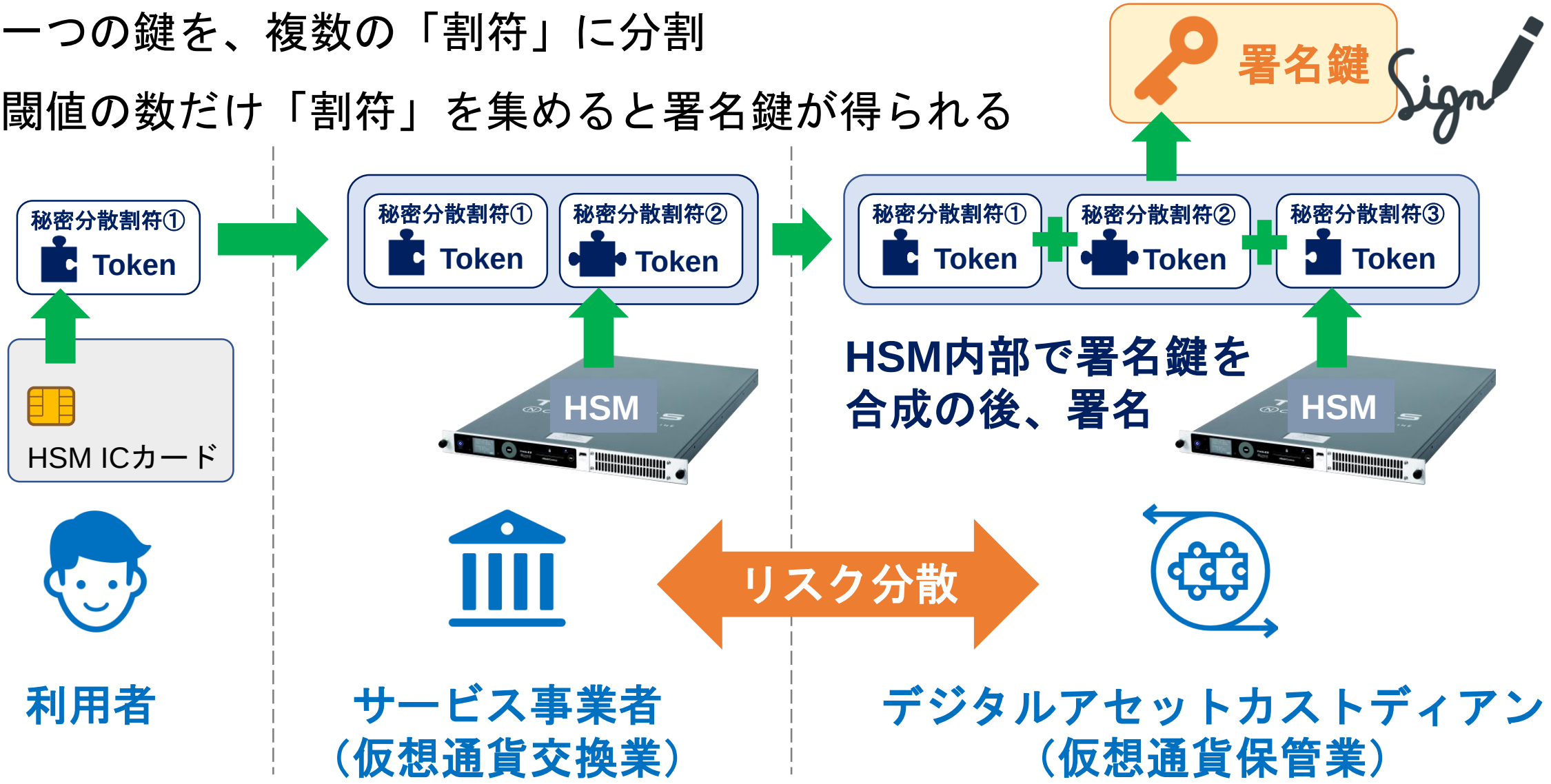
閾値３の秘密分散
2次関数

デジタルアセットカストディアンの例

CurrencyPort

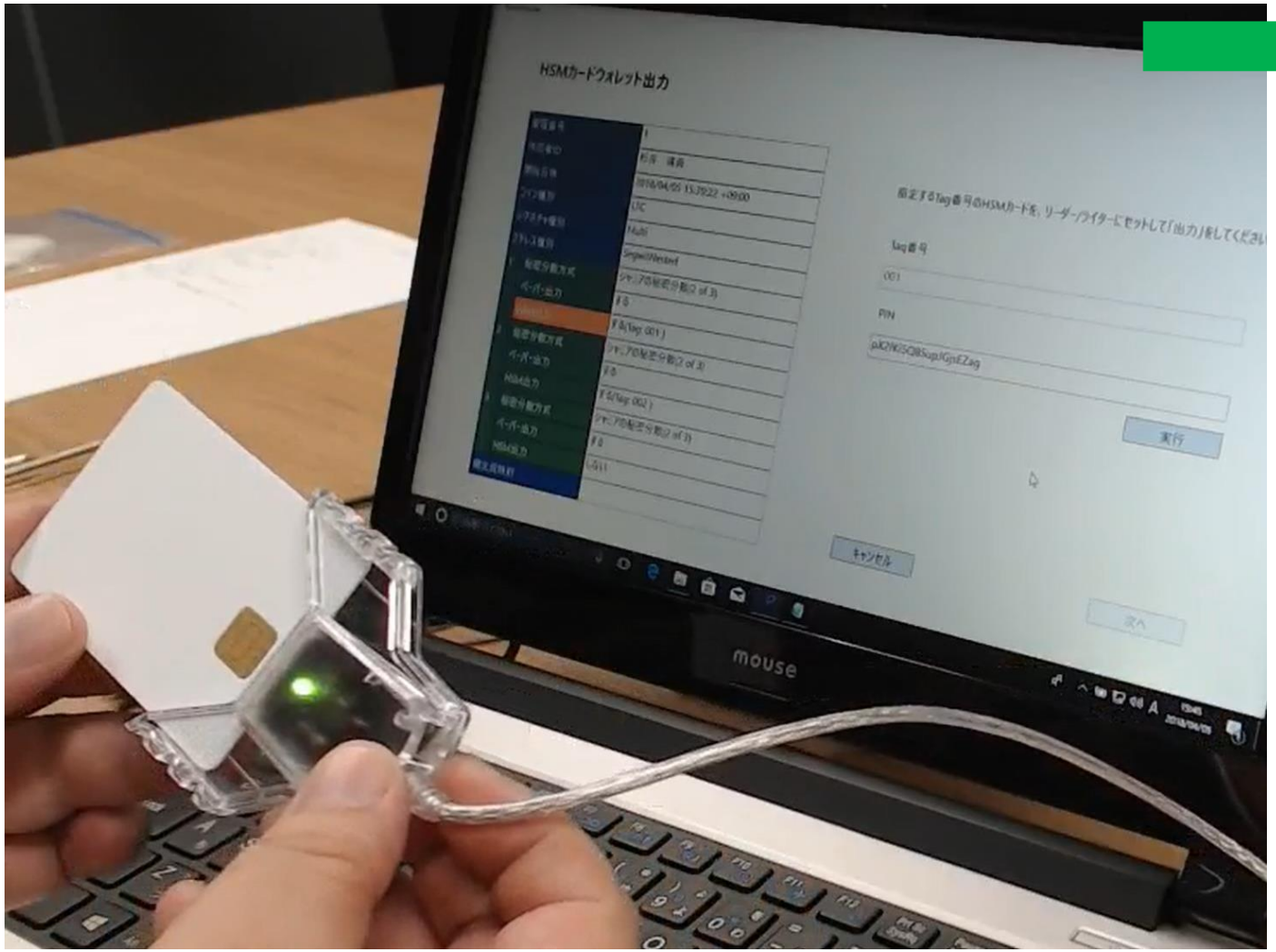
① 一つの鍵を、複数の「割符」に分割

② 閾値の数だけ「割符」を集めると署名鍵が得られる



ICカード型HSM・ブロックチェーン署名システム

CurrencyPort



カードタイプ

業務用署名システム（2018年）

一般向け実用化（2019年～）

ATM対応（2019年・後半～）

EMV決済対応（2020年頃～）

秘密鍵管理とトランザクション署名部の保護

CurrencyPort

コインチェック事件を受けて以来、業務用ブロックチェーンシステムの鍵管理技術の向上および、態勢は格段に改善しており、事業者の管理する**秘密鍵を直接奪取することは困難な水準**に達しつつある。

しかし…

周辺業務システムの脆弱性対策には課題が残っている。

ウォレットの攻撃例

CurrencyPort

利用者

管理者

出庫指図

トランザクション作成部

移転指図

取引指図

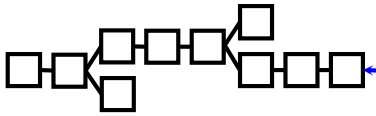
資産情報

トランザクション署名部

トランザクション送信部

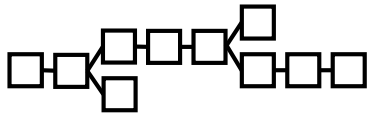
守るべき本丸

秘密鍵



ブロックチェーン

入庫判定部



ブロックチェーン

入庫用
アドレス

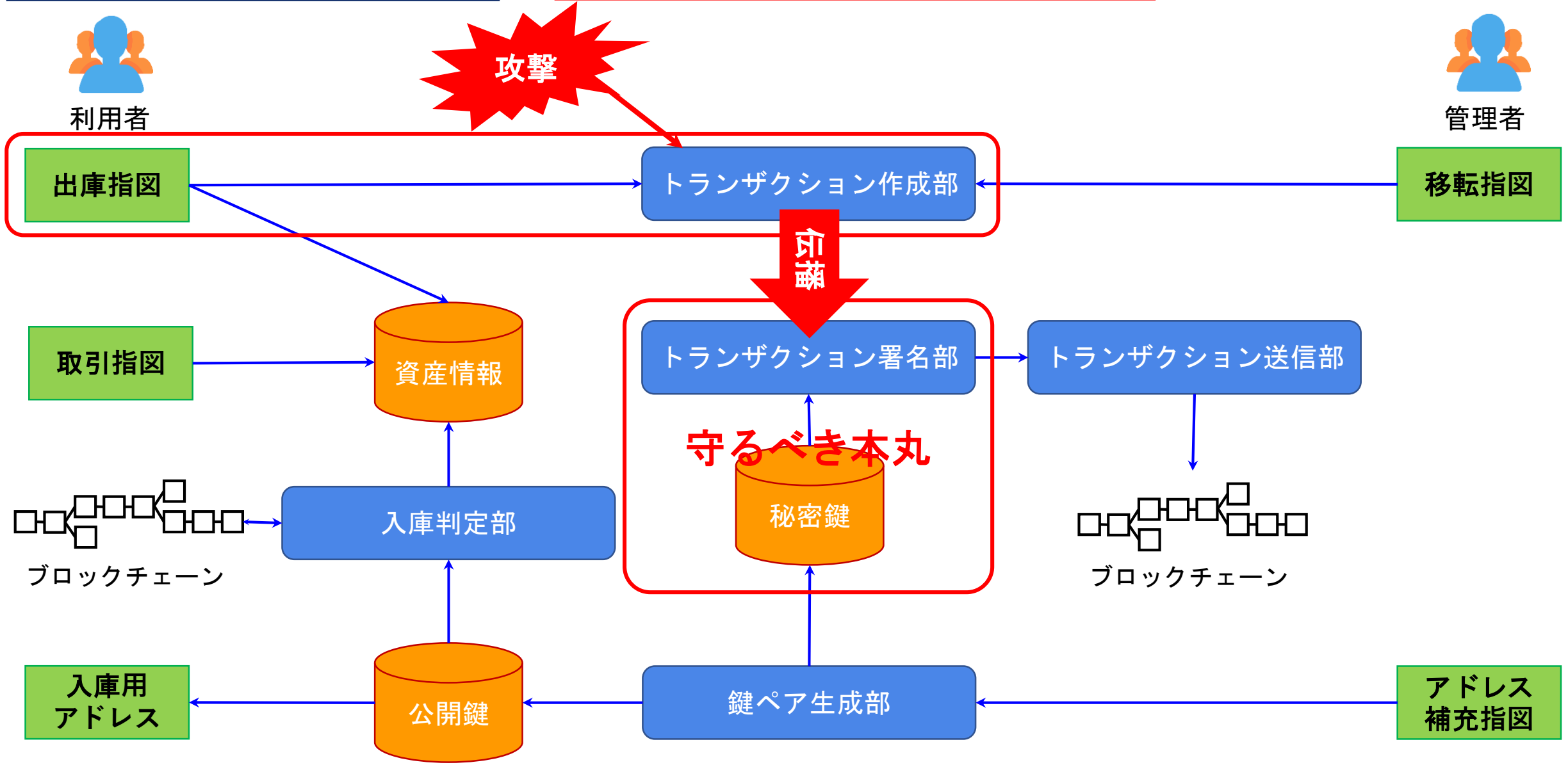
公開鍵

鍵ペア生成部

アドレス
補充指図

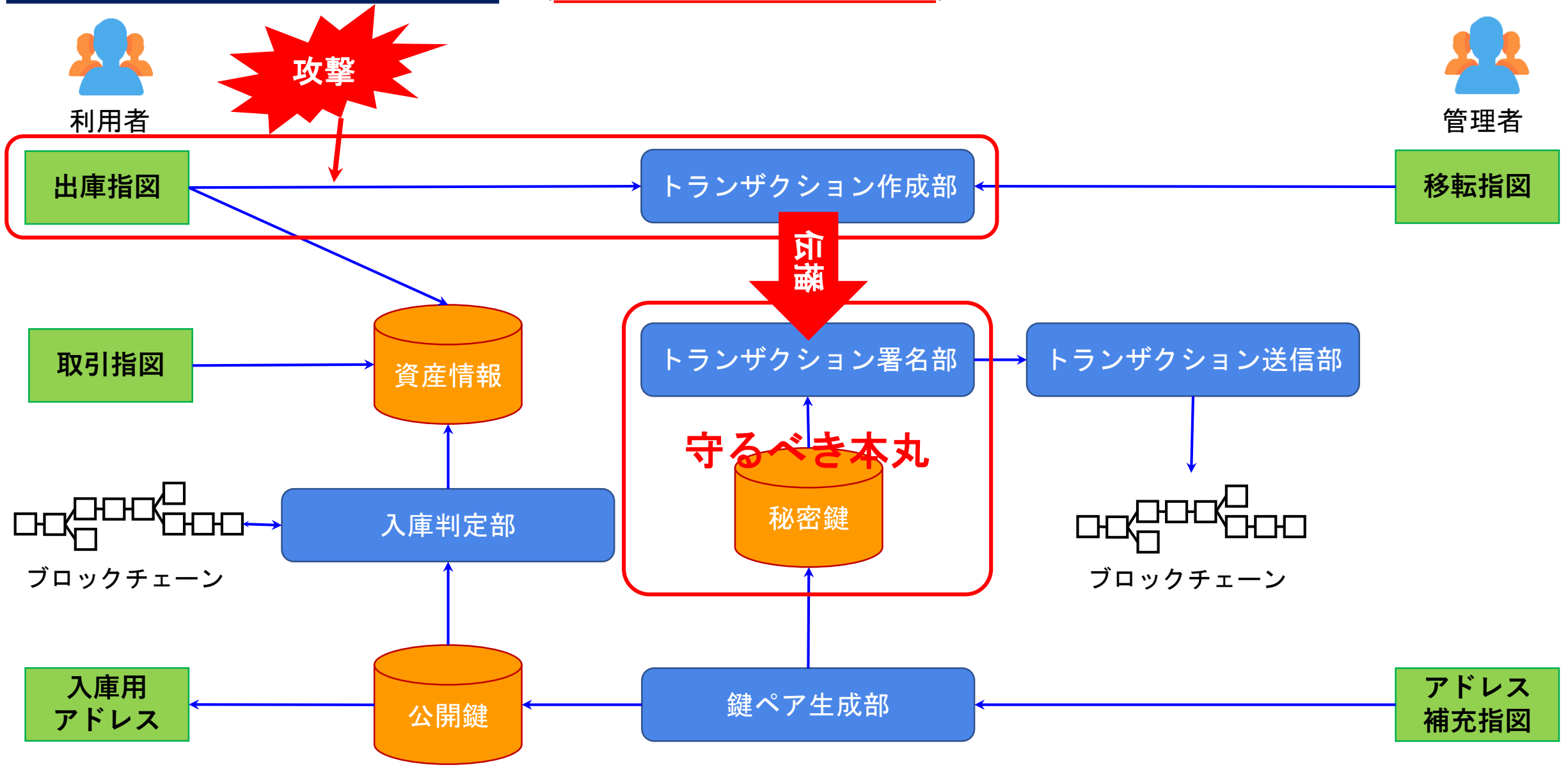
ウォレットの攻撃例（トランザクション改ざん）

CurrencyPort



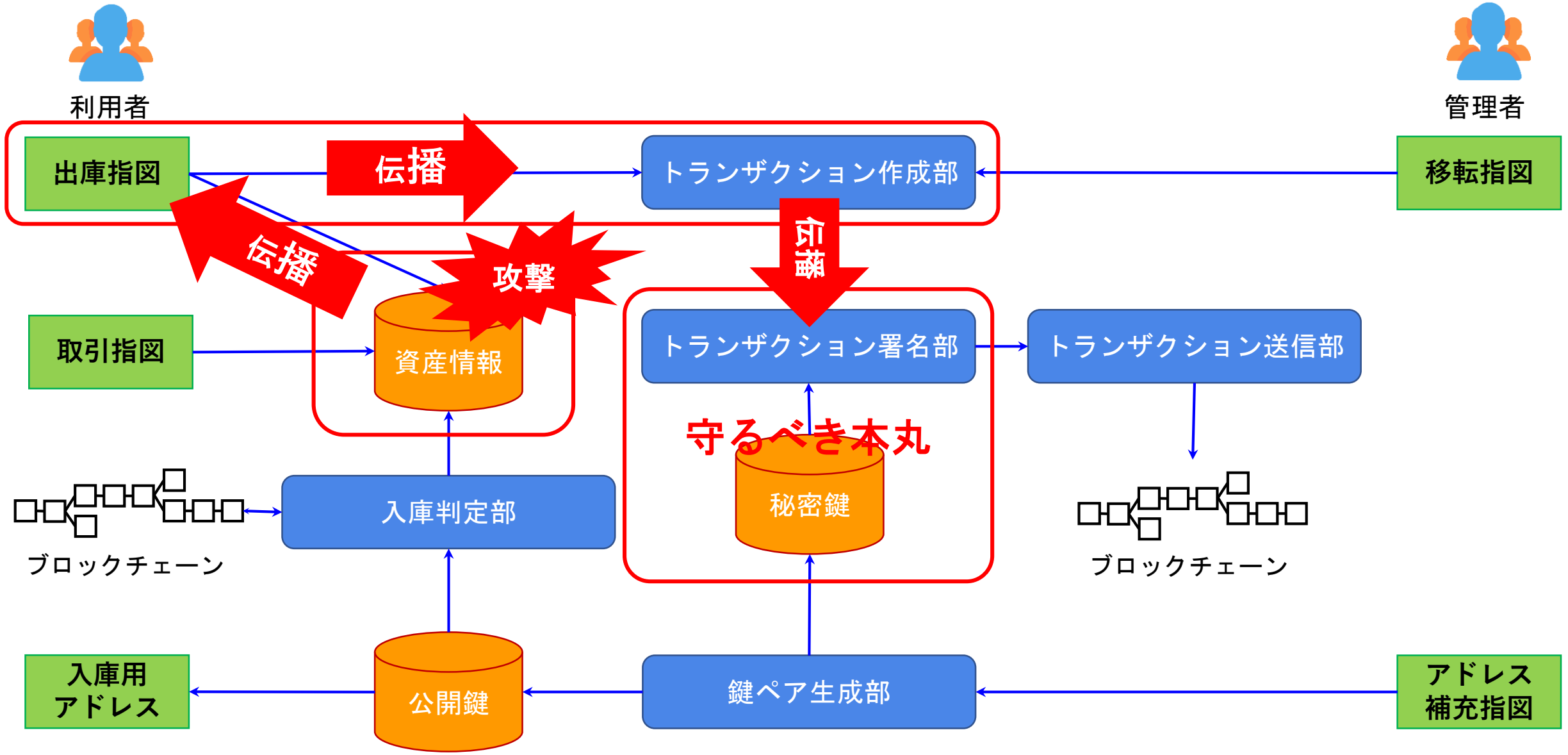
ウォレットの攻撃例（出庫指図改ざん）

CurrencyPort



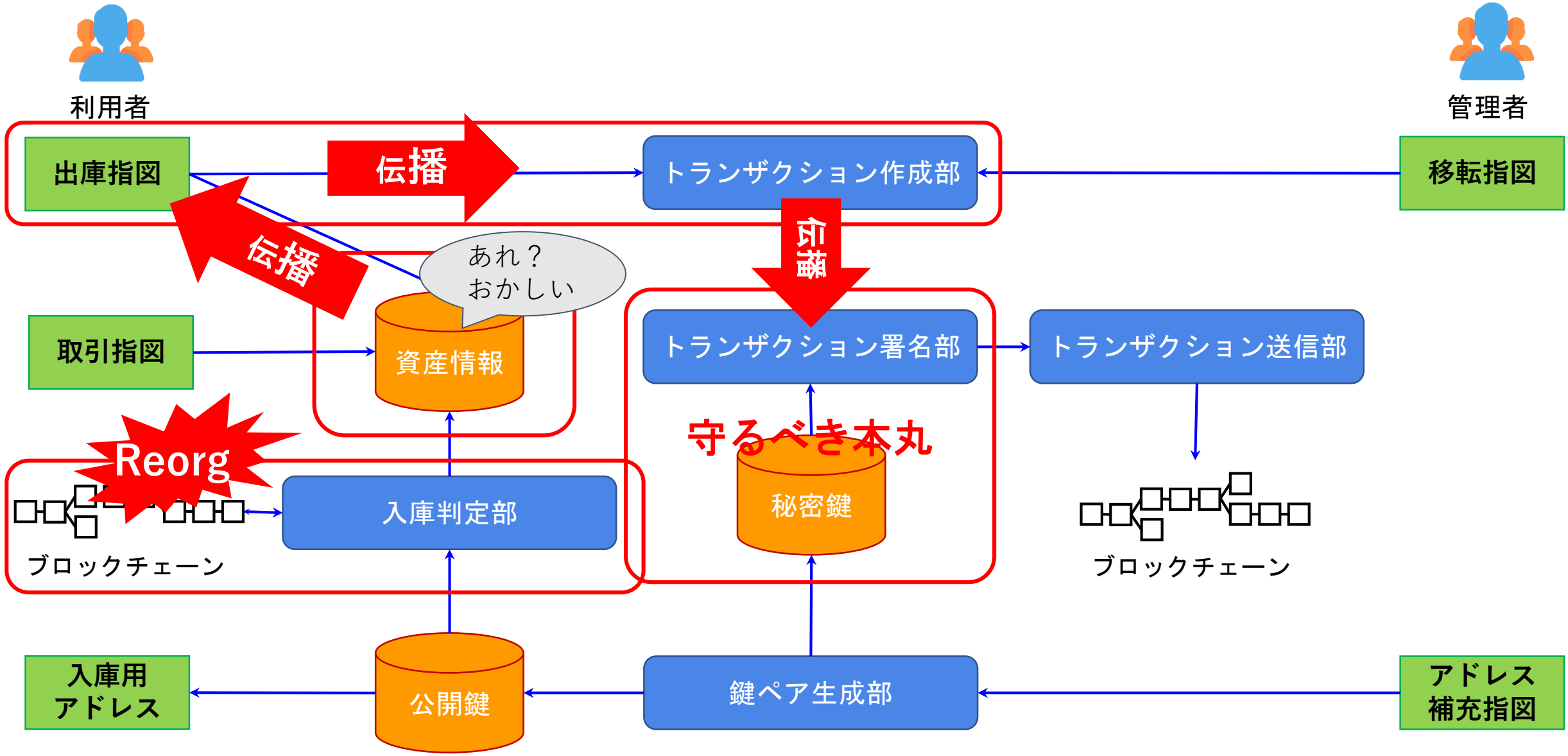
ウォレットの攻撃例（資産情報DB改ざん）

CurrencyPort



ウォレットの攻撃例（資産情報DB記録不良）

CurrencyPort



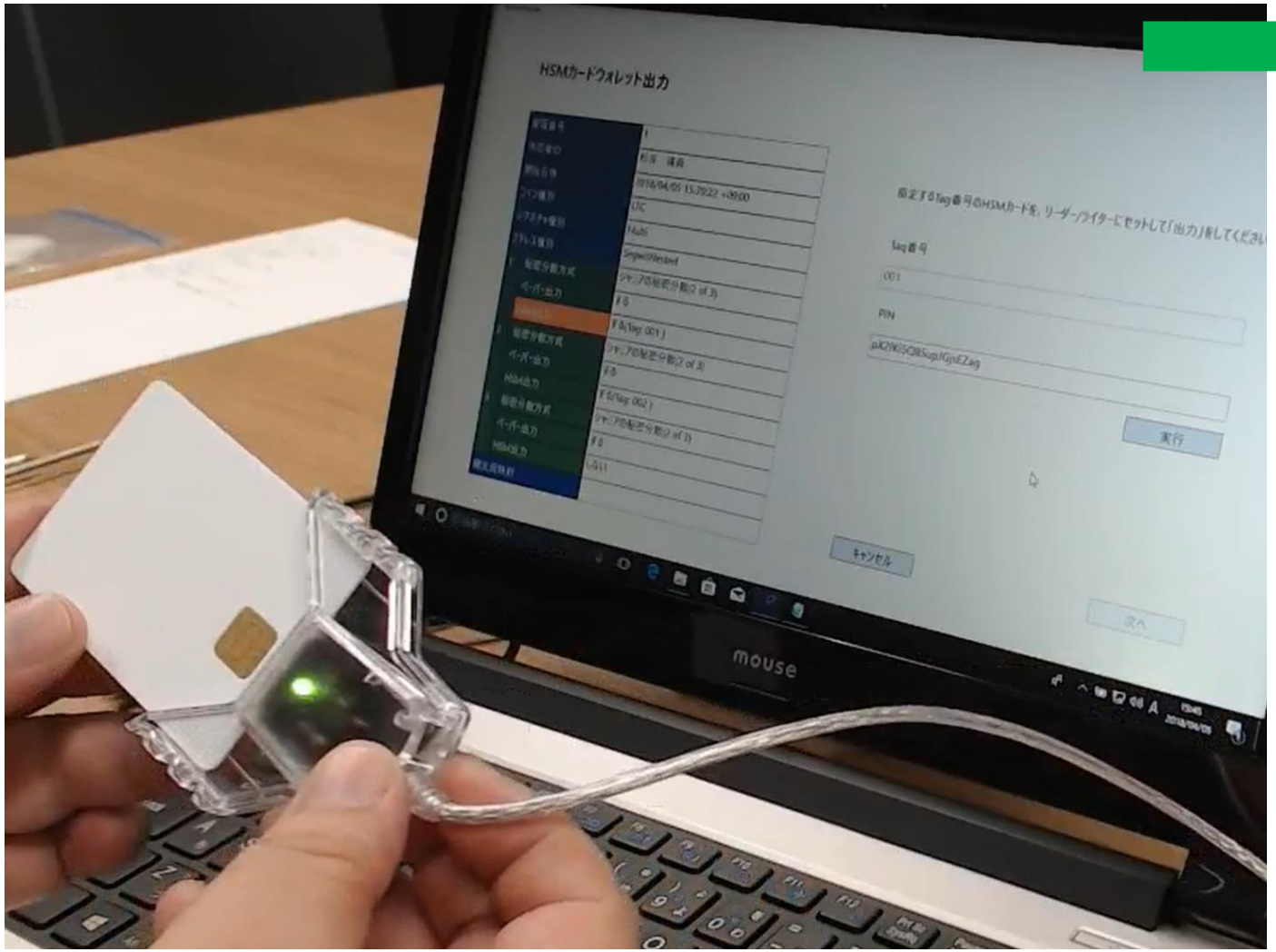
取引所のシステムも多層防御セキュリティが重要

CurrencyPort

1. ネットワーク層の安全対策
2. コンピューター・ノード層の安全対策
3. アプリケーション・ロジック層の安全対策
4. メッセージング・トランザクション層の安全対策
5. 署名鍵管理
6. 認証と認可

SIM型HSM・ブロックチェーン署名システム

CurrencyPort



カードタイプ

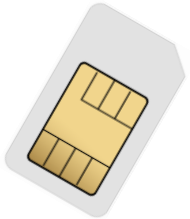
業務用署名システム（2018年）

一般向け実用化（2019年～）

ATM対応（2019年・後半～）

EMV決済対応（2020年頃～）

SIMタイプ



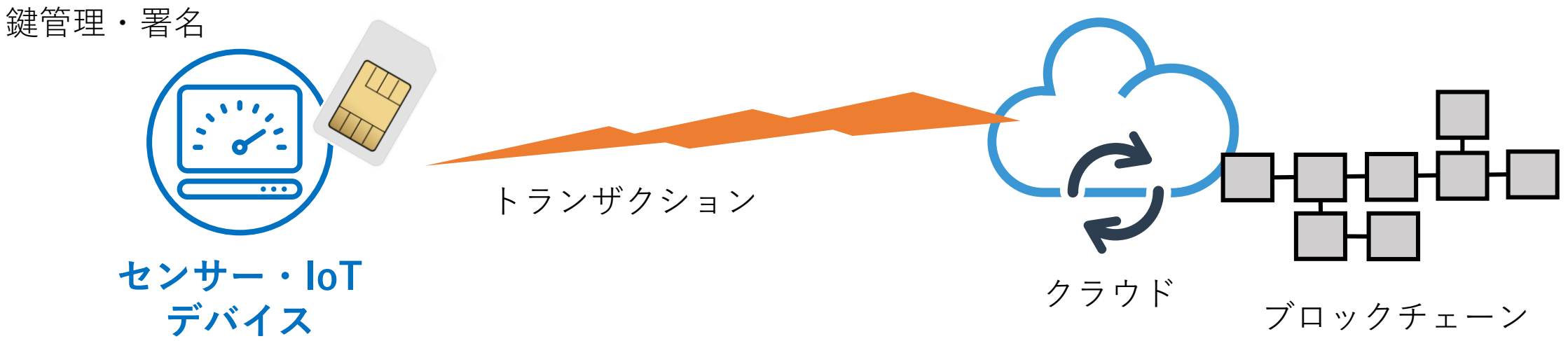
IoT・センサー等

モビリティデバイス向け

（2019、20年頃～）

SIM型HSM・ブロックチェーン署名システム

CurrencyPort



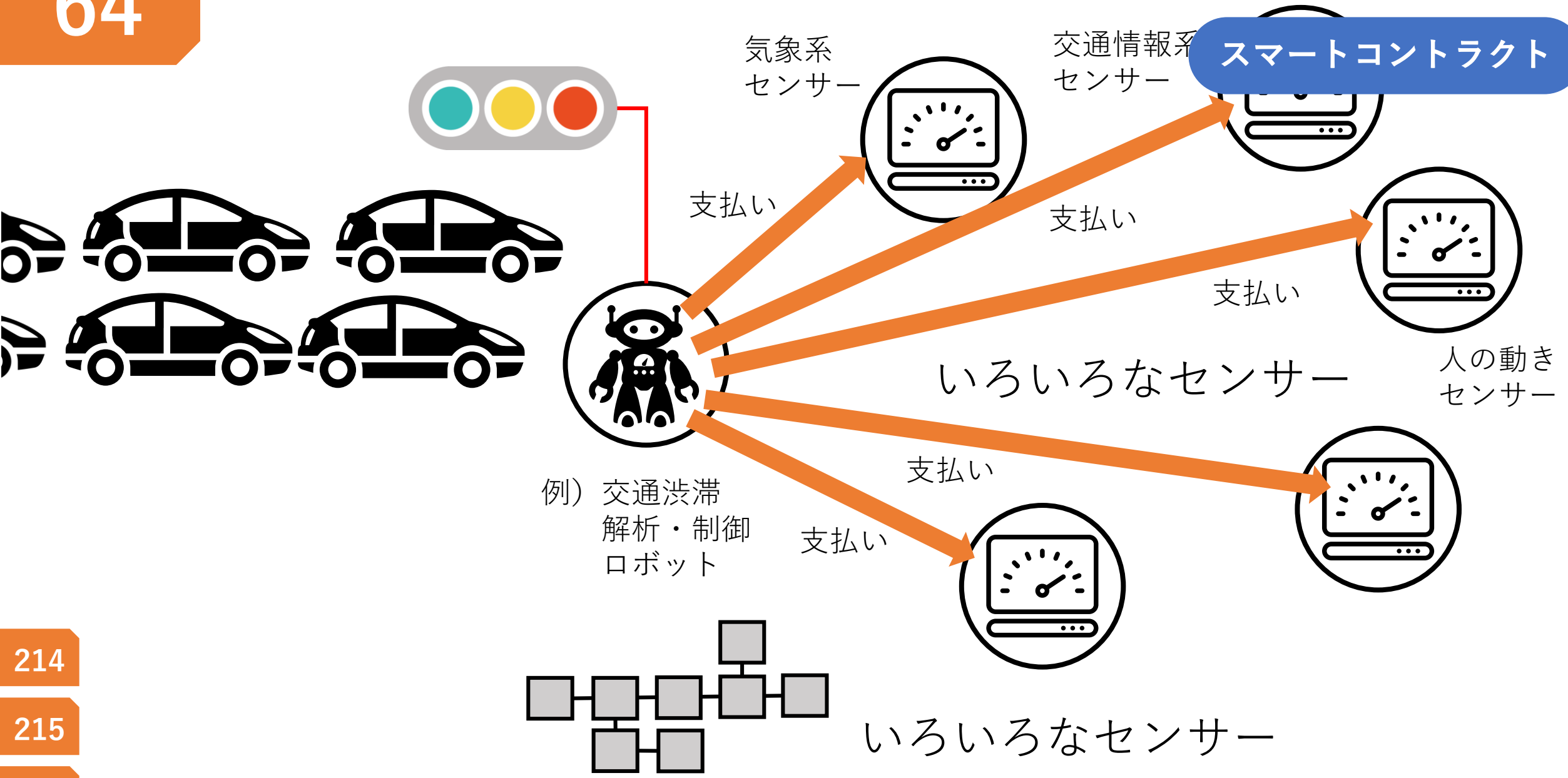
- IoTデバイス向けSIMカード
- ブロックチェーンシステム向けのトランザクション署名機能
- トランザクションを送信するだけのシンプルで安全な通信機能
- クラウドシステムとの連携

Lesson
64

マシン対マシンの支払いが普通になる未来

CurrencyPort

スマートコントラクト

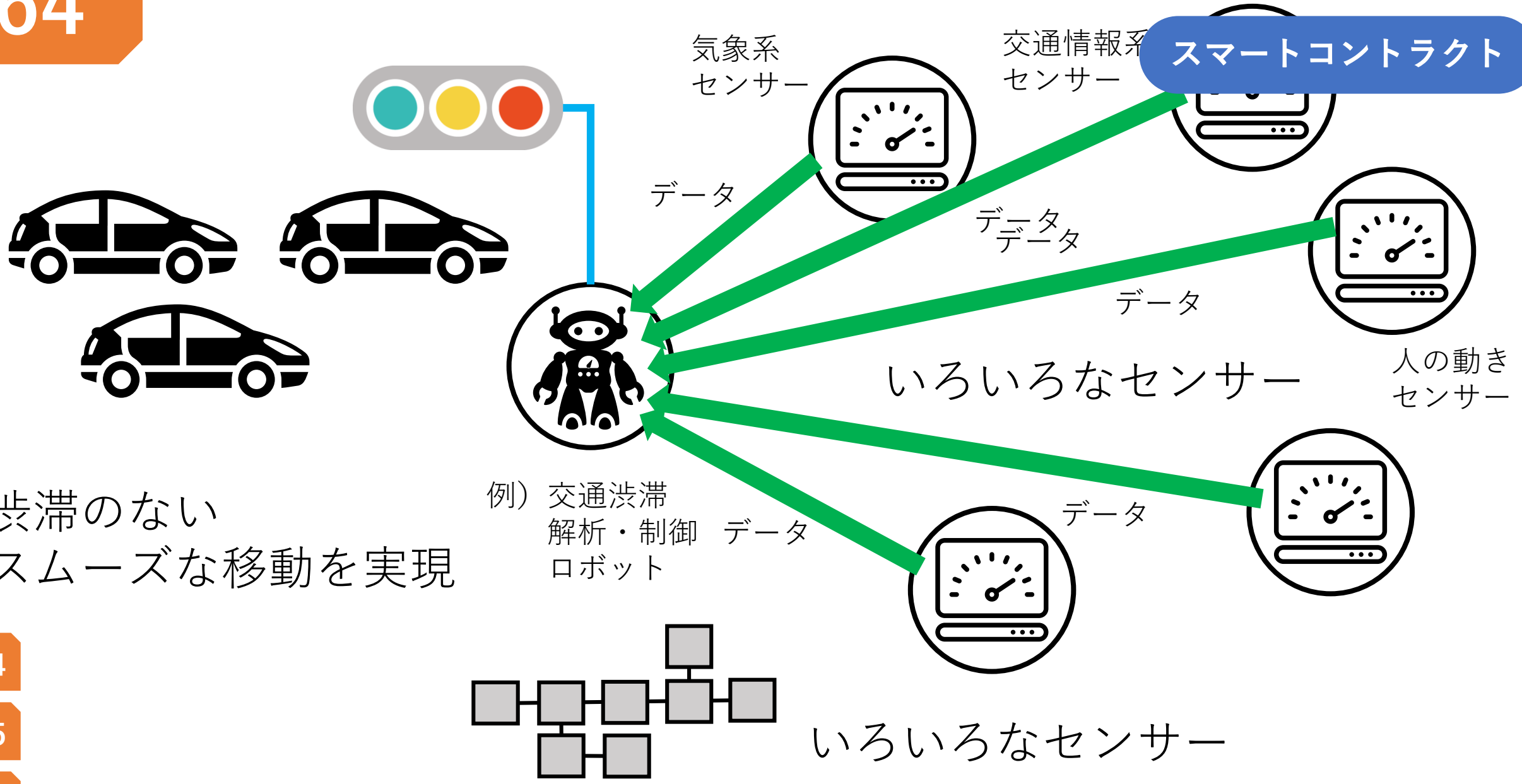


Lesson
64

マシン対マシンの支払いが普通になる未来

CurrencyPort

スマートコントラクト



自律分散社会のエコシステム

CurrencyPort

情報蓄積

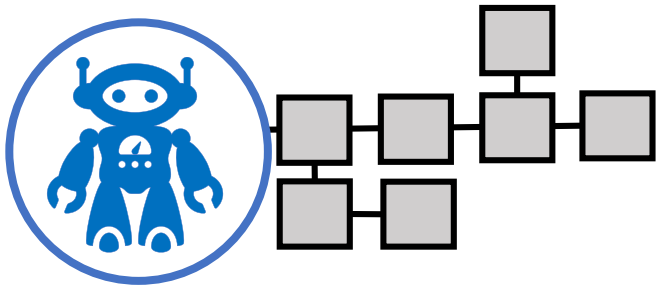
ブロックチェーン

お支払い

お支払い

情報収集

情報活用



センサー・IoT
デバイス

お支払い

お支払い

情報処理

スマートコントラクト

情報利用者

自律分散社会のエコシステム

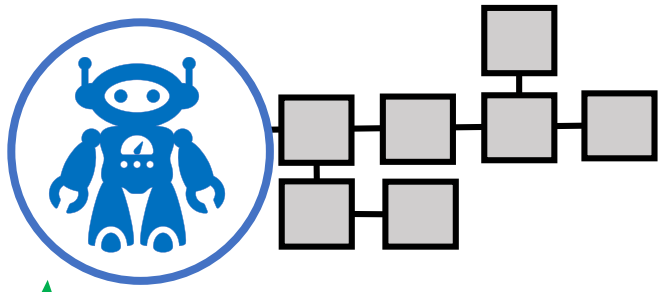
情報提供

情報蓄積

ブロックチェーン

情報提供

情報収集



センサー・IoT
デバイス

情報提供

情報処理

スマートコントラクト

情報提供

情報活用

情報利用者