

CSS2023 2023/11/01

ブロックチェーンによる仮想都市 “Crypto Town”構想について

近畿大学 山崎重一郎

埋込金融

FinTech

2015年 FinTechブーム

- 金融機関がIT産業に生まれ変わる



2021年 エンベッドドファイナンス（埋込金融）

- すべての企業が金融機関として顔を持つようになる



- ライセンスホルダー（金融機関）は黒子としてAPIを提供（法整備）

金融庁など法整備側はがんばっている！

**FinTech関連の法整備をすすめているおかげで
日本は世界的にみても FinTech のよい環境が整いつつある**

いまはテクノロジー側の努力が試されている

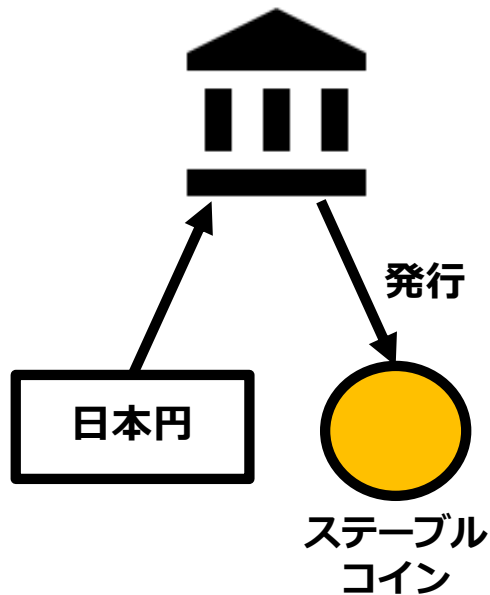
ステーブルコインと改正資金決済法

改正資金決済法（2023年6月施行）

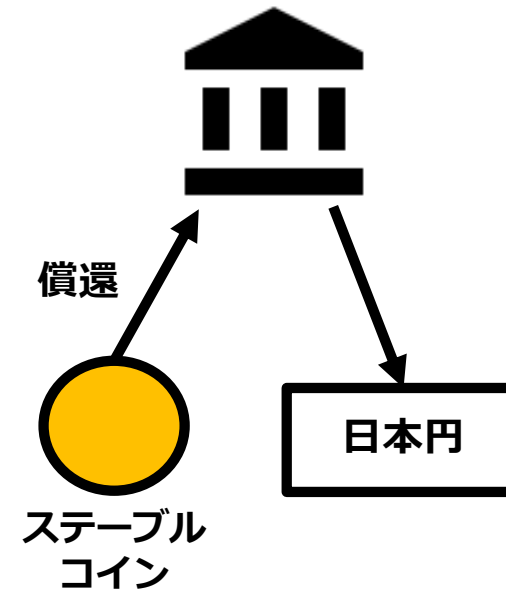
「デジタルマネー類似型」ステーブルコインが電子決済手段と位置づけられた

- 発行, 償還 → 為替取引に該当
- 銀行業免許又は資金移動業の登録が必要

銀行／資金移動業／特定信託会社



銀行／資金移動業／特定信託会社



ステーブルコイン

コイン（ペイメントトークン）

- 支払い手段として使用されるブロックチェーン上のトークン

ステーブル

- 特定の資産（法定通貨など）にペグする／価格調整アルゴリズムで価値の安定がはかられているもの



ステーブルコインの法的定義

ステーブルコインの定義（金融審議会「資金決済ワーキンググループ 報告」）

- 特定の資産と関連して価値の安定を目的とするデジタルアセットで分散台帳技術（又はこれと類似の技術）を用いているもの

分類

1. デジタルマネー類似型

「通貨建資産」（資金決済法第2条第6項）⇒ デジタルマネーとして規律

法定通貨の価値と連動した価格で発行され、発行価格と同額で償還を約するもの

2. 暗号資産型

「暗号資産」（資金決済法第2条第5項）⇒ 暗号資産として規律

デジタルマネー類似型以外（アルゴリズムで価値の安定を試みるもの等）

資金決済法のステーブルコインの規制

発行数量等の情報管理と報告義務 - 資金決済に関する法律 第六十二条の十九 (2)

内閣府令で定める期間ごとに（中略）利用者の電子決済手段の数量その他当該電子決済手段の管理に関する報告書を作成し、内閣総理大臣に提出しなければならない

移転及び償還を停止できる - 金融庁 電子決済手段等取引業者関係事務ガイドライン

自らが管理しないウォレットに係る電子決済手段の移転及び償還を停止するための態勢を整備する必要がある

発行者による取引確認 - 金融庁 電子決済手段等取引業者関係事務ガイドライン

デジタルマネーであって、その発行者が（中略）取引時確認をした者にのみ移転を可能とする技術的措置が講じられており、かつ、移転の都度発行者の承諾その他の関与が必要となるものは、（中略）電子決済手段に該当しない

資金決済法のステーブルコイン規制の目的別の整理

1. 法規制への取締可能性

- 犯罪収益移転防止法, テロ資金供与対策, 経済制裁など
- 法規制の遵守を可能にする技術的手段

2. 発行者規制

- 償還義務
- 利用者財産の保護

3. 仲介者規制

- 発行者との契約締結義務

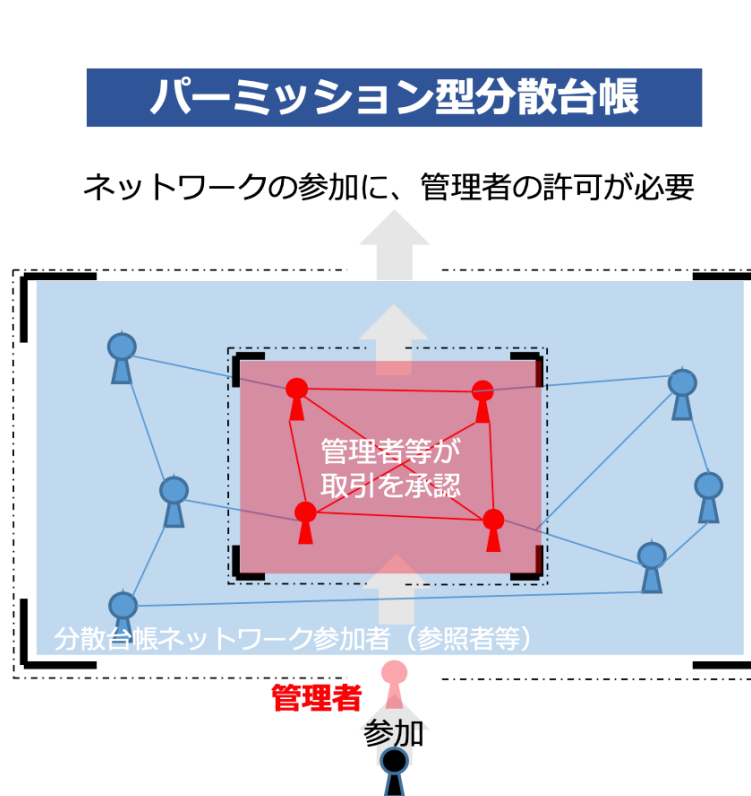
4. 日本円の通貨供給量に影響を与えない

- 発行量, 償還量の管理
- 価格安定の仕組みの提供 (投機対象にしないなど)

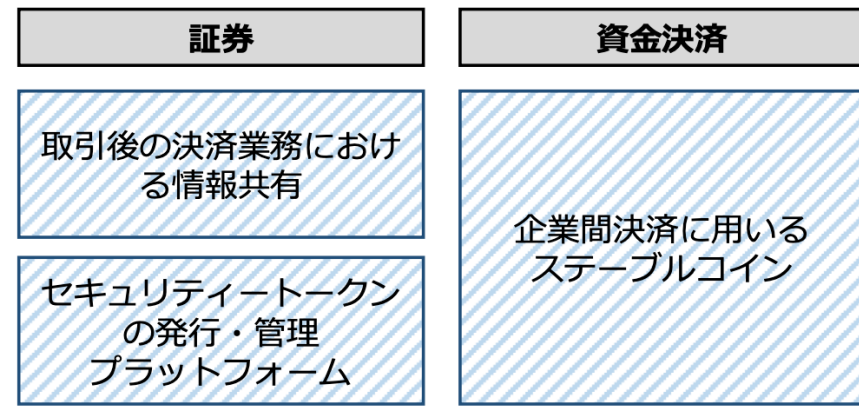
パーミッション型分散台帳での実現が想定されている

金融庁 説明資料より

- 安定的かつ効率的な資金決済制度の構築を図るための資金決済に関する法律等の一部を改正する法律案



金融分野における具体的なユースケース



- 証券決済・企業間決済等の高度化に向けた動き

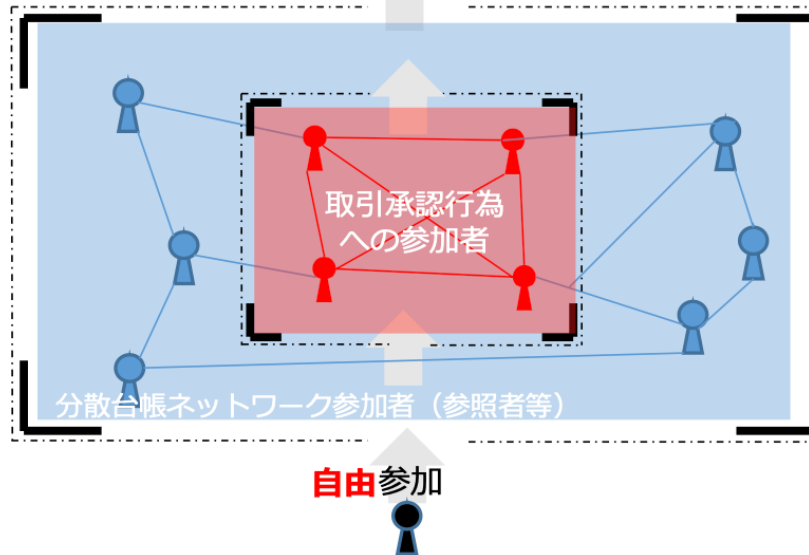
パブリック型分散台帳での実現が困難な理由

金融庁 説明資料より

- 安定的かつ効率的な資金決済制度の構築を図るための資金決済に関する法律等の一部を改正する法律案
- パブリック型ブロックチェーン = パーミッションレス型分散台帳（NISTIR 8202等による定義）

パーミッションレス型分散台帳

ネットワークの参加は自由

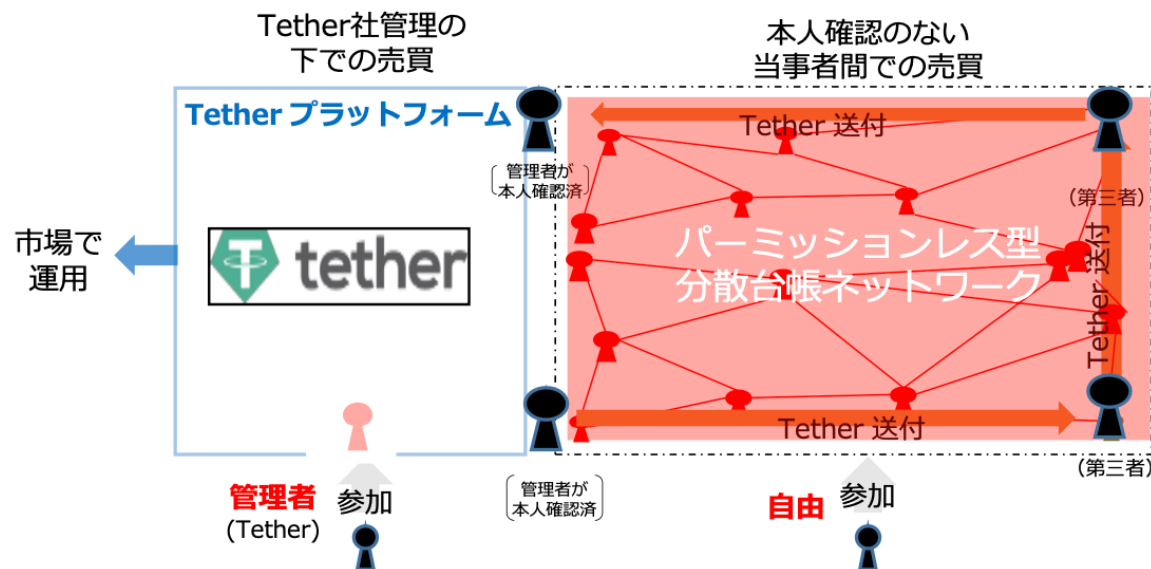


パブリック型ブロックチェーン上のステーブルコインの問題

適切な法規制が難しい（金融庁）

- 運営主体への規制監督
- 情報開示が不十分
- マネロン対策
- テロ資金供与対策
- 拡散金融対策

金融サービスのスキーム例（Tether（ステーブルコイン））



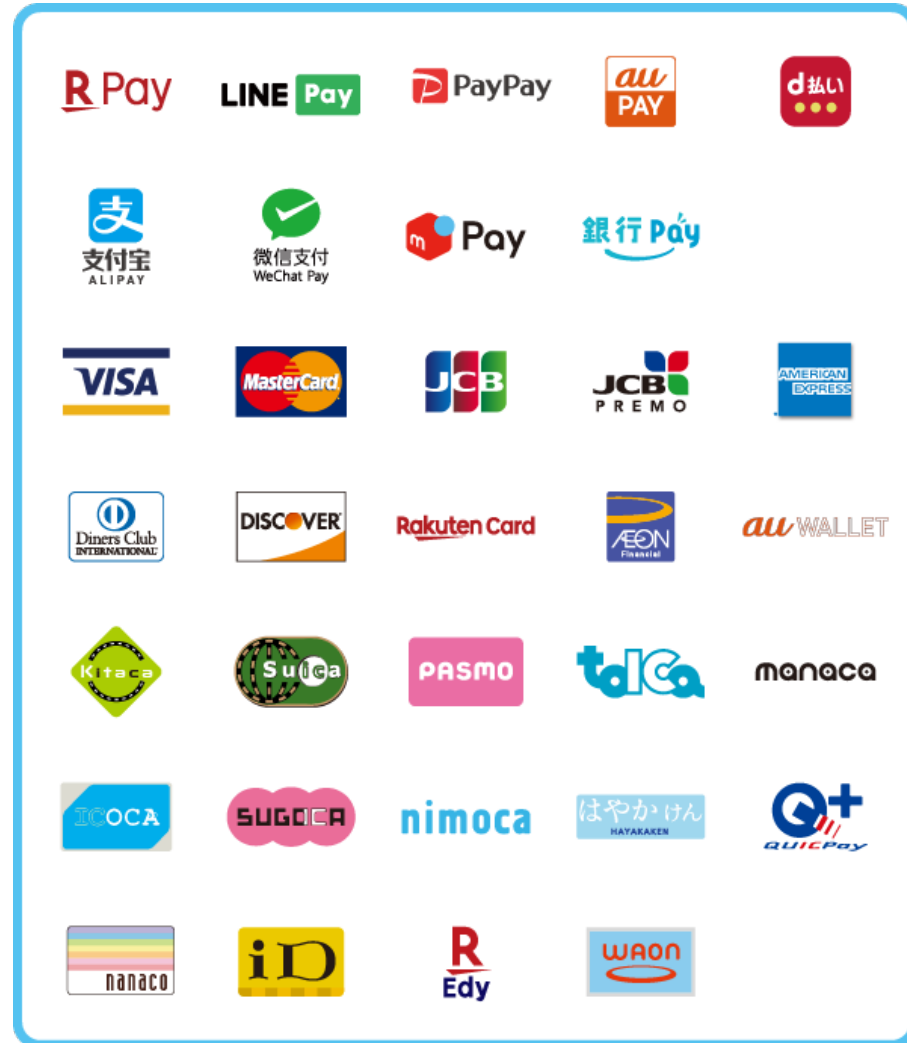
- (運営主体に対する規制監督なし)
- 情報開示が不十分
 - 償還可能性に疑義あり

- マネロン等対策が不十分

ステーブルコインの用途

すでに日本の電子マネーは乱立状態

それが増えるだけ？



お金の機能

決済手段 価値評価尺度 資産の保存

資本としてのお金



我々のステーブルコインの設計目的

Web3ブーム

Web3 の4原則 (Gavin Wood)

1. 所有者たちによる Decentralized なネットワークであること
2. **パーミッションレス型であること**
3. 暗号通貨によるネイティブな支払い機能を備えること
4. **トラストレスであること**



4原則すべてがパブリック型ブロックチェーンの特性



Gavin Wood

ゼロトラストネットワーク

ネットワーク・セキュリティにおける境界型防衛の限界

- 「組織内部トラフィックは信頼できる」というのは幻想

マルウェアは必ず内部まで入ってくる（標的型攻撃など）

モバイルアプリ, リモートワークの普及

ゼロトラスト

- 組織内のトラフィックも外部と同じくらい信用しないという前提

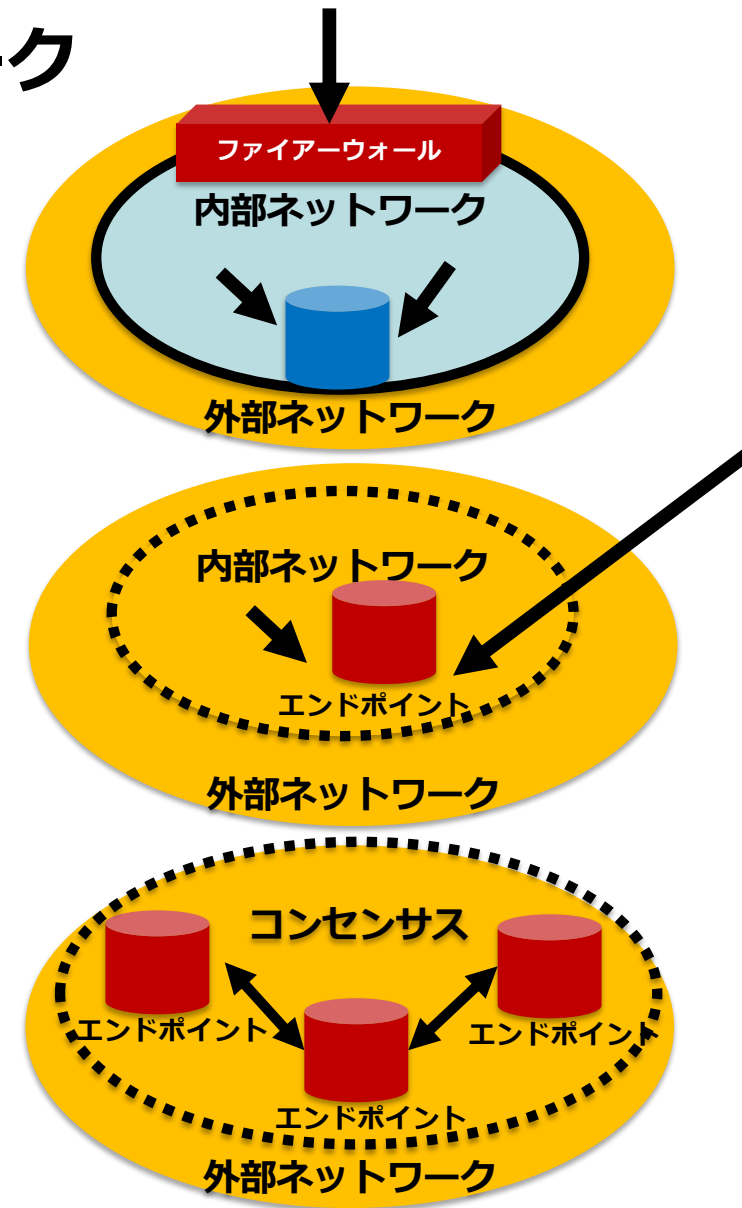
全ネットワークフローを

エンドポイントで認証, 暗号化, フィルターする

ゼロトラストネットワークとしてのブロックチェーン？

コンセンサスとネットワークとの外部との関係によって

トラストを創発し強化



エンタープライズ・ブロックチェーン

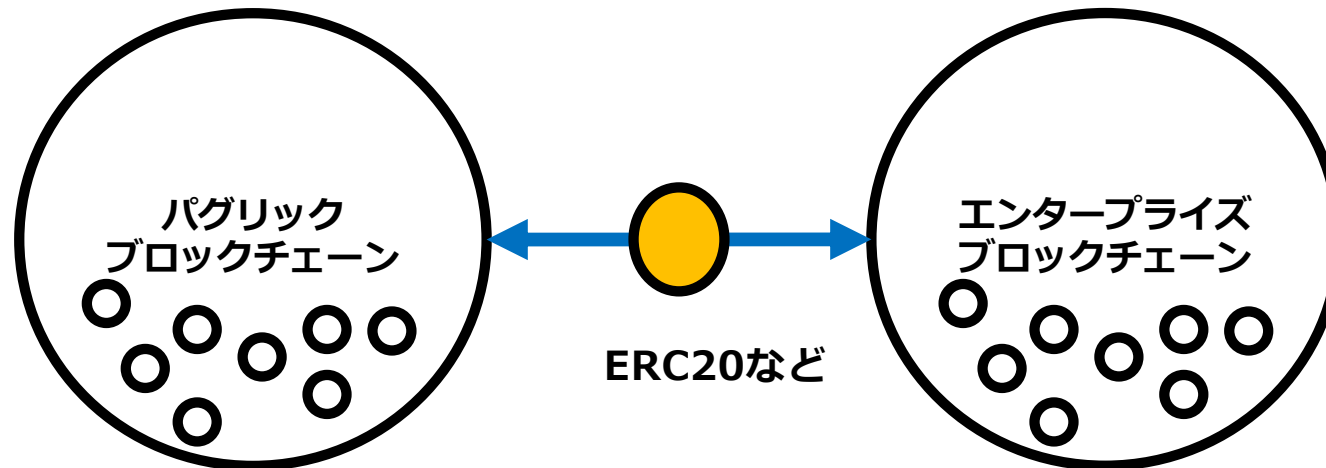
境界モデルも必要

- ゼロトラストだけでネットワークシステムを構成することは現実的ではない

シングルトンマシンとしてのブロックチェーン

$$\{1,1,1,1\} = \{1\}$$

- ブロックチェーン・ネットワークは = 1ノード（相互に相手は1ノードに見える）
- トークンのプロトコル化



DAO
(Decentralized Autonomous Organization)

DAO の提案

Ethereum White paper (2014) Vitalik Buterin

- **DAC (Decentralized Autonomous Corporation)**
配当金の受け取りを目的にした資本家を中心にした企業
- **DAO は DACの概念を一般の組織に拡張したもの**
非営利団体
仮想国家

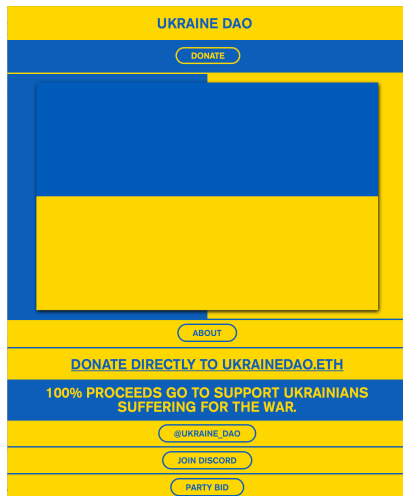


ヴィタリック・ブテリン

UKRAINE DAO (2022年2月25日設立)

ウクライナへの支援を行うDAO (ロシア軍のウクライナ侵攻 2月24日の24時間後)

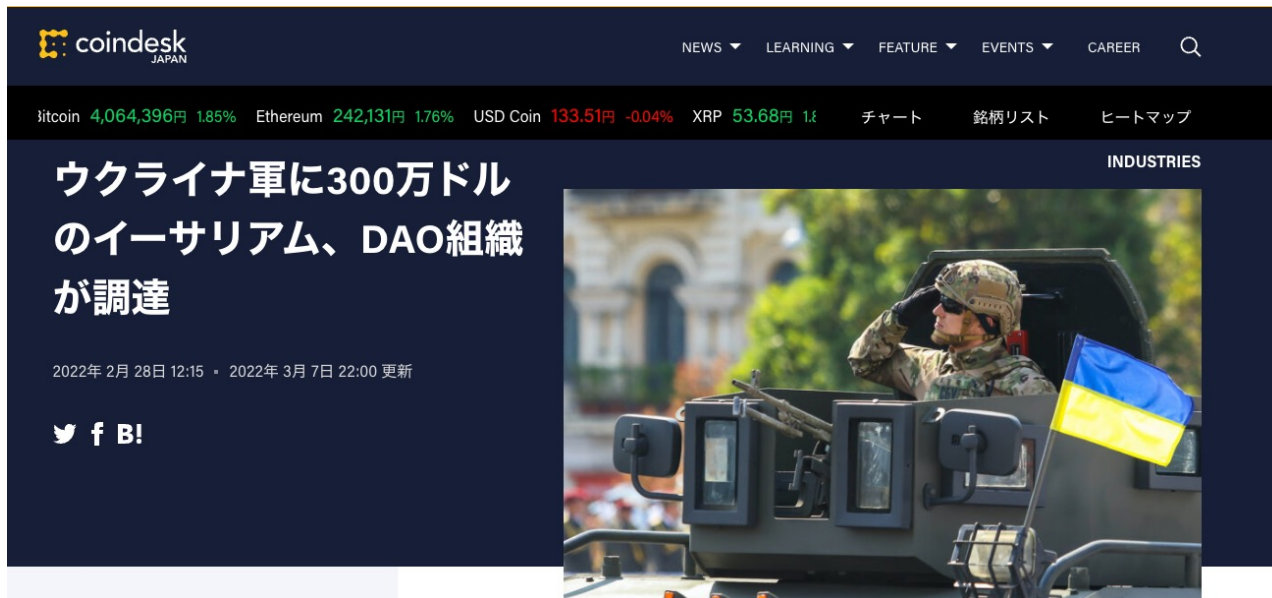
- ウクライナ国旗NFTの購入として寄付を行う
- ウクライナ政府所有の Ethereumアドレス, bitcoinアドレスへ寄付金やNFTを送金するシステム
- お礼として LOVE トークンがもらえる (無価値だったが、すでに市場取引が可能になっている)



発起人は、プッシー・ライオット
ロシアのフェミニスト・パンク・ロック・グループ (7人)



2022年2月28日時点で300万ドル調達



The screenshot shows the CoinDesk Japan website. At the top, there is a navigation bar with links for NEWS, LEARNING, FEATURE, EVENTS, and CAREER. Below this is a market data bar showing prices for Bitcoin (4,064,396円, +1.85%), Ethereum (242,131円, +1.76%), USD Coin (133.51円, -0.04%), and XRP (53.68円, +1%). The main headline reads "ウクライナ軍に300万ドルのイーサリアム、DAO組織が調達" (Ukrainian military receives 300,000 dollars in Ether, DAO organizations). The article is dated "2022年 2月 28日 12:15" and was updated on "2022年 3月 7日 22:00". Social media icons for Twitter, Facebook, and B! are visible.

高額で有名なCryptoPunks のNFTも ウクライナ政府のウォレットに寄付された

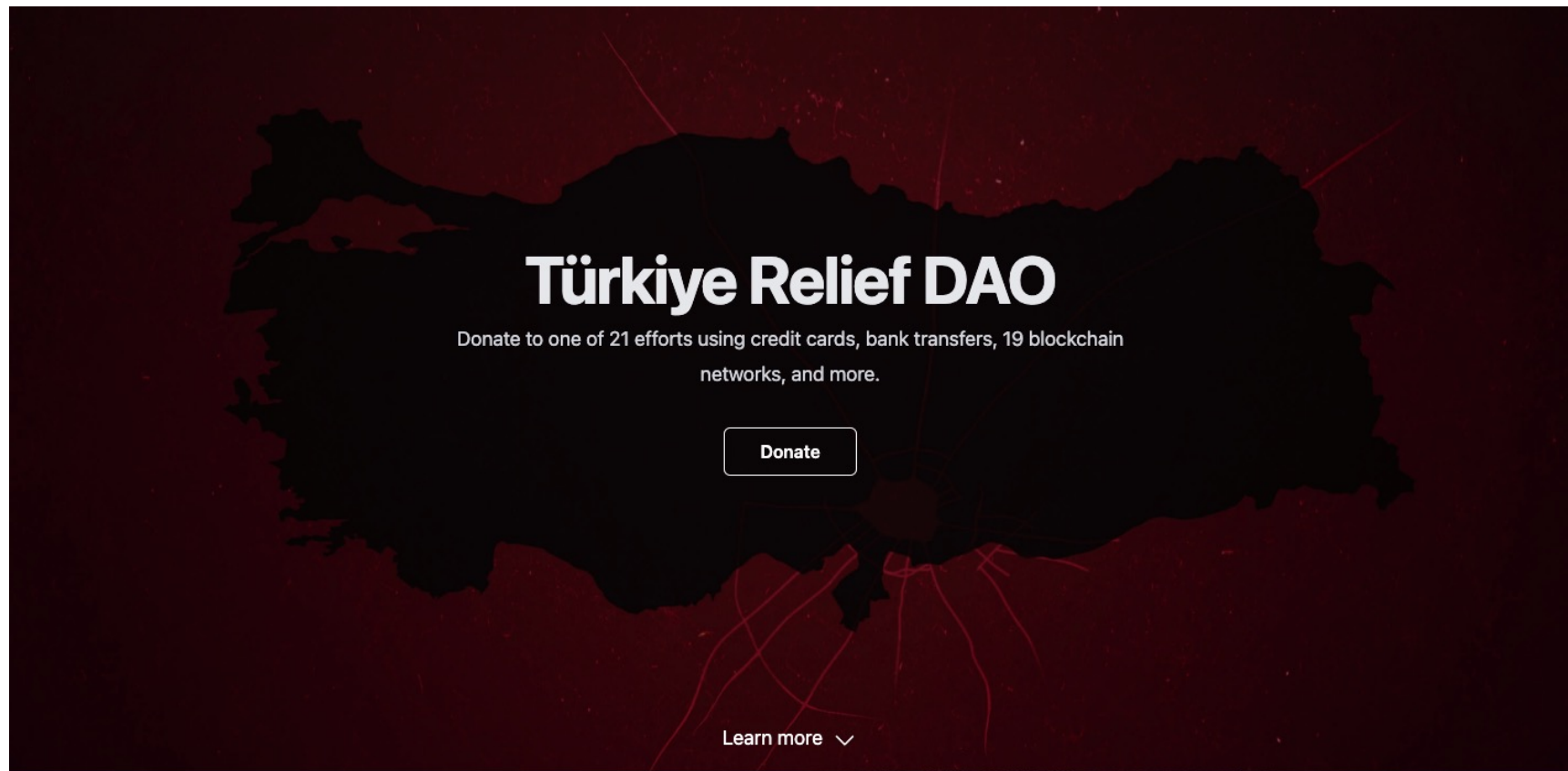
CryptoPunks

10,000 unique collectible characters with proof of ownership stored on the Ethereum blockchain. The project that inspired the modern CryptoArt movement. Selected press and appearances include [Mashable](#), [CNBC](#), [The Financial Times](#), [Bloomberg](#), [MarketWatch](#), [The Paris Review](#), [Salon](#), [The Outline](#), [BreakerMag](#), [Christie's of London](#), [Art|Basel](#), [The PBS NewsHour](#), [The New York Times in 2018](#) and [again in 2021](#). The Cryptopunks are one of the earliest examples of a "Non-Fungible Token" on Ethereum, and were inspiration for the [ERC-721 standard](#) that powers most digital art and collectibles.




Turkey Relief DAO

2023年2月6日に発生したトルコ・シリア地震救済目的のDAO




このDAOは 2023年2月10日時点で470万ドル集めていた

Discover Favorites My Creations ...



Docs Discord Community
New Query
Sign in


@davy42 / Turkiye Earthquake Donations 🔴

7 ☆
Share

Turkiye Earthquake Donations 🔴

[Donations info here](#)

tracked addresses:

- 0xbe4cde5eeeed1f0a97a9457f6ef5b71eae108652
- 0xE67922e36eD2422d391306f6f6ECC19d58EAa4f
- 0xe1935271D1993434A1a59fE08f24891Dc5F398Cd - (eth)
- 0x868D27c361682462536DfE361f2e20B3A6f4dDD8 - (avax)
- 0xB67705398fEd380a1CE02e77095fed64f8aCe463 - (bsc)
- 0xf3BFbC8701c2CF7c837CC30997f5da3829c5ABd8 (humanitycheck nft)

total donations Turkiye earthquake donations @davy42

6,086,446 \$

total donations

contributions Turkiye earthquake donations


11,842

contributions

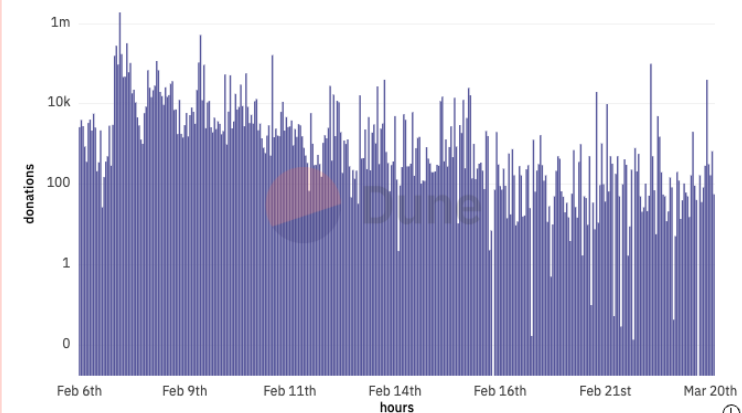
unique addresses Turkiye earthquake donations


3,998

unique addresses


@davy42

Turkiye earthquake donations in time




@davy42

Contributors Turkiye earthquake contributors

address	donation	contributions
0xc5a3b4dbd15b369f32aa7608e59e47d132cf97dc	1052642.00 \$	2
0x9acbb72cf67103a30333a32cd203459c6a9c3311	608204.94 \$	56
0x3a8dc2c8d3121290cb09b421792d8e79b7402ec5	600000.00 \$	7
0x5846711b4b7485392c1f0feaec203aa889071717	200000.00 \$	1
0x8894e0a0c962cb723c1976a4421c95949be2d4e3	191436.84 \$	1224
0xd8da6bf26964af9d7eed9e03e53415d37aa96045	166500.00 \$	2
0xdfd5293d8e347dfe59e90efd55b2956a1343963d	162662.65 \$	31
0xeb2d2f1b8c558a40207669291fda468e50c8a0bb	146648.92 \$	1048
0xe2fc31f816a9b94326492132018c3aecc4a93ae1	129666.85 \$	1259
0x5f4f41f781f076e78735cfd5fe862b700be3882f	126843.91 \$	2
0x0d0707963952f2fha59dnd06f2hd25ace40hd492fe	111301.73 \$	203

3,916 rows

<<
<
Page 1
>
>>

DAO法

DAO法勉強会（2022年）

「DAO法」の法整備に対する技術と制度の両面からの分析が目的



岡田仁志 先生
国立情報学研究所准教授



駒澤綜合法律事務所所長
高橋郁夫 弁護士



吉井和明 弁護士
光雲法律事務所共同代表
情報ネットワーク法学会副理事長



後藤大輔 弁護士
光雲法律事務所共同代表
日弁連 民事裁判手続等のIT化に関する検討WG

情報ネットワーク法学会にDAO法分科会を創設

メンバー5名でDAO法分科会の発表を行いました（2022年12月4日）

- 我々のDAO法勉強会の成果報告

情報ネットワーク法学会

The Information Network Law Association JAPAN

第22回研究大会

22nd Information Network Law Association JAPAN Conference

2022年12月3日（土）～4日（日）

九州大学病院キャンパス医学部百年講堂

米国のセーフハーバー

米国の特殊な法制度メカニズム

- 既存の法規制が現実的に実施不可能な事態への対応

代表例：オンライン仲介事業者を保護する法律（インターネットの黎明期）

- 1996年 米国電気通信法 230条

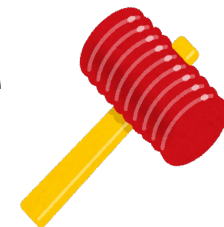
オンライン仲介事業者は、コンテンツの発行者とはみなさないことを明記

- 1998年 米国デジタルミレニアム著作権法 512条

要請に応じてコンテンツを削除しさえすれば、オンライン仲介事業者は著作権侵害責任を問われない

米国でGAFAが誕生した要因の一つと言われている

- YouTube は無限もぐらたたきをしていれば、事業者は著作権侵害を問われない



ブロックチェーンのセーフハーバー

米国 デラウェア州

- 2018 年米国デラウェア州 改正会社法

ブロックチェーンを含む電子ネットワークを、
企業の記録の保管や議決権行使に使用できるようにした

米国 ワイオミング州

- 2021年7月1日 DAO法

ワイオミング州内に登録代理人を維持し、
LLCとしてのその他の要件を満たしていれば、
DAOがLLCとして認められる



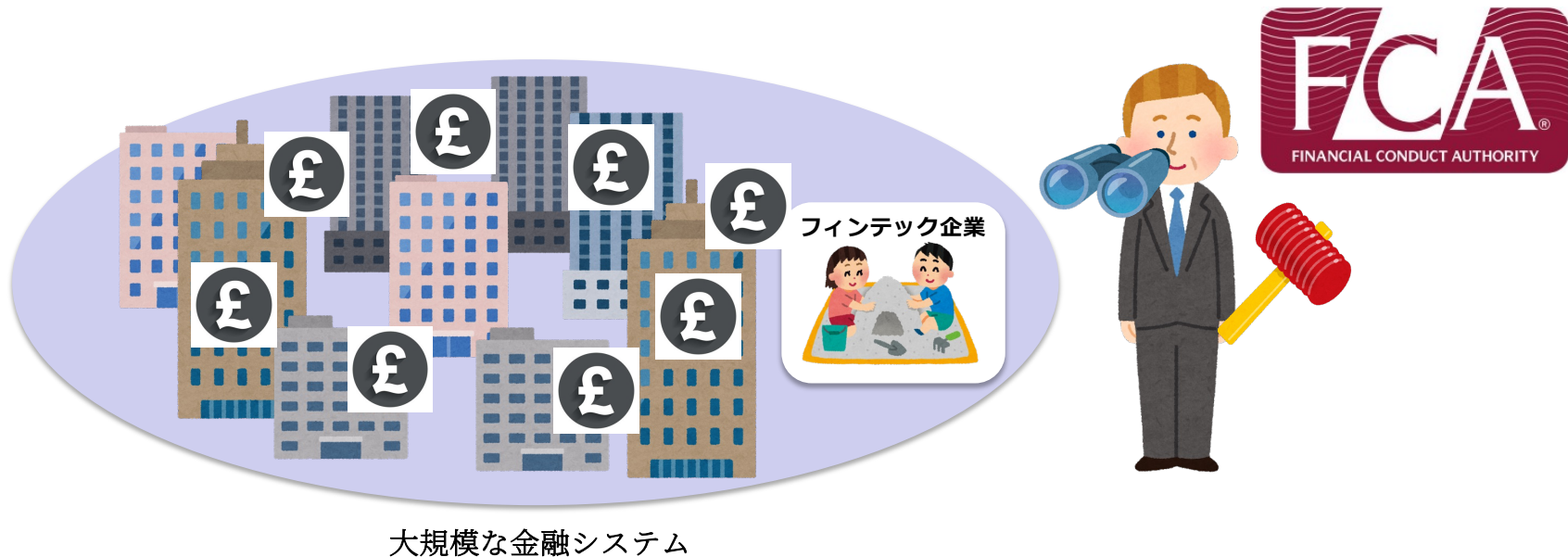
サンドボックス

大規模な社会システムには影響を与えない、影響範囲を限定した規制緩和プログラム

- 期間、範囲、規模などを限定し、公的機関からの監督を受ける
- イノベーションを推進が目的

例：英国 金融行動監視機構（FCA）：フィンテック・サンドボックス・プログラム

承認された参加者の多くがブロックチェーン企業



日本の特区制度（内閣府地方創生推進事務局）

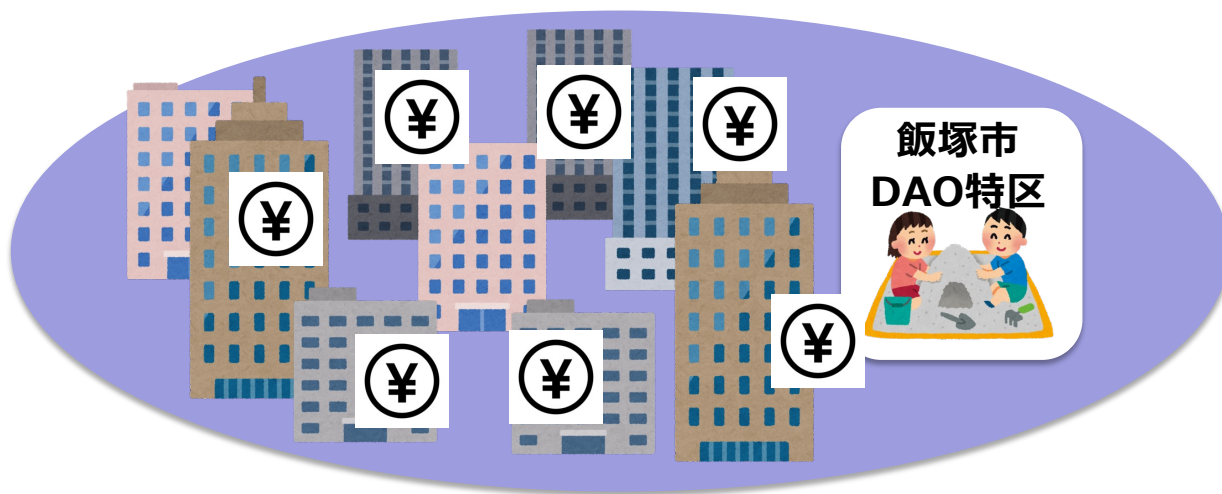
国家戦略特区、構造改革特区、総合特区

令和2年度、改正国家戦略特別区域法

- 地域限定型規制のサンドボックス制度の活用

高度で革新的な技術に関する実証実験を、積極的かつ大胆に実現していく。

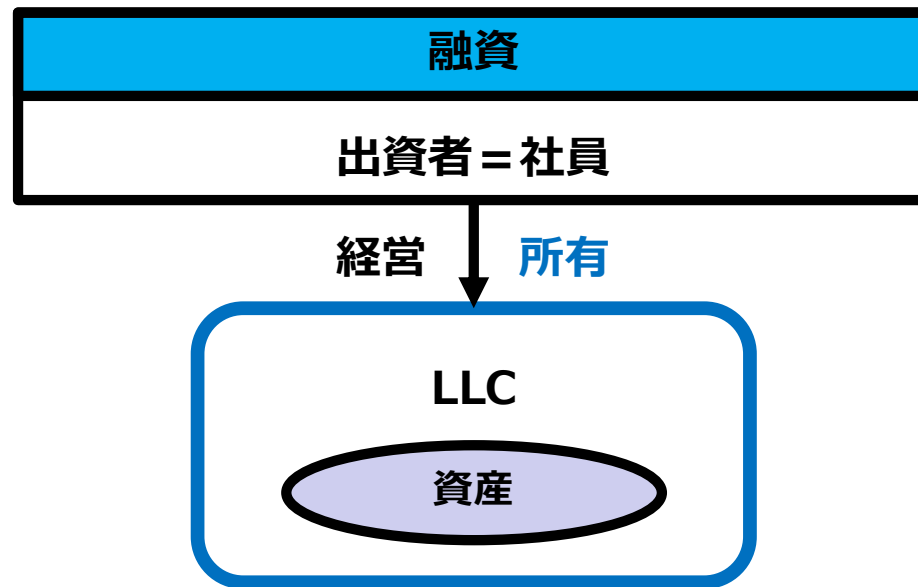
地域を限定するという特性を活かし、安全確保を大前提に、一歩進んだ実証実験の実現に向けて関係省庁が連携しながら取り組みを進めていく。



LLC（合同会社）

会社の所有者と経営者は原則同一

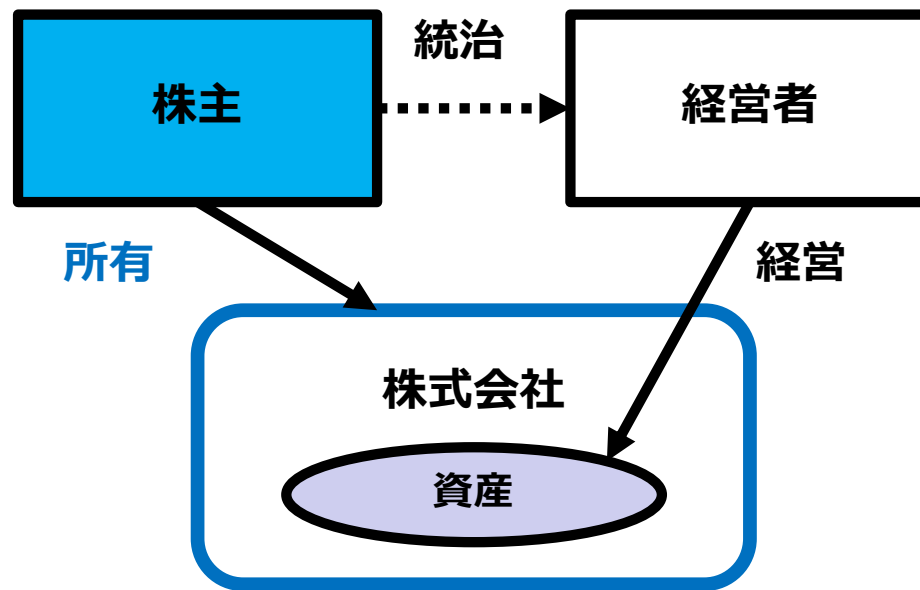
- 出資比率に関係なく利益配分を決めることができる
- 株式という概念がないので資金調達に限界がある（上場できないなど）



株式会社と所有権

所有と経営の分離

- 所有者：株主
- 経営：経営者
- 統治（ガバナンス）：株主の投票で取締役を選出するなど

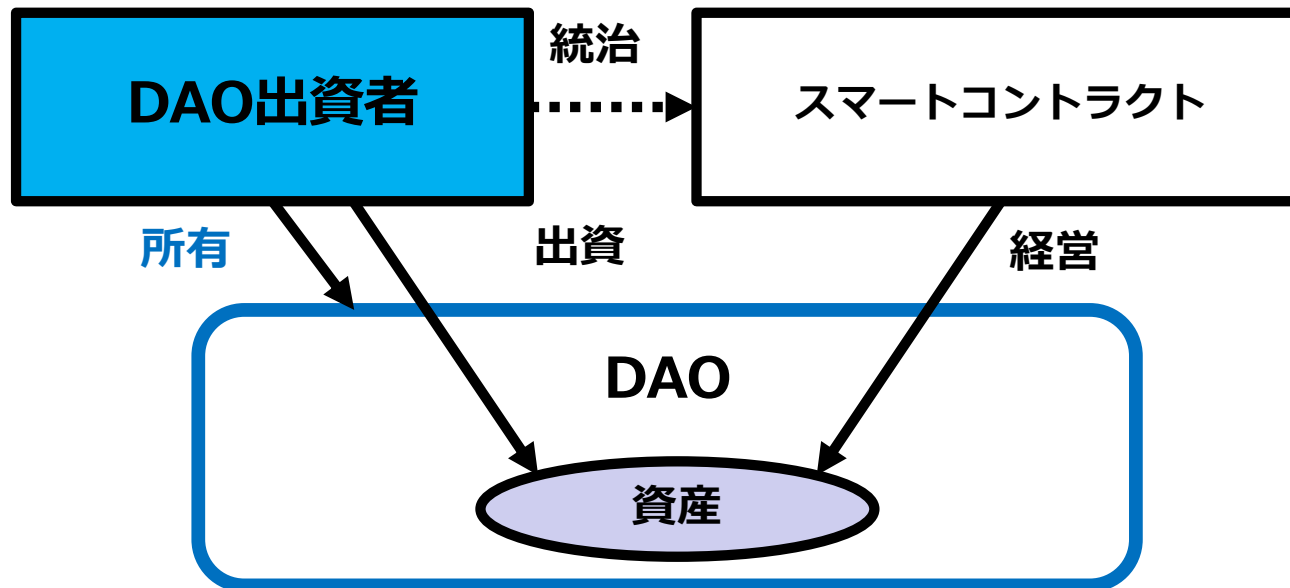


DAOの統治構造は株式会社似ている

所有と経営の分離（株式会社似ている）

- 所有：DAOの投資家／参加者（人間の集団の共同体）
- 経営：スマートコントラクト（ブロックチェーン上で自律的に稼働するプログラム）
- 統治（ガバナンス）：投票によるスマートコントラクトの仕様の提案／選択／修正／承認

Coin voting (ガバナンストークンによる投票)

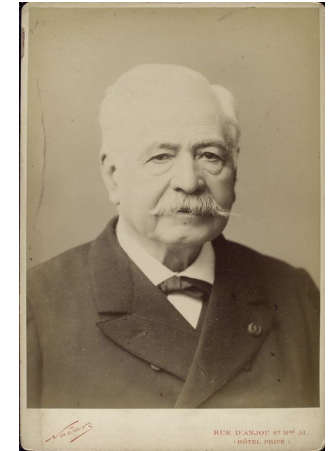


株式会社

国際スエズ運河株式会社

- 株式で資金を調達
- 大規模工事が国家事業ではなく民間の会社が主体

← 渋沢栄一が驚いた



フェルディナン・ド・レセップス

株式会社

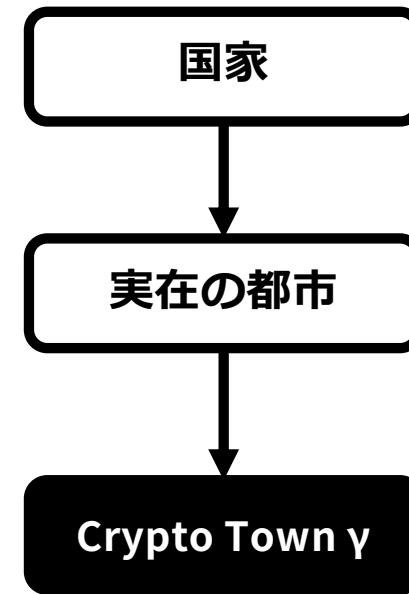
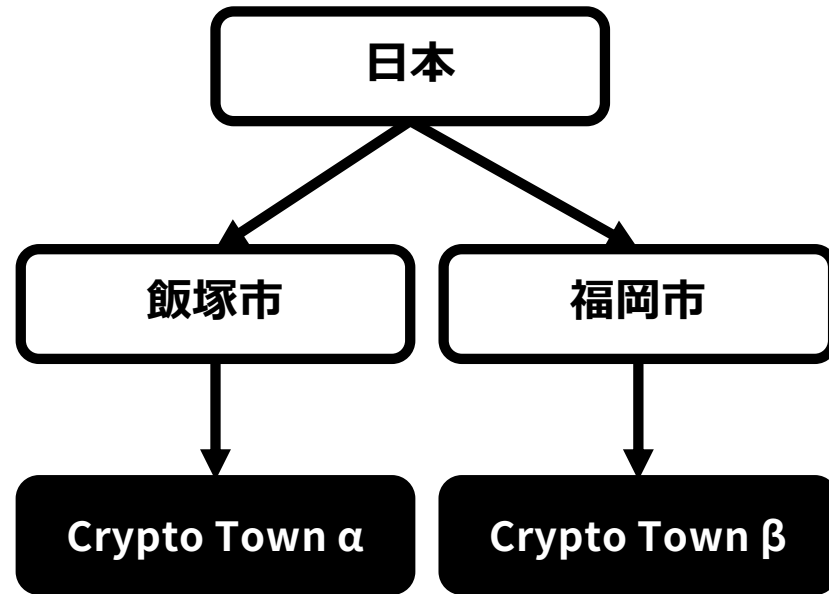
- 大航海時代 → 産業革命（運河、鉄道、石油network） → 資本主義の発展 = 会社設立

スタンフォード, ロックフェラー

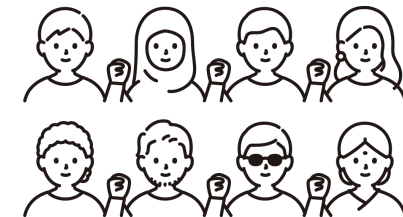
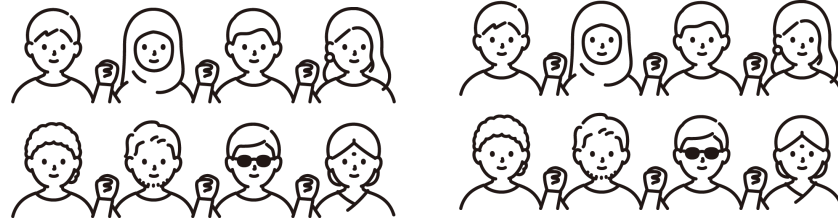
Crypto Towns構想

「秘密の街」ではなく，実在の都市の仮想特区とその市民

Crypto Town = 実在の都市の仮想特区とその市民



市民



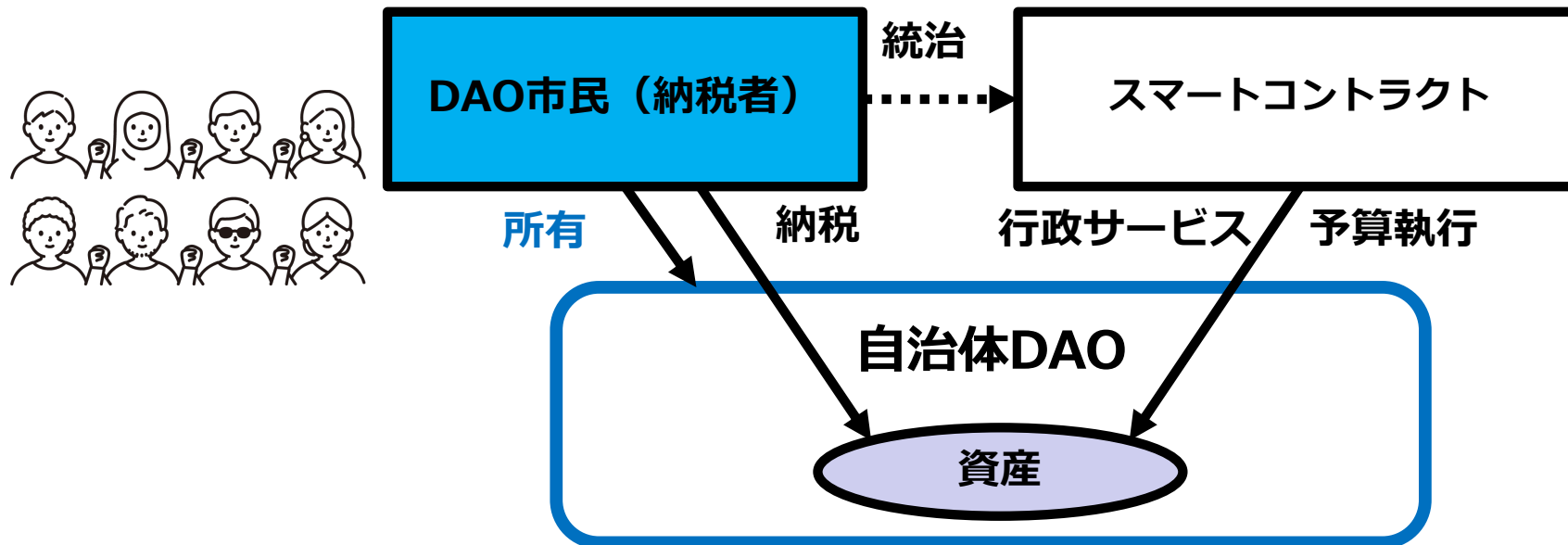
市民

DAOによる仮想国家／自治体

所有と行政機能の分離

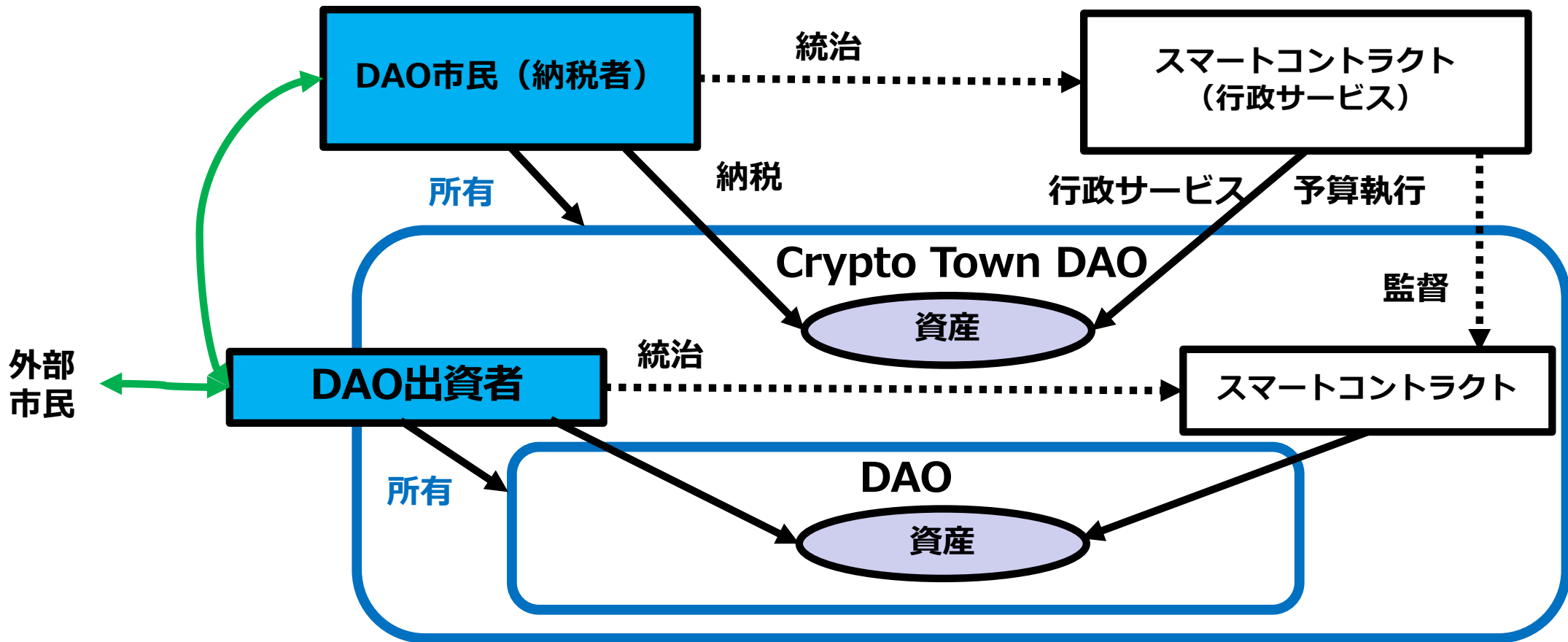
- 所有：納税者である市民
- 行政：スマートコントラクト（ソフトウェアロボットにより執行）
- 統治（ガバナンス）：投票によるスマートコントラクトの仕様の提案／選択／修正／承認

Coin voting (ガバナンストークンによる投票)



自治体DAO (Crypto Town) の下でのDAOの経営

Crypto TownのDAOが存在する



想定するCrypto Town 内のDAO

災害や非常事態が発生したときに、24時間以内に義援金DAOを設立する

- 他の自治体などでは不可能なスピード
- 必要なタイミングで支援を届けることができる
- 義援金を安全に集める（資金洗浄、テロ資金供与、経済制裁などの規制の遵守が可能）
- 集めた義援金は、自治体が主体となって相手に届ける

音楽イベントのDAOも検討中

- ミュージシャンは「雇用関係ではなく出資者」で配当として報酬を得る

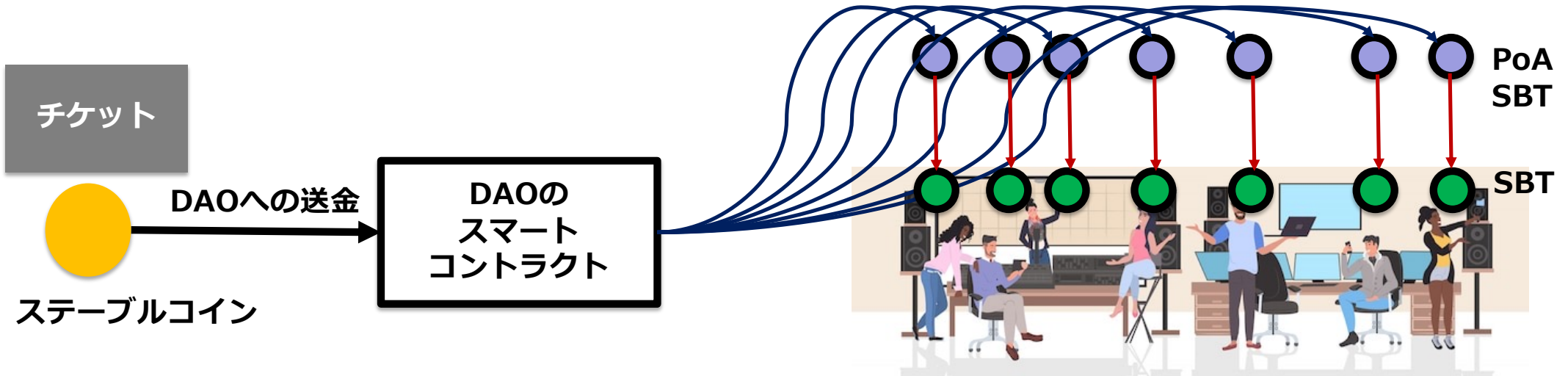
音楽イベントDAOの例

すべての参加者がDAOの所有者

- 関係者は、出資者で、労働報酬ではなく配当を得る権利を持つ
- スマートコントラクトによる配当を受け取る

ステーブルコインの利点

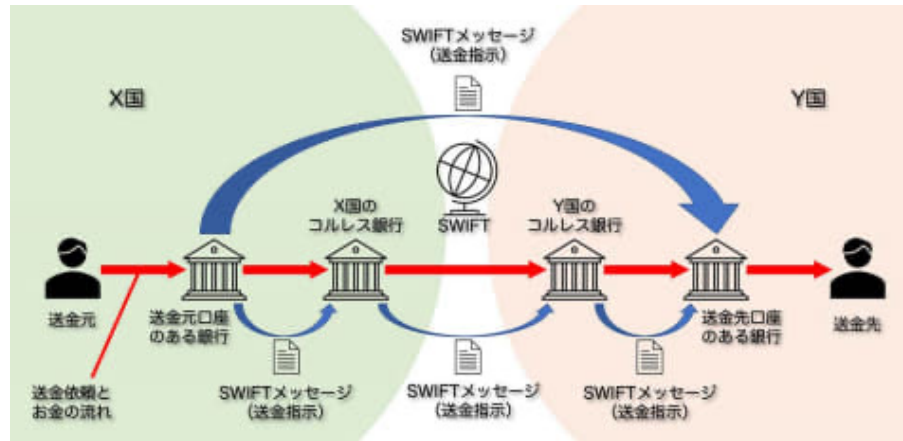
- スマートコントラクトとの連動ができること
- 決済手段（電子マネー）ではなく、自動配当システムとなること



クレジット決済の4コーナーモデル

クレジットカードの利便性

海外送金は非常に敷居が高い



でも

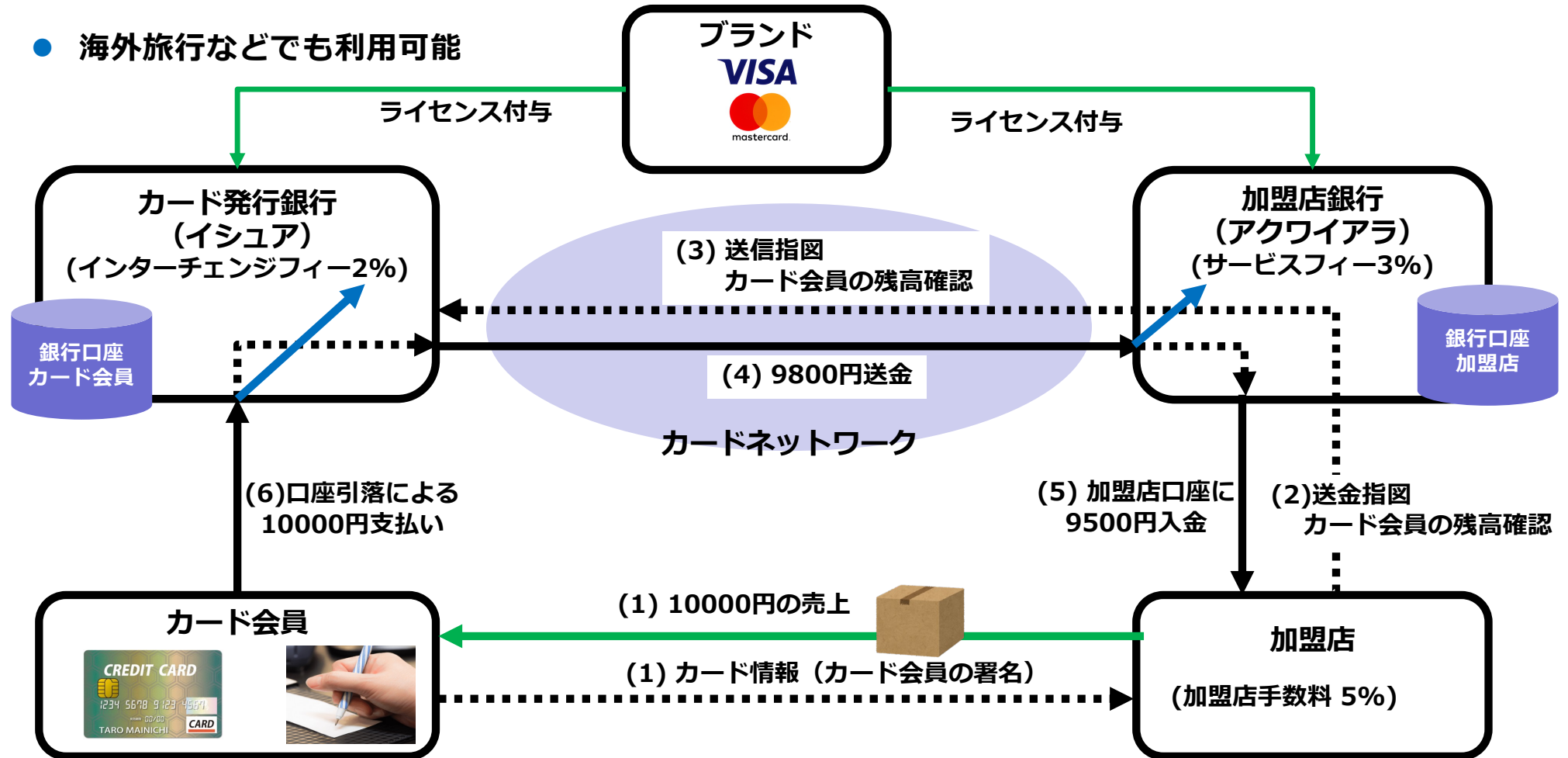
クレジットカードを持っていれば、海外で簡単に買い物ができるのはなぜ？



クレジットカードの4コーナーモデル

地域（国家）毎の銀行業規制を遵守しながら，地域を超えた決済が可能

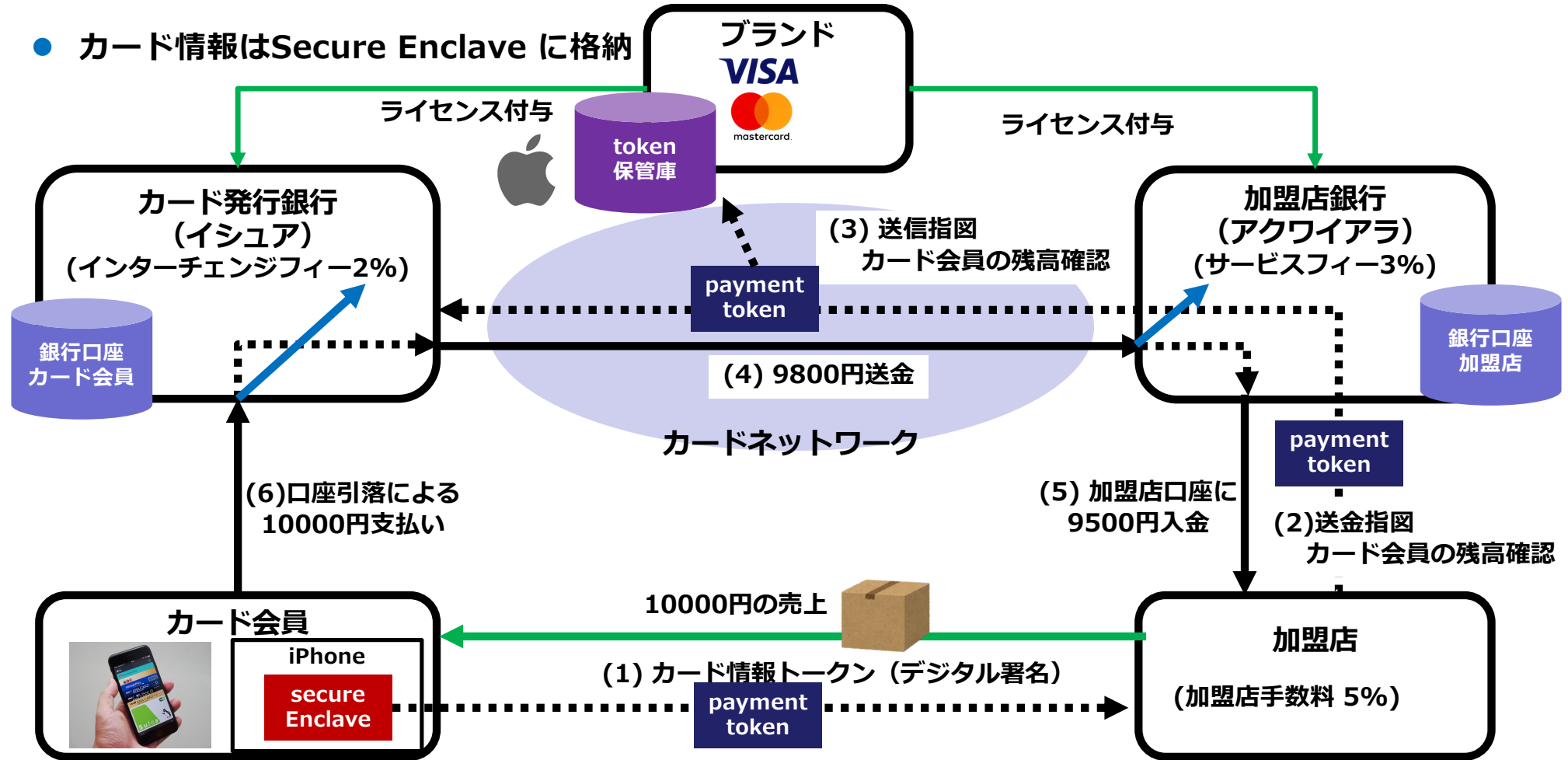
- 海外旅行などでも利用可能



クレジットカードのワレット化とカード情報トークン

スマートフォンアプリのワレットがペイメントトークンを発行し決済ネットワークを還流

- カード情報はSecure Enclave に格納

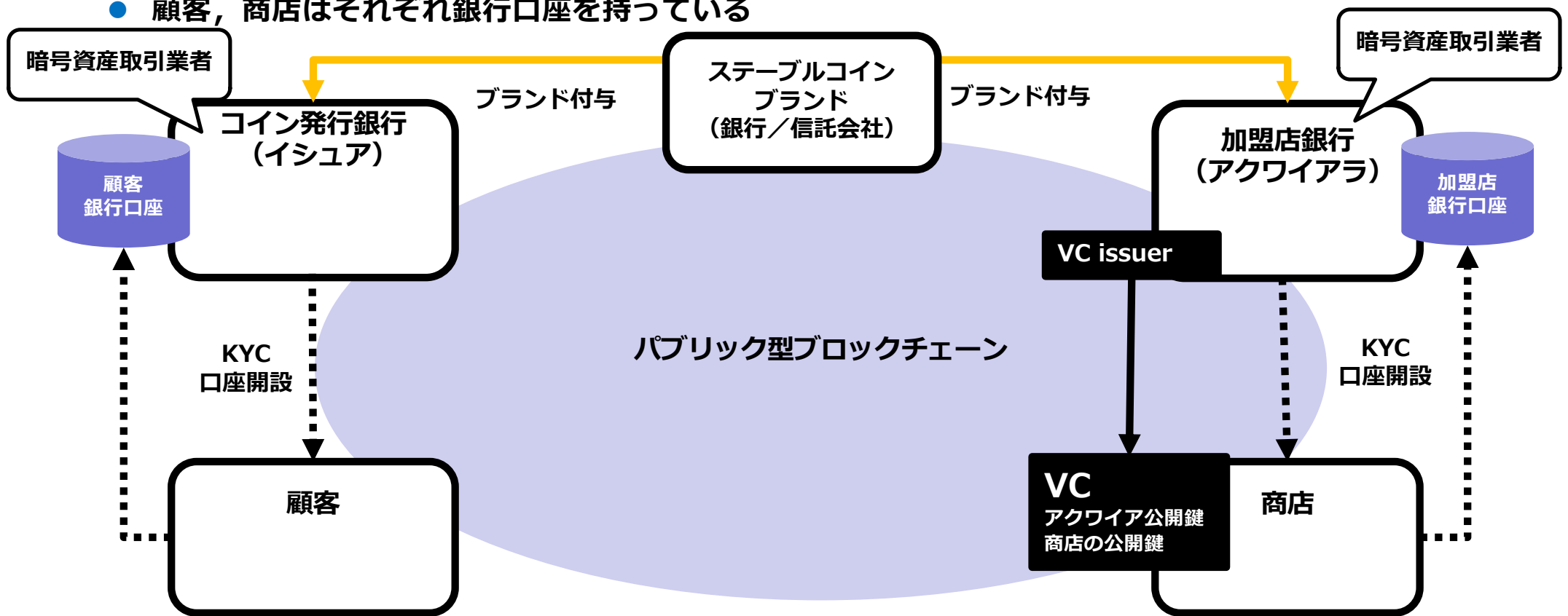


4コーナーモデルによるステーブルコインの提案

基本構造（4コーナーモデル）

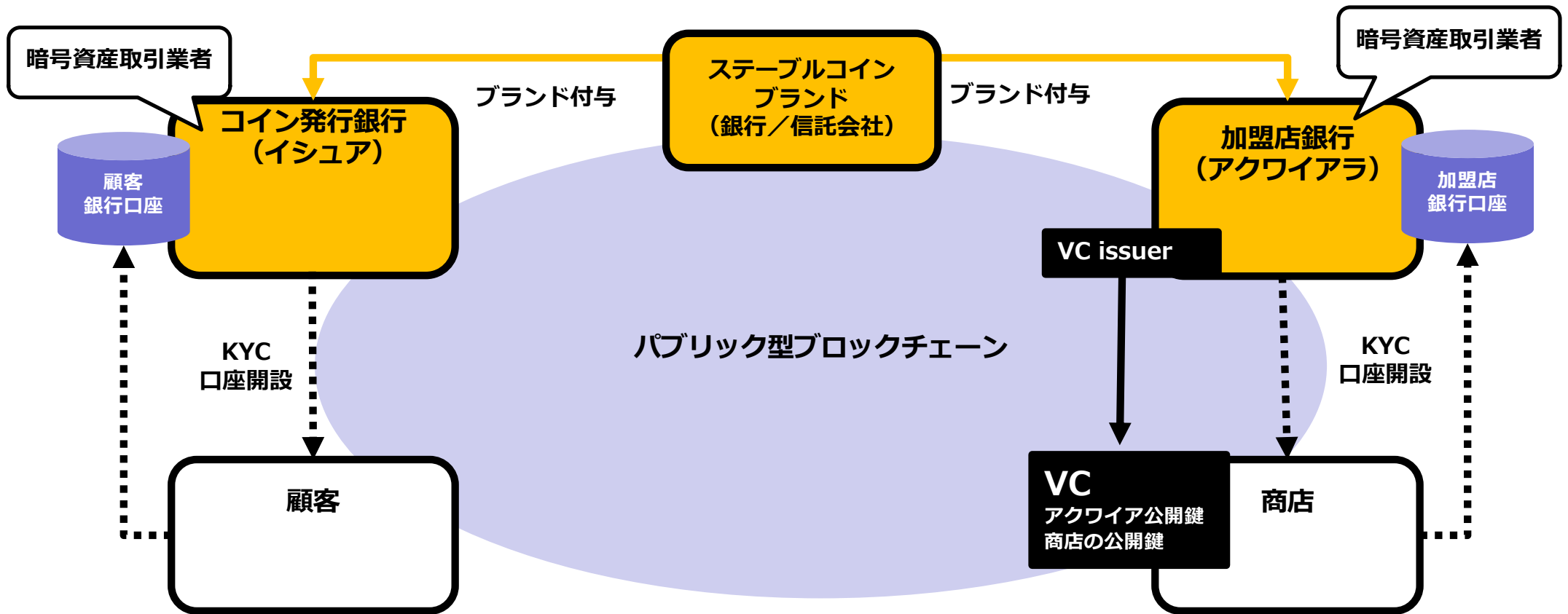
銀行業規制（AML/CFT/経済制裁）の遵守が目的

- パブリック型ブロックチェーンを利用
- 顧客、商店はそれぞれ銀行口座を持っている



銀行の存在が絶対に必要

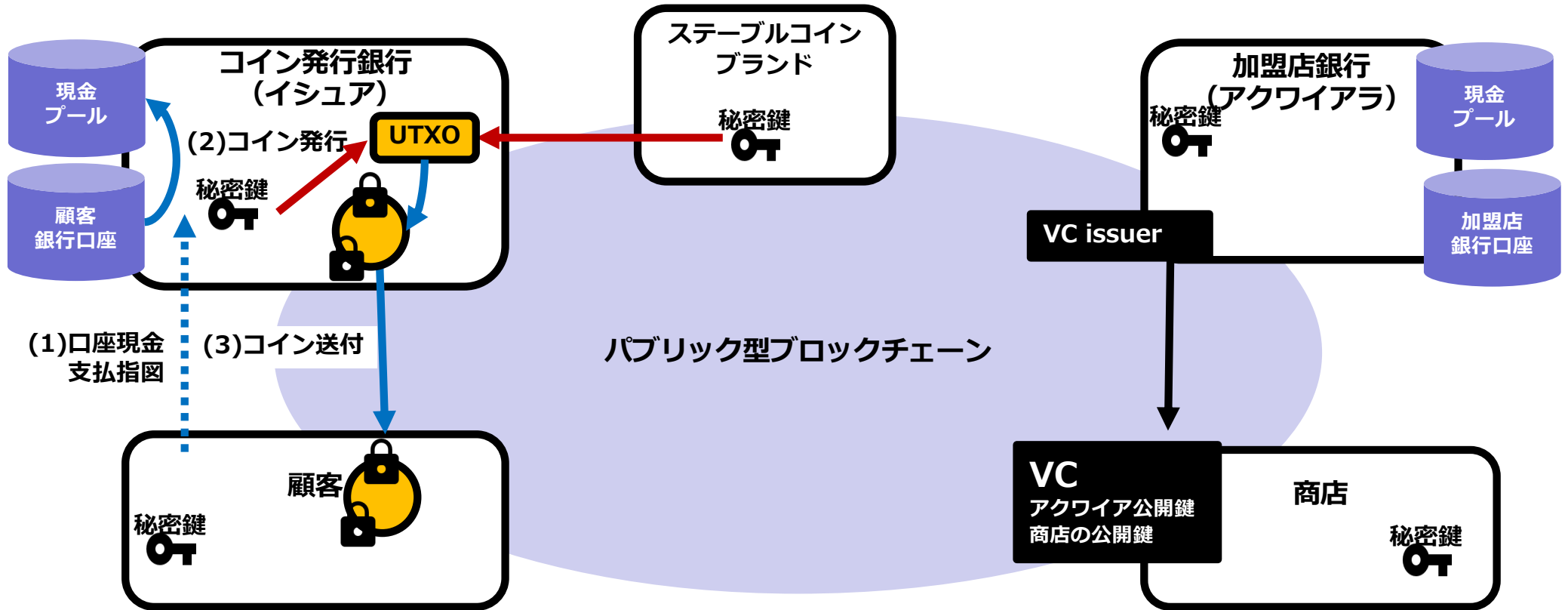
実験に参加してくれる銀行さん募集！



ステーブルコインの発行

銀行が顧客の銀行口座の資金を原資にコインを発行する

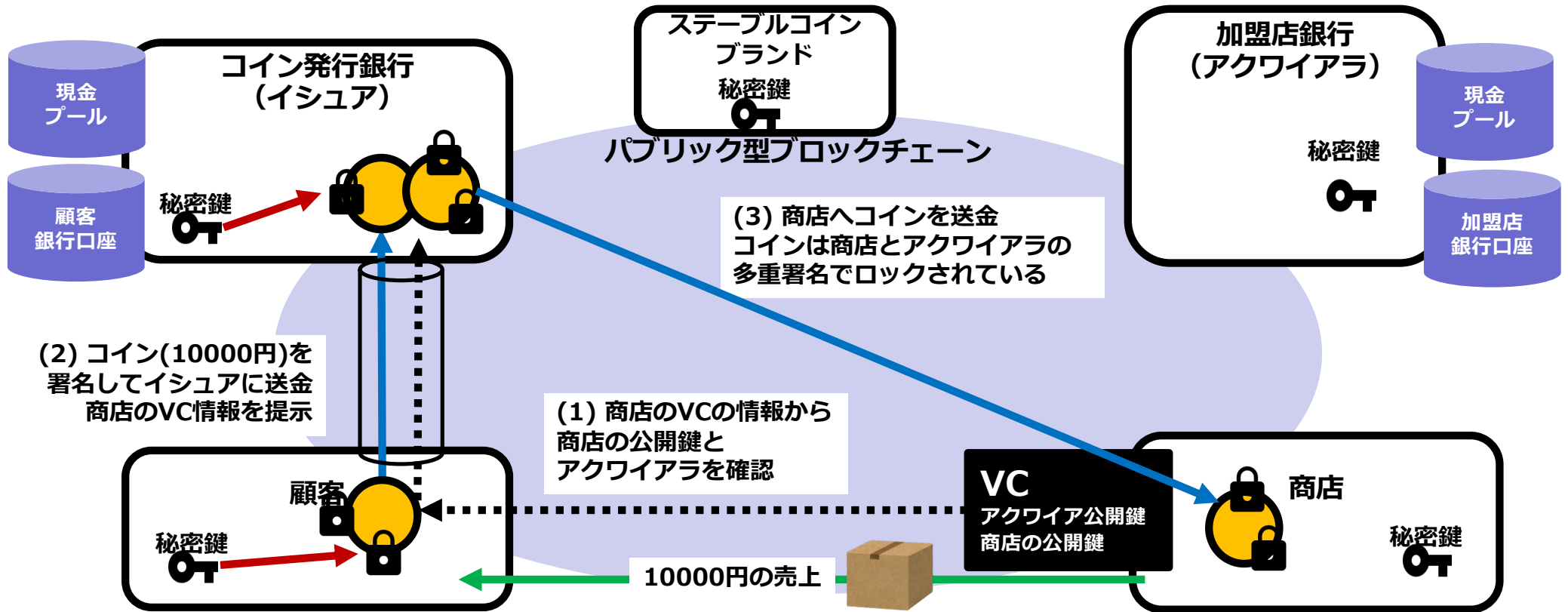
- 発行元UTXOは 2-of-2 multiSigでロックされているのでイシュアとブランドの署名が必要
- 発行したコインは、顧客、イシュア、ブランドの2-of-3 multiSig でロック



ステーブルコインの正規な送金

顧客は直接商店に送金できない

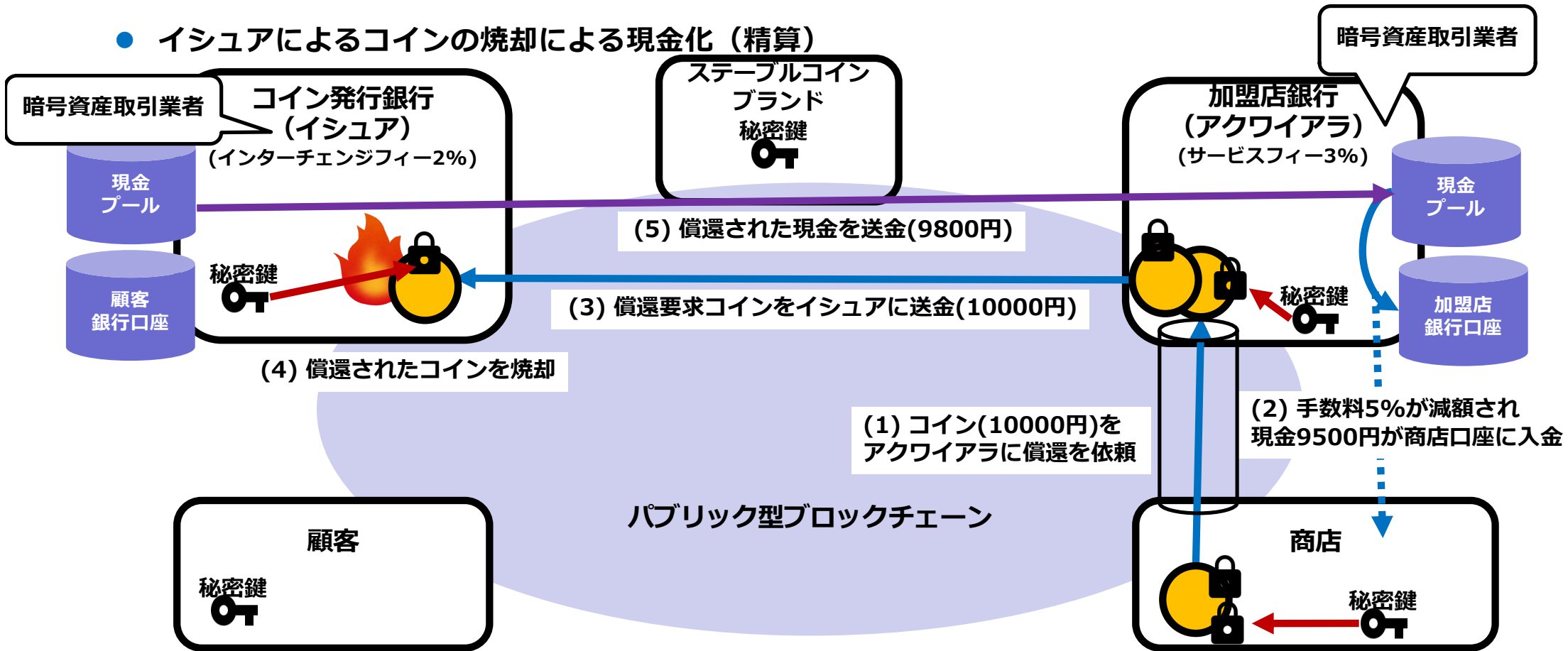
- アクワイアラの情報を含んだVCによるアドレスへ送付
- コインは multiSig でロックされている（顧客 → イシュア の順で署名してアンロック）



ステーブルコインの償還（手数料は仮の設定）

2段階の償還

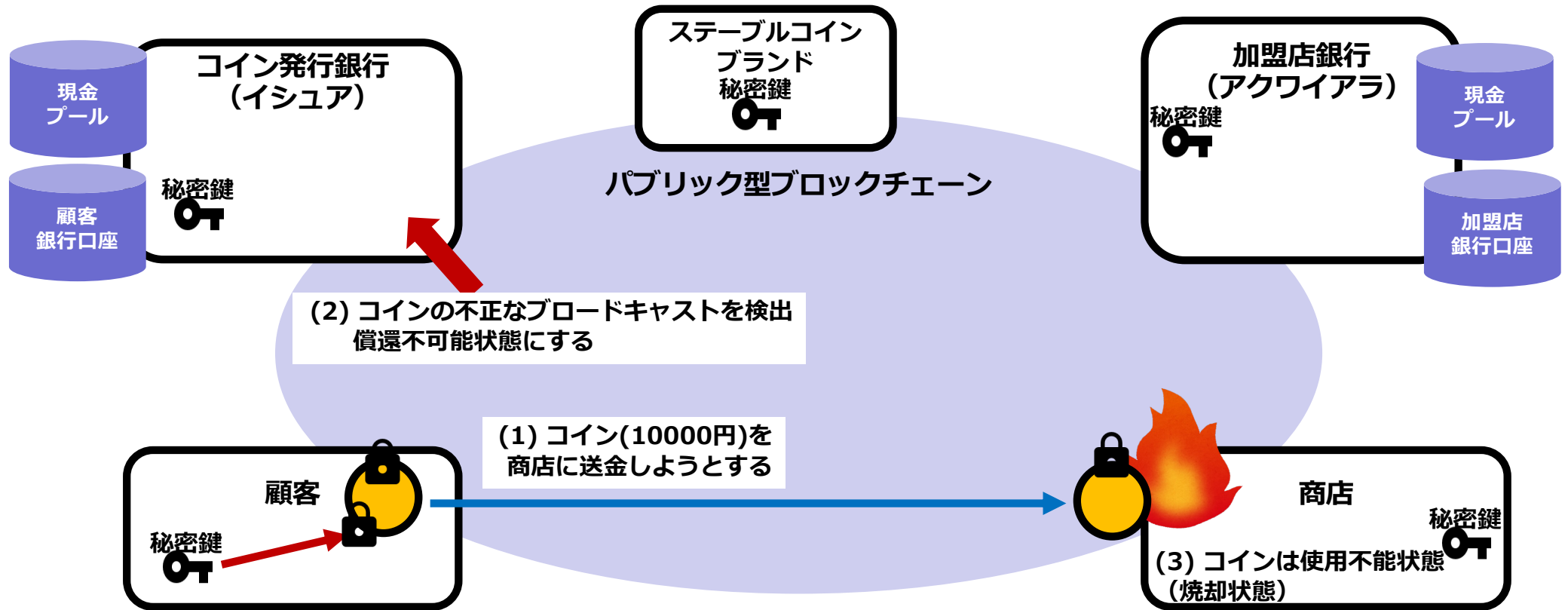
- アクワイアラによるコインの現金化
- イシュアによるコインの焼却による現金化（精算）



コインの非正規な送金ができない理由

コインは多重署名でロックされている

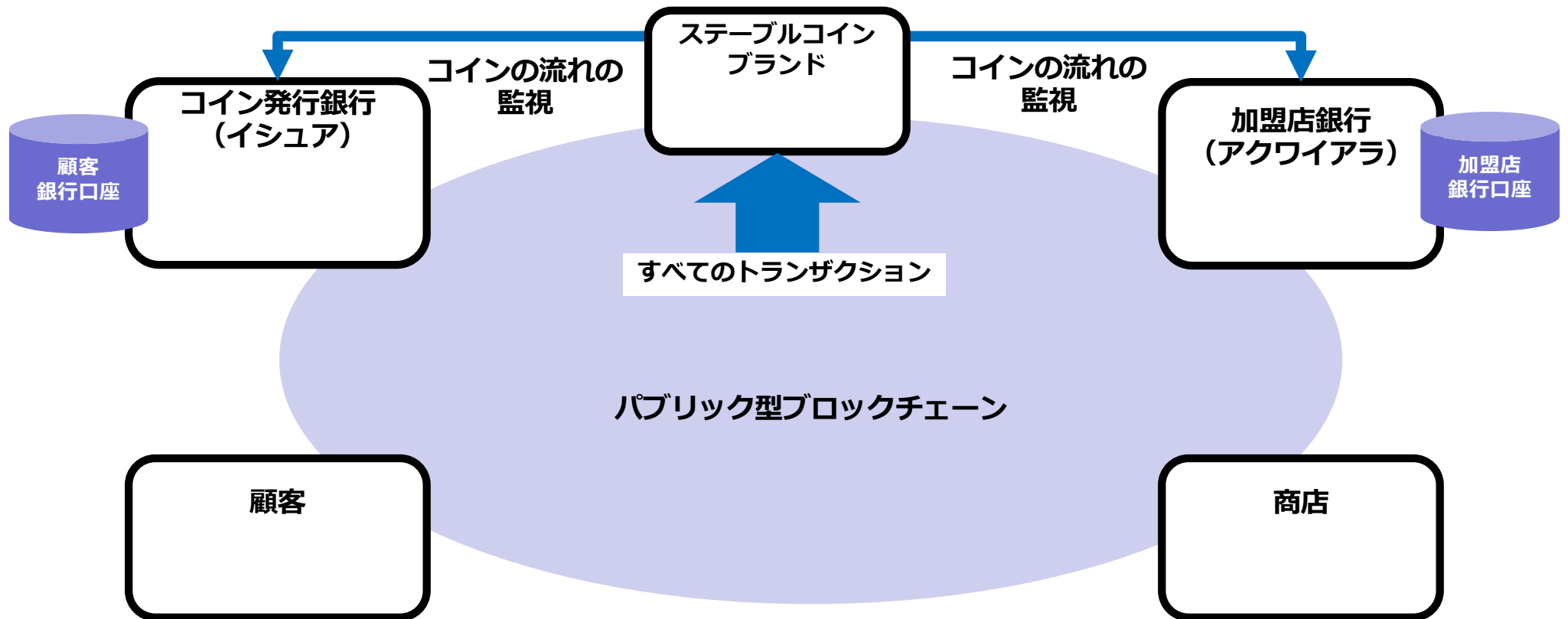
- コインはイシュアかブランドに返却しない限り永久に誰にも使用できない（事実上焼却状態になる）



ブランドによる送金履歴の監視

ブロックチェーンのモニタリングですべてのトランザクションを参照可能

- 特に、イシュアやアクワイアラを経由するコインの流れを監視する



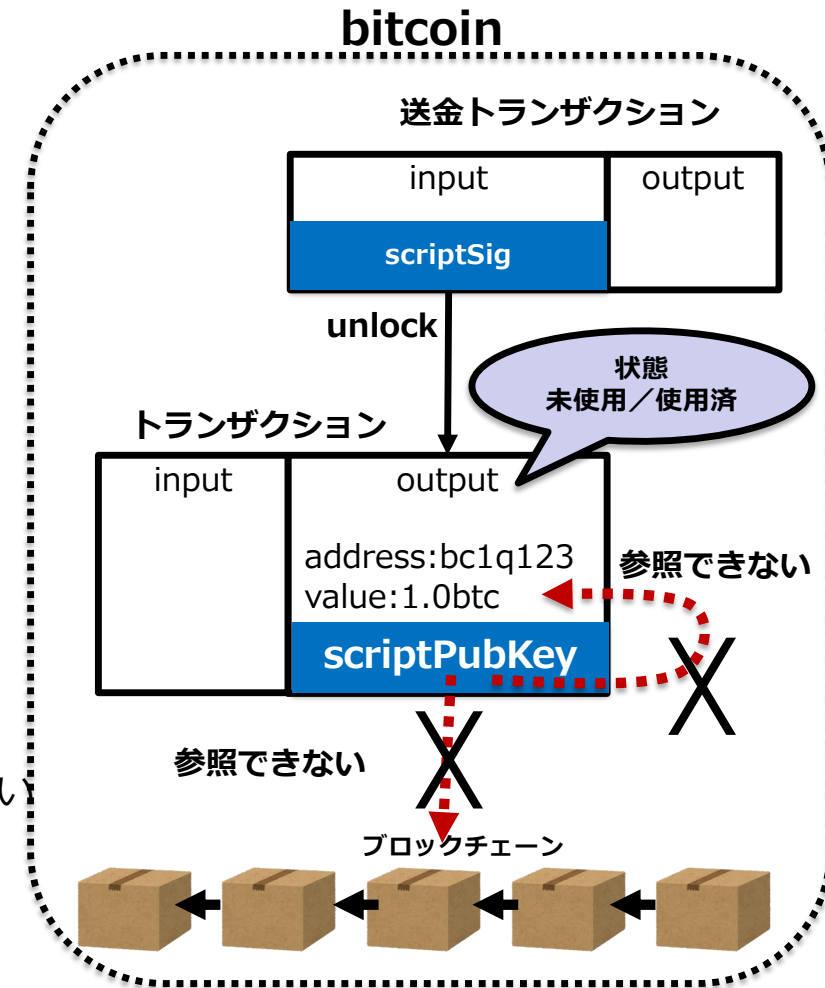
Vitalik Buterin の bitcoin スクリプトへの批判

チューリング完全性の欠如

- ループなどの繰り返し制御を記述できない
(reentrancy は危険性もある)

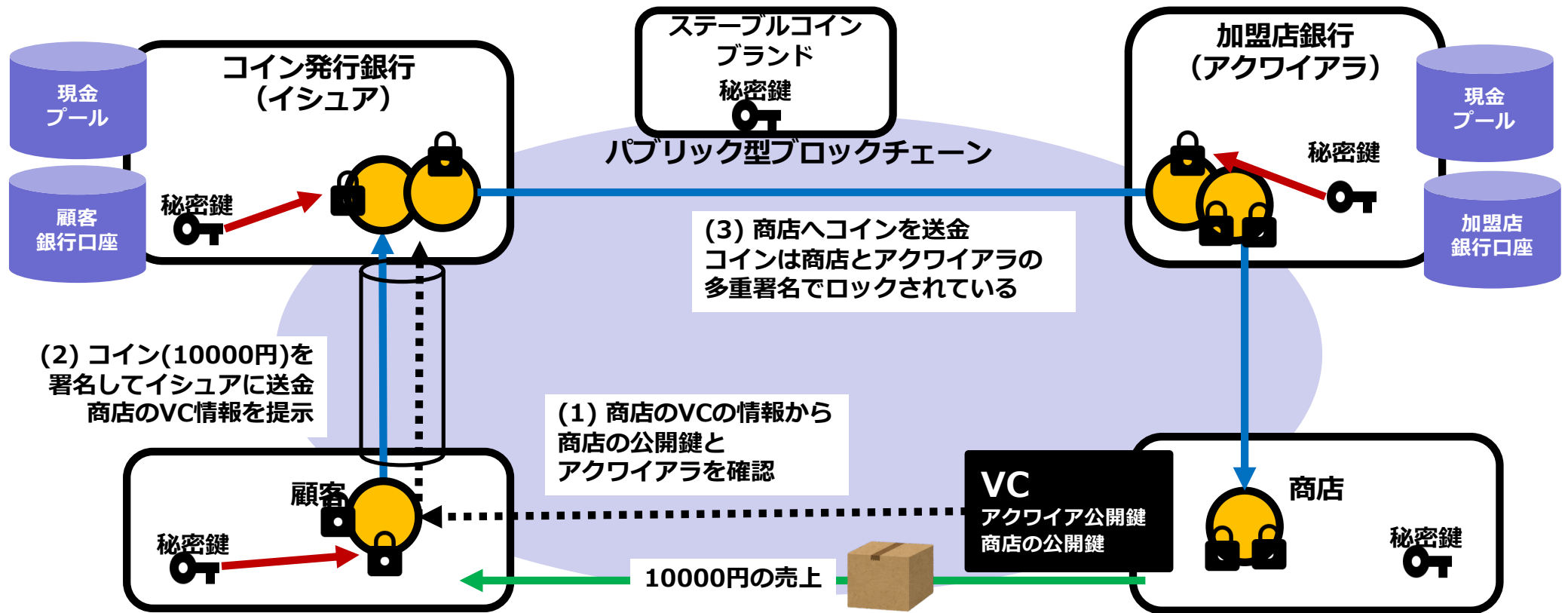
★バリューブラインドネス (こちらの方が重大)

- UTXOの保有金額を参照したり送金先を制御したりできない
(covenants に対応が進められている)
- ステートの欠如
bitcoin のUTXOの状態は未使用/使用済だけ
- ブロックチェーンバラインドネス
スクリプトからブロックチェーンの情報にアクセスできない



covenants が利用可能になった場合のコーナーの曲がり方

アクワイアラ宛のUTXOにパラメタとして商店の公開鍵を入れることができる

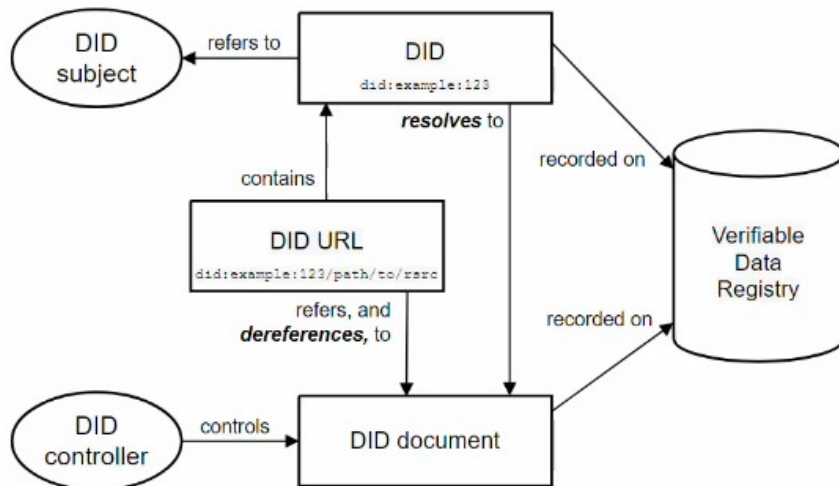


VCとアイデンティティワレットによる市民登録

DID/VCによるアイデンティティ管理

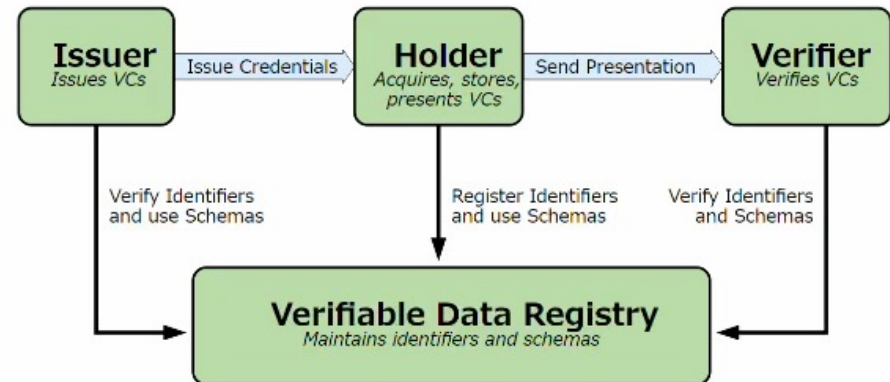
Decentralized Identifiers (DIDs) ¹

- サブジェクト（人、組織、モノ等）自身が特定のレジストリやIDプロバイダーから分離されたグローバルに一意的な識別子（DID）を発行・活用するための仕様を規定する国際標準であり、DIDの形式やそのメタデータを記録したDID Document、及びそれらが登録される検証可能なデータレジストリ、DID Documentの検索・取得を行うDID Resolverといった要素から構成される



Verifiable Credentials (VCs) ²

- 運転免許証などの資格情報について、インターネット・Web上でその内容を検証することができる資格情報を発行・提示・検証するための仕様を規定する国際標準であり、ある資格情報を発行するIssuerと、それを受け取るエンティティであるHolder、資格情報の提示を受けるVerifierが、検証可能なデータレジストリを介して発行・提示・検証を行うデータモデルとなっている



Digital Identity Wallet (DIW)

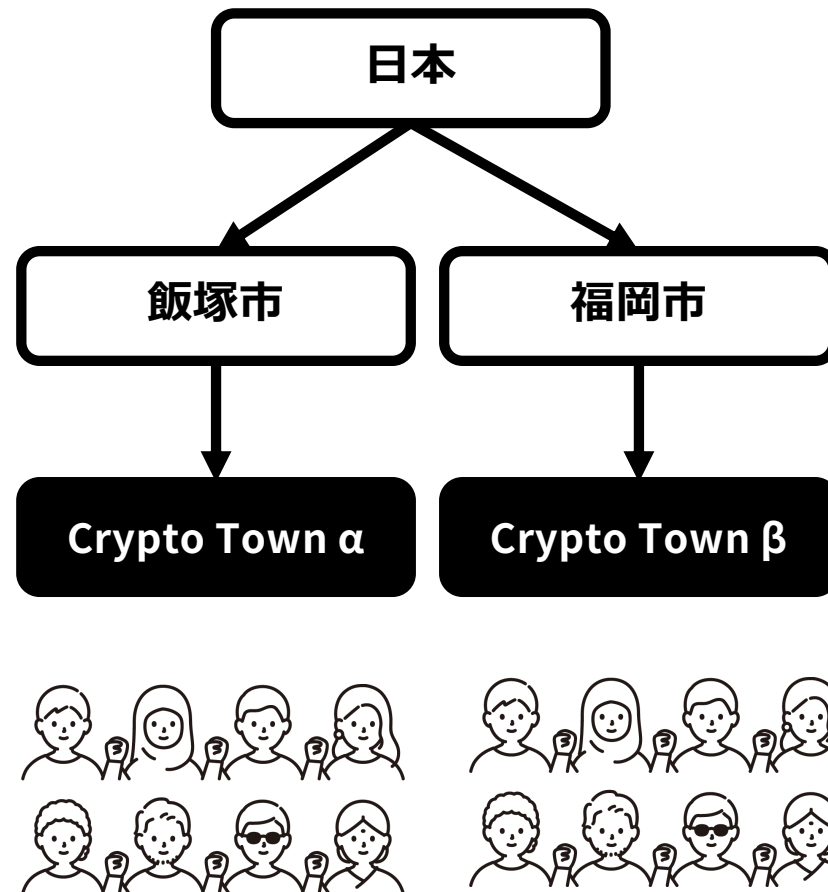
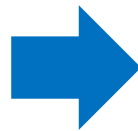
Crypto Town DIW

- VCとして市民登録を行う
- スマートフォンのウォレット
- 暗号鍵 + 生体認証



Verifiable
Credential

市民登録

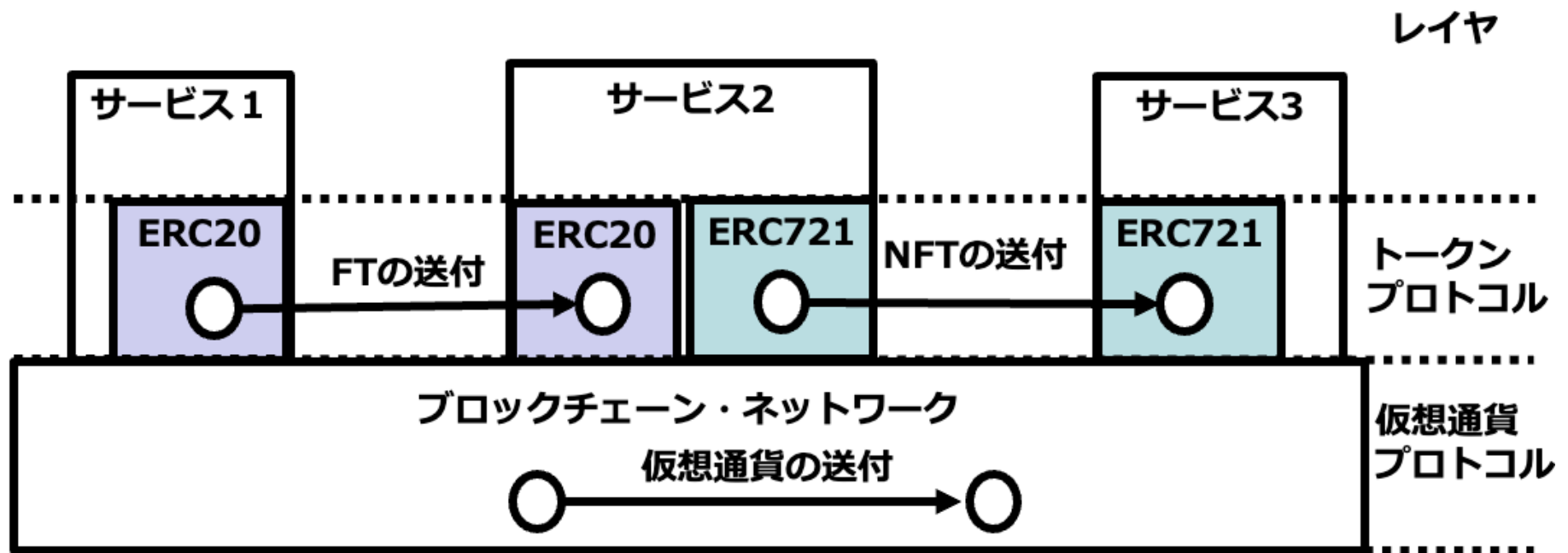


トークンのプロトコル化とERC標準

流通性を持つトークンのプロトコルの例

ERC20: FT（計量可能なトークン）の標準プロトコル

ERC721: NFT（唯一性を持つトークン）の標準プロトコル



流通性を持つトークンを作成する方法

トークンの仕様を標準化文書として提案し、コミュニティに承認してもらうこと

- 承認されると 文書番号が与えられる（ERC20やERC721など）
- 標準化によってプロトコルになる

標準化はブロックチェーンビジネスの主戦場

- Ethereumの標準化文書は ERC
- bitcoinの標準化文書は BIP
- 2023年8月現在， NFT関連の提案ERCは 20以上

Ethereum Improvement Proposals		
All Core Networking Interface ERC Meta Informational		
ERC		
Final		
Number	Title	Author
20	Token Standard	Fabian Vogelsteller <fabian@ethereum.org>, Vitalik Buterin <vitalik.buterin@ethereum.org>
55	Mixed-case checksum address encoding	Vitalik Buterin <vitalik.buterin@ethereum.org>, Alex Van de Sande <avsa@ethereum.org>
137	Ethereum Domain Name Service - Specification	Nick Johnson <arachnid@notdot.net>
162	Initial ENS Hash Registrar	Maurelian, Nick Johnson <nick@ethereum.org>, Alex Van de Sande <avsa@ethereum.org>
165	Standard Interface Detection	Christian Reitwießner <chris@ethereum.org>, Nick Johnson <nick@ethereum.org>, Fabian Vogelsteller <fabian@lukso.network>, Jordi Baylina <jordi@baylina.cat>, Konrad Feldmeier <konrad.feldmeier@brainbot.com>, William Entriken <github.com@phor.net>
173	Contract Ownership Standard	Nick Mudge (@mudgen), Dan Finlay <dan@danfinlay.com>
181	ENS support for reverse resolution of Ethereum addresses	Nick Johnson <arachnid@notdot.net>

ステーブルコインのERC番号取得

コミュニティに承認されプロトコル標準にする

- 標準化文書の作成
- 参照実装（完成）

Ethereum Improvement Proposals		
All Core Networking Interface ERC Meta Informational		
ERC		
Final		
Number	Title	Author
20	Token Standard	Fabian Vogelsteller <fabian@ethereum.org>, Vitalik Buterin <vitalik.buterin@ethereum.org>
55	Mixed-case checksum address encoding	Vitalik Buterin <vitalik.buterin@ethereum.org>, Alex Van de Sande <avsa@ethereum.org>
137	Ethereum Domain Name Service - Specification	Nick Johnson <arachnid@notdot.net>
162	Initial ENS Hash Registrar	Maurelian, Nick Johnson <nick@ethereum.org>, Alex Van de Sande <avsa@ethereum.org>
165	Standard Interface Detection	Christian Reitwießner <chris@ethereum.org>, Nick Johnson <nick@ethereum.org>, Fabian Vogelsteller <fabian@lukso.network>, Jordi Baylina <jordi@baylina.cat>, Konrad Feldmeier <konrad.feldmeier@brainbot.com>, William Entriken <github.com@phor.net>
173	Contract Ownership Standard	Nick Mudge (@mudgen), Dan Finlay <dan@danfinlay.com>
181	ENS support for reverse resolution of Ethereum addresses	Nick Johnson <arachnid@notdot.net>

ステーブルコインの設計目的

資本としてのお金

出資, 税金, 配当, 寄付

まとめ

Crypto Townによる実証

- 自治体との特区申請
- 金融機関の協力
- 資本としてのお金の実現

