Discussion Purpose Only

託された未来をひらく
三井住友トラストグループ

日本銀行CBDCフォーラムWG4

トークン規格とコンプライアンス
海外事例を踏まえた議論

2025年10月14日
デジタル企画部

三井住友信託銀行

目次

- 当資料は、CBDCフォーラムWG4で議論を行うための情報提供を目的として作成されたものです。
- 特定の金融商品の売買を推奨・勧誘するものではありません。
- 当資料は当社が信頼性が高いと判断した情報等に基づき作成しておりますが、その正確性・完全性を保証するものではありません。

1 イントロダクション

1. ディスカッションポイント
2. コンプライアンス（KYC/AML等）対応に関する論点

ディスカッションポイント

2025年/3月のプレゼンテーションでは、MMFトークン（BUIDL）を中心に海外事例を紹介。
パブリックブロックチェーンを活用した金融商品が拡大する中でコンプライアンス・セキュリティなどの観点での事例を紹介して、以下のようなポイントで議論：

相互運用性（interoperability）を意識した規格が必要なことは異論なしだろうが、どのような規格が必要か？
共通の業務＋各社（資産管理等）ごとに発生する対応は異なるが、どのような線引きが必要か？

デジタル通貨に求められる「標準的な機能」とは？
- 送金のみ？　必要なコントロールとは？（保有者・利用ケースの整理）
- 通貨を授受する根拠となる商取引側で適切な相手かを判断するか。（対応アセット・取引への依存）
- （中央銀行）デジタル通貨は「現金代替？」、「預金代替？」、あるいは新しい形態となるのか？
- 人間の判断に近いAI活用ができればリスクベースもルール化できるか？（適合性）
- AIエージェントを利用した取引の決済については新たな機能が必要か？

コンプライアンス（KYC/AML等）対応に関する論点

ルールベースとリスクベース

伝統金融において、KYC/AMLはコンプライアンス対応の中で重要なトピック。
証券会社・銀行等の仲介者を経由して取引を行う（取引所への発注もブローカー経由）から、
仲介者あるいは相対取引を行う金融機関が顧客の管理を行っている。
→確認に必要な書類を顧客から提出いただいた上で、仲介者である各社で判断する。

（ルールベース・リスクベース）
確認する情報について、ルールベースに進めやすいものだけではない。
- 判断が不要な例：国籍・住所・氏名・生年月日の照合は一定の手順（＝ルール）で判断
- 判断が必要な例：適合性確認、（AML観点での）リスク判定は機械的なルールでなくリスクを判断が必要

トークン発行主体が“リスト”を管理しており、その範囲で移転が可能
トークン発行主体とは別にID管理を行う主体がいて、トークンはID保有者の範囲で移転が認められる

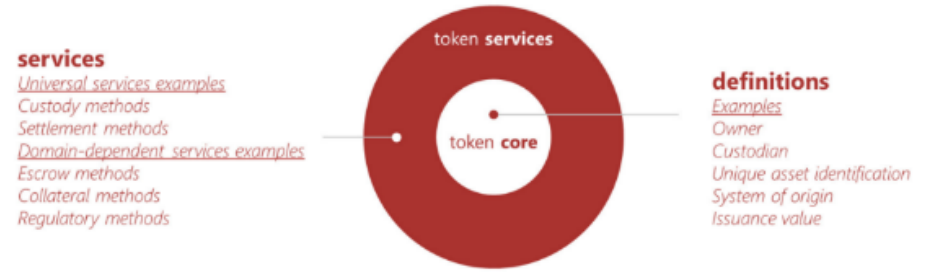
発行体（またはプラットフォーム やスマートコントラクト）によるリスト化や外部認証サービスの活用が考えられる

【参考】ルールを組み込む、アイデア

ビジネスロジックの埋め込み

ビジネスロジックをコードに組込むことで自動執行が期待できることはトークン化のメリットの一つ。
コードの執行には「ルールベース」に落とし込む必要はあるが、外部からのインプット（オラクル）を利用する際にLLMの応答を利用するなど拡張は検討可能か。（ヒトの判断とLLMの出力の信頼性の比較）

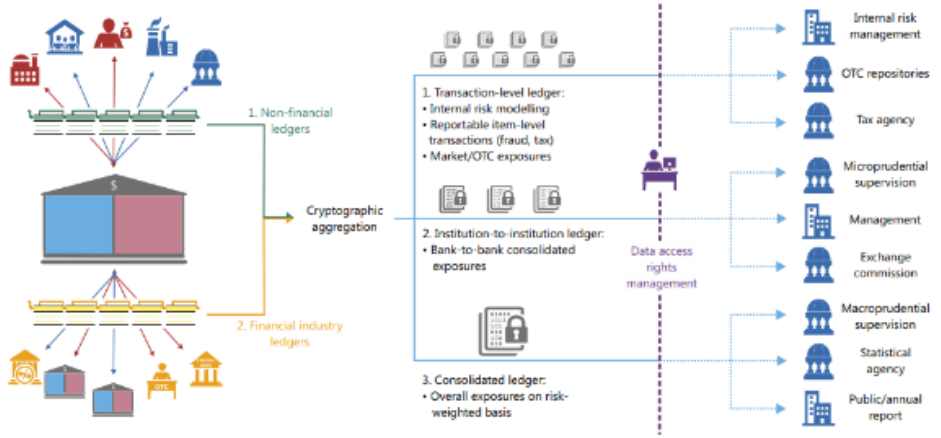
The anatomy of a token: core and service layer — Graph 2



Source: Authors' elaboration.

出所：The tokenisation continuum

Compliance process using embedded supervision — Graph 4



Embedded supervision can verify compliance with regulations by reading the distributed ledgers in both wholesale (symbolised by the green blockchain) and retail banking markets (symbolised by the yellow blockchain). Supervisors could access all transaction-level data. Alternatively, the use of smart contracts, Merkle trees, homomorphic encryption and other cryptographic tools might give supervisors verifiable access just to selected parts of such micro data, or relevant consolidated positions such as to institution-to-institution or sectoral exposures. Firms would only need to define the relevant access rights, obviating the need for them to collect, compile and deliver data.

Source: Author's elaboration.

出所：Embedded supervision: how to build regulation into blockchain finance

【参考】トークン規格の類例

よく使われているトークン規格についての比較。それぞれ独立ではなく拡張や一部機能重複はあり

トークン規格・種類	用途・特徴	譲渡制限	主なデータ	ユースケース
FT（ERC-20）	基本的な規格。	規格では制限しない カスタマイズ実装は可	残高	ステーブルコイン、各種トークン
NFT（ERC-721）	識別子(token id)を付与	規格では制限しない カスタマイズ実装は可	固有ID	デジタルアート、証明書
SFT（ERC-1155）	FT・NFTの性質を組合わせたトークン規格	規格では制限しない カスタマイズ実装は可	固有ID＋数量	CASTの基礎設計、ゲームアイテム（The SandBoc等）
T-REX（ERC-3643）	コンプライアンスを意識IDと組み合わせた保有制限など	連携IDによる制御	連携IDによる制御	セキュリティトークン
Vault（ERC-4626）	資産を預入⇒シェアファンドのような扱い	規格では制限しない カスタマイズ実装は可	シェア残高	DeFiトークン、sToken等

2 トークン規格の活用事例

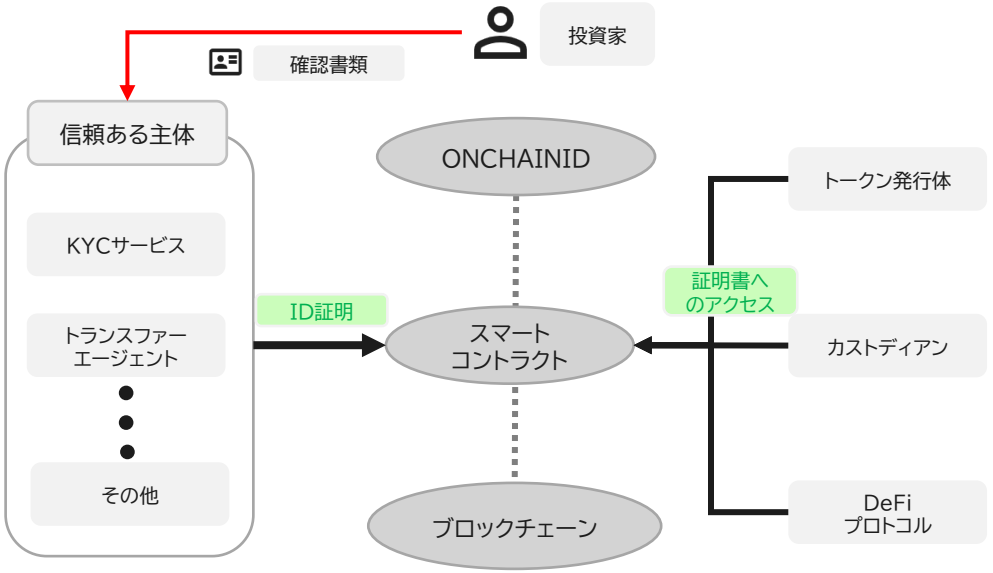
ERC-3643/T-REX

ERC-3643

ERC-3643はT-REX(Token for Regulated Exchange)とも言われ、コンプライアンス対応を念頭に置いて開発された規格。ERC-20をベースにAML/KYC等コンプライアンス機能を付加したもの。
トークン保有に当たってはONCHAINIDなど、外部のKYCの仕組みを利用。

ABN AMROがCPやグリーンボンドの発行で利用実績。
開発を進める団体にDTCCが加入したり、SECのヒアリングで言及されるなど注目を集めている。

出所:ERC-3643 Permissioned Tokens | ERC3643 を参考に作成

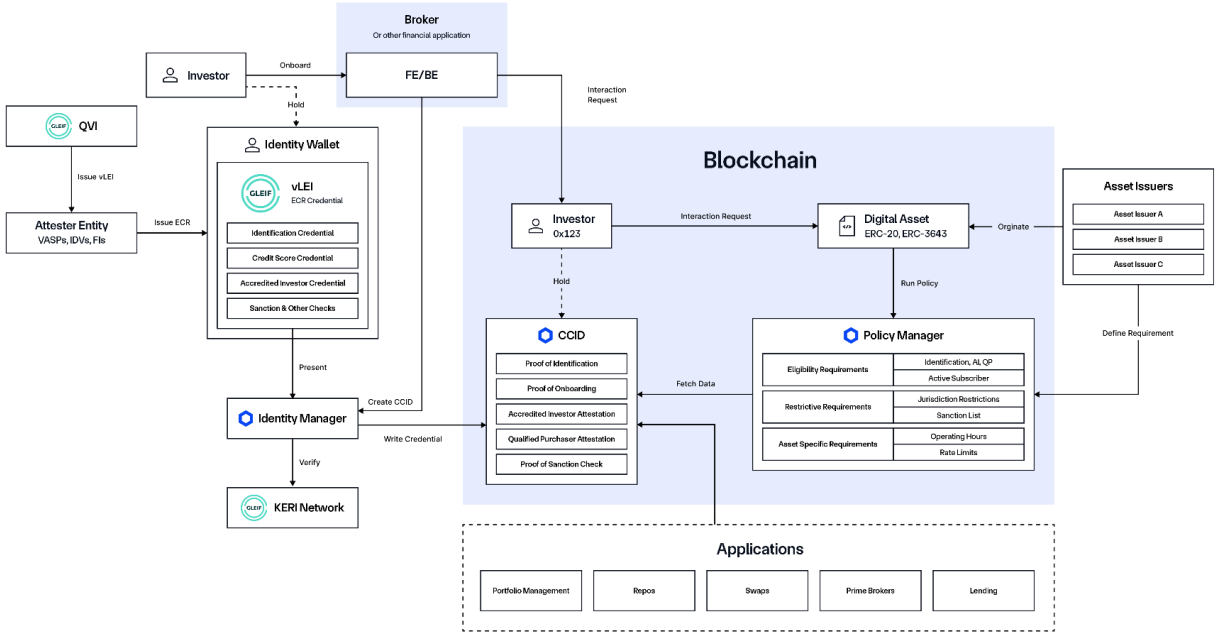


出所:ONCHAINID - The Identity System for Compliant Digital Assetsを参考に作成

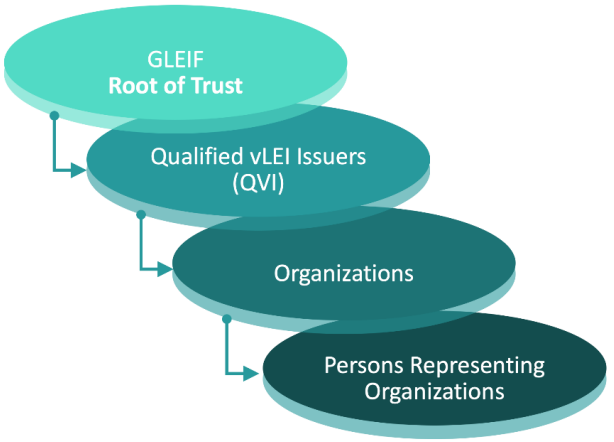
ERC-3643/LEIとの統合

LEIとの統合

Chainlink,GLEIFらと共同してChainlink Automated Compliance Engineのローンチ(2025/6)
GLEIFの提供するvLEI(verifiable Legal Entity Identifier)をT-REXのID機能に統合したもの
ChainlinkからはvLEIが提供する情報とトークンのコントラクトを連携する機能を提供



出典:Chainlink Automated Compliance Engine (ACE): Technical Overview



出所;GLEIF HP LEI を使用したデジタル識別および検証 – 検証可能な LEI (vLEI) - 組織のアイデンティティ – GLEIF

リスクベースを担う認証局(QVI)
vLEI認証を基にルールベースでトークンは移転

CAST（Compliance Architecture for Security Token）

Compliance Architecture for Security Tokens

CASTはSociete Generale Forgeによって提案された規制遵守のためのセキュリティトークンのフレームワーク。
ERC-1155をベースにして必要な機能を追加しており、データモデルはICMA（International Capital Market Association）、Finos CDMやDTI(Digital Token Identifier, ISO 24165)の標準的な規格を統合して利用している。
※あくまでフレームワークであり、実装時には商品に応じた設計を行っている。

カバードボンドの発行やMiCA対応のステーブルコイン(CoinVertible)をユーロ並びに米ドル建で発行している。

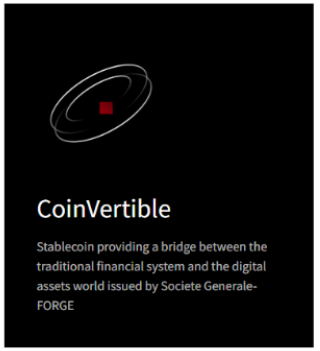
Description

The `SecurityToken` contract is an ERC1155 with a few specifics.

The mapping of the CAST framework with industry standards is based on:

- The ICMA Bond Data Taxonomy pack (1.2) dated 2 February 2024 available **on the ICMA website**,
- The Finos CDM - Common Domain Model in its Version 5.4.0 released on 30 January 2024 available **on the FINOS website**,
- The DTI - Digital Token Identifier, implementing the **ISO 24165 standard** in its version Release number 2.2.0, release date April 2024 available **on the DTIF website**.

出典:Full documentation | CAST Framework & GitHub - castframework/cast2: New CAST Smartcontract based on ERC-1155



出典:CoinVertible | SG Forge

Electronic money on blockchain technology

- USD CoinVertible (USDCV) and EUR CoinVertible (EURCV) combine the stability of fiat currency and availability on public blockchains (Ethereum and Solana)
- After successful onboarding process by SG-FORGE, an institutional investor (for ex. exchange or market maker) can submit subscription for USDCV and EURCV
- The institutional investor can buy USDCV, 1:1 by sending USD to SG-FORGE bank account or buy EURCV, 1:1 by sending Euro to SG-FORGE bank account
- SG-FORGE sends USDCV or EURCV to the institutional investor's wallet
- USDCV or EURCV can be redeemed 1:1 against fiat USD (for USDCV) or EUR (for EURCV)

Technical implementation through the CAST* Framework provides streamlined solutions that are compatible and compliant with traditional financial practices, e.g. know-your-customer (KYC) and anti-money-laundering (AML) regulations.

(*) The Compliant Architecture for Security Token (CAST) framework provides practical open-source propositions for distributed ledger technology integration within current financial infrastructures.

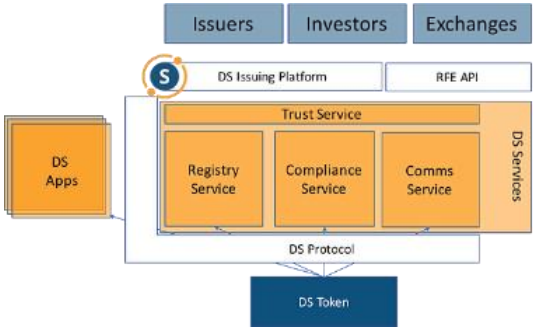
DS Protocol（Securitize）

DS Protocol

BUIDLなどを取り使うSecuritizeではDS Protocolという規格にてホワイトリスト形式を利用。
米国でのST取扱いにおいては、Securitize社がTransfer Agent（名簿管理人）の役割を担っている。
DeFiプロトコルAaveと連携して規制トークンを利用したステーブルコインの調達プログラム

DS Protocol

- ERC-20 を拡張し、KYC/AML・転送制限・投資家属性管理 など法令遵守機能を組み込み
- Trust/Registry/Compliance Services により、発行者・投資家・取引条件をオンチェーンで管理
- 証券ライフサイクル全体をスマートコントラクトで処理可能



引用：Introducing DS (Digital Securities) protocol: Securitize's Digital Ownership Architecture for complete lifecycle management of security tokens | by Carlos Domingo | securitize | Medium

sToken（ERC-4626準拠）

- 「資産⇔シェア変換」を表現し、金融でいう「ファンド口」をオンチェーンで標準化した
- 分散型金融（Aave, Yearn, Lido など）の運用トークンを共通の形式で扱え、アグリゲータ統合が容易
- sToken は ERC-4626 を利用した事例でBUIDLをsBUIDLへ変換して分散型金融で利用可能に。

DAMA2 / ”Layer1-2-3”Solution

Digital Asset Management Access（DAMA）

DAMA 2は、ドイツ銀行、Memento Blockchain、Interop Labs（Axelar Network）の協力により開発。
デジタル資産市場への参入障壁、特に流動性の断片化、複雑性、アクセシビリティの問題を解決を目指した「レイヤー1-2-3」アーキテクチャを持つトークン化プラットフォーム。

Layer 3: The User Application Interface	ユーザが直感的な操作を可能にする機能を準備。 標準化プロセス、ガスレス機能などをアプリストアのように提供
Layer 2: The Capabilities Platform	ZKPに対応したMemento Blockchainを利用 特定のユーザにのみ取引を開示する（当局監査等）managed privacy
Layer 1:The Security Foundation	レイヤー2から提出されるゼロ知識証明を検証し、取引の正当性を保証。 万一の事態に備え、公開された記録の完全性と回復可能性を確保。

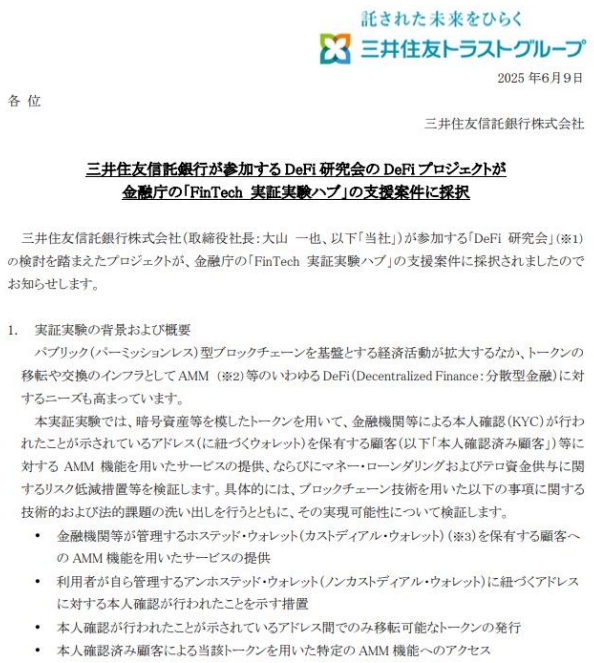
出典:DAMA 2 Lite Paper Jun 17 2025 を参考に作成

【参考】(国内事例)金融庁実証実験ハブでの実証について

- 銀行・証券・信託・暗号資産交換業者からなる「DeFi研究会」の実証実験が金融庁実証実験ハブの支援案件に採択
- パブリックブロックチェーンを基盤とする分散型金融を金融機関による認証が済んだ環境で提供する方法を検討

本実証実験では、暗号資産等を模したトークンを用いて、金融機関等による本人確認(KYC)が行わ れたことが示されているアドレス(に紐づくウォレット)を保有する顧客(以下「本人確認済み顧客」)等に 対する AMM 機能を用いたサービスの提供、ならびにマネー・ローンダリングおよびテロ資金供与に関 するリスク低減措置等を検証します。具体的には、ブロックチェーン技術を用いた以下の事項に関する 技術的および法的課題の洗い出しを行うとともに、その実現可能性について検証します。

- 金融機関等が管理するホステッド・ウォレット(カストディアル・ウォレット)を保有する顧客へ の AMM 機能を用いたサービスの提供
- 利用者が自ら管理するアンホステッド・ウォレット(ノンカストディアル・ウォレット)に紐づくアドレス に対する本人確認が行われたことを示す措置・
- 本人確認が行われたことが示されているアドレス間でのみ移転可能なトークンの発行
- 本人確認済み顧客による当該トークンを用いた特定の AMM 機能へのアクセス



託された未来をひらく
三井住友トラストグループ

2025 年6月9日

各 位

三井住友信託銀行株式会社

三井住友信託銀行が参加する DeFi 研究会の DeFi プロジェクトが金融庁の「FinTech 実証実験ハブ」の支援案件に採択

三井住友信託銀行株式会社(取締役社長:大山 一也、以下「当社」)が参加する「DeFi 研究会」(※1)の検討を踏まえたプロジェクトが、金融庁の「FinTech 実証実験ハブ」の支援案件に採択されましたのでお知らせします。

1. 実証実験の背景および概要

パブリック(パーミッションレス)型ブロックチェーンを基盤とする経済活動が拡大するなか、トークンの移転や交換のインフラとして AMM (※2)等のいわゆる DeFi(Decentralized Finance:分散型金融)に対するニーズも高まっています。

本実証実験では、暗号資産等を模したトークンを用いて、金融機関等による本人確認(KYC)が行われたことが示されているアドレス(に紐づくウォレット)を保有する顧客(以下「本人確認済み顧客」)等に対する AMM 機能を用いたサービスの提供、ならびにマネー・ローンダリングおよびテロ資金供与に関するリスク低減措置等を検証します。具体的には、ブロックチェーン技術を用いた以下の事項に関する技術的および法的課題の洗い出しを行うとともに、その実現可能性について検証します。

- 金融機関等が管理するホステッド・ウォレット(カストディアル・ウォレット)(※3)を保有する顧客へ の AMM 機能を用いたサービスの提供
- 利用者が自ら管理するアンホステッド・ウォレット(ノンカストディアル・ウォレット)に紐づくアドレス に対する本人確認が行われたことを示す措置
- 本人確認が行われたことが示されているアドレス間でのみ移転可能なトークンの発行
- 本人確認済み顧客による当該トークンを用いた特定の AMM 機能へのアクセス

出典:250609.pdf

3 デジタル通貨を考える

現金・預金によるUXとデジタル通貨への示唆

- 対面で日本銀行券を利用する「現金」と日銀当座預金を基礎として市中銀行の「預金」が一般利用者の「通貨」
- さらに決済手段として資金移動業資金や前払式決済手段、さらには電子決済手段などが取扱われている。

現金型

対面・台帳レス（現金その場限り）
匿名あるいは利用者を制限しない
券面の信用は保証されていて、どこでも使える。
→仕組は用意をされていて、信用の上に成立。

預金型

非対面利用も可。
利用に当たって登録（KYC）が必要。（一部除）
一般的に台帳はサービス提供者が個別管理。
→ネットワーク間の連携は課題（⇒オープンバンキングの議論）

デジタル通貨の導入での期待

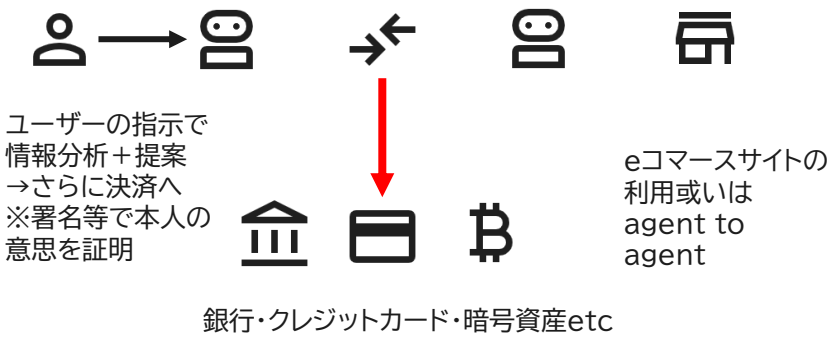
誰でも、簡単に利用できる決済手段
→ICカード等をかざすだけで利用できる、等
個人間で、なるべく環境に依存せず利用できる
P2Pでもコミュニケーションのお作法はみんな同じ

共通のプロトコル（interoperability）
→効率化した処理の実装。
→どのプロトコルにするかの論争
各種サービスと効率的に結合ができる（composability）
→コミュニケーションのレールに組込める

AIエージェントとおカネ

- AI活用の拡大ペースはとても早く、情報分析・資料作成だけでなく一定の裁量の下で利用されるエージェントも出現。
- AIエージェントが商取引を行う際には資金決済を手当てする必要があり、APIなどで金融機関にアクセスなどを利用。
- Googleからは”Agent Payment Protocol”が公表されており、裁量（＝ユーザーの意向、intent）は暗号学的に検証が可能なVCとして与えられ、その裁量の範囲でAIエージェントが取引を進める。
- 但し、「人間と同じ」設計である必要あるか？AIにとって現金相当な仕組みはありえるのか？

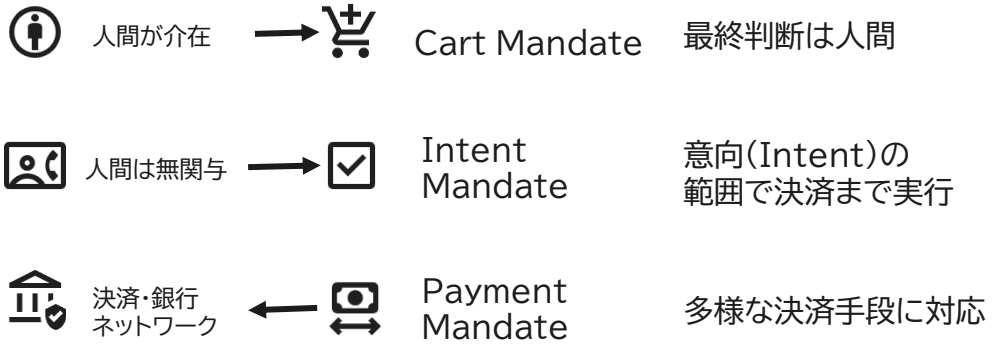
情報収集⇒分析⇒決済まで人の介在なく実行



決済手段は人間と共通であり続けるべき？

筆者作成

Google：Agent Payment Protocol



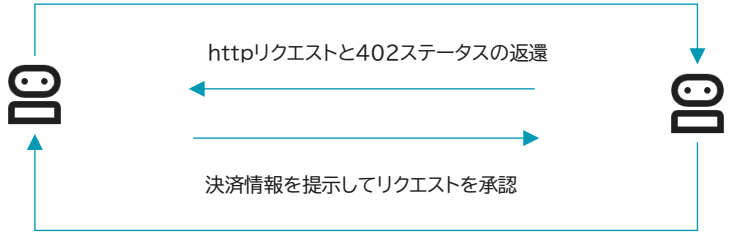
出所：The Agent Factory - Episode 8: Agent payments, can you do my shopping? の図表の拙訳

AIエージェントとおカネ/x402

- HTTP 402「Payment Required」は本来「支払いが必要」を示す予約コードで、長年未活用。
- Coinbase らはこの枠組みを活用し、オンチェーン決済を HTTP レベルに組み込む x402 プロトコル を提唱。

x402;HTTP通信内の決済コミュニケーション

- 402 は「支払いが未完了」を示すステータスコード(200:成功、404;存在しない、等)で、従来は標準利用が未定義だったが、マイクロペイメントや課金 API に検討されているもの。
- x402 は、API やウェブサービスが 支払い要求 → 決済 → リソース提供 を HTTP レスポンス／リクエストの流れで実現
- 支払は主に USDC 等のステーブルコイン を想定し、オンチェーンで検証する。
- AI エージェントや M2M(機械同士)取引が自律的に決済可能になる基盤を目指す。
- 課金モデルの柔軟化(従量課金・都度払い)が容易になり、従来の API キー管理やカード決済より摩擦が少なくなる。



①登録
アカウントをAPI提供者で作成

②決済情報登録
API提供者に決済情報を登録

③購入
クレジット購入またはサブスク登録

④セキュリティ
APIキーの管理

⑤利用
決済⇒利用

①リクエスト
AIエージェントがHTTPリクエストを送って(決済要求の)402を受領。
(アカウント作成が不要※)

②決済
AIエージェントがそのまま
ステーブルコインで支払う。

③利用
APIアクセス承認。
手動手続きやAPIキー管理不要

出所:x402 - The internetnative payment を基に作成

※Coinbase Developer Platform(CDP)でファシリテータとしてKYTに対応する機能を提供する準備も。

ディスカッションポイント（再掲・加筆）

パブリックブロックチェーンを活用した金融商品が拡大する中でコンプライアンス・セキュリティなどの観点での事例を紹介して、以下のようなポイントで議論：

相互運用性（interoperability）を意識した規格が必要なことは異論なしだろうが、どのような規格が必要？
共通業務【業界標準・フレームワーク】＋各社の個別対応【実装】について、どのような線引きが必要？
コンプライアンス対応には画一的なルールではリスク対応は困難だが、AIなどテクノロジーを活用してルールでカバーできる範囲を拡張できないか？【リスクの言語化・データ化】

デジタル通貨に求められる「標準的な機能」は？
- 送金のみ？　必要なコントロールとは？（保有者・利用ケースの整理）
- 通貨を授受する根拠の商取引で適切な相手かを判断するか。（対応アセット・取引への依存）
- （中央銀行）デジタル通貨は「現金代替？」、「預金代替？」、あるいは新しい形態となるのか？
- 人間の判断に近いAI活用ができればリスクベースもルール化できるか？（適合性）
- AIエージェントの利用など、変わりゆく【商取引・コミュニケーションと親和性のある】「通貨」とは？

- Appendix

【参考】vLEIの仕組みについて

LEIは法人の識別子としてグローバルに利用されている規格。（ISO17442）
vLEIはDID、VC（KERI）を利用してLEIをデジタル化したもの（ブロックチェーンを使うとは限らない）

DID/VC

Figure 1 A simple example of a decentralized identifier (DID)

引用：Decentralized Identifiers (DIDs) v1.1

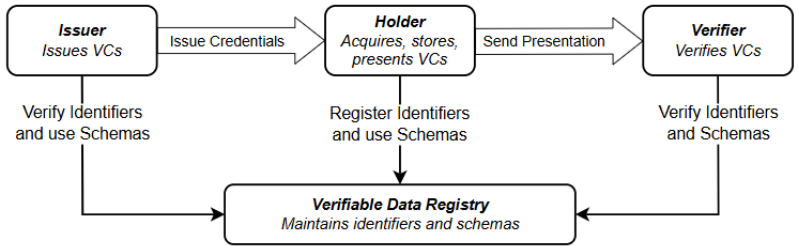
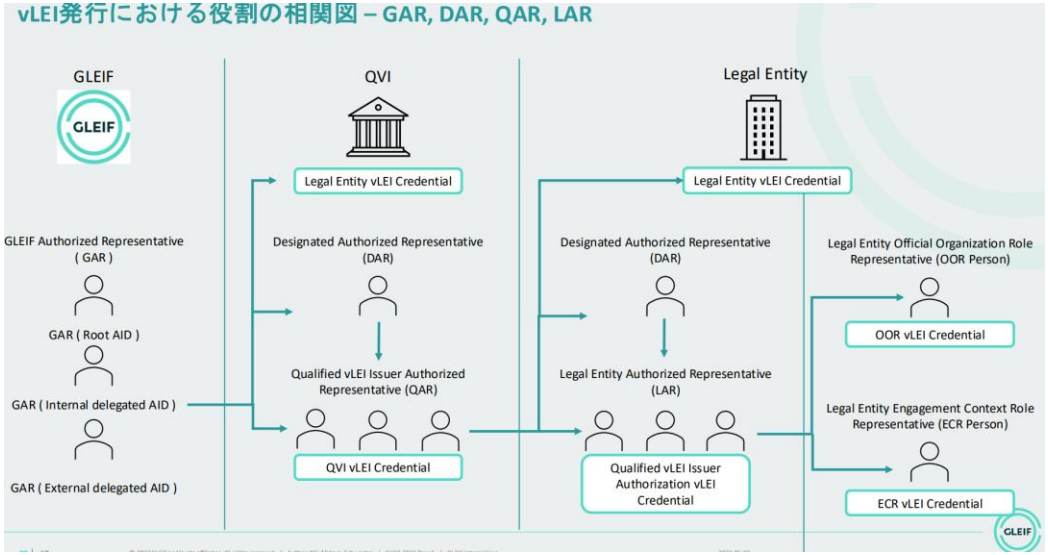


Figure 1 The roles and information flows forming the basis for this specification.

引用：Verifiable Credentials Data Model v2.0

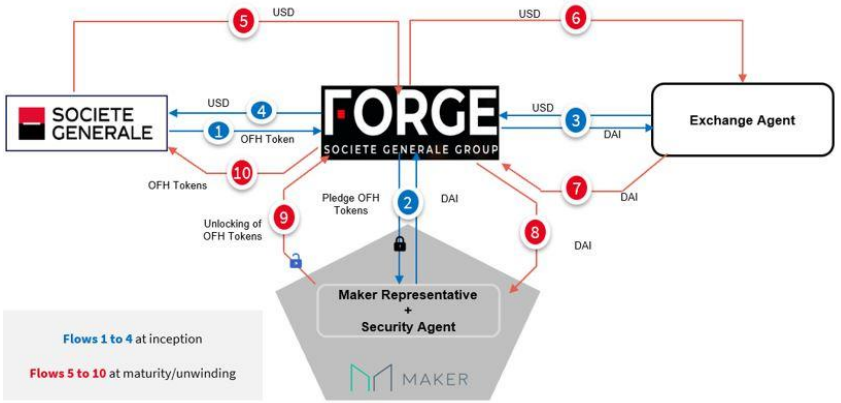
vLEI



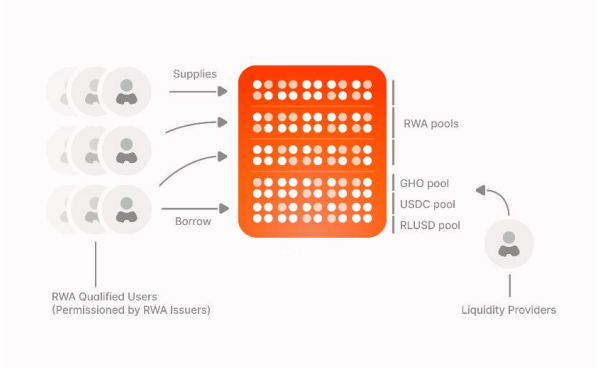
引用：ISOパネル（第9回）資料「LEI活用の世界的な広がりと新サービスvLEIの特徴・ユースケースについて」

RWA取引とステーブルコイン

Societe Generale Forgeはカバードボンドをトークン化したOFHを旧MakerDAO(現SKY)のコラテラルに利用することを提案し、OFHトークンを利用して(広い意味での)ステーブルコインDAIを調達し法定通貨に戻す取引を実施。
Aaveでは(BUIDLなどの認証された)RWAを利用してステーブルコインを借受けるプロトコルをリリース
→RWA側はPFで認証＋SC保有はそれぞれのプロトコルで判定。



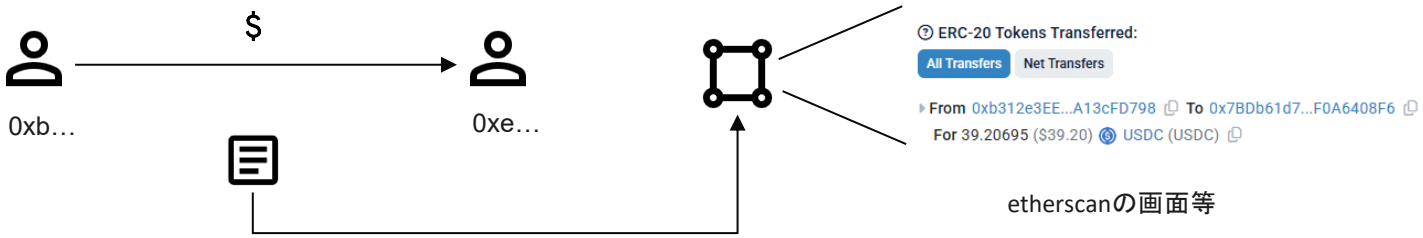
出典:[Security Tokens Refinancing] MIP6 Application for OFH Tokens - Legacy / Collateral Onboarding Applications - Sky Forum



出所:Aave's RWA Market Horizon Launches | Aave

【参考】パブリックブロックチェーンの決済とプライバシー

Ethereumなどパブリックブロックチェーンでは取引内容は公開される。
取引内容の証明として機能はするものの、全てを公開したいとは限らない。
例えばB2Bや高額決済では決済情報を関係者外に公開することは好ましくなく、
プライバシー保護と情報の透明性を担保することは大きな課題。
DAMA2においても必要最小限の情報をパブリックチェーンに記載。



etherscanの画面等

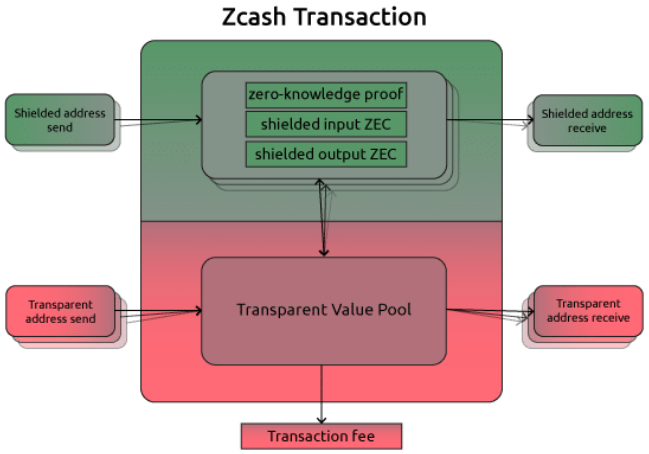
取引情報はブロックチェーンに書き込まれる

出所:core-program/week5 at main・zk-tokyo/core-program・GitHub

【参考】ZCash/TornadoCash/Privacy Pool

ZCash

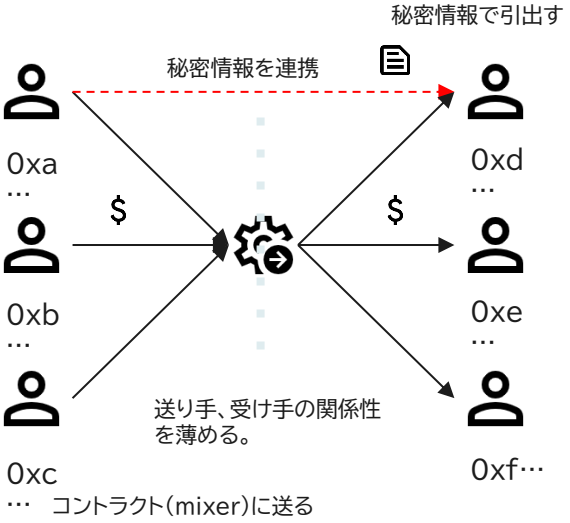
2016年にBitcoinをベースにプライバシー機能を拡張してzkSNARKSを組み込んだ新しい暗号資産として開発。



出典:Anatomy of A Zcash Transaction - Electric Coin Company

Tornado Cash

一定数の同じような送金を混ぜ合わせることで、引き出した資金が誰のものかわからなくなる。
資金の送り手はミキシングサービスに資金を預け、引出に必要となる情報を別途受け手に渡す。

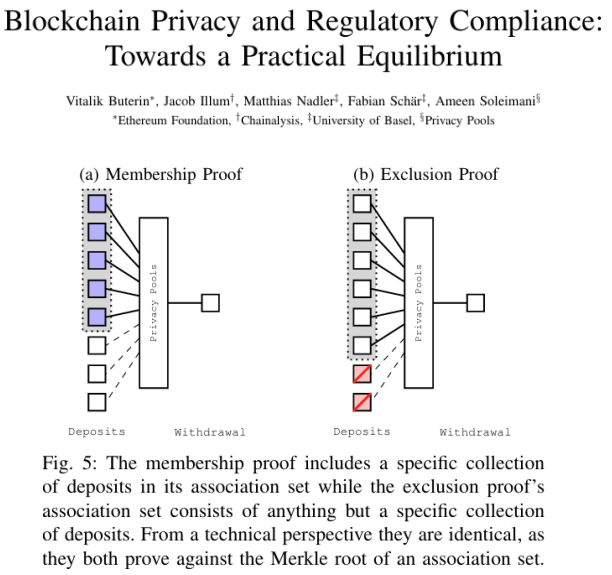


出所:core-program/week5 at main · zk-tokyo/core-program · GitHub

Privacy Pool

ミキサーを利用する点はTornado Cashらと同じ仕組みであるが、プライバシー保護とコンプライアンス遵守を実現するため引出す際に「自分は正当な参加者グループに属している」ことを証明する。

グループは、例えば既知のKYC済アドレスやホワイトリストなど、合法性を証明可能な集合として設計可能であり、AML対応などへの活用が期待される。


Blockchain Privacy and Regulatory Compliance: Towards a Practical Equilibrium

Vitalik Buterin*, Jacob Illum†, Matthias Nadler‡, Fabian Schär‡, Ameen Soleimani§
*Ethereum Foundation, †Chainalysis, ‡University of Basel, §Privacy Pools

(a) Membership Proof (b) Exclusion Proof

Deposits Withdrawal Deposits Withdrawal

Fig. 5: The membership proof includes a specific collection of deposits in its association set while the exclusion proof's association set consists of anything but a specific collection of deposits. From a technical perspective they are identical, as they both prove against the Merkle root of an association set.

出所:Vitalik. B ,et al, “Blockchain Privacy and Regulatory Compliance: Towards a Practical Equilibrium“

【参考】技術発展と比較表

時期	技術	主な特徴	解決した課題	残された課題
2016年～	ZCash	zk-SNARKで完全匿名	ブロックチェーンでの強固なプライバシー	専用チェーン・匿名性集合が小さい
2019年～	Tornado Cash	Ethereumでミキサー型匿名化	Ethereum互換性・手軽な匿名送金	マネロン・規制リスク
2023年～	Privacy Pools	証明可能な選択的匿名性	コンプライアンス対応・合法性証明	実利用（参加者グループ基準の決定）

出所：core-program/week5 at main · zk-tokyo/core-program · GitHub

Disclaimer

- 当資料は、CBDCフォーラムWG4で議論を行うための情報提供を目的として作成されたものです。
- 特定の金融商品の売買を推奨・勧誘するものではありません。
- 当資料は当社が信頼性が高いと判断した情報等に基づき作成しておりますが、その正確性・完全性を保証するものではありません。