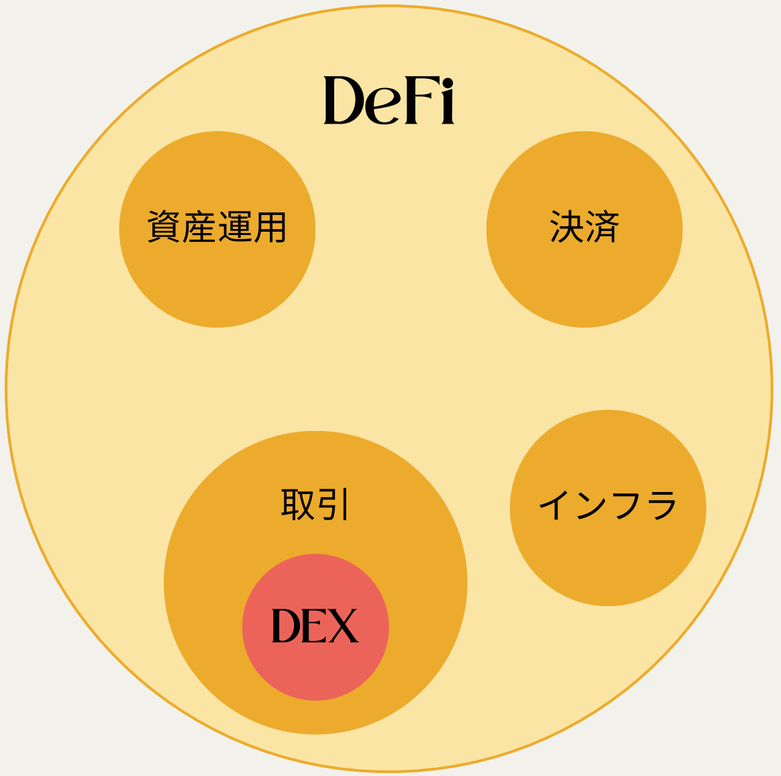
DEX

いろいろ略語

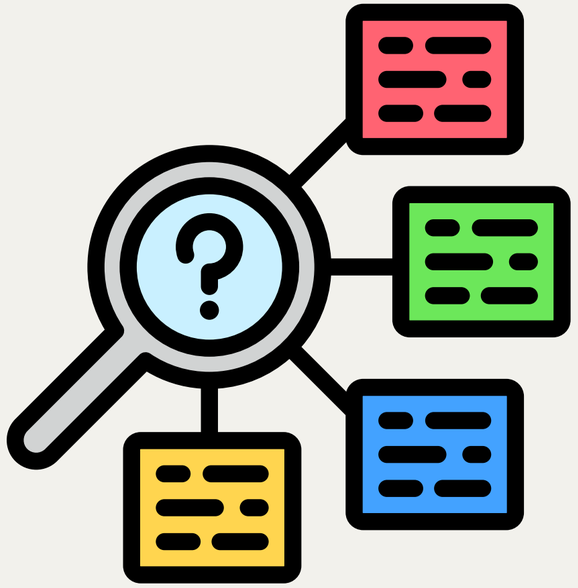
- DEX : Decentralized EXchange
  - 分散型取引所
- CEX : Centralized EXchange
  - (分散していない)取引所
- DeFi : Decentralized Finance
  - 分散金融



DeFi のカテゴリー

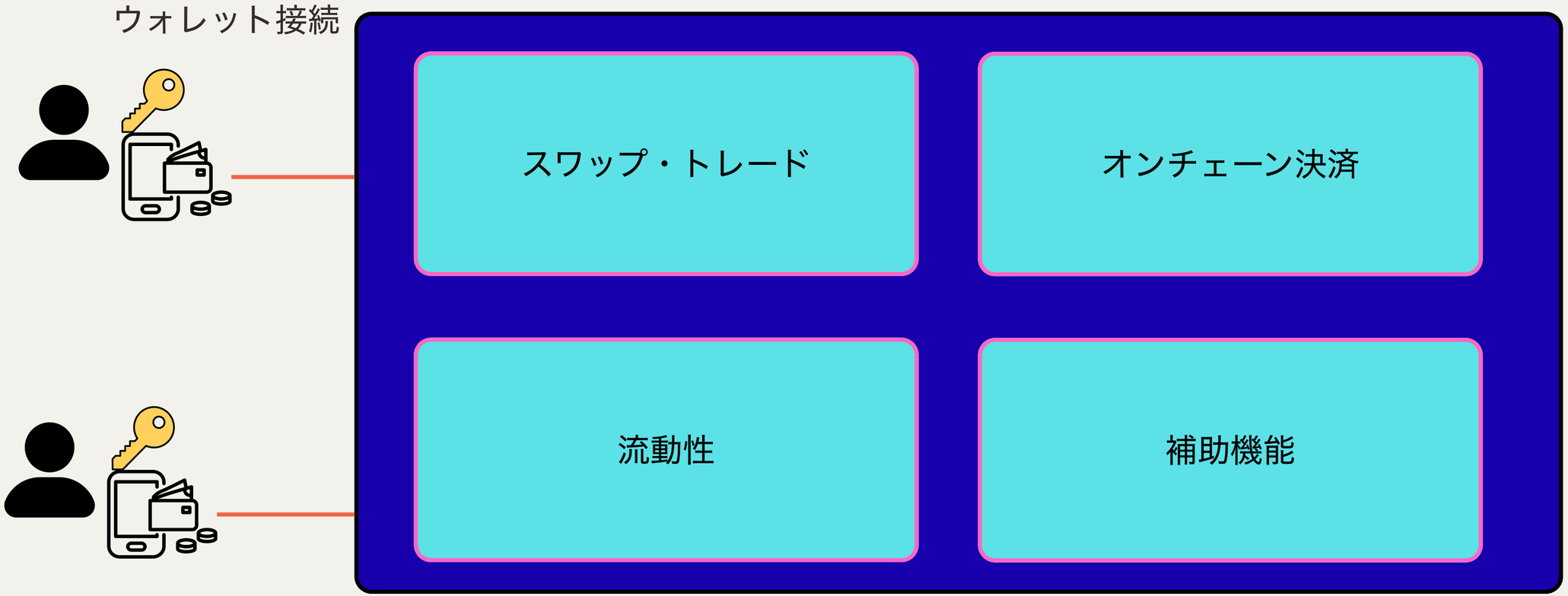
- 取引・マーケット系
  - **DEX：分散取引所**
  - アグリゲーター：複数のDEXを横断して最適なレートを提示
  - デリバティブ取引：先物・オプション・永続スワップ
  - 予測市場：イベント結果に基づくトークン取引
- 資産運用・利回り系
  - レンディング、ステーキングプールなど
- 決済・通貨系
  - ステーブルコイン、LNなど
- インフラ・保険系
  - 分散型保険など
- 新興領域
  - RWA、ゲーム、NFTなど

Layer 1 を DeFi に分類するかどうかは解釈次第らしい



DEXとは

- 分散取引所
- 共通する機能

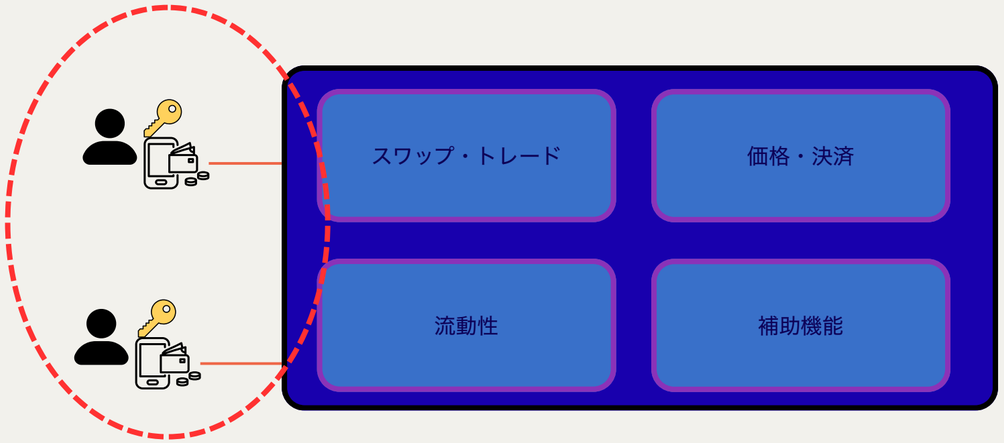


資産管理

- 取引所はユーザの資産を預からない
  - ノンカストディアル
    - 「俺たちは預からないぜ」というときは「ノン」
    - 「持ち主が自分で管理するぜ」というときは「セルフ」
  - 預かる場合は CEX という扱いになりそう
- MetaMask や WalletConnect などでユーザのウォレットを接続
  - 鍵はユーザが管理する



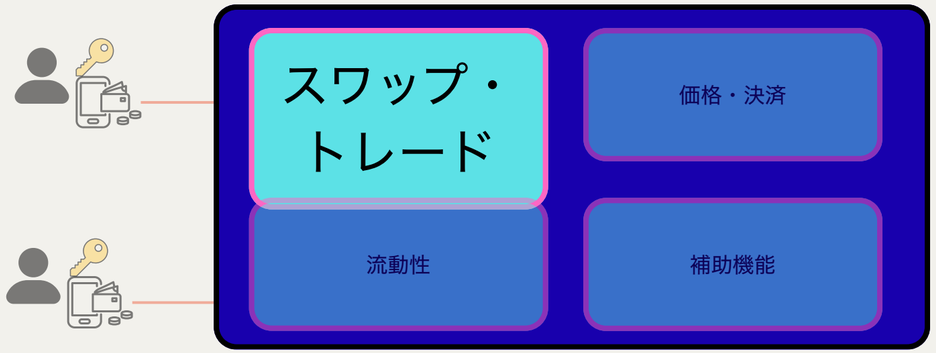




トレード機能

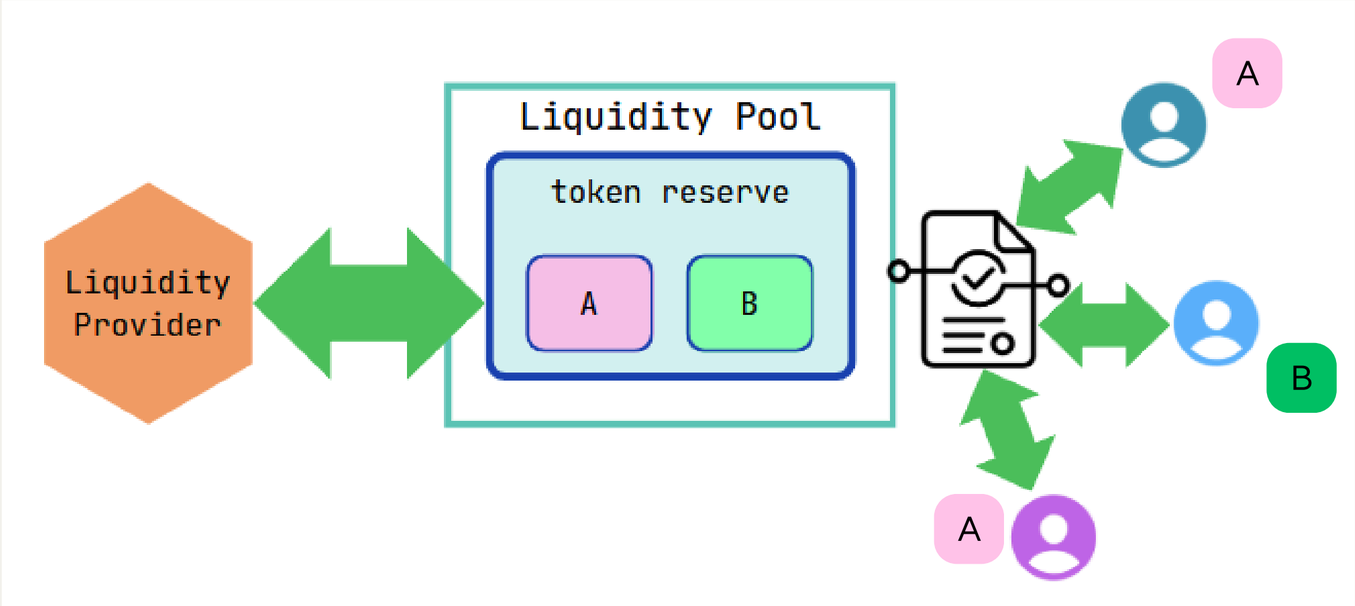
- トークンの交換
  - AMM方式
    - 後ほど
  - オーダーブック方式
    - いわゆる板取引
- 複数の流動性プールやDEXをまたいで最適レートで交換

売りの希望注文数	注文価格	買いの希望注文数
200株	102円	
500株	101円	
	100円	1,000株
	99円	300株
	98円	200株



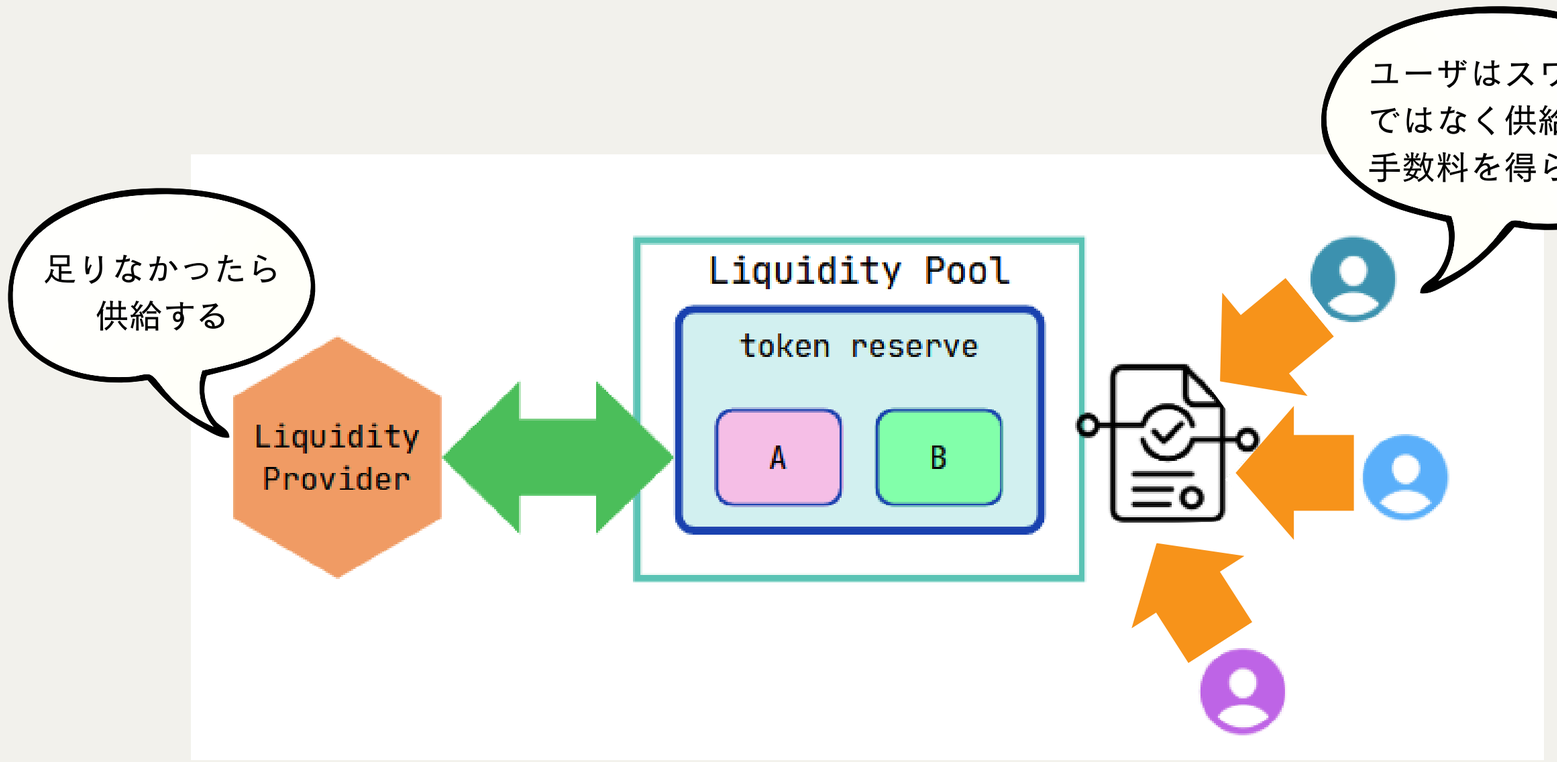
AMM 方式

- Automatic Market Maker
- Bancor が開発して広まった
- トークンAとBを交換する AMMの例
  - ユーザはスマコンを介して Liquidity Pool にアクセス
  - A=10に対してB=1という比率、というような感じ
    - 交換比率や手数料はスマコンが判定

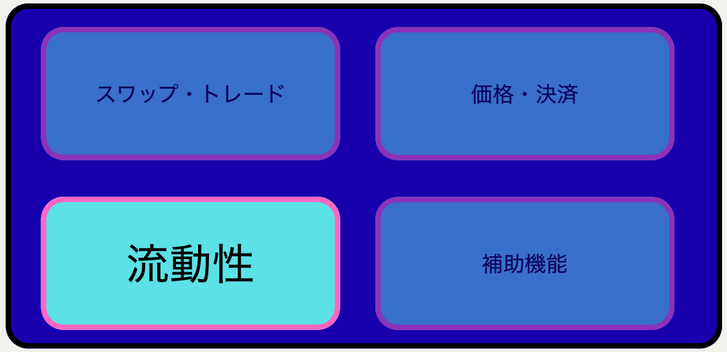


流動性提供(Liquidity Provision、LP)

- 主に AMM型 DEX
- 流動性プール
  - DEX が Liquidity Pool に供給する
  - ユーザが Liquidity Pool に供給して報酬を得る



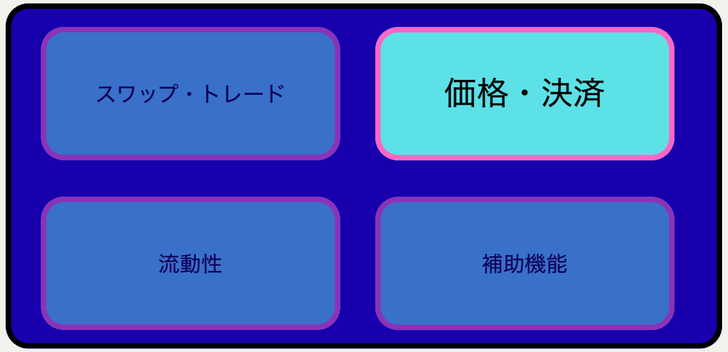
完全分散型DEXでは
こちらの方がメイン



価格発見と決済

- 「価格発見(Price Discovery)」は金融・経済用語で「市場において資産の取引を通じて妥当な価格が形成されていくプロセス」
  - AMMや板取引などで市場価格(fair market value)が決まっていくが発見される
- すべてはブロックチェーン上で完結する
  - 最終的に L1かどうかというだけで L2も対象になる
  - オフチェーンだけで完結するようなものは対象外

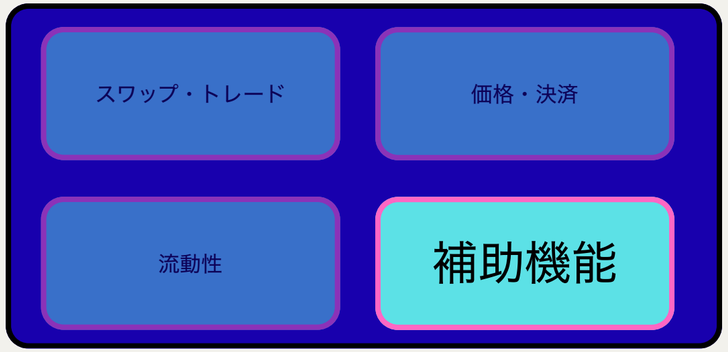




その他

- 中央の管理者を介さずコードに従って取引
- スマコンのコードや流動性は誰でも確認できる
- ガバナンストークンを使って投票
- MEV対策
- 取引の透明性
- 手数料などの計算式
- そういったもの自動化





DEXの差別化

- 取り扱うトークンの種類
- クロスチェーン対応
- NFT や RWA のような資産クラスを扱うかどうか
- ネットワーク選択
  - Ethereum メイン
  - L2 特化
  - マルチチェーン対応
- 手数料設計
  - スワップ手数料
  - LP へのインセンティブ
- その他
  - レンディング、レバレッジ
  - 準拠する規制や KYC要件

- 取引の成立しやすさ
- 手数料とレート
- ユーザビリティや追加機能

RWA - Real World Asset token

- RWA ... 現実資産を裏付けとして証券やトークンとして扱う
  - 概念としては昔からあり、不動産の REIT も RWAの 1つ
- 裏付けが現実資産という意味ではステーブルトークンもその1つと考えられる。
- 裏付け資産は、特別目的会社(SPV)の設立、トークン所有者の登記簿登録、監査法人による定期監査など
  - 通常は法制度で資産の存在を示し続ける
  - 技術的に裏付け資産を保証する方法はない



ステーブルコイン

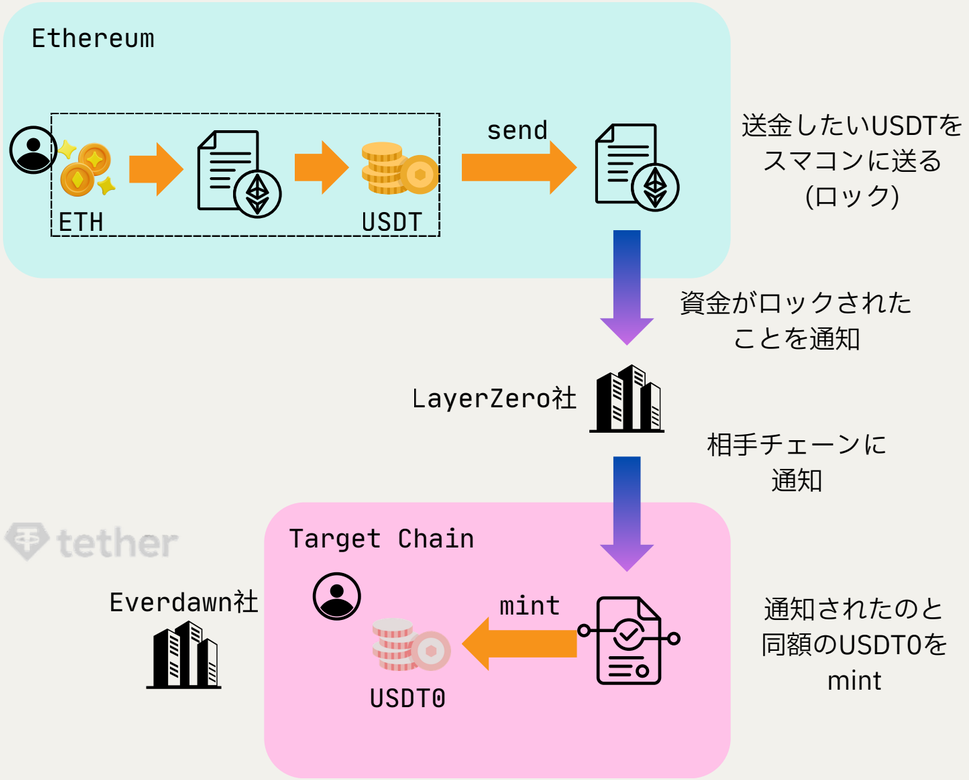
- JPYC
  - 預金や日本国債など
    - 日本国債は現金同等物ということになっている
- USDT
  - 多数のチェーンで発行
    - Tronでの送金コストが低いため新興国や取引所間送金で普及
  - 準備金透明性への疑念が多い
    - 現金・現金同等物：約60%
    - 米国短期国債：約10–20%
    - 商業手形・コマーシャルペーパー：約10–20%
    - 暗号資産やその他資産：約5–10%
- USDC
  - 投資家や機関にとって透明性が高い
    - 現金・米ドル預金：大部分（80–90%以上）
    - 米国短期国債：残り
- mUSD
  - MetaMask の USD連動型ステーブルコイン
  - 米国短期国債





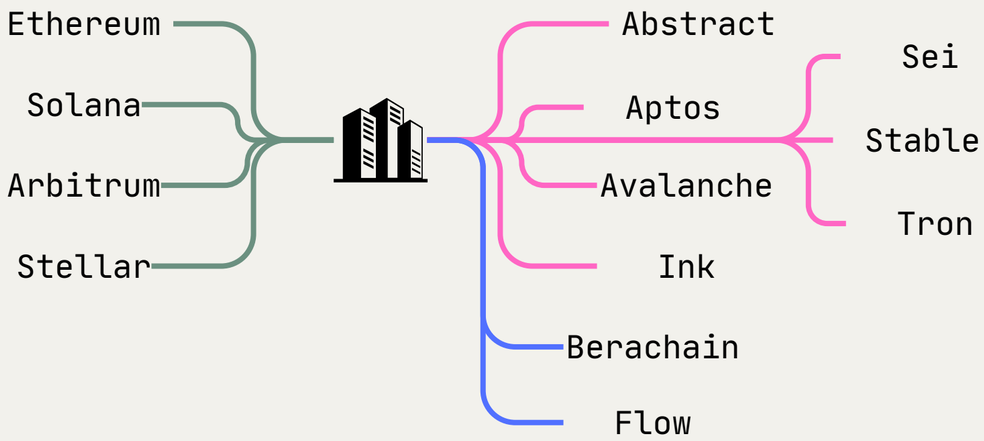
ラップコイン、ブリッジトークン

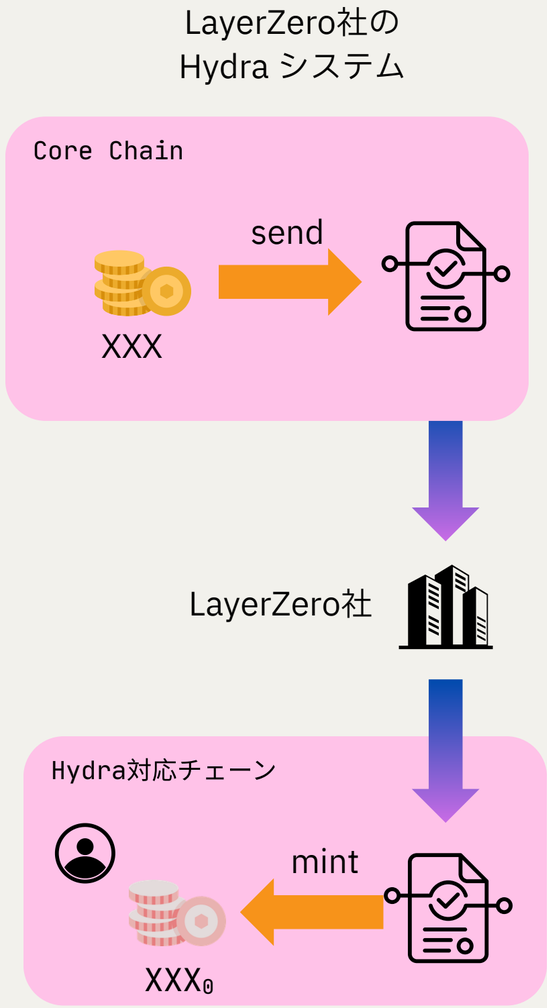
- USDT0
  - 最近 Rootstockから扱えるようになったとニュースになった
  - これはステーブルトークンではない。wrapped token と呼ばれる。
  - USDT と 1:1 で交換できるというトークン
  - チェーン間移動については LayerZero社
  - USDT0自体の管理は Everdawn社
    - Tether社の影が.....
- USDT0以外にもそういったトークンがある
  - TetherがUSDTを発行していないチェーン
  - 既存のUSDTを別のチェーンで使いたい
    - 転送せず担保として使うなど



2025/09/19 PayPal

- PayPal のステーブルコインPYUSD が LayerZero 社の OFT標準プロトコルを使って Tron 上に PYUSD0 を発行
- StargateとかHydraとか名前が何が何やら。。。
  - Stargateというのがプロトコル名で、今はV2
    - クロスチェーン流動性トランスポートプロトコル
  - Hydraはその中で使われている機構
    - 「Hydra対応チェーン」のような使い方
  - Hydraのコア技術として OFTが使われている





FATF



最近のFATF

- 2021年にグローバルスタンダードを更新
  - プロジェクトが自称する「分散型」という性質を無視し、その「機能」に焦点を当てることです 。
  - VASPとされるのは、分散型プロトコル自体ではなく、「他者または他者の代理として、以下の活動または業務の1つ以上を事業として行う自然人または法人」です 。
  - 管理権限を持つ設立チームや管理者キーを持つプロジェクトは、VASPとして分類されるリスクが高いと明記しています 。これは、DeFiプロジェクトがその自称に関わらず、責任主体が特定される可能性を強く示唆しています。

完全に分散化

- サービス提供についてユーザーが契約を締結できる相手方を特定できない場合、そのサービスは「完全に分散化されている」と分類される可能性があります(デンマーク金融監督庁の指針より)。

MiCAの要求事項	真に分散化されたプロトコルの特性
法的事業体	不変のスマートコントラクトによって運営される、中心的な事業体を持たない
中央集権的ガバナンス体制	自律的なガバナンス、コミュニティによる意思決定、主要な管理機能の最小化
ホワイトペーパーの当局による承認	特定の責任主体が存在しないため、承認の対象となる事業体がない
KYC/AML義務付け	パーミッションレスであり、ユーザーを識別する必要がない
EU域内でのオフィス設立	チームメンバーが世界中に分散して活動しており、物理的な拠点が不明確



最近のDeFi開発の傾向

- 「ガバナンスの最小化」という新しい法的戦略を採用しつつあります。
- プロトコルのコア機能に対する支配権を不変のスマートコントラクトに移譲し、中央の事業体やDAOが「支配または十分な影響力」を行使する必要性を減らすことです。
- これは、FATFやEUの機能的アプローチに直接対処するものです。人的要素を最小化することで、プロジェクトは真に「パーミッションレス」となり、VASPの規制範囲外に位置づけられることを目指します。
- しかし、米国の一部の判決は、DAOのメンバーが「ジェネラルパートナー」（無限責任組合員）として法的責任を問われる可能性を示唆しています。

じっと手を見る



プライバシー保護型コンプライアンス

- DID
  - サービス提供者は生データを見ることなく資格情報を検証
  - ユーザーの機密情報を保管しない
- ZKP
  - zkKYC
  - 基礎となる情報を一切明かさず主張が真実であることを証明
  - EUが採用を検討
- このようにフロントエンドでのやりとりが法的責任のポイントになり得る。



Hyperliquid



Hyperliquid

- ベースレイヤー: Hyperliquid
  - Hotstuff などのアルゴリズムを改良した HyperBFT
  - 仕様は未公開
  - ネイティブコインは HYPE
- 実行レイヤー
  - HyperEVM: EVM
  - HyperCore: DEX 機能

Hyperliquid は L1 の名称だが、
DEXの話をするときでもそう呼ぶのが
通例になっているようだ。

