DeFi

ChatGPT

DEX AMM型

英米法と大陸法におけるDeFi規制の展望：グローバルな機能的アプローチとKYC/AMLの統合

法律による影響は大きいが、法律体系よりも FATF の規制の方がより強そう

Decentralized Finance の略で「分散金融」を意味する。
金融サービス全般をブロックチェーン上で自律的に実装したしくみの総称。

- 完全自律型：プロトコルが完全にスマコン上に固定されて人間の関与が不要
- 半自律型：パラメータ調整や緊急停止がDAOやMultiSigによって管理される
- 中央依存型：裏でオペレーターが強く関与(クロスチェーンブリッジの一部など)
  - ZKPなど暗号学的な手法が使えるのがベストなのだが、難しいところがある
  - マルチシグ型がよくあるが、ハッキングで突破されることがあるそうだ
    - 署名鍵の流出：ホッとウォレットになっているのでインフラ侵入によって漏洩したことがある
    - 署名プロセスの脆弱性：トランザクションを確認せずに自動署名してたりして不正なメッセージを通した
    - 署名者の集中：その署名しているグループが1つで鍵をまとめて取られたことがある

カテゴリー

- 取引・マーケット系
- 資産運用・利回り系
- 決済・通貨系
- インフラ・保険系
- 新興領域

Layer 1はインフラであって金融機能を直接提供しているわけではないので当てはまらない、という解釈

取引・マーケット系

- DEX
  - 分散取引所

- Uniswap, Curve, SushiSwap など
- 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
  - どのマーケットで取引するのが最適かを探す仕組み(瞬間的最適化)
    - DEXアグリゲーター
      - 複数のDEXのプールを比較し、最適なスワップルートを自動選択
      - 1inch, Paraswap
    - レンディングアグリゲーター
      - Aave, Compoundなど複数の貸借市場を横断し、金利最適化
      - Instadapp
- デリバティブ取引
  - 先物・オプション・永続スワップ
  - dYdX, GMX, Synthetix
- 予測市場
  - イベント結果に基づくトークン取引
  - Augur, Polymarket

資産運用・利回り系

- レンディング/借入プロトコル
  - Aave, Compound, MakerDAO
- イールドアグリゲーター
  - 最適な利回り戦略に自動運用
  - ユーザーの資産を最適な運用先に自動的に移動・再投資し、利回りを最大化
  - どの運用戦略が一番儲かるかを選んで自動で回してくれる仕組み(長期的最適化)
    - Yearn
      - 複数のDeFi戦略を自動実行してリターンを最適化
    - Beefy Finance
      - クロスチェーンでのオートコンパウンド運用
- ステーキングプール / リキッドステーキング
  - Lido, Rocket Pool

決済・通貨系

- ステーブルコイン
  - DAI, USDC, USDT, FRAX
- クロスチェーンブリッジ
  - 資産をチェーン間で移動

- Multichain, Wormhole
- 決済レイヤー
  - Lightning Network的な送金用途も広義では分散金融に含まれる

インフラ・保険系

- 分散型保険
  - スマートコントラクトのリスクをカバー
  - Nexus Mutual, InsurAce
- 資産管理ツール
  - 分散型ファンドや自動化ポートフォリオ
  - Enzyme Finance
- オラクル
  - 価格や外部データをオンチェーンに供給
  - Chainlink, Band Protocol

新興領域

- RWA（Real World Assets）
  - トークン化：国債・不動産・株式をトークン化して流通
  - Ondo, Maple Finance
- ガバナンスDAOの財務運営
  - DeFiトレジャリー管理やDAOバンキング
- ゲーム・NFT金融化
  - NFT担保ローン、NFTデリバティブ、GameFi内レンディング