資料３

事務局説明資料

（DeFiのトラストポイントに関する分析）

【出典　㈱クニエによる委託調査報告書（注）に基づき、金融庁において作成】

（注）「分散型金融システムのトラストチェーンにおける技術リスク等に関する研究」（2022年6月16日公表）
https://www.fsa.go.jp/policy/bgin/information.html

2022年６月20日

分析の目的・背景

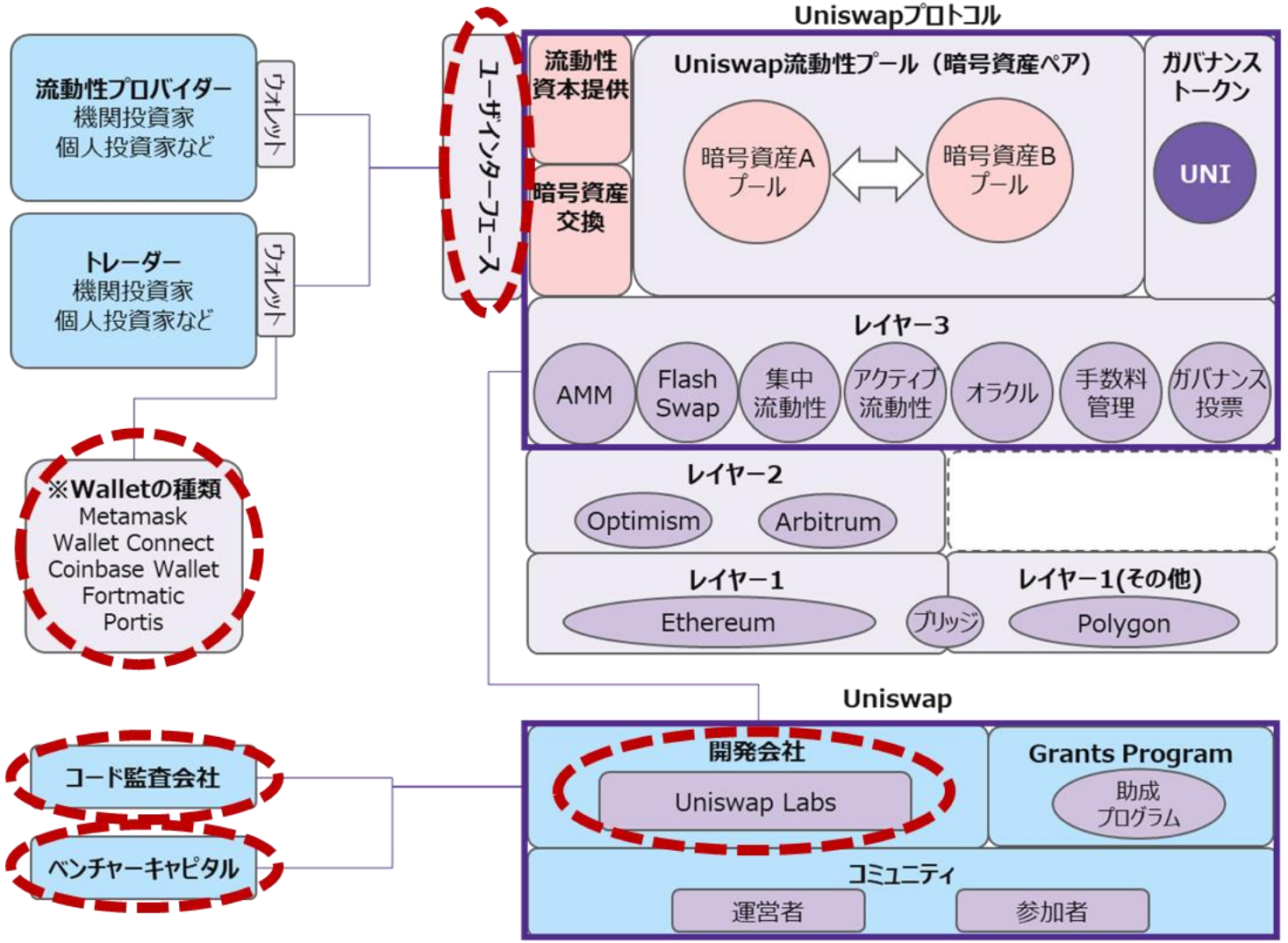
- **現在の主要なDeFiプロジェクトは一定のトラストポイント（利用者等が無条件にトラストせざるを得ない中央集権的要素）を有しているとの仮定に基づき、代表的なDeFiであるUniswap（分散型取引所：DEX）、Maker（暗号資産担保型ステーブルコイン）、Aave（レンディング）の事例分析を行ったもの**
  - ✓ DAO（Decentralized Autonomous Organization）の“Autonomous”である部分（スマートコントラクトにより自律的に運営が行われる部分）と、そうでない部分はどこか

    ※DAOの確立された定義は存在しないが、一般的には、中央集権的なリーダーシップが不在のメンバー所有のコミュニティで、コンピュータプログラムとしてエンコードされたルール（スマートコントラクト）によって運営が行われる組織のことを指す
  - ✓ ガバナンストークンを用いたオンチェーン・ガバナンスの実態把握

- **トラストポイントに関する金融規制上のインプリケーションの把握**
  - ✓ 一般的には、利用者などからトラストを受ける主体には責任が生じ、規制対象となりうる（例：銀行）
  - ✓ パラメータ変更やスマートコントラクトのアップグレード、資金使途の決定などがコミュニティに（一定程度）委ねられているDeFiでは、責任の分散化により規制対象の特定に困難が生じる可能性があり、各プロジェクトの詳細なトラストポイントの分析が必要

ケーススタディ①：Uniswap（分散型取引所）

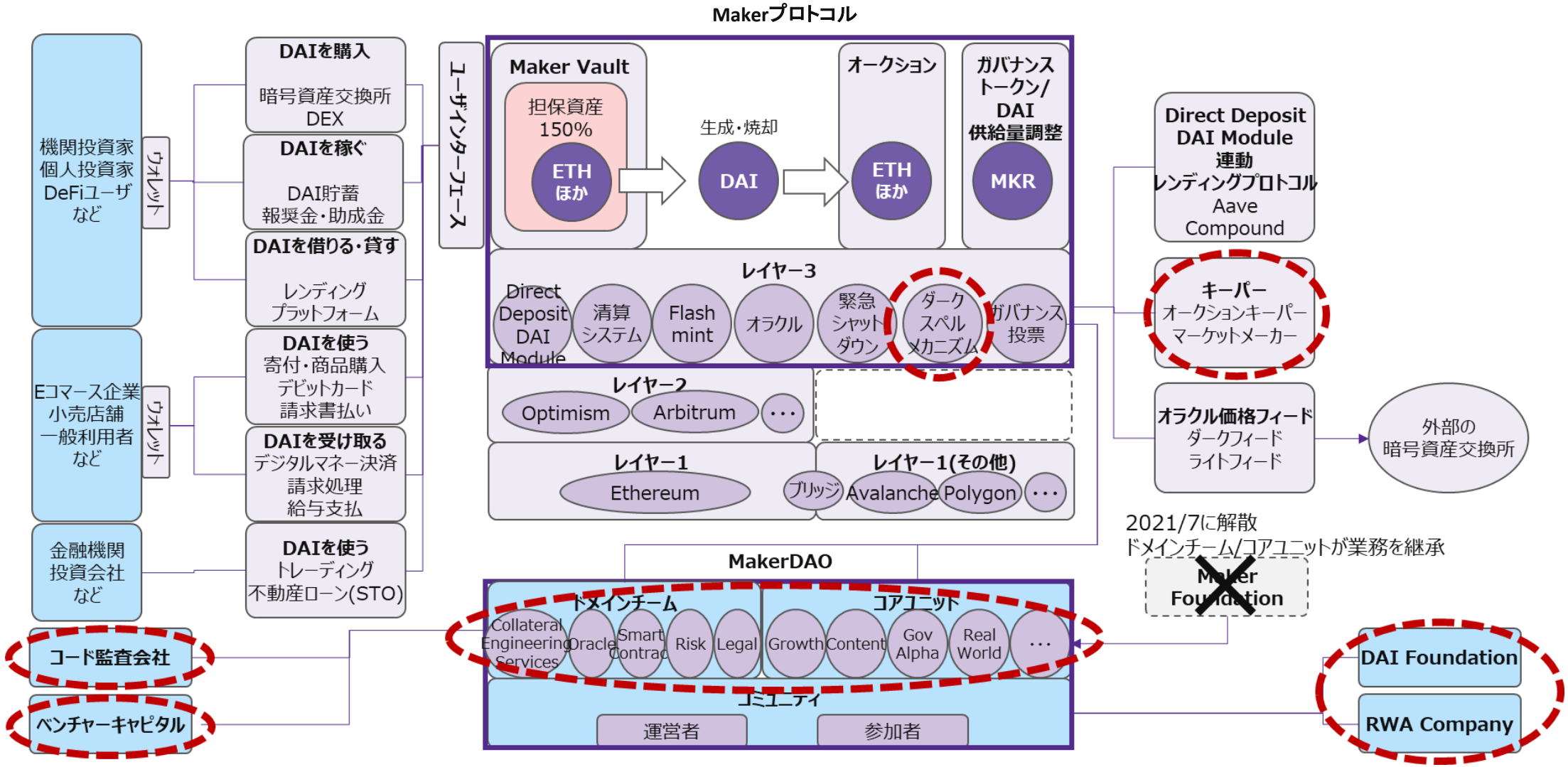
- Uniswap Labs（米国拠点の開発チーム）が暗号資産交換のためのユーザーインターフェース（ウェブサイト）を提供
- その他のトラストポイント：ウォレットプロバイダー、コード監査会社、VC（ガバナンストークンを大量保有）



トラストポイントと考えられる点

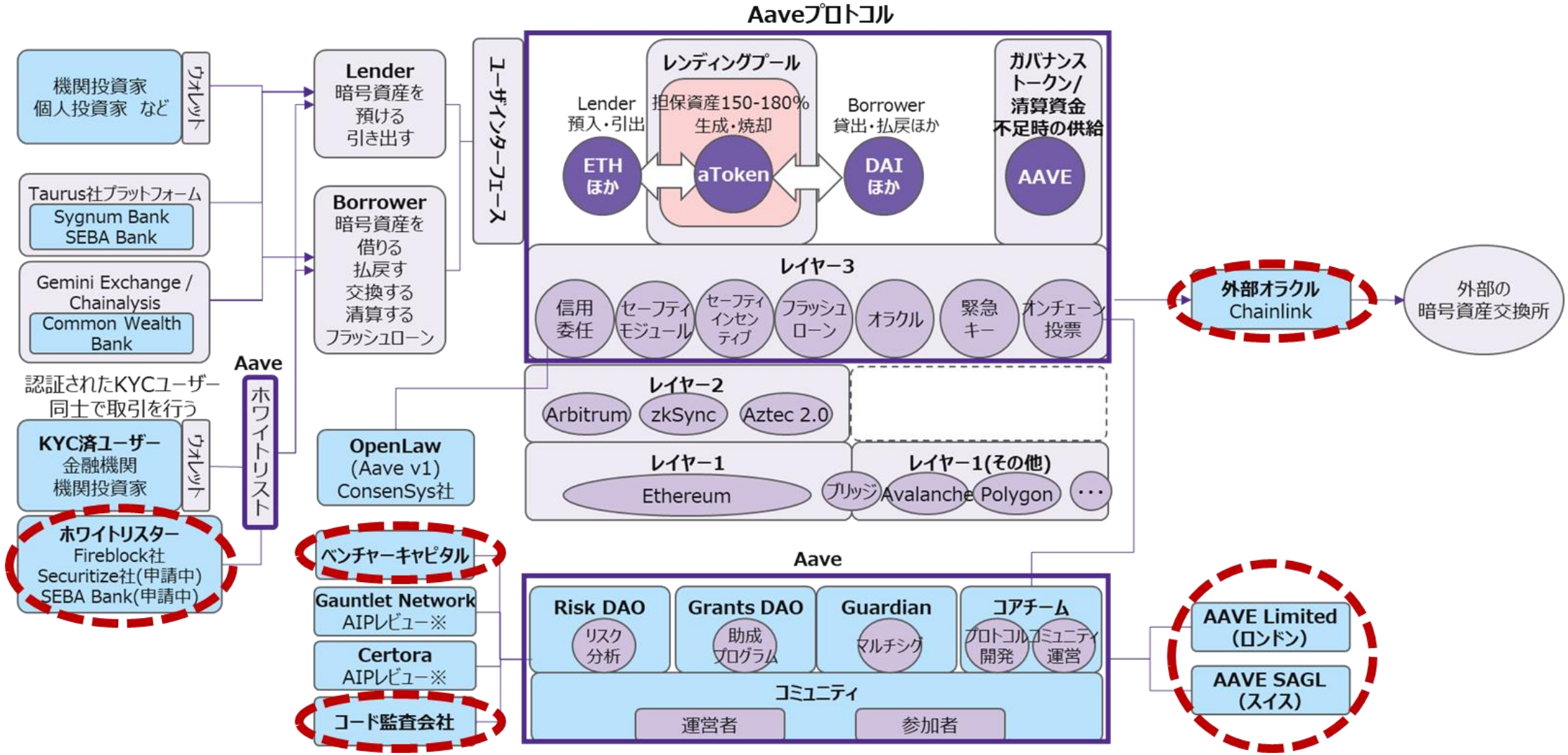
ケーススタディ②：Maker（暗号資産型ステーブルコイン発行プラットフォーム）

- かつてコミュニティ運営の中心だったMaker Foundationは昨年解散し、現在はMakerDAOが主に運営を担っている
- 引き続き一定のトラストポイントは存在するか：キーパー（裁定取引のために動く外部エージェント）、関連法人（例：DAI Foundation）、ドメインチーム（Makerプロトコルの管理等を行うために存在するコミュニティ内のチーム）など



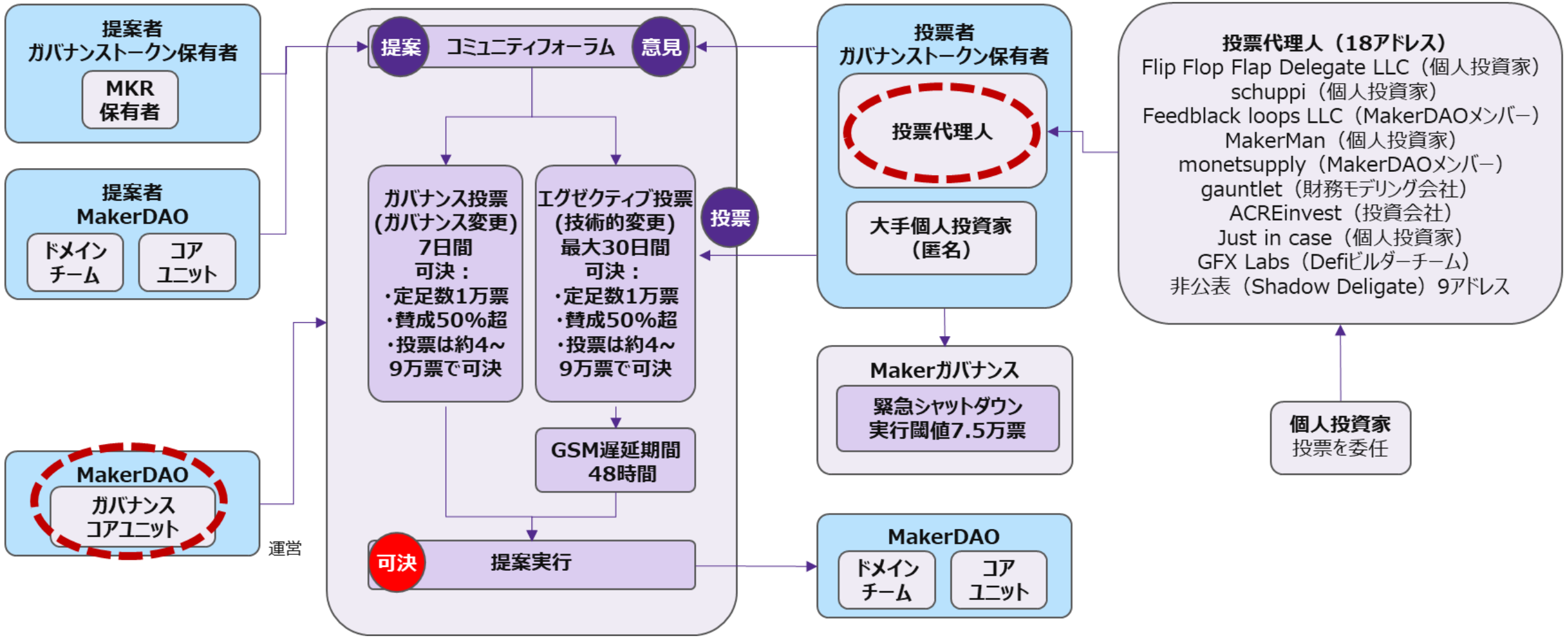
ケーススタディ③：Aave（レンディングプラットフォーム）

- ホワイトリスター（KYCプロバイダー）が関与し、機関投資家向けのレンディングサービスを提供
- Guardian：コミュニティから選ばれた10名がマルチシグを管理し、プロトコルの一時停止等の権限を有する



ガバナンス投票（例としてMakerDAO）

- 少数の投票代理人等の大口ガバナンストークン保有者が意思決定に強い影響力を有する
- MakerDAOのドメインチーム及びコアユニットがガバナンス提案・投票・提案実行の各段階で一定の関与を行っている



特定された論点・リスク事項など

- **現状のDeFiプロジェクトには様々なトラストポイントが存在**
  - ✓ 開発チーム（法人）、管理権限保有者、関連法人、ユーザーインターフェース提供者、大口ガバナンストークンホルダー、ウォレット提供者、コード監査会社、インフラ提供者、ライブラリ提供者、双方向ブリッジ管理者など
  - ✓ トラストポイントが特定できた場合でも、なお規制の執行は困難である可能性（例：アドレスベースでの特定に留まり実在の主体の特定が難しい、個人ベースの活動が多く国境の移転が容易）

- **トラストポイントがWeakest Link（DeFiのセキュリティ上最も弱い部分）となりうる**
  - ✓ 多くのインシデントがトラストポイントにおいて発生（例：バリデータの秘密鍵の窃取、コード監査で発見されなかった脆弱性を突いた攻撃、インフラ提供者の不具合に伴う障害）
  - ✓ 他方、脆弱性が発覚した際に管理者権限で緊急対応を行うことが可能であるなど、トラストポイントが存在する利点も

- **“DAO”や“ガバナンストークン”と呼称されていても、プロジェクトによって大きな違いが存在**
  - ✓ Uniswapのガバナンストークン（UNI）で出来ることは限定的（例：コアコントラクトのアップデートは不可）だが、Makerのガバナンストークン（MKR）では比較的大きな権限を行使可能。ガバナンストークンに投票権以外の機能が付与されている場合も存在。
  - ✓ 少数の大口投資家や投票代理人が意思決定に強い影響力を持つと考えられるプロジェクトも存在。

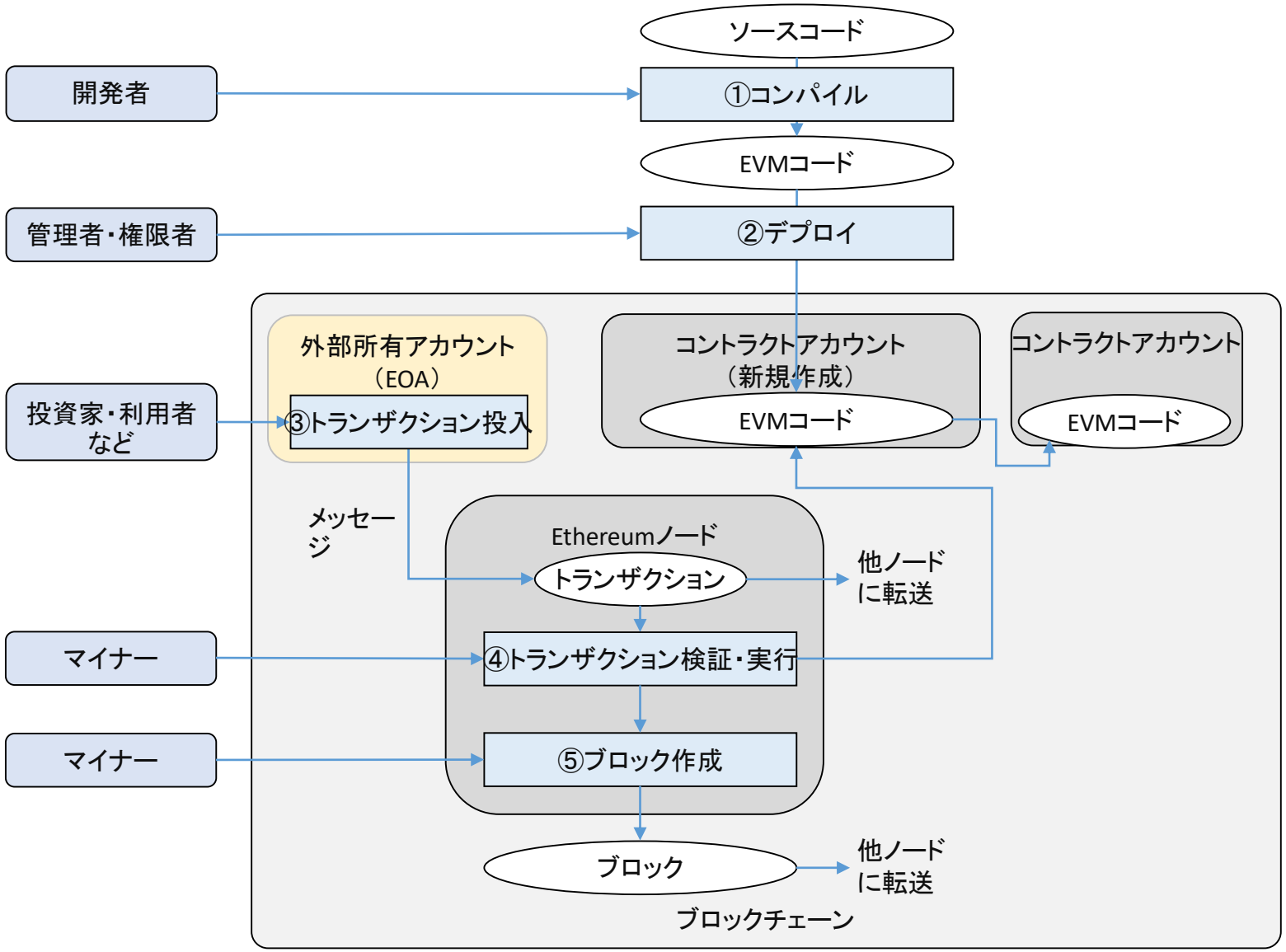
- **イノベーション促進・技術革新支援の視点**
  - ✓ プロジェクトの初期段階では責任主体の特定が容易である可能性が高いが（例：解散前のMaker Foundation）、分散化の阻止はプロジェクトの成長（≒イノベーション）を阻害することにも繋がりうる
  - ✓ 技術中立性に関する論点：トークン交換などの金融機能は特定のエンティティではなくプログラム（スマートコントラクト）が提供しており、“技術”と“ビジネス”の境界が曖昧化している可能性

補足資料

分散型金融システムの主要な構成要素

#	構成要素	概要
(1)	**基盤ブロックチェーン**	**メインチェーン（例：Ethereum）** • DeFiプロトコルを実行するためのベースとなるブロックチェーンであり、サイドチェーンやレイヤー2スケーリングソリューションの親チェーンとなる • DeFiプロトコルをデプロイするためには、柔軟なスマートコントラクト機能を備えたブロックチェーンが必要とされる。Ethereumの場合、ブロックチェーンに保持される2種類のアカウントが存在 ➢ **外部所有アカウント**：秘密鍵で管理され、ネイティブトークン（ETH等）やトークン（ERC20トークン等）の送受信およびスマートコントラクトのデプロイ・実行ができる ➢ **コントラクトアカウント**：デプロイされたスマートコントラクトのアカウントであり、ユーザアカウントや他のコントラクトアカウントからのメッセージの受信に応答してスマートコントラクトが実行される • メインチェーンを構成するクライアント（Ethereumノード）は、Ethereum Foundation等から提供されている共通ソフトウェアであるEthereumノードソフトウェア、およびスマートコントラクトを実行するために必要な仮想マシン（EVM）を搭載している。
		サイドチェーン（例：Polygon） • メインチェーンの処理速度向上等のスケールアップを行うため、メインチェーンと並列で動作する構造のブロックチェーン。 • メインチェーンと独立したコンセンサスアルゴリズム（DPoS：委任されたプルーフオブステーク　等）を用いることで、電力消費を抑えてCO2排出量を削減し、取引処理速度の向上やガス代を削減することを目指すものが多い • 双方向ブリッジでメインチェーンに接続されることが一般的で、チェーン間で資金をやりとりする場合、双方向ブリッジに資金をロックして二重支払いを防ぐ
(2)	**レイヤー2スケーリング ソリューション**	• Ethereumブロックチェーンの処理速度向上等のスケールアップを行うソリューションを指し、例えばEthereumでは以下が存在 **Optimistic Rollup:** Rollupは、Ethereumメインチェーン(レイヤー1）の外部のオフチェーン（レイヤー2）でトランザクションを実行し、結果データのみをレイヤー1に送信することで処理速度を向上する仕組み。Optimistic Rollupは、トランザクションがデフォルトで有効であると想定し、書き込まれるデータの有効性の検証に必要な計算を行わないため、処理速度を向上させることができるとされる。
(3)	**ネイティブトークン（ETH等）**	• 基盤ブロックチェーン内で共通して利用されるトークン（暗号資産）であり、トランザクションの実行手数料（ガス代）等として必要
(4)	**スマートコントラクト**	• 一般に、**プログラムとして記述され、ブロックチェーン上で自動的に実行処理されるルール（契約）**を指す。 • Ethereum等では、スマートコントラクトはブロックチェーンに書き込まれ、トランザクションの検証の過程でマイナーもしくはバリデータにより実行される。その実行ログと実行後の証憑がブロックに記録されることで、誰もが真正なプログラムコードが実行されたことを確認でき、また状態を共有できる。 • スマートコントラクトは通常は修正や削除ができず、実行結果は元に戻せないが、開発ツールによるサポート等を通して間接参照を用いれば、参照先を新たなコントラクトアドレスで置き換えることで**スマートコントラクトをアップグレード可能にできる余地も存在**する。 • スマートコントラクトはブロックチェーンにデプロイすることで実行可能になるが、DeFi におけるデプロイ作業は一般に管理者や権限者（スマートコントラクトのデプロイに必要な秘密鍵を保持している者）が保有する外部所有アカウントの秘密鍵が必要になる。 • 本資料では、**DeFiの機能・サービスを実現するスマートコントラクトを「DeFiプロトコル」と呼称**する。

（参考）スマートコントラクトの実行の流れ（Ethereum）



① 開発者がソースコードを開発・コンパイルしてEVMコードを生成し、テストを行う。

② 管理者・権限者がEVMコードをデプロイし、コントラクトアカウントが新規作成される。

③ 投資家・利用者などが外部所有アカウントから投入したトランザクションが、メッセージとしてEthereumノードに送信される。ノードに送信されたメッセージは、他のノードに転送される。

④ マイナーがトランザクションの検証・実行を行う。この際、コントラクトアカウントに紐づいたEVMコードが実行される※（他のコントラクトアカウントへのメッセージを含む）。

⑤ マイナーがトランザクションの実行結果（実行ログ、実行後の状態）をブロックに記録する。

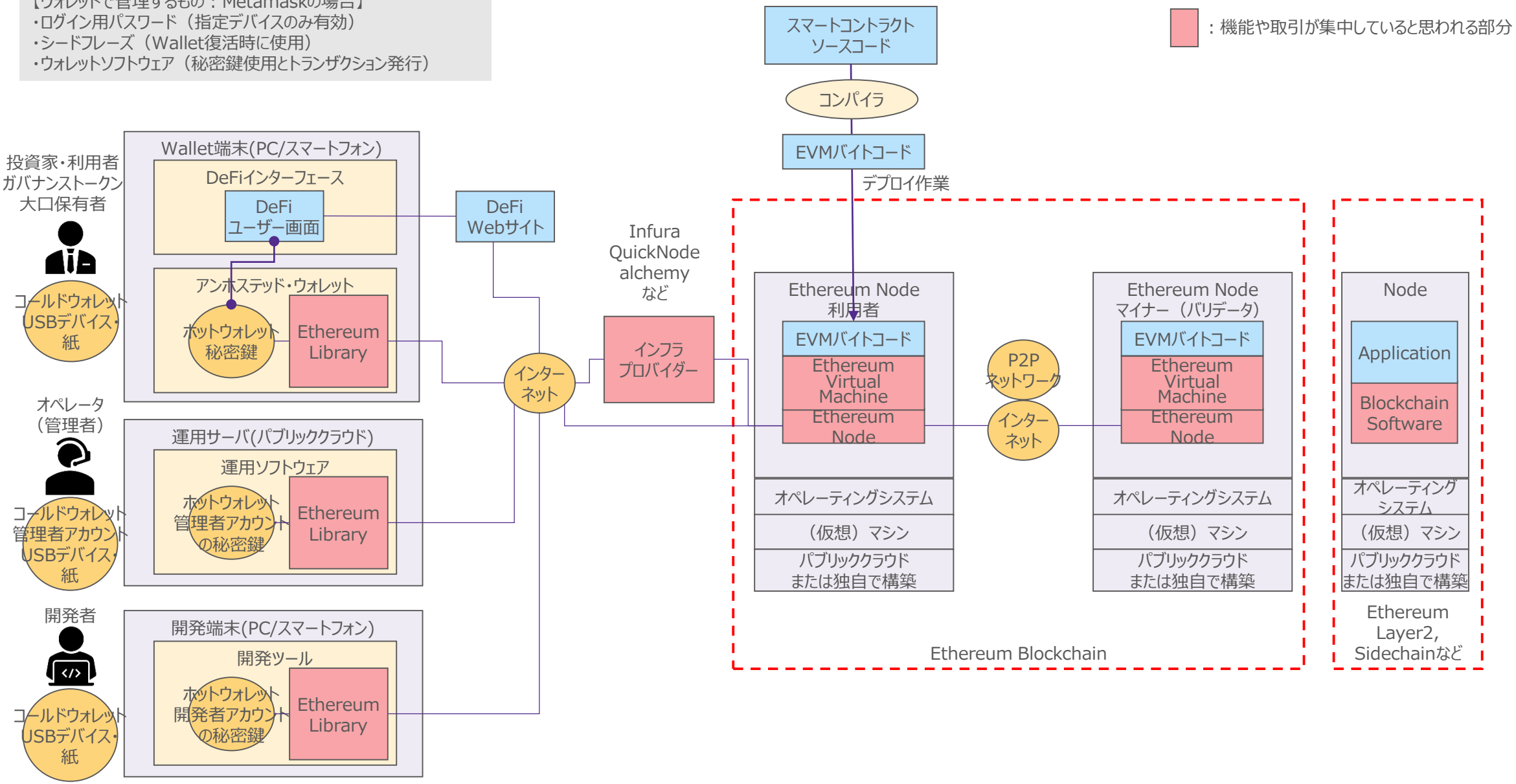
※ EVM コードにメッセージに対応する処理が記述されていればそれを実行し、無ければデフォルトとして記述されている処理(Fallback 関数) を実行する。

分散型金融システムの主要な構成要素

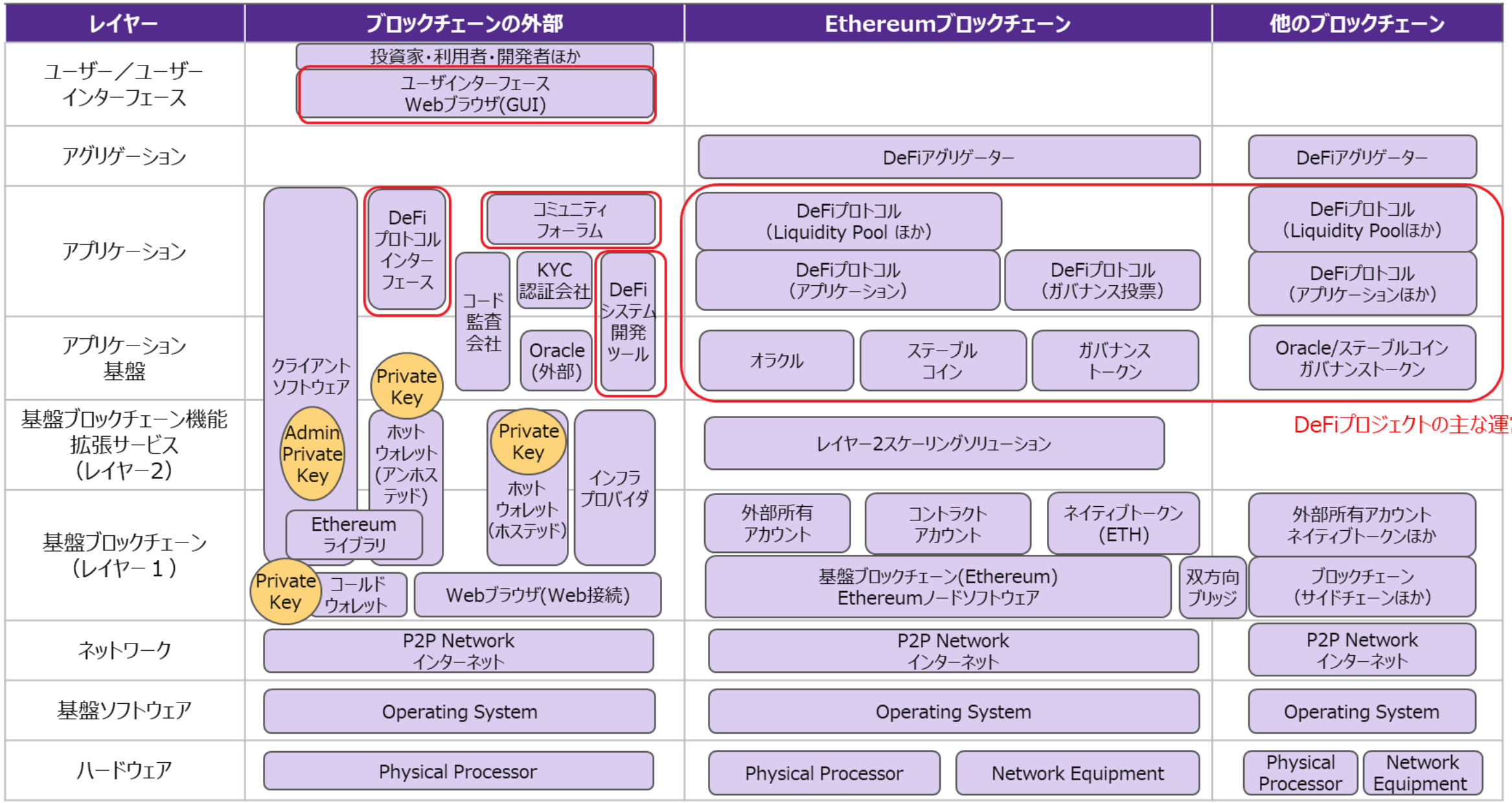
#	構成要素	概要
(5)	**ウォレット**	• ユーザの秘密鍵を管理し、ユーザが秘密鍵を使ってトランザクションを実行するためのウォレットアドレスなどの情報の保持と、ユーザインターフェース（Webブラウザやスマートフォンアプリの操作画面など）の提供を行う。DeFiの機能・サービスを利用する場合はDeFiに自身のホット・ウォレットを接続する。
(6)	**ユーザインターフェース**	• DeFiの文脈においては、DeFiサービスを利用する際のWebブラウザやスマートフォンアプリのユーザ認証画面やユーザ操作画面（GUI：Graphical User Interface）、運用オペレータが使用するコマンド（CLI：Command Line Interface）などを指す。
(7)	**インフラプロバイダ**	• ブロックチェーンノードのホスティングサービスで、DeFi開発者やウォレットプロバイダなどがDeFiの機能・サービスを構築するにあたり、基盤ブロックチェーンへのアクセスなど基盤となる部分の機能をAPIなどで提供する主体である。代表的なものとしてInfura（Consensys社が提供）やQuicknode（QuickNode社が提供）、alchemy（alchemy社が提供）など。
(8)	**DeFiシステム開発ツール**	• DeFiシステムの開発者がDeFiプロトコルのスマートコントラクトなどを開発/テストするための開発ツールであり、EthereumではTruffleやHardhatなどがある。 • 開発ツールの機能として、スマートコントラクトの開発／デバッグ、ソースコードのコンパイル、ローカルノードでのテスト、開発用ブロックチェーンへのデプロイなど。
(9)	**コード監査会社**	• スマートコントラクトのコードについて、コード監査ツールによる静的検証（コード分析・形式検証など）、動的検証やコード監査者による机上検証などにより、設計上の問題、コードのエラー、セキュリティ上の脆弱性を検出するための分析サービスを提供する会社。
(10)	**クライアントソフトウェア**	• DeFiの開発者や運営者が、スマートコントラクトのデプロイやメンテナンス、DeFiプロトコルの稼働監視などのオペレーションを行う場合に外部からEthereumノードにアクセスするためのソフトウェアであり、ターミナルエミュレータやWebブラウザ（インフラプロバイダを経由して利用する場合）などがある。
(11)	**オラクル**	• スマートコントラクトがオフチェーンの外部データを取得するためのデータフィードであり、主に価格オラクルとして外部の市場価格や利率を取得するために使用されている。
(12)	**ガバナンストークン・ガバナンス投票**	• 一般に、コミュニティの意思決定に係る投票権（議決権）が付与されたトークンのことを指す。 • DeFiプロトコルの機能修正・追加や利率などのパラメータ変更、コミュニティ資金の使用などについて、ガバナンストークン保有者が保有量に応じて決められたルールに従って投票を行い、可決した提案が実行される。
(13)	**KYC認証会社（ホワイトリスター）**	• DeFiプロジェクトに代わり機関投資家などのKYC等を行う会社（一例として、KYC認証会社が認証した機関投資家をホワイトリストに登録してDeFiに通知し、DeFiでKYC済ユーザとして認識するなど）
(14)	**アグリゲーター**	• ブロックチェーン上に存在する様々なDeFiサービスを1つの場所（ウェブサイト等）に集約し、ユーザへ効率的な暗号資産取引の機会を提供する機能・サービスのことを指す。 • Instadappや1inch等のDeFiアグリゲーターは、分散型取引所、レンディングプロトコル、流動性プールなどから最適なトークン交換条件や利回りを見出し、プラットフォーム上で提供する。

（参考）ウォレット・ノード等に関するトラストチェーン（Ethereum）

【ウォレットで管理するもの：Metamaskの場合】
・ログイン用パスワード（指定デバイスのみ有効）
・シードフレーズ（Wallet復活時に使用）
・ウォレットソフトウェア（秘密鍵使用とトランザクション発行）



分散型金融システムを構成する主要な構成要素のマッピング



調査対象プロジェクト（Uniswap・Maker・AAVE）の比較

項目	内容	Uniswap	Maker	Aave
概要	提供サービス	分散型取引所（DEX）	ステーブルコイン（DAI）発行	暗号資産担保レンディング
	サービス開始時期	2018/11	2014/12	2017/5
	TVL （2022/2/13時点）	82.9億ドル	169.5億ドル	107.4億ドル
	手数料総額 （2021年）	16.5億ドル 流動性プール手数料による収入 （内訳）UniswapV2　8.27億ドル UniswapV3　8.17億ドル　ほか	0.69億ドル 安定化手数料、清算ペナルティなどによる収入	3.10億ドル 貸出手数料による収入 （内訳）Aavev2　2.56億ドル Aavev1　0.27億ドル　ほか
	ガバナンストークン	UNI（保有アドレス：27.6万）	MKR（保有アドレス：8.3万）	AAVE（保有アドレス：10.6万）
コミュニティ・ 関連組織	コミュニティ	Uniswapコミュニティ（DAO）	MakerDAO	AAVEコミュニティ（DAO）
	創立者	Hayden Adams	Rune Christensen	Stani Kulechov
	コミュニティ運営	• ガバナンストークン保有者を中心とした運営 • 関連組織やDAO内チームによるコミュニティ運営への一定の関与あり		
	主な関連組織	• Uniswap Labs（米）：プロトコル開発・管理やコミュニティ運営への関与など	• DAI Foundation（デンマーク）：知財管理等 • RWA Company LLC（ケイマン諸島）:実世界の資産への投資管理、クライアントとの契約締結等	• Aave Limited（英）：FCAから電子マネー業者ライセンスを取得済
	解散済組織	-	• Maker Foundation（デンマーク） ➢ 2021/7の解散に伴いMaker Foundationの資産はMakerDAOに移管され、業務はMakerDAO内のドメインチーム／コアユニットが継承	-

調査対象プロジェクト（Uniswap・Maker・AAVE）の比較

項目	内容	Uniswap	Maker	Aave
技術特性	主な技術特性	• AMM（自動マーケットメーカー） • Flash Swap • 流動性集約機能 • 手数料の拡張	• Maker Vault（DAI生成） • 清算システム2.0 • Dai Direct Deposit Module（D3M） • キーパー（マーケットメーカー・オークション） • Flash Mint	• Aave interest bearing tokens (aToken) • Flash Loan • 信用委任 • Aave Arc／ホワイトリスター • 担保スワップ・担保返済
	オラクル機能	自己プロジェクト内で算出 • 暗号資産ペアの価格累積合計取得してTWAP（時間加重平均価格）を計算 • 全ての暗号資産ペアについて、取引が行われる前に市場価格を測定	自己プロジェクト内で仕組みを構築 • 複数の外部市場の価格を「オラクル価格フィード」が取得 • 全体の中央値を算出し、1時間後に内部価格に反映	外部サービスに依存 • 分散型オラクルサービスのChainlinkを利用して市場価格および貸付レートを取得し、内部に反映
	アップグレード可否	• コアコントラクトは設計上アップグレード不可（AMM、流動性集約機能、オラクル機能など） • 一部パラメータ（手数料）は変更可能 • コア以外のコントラクト（周辺機能、インターフェース、ガバナンス投票など）は変更可能	• スマートコントラクトはアップグレード可能 • スマートコントラクトに事前にアップグレードが可能になる機能を組み込んでおくことで対応している	
	対応ブロックチェーン（Scalability） ※プロトコルのデプロイ先及びトークンが利用可能なチェーン	• Ethereum • Ethereum 2nd Layer ソリューション（Optimism、Arbitrum） • サイドチェーン（Polygon）	• Ethereum • Ethereum 2nd Layer ソリューション（Optimism、Arbitrum、Loopring、zkSync、Aztec2.0） • サイドチェーン（Avalanche、Polygon、BSC、Fantom、Klaytn、xDAI、Harmony など）	• Ethereum • Ethereum 2nd Layer ソリューション（Arbitrum、zkSync、Aztec2.0） • サイドチェーン（Avalanche、Polygon、BSC、Fantom、xDAI、Heco、Sora）
緊急時対応	悪意のあるガバナンス提案のキャンセル	詳細不明 • スマートコントラクト上は管理者による提案キャンセルが可能になっているが、提案キャンセル機能および実行できる管理者は定義されていない（緊急時は開発会社やコアユニットが実施することを想定か）		ガバナンス提案をキャンセル可能 • 悪意のある提案が行われた場合の対策として、ガバナンス投票の待機時間内に、選ばれた権限者（Guardian）がマルチシグ承認により提案をキャンセルすることができる
	緊急のスマートコントラクト修正	• コアコントラクトがアップグレード不可のため、原則対応不可	• ダークスペルメカニズムによる緊急修正が可能	• 対応可否不明（ドキュメントで未定義）
	攻撃を受けた時の対応		• 緊急シャットダウンによるプロトコル停止が可能	• 緊急キーによるプロトコルの一時停止が可能

調査対象プロジェクト（Uniswap・Maker・AAVE）の比較

項目	内容	Uniswap	Maker	Aave
意思決定（ガバナンス投票）	ガバナンストークン配布数	UNI：10億トークンを順次配布中 （2020/9より4年間で配布中）	MKR：98.5万トークンを配布済 （2022/1時点）	AAVE：1,600万トークンを配布済 （2022/1時点）
	ガバナンストークンの初期配布 (1)無償配布	以下の割合で初期配布中 • コミュニティメンバー　60% • チームメンバー、従業員　21.266% • 投資家　18.044% • アドバイザー　0.69%	• アーリーアダプターに配布	• 旧LENDトークン保有者　1,300万トークン 内訳：Founder&Project　23% 投資家　77% • リザーブ資金：300万トークン
	ガバナンストークンの初期配布 (2)有償配付	なし	• ベンチャーキャピタルにICOで販売 （Andreessen Horowitz, Polychain Capital ほか）	なし
	ガバナンストークンの主な役割	① オンチェーン投票	① オンチェーン投票 ② ステーブルコインDAIの再資本化（DAIの追加・削除）に使用	① オンチェーン投票 ② 清算資金不足時の予備資金（セーフティモジュール）として使用
	ガバナンス投票で提案できる主な事項 (1)アプリケーション	① スマートコントラクトの変更 ・コア以外のアプリケーション処理（周辺機能、インターフェース、ガバナンス投票など） ・パラメータ値（手数料など）の変更 ・流動性プールの追加変更削除	① スマートコントラクトの変更 ・アプリケーション処理（D3M、Vaults、清算システム、オラクルなど） ・パラメータ値の変更 新しい担保資産タイプの追加変更 既存のリスクパラメータの追加変更 DAI貯蓄率の変更 ・システムのアップグレードの決定 ② オラクル価格フィードの選択	① スマートコントラクトの変更 ・アプリケーション処理（Lending、SM/SI、Flash Loan、信用委任など） ・パラメータ値（手数料など）の変更 ・システムのアップグレードの決定
	ガバナンス投票で提案できる主な事項 (2)ガバナンス	① コミュニティ運営の変更（コミュニティ資金の配布、ガバナンス投票の変更など） ② コアコントラクト商用ライセンスの期間変更、免除	① コミュニティ運営の変更（コミュニティ資金の配布、ガバナンス投票の変更など） ② 緊急シャットダウンの実行（常時投票可）	① コミュニティ運営の変更（コミュニティ資金の配布、ガバナンス投票の変更など） ② Guardianの推薦
	ガバナンス投票で提案できない事項	①コアコントラクトの変更 ・システムのアップグレード（開発会社が実行）	－（特に制約なし）	－（特に制約なし）

調査対象プロジェクト（Uniswap・Maker・AAVE）の比較

項目	内容	Uniswap	Maker	Aave
意思決定（ガバナンス投票）	ガバナンス投票の流れ	・スナップショット投票とガバナンス投票の2段階投票 ①スナップショット投票 投票2日間、定足数0.05%、50%以上賛成 ②ガバナンス投票 投票5日間、定足数4%、50%以上の賛成	・提案内容によりガバナンス投票とエグゼクティブ投票のどちらかを選択 A.ガバナンス投票 （金額・利率や人選などスマートコントラクトの変更以外の方針等を決定） 投票7日間、定足数1%、50%以上の賛成 B.エグゼクティブ投票 （スマートコントラクトの変更部分のみを決定） 投票30日間、定足数1%、50%以上の賛成	・スナップショット投票とガバナンス投票の2段階投票 ①スナップショット投票 投票3日間、定足数50票、50%以上賛成 ②ガバナンス投票 ・ショートタイムロック（ガバナンスに関連しない） 投票3日間、定足数2%、50.5%以上の賛成 ・ロングタイムロック（ガバナンスに影響する提案） 投票10日間、定足数20%、57.5%以上の賛成
		・提案可決後の待機期間　2日間 ・待機期間中に管理者が提案をキャンセルできる ・待機期間終了後、管理者によりデプロイされる	・提案可決後の待機期間　2日間（Bのみ） ・待機期間中に権限者が提案をキャンセルできる ・待機期間終了後、誰でもデプロイできる	・提案可決後の待機期間　①1日間、②7日間 ・待機期間中に選ばれた権限者（Guardian）が提案をキャンセルできる ・待機期間終了後、管理者によりデプロイされる
	ガバナンス投票率（2021年実績）	約5-9%	約4-9%	約2-3%
	ガバナンス提案可決率（2021年実績）	スナップショット投票　77%（27/35件） ガバナンス投票　86%（6/7件）	ガバナンス投票　90%（275/307件） エグゼクティブ投票　100%（47/47件）	ショートタイムロック　88%（45/51件） ロングタイムロック　50%（1/2件）
	主な投票者	・大手トークン保有者　主に10団体 - 4大学（Berkelay, Stanford, Harvard, UCLA） - フィンテック（Gauntlet、Dharma、Kiva） - VC（Andreessen Horowitz, Monet Supply, Index Corp） →　個人投資家が投票権を委任可能 ・他の投票者　主に3名 DeFiプロジェクト関係者 （Ethrerum Foundation, Varient, Compoundなど）	・投票代理人　18アドレス （公開代理人9アドレス、非公開代理人9アドレス） →　個人投資家が投票権を委任可能 ・大手個人投資家（匿名）	・大手トークン保有者　4アドレス Aave、Binance、Balancer、Polygon ・常連の投票者　4アドレス（匿名） - 当4名の投票により、①スナップショット投票の殆どの提案が意思決定されている

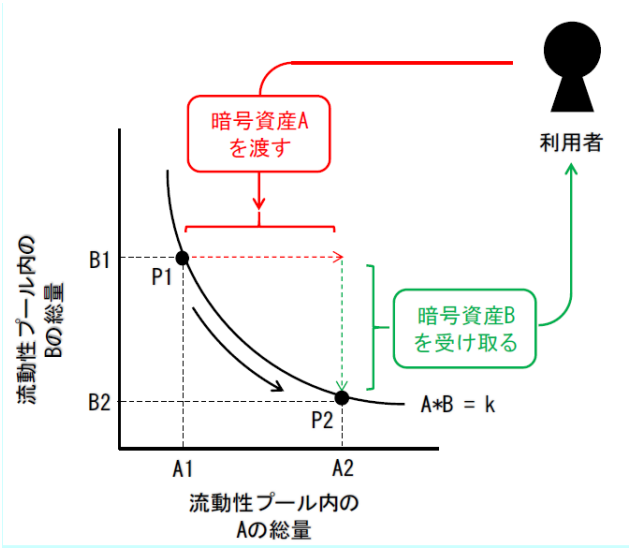
Uniswapの主な技術特性

(1) AMM（Autmated Market Maker：自動マーケットメーカー）

機能概要

- スマートコントラクトがUniswapの流動性プール（交換する暗号資産のペア）に預けられている暗号資産の量から取引価格（交換レート）を自動的に計算する仕組み
- 初期のDEXで主に活用されていたオーダブック方式と比較して、オフチェーン処理が不要であり、かつ注文スピードが早いことが特徴とされる
- Uniswap v1から実装

【暗号資産Aと暗号資産Bの交換例】



・取引前P1の状態
暗号資産A1＝10
暗号資産B1＝500
k＝10＊500＝5,000

・取引後P2の状態　暗号資産Aを1追加
手数料A＝1＊0.3%＝0.003
暗号資産A2
＝10＋1－0.003＝10.997
暗号資産B2
＝5,000÷10.997＝454.67
k＝10.997＊454.67=5,000

・利用者が受け取る暗号資産B
500－454.67＝45.33

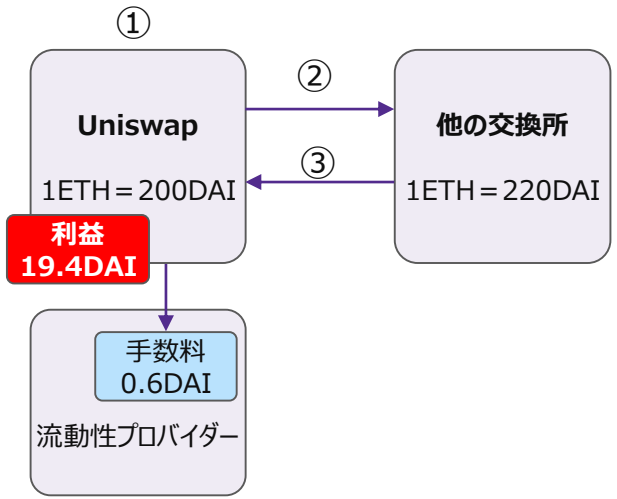
・手数料Aの0.003は流動性プロバイダーが取得する

(2) Flash Swap

機能概要

- 暗号資産A・Bからなる流動性プールにおいて、1回のトランザクション内でAと同額のBおよび手数料の合計を返却すれば、無担保で暗号資産Aを引き出して利用できる仕組みであり、主にアービトラージのために利用される。
- 暗号資産Bが返却されなかった場合は、暗号資産Aを引き出すトランザクション自体が無かったことになり、無担保であることのリスクが軽減されているとされる
- Uniswap v2から実装

【資本のない裁定取引の例】



下記①～③を1トランザクションで実行

①無担保で1ETH借りる

②1ETH＝220DAIで交換

③200DAI＋手数料0.3%を返却
手数料200＊0.3%＝0.6DAI
利益220-200-0.6＝19.4DAI

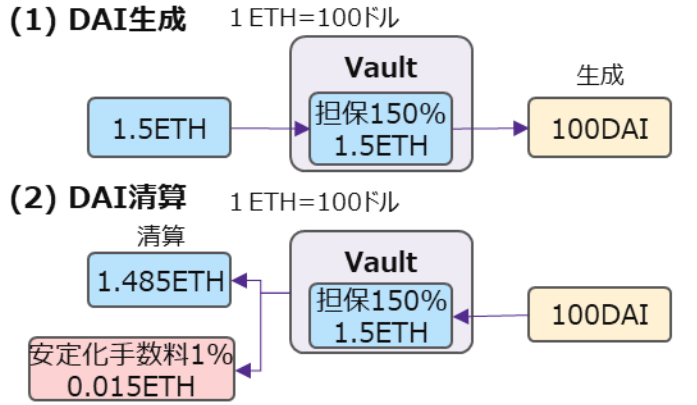
※DAI：Makerの暗号資産型ステーブルコイン

Makerの主な技術特性

(1) Maker Vault

機能概要

- Maker Vaultコントラクトに担保資産（ETH等の暗号資産やUSDC等のステーブルコイン）を預け入れることで、ステーブルコインDAIが生成される
- DAIの返却時に安定化手数料（Stability Fee）が発生。同手数料はMakerプロトコル内のバランスシートに蓄積され、閾値を超過した場合は超過オークション（Surplus Auction）でDAIとMKRの交換が行われ、入札に使われたMKRは焼却される
- Oasis やコミュニティによって構築されたインターフェース（Instadappなど）によりMaker Vaultへの簡易なアクセスが可能
- 担保資産の価格下落等により担保資産が清算比率を下回った場合は、担保オークションにより自動（強制）清算される
- 清算比率は担保資産毎にオンチェーン投票で選択される（ETHの場合は150%前後、USDCは101%など）



(1)DAI生成
Vaultに150%の担保資産を入れ、DAIを生成する

(2)DAI清算
Vaultの担保を買い取り、安定化手数料を差し引いて返却する

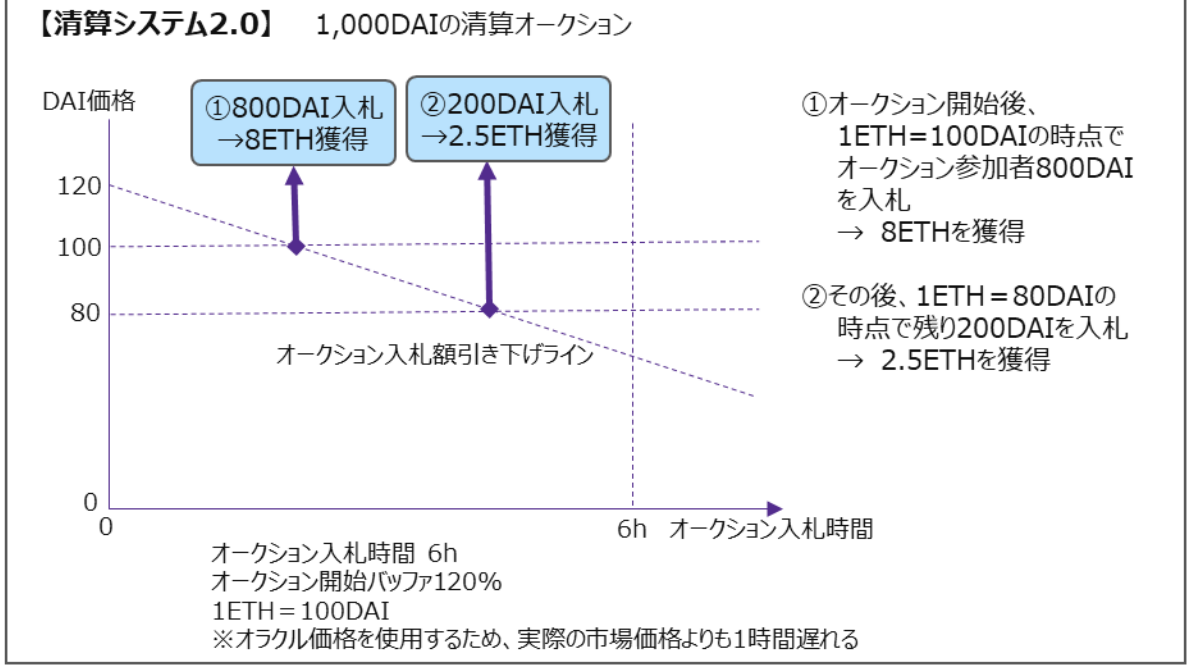
(3)DAI強制清算
担保資産の価格下落により担保が清算比率を下回る場合は、清算ペナルティを差し引いて担保オークションが起動されて担保資産を返却する

清算比率（120%など）を下回る→担保オークションが起動

(2) 清算システム2.0

機能概要

- 所定の担保比率を下回り強制清算に移行した際に、担保不足となったVaultに預けられていた担保資産をオークションにかけて負債（DAI）の清算を行う仕組み。オークション参加者はDAIを入札することで担保資産を取得する
- 2021/4にローンチしたダッチオークション方式の新たな清算メカニズム
- 担保が購入されるまでオークションの入札額が引き下げられる
- 部分入札を可能とし、オークション額を1人または複数の入札者が提示価格を分割して担保を購入できる
- フラッシュローンをサポートし、元手がなくても借入と返済を同時に行うことでオークションに参加が可能となる
- オークション入札時間や入札額引下率はオンチェーン投票で選択される



①オークション開始後、1ETH＝100DAIの時点でオークション参加者800DAIを入札
→ 8ETHを獲得

②その後、1ETH＝80DAIの時点で残り200DAIを入札
→ 2.5ETHを獲得

Aaveの主な技術特性

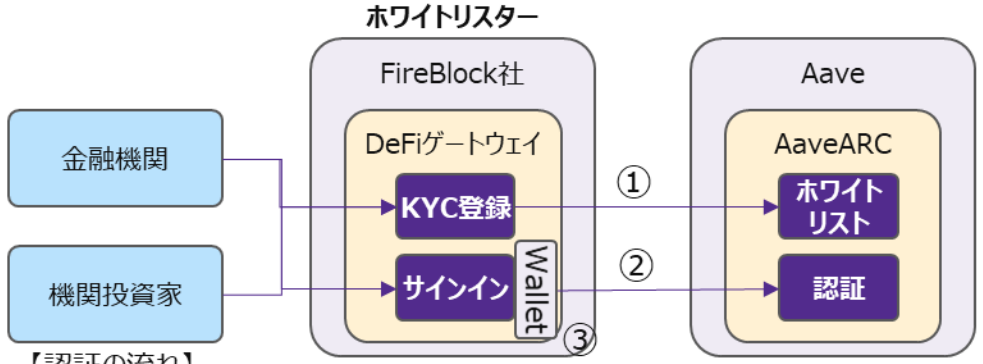
AaveArc / ホワイトリスター

機能概要

【AaveARC】
- 機関投資家等がコンプライアンスに準拠した形でDeFiエコシステムに参加することを目的とした、Permissioned型の機関投資家向けDeFiプロトコル
- KYC及び財務デューデリジェンスを機関投資家が、同様の承認を受けた他の機関投資家との 間のみでAAVEプロトコルの主要機能を活用して、運用を行うことができる。現時点での対象の暗号資産は、ETH、WBTC、USDC、AAVEの4つ。
- 2022年1月にEthereumのL2ソリューションであるArbitrumとOptimism上でデプロイ

【ホワイトリスター】
- AaveArcを介してAAVEプロトコルにアクセスする機関投資家に対してデューデリジェンスを 実行し、すべての参加機関がKYCおよびAML規制に準拠できるように承認し、「ホワイトリスト」に登録する。
- 米Fireblocks社が1社目としてローンチ済、米Securitize社、スイスSEBA Bankはガバナンス提案実施中（2022/2現在）

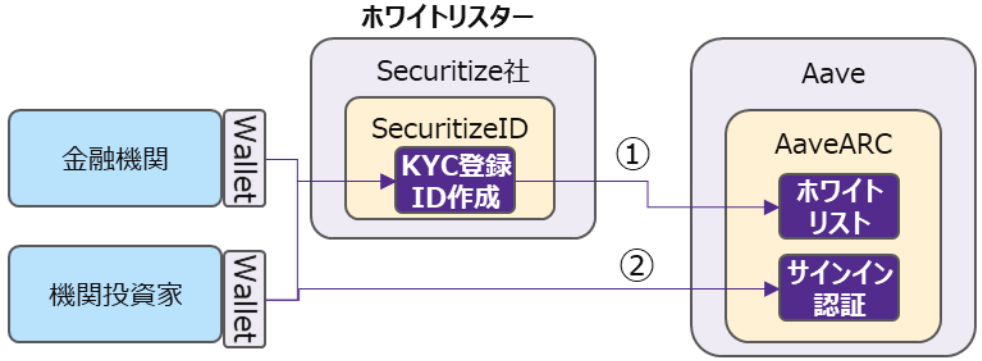
【FireBlock社 DeFiゲートウェイ】



【認証の流れ】
①Fireblocks社フレームワークでKYCを実行し、機関投資家をホワイトリストに登録する
②金融機関・機関投資家がFireblocksユーザーとなり、FireblocksのDeFiゲートウェイを介してAaveArcにアクセスする
③Fireblocks社のセキュアなMPC（Multi Party Computing）Walletを使用する

【登録する金融機関・機関投資家】 30機関を登録済
Bluefire Capital、Celsius、CoinShares、Seba Bank、GSR、Ribbit Capital、QCP Capital、Wintermuteなど

【Securitize社 SecuritizeID】



【認証の流れ】
①自分のWalletからSecuritizeiDを作成すると、WalletがAaveARCのホワイトリストにリンクされる
②自分のWalletからAaveArcにサインインして認証を取得すると、Walletアドレスに AaveArcで取引するための個別の権限（供給、借用、清算など）が付与される