金融庁　御中

「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」
研究結果報告書（概要版）

令和4年6月

株式会社クニエ

研究の目的・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）の事例分析等を行ったもの**
  - 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
  - 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。

謝辞・免責事項

謝辞

- 本報告書作成にあたっては、京都大学・岩下直行教授、早稲田大学・佐古和恵教授、慶応義塾大学・鈴木茂哉特任教授、米ジョージタウン大学・松尾真一郎研究教授から有益な助言やコメントを得た。また、デジタル庁・日本銀行のオブザーバー及び金融庁のご担当者からも有益な示唆・助言をいただいた。
- もっとも、本報告書に関する内容の誤りは、すべて受託者である株式会社クニエに帰する。

免責事項

- 本報告書の内容は金融庁の公式見解を示すものではない。
- 本報告書で記載している過去または現在の事実以外の内容については、本稿執筆時点で入手可能な情報に基づいた見通しであり、実際の動向等は種々の不確定要因によって変動する可能性がある。

目次

目次

用語集

用語	定義
AML/CFT	Anti Money Laundering and Combating the Financing of Terrorism マネー・ローンダリング及びテロ資金供与対策
BIS	Bank for International Settlements 国際決済銀行
DAO	Decentralized Autonomous Organization 分散型自律組織
DeFi	Decentralized Finance 分散型金融
ERC	Ethereum Request for Comments イーサリアム技術提案
EVM	Ethereum Virtual Machine イーサリアム仮想マシン：Ethereumスマートコントラクトを実行する仮想マシン
FATF	Financial Action Task Force 金融活動作業部会
FSB	Financial Stability Board 金融安定理事会
FISC	The Center for Financial Industry Information Systems 金融情報システムセンター
IEC	International Electrotechnical Commission 国際電気標準会議
IPA	Information-technology Promotion Agency, Japan 独立行政法人 情報処理推進機構
IOSCO	International Organization of Securities Commissions 証券監督者国際機構
ISO	International Organization for Standardization 国際標準化機構
KYC	Know Your Customer 顧客確認のプログラム
TVL	Total Value Locked DeFiに預けられた暗号資産の総額

第１章　分散型金融システムのトラストチェーンについての全体像の把握

1-1　分散型金融システムに関する主な定義

分散型金融システム (Decentralized Financial System)

2019年のFSBの報告では、分散型金融システムを「**分散型金融テクノロジーがもたらす可能性のあるシステム**」と定義している。さらに、分散型金融テクノロジーを「**金融サービスの提供における１つ以上の仲介者または集中型プロセスの必要性を削減または排除する可能性のあるテクノロジー**」と定義している。当報告書においても上記の定義を用いる。

※ 分散型金融システムは、既存の金融システムなどに見られる中央集権型（centralized)に対して非中央集権型(decentralized)のシステムの構築を目指しているとされる。一方、分散型システムの記述においては、分散型(distributed)とは計算機を分散配置することを意味しており、中央集権型のシステムも分散型システムの一形態と整理される。分散型金融システムに焦点を当てる本報告書においては、「分散」は非中央化の意味を含んでいるとして用いることとする。

DeFi（Decentralized Finance）

いわゆるDeFiについては、様々な文献や記事などで論じられているが明確な定義はされていない。当報告書では参考文献に従い「**分散型金融システムの一部を構築する金融アプリケーション**」と定義する。DeFiは、Ethereumブロックチェーンのローンチの後、当初は資金調達のための独自トークン発行や、トークンの交換に従来型の取引所の仲介を必要としないDEX（分散型取引所）が主であったが、DeFiエコシステムの拡大に伴い、レンディングやデリバティブ、保険など伝統的金融を踏まえて様々な取り組みが発生している。また、複数のDeFiの取引を1つにまとめてサービスを提供するアグリゲーターなどもある。

DAO (Decentralized Autonomous Organization)

DeFiを運営する分散型自律組織（DAO）について、定まった定義は存在していないが、当報告書では、参考文献やMakerDAOの事例などを踏まえて、「**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**」と定義する。

※ 主なDeFiプロジェクトにおけるDAOの特徴

- 運営する会社や代表者・取締役会などが存在せず、参加者が自律的に運営を行う組織
- 組織の運営ルールがスマートコントラクトによってコード化されている
- ガバナンストークンなどと呼称されるトークンに紐づく形で一種の議決権（投票権）がトークン保有者に付与され、組織・コミュニティの意思決定（の一部）について、スマートコントラクトのルールに基づいて投票が行われる
- 複数の国に所属する参加者がグローバルに活動する組織であり、また必ずしも管理法人が明確でないため、組織が所属する国や地域が特定されない

1-1　分散型金融システムに関する主な定義

トラストポイント／トラストチェーン

トラストについて、金融庁の「デジタル・分散型金融への対応のあり方等に関する研究会」中間論点整理においては、「相手の監視や制御が可能かどうかに関係なく、相手が自分にとって重要な行動をとってくれるという期待に基づいて、相手の行動に自身の「ヴァルネラビリティ」を託する意志」および「事実の確認をしない状態で、相手先が期待したとおりに振る舞うと信じる度合い」※1と定義されている。

　この定義に則った上で、当報告書では、トラストポイントを分散型金融システムにおける「**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**」と定義し、トラストチェーンは「**依存関係の連なりの中にトラストポイントが含まれているもの**」と定義する。

Weakest Link

Weakest Linkとは、当報告書では、DeFiの構成要素及び構成要素間の接続部分のうち、セキュリティ上最も弱い部分を指す。攻撃者は Weakest link を狙うことで、攻撃が成功する可能性を最も高めようとする。

1-2 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の例）

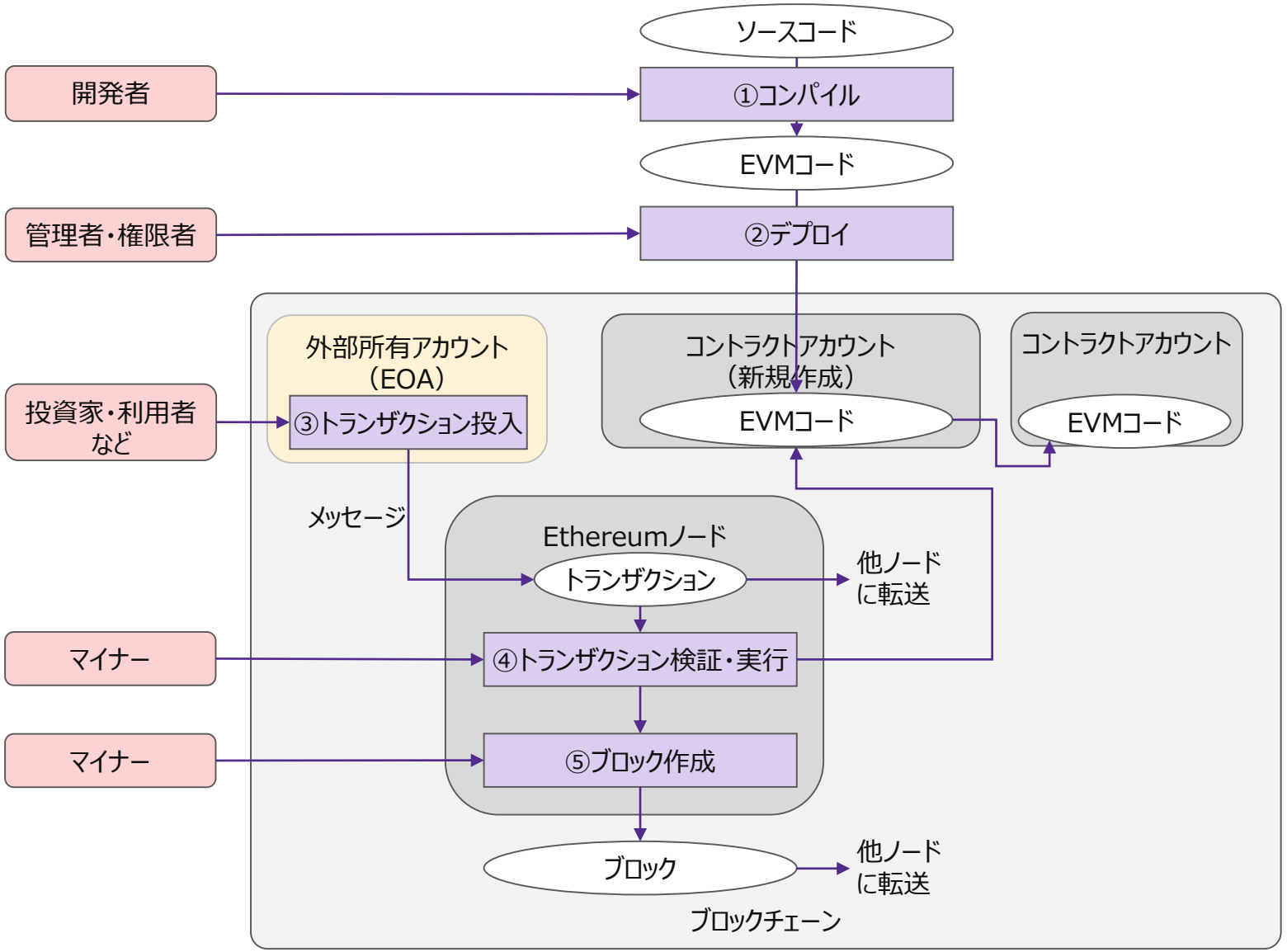


図 1-2　スマートコントラクトの実行の流れ（Ethereumの例）

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。

1-2　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。

1-3　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

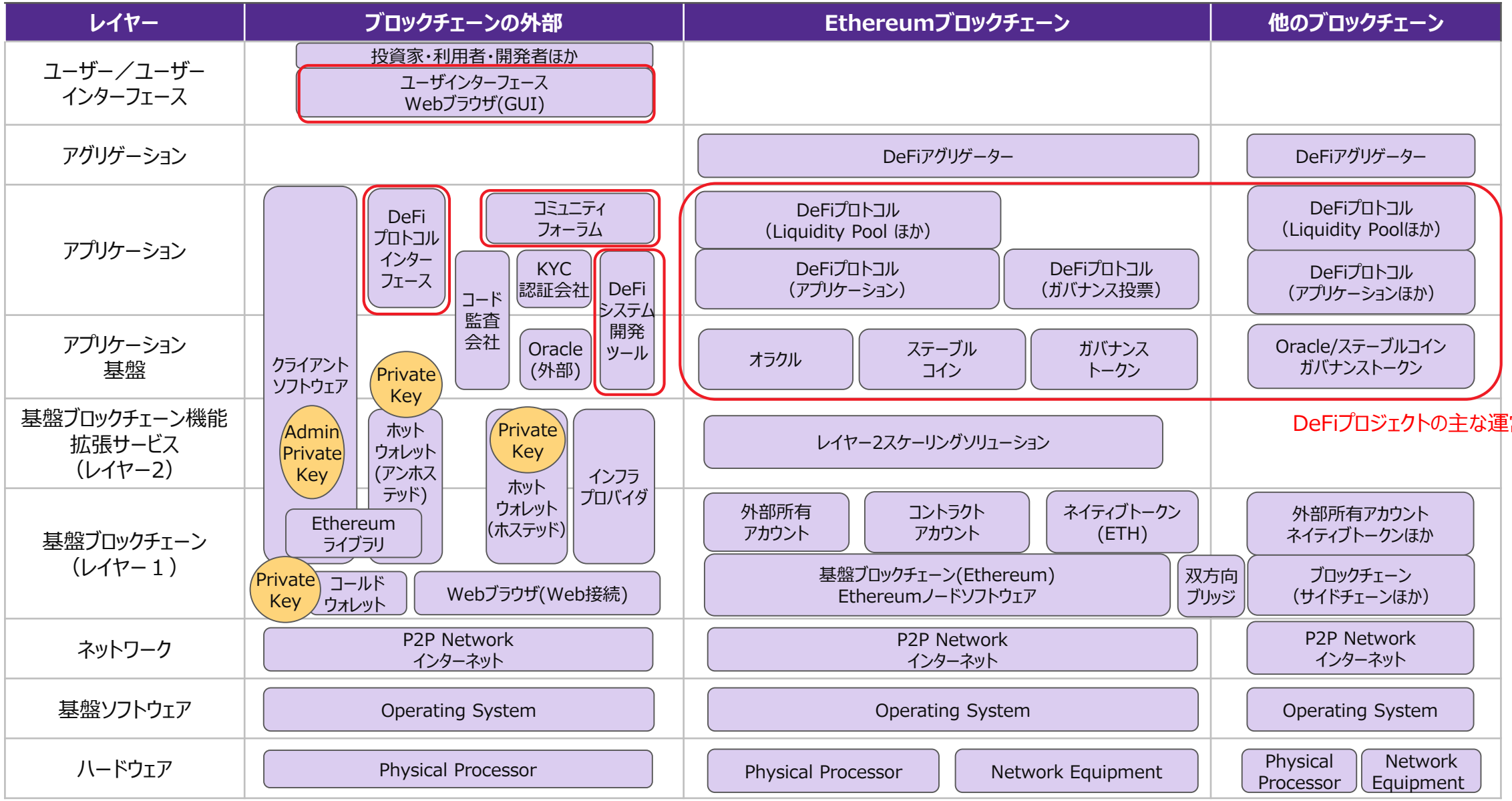


図 1-3　分散型金融システムの主な構成要素のマッピング

第２章　主要なDeFiプロジェクトについての分析

2-1　調査対象プロジェクトの概要

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	-

2-1　調査対象プロジェクトの概要

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

2-1　調査対象プロジェクトの概要

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）

2-1　調査対象プロジェクトの概要

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

2-1　調査対象プロジェクトの概要

項目	内容	Uniswap	Maker	Aave
金融機関との連携	決済関連	デビットカードの決済資金に利用する ・Crypto.com UNI・MKR・AAVE等で商品購入（Shopping.io）や旅行（Travala.com）など約30店舗への支払いが可能		
			・Monolith DAIを法定通貨に交換し、VISAデビットカードにロードして使用する	
	金融商品	DeFi Technologies（カナダのTech企業）の子会社Valour（スイス資産運用会社）を通して、UNIにパッシブ連動するETP（上場投資商品）を上場 ・ドイツフランクフルト株式市場（2021/10） ユーロ建Valour Uniswap ETP ・スウェーデン株式市場（2021/12） クローナ建Valour Uniswap SEK	–	–
	カストディ・トレーディングサービス	Sygnum Bank AG（スイスのデジタルバンク）がAAVEトークンを含む複数のDeFiトークン（ガバナンストークン）及びステーブルコイン（USDC）のカストディ、トレーディングサービスを開始することを発表 （2021/6）		
		Commonwealth Bank (オーストラリア)がGemini Exchange、Chainalysisとパートナーシップを組んで、10種類の暗号資産の交換（crypto exchange)とカストディサービスを開始（2021/11）	–	Commonwealth Bank (オーストラリア)がGemini Exchange、Chainalysisとパートナーシップを組んで、10種類の暗号資産の交換（crypto exchange)とカストディサービスを開始（2021/11）
		Arab Bank Switzerland（スイス）が10種類の暗号資産関連サービスを提供（2022/1）	–	Arab Bank Switzerland（スイス）が10種類の暗号資産関連サービスを提供（2022/1）

2-1　調査対象プロジェクトの概要

項目	内容	Uniswap	Maker	Aave
金融機関との連携	STO不動産ローン ※STO：Security Token Offering	–	・Forge（仏Société Généraleのデジタル資産子会社）とSTOによる不動産ローンで提携（2021/10） ※DAI発行計画における6つの事業体 ①Société Générale ②Forge ③MakerDAOプロトコル ④MakerDAOのリーガル代表者 ⑤DIISグループ（仏債券投資家）証券エージェントの役割 ⑥取引所	–
	その他の取組み	Fintech企業とタイアップして市場参入を検討中との報道（2021/7） ・PayPal ・Robinhood（米株式運用アプリ運営） ・E*Trade（米オンライン証券会社） ・Stripe（米オンライン決済）等	・チャリティに寄付する（USDとして支払う） ユニセフ（慈善団体） NeedsList（災害支援） PoolDai（慈善団体寄付基金） ・給与ソリューション Whisp Money（一部のコミュニティではKYCが不安定な外部雇用者にDAIで給与支払を行っている）	・AaveARC 財務デューデリジェンスを受けた機関投資家が、他に承認を受けた機関投資家と暗号資産を貸借できるようにする機能 ・ホワイトリスター AaveARCホワイトリストに登録する機関投資家を登録するためにAaveから承認された会社 登録済：米Fireblocks社（2022/1） 登録手続中： 米Securitize社、スイスSEBA Bank

2-2 分散型取引所 Uniswapの分析

2-2-1 プロジェクト全体概要

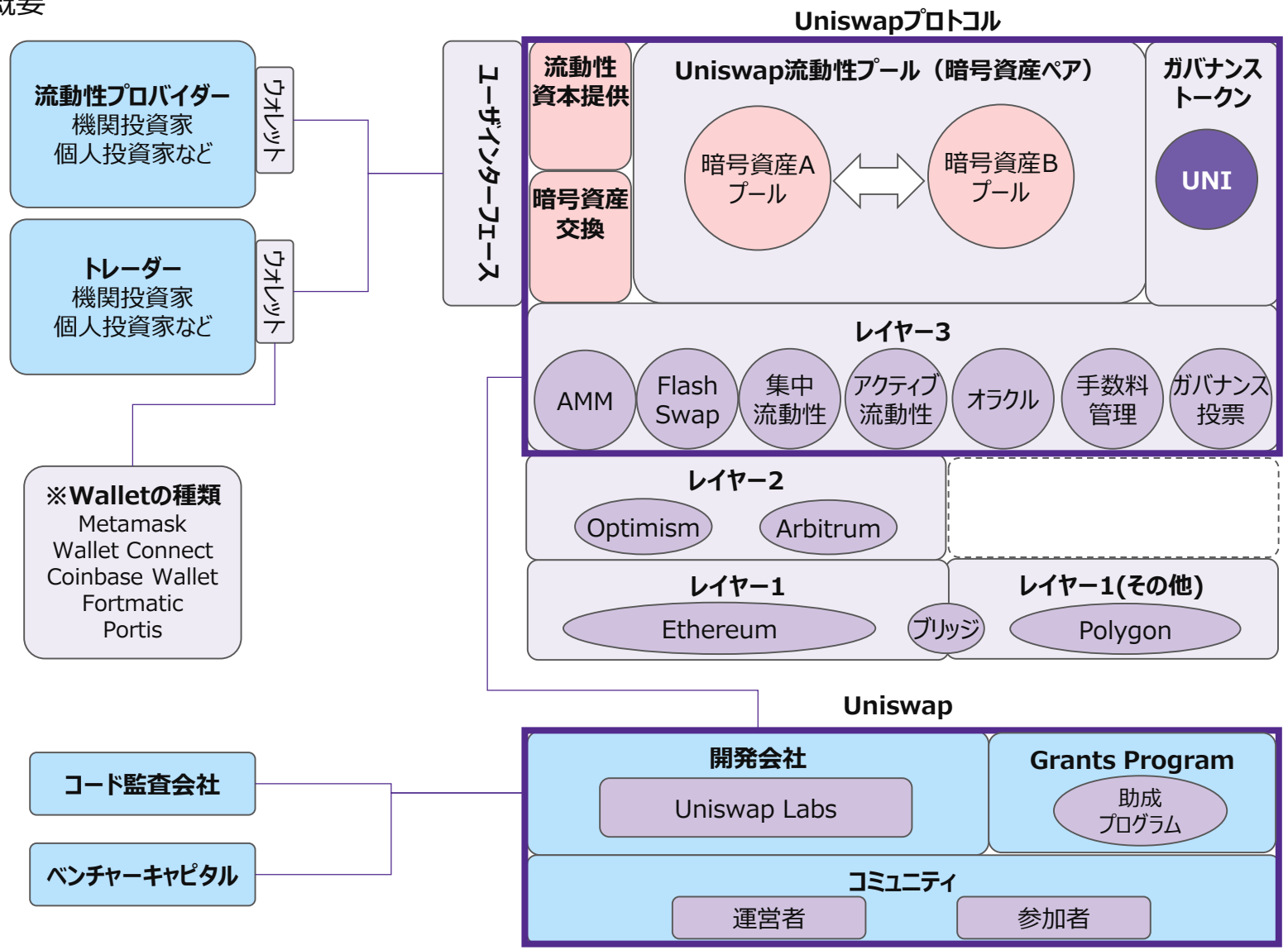
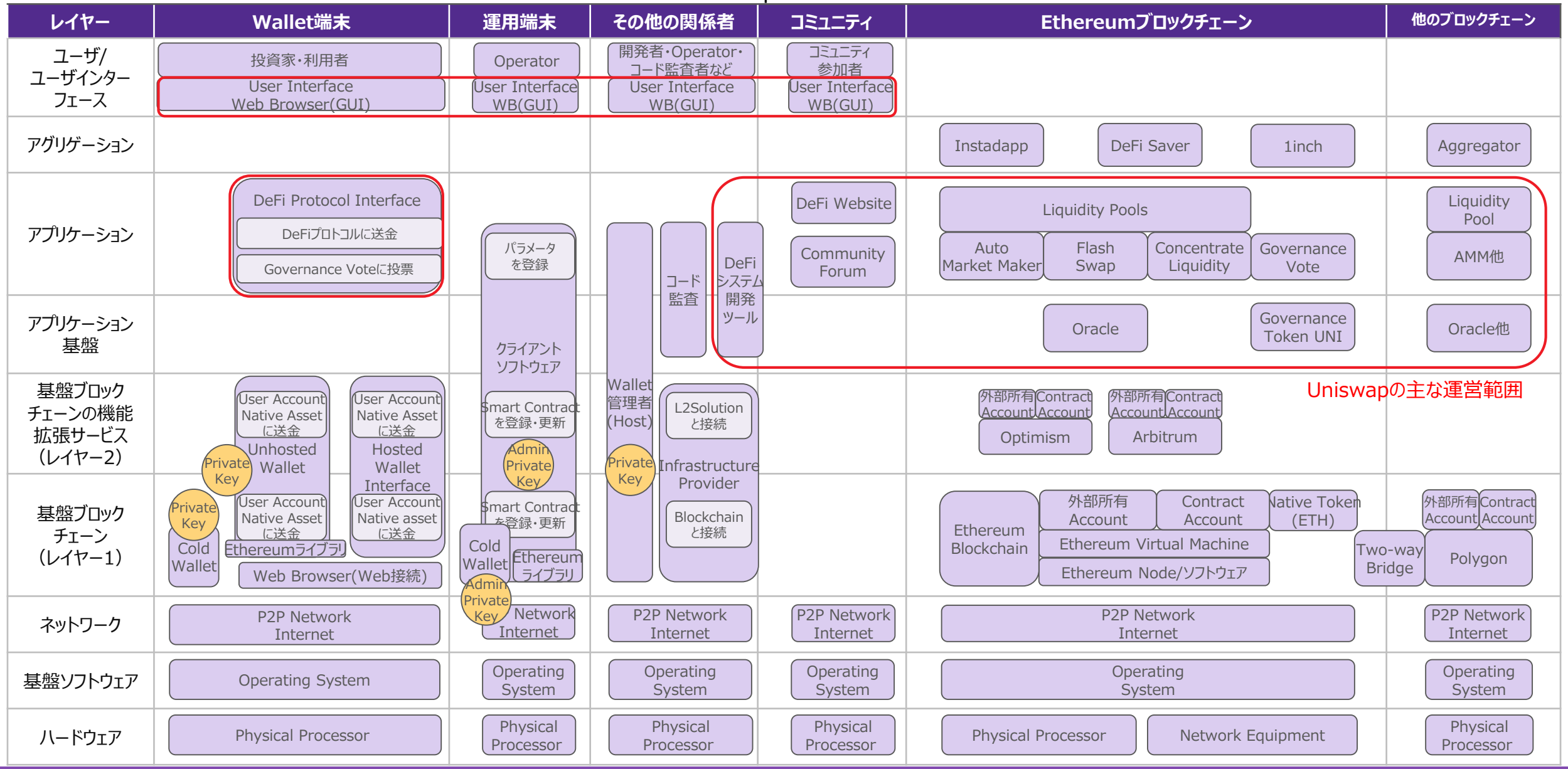


図 2-2-1-1 Uniswapの主な構成要素

2-2 分散型取引所 Uniswapの分析

2-2-1 プロジェクト全体概要

図 2-2-1-2 Uniswapの主な構成要素のマッピング



2-2 分散型取引所 Uniswapの分析

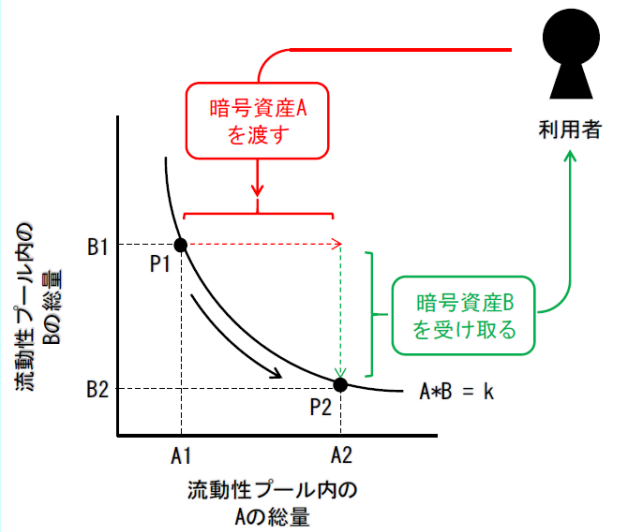
2-2-2 主な技術特性

(1) AMM（Automated 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

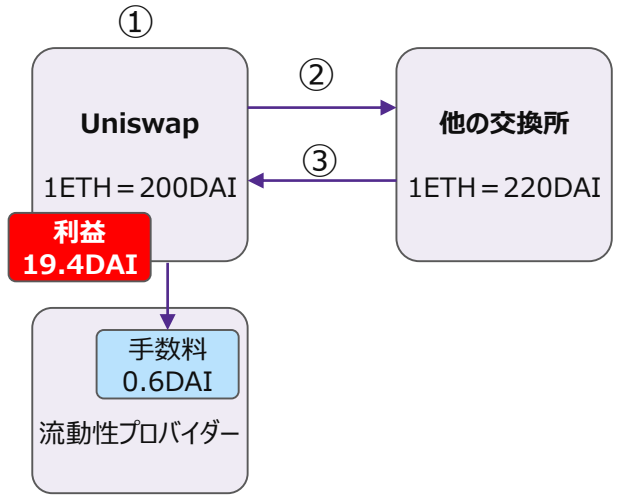
・手数料Aの0.003は流動性プロバイダーが取得する

(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

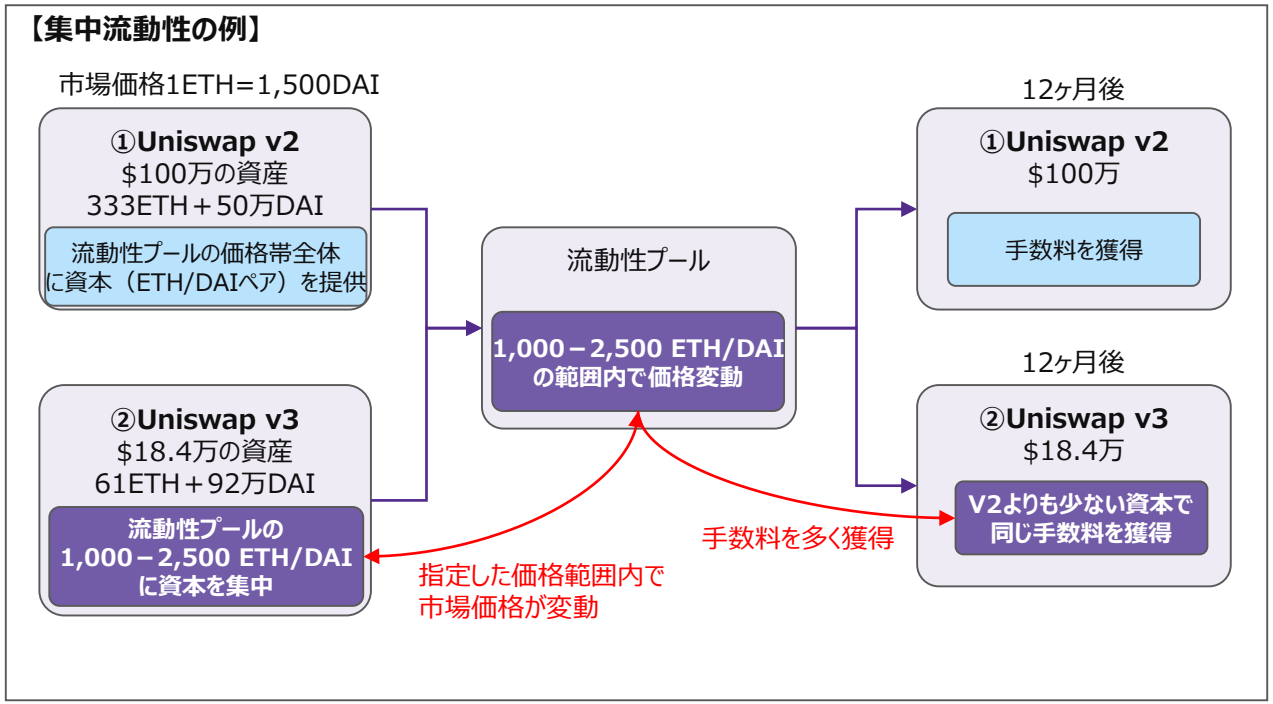
2-2 分散型取引所 Uniswapの分析

2-2-2 主な技術特性

(3) 流動性集約機能

機能概要	・流動性プールに流動性を提供する際に、交換に応じる価格帯を指定できる機能。 ・流動性プールの価格範囲を指定して、資本を集中させることにより流動性プロバイダの資本効率を上げるもの（上値・下値の価格範囲を指定して、市場価格が範囲に入るとプールの暗号資産に交換される指値注文に類似した形）。Uniswap v3で導入され、v2と比べて資本効率を4,000倍向上できるとされる。 ・市場価格が指定した価格範囲の外に移動した場合には暗号資産ペアのうち一方の流動性が枯渇するため、それ以上の手数料が獲得できなくなる。 ・流動性プロバイダ毎の流動性ポジションが異なる価格帯・異なる流動性で形成されるため、従来の代替性トークン（ERC20）ではなく非代替性トークン（NFT）で流動性ポジションを管理。スワップ手数料はv1, v2では継続的に流動性プールに再投資されていたが、v3より再投資されなくなった。

【集中流動性の例】



①Uniswap v2は、資本を流動性プールの価格帯全体に提供する

→ ほとんどの流動性プールでは、この大部分が使用されることがなく資本効率が低かった
例）DAI/USDCペアは$0.99~$1.01の間の取引のために、資本のわずか0.50%しか使用しないが、最も多くの手数料を獲得する価格範囲になる

②Uniswap v3は、資本を流動性プールの指定した範囲に集中して提供できる

→ 市場価格が指定した範囲内で変動する場合は、資本が有効に使われるため資本効率が向上（少ない資本で多くの手数料獲得が可能に）

→ 万一、資本の価値がゼロになった場合、v3はv2に比べて提供する資本が小さいため損失が小さくなるメリットがある

※USDC（USD Coin）：Centre社が発行するドル資産担保型のステーブルコイン

2-2 分散型取引所 Uniswapの分析

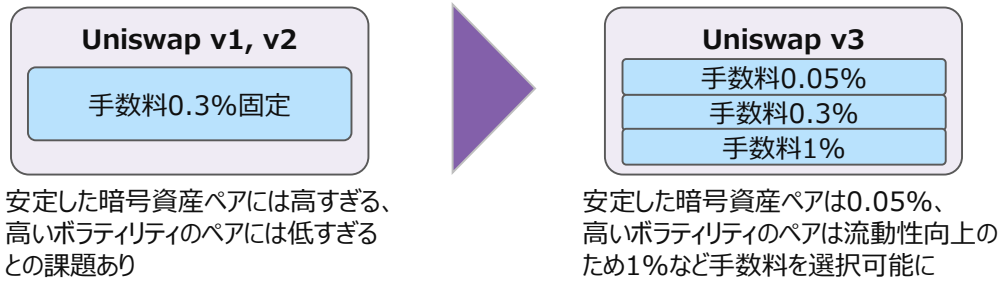
2-2-2 主な技術特性

(4) 手数料の拡張

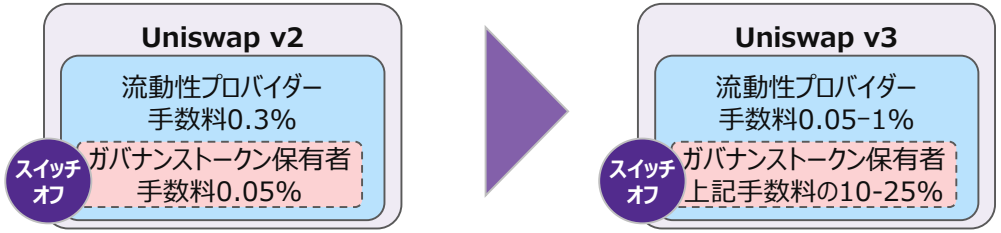
機能概要

- 流動性プールおよび流動性プロバイダー毎に複数の料金階層を提供する
  - －Uniswap v1, v2：0.3%に固定（ハードコーディングされている）
  - －Uniswap v3：0.05%, 0.3%, 1%の3つを選択できるように改善
- プロトコル料金スイッチを導入し、ガバナンス投票によりスイッチオンにするとガバナンストークン保有者が手数料を得ることができる（デフォルトはオフ）
  - －Uniswap v2：ガバナンス投票により手数料0.3%のうち0.05%を得る
  - －Uniswap v3：ガバナンス投票により手数料の10-25%の間に設定可能

【手数料の複数化】



【プロトコル料金スイッチ】 スイッチオンはガバナンス投票で決定（デフォルトはオフ）

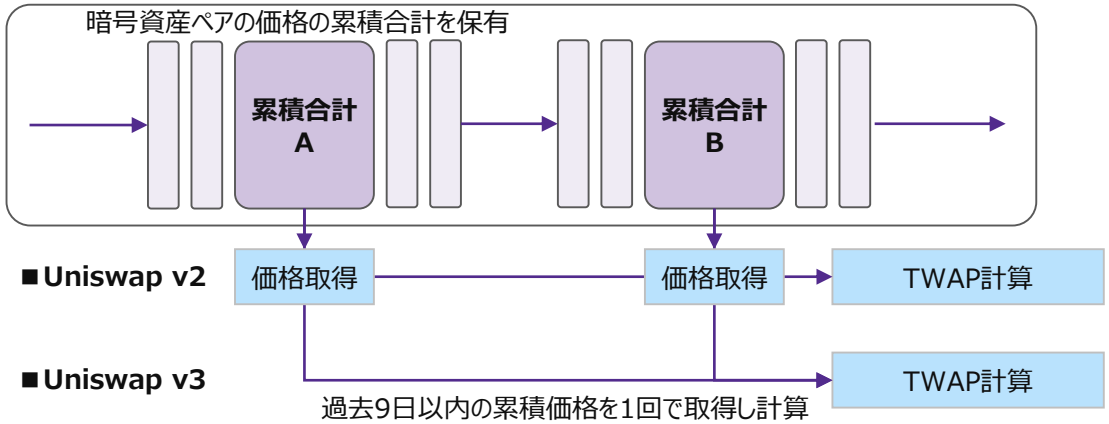


(5) オラクルの高度化

機能概要

- Uniswap v2
  - －TWAP（時間加重平均価格）オラクル
    暗号資産ペアの価格累積合計の開始時・終了時を取得しTWAPを計算
  - －オンチェーン価格フィード
    取引が行われる前に、各ブロックの開始時に市場価格を測定する
- Uniswap v3
  - －過去9日以内の累積合計を1回で取得しTWAPを計算、ガス代50%削減

【TWAP（時間加重平均価格】



2-2 分散型取引所 Uniswapの分析

2-2-2 主な技術特性

項目	概要	補足事項
(7) スマートコントラクトの変更可能性	①コアコントラクト • Uniswap v1,v2 コアコントラクトは設計上アップグレードが不可能 • Uniswap v3 コアコントラクトは設計上アップグレードはできないが、コアコントラクト外の手数料パラメータは変更可能	• コアコントラクト：重要なロジックが対象で、最小限の設計 - 流動性プール、AMM、Flash Swap、流動性集約機能、手数料機能、オラクル機能 • コアコントラクトのアップグレードはできないため、異なるセットを新しいバージョンとして実装し、それに併せて脆弱性の修正や機能改善を行う
	②コア以外の外部コントラクト 制約なく変更・追加・削除ができる	• ガバナンス投票の可決を受けてUniswap Labsが実施する
(8) ライセンス管理	Uniswap v3プロトコルの商用ライセンス保護 • Business Source License 1.1により、ライセンスは商用または実稼働環境でのv3ソースコードの使用を最大2年間制限する • ガバナンス投票により、いつでもライセンス期間の変更や免除ができる • ライセンス対象は、スマートコントラクト、数学ライブラリ、周辺機器コントラクト、インターフェイス、開発者SDKを含む • ソースコードの参照は可能 以前のバージョンでSushiswapにスマートコントラクトを流用されたことも踏まえ、一定期間は他の流用を防止することが目的	• 開発したUniswap Labsが、ソースコードのライセンス管理権限をガバナンスに委託した形となる • 再利用可とせずオープンソースでは無いことを明確化した事例

2-2　分散型取引所　Uniswapの分析

2-2-3　ガバナンス運営

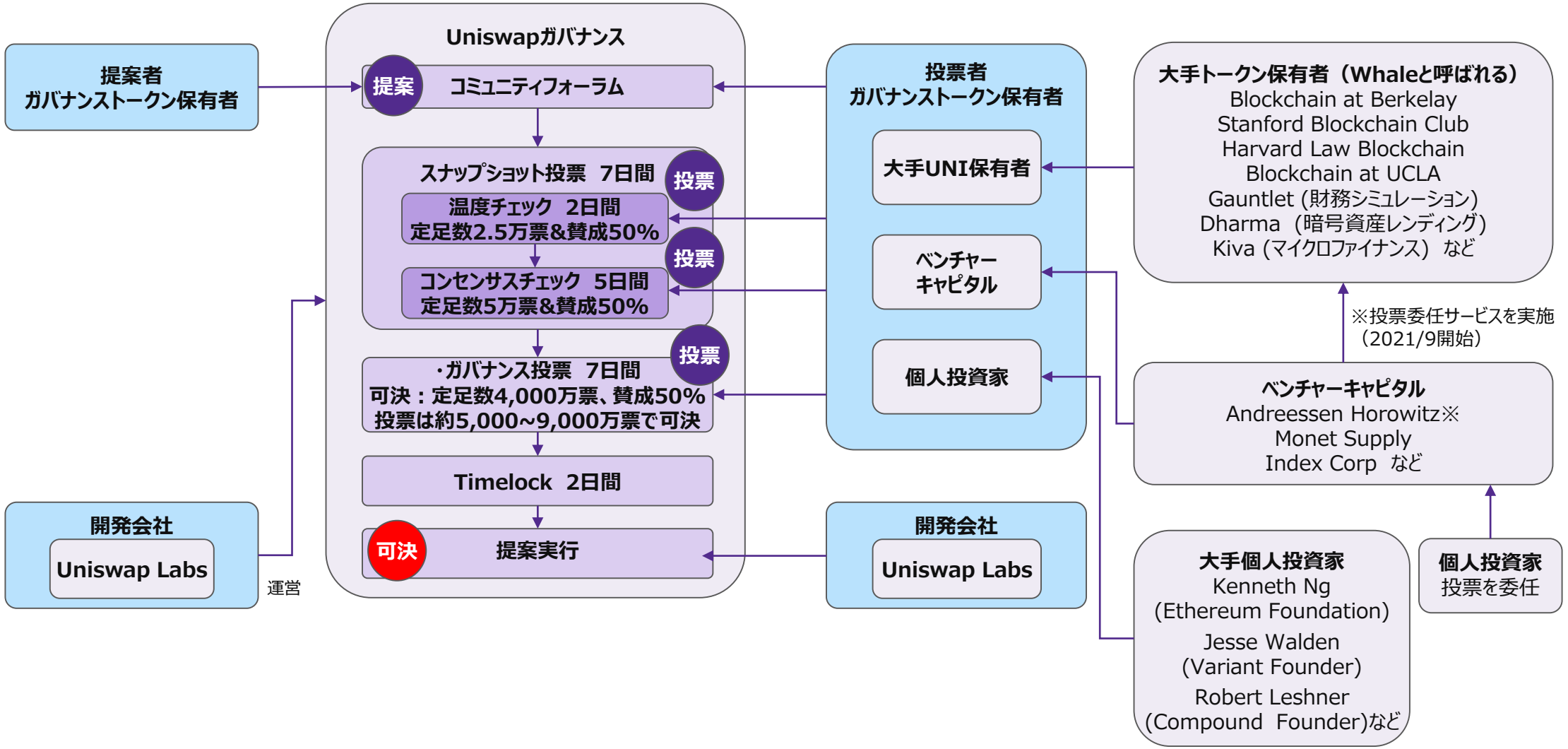
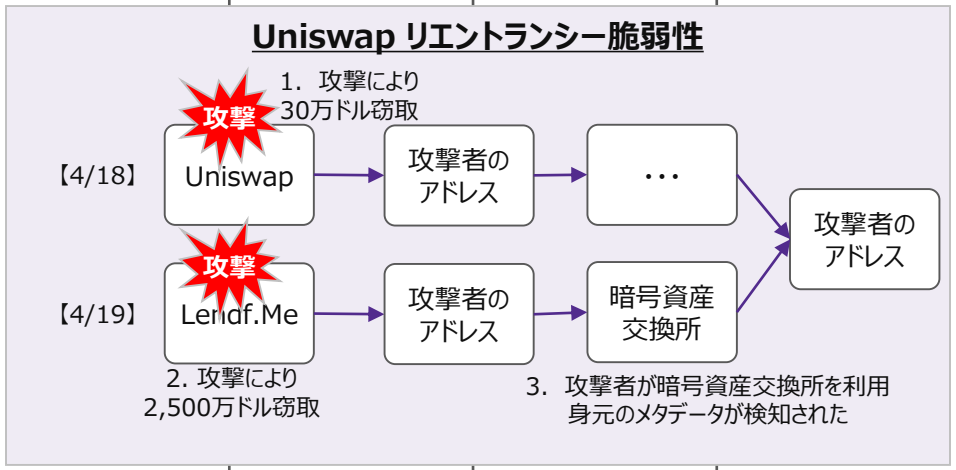


図 2-2-3　UNIを用いたガバナンス投票プロセス

2-2 分散型取引所 Uniswapの分析

2-2-4 インシデント事例

発生日	被害額	関連DeFi	関連する要素	事件の概要	発生原因
2020/4/18	約30万ドル	Uniswap Lendf.Me※1	ERC-777トークン	• 4/18にUniswapが攻撃者に攻撃を受け、約30万ドルを窃取された。 • 4/19に同じ手口でLendf.Meが攻撃され、約2,500万ドルが搾取された。 • Lendf.Me攻撃後の資金移動において、攻撃者が暗号資産取引所のサービスを直接利用していたことにより、身元の特定に繋がる情報が検出された。この情報によりLendf.Meが攻撃者と交渉し、資金の99%が返還された。 【事件の流れ】 1. 4/18 Uniswapがリエントランシー攻撃※1を受け、約30万ドルが搾取された 2. 4/19 Lendf.Meが同じ手口で攻撃を受け約2,500万ドルが搾取された 3. 4/19 攻撃者が資金移動中に暗号資産交換所のサービスを直接利用し身元のメタデータが検知された 4. 4/21 攻撃者の身元が判明し、Lendf.Meが交渉した結果、資金の99%が返還された 【搾取された資金と暗号資産】 • Uniswap 約30万ドル imBTC, ETHの２種類 • Lendf.ME 約2,500万ドル WETH, USDT, HBTC, imBTCなど計12種類	• UniswapおよびLendf.Meのスマートコントラクトのリエントランシー脆弱性 ⇒ERC-777トークン対応が未整備だったことによるリエントランシー脆弱性があった



※1 Lendf.Me：分散型レンディングサービス ※2 ERC-777トークン：ERC20として振舞いながら、トークンを送受信できるスマートコントラクト用のインターフェイス
※2 リエントランシー脆弱性：不正に再帰的な処理の実行（スマートコントラクトの処理が終了する前に同じ処理を再度呼び出すことで、例えば残高が引かれる前に何度も送金を実行させる）を引き起こす脆弱性

2-2 分散型取引所 Uniswapの分析

2-2-4 インシデント事例

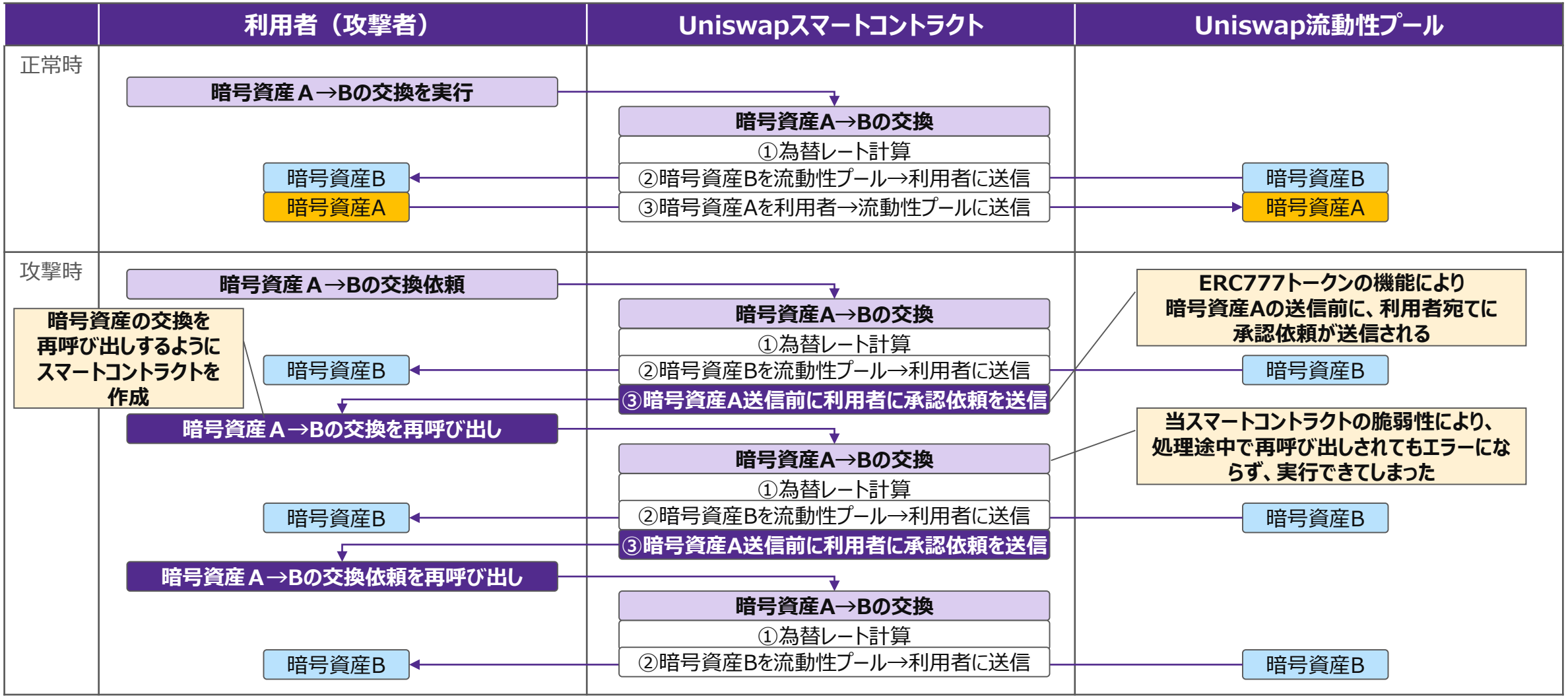
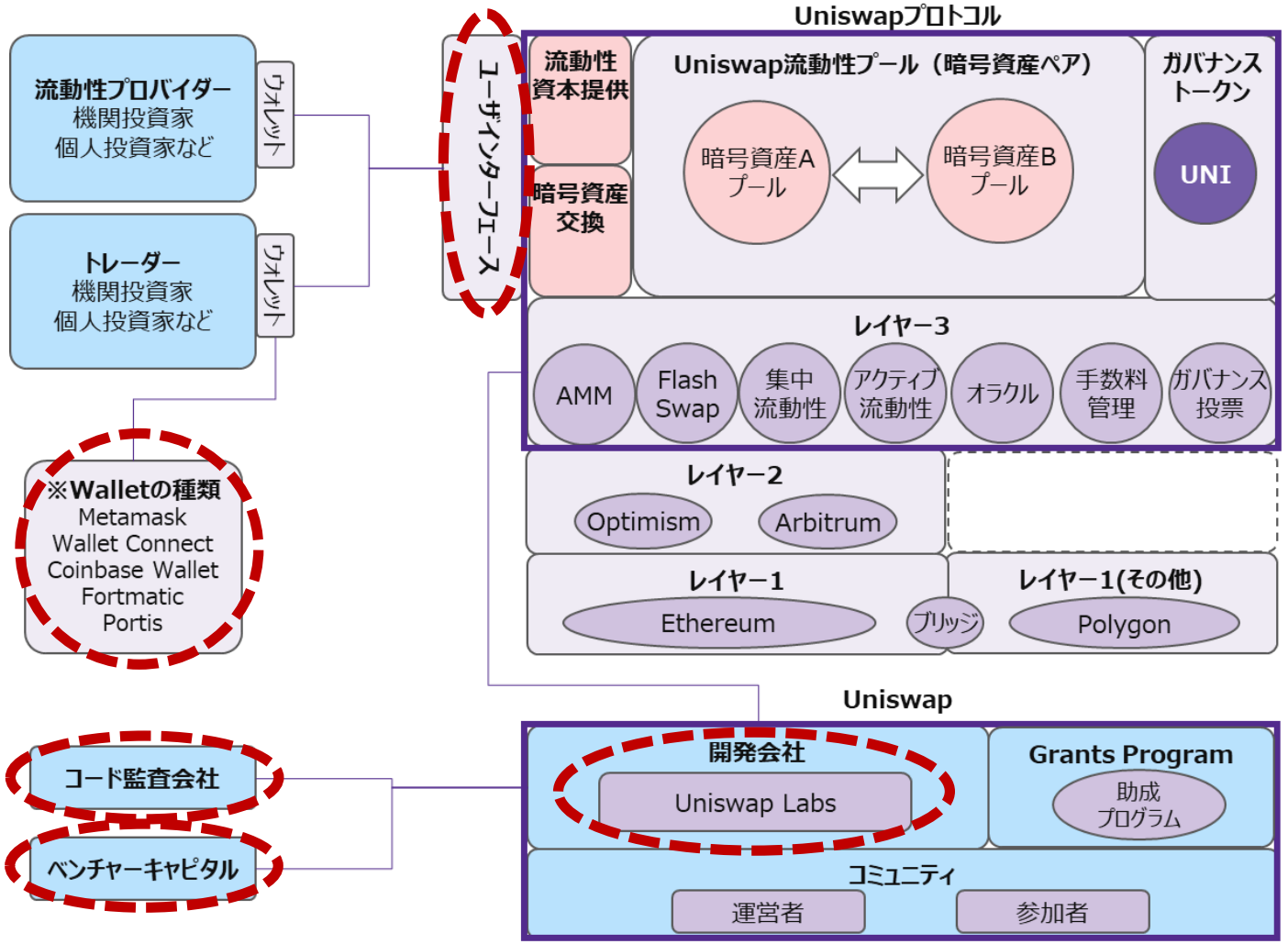


図 2-2-4 Uniswapリエントランシー脆弱性に起因した攻撃の概要

2-2 分散型取引所 Uniswapの分析

2-2-5 Uniswapの主なトラストポイント

- 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）等を提供
- 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）など



トラストポイントと考えられる点

図 2-2-5-1 Uniswapの主なトラストポイント

2-2 分散型取引所 Uniswapの分析

2-2-5 Uniswapの主なトラストポイント

- 初期投資家としてUNIの約18%の配布を受けたVCも含め、大口ガバナンストークン保有者が意思決定に影響力を有する可能性
- コミュニティの運営等においてUniswap Labsが一定程度の関与

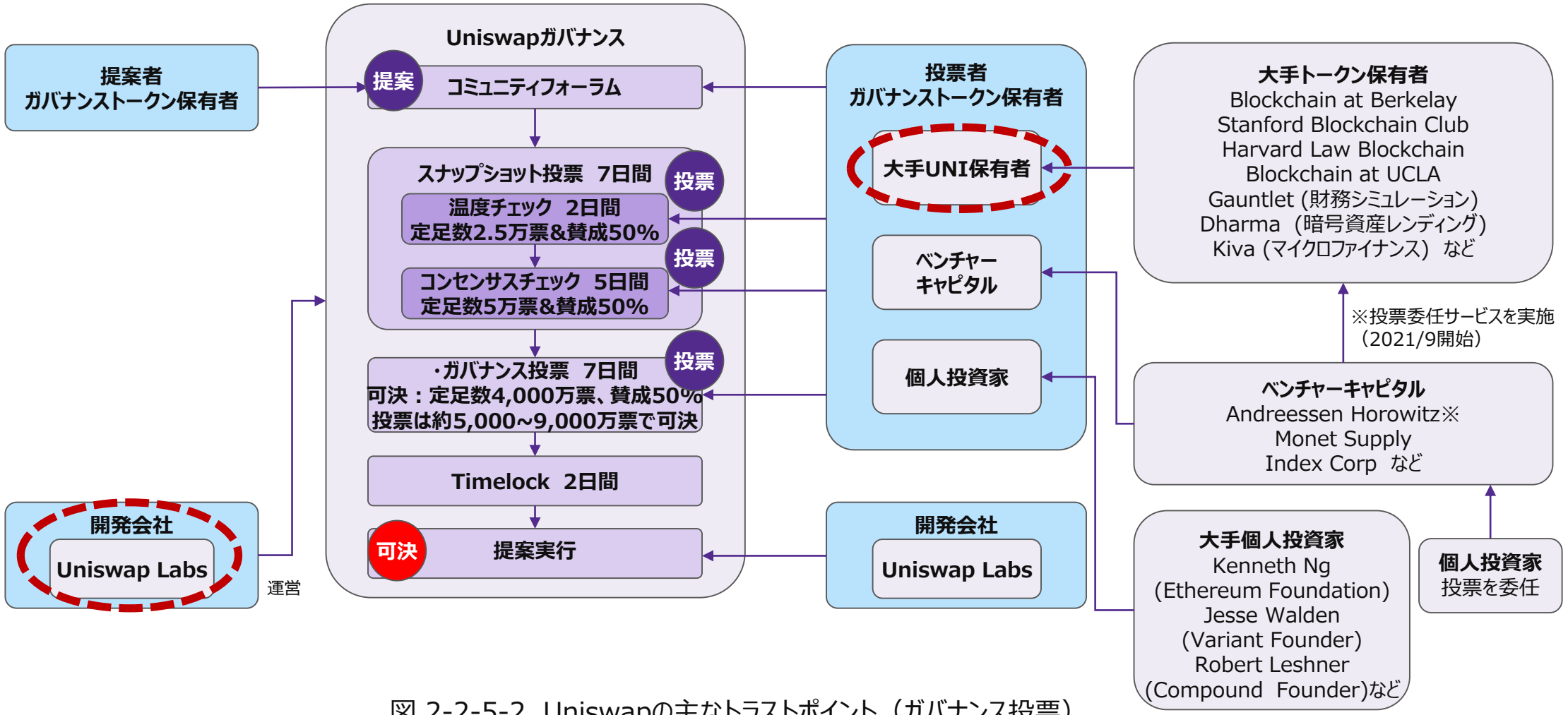


図 2-2-5-2 Uniswapの主なトラストポイント（ガバナンス投票）

2-3 ステーブルコイン Maker（DAI）の分析

2-3-1 プロジェクト全体概要

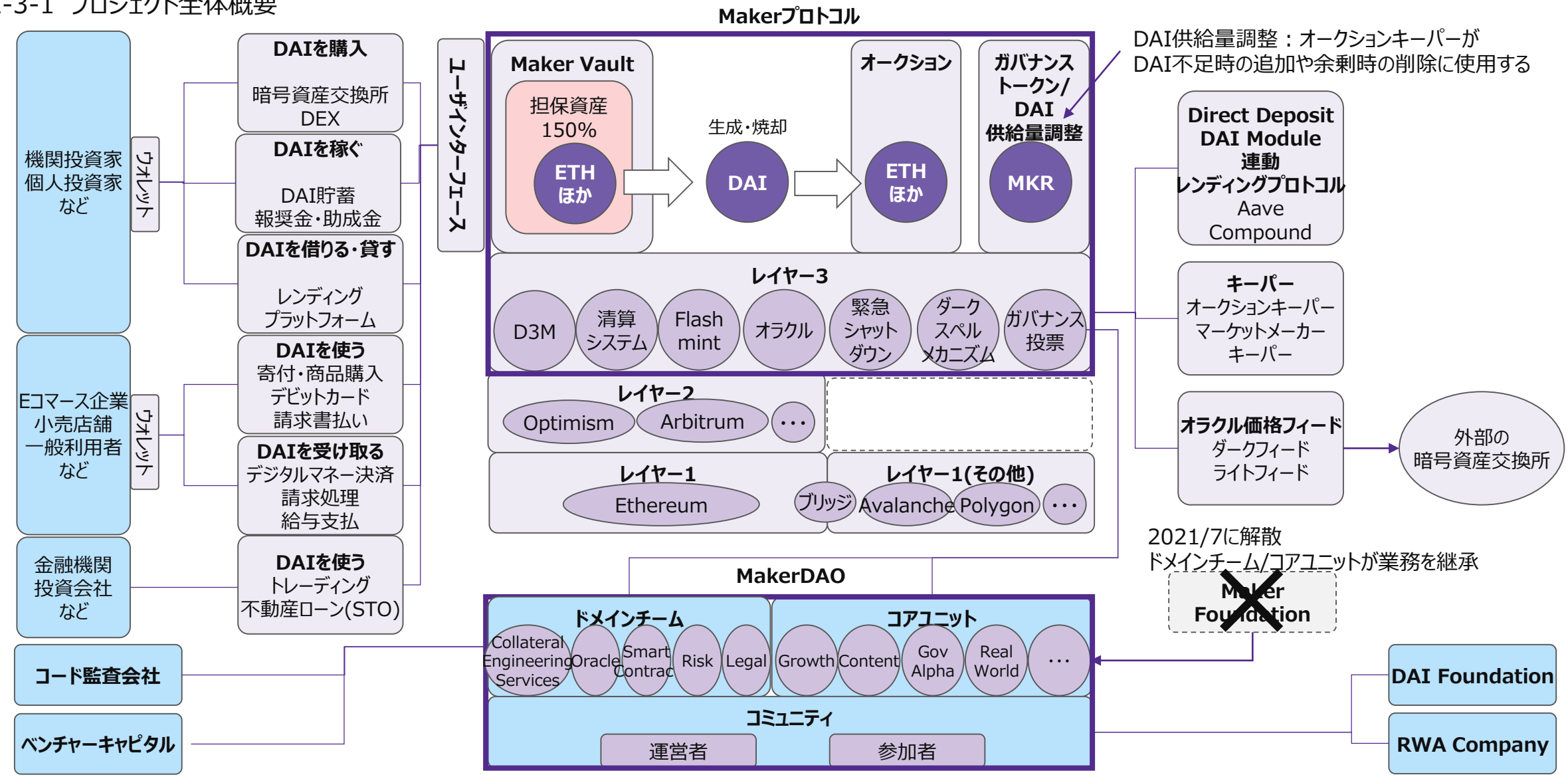
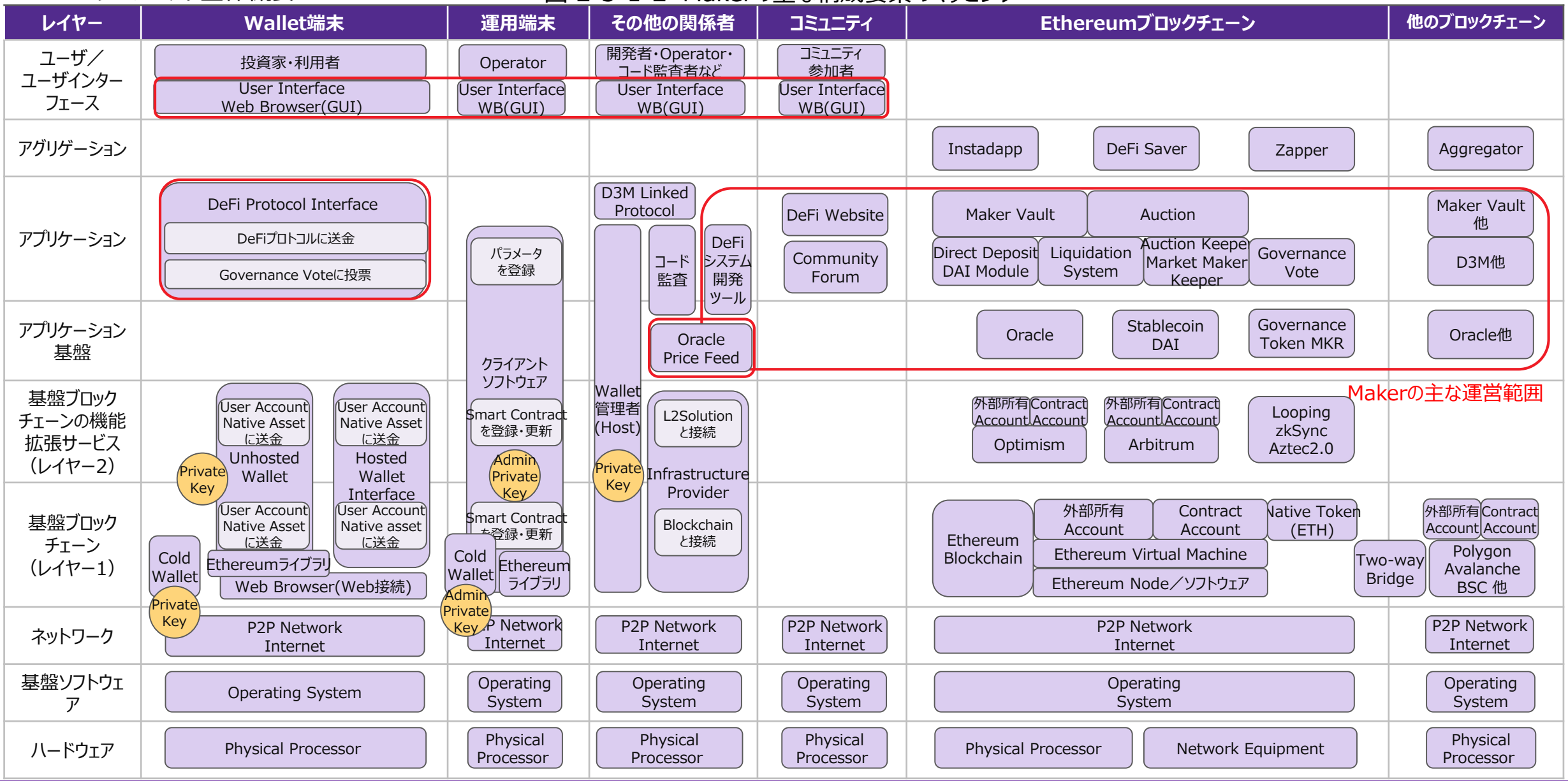


図 2-3-1-1 Makerの主な構成要素

2-3 ステーブルコイン Maker（DAI）の分析

2-3-1 プロジェクト全体概要

図 2-3-1-2 Makerの主な構成要素のマッピング



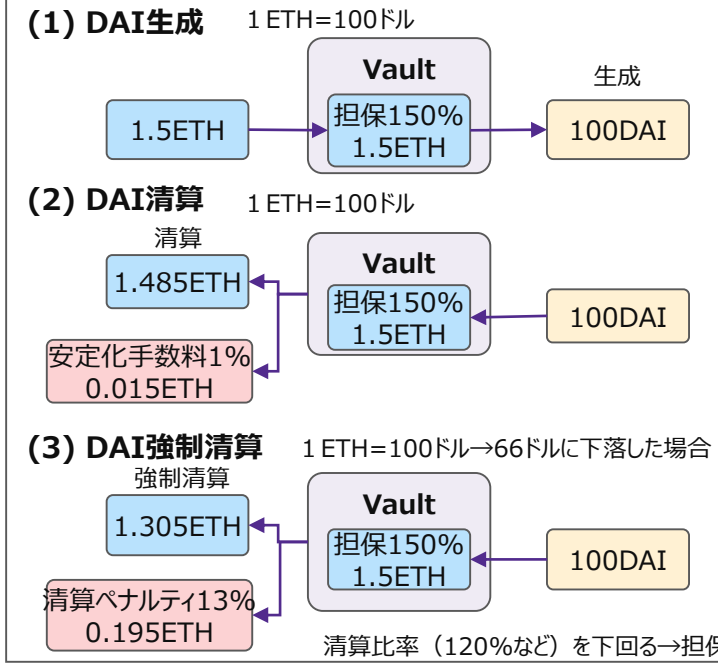
2-3 ステーブルコイン Maker（DAI）の分析

2-3-2 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

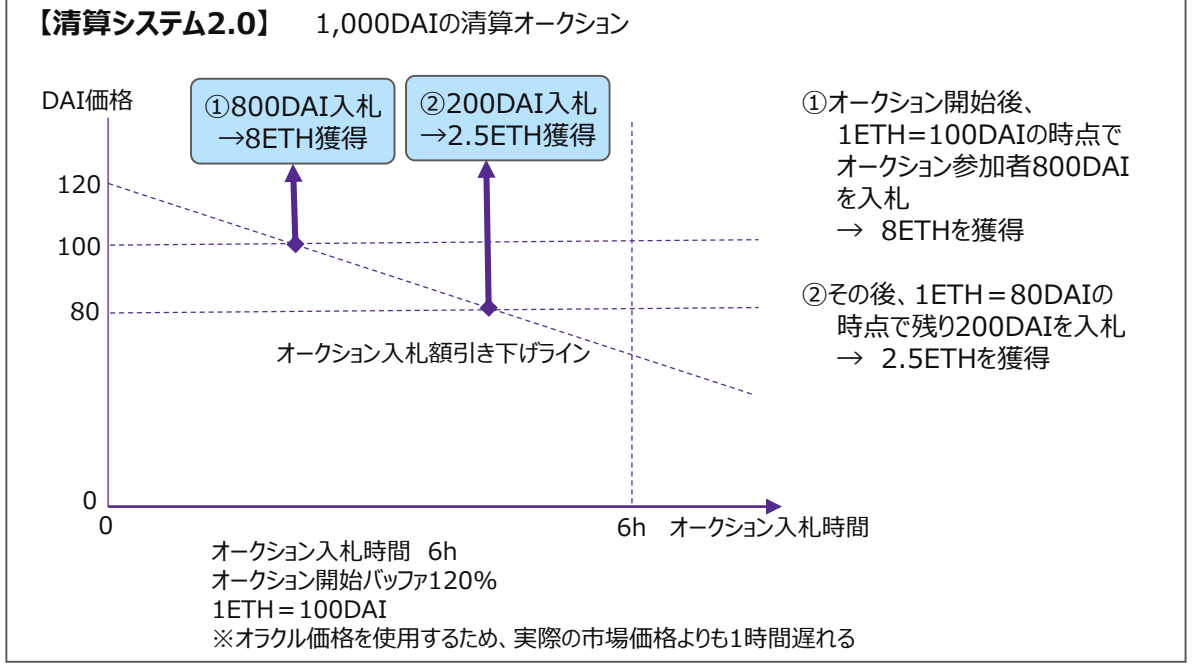
(2)DAI清算
Vaultの担保を買い取り、安定化手数料を差し引いて返却する

(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

(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

2-3 ステーブルコイン Maker（DAI）の分析

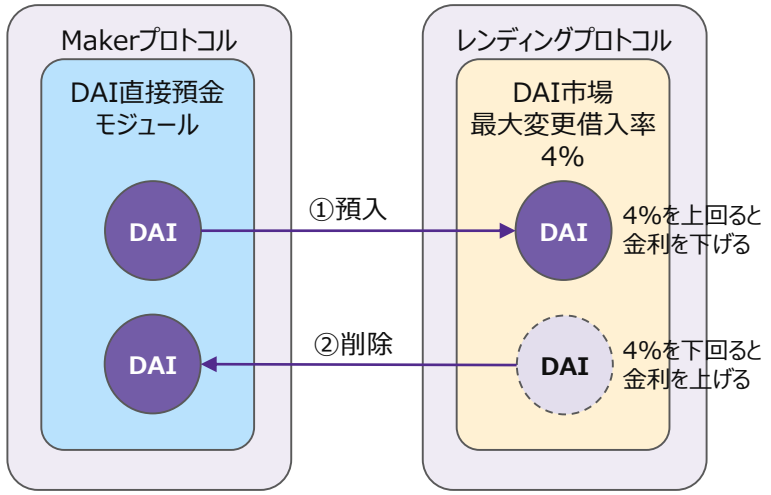
2-3-2 主な技術特性

(3) Direct Deposit DAI Module (D3M)

機能概要

- サードパーティのレンディングプロトコルと連動して、当該プロトコルの流動性プールにDAIを効率的に移転することで、DAIの変動金利がMakerガバナンス（ガバナンス投票）で決定された目標金利以下となるように調整するメカニズム
- 目標金利が確実に達成されるように、DAIを自動的に預入/引出
- Aave、Compoundに適用済。Mapleに適用検討中（投票中）（2022/3時点）

【Makerプロトコルとレンディングプロトコルの動き】



選択した資産毎に最大変動借入率（4%など）が適用される

①DAIの需要が高い場合
DAIはレンディングプロトコルを介して作成・預入される
（最大変動借入率に達するか債務上限まで継続）
→ DAIの金利を下げる

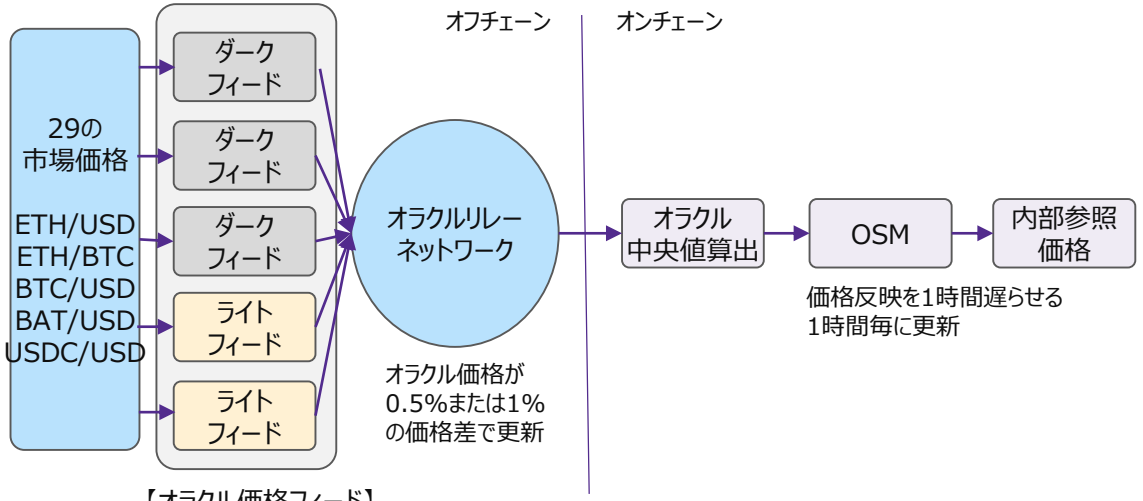
②DAIの需要が低い場合
DAIの金利を競争レベルに引きあげるため、DAIの流動性を削除する
→ DAIの金利を上げる

(4) オラクル管理

機能概要

- Makerプロトコルは、ETH/USD等の必要な市場価格について、オラクル価格フィードから受け 取る価格群（Aave, Compound, Uniswapなど外部の24の市場価格を参照 （2022/4時点））から中央値を算出し、DAI発行時や担保清算時等に必要な参照価格を決定
- オラクルセキュリティモジュール（OSM）により、価格反映を意図的に1時間遅らせることで、相場の急激な変動やオラクル攻撃への対応を行っている（例えば、担保資産価格が大幅に下落した際に、清算回避のために追加担保の差し入れ等の措置を取ることが可能）
- 参照する価格フィード先などはオンチェーン投票で選択される

【オラクル価格算出の仕組み】



【オラクル価格フィード】
・ダークフィード：匿名の個人によって実行されるBOT（2022/4現在15フィード）
・ライトフィード：公表された組織によって実行されるBOT（2022/4現在9フィード）
dYdX, KyberNetwork, Infura, Etherscanなど
・1価格あたり20フィード（定足数13フィード）の中央値を算出する

2-3 ステーブルコイン Maker（DAI）の分析

2-3-2 主な技術特性

区分	概要	補足事項
(5) Makerプロトコル オークション	• 強制清算時、Makerプロトコルは清算されたVault担保を取得し、オークションメカニズムを使用してそれを販売する ①余剰オークション DAIがMakerバッファーの上限額を超える場合、超過分のDAIを余剰としてMKRトークンを買い取り、MKRトークンの量を減らす ②債務オークション 未払いの債務がある場合にDAIが不足すると、MKRトークンを発行して入札者に売却し、DAIを確保する ③担保オークション トークン価格の下落などで担保不足の場合に、清算ペナルティを徴収して担保を強制清算する	• 内部の市場価格に応じて清算されるため、作成時点の資産は保証されない
(6) キーパー	・キーパーはアルゴリズムに従いアービトラージのために自動的に動く外部エージェント（主にBOT） ①マーケットメーカーキーパー DAIが目標価格（1USD）を上回った時にDAIを販売し、下回った時にDAIを購入する。指定された24取引所（Binance, Coinbaseなど）がキーパーを構築できる ②オークションキーパー 余剰・債務・担保オークションに参加し、入札を行う	• マーケットメーカーキーパーは、指定された取引所の市場価格を参照して自動的に取引を行う
(7) Flashmint	・1トランザクションで借入と返却（手数料を含む）を行う条件でDAIを作成できる ・担保不要でアービトラージの機会が利用できる	• 債務上限額の設定がある（ETH/DAI：150億など）
(8) DAI貯蓄率 （DSR）	・任意のDAI保有者が貯蓄により利子を獲得できる ・Oasis Saveポータル等を介してアクセスする ・DAI保有者が得る金額を決定するパラメーターは、オンチェーンガバナンスで決定する ・DAIが1USDを超えるとMKR保有者はDSRを引き下げ、1USD未満ならMKR保有者はDAIを引き上げる	

2-3 ステーブルコイン Maker（DAI）の分析

2-3-2 主な技術特性

項目	概要	補足事項
(9) GSM （Governance Security Module）	• GSMにより、ガバナンス投票による提案可決後のコード修正などの執行が一定時間待たされる • システムに加えられる変更を確認し、それらの変更が悪意があると見なされた場合は、GSM遅延時間の間に提案キャンセル（コアチームが実施すると考えられる）やEmergency Shutdown（MKR保有者が投票）による対応を行う	• GSM遅延時間は48時間（2022/1）
(10) ダークスペルメカニズム	• 重大な脆弱性の修正を行うためにスマートコントラクトを修正する仕組み • 特別な操作を使用して、ダウンタイムなしでプロトコルの修正を適用する • 修正コード適用前のオンチェーン投票やGSM遅延期間中に、リバースエンジニアリングで内容を読み取られないよう、修正反映までコードを隠蔽する 【修正プロセス】 ①ダークスペル（修正コード）をスマートコントラクトドメインチームが開発 ②コミュニティの特定者と信頼できるサードパーティにダークスペルを伝達 ③信頼できるサードパーティが迅速に議論を調整し、投票を認識 ④信頼できるサードパーティがガバナンスファシリテーターに投票を指示 ⑤投票がスケジュールされ、通過した後にGSM遅延期間を待つ ⑥GSM遅延期間経過後、コード修正を適用する ⑦信頼できるサードパーティとスマートコントラクトドメインチームが、ダークスペルの事後分析を作成し、コミュニティ全体に公表する	• 利害関係者 - スマートコントラクトドメインチーム - ガバナンスファシリテーター - 信頼できるサードパーティ （オンチェーン投票で選定。現在は登録なし） - Makerコミュニティの特定者（非公表） • 本件はガバナンス投票やエグゼクティブ投票とは異なるプロセスで行われる - 投票時間は24時間に設定（固定） - 投票の定足数や可決の閾値は定義されていない

2-3 ステーブルコイン Maker（DAI）の分析

2-3-2 主な技術特性

項目	概要	補足事項
(11) 緊急シャットダウン	• 悪意のある攻撃からMakerプロトコルを保護する、またはMakerプロトコルのアップグレードを容易にするためにプロトコルをシャットダウンする機能 • MKR保有者がMKRを緊急シャットダウンモジュール（ESM）に預け、閾値を超えると即座に実行される • 実行は3フェーズで行われ、その後、発生要因に応じて再展開が行われる ①Makerプロトコルがシャットダウン ・オラクル価格フィードが凍結され、Vault所有者が資産を引き出す ②緊急停止後のオークション処理 ・シャットダウン開始後、担保オークションによる強制清算が開始され、全てのオークションが終了するまでプロトコルの停止が待たされる ③DAI保有者が残りの担保を請求する ・DAI保有者は固定レートで直接担保を請求する ・Vault保有者がDAI保有者よりも優先される ④攻撃の内容に応じてプロトコルを再デプロイする ・ガバナンス攻撃 → 攻撃者を無効にして、他はそのままで再デプロイ ・オラクル攻撃 → オラクルモジュールを修正し、他はそのままで再デプロイする ・ブラックスワンイベント → 新しい改善を加えて再デプロイする ・不当な緊急シャットダウン → 攻撃者を無効にして他はそのままで再デプロイする	・緊急シャットダウン開始の閾値は75,000MKR（2022/1） ・ブラックスワンイベント：重大な奇襲攻撃 オラクル攻撃など高度に調整された外部からの価格操作など対策が難しく、直接の回避策がない

2-3 ステーブルコイン Maker（DAI）の分析

2-3-3 ガバナンス運営

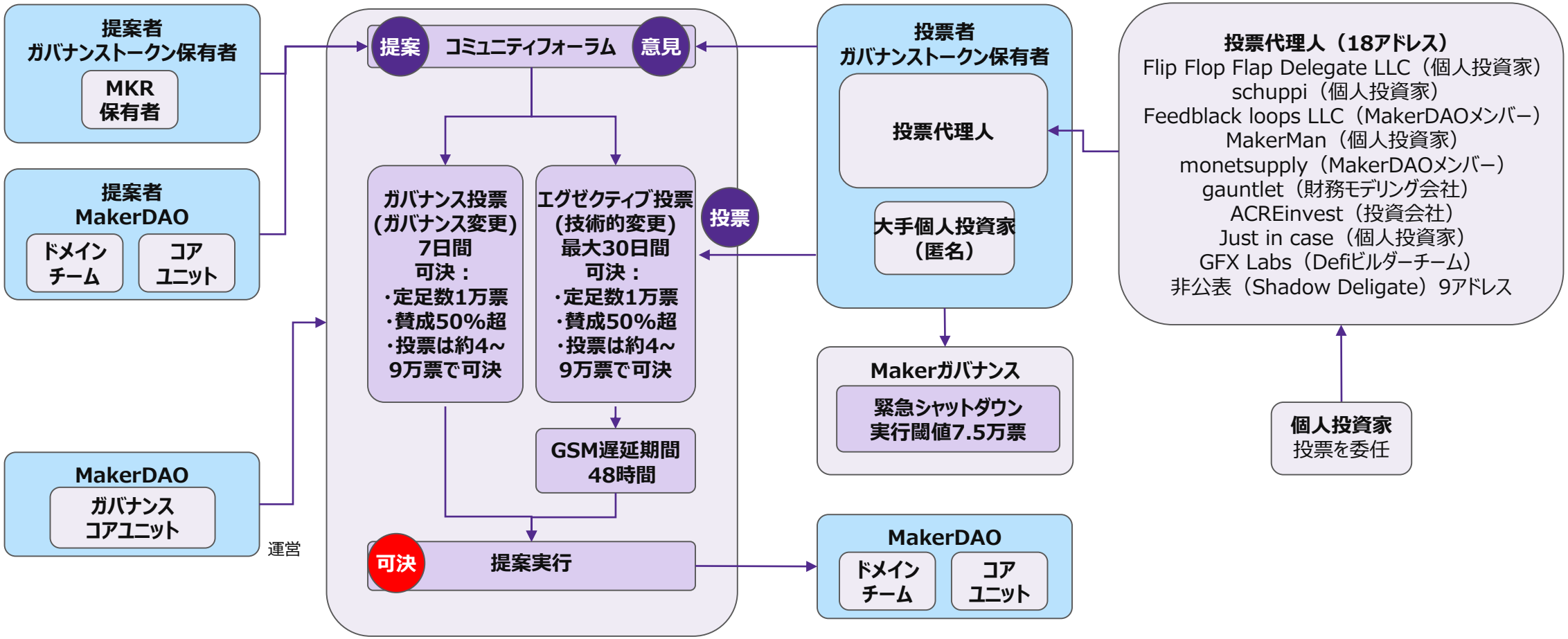
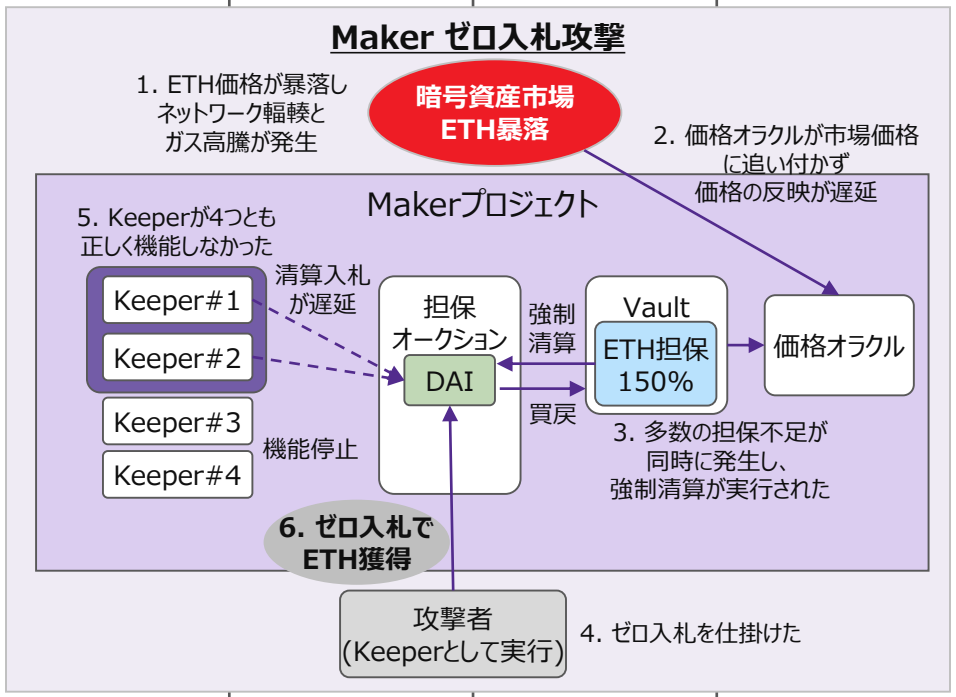


図 2-3-3 MKRを用いたガバナンス投票プロセス

2-3 ステーブルコイン Maker（DAI）の分析

2-3-4 インシデント事例

発生日	被害額	関連DeFi	関連する要素	事件の概要	発生原因
2020/3/12	約832万ドル	Maker	Ethereum Oracle DAO ステーブルコイン	ETH価格暴落によるネットワーク輻輳やガス高騰により、Makerの担保強制清算が発生した際に入札が正しく行われない弱点を攻撃され、ゼロ入札により約832万ドル相当のETHの損失が発生。 【事件の流れ】 1. Black Thursday（COVID-19や米国の渡航禁止例などによる株式市場の暴落）によりETH等の暗号資産が暴落（ETH：$194→$111に43%下落）。Ethereum上のトランザクションが急増し、ネットワークの輻輳とガス価格の急騰が発生。 2. 上記により、Makerの価格オラクルが価格を更新できず遅延。ETHの市場価格に追いつかず、価格の反映が遅延した。 3. その後、価格オラクルが一気に更新された結果、Maker内のETH価格が約20%下落。多数のVaultでDAIを借りたETHの担保不足が同時に発生し、約1,200Vaultの強制清算（担保オークション）が実行された。 4. 強制清算に対して、攻撃者が「ゼロ入札」（DAI=0でETHに交換）を仕掛けた。 5. 強制清算により、4つのキーパーが清算のためのDAI買取り入札を行うが、4つとも正しく機能せず入札ができなかった。 ・Keeper#1,#2 ガスの高騰に起因して、入札のトランザクションが制限時間（10分）以内に処理されなかった。 ・Keeper#3 Maker Foundationが運営していたが、ネットワーク輻輳により技術的な問題が発生し、機能しなかった。 ・Keeper#4 清算するためのDAIが枯渇し、処理が数時間停止した。	ETH価格暴落によるEthereumのガス高騰により、、Keeperが正しく動かないことを悪用してゼロ入札を仕掛けたことによるもの。 事件後の調査で、Ethereumのネットワーク輻輳は意味のない大量のトランザクションにより意図的に行われた可能性があり、攻撃者がガス高騰を引き起こしてKeeperが正しく動かない状態を作り上げ、ゼロ入札攻撃を行ったとの指摘もある。



2-3 ステーブルコイン Maker（DAI）の分析

2-3-4 インシデント事例

発生日	被害額	関連DeFi	関連する要素	事件の概要	発生原因
–	–	–	–	6. 攻撃者がゼロ入札を勝ち取り、合計832万ドル相当のETHを搾取した。 （Keeperや攻撃者が行ったオークション入札4,447件のうち、1,462件がゼロ入札であった） 7. 3/19にMakerプロトコルによる債務オークションを実施し、ゼロ入札による540万ドルの担保不足解消を行い、3/29時点で20,980MKRを生成して530万DAIが供給された。	–

2-3 ステーブルコイン Maker（DAI）の分析

2-3-5 Makerの主なトラストポイント

- 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

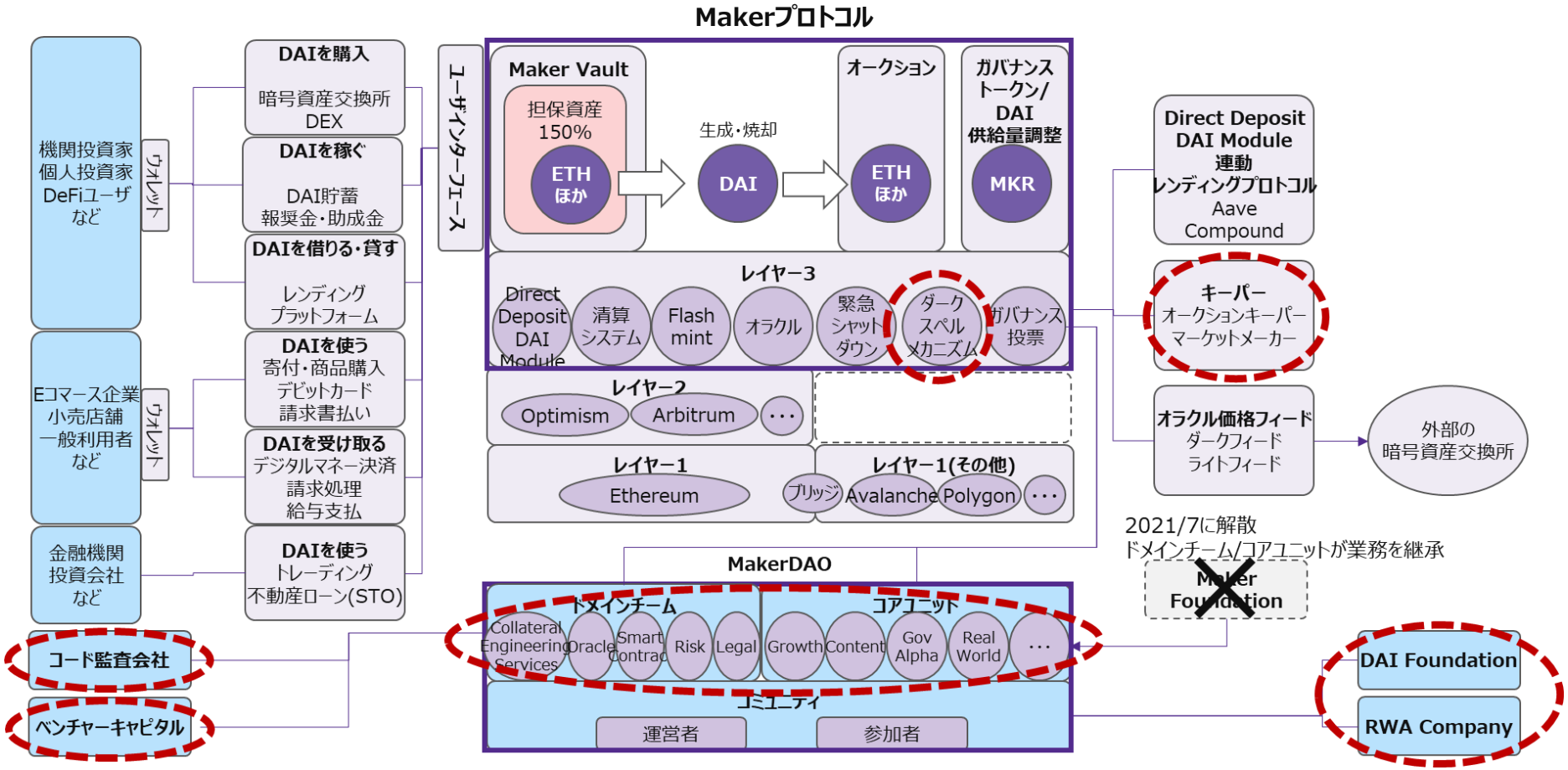


図 2-3-5-1 Makerの主なトラストポイント（構成要素）

2-3 ステーブルコイン Maker（DAI）の分析

2-3-5 Makerの主なトラストポイント

- 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

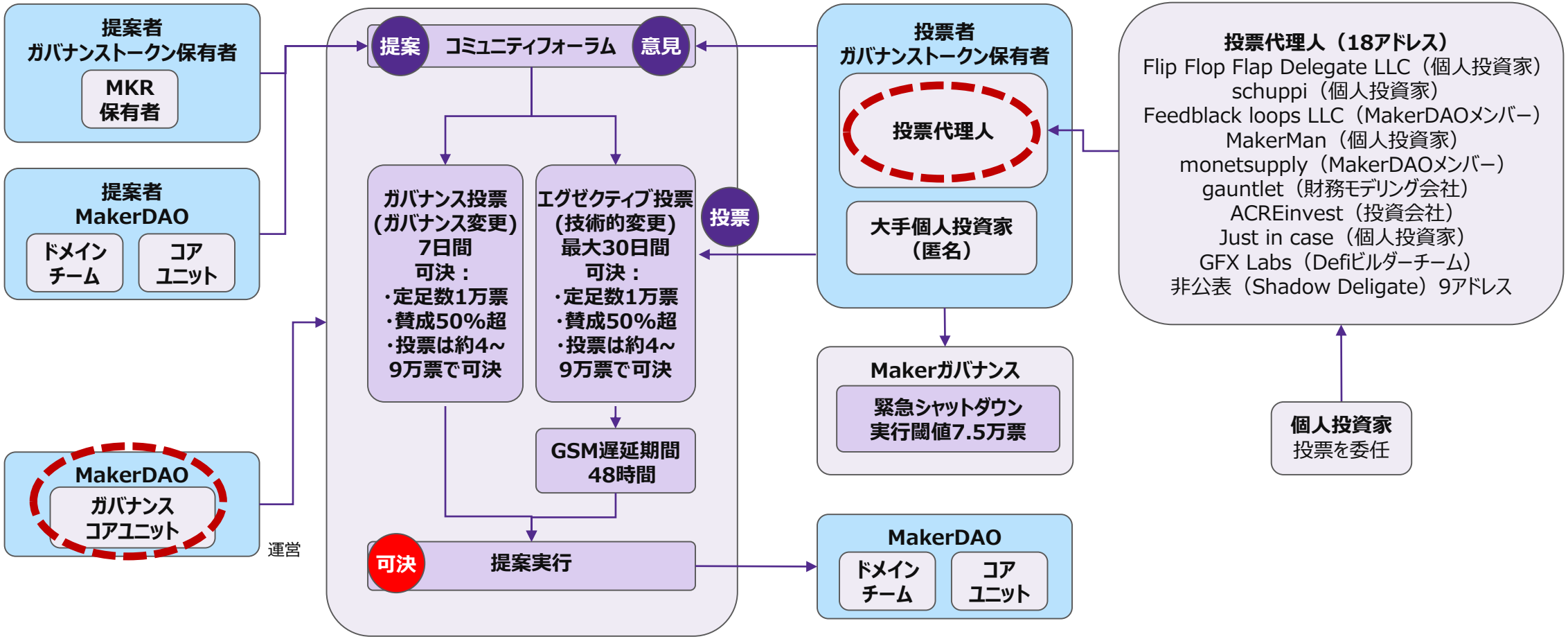


図 2-3-5-2 Makerの主なトラストポイント（ガバナンス投票）

2-4 レンディング Aaveの分析

2-4-1 プロジェクト全体概要

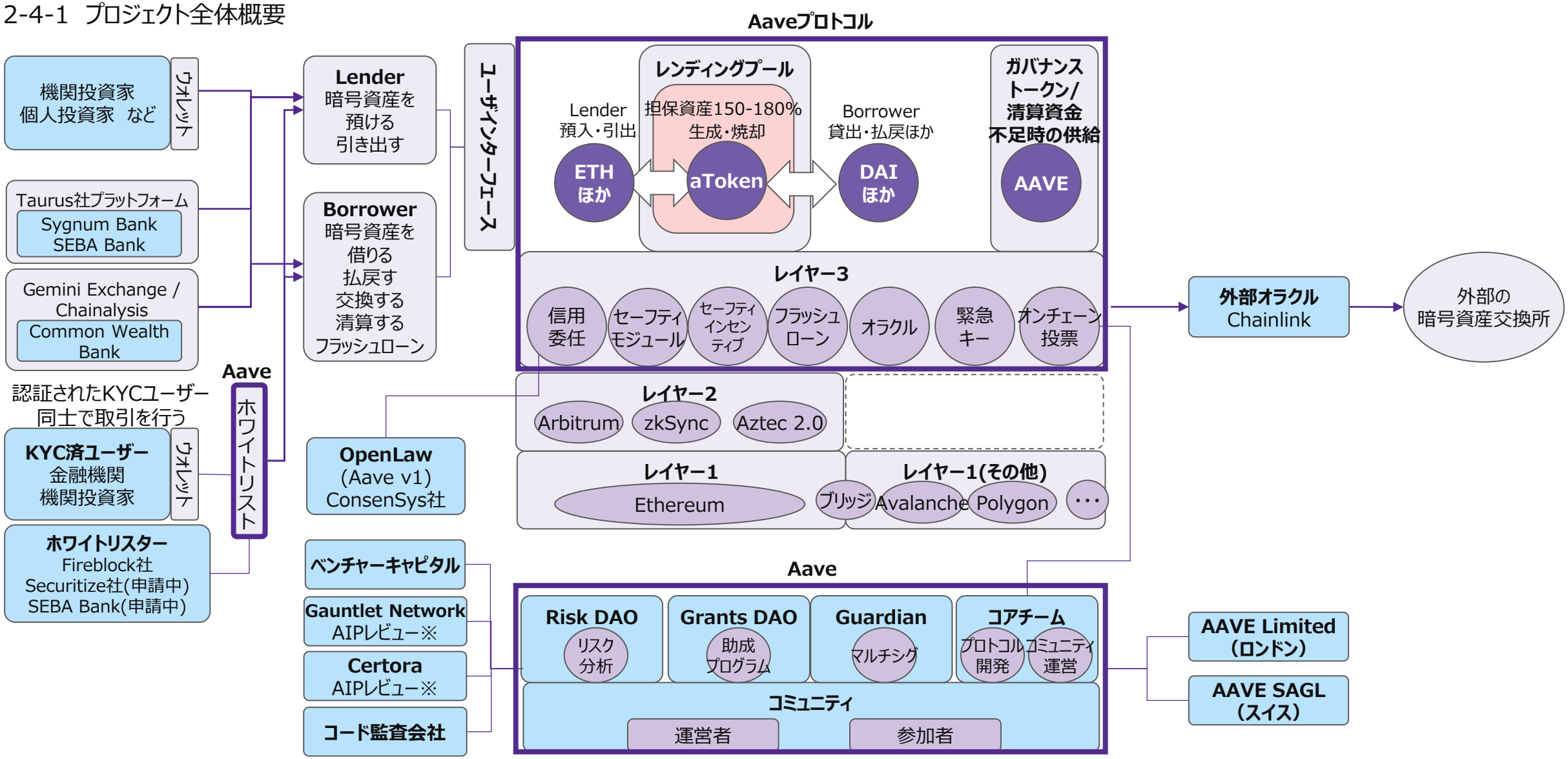
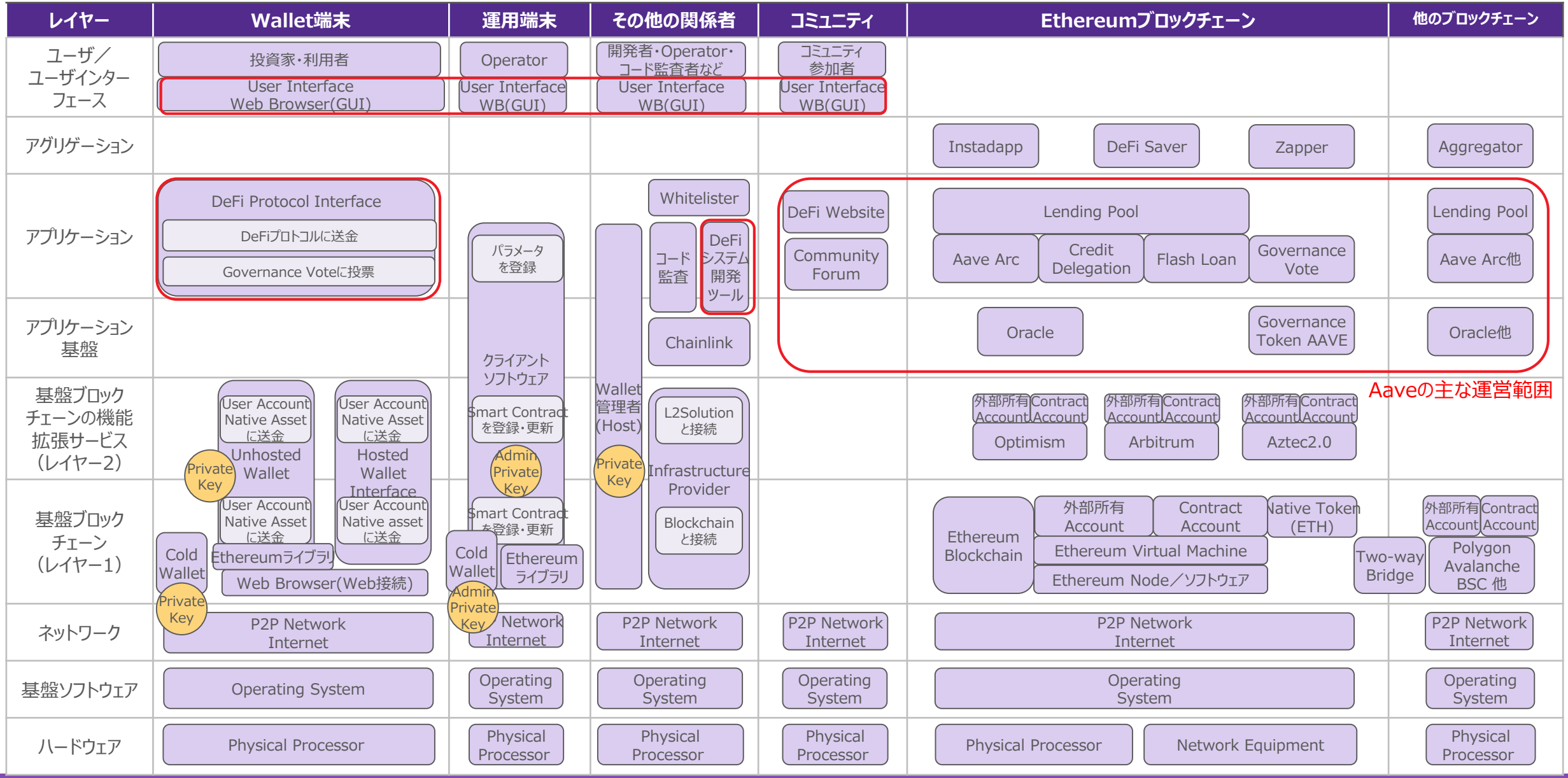


図 2-4-1-1 Aaveの主な構成要素

2-4 レンディング Aaveの分析

2-4-1 プロジェクト全体概要

図 2-4-1-2 Aaveの主な構成要素のマッピング



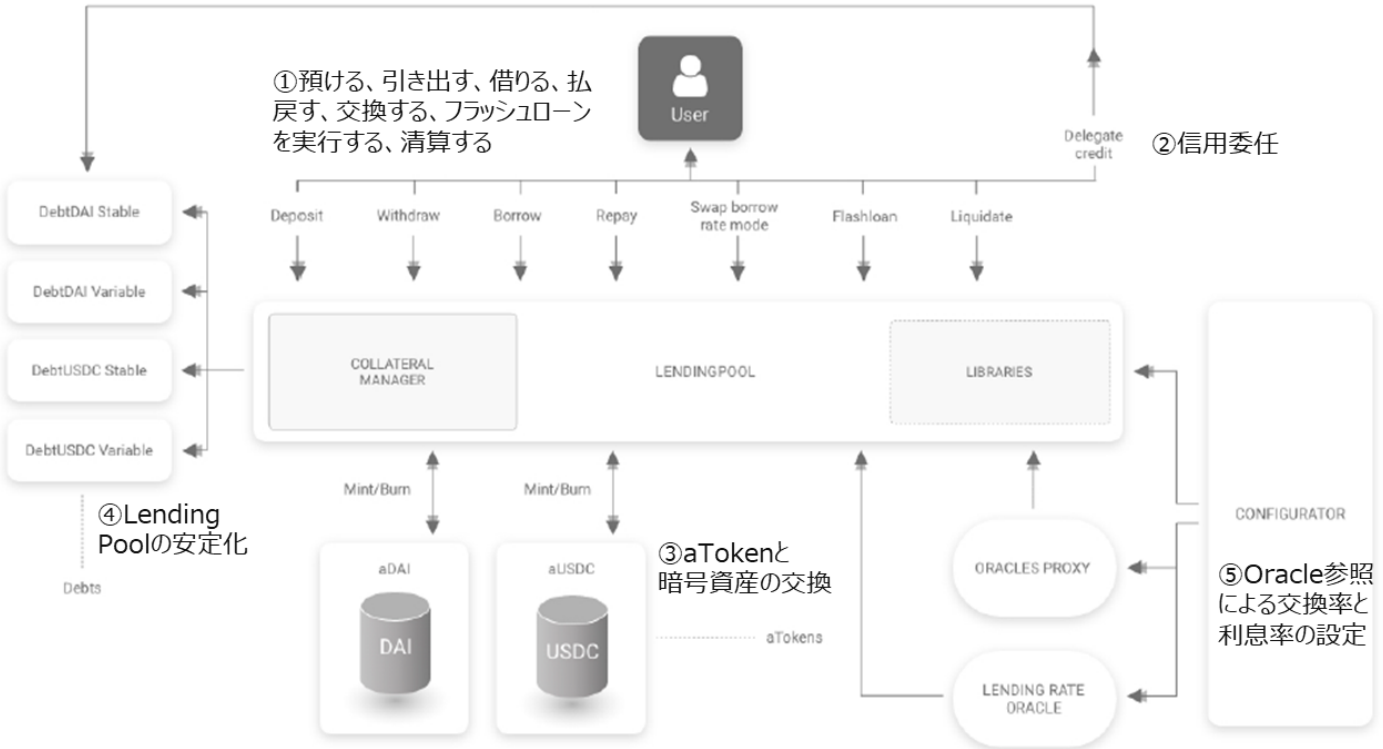
2-4 レンディング Aaveの分析

2-4-2 主な技術特性

(1) Lending機能の全体像

機能概要

- ユーザ（個人／機関投資家など）は、Aaveプロトコルのレンディングプール（スマートコン トラクト）に暗号資産（一部のステーブルコイン含む）を預け入れることで金利を獲得で き、また所定の担保資産を預け入れることを前提に同プールから借り入れを行うことができ る（2022/1時点でETH、LINK、USDT、AAVEを含む30以上の暗号資産・ステーブルコインに対応）
- レンディングプールに暗号資産を預け入れると、1:1で当該暗号資産の頭文字にaを付与した aToken （例：aETH）を受け取り、同プールが獲得した収益はaToken保有者に配分される。当 該暗号資産を引き出す際にはaTokenを焼却する
- 暗号資産価格は外部オラクル（Chainlink）を参照する 。
- 貸出・借入金利はオラクルを参照することで、システム的に算出される。
- 借入時、担保資産価格が下落した場合には清算が発生する
- 暗号資産を預け入れたユーザは、当該暗号資産を担保とする与信枠を他者に譲渡することができ、譲渡を受けた者は無担保で借り入れを行うことができる（信用委任）。信用リスクの対価として譲渡人（Delegator）は追加的な収益を得る。



2-4 レンディング Aaveの分析

2-4-2 主な技術特性

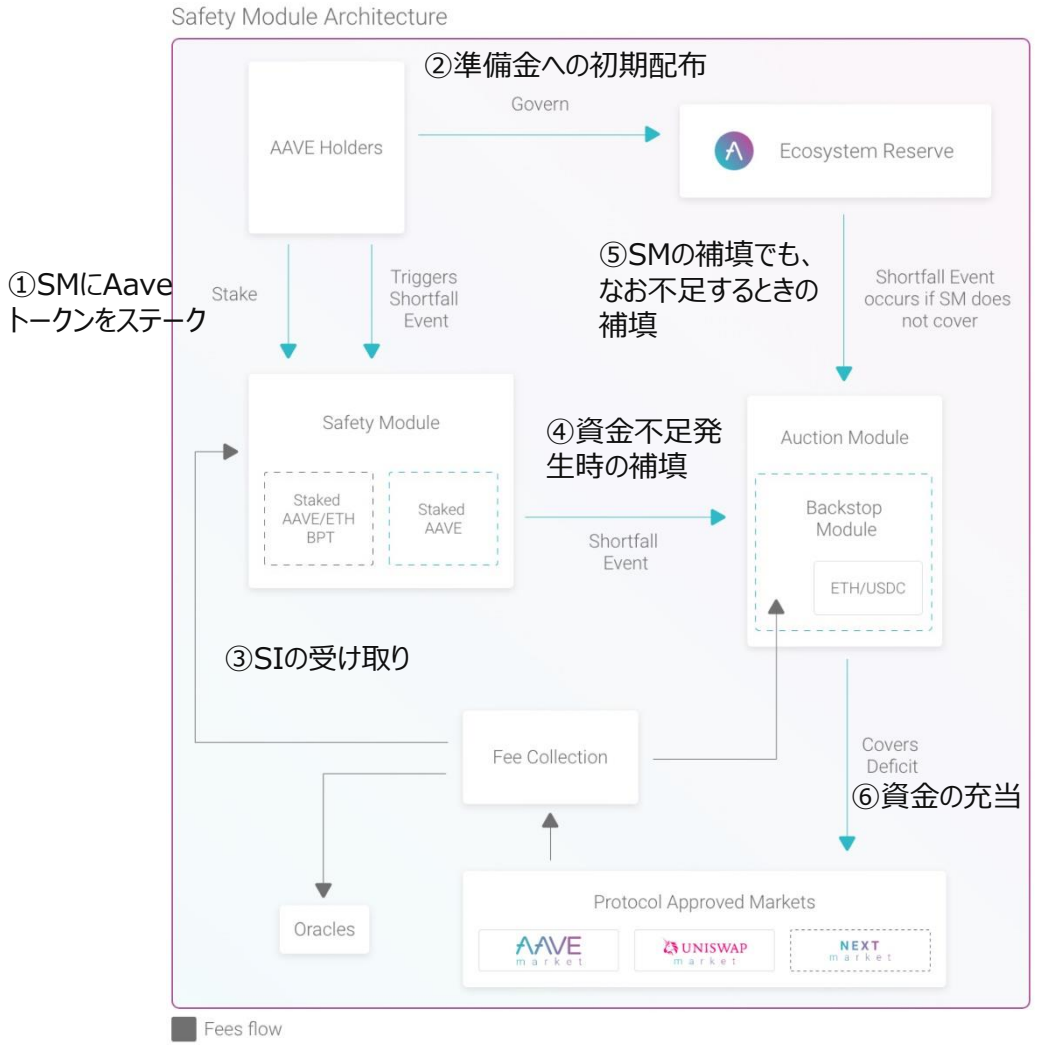
(2) Safety Module/ Safety Incentive

機能概要

- Safety Module（SM）：大量の清算発生時において、プロトコルの債務超過解消を目的としてユーザが任意でステーキングを行ったAAVEトークンから補填を行う仕組み
- Safety Insentive（SI）：SMへのステーキングを行う対価として手数料が得られる仕組み

【Safety Module/ Safety Incentiveの詳細】

手順	説明
①	AAVEトークン保有者は、SMにAAVEトークンをステーキング（ロック）する。
②	Aaveトークンは初期配布時に総発行1600万トークンのうち、ユーザーに1300万トークンを、Aaveエコシステム運用準備金に300万トークンが配布されている。
③	ステーキングを行った者に対して、AAVEの手数料収入の一部が対価として支払われる
④	大規模清算の発生等により資金不足が生じた際には、SMに預けられたAAVEトークンがオークション（Auction Module）によって売却される（ステークされたAAVEトークンの最大30%から補填される
⑤	オークション実施後もなお資金が不足した場合は、運用準備金（Ecosystem Reserve）から補填される。
⑥	Auction Moduleで売却された資金をAave Marketの資金不足解消に充当する。



2-4 レンディング Aaveの分析

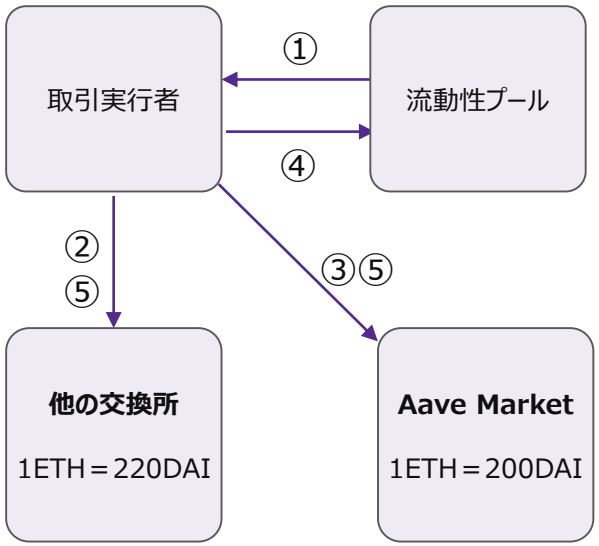
2-4-2 主な技術特性

(3) Flash Loan

機能概要

- 1トランザクション内で借入から返済まで完結させることで、事前に担保を預け入れることなく借入等を可能とする仕組み
- 主な用途として、アービトラージや、担保交換などが想定されている
- 手数料は借りたトークン建て債務の0.09%。そのほかに、デプロイとスマートコントラクトの実行にガス代が発生する。
- 流動性プールを介することで、暗号資産の需要よりも供給を潤沢に用意することで、フラッシュローンを利用した攻撃を防ぐ設計となっている

【フラッシュローンの例】



【Flash Loanの具体例（AAVEマーケットと他の取引所の間でアービトラージの機会が生じている場合を想定）】
・下記①~⑤を1トランザクションで実行する

手順	説明
①	無担保で流動性プールから1ETHを借りる。 このとき、AaveMarketでは1ETHを200DAIで交換できる状態とする。
②	交換レートに差がある他の交換所で、①で借りた1ETHを220DAIで交換取引予約する
③	AaveMarketで200DAIと1ETHの交換予約を行う。
④	1ETHと手数料0.09%の0.0009ETHを返却する。
⑤	交換取引予約を実行する。結果として、19.82DAI(20DAI-0.0009ETH(0.18DAI))相当の利益を獲得する。 （実際にはこれにガス代が引かれる）

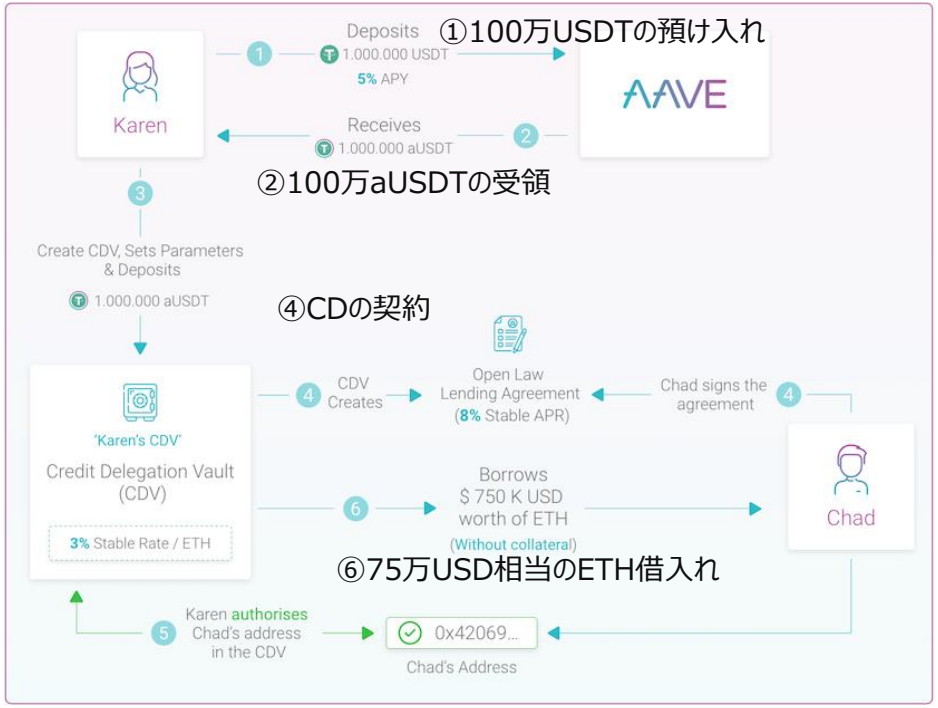
2-4 レンディング Aaveの分析

2-4-2 主な技術特性

(4) 信用委任（Credit Delegation）

機能概要	• 信用委託とは、Aaveに暗号資産を預けた人が、その暗号資産を担保とする与信枠を他者に譲 渡することで、さらに追加利回りを享受できる仕組みをいう。 • 貸手・借手の間で利率や期限について合意し、契約を締結する。現在は担保資産毎に譲渡先 を１人指定できるが、今後は複数人への譲渡機能を検討予定。 【信用委任の具体例】 • 例では、カレンがチャドの代わりに担保を差し入れることで、チャドが暗号資産 を借りることを可能にしている。 • カレン・チャド間の契約締結時において、V1では両者のオフチェーンでの合意に基づきOpenLaw※というスマートコントラクトを内包する電子契約サービスを活用して契約の強制力を持たせる仕組みを取り入れている。V2では、電子契約機能をAave自体に取り入れている。 ※OpenLaw：ConsenSys社が提供するブロックチェーンを用いた電子契約サービス

【信用委任の例】



手順	説明
①②	カレンはAaveのレンディングプールに100万USDTを預け入れ、100万aUSDTを取得する。
③	カレンはCDV（Credit Delegation Vault）に100万aUSDTを預け入れることで、3%の固定金利でETHを獲得する。
④	無担保での借入を希望するチャドとカレンの間で、与信額・金利（図では年利8%）等の借入条件について合意し、契約を締結する（AaveV1ではOpenLawにより信用委任契約に署名）
⑤	契約締結後、カレンは契約に従ってチャドの与信額を設定する
⑥	チャドは当該与信額の範囲で借入れを行う（図では75万USD相当のETHを借入れ）。信用委任によって、カレンはより高い利回りを獲得でき、チャドは担保なしで資金を調達できている。

2-4 レンディング Aaveの分析

2-4-2 主な技術特性

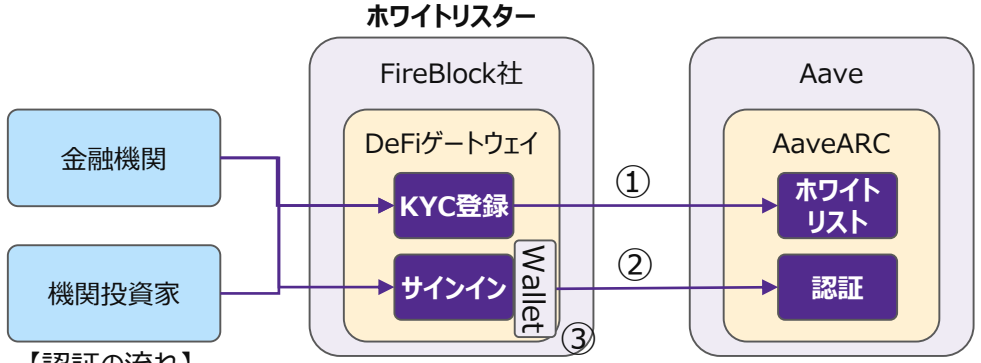
(5) AaveArc / ホワイトリスター

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）

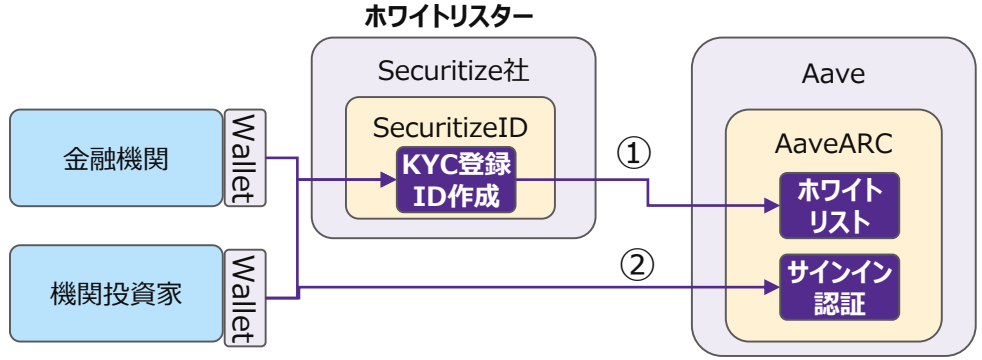
【FireBlock社 DeFiゲートウェイ】



【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

2-4 レンディング Aaveの分析

2-4-3 ガバナンス運営

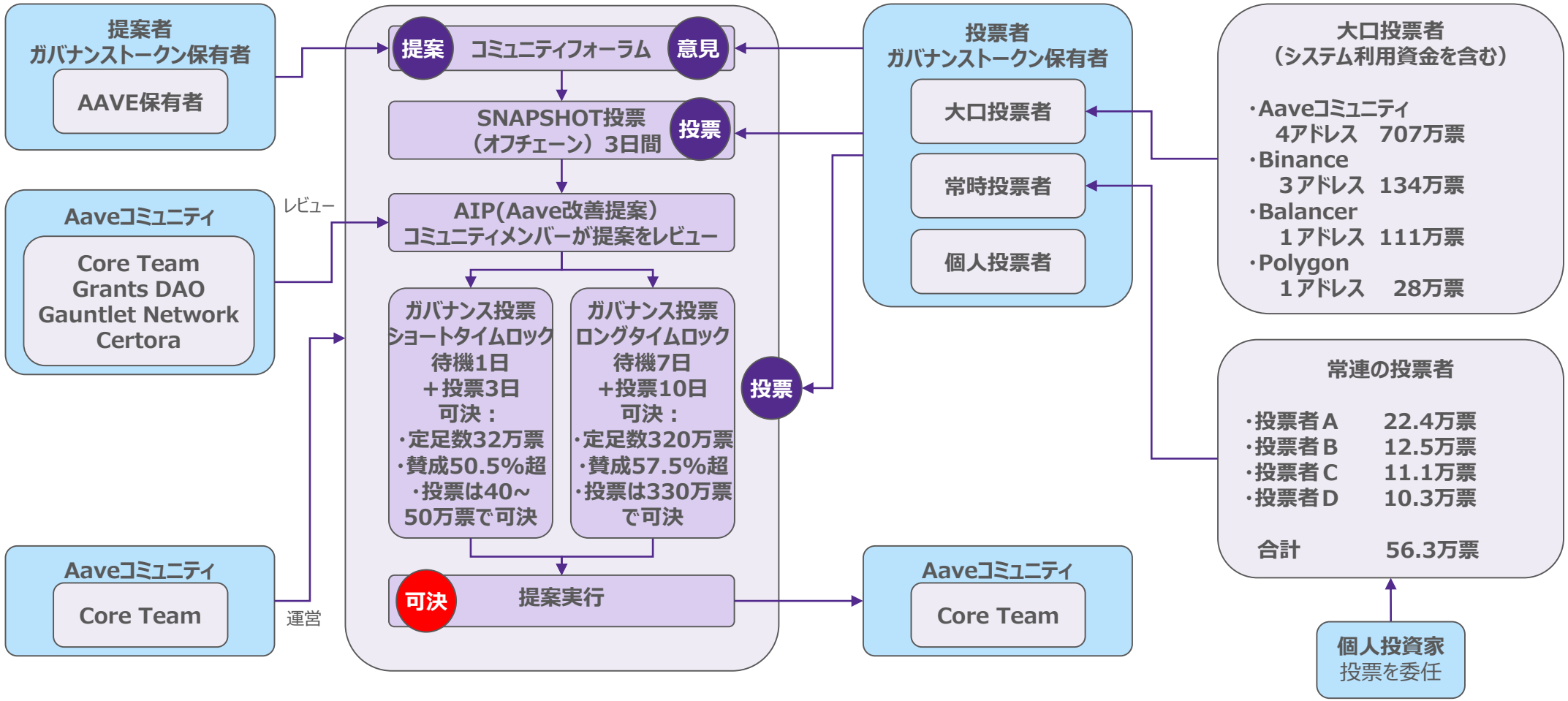


図 2-4-3 AAVEを用いたガバナンス投票プロセス

2-4 レンディング Aaveの分析

2-4-4 AAVEの主なトラストポイント

- 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

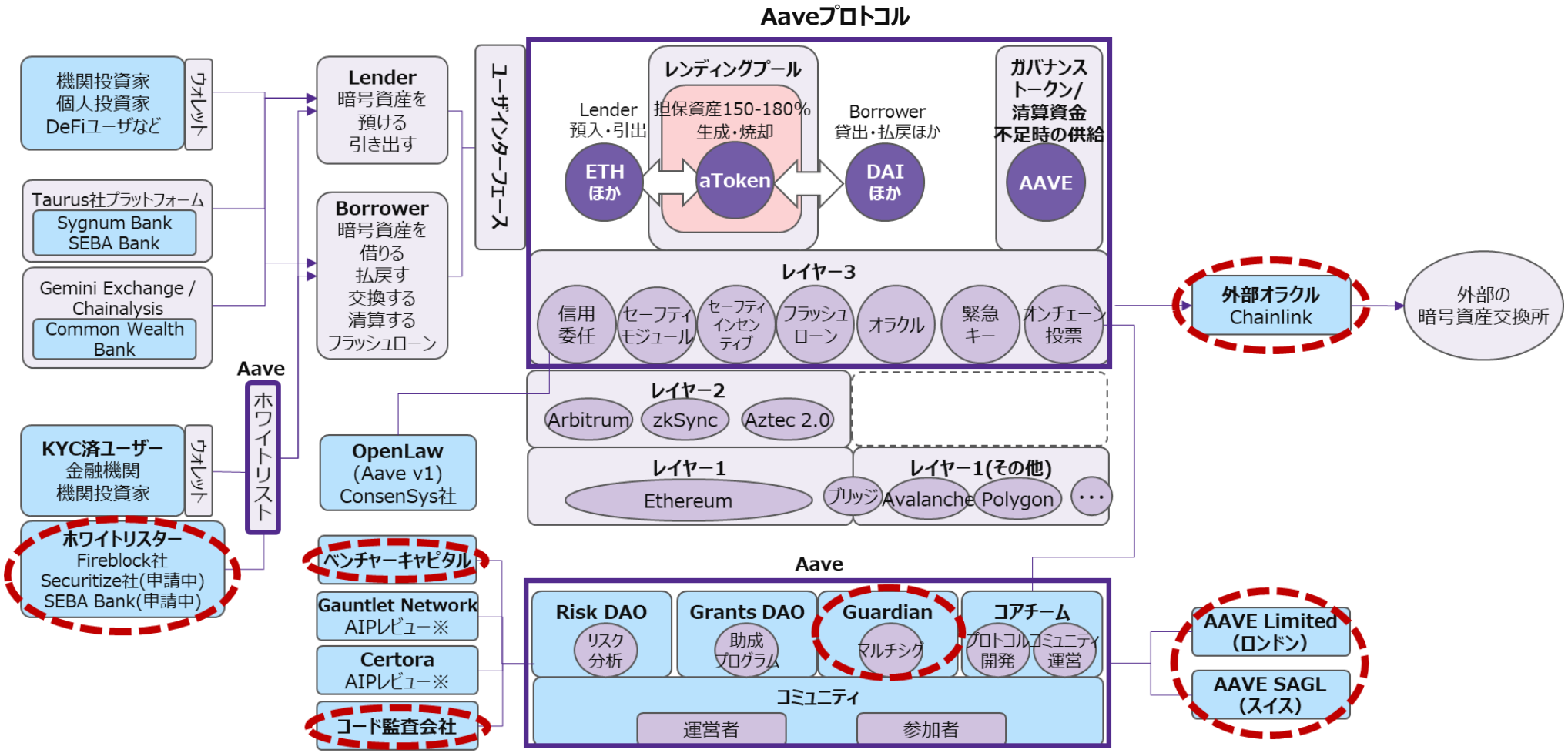


図 2-4-4-1 Aaveの主なトラストポイント（構成要素）

2-4 レンディング Aaveの分析

2-4-4 AAVEの主なトラストポイント

- 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

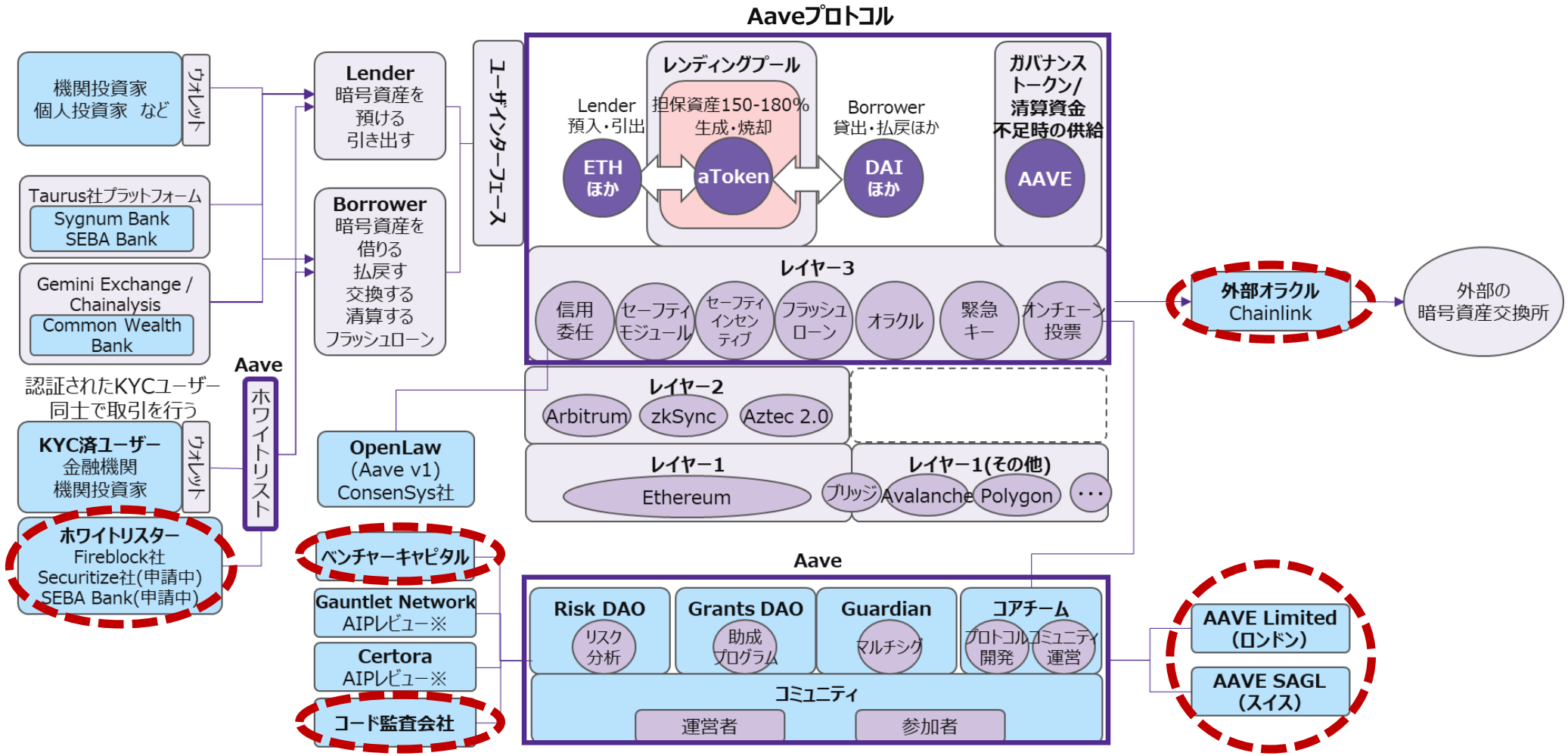


図 2-4-4-1 Aaveの主なトラストポイント（構成要素）

2-4 レンディング Aaveの分析

2-4-4 AAVEの主なトラストポイント

- 大口投票者や常時投票者等の一部のガバナンストークン保有者が大きな影響力を有すると考えられる。
- DAOのコアチームや協力会社がAIPのレビューを行い、品質を担保している。

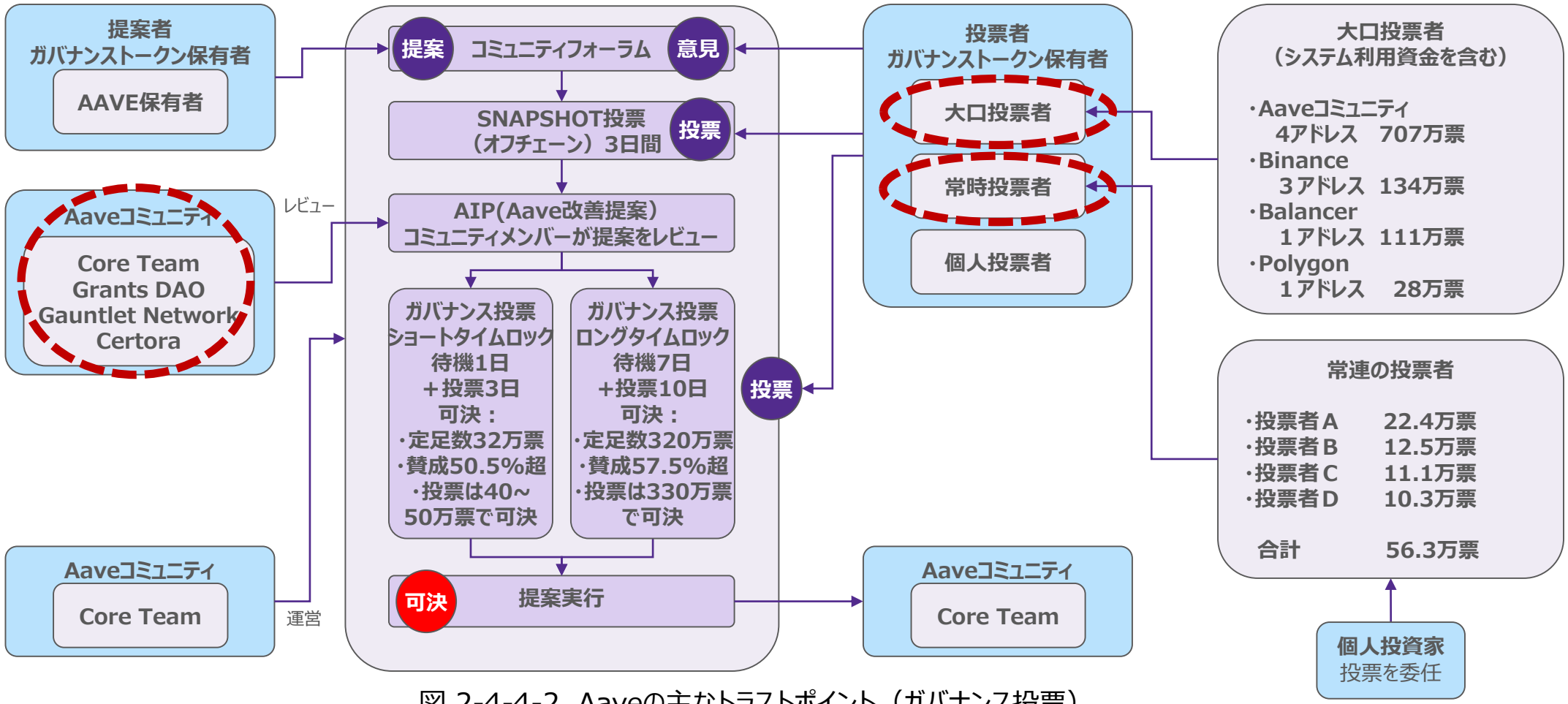
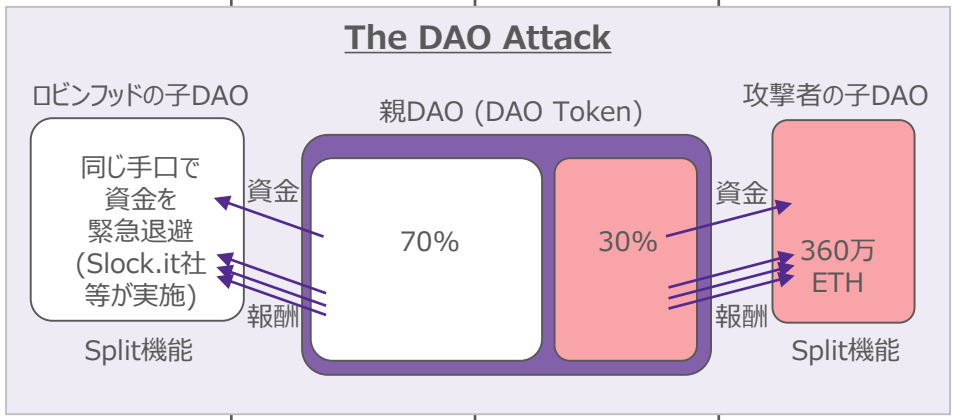


図 2-4-4-2 Aaveの主なトラストポイント（ガバナンス投票）

2-5 他のDeFiプロジェクトの主なインシデント事例分析結果

2-5-1 The DAO Attack

発生日	被害額	関連Defi	関連する要素	事件の概要	発生原因
2016/6/17	ハードフォークにより被害なし 一時的に搾取された被害額は約7,000万ドル(360万ETH)	The DAO ※1	DAO Token ※2 Ethereum ETH ※3	攻撃者は、The DAOの報酬送金機能の脆弱性を利用して、親DAOに紐づく自身の子DAO（自分専用の資金の払出用アドレス）に大量の報酬を送金して360万ETHを獲得した。但し、子DAOの資金は27日間移動できない仕様であったため、その前にEthereumのハードフォーク（取引の無効化）を行うことで被害を回避した。 【事件の流れ】 1. The DAO のSplit機能 を利用し、親DAOから独立した自身の子DAOを作成。 2. Split機能の脆弱性を悪用し、親DAOから子DAOへの資金移動に伴う親DAOの残高が更新される前に、報酬の送金を自動的に繰り返すスマートコントラクトを埋め込み、自身の保有分以上の 資金を子DAOに何度も送金して合計360万ETHを獲得した。 3. 緊急対策として防御者が「RobinHoodGroup」を立ち上げ、攻撃者と同じ手法により、全体の70%の資金を退避した。（攻撃者よりも多い報酬を得るように工夫して資金を素早く退避した） 4. Split機能を使った子DAOにある資金は、27日間は移動ができないという制約があったため、攻撃者は360万ETHの資金を子DAOから移転させることはできなかった。 5. 事件の解決策として以下 3 案が検討され、③ハードフォーク が実行された。 ①フォークを行わず、資金を攻撃者に明け渡す ②ソフトフォークを行い攻撃者のアカウントを凍結 ③ハードフォークを行い取引自体をなかったことにする 6. ハードフォークの反対派がEthereumの内部で分裂し、元の取引記録を維持したEthereum Classicが誕生した。	(1)現象的要因 ①リエントランシー脆弱性 TheDAOのスマートコントラクトがリエントランシーの可能性を考慮しておらず、資金と報酬を送金した後に内部トークン残高を更新していた ②動いているスマートコントラクトをアップデートする仕組みが欠けていた (2)動機的要因 Slock.it社が上記②の認識に欠けており、攻撃される前に修正コードのデプロイに至らなかった



※1 The DAO：Slock.it社（ドイツ）が設立した自律分散投資ファンド
※2 DAO Token：The DAOの暗号資産
※3 ETH：Ethereumの暗号資産名
※4 Split機能：投資の提案に反対するユーザーがその投資に対する自分の資金を受け取ることができるよう、自分の資金を親DAOから切り離し、子DAOに分割できる機能。
Split機能による子DAO作成には、キュレーターの承認およびDAO投票（1週間）による承認が必要。
※5 ソフトフォーク：旧バージョンにルールを新たに追加することによって発生するブロックチェーンの仕様の分岐。前方互換性を保証し、フォーク以降のブロックの後方互換性を必ずしも保証しない。
※6 ハードフォーク：前方互換性と、フォーク以降の後方互換性を保証しないアップデート。ルールを書き換えるため、永続的な分岐となる

2-5 他のDeFiプロジェクトの主なインシデント事例分析結果

2-5-1 The DAO Attack

■事件発生の経緯（1/2）

日付	イベント	内容	補足
2015/11	DAOの提案	ドイツ企業 Slock.it UG が立ち上げた投資ファンド組織The DAOが、「クラウドファンディング」と称して仮想通貨ETHとの交換によってDAOトークンを発行することを表明した	ロンドンで開催されたEthereum Developer Conferenceで、Slock.it社CEOのChristoph Jentzschは、DAOの提案を「営利目的のDAO」として説明した
2016/4/29	The DAOコードのデプロイ	Slock.it社は、EthereumブロックチェーンにDAOコードをデプロイした	－
2016/4/30 ～ 2016/5/28	DAOトークンの提供・販売	DAOトークンの提供および販売を開始した 提供期間中、DAOは合計約1,200万ETHと引き換えに約11.5億DAOトークンを販売した（当時の評価額は約1億5,000万ドルと評価）	トークンの価格は、提供期間中にトークンを購入した時期に応じて、100DAOトークンあたり約1～1.5ETHの範囲で変動した （注）DAOトークンは有価証券であるため、本来はDAOトークンの提供と販売を登録する必要があったと米SECが2017年7月の報告書において指摘
2016/5/26	The DAOコード脆弱性の表面化とセキュリティ提案	スマートコントラクトのコードに欠陥があることをGitHubのユーザが発見 このユーザは、Ethereum開発者とBitcoin Foundation創設者のPeter Vessenesに通知した これらの懸念に応えて、Slock.it社はThe DAOのコードの特定の更新の開発とセキュリティ専門家の任命を求める「DAOセキュリティ提案」を公表した	Slock.it社は当初、「DAOセキュリティ」グループの結成、「バグ報奨金プログラム」の設立、DAOのコードに対する定期的な外部監査などを含む、より広範なセキュリティ提案を行っていたが、この提案にかかる費用（125,000ETH：The DAOの資金から支払われる）が即座に高すぎると批判され、Slock.itは提案を修正して提出することにした
2016/6/3	DAO提案の一時停止提案	Slock.it社CEOのChristoph Jentzschが、Slock.it社を代表して、DAOのコードの脆弱性を修正するための変更が実装されるまで、すべての投資提案を一時停止することを提言した	－
2016/6/12	DAO脆弱性の公表	The DAOのスマートコントラクトに脆弱性があることをSlock.it社が発表した 同日にGitHubにコードのアップデートがあった	Slock.it社はThe DAOの脆弱性の回避策が作成され、もはや脆弱性のリスクにさらされているDAOファンドはないと述べた 但し、回避策のコードは開発されたがデプロイされなかった
2016/6/17	DAO事件発生	攻撃者が約360万ETH（DAOオファリングによって調達されたETHの30%）を窃取	窃取されたETHは攻撃者が制御するアドレスに保持されたが、攻撃者はDAOのコードによって、27日間はETHをそのアドレスから移動できなかった

2-5 他のDeFiプロジェクトの主なインシデント事例分析結果

2-5-1 The DAO Attack

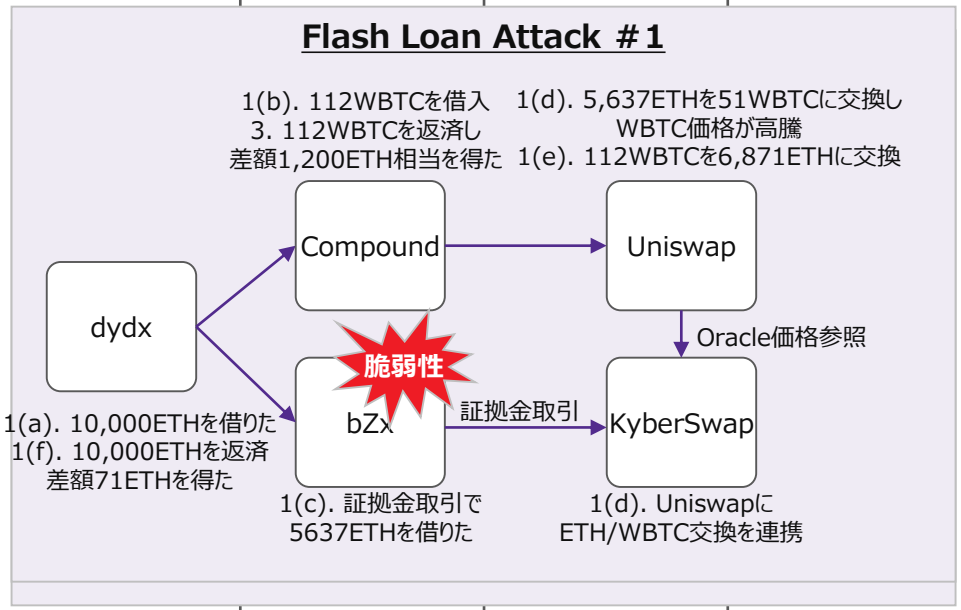
■事件発生の経緯（2/2）

日付	イベント	内容	補足
–	DAO資金の流出防止	スマートコントラクトを更新する迅速な解決策がなかったため、The DAOの利害関係者は「RobinHoodGroup」を構成。コミュニティや投資家から6万ドルのDAOトークンを寄付で集め、攻撃者と同じ手口を使って資金の70%を回収した	「RobinHoodGroup」の主要メンバー Slock.it社コミュニティマネージャー　Griff Green Ethereum開発者　Alex Van de Sander Slock.it社CEO　Christoph Jentzch　など
2016/6/28 ～ 2016/7/15	解決策の検討	窃取された360万ETHについて、解決策として以下の3案が議論された 1. 何もしない 　攻撃者は360万ETHを獲得する 2. ソフトフォーク 　攻撃者の子DAOを凍結し、移転できないようにする。但し、360万ETHは投資家に戻らず、投資家の損失となる 3. ハードフォーク 　窃取された360万ETHを含む全ての投資家の資金をThe DAOから回復用アドレスに移すことで、投資家の損失を回避する	・ハードフォークは、Ethereum Foundationが提案した緊急計画であり、取引の巻き戻しは不可能であるべきというブロックチェーンの理念に反する提案であるとして、コミュニティ内で大きな議論となった ・ハードフォーク賛成派の意見 　人間が社会的なコンセンサスを通じて最終的な判断を下すべき。 　攻撃者が利益を得ることは倫理的に間違っておりコミュニティの介入が必要。 　ETHを攻撃者の手に残しておくと将来的にその価値が下がる可能性がある。 ・ハードフォーク反対派の意見 　取引の巻き戻しが「Code is Law」「信頼性」「不変性」というブロックチェーンの理念に反している。 　Ethereumブロックチェーンの本来の目的を損ない、コードベースのルールが人間の利益に左右されてしまう。
2016/6/24	ソフトフォークの検討～断念	Ethereum Foundationとコミュニティは、当初はソフトフォークによる解決を目指したが、ソフトフォークのコードにDoS攻撃を可能にする欠陥が見つかり、ソフトフォークを実施しないことを決定した	
2016/7/15	ハードフォークの決定	投票プラットフォームに少額のETHを送る形式でハードフォーク案の投票が行われ、可決された	
2016/7/20	ハードフォークの実施	Ethereumブロックチェーンのノードの大部分が必要なソフトウェアアップデートを採用した後、新しいフォークされた新たなEthereumブロックチェーンがアクティブになった	
2016/7/20	Ethereum Classicの誕生	ハードフォークの数時間後に、ハードフォーク反対派が元のブロックチェーンの採掘を再開し、Ethereum Classicが誕生した	–

2-5 他のDeFiプロジェクトの主なインシデント事例分析結果

2-5-2 Flash Loan Attack #1

発生日	被害額	関連DeFi	関連する要素	事件の概要	発生原因
2020/2/15	約35万ドル (1,271ETH)	dYdX ※1 Compound ※2 bZx ※3 KyberSwap ※4 Uniswap ※5	Flash Loan ※6 Oracle ※7 ETH※8	bZxの証拠金取引スマートコントラクトの脆弱性を攻撃して、ETHの大量交換により故意にWBTC価格を高騰させ、アービトラージにより1,271ETHを窃取した。 【事件の流れ】 1. Flash Loanにより以下(a)-(f)を1トランザクションで連続実行した。 a) dYdXから、Flash Loanで10,000ETHを借りた。 （Flash Loan機能を提供している主なDeFi：Aave、dYdX、Equalizerなど） b) Compoundから、5,500ETHを担保として112WBTCを借りた。 c) bZxから、1,300ETHを担保として証拠金取引で5,637ETHを借りた。 （約4.3倍のレバレッジ） d) bZxで借りた5,637ETHを、KyberSwapで51WBTCに交換した。KyberSwapは、提携する複数の分散型交換所のうちUniswapでETHをWBTCに交換した。ETHを大量に交換したことによりUniswapのWBTC価格が通常時の約3倍に高騰した。 （Uniswapの交換レート：通常時の38ETH/WBTC → 約3倍の109ETH/WBTCに高騰） e) UniswapのWBTC価格が高騰したところを狙って、Uniswapで Compoundから借りていた112WBTCをETHに交換し、6,871ETHを得た。 f) dYdXで、Flash Loanで借りていた10,000ETHを返済し、差額として利益71ETHを得た。（利益 71ETH＝交換した6871ETH＋未使用の4,200ETH－返済した10,000ETH） 2. その後、WBTC価格が通常時に戻り、38ETH/WBTCになった。 3. Compoundで借りていた112WBTCを返済し、4,300ETHで清算。担保との差額として利益1,200ETH相当のWBTCを得た。	・bZxの証拠金取引スマートコントラクトの脆弱性を突かれた攻撃のため。 bZx証拠金取引機能を利用して大量のETHをWBTCに交換し、WBTC価格が高騰（ETH価格が下落）していたにも関わらずETHの担保不足でポジション清算がされない脆弱性により、故意にWBTC価格を高騰させてアービトラージで差額を窃取された。

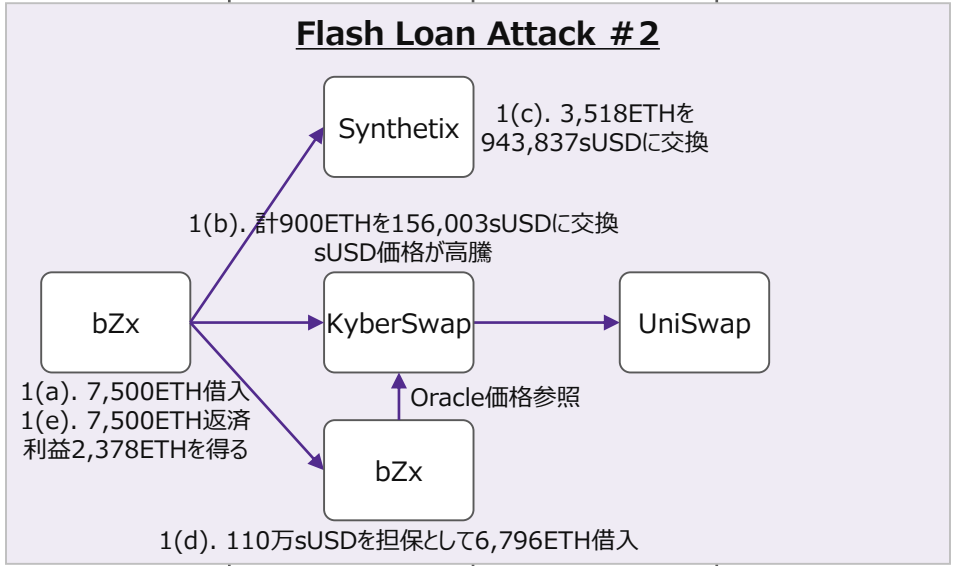


※1 dYdx：DEXアプリケーション
※2 Compound：レンディングアプリケーション
※3 bZx：トレーディングとレンディングアプリケーション　レンディング市場23位
※4 KyberSwap：DEXアプリケーション
※5 Uniswap：DEXアプリケーション
※6 Flash Loan：Ethereumの1ブロック生成時間内(約15秒)にKYCなく、無担保・格安手数料で借入・返済するローンの仕組み
※7 Oracle：ブロックチェーンの外に存在するデータや出来事（暗号資産価格など）をブロックチェーンの内部に伝えるブリッジの役割
※8：ETH：Ethereumの暗号資産名
※9 WBTC：Ethereum上でBitcoinと連動するステーブルコイン
※10 利益71ETH：6871.4+(10,000-5,500-1.300)-10,000=71

2-5 他のDeFiプロジェクトの主なインシデント事例分析結果

2-5-3 Flash Loan Attack #2

発生日	被害額	関連DeFi	関連する要素	事件の概要	発生原因
2020/2/18	63.3万ドル (2,378ETH)	bZx ※1 KyberSwap ※2 Synthetix ※3	Flash Loan ※4 Oracle ※5 ETH ※6	bZxのOracle脆弱性を攻撃して、ETHの大量交換により故意にsUSD 価格を高騰させ、アービトラージにより2,378ETHを窃取した。 【事件の流れ】 1. Flash Loanにより以下(a)-(e)を1トランザクションで連続実行した。 a) bZxから、7,500ETHをFlash Loanで借りた。 b) KyberSwapで、540ETHを92,419sUSDに交換。続けて360ETHを63,584sUSDに交換。(合計900ETHを156,003sUSDに交換) KyberSwapは、提携する複数の分散型交換所のうちUniswapでETHをsUSDに交換した。これにより、KyberSwapのsUSD価格が約3倍に高騰した。（KyberSwapの交換レート：通常時の0.00372ETH/sUSD → 約3倍の0.00899ETH/sUSDに高騰） c) Synthetix で、6,000ETHをsUSDに交換。sUSD不足のため、3,518ETHを943,837sUSDを交換し、2,482ETHが払戻しとなった。（交換レート：通常時の0.00372ETH/sUSD） d) bZxから、110万sUSDを担保に6,796ETHを借りた。通常時のsUSD価格では約4,000ETHが借入限度となるところ、bZxがKyberSwapをOracle参照しているため、sUSDの高騰により6,796ETHを借りることができた。（攻撃者は借りた状態のまま返済せずに放置） e) bZxに借りた7,500ETHを返済し、利益2,378ETHを得た。（利益2,378ETH＝借りた6,796ETH＋未使用の3,082ETH－返済した7,500ETH）	bZxがOracle価格参照をKyberSwapに依存していたことにより、kyberSwapでsUSD価格を故意に高騰させ、通常価格との相違が大きくなったところをアービトラージにより差額を窃取された。

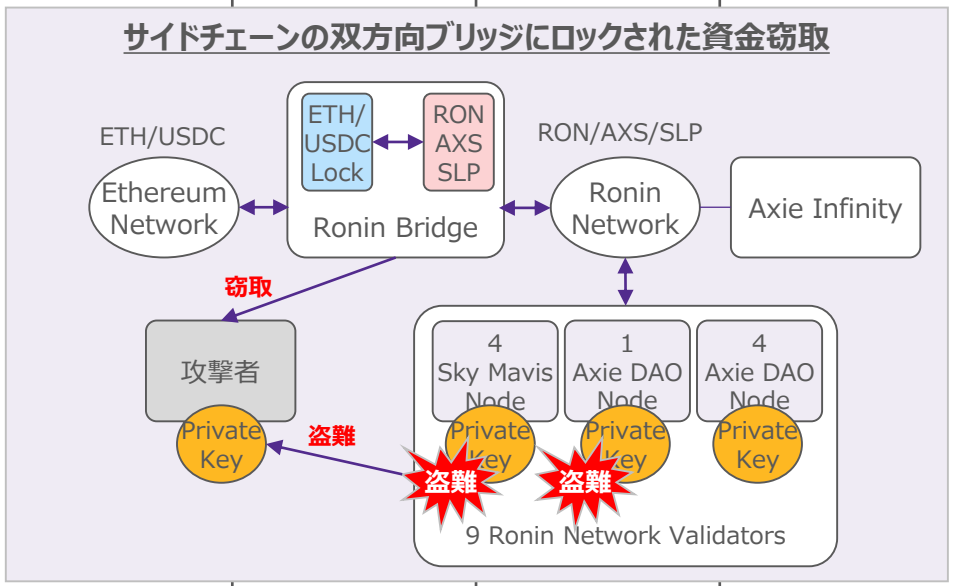


※1 bZx：トレーディングとレンディングアプリケーション
※2 KyberSwap：DEXアプリケーション
※5 Synthetix：DEXアプリケーション
※4 Flash Loan：Ethereumの1ブロック生成時間内(約15秒)にKYCなく、無担保・格安手数料で借入・返済するローンの仕組み
※5 Oracle：ブロックチェーンの外に存在するデータや出来事（暗号資産価格など）をブロックチェーンの内部に伝えるブリッジの役割
※6 ETH：Ethereumの暗号資産名
※7 sUSD：Synthetixの暗号資産名
※8 利益2,378ETH：6,796+(7500-900-3518) -7500=2,378

2-5 他のDeFiプロジェクトの主なインシデント事例分析結果

2-5-4 サイドチェーンの双方向ブリッジにロックされた資金の窃取（Ronin Network）

発生日	被害額	関連DeFi	関連する要素	事件の概要	発生原因
2022/3/23	約6億2,010万ドル	Axie Infinity	Ronin Network Ronin Bridge PoA	・3/23 Axie Infinity が稼働するRonin Network の一部ノードのバリデータの秘密鍵が盗難され、EthereumネットワークとRoninネットワークを繋ぐ双方向ブリッジ（Ronin Bridge ）の資金が窃取された。 ・3/29 ユーザがRonin Bridgeから資金が引き出しできず、事件が発覚した。 Ronin Bridge運営元のSky Mavis社がRonin Bridgeを停止し、原因を調査。 ・4/6 損失補填のため、Sky Mavis社（ベトナム）が複数のVCから1億5,000万ドルの資金調達。 ・4/14 米連邦捜査局（FBI）が、北朝鮮のハッカー集団「ラザルス・グループ」と「APT38」の犯行であることを発表。 ・4/20時点で、Ronin Bridgeは停止中。 【事件の流れ】 1. 3/23 Ronin Network Validatorの9 ノードのうち5 ノードの秘密鍵が窃取され、Ronin Bridgeにロックされていた ETH/USDCが窃取された。（9ノードのうち、5ノードの承認が必要な仕組みだった） 2. 3/29 ユーザがRonin BridgeからETHを引き出すことができず、事件が発覚。即時にバリ データの閾値を5→8に修正。窃取された資金の殆どは攻撃者のウォレットに保有されていること を確認。政府機関と協力して攻撃者の捜査とウォレット監視を実施中。 3. 3/31 窃取されたSky Mavis社管理の 4ノードとAxie DAO（Sky Mavis社がDAOへの移行を計画しており、移行先候補のDAO）の 1ノードを置き換えた。新しいValidatorの追加を検討中。 【窃取された資金と暗号資産】 合計6億2,010万ドル ・ETH 173,600ETH（5億9,460万ドル） ・USDC 2,550万ドル	・Ronin Network Validatorsの9個のNodeのうち、5個のノードの秘密鍵が盗難されたため。 ・バリデータの秘密鍵はバリデート処理の署名用であり、新たな秘密鍵の作成やバリデータの 追加は別の権限（管理者権限）が必要であったが、管理者の秘密鍵が窃取されたかは不明。 ① Sky Mavis 4 Node Sky Mavisシステムへの攻撃により、集中サーバーに保管されていたバリデータの秘密鍵が4 Nodeとも盗難された。（攻撃手段は未発表） ② Axie DAO 1 Node 2021年11月、Ronin Networkの急激なトランザクション増加に伴う手数料高騰への対策として、ユーザに無料のトランザクションを提供するため、Axie DAOを1Node追加し、Sky Mavis Nodeの代理署名を許可した。 その対応は2021年12月に終了したが、Sky Mavis社が代理署名許可リストの削除を行っていなかった。その結果、Sky Mavis社の4ノードの盗難に伴い自動的に盗難された。



2-5 他のDeFiプロジェクトの主なインシデント事例分析結果

2-5-5 2020年以降の主なインシデント事例

発生日	原因	関連Defi	被害額	事件の概要
2020/4/19	ソフトウェアの脆弱性（リエントランシー）	Lendf.Me（レンディング）	2,500万ドル うち2,100万ドルを回収	・イーサリアムの脆弱性を突いたERC777トークンのリエントランシー攻撃を受けた ・攻撃者が窃取した暗号資産（ETH等）の現金化に手間取り、大半は返却された
2020/8/25	ソフトウェアの脆弱性（ステーキングプール処理の不具合）	YFValue (現Value DeFi)（イールドファーミング）	最大1億7,000万ドル 全額回収	・YFValue（YFV）のステーキングプールの脆弱性により、YFValueのタイマーがリセットされ、プールに一部の資金がロックされて引き出せなくなった ・ステーキングプールにある合計1億7,000万ドルがロックされて引き出せなくなる危険性があり、攻撃者から恐喝を受けた ・その後、運営チームがステーキングプールにロックされている資金を救済した
2020/9/14	ソフトウェアの脆弱性（トークン不正増刷）	bZx（デリバティブ）	800万ドル 全額回収	・bZxのiToken（利息を蓄積できるトークン）が不正に増幅できる脆弱性を悪用されて、約800万ドルが盗まれた ・後日、攻撃者を発見し、全額を取り戻した
2020/10/26	オラクル価格の不正操作（担保資産の枯渇）	Harvest Finance（イールドファーミング）	3,400万ドル うち250万ドルを回収	・攻撃者が20WETHをHarvest Financeのコントラクトに送金し、Curveの価格を操作して、暗号資産（fUSDT, fUSDC）の資金を枯渇させた。その後、攻撃者は資金をrenBTCに変換し、総額約3,400万ドルを窃取した。攻撃者は応答時間を与えず、7分間にわたってエンドツーエンドで攻撃した ・攻撃者はEthereumのミキシングプラットフォーム「Tornado.cash」を使用して資金移動を隠した。 ・攻撃者は250万ドルをUSDTとUSDCで開発者に返した
2021/5/18	オラクル価格の不正操作（担保資産の枯渇）	Venus（レンディング）	7,700万ドル	・Venusのトークン（XVS）の価格が、大口取引によって価格操縦され2倍に上昇。上昇したXVSを借入の担保に使用し、数億ドル相当のBTCとETHが借入された。 ・XVS価格が下がり、XVSを担保にして借入れた暗号通貨の返済をする時、XVSの流動性が低かったために期日内の返済にシステムが対応出来ず、Venusプロトコルで7、700万ドルの損失が発生した ・流動性を供給する際は10%の手数料が掛かるため、本件で攻撃者は5,500万ドル、流動性供給者は2,000万ドル、転売者は200万ドルの利益を得た
2021/8/10	ソフトウェアの脆弱性（ブロックチェーン間取引の不具合）	Poly Network（クロスチェーンブリッジ）	6億1,000万ドル 全額返還	・Poly Networkが、ブロックチェーン間取引の脆弱性を突かれたハッキング攻撃を受け、6億1,000万ドルを超える暗号資産が窃取され、Binance Smart Chain, Ethereum, Polygon等の複数口座に送金された ・脆弱性を知らしめるために攻撃をしたという声明が出され、数日後には全額が返還された

出典 https://hacked.slowmist.io/en/

2-5　他のDeFiプロジェクトの主なインシデント事例分析結果

2-5-5　2020年以降の主なインシデント事例

発生日	原因	関連Defi	被害額	事件の概要
2021/10/27	ソフトウェアの脆弱性（フラッシュローン攻撃）	Cream Finance（レンディング）	1億3,000万ドル	・フラッシュローン攻撃によりCream LPトークンやERC-20トークンの合計約1億3,000万ドルを窃取された ・コードの脆弱性を狙われたとし、該当部分の究明と対応は完了と発表。Cream Financeにとって2月、8月に続く3度目のフラッシュローン被害となった
2021/10/30	秘密鍵の管理不備	BoyX High Speed（BXH）（DEX）	1億3,900万ドル	・管理者キーの漏洩により1億3,900万ドルの資金が流出 ・攻撃者は管理者キーホルダーのコンピューターに侵入したか、BXHの技術スタッフの1人だった可能性
2021/11/5	秘密鍵の管理不備	bZx（デリバティブ）	5,500万ドル 全額返還	・PolygonとBSCの間でプロジェクトの展開を制御するために使用された開発者の秘密鍵が漏洩し、55百万ドルが窃取された ・bZx DAOの投票により、損害全額の補償計画が承認された
2021/11/30	ソフトウェアの脆弱性（トークン価格設定の不備）	Monox（DEX）	3,100万ドル	・スマートコントラクトの脆弱性（トークンの売却と購入の参照価格に同じトークン価格が使用されていた脆弱性）を攻撃され、Monoトークンの価格を操作し上昇させた上で、別のトークンに交換・引出しされた
2021/12/2	ソフトウェアの脆弱性（フィッシングUIの不正挿入）	Badger DAO（イールドファーミング）	1億2,000万ドル	・外部ネットワークのCloudflareの欠陥を攻撃されて、攻撃者が悪意のあるAPI keyを作成し、フィッシング用のUI（User Interface）を挿入した ・ユーザがそのUIをクリックすることでユーザのアドレスが犯人に盗まれて、資金が窃取された
2021/12/3	ソフトウェアの脆弱性（トークン不正増殖）	Polygon（サイドチェーン）	200万ドル	・12/3にホワイトハッカーにより重大な脆弱性（攻撃者がPolygonのコントラクトを使ってトークンを任意に生成できる）がPolygonに通知され、12/5に修正パッチがリリースされたが、パッチ適用までの間に、悪意あるハッカーにより200万ドル相当のMATICコインが盗まれた ・責任ある開示により脆弱性の発表を遅らせ、12/29に修正情報を開示した

出典　https://hacked.slowmist.io/en/

2-5 他のDeFiプロジェクトの主なインシデント事例分析結果

2-5-5 2020年以降の主なインシデント事例

発生日	原因	関連Defi	被害額	事件の概要
2022/2/2	ソフトウェアの脆弱性（署名検証処理のの不具合）	Wormhole（双方向ブリッジ）	3億2,000万ドル	・スマートコントラクトの脆弱性（署名を検証するコントラクトの不具合）を攻撃され、ブリッジにロックしていた資金が窃取された ・Wormholeの親会社であるJumpCrypto社はSolanaエコシステムをサポートするために損害を独自の資金でカバーした
2022/4/17	ソフトウェアの脆弱性（緊急コミット条件の不備）	Beanstalk（ステーブルコイン）	1億8,200万ドル	・ガバナンス投票スマートコントラクトの脆弱性を悪用され、Flash Loanにより資金を窃取された。 ・事件の流れ ①事件の前日に悪意のあるガバナンス提案（悪意のあるスマートコントラクトアドレスを指定）と通常の提案（ダミーのウクライナ寄付提案）の2件を提案し、1 件目がアドレス指定間違いの提案のように見せて、悪意のある提案をごまかした ②事件当日にAaveでFlash Loanにより以下を実行 ・AaveからETH・USDC・USDTで計10億ドルを借用 ・借りた資金でBeanstalkのガバナンストークンの2/3を購入 ・購入したガバナンストークンで悪意のある提案に投票 ・BeanstalkのEmergency Commitを起動して悪意のあるスマートコントラクトの実行に成功し、Beanstalkの資金を窃取した ・原因 ①悪意のある提案にコミュニティの誰も気づかなかった 提案の検証はコミュニティメンバーの協力に依存されており、誰も悪意のある提案を発見できなかった ②Emergency Commitに悪意のある提案をキャンセルする仕組みがなかった 提案をキャンセルする仕組み、およびキャンセル期間を設ける必要があった ③BeanstalkのEmergency Commitの起動条件の不備 （起動条件）提案後1日経過＆2/3以上の賛成票で実行される 提案可決後に一定期間（2日間など）を待つ仕様にすればFlash Loanによる攻撃は受けない ④AaveのFlash Loanが悪用された AaveのFlash Loanが無担保無制限に借りられるため、他のDeFiプロジェクトの攻撃に悪用された

出典 https://hacked.slowmist.io/en/

2-5　他のDeFiプロジェクトの主なインシデント事例分析結果

2-5-5　2020年以降の主なインシデント事例

発生日	原因	関連Defi	被害額	事件の概要
2022/5/10	ステーブルコインの大量売りによる市場価格の大幅下落	Terraブロックチェーン TerraUSD（UST） Anchor Protocol	市場価格の下落 UST 83% LUNA 99%	・ステーブルコインUSTの大量売りにより市場価格が1USDを維持できず、大幅に下落した。これまで1USDを一時維持できない事態が2度発生していたが、今回は価格が戻せなくなった。 ・事件の流れ ①5/5　BitcoinやETHなど暗号資産全体の価格が下落。（Bitcoinは5/12に最大32%下落） ②5/7　Anchor Protocolから大口出金（14億ドル）があり預金量が減少し、ステーブルコインUSTの価格が下がり始める。（大口出金者は不明。資産運用会社のブラックロック、シタデルは関与を否定） ③5/8　USTが2億5,800万ドル売られ、更に価格が下がる。 ④5/9-10　USTが2%下落し、1USDを維持できなくなった。LFG（Luna Foundation Guard）が価格維持のために保有していたBitcoin約40億ドルの全額を放出したが、売りに対して資金不足のため1USDに戻らなかった。（5/8時点のUST時価総額186.4億ドル） USTが取り付け騒ぎで大量に売られて価格が暴落し、アルゴリズムによりネイティブトークンLUNAが大量鋳造され、LUNAの価格が下落した。 LUNA総供給量：5/5時点約7.3億トークン→5/13時点6.5兆トークンに増加（約8,900倍） ⑤5/13　Terraブロックチェーンの運用を一時停止。 市場価格　UST：$1.0→$0.17（83%下落）、LUNA：$80→$0.02（99%下落） ※Anchor Protocol：Terraブロックチェーンの貯蓄プロトコル。USTトークンを預けると最大19.5%の利回りを提供する。 LUNA：Terraブロックチェーンのネイティブトークン。USTの価格維持のために使用される。（USTが1USDを超えると焼却、1USDを下回ると鋳造してUST＝1USDを維持する）

出典　https://hacked.slowmist.io/en/

2-6 トラストポイントの分析

区分	構成要素	トラストポイントの内容
トラストポイント	Ethereumライブラリ	・Ethereum ブロックチェーンにアクセスするウォレットなどブロックチェーン外部の各種サービスは、Ethereum Foundation等から提供されている共通ライブラリを利用しており、利用者はこのライブラリが正しく振る舞うことを前提としている
	Ethereum Nodeソフトウェア	・Ethereum ブロックチェーンで稼働するノードは、Ethereum Foundation等が提供する共通ソフトウェアの利用が推奨されており、ノード運用者はこのソフトウェアが正しく振る舞うことを前提としている ・Ethereumノードソフトウェアは複数の共通ソフトウェアが提供されており、ノード運用者はそれぞれのソフトウェアの開発者やサプライヤーなどが脆弱性などの問題がないコードを提供していることを前提としている
	インフラプロバイダ提供サービス	・Ethereum ブロックチェーンを利用するためにはEthereum Nodeからトランザクションを実行するが、このNodeを自分で構築するには負荷が高く、安価なインフラプロバイダのサービスを利用する場合がある。このサービス利用者は、インフラプロバイダのサービスが正しく振る舞うことを前提としている
	Webブラウザ	・DeFiやウォレットの利用時にWebブラウザで動くコードは、DeFiやインフラプロバイダ等が提供するものが稼働しており、DeFiやインフラプロバイダ等が組み込んだコードが正しく振る舞うことを前提としている
	DeFiで使用する汎用コード	・DeFiプロトコルや周辺機能などを開発する際に、特定機能の実現などのためにサプライチェーンなどの外部から汎用的なオープンソースのコードを取り込んで利用することがあり、その場合はサプライヤーが提供したコードが正しく振る舞うことを前提としている
	インターネット	・投資家や利用者のウォレットとインフラプロバイダの接続やマイナーが運営するEthereumノード間のP2Pネットワークなど、分散型金融システムのネットワーク接続はインターネットを経由しており、インターネットサービスプロバイダやデータセンタ事業者など複数の異なるインターネットが相互接続されたサービスを利用している。投資家や利用者、マイナーなどは、インターネット接続サービスが正しく振る舞うことを前提としている
	外部オラクルサービス	・一部のDeFiプロジェクトはオラクル攻撃防御などの目的で、自己プロジェクト内ではオラクル価格を算出せず、Chainlinkなどの外部オラクル価格提供サービスを利用してトークンの市場価格や手数料利率を入手している。このDeFiプロジェクトは、外部オラクル価格提供サービスが正しく振る舞うことを前提としている

2-6 トラストポイントの分析

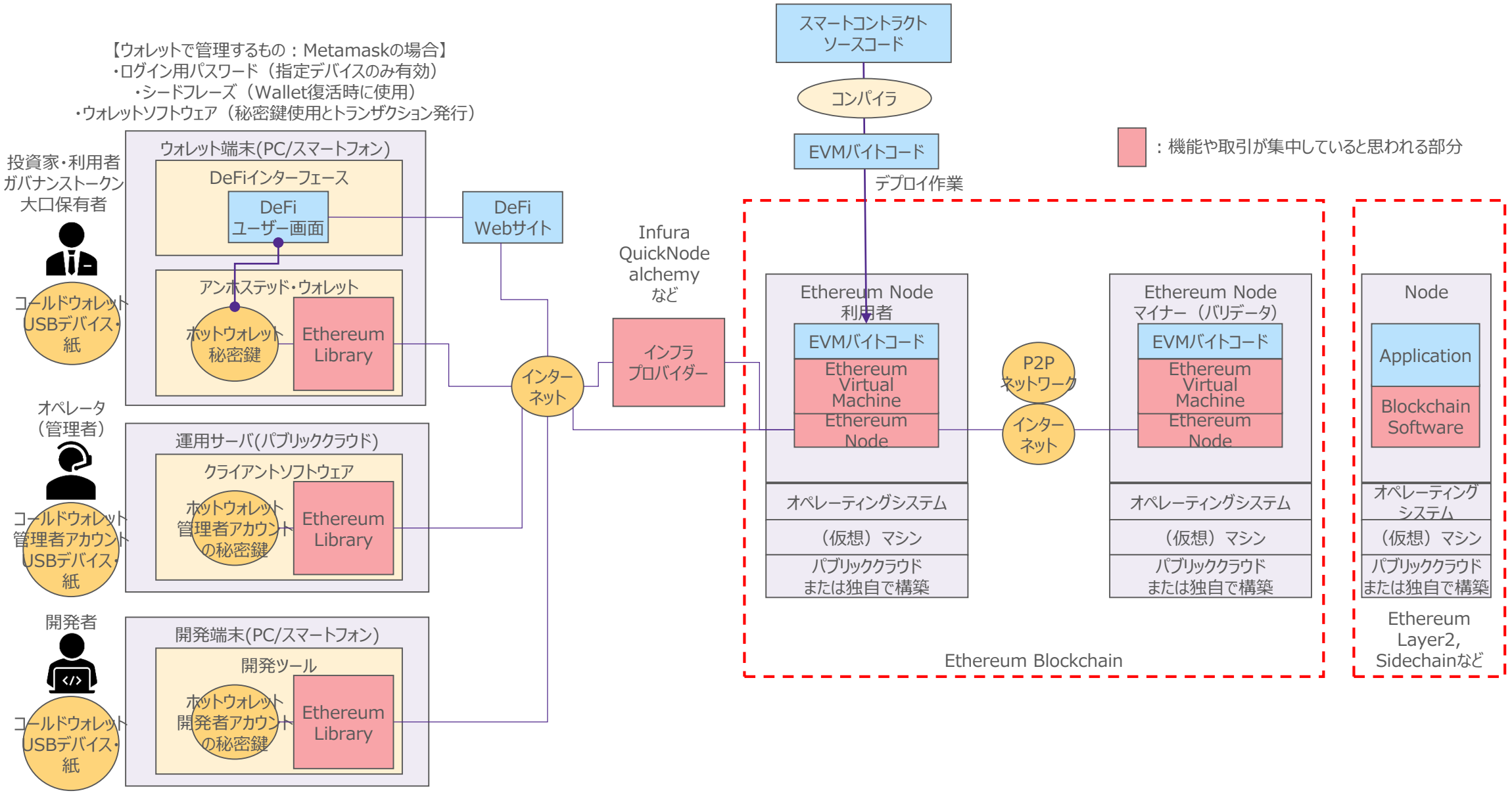


図 2-6-1 トラストチェーンにおけるトラストポイントの分析（ウォレット端末・運用サーバ・Ethereumノード）

2-6 トラストポイントの分析

区分	構成要素	トラストポイントの内容
トラストポイント	DeFiプロトコルの処理実行（清算などを実行するBOT処理）	・DeFiプロトコルで提供されているサービスでは、トークン価格維持や清算処理などを実行するために外部の複数のBOT（一定のタスクや処理を自動実行するアプリケーション）を使用して処理を実行しているが、その詳細内容は公開されておらず、利用者はそのBOTが正しく振る舞うことを前提としている
	DeFiプロトコル開発（スマートコントラクトの修正など）	・ガバナンス投票の提案などによりスマートコントラクトの修正を行う場合、大半のガバナンス投票参加者はスマートコントラクトのコード内容を理解しておらず、提案の内容通りに正しく振る舞うことを前提としている
	ガバナンス投票の委任	・ガバナンス投票は実際には少数者の投票で運営されており、多くの個人投票者は大手トークンホルダーに投票を委任している場合がある。この個人投票者は、委任した大手トークンホルダーが自分の期待した通りの投票を行ってくれることを前提としている
	ガバナンス投票で可決したスマートコントラクトやパラメータ修正などのデプロイ	・機能追加や利率変更などスマートコントラクトやパラメータを修正する提案がガバナンス投票で可決した後、自動ではデプロイされず、管理者や権限者がデプロイ作業を行う必要がある。提案者は、この管理者や権限者が可決した内容を正しく速やかにデプロイすることを前提としている
	緊急時のスマートコントラクト修正	・脆弱性の発見など緊急のスマートコントラクト修正が必要になった場合、Ethereumの開発ガイド等に従い、脆弱性を外部に公表せず関係者のみで対応を行う場合がある。利用者は、DeFiプロジェクトのコアチームなどの管理者や開発者がスマートコントラクトを正しく修正し、損害を出さずに対応してくれることを前提としている
	権限者による緊急時のシステム停止・悪意のある提案のキャンセル	・一部のDeFiプロジェクトでは、緊急時のシステム停止や悪意のある提案キャンセルをガバナンス投票で選任された権限者のマルチシグ投票で可決するルールとしている。利用者は権限者によるシステム停止や提案キャンセルが正当な理由で実行されることを前提としている
	サイドチェーンに接続する双方向ブリッジの資金ロック	・メインチェーンとサイドチェーンを接続する双方向ブリッジに、チェーン間で移動する資金がロックされる仕様になっており、多額の資金が双方向ブリッジに集中して保管される。チェーン間で移動する資金は双方向ブリッジにロックされた資金が担保となっており、ロックされた資金が攻撃などで流出するとチェーン間の資金移動ができなくなった。（Ronin Networkインシデント事例）

2-6 トラストポイントの分析

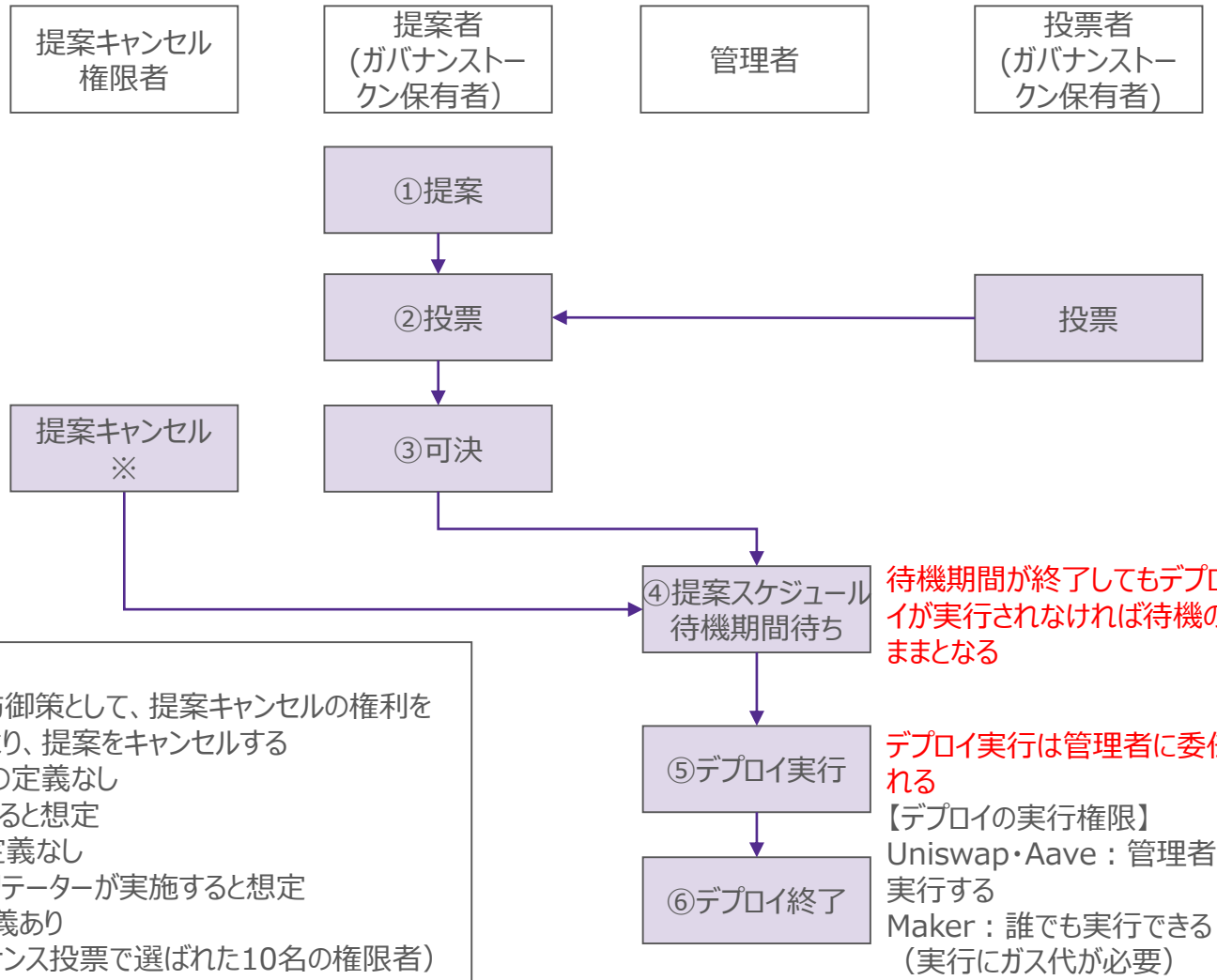
項目	スマートコントラクトの処理概要	説明
ガバナンス投票からスマートコントラクトのデプロイの流れ 【調査対象】 Uniswap Maker Aave		①提案者がオンチェーンで提案を書き込む ②投票期間中にガバナンストークン保有者が投票する ③事前にされた投票定足数や賛成数などの条件が満たされれば提案が可決される ④管理者が提案をスケジュールし、待機期間待ちに入る ・待機期間終了までに権限者がキャンセルを行うと提案を削除する ⑤待機期間終了後、管理者がデプロイを実行する ⑥デプロイが終了し、提案された内容がスマートコントラクトに反映される

図 2-6-2 トラストチェーンにおけるトラストポイントの分析（ガバナンス投票・デプロイ）

2-6 トラストポイントの分析

区分	構成要素	トラストポイントの内容
Weakest Link	サイドチェーンのバリデータ秘密鍵管理	・サイドチェーンを構成する基盤ブロックチェーンやDeFiなど複数のレイヤーの構成要素のうち、バリデータの秘密鍵管理に弱点があり、この弱点を攻撃されて双方向ブリッジにロックされている資金が窃取された。（Ronin Networkインシデント事例）
	悪意のある提案に対する検証	・悪意のある提案が行われた場合、その検証はコミュニティメンバーの協力に依存されているため、検証を実施する役割が明確でなく、誰も悪意のある提案を発見できなかった。分散型の組織において、コミュニティは自由参加であり役割が明示されていないため、悪意のある提案に対して検証が確実に行われるかどうかは不明である（Beanstalkインシデント事例）

第３章　分散型金融システムにおけるリスクおよびリスク低減策についての分析

3．分散型金融システムにおけるリスクおよびリスク低減策についての分析

3-1　システム運用におけるリスク

大項目	中項目	リスク事象	考えられるリスク要因	リスク低減策（案）	留意事項等
インフラプロバイダ	インフラプロバイダ提供サービスの利用集中	• 利用者（開発者等）のスマートコントラクト処理が、利便性の高い一部のインフラプロバイダに集中している	• 利用者が独自にEthereumノードなどのブロックチェーン接続機能を構築することが技術やコストの問題で難しいため、基盤部分は利便性の高いインフラプロバイダが利用される	• インフラプロバイダが、利用者に対してサービス利用集中によるリスクを周知する（サービス利用時にリスクを確認できる仕組みの提供など） • DeFiのサービスが停止する事態の重要度に応じて、複数のインフラプロバイダを冗長に使用することを推奨する	• リテラシーの低い利用者に、リスクを認識させたうえで利用させることが必要である。
	インフラプロバイダ提供サービスの中断	• インフラプロバイダのソフトウェア脆弱性等によりサービスが中断すると、それを利用するスマートコントラクト駆動ソフトウェアが実行できなくなる（Infuraのインシデント事例）	• 利用者がインフラプロバイダのサービス停止を想定した対応を検討していない（複数のプロバイダの利用など）		
	インフラプロバイダ提供サービスへの依存	• 利用者はインフラプロバイダのサービスに不具合がないことを信頼して利用しており、不具合を想定した対策を行っていない	• 利用者がインフラプロバイダのサービス停止を想定した対応を検討していない	• インフラプロバイダが、不慮のサービス停止を防止するため、カオスエンジニアリングなどの不具合による耐性強化策を実施する • インフラプロバイダが、品質に関する認証（SOC2）を取得し、サービス停止のリスクを低減する	対策として考えられる施策 • カオスエンジニアリング：本番環境に障害を注入し、回復する機能を常に動かしておく手法。 • SOC2：System and Organization Controls 2 アウトソーシング事業者（受託会社）における内部統制・保証報告の枠組みを利用する

3．分散型金融システムにおけるリスクおよびリスク低減策についての分析

3-1　システム運用におけるリスク

大項目	中項目	リスク事象	考えられるリスク要因	リスク低減策（案）	留意事項等
DeFiプロトコル	フラッシュローンによる無制限の資金借用	• フラッシュローンで巨額の取引を行うと流動性プールの資金が枯渇し、トークン価格が暴落する	• フラッシュローンを無担保無制限で借りることができる	• DeFiプロトコル開発者が本件のリスクを認識し、取引上限額などの設定を検討する ⅰ)フラッシュローン利用時の担保額設定(借入資金のn%) ⅱ)フラッシュローン利用額の上限設定	• 無担保借入を担保必要に変更することで、巨額の借入には巨額の担保が必要になり、悪用が防止できる
	緊急時のDeFiサービス停止	• 外部からの攻撃による資金流出やトークン不正発行などが発生した場合、DeFiサービスの緊急停止ができず、被害が止められない	• 緊急時の手段としてDeFiプロトコルを緊急停止する対応を検討していない • ブロックチェーンの仕様では通常スマートコントラクトは止められないため、DeFiプロトコルで対応する必要がある	• DeFiプロジェクトに対して、緊急時にDeFiプロトコルを緊急停止できる機能を設けるよう指導する	• 攻撃を受けても影響しない完全なスマートコントラクトの開発は極めて難しいと考える • よって、緊急時に被害を最小限に抑える手段として緊急停止機能を備えておくことが重要である
	不測時の対応	• 不測の事態（市場価格暴落や外部からの攻撃など）が発生した場合に、迅速な対応ができずサービスに影響を出す • 不測の事態における対応策が明確になっていない可能性	• 不測の事態に対する対応方針や手順を準備していない • 不測の事態を想定した仕組みや機能を実装していない	• DeFiプロジェクトが不測の事態に対するコンティンジェンシープランを策定し、必要なシステム対応を明確にする • その方針に従い緊急停止などの対応を実装する • コンティンジェンシープランの定期的な訓練を計画・実施する	• コンティンジェンシープランは、ブロックチェーン管理団体がDeFiプロジェクト向けにガイダンスを出す方法が考えられる • 定期的な訓練として、ハードニングなどの手法が考えられる ※ハードニング： 運営者と攻撃者の2チームに分かれて実地で経験を積む

3．分散型金融システムにおけるリスクおよびリスク低減策についての分析

3-1　システム運用におけるリスク

大項目	中項目	リスク事象	考えられるリスク要因	リスク低減策（案）	留意事項等
オラクル	オラクル攻撃	• オラクル価格決定における脆弱性を狙われて外部攻撃を受ける（市場価格と内部オラクル価格の差額を故意に発生させることによる裁定取引など）	• オラクル価格決定方法はDeFiプロジェクトにより異なり、安全な実装方法が確立していない • DeFiプロジェクトのうち、オラクル価格が特定プロジェクトの市場価格に連動している場合がある	• 関連組織やDAOの担当チーム等が、DeFiプロジェクト横断でオラクル価格決定方法の標準化や推奨方式の検討・周知を行う	-
	外部オラクル価格の反映遅延	• ネットワーク混雑などによる外部オラクルの価格参照が遅延した場合、外部市場と内部オラクル価格の差額が発生する	• オラクル価格の反映を故意に遅らせている場合、市場価格が急変するとオラクル価格が追い付かず差額が大きくなってしまう		

３．分散型金融システムにおけるリスクおよびリスク低減策についての分析

3-2　システム開発におけるリスク

大項目	中項目	リスク事象	考えられるリスク要因	リスク低減策（案）	留意事項等
スマートコントラクト	スマートコントラクトがアップグレード不可	• アップグレード不可のスマートコントラクトで脆弱性が発見されると、修正ができず攻撃による被害が増大する懸念がある • Upgradabilityに関する不具合があると、想定した修正ができない	• スマートコントラクトの脆弱性を全て解消することは極めて難しく、アップグレード不可はリスクが高いと考える	• スマートコントラクトをアップグレード可能にすることで、リスクが低減されると考える	• スマートコントラクトのアップグレードには、一般的にインフラプロバイダの提供サービス（OpenZeppelin Upgrades Pluginsなど）を利用することになり、どのサービスを導入するか検討が必要になる
	コードの脆弱性	• 既知のコード脆弱性が再発している事例があり、脆弱性が防止できない ⅰ)リエントランシー脆弱性（The DAO, Uniswapなど） ⅱ)フラッシュローン攻撃（bZx, Harvest Financeなど）	• スマートコントラクトは複雑な機能があり、脆弱性を全て検出することが技術的に難しい	• DeFiプロトコルの開発において、ソフトウェア開発の品質を確保するための最新技術を駆使し、脆弱性をできる限り排除する ⅰ)形式検証 ⅱ)機械学習による自動テスト ・開発技術の事例周知や推奨は、ブロックチェーン管理団体が行うことが望ましい	• ブロックチェーン管理団体への働きかけを行う方法の検討が必要

3．分散型金融システムにおけるリスクおよびリスク低減策についての分析

3-2　システム開発におけるリスク

大項目	中項目	リスク事象	考えられるリスク要因	リスク低減策（案）	留意事項等
スマートコントラクト	テスト検証の制約	• テストネットでは一部のテスト検証ができないが、メインネットでもテストに制約があり、完全なテスト検証ができない	• テストネットではインセンティブに関わる取引確認ができないため、十分なテストをせずにメインネットにデプロイする場合がある（機能はメインネットと同じだが、トランザクションフィーが無料、取引の混雑度が異なるなど）	• テストネットにインセンティブに関わる取引確認の手段を提供する • 内容により、メインネットにおけるテスト手法を検討する	• 対策はテストネットの機能強化が好ましいが、コスト面など実現性が難しい問題があると考えるため、実現性の検討が必要
	コード監査の懸念	• 複雑な処理はコード監査で脆弱性を発見できない懸念がある（複数のスマートコントラクトを跨る場合など）	• スマートコントラクトに対する攻撃は高度化しており、コード監査者の専門スキルや監査ツールの検証技術が新しいまたは複雑な攻撃パターンに追い付かない	• コード監査会社が、スマートコントラクト脆弱性検知技術やツールの検知精度を向上させる • コード監査会社が協業して技術向上の仕組みを行う（定期的にコンペを行いランク付けするなど）	• コード監査ツールの分析技術 ⅰ)静的検証 ⅱ)動的検証 ⅲ)形式検証
ブロックチェーン	双方向ブリッジにロックされた資金の攻撃	• Ethereumとサイドチェーン間の双方向ブリッジにロックされた資金を狙われて、バリデータの秘密鍵を窃取された攻撃により多額の損失が発生する • PolygonやAvalancheでは数十億ドルの資金がロックされており、甚大な被害の懸念あり	• Ethereumの仕様により、サイドチェーンとの資金のやりとりで双方向ブリッジに多額の資金がロックされるため、攻撃者から狙われやすい	• 資金を狙う攻撃の防止策の実施 秘密鍵管理技術の高度化、安全な秘密鍵管理の周知 • 双方向ブリッジに資金をロックする仕様の見直し 巨額の資金が１ヶ所に集中しないように考慮する必要あり	• 秘密鍵の保管技術の例 ⅰ)秘密分散 ⅱ)ソーシャルウォレット • 双方向ブリッジの仕様見直しは実現性の検討が必要

３．分散型金融システムにおけるリスクおよびリスク低減策についての分析

3-2　システム開発におけるリスク

大項目	中項目	リスク事象	考えられるリスク要因	リスク低減策（案）	留意事項等
ブロックチェーン	ブロックチェーン間の接続	• ブロックチェーンを跨る処理の脆弱性を狙った外部攻撃を受ける • クロスチェーンのスマートコントラクト呼び出し脆弱性の事例（PolyNetwork） • トークンブリッジプロトコルの署名検証脆弱性の事例（Wormhole）	• ブロックチェーンを跨る取引が複雑であり、テストでの検証が難しい（テストケースが網羅的でない、異常系テスト・境界条件テスト等が不足）	• DeFiプロトコルの開発において、ソフトウェア開発の品質を確保するための最新技術を駆使し、脆弱性をできる限り排除する ⅰ)形式検証 ⅱ)機械学習による自動テスト • 開発技術の事例周知や推奨は、ブロックチェーン管理団体が行うことが望ましい	• ブロックチェーン管理団体への働きかけを行う方法の検討が必要
	他のブロックチェーンやレイヤー2ソリューションの品質問題によるメインチェーンの影響	• Ethereumのスケーリング対策として、サイドチェーン・階層化チェーンやレイヤー2ソリューションの利用が増加している • 品質に懸念がある他のブロックチェーンやレイヤー2ソリューションと接続すると、メインチェーンが脆弱性攻撃などの影響を受けるリスクが高まる（Polygonは複数の脆弱性が報告されているなど）	• ブロックチェーンやレイヤー2ソリューションが多数存在しており、そのうち脆弱性などに懸念があるものが存在する • プラットフォームの脆弱性などを比較・情報開示する仕組みがない	• レイヤー2ソリューションや他のブロックチェーンとの連携検討時に、品質確保についてDeFiプロジェクト関係者間で検討を行う	• インフラプロバイダでは、連携するDeFiプロジェクトの開発者同士でプロトコル間の影響などを直接確認し、品質確保に努めているとされる

3．分散型金融システムにおけるリスクおよびリスク低減策についての分析

3-2 システム開発におけるリスク

大項目	中項目	リスク事象	考えられるリスク要因	リスク低減策（案）	留意事項等
DeFiプロトコル	DeFiプロトコル一部機能の不具合（ガス高騰時の考慮もれ）	• 市場価格暴落などの外部要因などにより大量のトランザクションが実行され、ガスの急激な高騰によりDeFiプロジェクトの清算処理等が正常に稼働せず、業務処理が中断する（Keeperのトランザクションがガス高騰に追いつかない）	• DeFiプロジェクトの業務処理について、急激なガス高騰が発生した場合に自分のトランザクションのガス価格を追い付かせる考慮がされていない	• Ethereumおよび2nd Layerのスケーリング技術の採用により、急激なガス高騰を発生させない仕組みを構築する	スケーリング対策として以下が計画、実施されている • Ethereum2.0（シャーディング）の利用（計画中） • 2nd Layerソリューションの利用 • サイドチェーンの利用
	DeFiプロトコル一部機能の不具合（ゼロ入札の防止もれ）	• ガス高騰により本来の処理が動かない状態で、ゼロ入札処理により資金が流出する	• ゼロ入札など本来発生しない取引の防止処理が組み込まれていない	• DeFiプロトコルにゼロ入札の防止策として最低金額を設定する • 本来の入札機能が稼働しなかった問題は、ガス高騰時の考慮もれ対策により解決される	• Makerでは入札の最低金額を元値の3%に設定した
	DeFiプロトコル間の連動	• DeFiプロトコル間の連動を悪用されて、外部からの要因で前提としていたものを破られる（オラクル価格など） • フラッシュローン（無担保無制限）で借りた巨額の資金を他のDeFiプロトコルの流動性プールに投入され、オラクル価格が急変する	• 取引額の上限を設定していない（流動性プールの預入額など） • 様々なDeFiプロトコルから連携されることを考慮した設計としていない	• DeFIプロトコルトが、外部の様々なDeFiプロトコルから連携されることを考慮し、自己防衛のためのテスト検証を行う必要があると考えられる • テスト検証の手法については、コードの脆弱性対策に含む	• ブロックチェーン管理団体への働きかけを行う方法の検討が必要

3．分散型金融システムにおけるリスクおよびリスク低減策についての分析

3-3 ガバナンスにおけるリスク

大項目	中項目	リスク事象	考えられるリスク要因	リスク低減策（案）	留意事項等
ガバナンス投票	投票の定足数が少ない	• ガバナンス投票の定足数が少なく、少数意見で意思決定がされてしまう（主なDeFiプロジェクトの定足数が1-4%と低い）	• ガバナンス投票の投票率が低いため、提案を可決するために定足数を少なくしていると考えられる	• ガバナンス投票の投票率の向上に合わせて、本来望ましい定足数に増やしていく	• ガバナンス投票が少数の意見に偏らないように、適切な投票率や定足数を維持するための運営組織のルールを設けるよう指導する • 運営組織への指導はブロックチェーン管理団体が行うことが望ましい
	投票率が低い	• ガバナンス投票の投票率が低く、一部の投票者で意思決定がされてしまう（主なDeFiプロジェクトの投票率が約2-9%と極めて低い）	• 暗号資産市場ではガバナンストークンに価値があり投機対象であるため、投機目的のトークン保有者は投票を行う意思が弱い	• 投票委任の仕組みや、投票によるトークン付与など、ガバナンストークン保有者の投票のインセンティブを向上する	
	悪意のある提案の検証	• 悪意のある提案が行われた場合、その検証はコミュニティメンバーの協力に依存されているため、検証を実施する役割が明確でなく、誰も悪意のある提案を発見できない懸念がある。	• 分散型の組織において、コミュニティは自由参加であり役割が明示されていない • 悪意のある提案に対して検証が確実に行われるかどうかは不明である	• 運営組織の役割として、提案の検証者を明示的に設ける（有償が望ましい）。形式検証による提案検証なども検討すべき。 • 悪意のある提案を検証するための作業期間（提案のタイムロック）を適切に設定する。	• 提案の検証者の設置や内容開示などの役割について、運営組織のルールを設けるよう指導する • 運営組織への指導はブロックチェーン管理団体が行うことが望ましい
	スマートコントラクト修正の依存	• ガバナンス投票によりスマートコントラクトを修正する場合、大半の投票者はスマートコントラクトのコード内容を理解しておらず、提案の内容通りに正しく振る舞うことを前提としている	• ガバナンス投票参加者のうち、スマートコントラクトを技術的に解釈できる人は一部である • 提案内容の情報開示が不十分であり、提案の正当性が保証されない懸念がある	• 運営組織の役割として、提案の検証者がスマートコントラクトの内容を投票者に開示する（提案内容と齟齬がないことをチェックする）	

３．分散型金融システムにおけるリスクおよびリスク低減策についての分析

3-4　金融市場との関わりにおけるリスク

大項目	中項目	リスク事象	考えられるリスク要因	リスク低減策（案）	留意事項等
金融機関との関わり	金融機関の損失リスク	• DeFiアプリケーションと接続して暗号資産取引を行った金融機関が、市場価格の下落やインシデント時に損失を計上する可能性	• 脆弱性が潜んでる可能性があるDeFiプロトコルの利用やボラティリティの高い暗号資産の保有に伴う損失リスク	• DeFiプロトコルの信頼性に関する検証を行う。 • 暗号資産のボラティリティを考慮して資産配分や上限額を設定する	• 暗号資産はボラティリティが高く、また攻撃などによる資金盗難リスクも考慮する必要があり、リスクを十分に考慮した資産運用が重要
企業との関わり	企業の損失リスク	• 企業のバランスシート上の暗号資が大幅に下落した場合に企業に損失が生じる可能性			
スマートコントラクト	市場安定性	• 特定の暗号資産の価格下落などがスマートコントラクトを通じて他に自動的に連鎖していき、市場全体の不安定化に繋がる	• スマートコントラクトはコードに従い決められた取引を自動実行するが、金融市場を安定させるための仕掛け（影響を伝播させない機能など）が組み込まれていない	• 不測の事態による金融市場への影響を防ぐ目的で、価格変動連鎖防止など市場安定化機能を検討する	暗号資産の市場安定化機能として、以下が考えられる • 急激な価格変動でオラクル価格を緩やかに反映する機能 • 基準額を超えた価格変動ではオラクル価格の反映を抑止する機能　など