# Research Report of JFSA Multilateral Joint Research on the Chains of Trust of Decentralized Finance

# (Summary)

June 2022

QUNIE Corporation

# Purpose and Background of the Study

- ✓ **Based on the assumption that current major DeFi projects have certain trust points (centralized elements that users and others are forced to trust unconditionally), we analyzed case studies of representative DeFi such as Uniswap (decentralized exchange: DEX), Maker (crypto-asset-backed stablecoin), AAVE (Lending).**
  - ✓ To understand which parts of a DAO (Decentralized Autonomous Organization) are “autonomous” (i.e., operated autonomously by smart contracts) and which are not
  - ✓ To understand the actual state of On-Chain Governance using governance tokens
- ✓ **Understanding the financial regulatory implications regarding trust points**
  - ✓ In general, entities trusted by users or other entities may be liable and subject to regulation (e.g., banks).
  - ✓ In DeFi, where parameter changes, smart contract upgrades, and decisions on the use of funds are left to the community (to a certain extent), the decentralization of responsibility may create difficulties in identifying regulatory targets, requiring a detailed trust point analysis for each project.



# Acknowledgement and Disclaimer


## Acknowledgement

- ✓ In preparing this report, we received useful advice and comments from Professor Naoyuki Iwashita of Kyoto University, Professor Kazue Sako of Waseda University, Project Professor Shigeya Suzuki of Keio University, and Research Professor Shin'ichiro Matsuo of Georgetown University. We also received useful suggestions and advice from observers from the Digital Agency and the Bank of Japan, as well as from officials of the Financial Services Agency.
- ✓ However, any errors in the content regarding this report are attributed to the trustee, Qunie Corporation.


## Disclaimer

- ✓ The contents of this report do not represent the official views of the JFSA.
- ✓ The contents in this report other than historical or current facts are forward-looking statements based on information available at the time of writing, and actual trends may vary due to a variety of uncertainties.

# Table of Contents

# Table of Contents

# Glossary

| Terminology | Definition. |
|---|---|
| AML/CFT | Anti-Money Laundering and Combating the Financing of Terrorism |
| BIS | Bank for International Settlements |
| DAO | Decentralized Autonomous Organization |
| DeFi | Decentralized Finance |
| ERC | Ethereum Request for Comments |
| EVM | Ethereum Virtual Machine: Virtual machine running the Ethereum client (node) |
| FATF | Financial Action Task Force |
| FISC | Financial Information Systems Center |
| IEC | International Electrotechnical Commission |
| IPA | Information-technology Promotion Agency, Japan |
| IOSCO | International Organization of Securities Commissions |
| ISO | International Organization for Standardization |
| KYC | Know Your Customer |
| TVL | Total Value Locked:Total value of crypto-assets deposited with DeFi |

# Chapter 1: Getting the Big Picture on Chains of Trust in Decentralized Financial Systems

# 1-1 Main definitions for decentralized financial systems

## ■ Decentralized Financial System

The 2019 FSB report defines a decentralized financial system as **financial system that decentralized financial technology may give rise**. It further defines decentralized financial technology as “**technologies that may reduce or eliminate the need for one or more intermediaries or centralized processes in the provision of financial services**. We use the above definition throughout this report.

The “decentralized financial system” is said to aim at building a non-centralized system, as opposed to the centralized system found in existing financial systems. On the other hand, in the description of “distributed systems”, "distributed" means to the decentralized arrangement of computers, and centralized systems are also considered to be a form of distributed systems. In this report, which focuses on decentralized financial systems, "distributed" is used to include the meaning of non-centralization.

## ■ DeFi (Decentralized Finance)

The so-called DeFi has been discussed in various literature and articles but not clearly defined. In this report, we define DeFi as **“financial applications that could consists a part of decentralized financial system"** according to the reference. DeFi initially focused on proprietary token issuance for funding and decentralized exchanges (DEX) that do not require the intermediation of traditional exchanges for token exchange. As the DeFi ecosystem has expanded, however, various initiatives such as lending, derivatives, and insurance have been introduced. There are also aggregators and other services that combine multiple DeFi transactions into a single location.

# 1-1 Main definitions for decentralized financial systems

## ■ DAO (Decentralized Autonomous Organization)

Although there is no set definition of a decentralized autonomous organization (DAO) that operates DeFi, based on references and the MakerDAO case study, this report defines DAO as an organization of **"a member-owned community where centralized leadership is absent and operations are conducted by rules encoded as computer programs** (smart contracts)**".**

<DAO features in major DeFi projects>

- ✓ An organization that is managed autonomously by the participants, without the existence of a company, representative, or board of directors to manage the organization.
- ✓ The organization's operating rules are coded by smart contracts.
- ✓ The token holder is granted a kind of voting right in the form of a token called a governance token, etc., and votes on certain decisions in the organization or community based on the rules of the smart contract.
- ✓ The organization is a global body with participants belonging to multiple countries, and the country or region to which the organization belongs is not necessarily specified because the governing legal entity is not always clear.

## ■ Trust Point/Chain of Trust

Trust is defined in the JFSA's "Study Group on Digital and Decentralized Finance" Interim report as "**The intention to entrust one's own vulnerabilities to the other party's behavior based on the expectation that the other party will take important actions regardless of whether the other party is monitored or controlled**", and **"the degree of belief that the other party will act as expected without confirming the actions**" .

Based on this definition, this report defines a trust point as "a centralized element in a decentralized financial system that users and others are forced to trust unconditionally", and a chain of trust as "a chain of dependencies that includes a trust point".

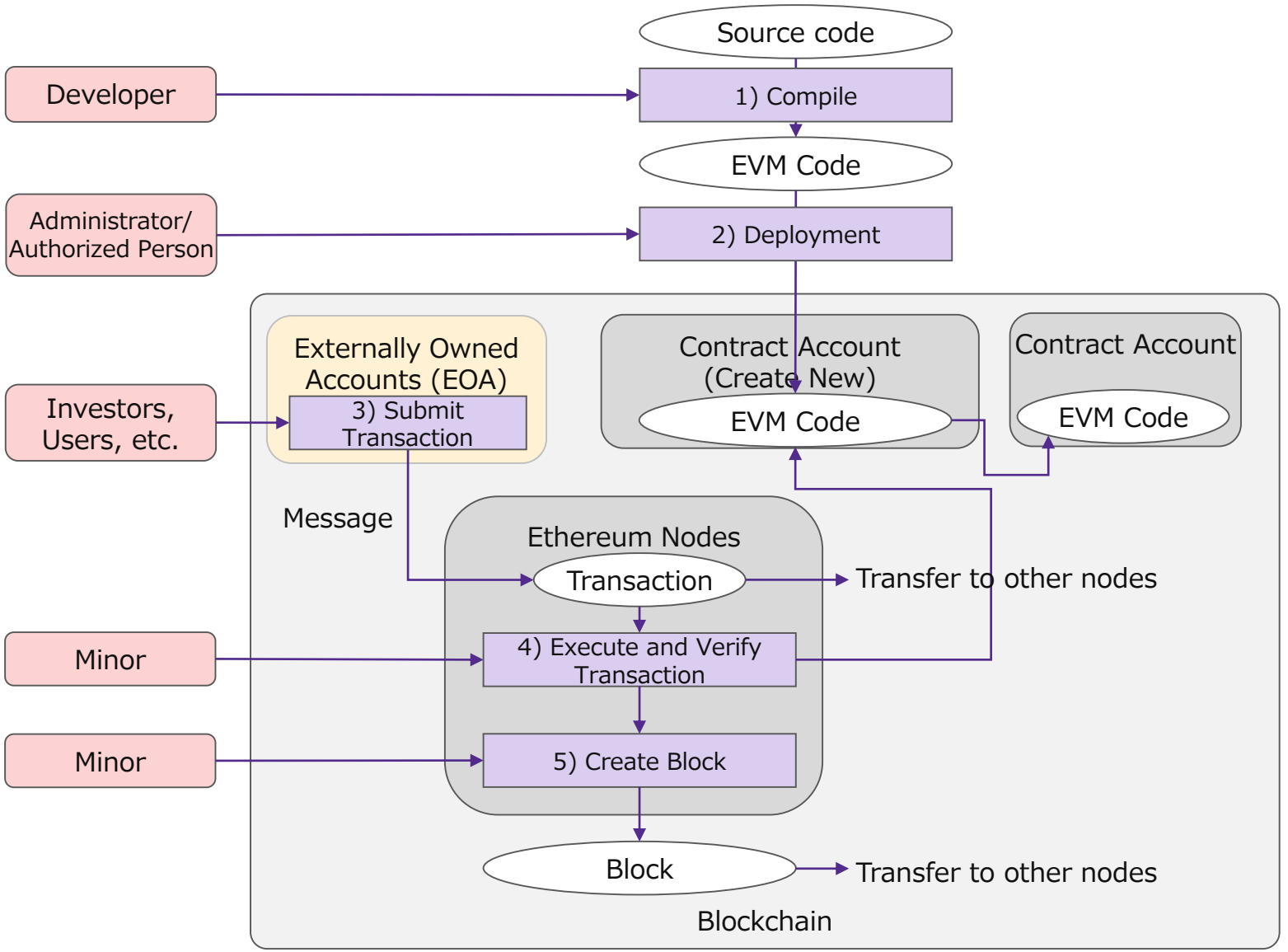
## ■ Weakest Link

Weakest Link, for the purposes of this report, refers to the components of DeFi and the connections between components that are the weakest in terms of security. By targeting the Weakest Link, attackers attempt to increase the likelihood of a successful attack the most.

# 1-2 Key components of a decentralized financial system

| # | Elements | Summary |
|---|---|---|
| (1) | **Blockchain Infrastructure** | **Main chain (e.g. Ethereum)**<br>✓ The base blockchain for running the DeFi protocol and is the parent chain for sidechains and Layer 2 scaling solutions.<br>✓ To deploy the DeFi protocol, a blockchain with flexible smart contract capabilities is required; in the case of Ethereum, there are two types of accounts held in the blockchain<br>➢ **Externally owned accounts**: Managed with a private key and can send and receive native tokens or other tokens and deploy and execute smart contracts (equivalent of an address of Bitcoin).<br>➢ **Contract account**: The deployed smart contract account, and smart contracts are executed in response to the receipt of messages from EOAs or other contract accounts.<br>✓ The clients (Ethereum nodes) that make up the main chain are equipped with Ethereum node software, which is common software provided by the Ethereum Foundation and others, and the virtual machines (EVMs) to execute smart contracts. |
| | | **Side chain (e.g. Polygon)**<br>✓ A a blockchain that operates in parallel with the main chain in order to improve the processing speed of the main chain and otherwise scale it up.<br>✓ Sidechains can reduce energy consumption and CO2 emissions by using consensus algorithms independent of the main chain (PoA: Proof of Authority, DPoS: Delegated Proof of Stake, BFT: Byzantine Fault Tolerance, etc.) and thereby improve transaction processing speed and reduce gas costs.<br>✓ It is connected to the main chain by a two-way bridge. When funds are exchanged between the main and side chains, funds are locked in the two-way bridge to prevent doubles pending. |
| (2) | **Layer 2 Scaling Solution** | ✓ There are off-chain solutions to scale up the Ethereum blockchain, such as increasing processing speed, as the following Rollup.<br>➢ **Optimistic Rollup:** Rollup is a mechanism to improve processing speed by executing transactions off-chain (Layer 2) outside the Ethereum main chain (Layer 1) and sending only the result data to Layer 1. Optimistic Rollup is said to improve processing speed because it assumes that transactions are valid by default and does not perform the calculations necessary to verify the validity of the data being written. |
| (3) | **Native tokens (e.g., ETH)** | ✓ A token (cryptocurrency) commonly used within the blockchain infrastructure and required as a transaction execution fee (gas fee), etc. |

# Reference: Flow of smart contract execution (in case of Ethereum)




1) The developer develops and compiles the source code, generates EVM code, and tests it.

2) The administrator/authorized person deploys the EVM code and a new contract account is created.

3) Transactions submitted by investors, users, and others from externally owned accounts are sent to the Ethereum node as messages. Messages sent to a node are forwarded to other nodes.

4) Minor verifies and executes the transaction. In this case, the EVM code associated with the contract account is executed* (including messages to other contract accounts).

5) Minor records the results of transaction execution (execution log, post-execution status) in a block.

If the EVM code describes a process corresponding to the message, it is executed; otherwise, the default process (Fallback function) is executed.

Figure 1-2 Flow of smart contract execution (in case of Ethereum)

# 1-2 Key components of a decentralized financial system

| # | Elements | Summary |
|---|---|---|
| (4) | **Smart Contract** | ✓ Generally, it refers to **rules (contracts) that are written as programs and automatically executed and processed on the blockchain.**<br>✓ In Ethereum and similar blockchains, smart contracts are held in a contract account and are invoked from externally owned accounts or other smart contracts via messages. The smart contract is written to the blockchain and executed by a minor or validator in the process of validating the transaction. Its execution log and post-execution vouchers are recorded in the block so that everyone can verify that the genuine program code has been executed and share the status.<br>✓ Smart contracts usually cannot be modified or deleted, and execution results cannot be undone, but there **is room for smart contracts to be upgraded by replacing** references with new contract addresses if indirect references are used, for example through support by development tools.<br>✓ Smart contracts can be executed by deploying them to the blockchain, but the deployment process in DeFi generally requires the private key of an externally owned account held by an administrator or authority (who holds the private key needed to deploy the smart contract).<br>✓ In this document, **the smart contract that enables DeFi functions and services is referred to as the "DeFi Protocol"**. |
| (5) | **Wallet** | ✓ Manages the user's private key, maintains the wallet address and other information for the user to perform transactions with the private key, and provides the user interface (e.g., web browser or smartphone app control screen). The user usually connects their own wallet to each DeFi service. |
| (6) | **User Interface** | ✓ In DeFi, it refers to the user authentication screen and user operation screen (GUI: Graphical User Interface) of a web browser or smartphone application when using the DeFi service, as well as the commands used by operational operators (CLI: Command Line Interface). |
| (7) | **Infrastructure provider** | ✓ Blockchain node hosting services that offer API and other services to DeFi developers and wallet providers to build DeFi functions and services, such as access to the blockchain. Major infrastructure providers include Infura (by ConsenSys), Quicknode (by QuickNode), and alchemy (by alchemy). |
| (8) | **DeFi System Development Tools** | ✓ Development tools for DeFi system developers to develop/test DeFi protocol smart contracts, etc., such as Truffle and Hardhat in Ethereum.<br>✓ Development tool features include developing/debugging smart contracts, compiling source code, testing on local nodes, and deploying to the blockchain for development. |

# 1-2 Key components of a decentralized financial system

| # | Elements | Summary |
|---|---|---|
| (9) | **Code Auditing Company** | ✓ A company that provides analysis services to detect design problems, code errors, and security vulnerabilities in smart contract code through static verification (code analysis, formal verification, etc.) using code auditing tools, dynamic verification, and desk review by code auditors. |
| (10) | **Client Software** | ✓ Software used by DeFi developers and operators to access clients (nodes) from the outside when performing operations such as deploying and maintaining smart contracts and monitoring the operation of the DeFi protocol, including terminal emulators and web browsers (infrastructure provider). |
| (11) | **Oracle** | ✓ A data feed for smart contracts to retrieve off-chain external data, mainly used as a price oracle to retrieve external market prices and interest rates. |
| (12) | **Governance Token / Governance Vote** | ✓ Generally refers to a token that is granted the right to vote on community decisions.<br>✓ Governance token holders vote on modifying the functionality of the DeFi protocol, changing parameters such as additions and interest rates, and using community funds, and implement what is passed according to rules determined by the amount held. This mechanism is called “governance voting”. |
| (13) | **KYC Certification Companies** | ✓ When DeFi services are provided to institutional investors, such as Aave, an external KYC certification company may perform KYC certification of institutional investors, etc. (As an example, an institutional investor certified by a KYC certification company is white-listed and notified to DeFi and recognized as a KYC-compliant user by DeFi, etc.). |
| (14) | **Aggregator** | ✓ A function or service that aggregates various DeFi services that exist on the blockchain into a single location (e.g., website) and provides users with opportunities for efficient crypto-asset transactions.<br>✓ DeFi aggregators will find optimal token exchange rates and yields from decentralized exchanges, lending protocols, liquidity pools, etc. and offer them on their platforms. |

# 1-3 Map of the main components that make up a decentralized financial system

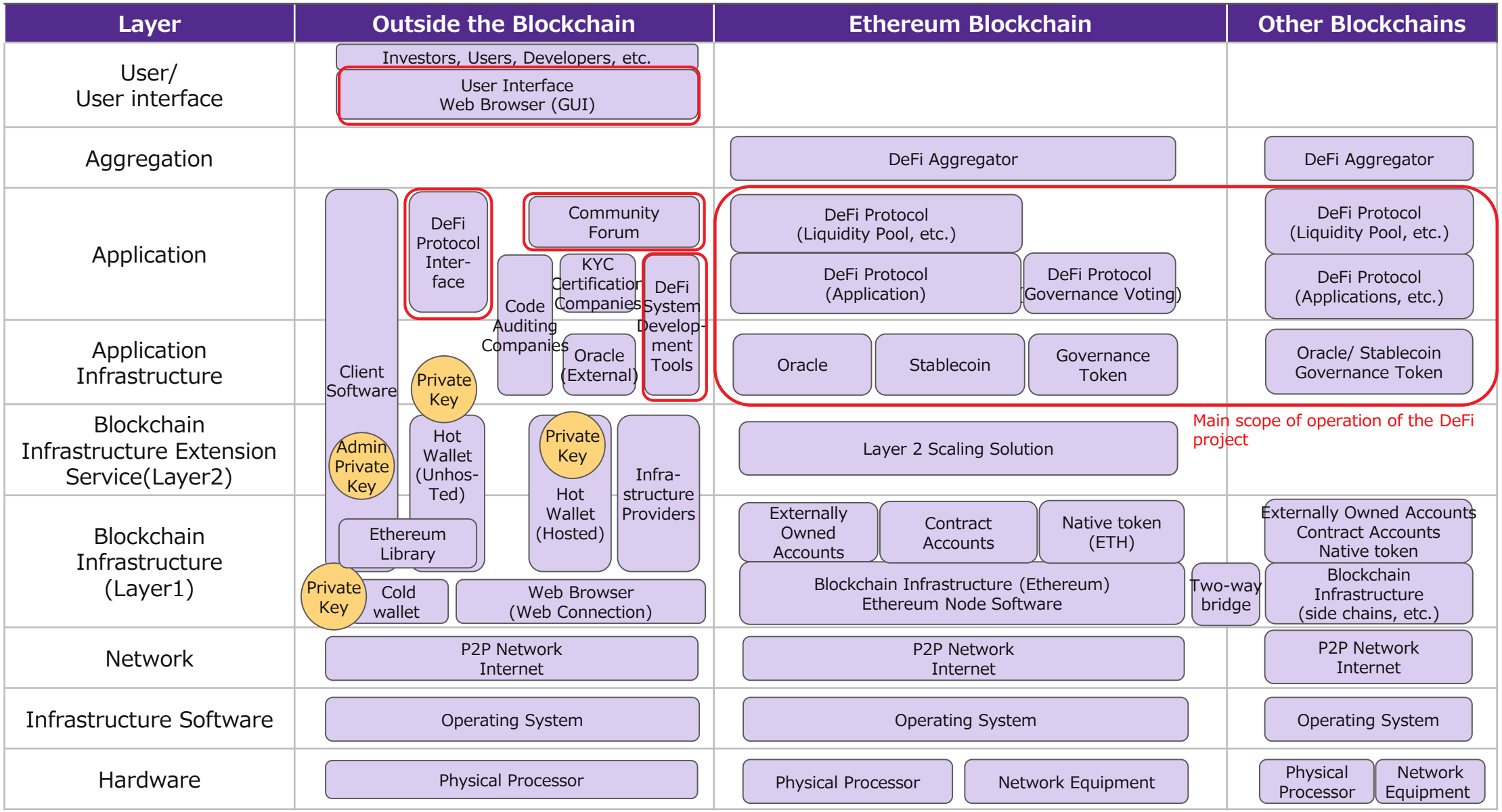



Figure 1-3 Mapping of the main components of a decentralized financial system

# Chapter 2: Analysis of Major DeFi Projects

# 2-1 Outline of the projects surveyed

| Item | Contents | Uniswap | Maker | Aave |
|---|---|---|---|---|
| Summary | Services provided | Decentralized Exchange (DEX) | Stablecoin (DAI) issuance | crypto-asset-Backed Lending |
| | Service Start Date | November 2018 | December 2014 | May 2017 |
| | TVL (as of February 13, 2022) | TVL $8.29 billion | Outstanding balance $16.95 billion | TVL $10.74 billion |
| | Total fees (in 2021) | 1.65 billion U.S. dollars<br>✓ Liquidity pool fee income<br>✓ UniswapV2 $827 million<br>✓ UniswapV3 $817 million and others | 0.69 billion U.S. dollars<br>✓ Income from stabilization fees, liquidation penalties, etc. | 3.1 billion dollars<br>✓ Income from loan fees<br>✓ Aavev2 $256 million<br>✓ Aavev1 $0.27 billion and others |
| | Governance Token | UNI (addresses held: 276,000) | MKR (addresses held: 83,000) | AAVE (addresses held: 106,000) |
| Community Related Organizations | Founder | Hayden Adams | Rune Christensen | Stani Kulechov |
| | Community | Uniswap Community (DAO) | MakerDAO | Aavenomics Community (DAO) |
| | Community Management | ✓ Governance token holders are the core of the company's operations<br>✓ Involvement in certain community operations of related organizations and teams within the DAO | Community Management | ✓ Governance token holders are the core of the company's operations<br>✓ Involvement in certain community operations of related organizations and teams within the DAO |
| | Main Related Organizations | Uniswap Labs (U.S.)<br>✓ Protocol development and management, involvement in community management, etc. | DAI Foundation (Denmark)<br>✓ Intellectual property management, etc.<br>RWA Company LLC (Cayman Islands)<br>✓ Manage investments in real-world assets, sign contracts with clients, etc. | Aave Limited (U.K.)<br>✓ Already licensed by FCA as an electronic money vendor<br>Aave SAGL, Switzerland<br>✓ Registered as a software manufacturer |
| | Dissolved Organization | - | Maker Foundation (Denmark)<br>✓ Upon dissolution in July 2021, Maker Foundation assets were transferred to MakerDAO and operations was taken over by domain teams/core units within MakerDAO | - |

# 2-1 Outline of the projects surveyed

| Item | Contents | Uniswap | Maker | Aave |
|---|---|---|---|---|
| Technological Characteristics | Main Technological Characteristics | ✓ AMM (Automated Market Maker)<br>✓ Flash Swap<br>✓ Concentrated Liquidity<br>✓ Flexisible Fee | ✓ Maker Vault (DAI generation)<br>✓ Liquidation System 2.0<br>✓ Dai Direct Deposit Module (D3M)<br>✓ Keeper (market makers/ auction)<br>✓ Flash Mint | ✓ Aave interest bearing tokens (aToken)<br>✓ Flash Loan<br>✓ Credit Delegation<br>✓ Aave Arc/White Lister |
| | Oracle Functions | ✓ Price calculation within own project without using Oracle<br>✓ Calculate TWAP (time weighted average price) by taking the cumulative total of prices of crypto-asset pairs<br>✓ Measure market prices for all crypto-asset pairs before any trades are made | ✓ Oracle's structure within self-projects<br>✓ Oracle Price Feed" gets prices from multiple external markets<br>✓ Overall median price is calculated and reflected in the internal price after 1 hour | ✓ Dependent on external oracle services<br>✓ Market prices and lending rates are obtained using Chainlink, a decentralized oracle service, and are reflected internally. |
| | Upgrade Availability | ✓ Core contract is not upgradeable by design<br>✓ (AMM, liquidity aggregation functions, oracle functions, etc.)<br>✓ Some parameters (fees) can be changed.<br>✓ Contracts other than the core (fees, peripherals, interface, governance voting, etc.) can be changed.<br>✓ It is believed that the development company has administrative privileges (administrator's private key) to modify the code. | ✓ Smart contracts are upgradeable.<br>✓ Supported by incorporating a feature in the smart contract that allows upgrades to be made in advance | |

# 2-1 Outline of the projects surveyed

| Item | Contents | Uniswap | Maker | Aave |
|---|---|---|---|---|
| Technological Characteristics | Supported Blockchains (Scalability) *Blockchains where the protocol is deployed and the token is available | ✓ Ethereum<br>✓ Ethereum 2nd Layer solution (Optimism, Arbitrum)<br>✓ Side chain (Polygon) | ✓ Ethereum<br>✓ Ethereum 2nd Layer solutions (Optimism, Arbitrum, Loopring, zkSync, Aztec 2.0)<br>✓ Sidechains (avalanche, Polygon, BSC, Fantom, Klaytn, xDAI, Harmony, solana, Celo, Moonriver) | ✓ Ethereum<br>✓ Ethereum 2nd Layer solution (Arbitrum, zkSync, Aztec 2.0)<br>✓ Side chains (avalanche, Polygon, BSC, Fantom, xDAI, Heco, Sora) |
| Emergency Response | Cancellation of malicious proposals | ✓ Details unknown<br>✓ The smart contract allows for proposal cancellation by the administrator, but does not define a proposal cancellation function or an administrator who can perform it (assuming it is performed by the developer or core unit in case of emergency?) | | ✓ Governance proposals can be canceled<br>✓ As a countermeasure in the event of a malicious proposal, the proposal can be cancelled by the selected authority (Guardian) via multisig approval during the waiting period of the governance vote |
| | Urgent smart contract fixes | ✓ In principle, not supported because the core contract is not upgradable. | ✓ Dark spell mechanism allows for emergency correction<br>✓ A mechanism to modify smart contracts to fix critical vulnerabilities.<br>✓ Only certain parties will be involved, and the content will not be made public until a certain period of time has elapsed after the correction is completed. | ✓ Unknown.<br>✓ Content unknown as not defined in documentation (assumed to be performed by core team in case of emergency) |
| | What to do when attacked | | ✓ Protocol can be stopped by emergency shutdown<br>✓ A certain number of governance vote protects Maker Protocol from Malicious attacks<br>✓ Vote at any time, regardless of the proposal. | ✓ Possible to pause the protocol with the emergency key<br>✓ In the event of an emergency, such as an external attack, Guardian's multisig approval can trigger an emergency key. |

# 2-1 Outline of the projects surveyed

| Item | Contents | Uniswap | Maker | Aave |
|---|---|---|---|---|
| Community Decision-Making | Number of Governance Tokens Distributed | ✓ UNI: 1 billion tokens being distributed sequentially<br>✓ (being distributed over 4 years starting in September 2020) | ✓ MKR: 1 million tokens already distributed<br>✓ (as of January 2022) | ✓ AAVE: 16 million tokens already distributed<br>✓ (as of January 2022) |
| | Initial Distribution of Governance Tokens<br>1) Free Distribution | ✓ Initial distribution in the following percentages<br>✓ Community members 60%<br>✓ Team members, employees 21.266%<br>✓ Investors 18.044%<br>✓ Advisors 0.69% | ✓ Distributed and sold 1 million tokens<br>✓ Distribute a portion to early adopters | ✓ Former LEND token holders 13 million tokens<br>✓ Breakdown: Founder & Project 23%, Investors 77<br>✓ Reserve fund: 3 million tokens |
| | Initial Distribution of Governance Tokens<br>2) Paid Distribution | None | ✓ Sold to venture capitalists via ICO (Andreessen Horowitz, Polychain Capital, etc.) | None |
| | Role of Governance Tokens | 1) On-chain voting | 1) On-chain voting<br>2) Used to recapitalize stablecoin DAIs (add or delete DAIs)<br>3) Used as funds (MKR issued) in case of shortage of liquidation funds | 1) On-chain voting<br>2) Used as a reserve fund (safety module) in case of insufficient liquidation funds |
| | Items that can be proposed in the Governance Vote<br>1) Application | 1) Smart contract changes<br>✓ Non-core application processing (additional liquidity pool changes, interfaces, governance voting, etc.)<br>✓ Change parameter values (e.g., fees) | 1) Smart contract changes<br>✓ Application processing (D3M, Vaults, Clearing Systems, Oracle, etc.)<br>✓ Change parameter values<br>➢ Additional changes to new collateral asset types<br>➢ Additional changes to existing risk parameters<br>➢ DAI Savings Rate Changes<br>- Decide on system upgrades<br>2) Selection of oracle price feeds | 1) Smart contract changes<br>✓ Application processing (Lending, SM/SI, Flash Loan, Credit Delegation, etc.)<br>✓ Change parameter values (e.g., commissions)<br>✓ Decide on system upgrades |

# 2-1 Outline of the projects surveyed

| Item | Contents | Uniswap | Maker | Aave |
|---|---|---|---|---|
| Community Decision-Making | Items that can be proposed in the Governance Vote 2) Governance | 1) Change in community management<br>✓ Distribution of community funds, changes in governance voting<br>2) Modification of the term of core contract commercial license, waiver | 1) Change in community management<br>✓ Distribution of community funds, changes in governance voting<br>2) Execution of emergency shutdown (always possible to vote) | 1) Change in community management<br>✓ Distribution of community funds, changes in governance voting<br>2) Guardian Recommendation |
| | Items that cannot be proposed in a governance vote | 1) Smart contract changes<br>System upgrades (performed by the developer) | (No specific restrictions) | (No specific restrictions) |
| | Governance Voting Process | Two-tier voting: snapshot voting and governance voting<br>1) Snapshot<br>✓ Voting 2 days, quorum 0.05%, over 50% in favor<br>2) Governance Vote<br>✓ Voting 5 days, quorum 4%, over 50% in favor | Choose between Governance Voting and Executive Voting, depending on the nature of the proposal.<br>1) Governance Poll<br>✓ Decide on policies, etc. other than changes to the smart contract, such as the amount, interest rate, and selection of personnel, etc.<br>✓ Voting 7 days, quorum 1%, 50% or more in favor<br>2) Executive Vote<br>✓ Determine only the portion of the smart contract that is changed<br>✓ Vote 30 days, quorum 1%, 50% or more in favor | Two-tier voting: snapshot voting and governance voting<br>1) Snapshot<br>✓ 3 days to vote, quorum 50 votes, 50% or more in favor<br>2) Governance Vote<br>✓ Short time lock (not related to governance): 3 days of voting, 2% quorum, 50.5% or more in favor<br>✓ Long time lock (proposals affecting governance: 10 days to vote, 20% quorum, 57.5% or more in favor) |
| | | ✓ 2-day waiting period after the proposal is approved<br>✓ Management can cancel proposals during the waiting period.<br>✓ Deployed by administrator after waiting period | ✓ Waiting period after the proposal is approved (2 days for B only)<br>✓ Authority can cancel proposals during the waiting period<br>✓ After the waiting period, anyone can deploy | ✓ Waiting period after the proposal is approved<br>1) 1 day<br>2) 7 days<br>✓ During the waiting period, the selected Guardian can cancel the proposal.<br>✓ Deployed by administrator after waiting period |

# 2-1 Outline of the projects surveyed

| Item | Contents | Uniswap | Maker | Aave |
|---|---|---|---|---|
| Community Decision-Making | Governance Voting Ratio (2021 Actual) | ✓ Governance turnout: approx. 5-9%. | ✓ Governance turnout: approx. 4-9%. | ✓ Governance turnout: approx. 2-3%. |
| | Percentage of Governance Proposals Passed (Actual results for 2021) | ✓ Snapshot Voting 77% (27/35)<br>✓ Governance Voting 86% (6/7) | ✓ Governance Voting 90% (275/307)<br>✓ Executive Voting 100% (47/47) | ✓ Short time lock 88% (45/51)<br>✓ Long time lock 50% (1/2 case) |
| | Main Voters | Large token holders Mainly 10 organizations<br>✓ 4 universities (Berkeley, Stanford, Harvard, UCLA)<br>✓ Fintech (Gauntlet, Dharma, Kiva)<br>✓ VC (Andreessen Horowitz, Monet Supply, Index Corp.)<br>Individual investors can delegate voting rights<br>Other voters Mainly 3<br>- DeFi project stakeholders (Ethereum Foundation, Variant, Compound, etc.) | Voting proxy 18 Address<br>✓ Public Agent 9 Address<br>✓ Non-public Agent 9 Addresses<br>Individual investors can delegate voting rights.<br>Large private investor (anonymous) | Large token holders 4 addresses (including funds for system use)<br>✓ Aave<br>✓ Binance<br>✓ Balancer<br>✓ Polygon<br>Regular voters 4 addresses (anonymous)<br>✓ The 4 addresses have made decision on most of the proposals on the 1) snapshot.<br>✓ Individual investors can delegate their voting rights. |
| Cooperation with Financial Institutions | Settlement-related | Use for debit card settlement funds<br>✓ Crypto.com<br>Payments can be made to about 30 stores such as UNI, MKR, AAVE, etc. for product purchases (Shopping.io) and travel (Travala.com) | | |
| | | - | ✓ Monolith<br>Convert DAI into fiat currency and load onto Visa debit card for use | - |

# 2-1 Outline of the projects surveyed

| Item | Contents | Uniswap | Maker | Aave |
|---|---|---|---|---|
| Cooperation with Financial Institutions | Financial Products | ✓ Listed an ETP (exchange-traded product) passively linked to UNI through Valour (Swiss asset management company), a subsidiary of DeFi Technologies (Canadian tech company).<br>✓ Frankfurt Stock Exchange in Germany: Euro-denominated Valour Uniswap ETP (October 2021)<br>✓ Stockholm's Nordic Growth Market in Sweden: Swedish Krona-denominated Valour Uniswap SEK (December 2021) | - | - |
| | Custody Trading Services | ✓ Sygnum Bank AG (Swiss digital bank) announced the launch of custody and trading services for several DeFi tokens (governance tokens) and stablecoins (USDC) (June 2021) | | |
| | | ✓ Commonwealth Bank (Australia) launched 10 crypto exchanges and custody services in partnership with Gemini Exchange and Chainalysis (November 2021). | - | ✓ Commonwealth Bank (Australia) launched 10 crypto exchanges and custody services in partnership with Gemini Exchange and Chainalysis (November 2021). |
| | | ✓ Arab Bank Switzerland to offer 10 crypto-asset-related services (January 2022) | - | ✓ Arab Bank Switzerland to offer 10 crypto-asset-related services (January 2022) |

# 2-1 Outline of the projects surveyed

| Item | Contents | Uniswap | Maker | Aave |
|---|---|---|---|---|
| Cooperation with Financial Institutions | STO Real Estate Loan<br><br>STO: Security Token Offering | - | ✓ Formed partnership with Forge (digital assets subsidiary of Société Générale) for real estate loans through STO (October 2021)<br>✓ *Six entities in the DAI issuance plan<br>1) Société Générale<br>2) Forge<br>3) MakerDAO protocol<br>4) Legal representative of MakerDAO<br>5) Role of the DIIS Group (French Fixed Income Investors) Securities Agent<br>6) Exchanges | - |
| | Other Initiatives | ✓ The company is reportedly considering entering the market through a tie-up with a Fintech company (July 2021).<br>✓ PayPal<br>✓ Robinhood (U.S. stock management application operator)<br>✓ E*Trade (U.S. online brokerage firm)<br>✓ Stripe (U.S. online payment), etc. | Donate to charity (pay as USD)<br>✓ UNICEF (charity organization)<br>✓ NeedsList (Disaster Relief)<br>✓ PoolDai (Charitable Giving Fund)<br>Payroll Solutions<br>✓ Whisp Money (in some communities, payroll is paid with DAI to outside employers with KYC unstable) | AaveARC<br>✓ Ability for institutional investors who have undergone financial due diligence to borrow and lend crypto-assets with other approved institutional investors<br>Whitelister<br>✓ Firms approved by Aave to register institutional investors on the AaveARC White List<br>✓ Registered: U.S. company Fireblocks (January 2022)<br>✓ In the process of registration: Securitize (U.S.), SEBA Bank (Switzerland) |

# 2-2 Analysis of decentralized exchange Uniswap

## 2-2-1 Project Overview

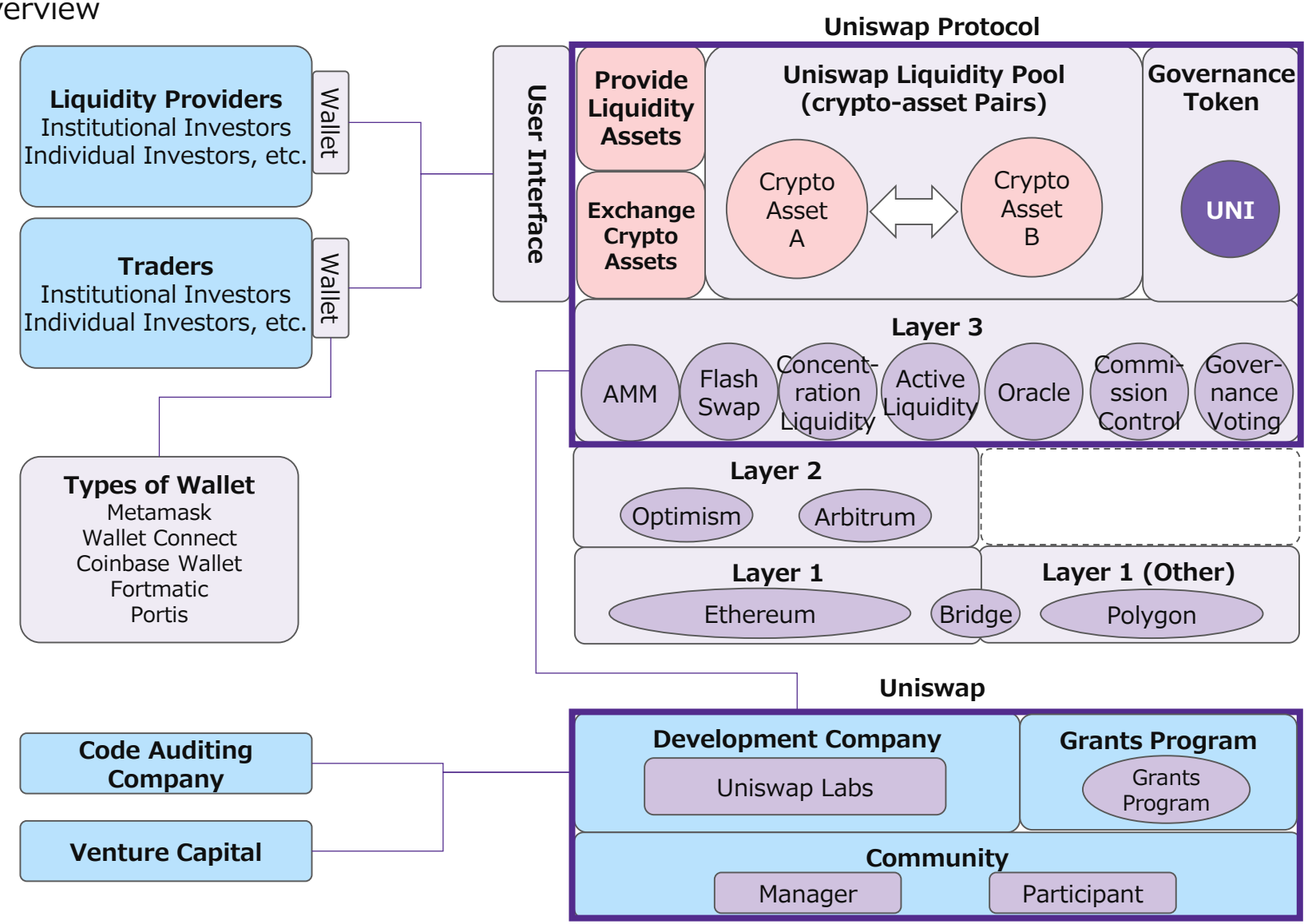
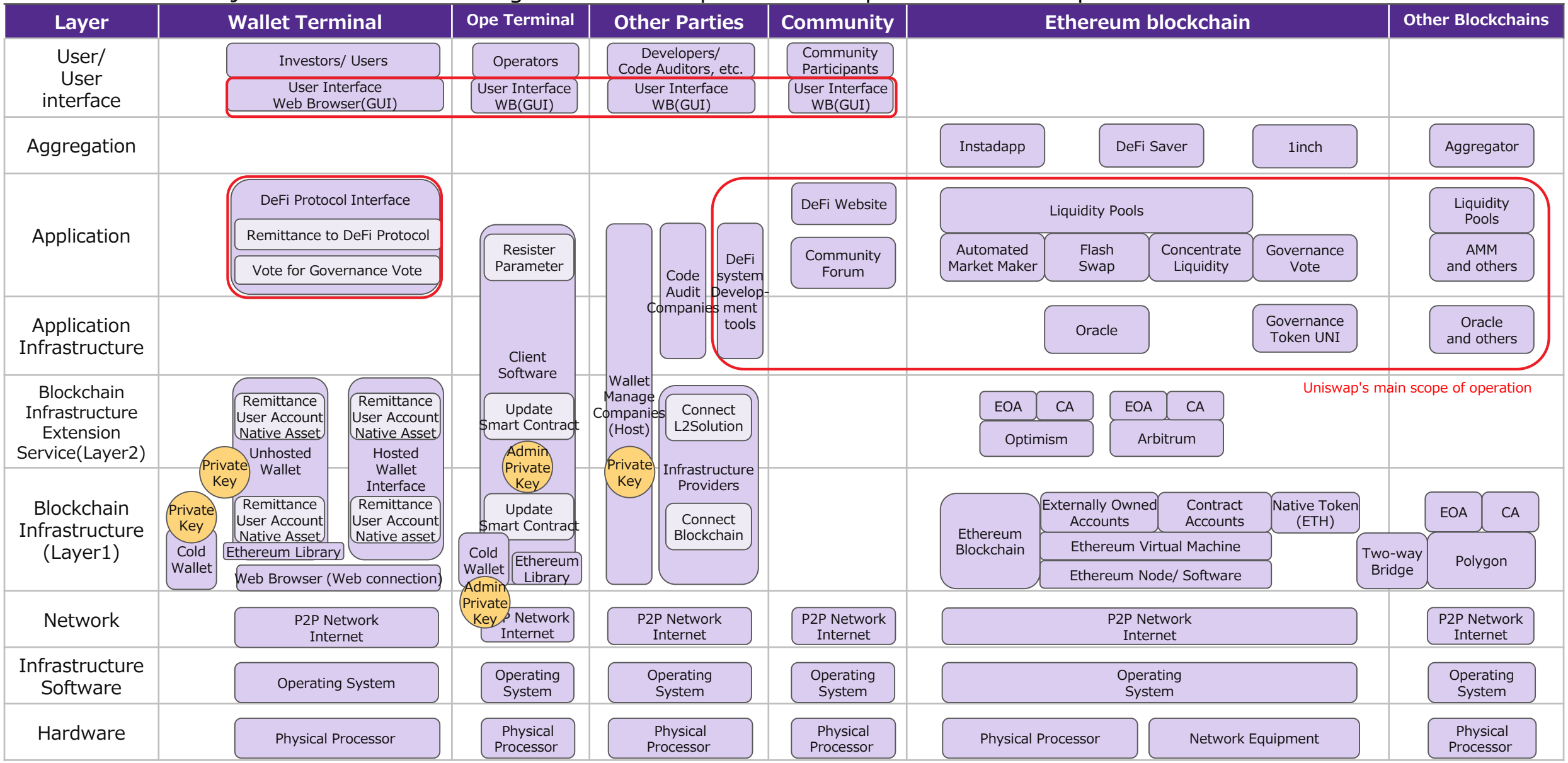



Figure 2-2-1-1 Main components of Uniswap

# 2-2 Analysis of decentralized exchange Uniswap

## 2-2-1 Overall Project Overview

Figure 2-2-1-2 Map of main components of Uniswap



# 2-2 Analysis of decentralized exchange Uniswap

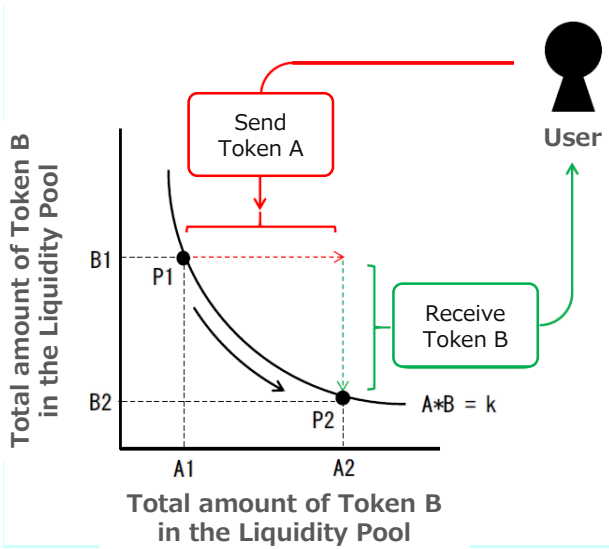
## 2-2-2 Main Technological Characteristics

### (1) AMM (Automated Market Maker)

**Functional Overview**

- ✓ The smart contract automatically calculates the transaction price (exchange rate) based on the amount of crypto-assets deposited in Uniswap's liquidity pool (pairs of crypto-assets to be exchanged).
- ✓ Compared to the order book method that was mainly used in the early DEX, off-chain processing is not required and the order speed is faster. (implemented in Uniswap v1)

**Example: Exchange between Token A and Token B**



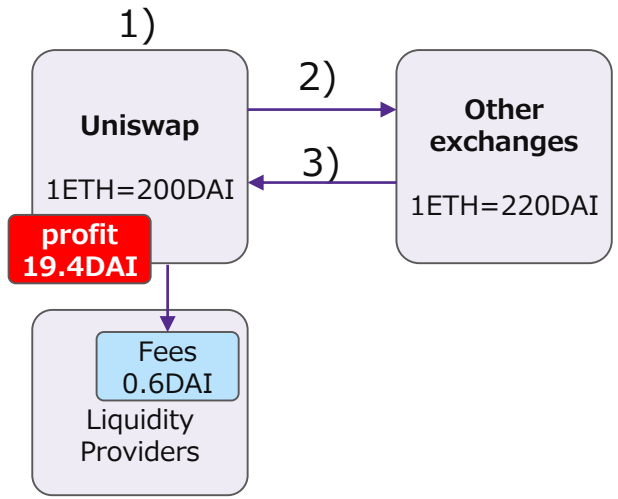

- ➢ Pre-transaction: P1
  Token A1 = 10
  Token B1 = 500
  k = 10*500 = 5,000
- ➢ Post-transaction: P2
  Add 1Token A
  Fee A = 1*0.3% = 0.003
  Token A2
  =10 + 1 - 0.003 = 10.997
  Token B2
  = 5,000 ÷ 10.997 = 454.67
  k = 10.997*454.67=5,000
- ➢ Token B that a user receives
  500-454.67=45.33
- ➢ Liquidity provider receives Fee A
  0.003

### (2) Flash Swap

**Functional Overview**

- ✓ This is a mechanism that allows unsecured withdrawal and use of crypto-asset A in a liquidity pool consisting of crypto-assets A and B, provided that the sum of B and fees equal to A are returned in a single transaction, and is mainly used for arbitrage.
- ✓ If crypto-asset B is not returned, there is no transaction to withdraw crypto-asset A, and the risk of being unsecured is said to be mitigated. (implemented in Uniswap v2)

**Example: Arbitrage transaction without capital**




Execute the following process within one transaction

1) Borrow 1ETH with no collateral

2) Exchange 1ETH for 220 DAI at other exchange

3) Return 200DAI + Fee 0.3%
   Fees 200 * 0.3% = 0.6 DAI
   Profit 220 - 200 - 0.6 = 19.4DAI

*DAI: Maker's crypto-asset type stablecoin

# 2-2 Analysis of decentralized exchange Uniswap

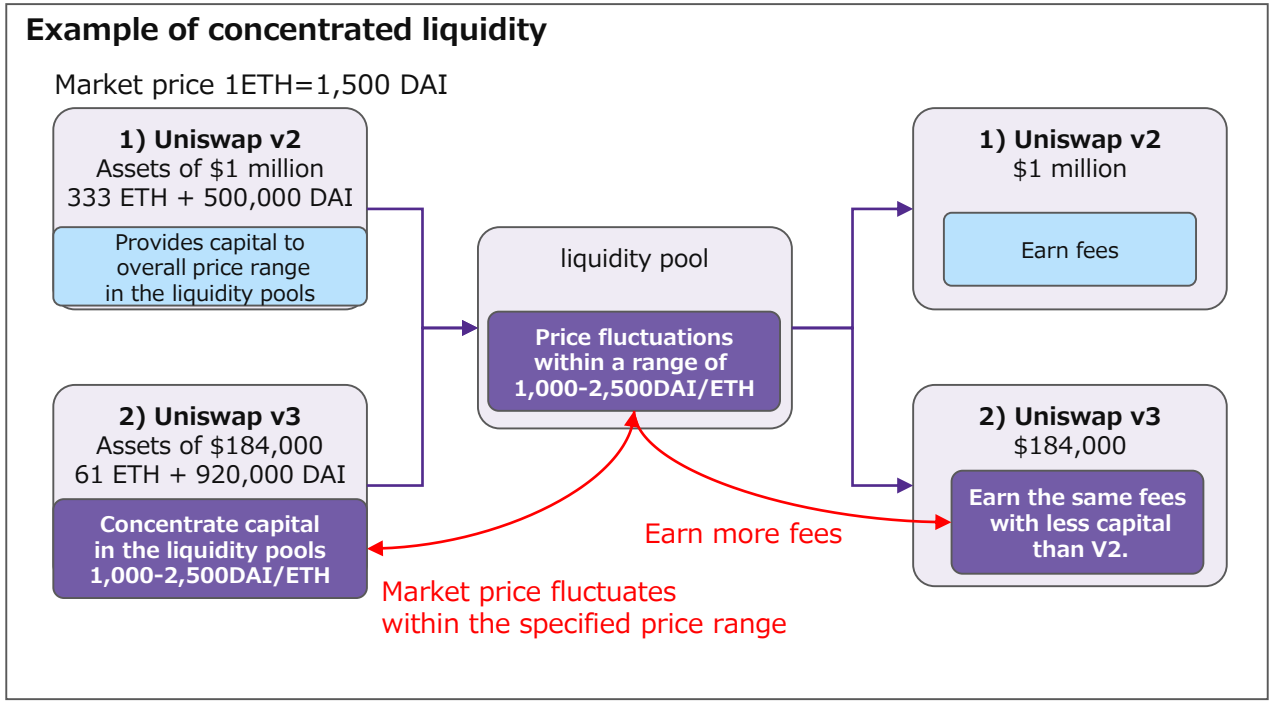
## 2-2-2 Main Technological Characteristics

### (3) Concentrated Liquidity

**Functional Overview**

- ✓ The ability to specify a price range at which liquidity is offered to the liquidity pool for exchange.
- ✓ It is a system that increases the capital efficiency of liquidity providers by specifying a price range for the liquidity pool and concentrating capital (similar to a limit order that specifies an upper and lower price range, and when the market price falls within the range, the pool's crypto-assets are exchanged). Introduced in Uniswap v3, and it is estimated to improve capital efficiency by 4,000x compared to v2.
- ✓ If the market price moves outside of the specified price range, the liquidity of one of the crypto-asset pairs will be depleted and no further commissions will be earned.
- ✓ Liquidity positions for each liquidity provider are formed at different price points and with different liquidity, so liquidity positions are managed with non-alternative tokens (NFT) instead of the traditional alternative token (ERC20). Swap fees were continuously reinvested in the liquidity pool in v1 and v2, but are no longer reinvested from v3.

**Example of concentrated liquidity**




1) Uniswap v2 provides capital to the entire liquidity pool price range
In most liquidity pools, this large portion was never used and had low capital efficiency.
Example: DAI/USDC pair uses only 0.50% of capital for transactions between $0.99 and $1.01, but it is the price range that earns the most commissions.

*USDC (USD Coin): A dollar asset-backed stablecoin issued by Centre

2) Uniswap v3 can provide a concentration of capital to a specified range of liquidity pools
When market prices fluctuate within a specified range, capital is used effectively and capital efficiency is improved.
It is possible to earn more commissions with less capital. In the event of large price fluctuations, v3 has the advantage of offering less capital than v2, resulting in smaller losses.

# 2-2 Analysis of decentralized exchange Uniswap

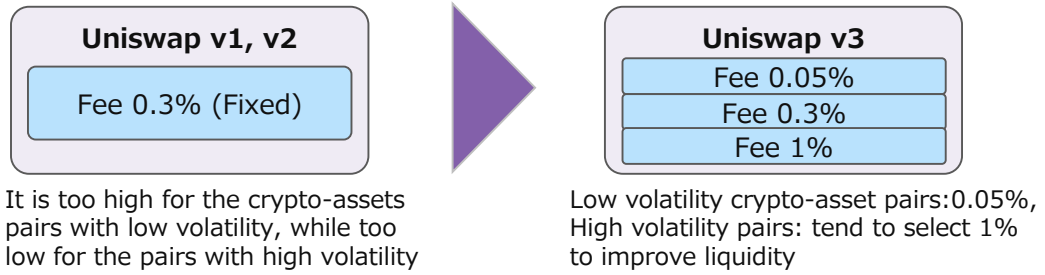
## 2-2-2 Main Technological Characteristics

### (4) Flexible Fees

**Functional Overview**

- ✓ Multiple fee categories offered per liquidity pool and liquidity provider
- ✓ Introduce a protocol fee switch, whereby governance token holders can earn a fee if switched on by governance vote (default is off; currently off as of May 2022)

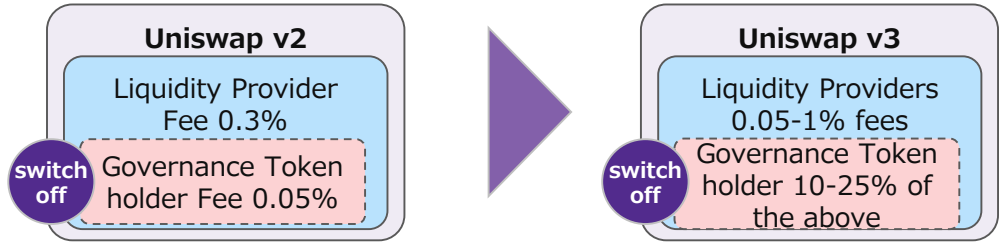
**Multiple Tier Fee**




It is too high for the crypto-assets pairs with low volatility, while too low for the pairs with high volatility

Low volatility crypto-asset pairs:0.05%, High volatility pairs: tend to select 1% to improve liquidity

**Protocol fee switch: Governance voting decides if switch is turned on or not (switch is off by default)**

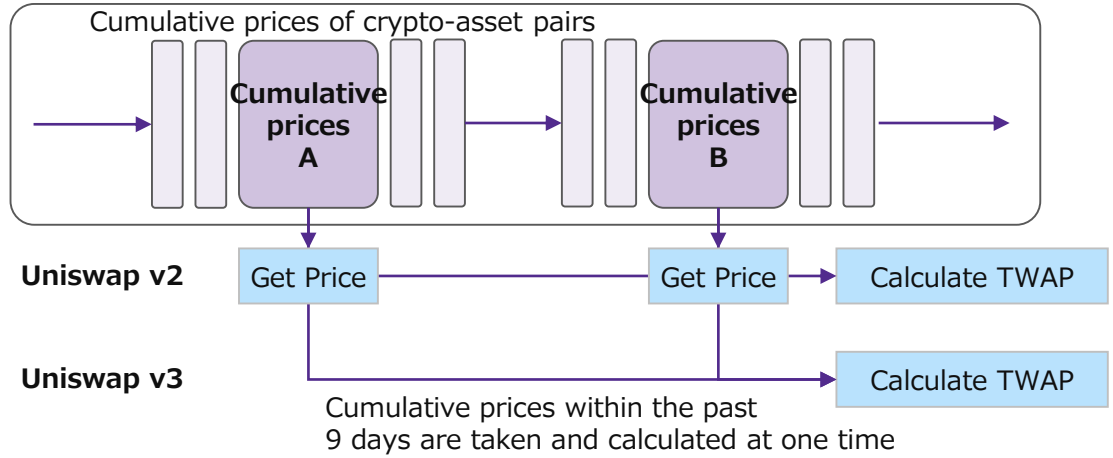



### (5) Advanced Oracles

**Functional Overview**

- ✓ Uniswap v2 : TWAP (Time Weighted Average Price) Oracle
  - ➢ Measure the market price at the start of each block, calculate the cumulative price of any crypto-asset pair from that price and the time required to generate between blocks, and calculate TWAP from the cumulative price and time difference between any two time points
- ✓ Uniswap v3 : TWAP efficiency improvement
  - ➢Efficiently obtain TWAP within the past 9 days, contributing to lower gas fees

**TWAP (Time Weighted Average Price)**



# 2-2 Analysis of decentralized exchange Uniswap

## 2-2-2 Main Technological Characteristics

| Item | Summary | Supplementary information |
|---|---|---|
| (6) Possibility to change smart contracts | 1) Core Contracts<br>✓ Uniswap v1, v2<br>Core contract is not upgradeable by design<br>✓ Uniswap v3<br>Core contract is not upgradeable by design (except for fee parameters) | ✓ Core contract: Critical logic covered, minimal design<br>✓ Liquidity Pool, AMM, Flash Swap, Concentrated Liquidity, Advanced Oracles<br>✓ Since the core contract cannot be upgraded, a different set will be implemented as a new version, and vulnerabilities will be fixed and functionality improved along with it. |
| | 2) External contracts other than core<br>✓ Can be changed, added, or deleted without restriction (including fee changes) | ✓ External contracts outside the core: fees, peripherals, interfaces, governance voting, etc.<br>✓ Uniswap Labs to implement following passage of governance vote |
| (7) License protection for core contracts | Commercial license protection for Uniswap v3 protocol<br>✓ Business Source License 1.1 limits the license to a maximum of two years of v3 source code use in a commercial or production environment.<br>✓ Licensing periods can be changed or waived at any time through a governance vote.<br>✓ Licensed includes Smart Contracts, Math Libraries, Peripheral Contracts, Interfaces, and Developer SDKs<br>✓ Source code can be referenced.<br>✓ Source code was diverted to Sushiswap in an earlier version, but it is said that the purpose is to prevent other diversions for a certain period of time. | ✓ Uniswap Labs, the developer, entrusted the license management authority of the source code to a governance token holder.<br>✓ The case of not making it clear that it is not open source without making it reusable |

# 2-2 Analysis of decentralized exchange Uniswap

## 2-2-3 Governance operations

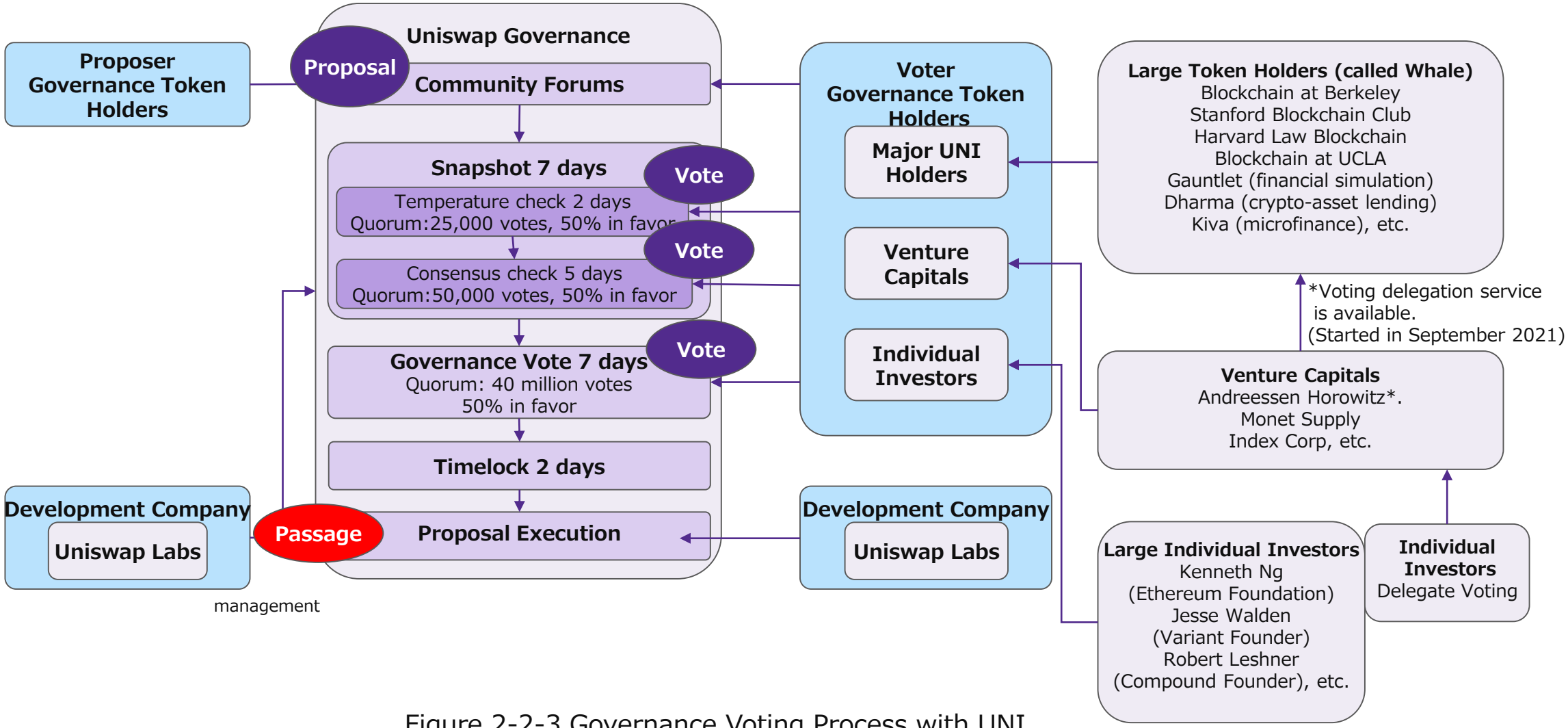
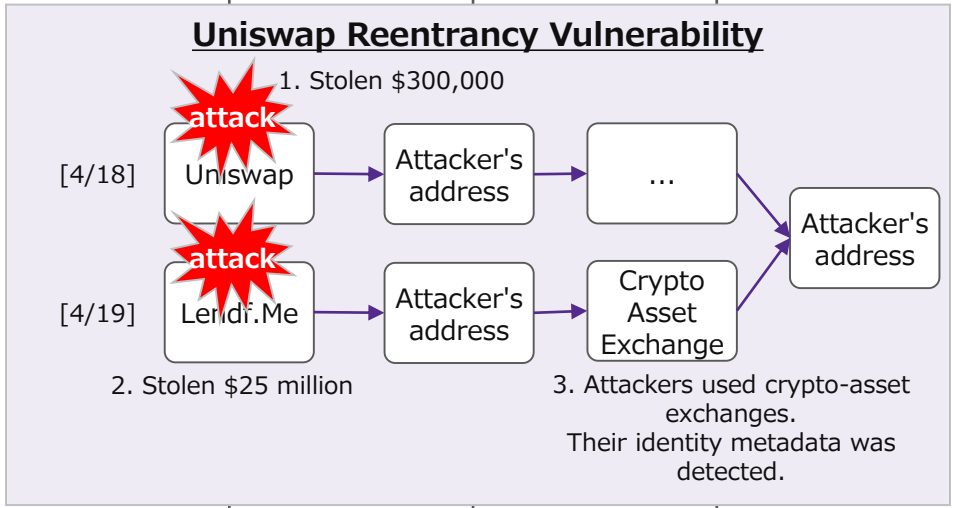



Figure 2-2-3 Governance Voting Process with UNI

# 2-2 Analysis of decentralized exchange Uniswap

## 2-2-4 Incident Cases

| Date of Occurrence | Amount of Damage | Related DeFi | Related Elements | Case Summary | Cause of Occurrence |
|---|---|---|---|---|---|
| April 18, 2020 | Approximately $300,000 | Uniswap<br>Lendf.Me | ERC-777 token | ✓ On April 18, Uniswap was subjected to a reentrancy attack by an attacker who stole approximately $300,000.<br>✓ On April 19, another DeFi protocol, Lendf.Me, was attacked using the same technique, and approximately $25 million was stolen.<br>✓ In the transfer of funds after the Lendf.Me attack, the attacker directly used the services of a crypto-asset exchange, which led to the detection of metadata that could lead to the identification of the attacker. This information allowed Lendf.Me to negotiate with the attacker and 99% of the funds were returned.<br><br><Case flow><br>1. April 18, Uniswap suffered a reentrancy attack and approximately $300,000 was stolen.<br>2. April 19, Lendf.Me was attacked with the same technique and approximately $25 million was stolen.<br>3. April 19, Attacker directly used the services of a crypto-asset exchange during a fund transfer and metadata of the attacker's identity was detected<br>4. April 21, Identity of attacker revealed, Lendf.Me negotiated, 99% of funds returned<br><br><Stolen funds and crypto-assets><br>✓ Uniswap about $300,000 imBTC, ETH<br>✓ Lendf.ME About $25 million WETH, USDT, HBTC, imBTC and 12 others in total | Due to reentrancy vulnerabilities in Uniswap and Lendf.Me smart contracts<br>✓ There was a reentrancy vulnerability due to the lack of ERC-777 token support.<br>✓ crypto-assets were received by abusing the approval request function of the ERC777 token and re-calling it during the processing of the crypto-asset exchange. |



# 2-2 Analysis of decentralized exchange Uniswap

2-2-4 Incident Cases

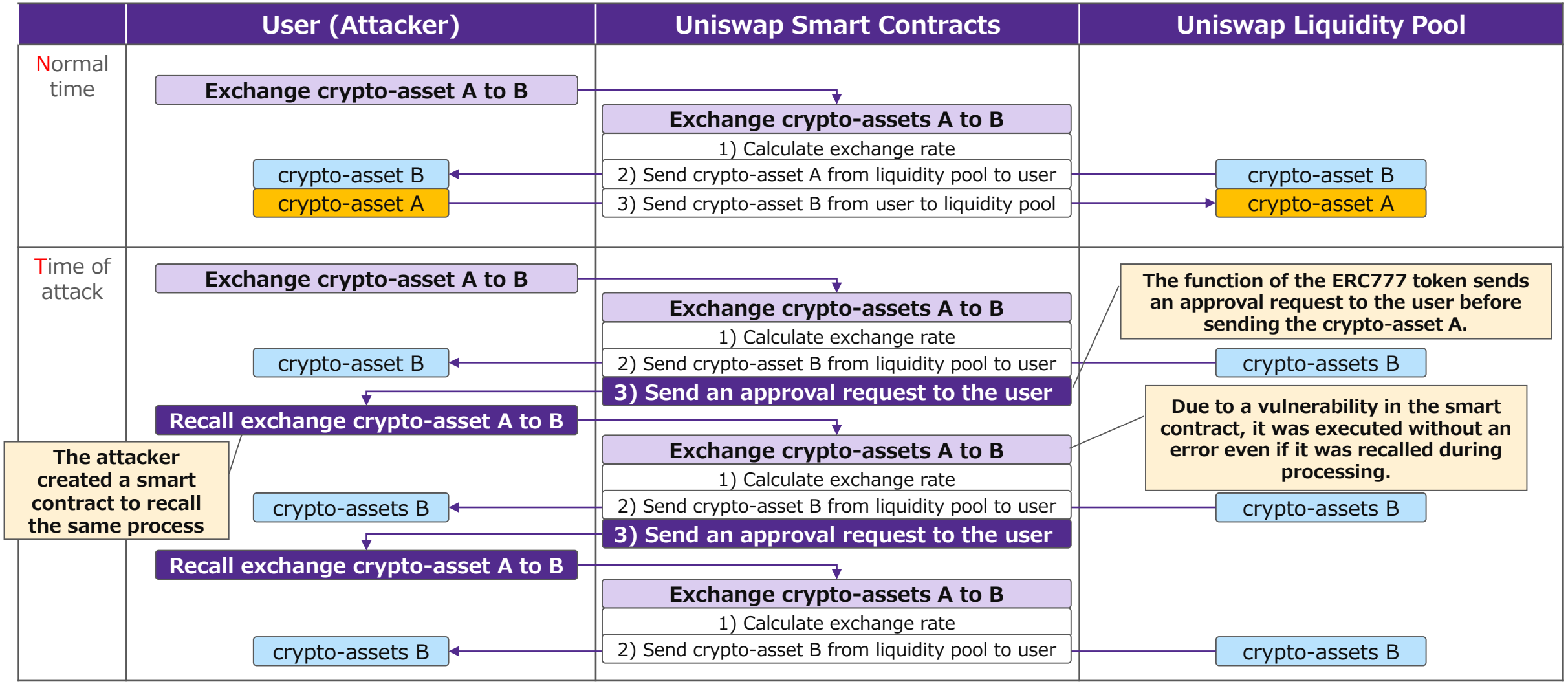
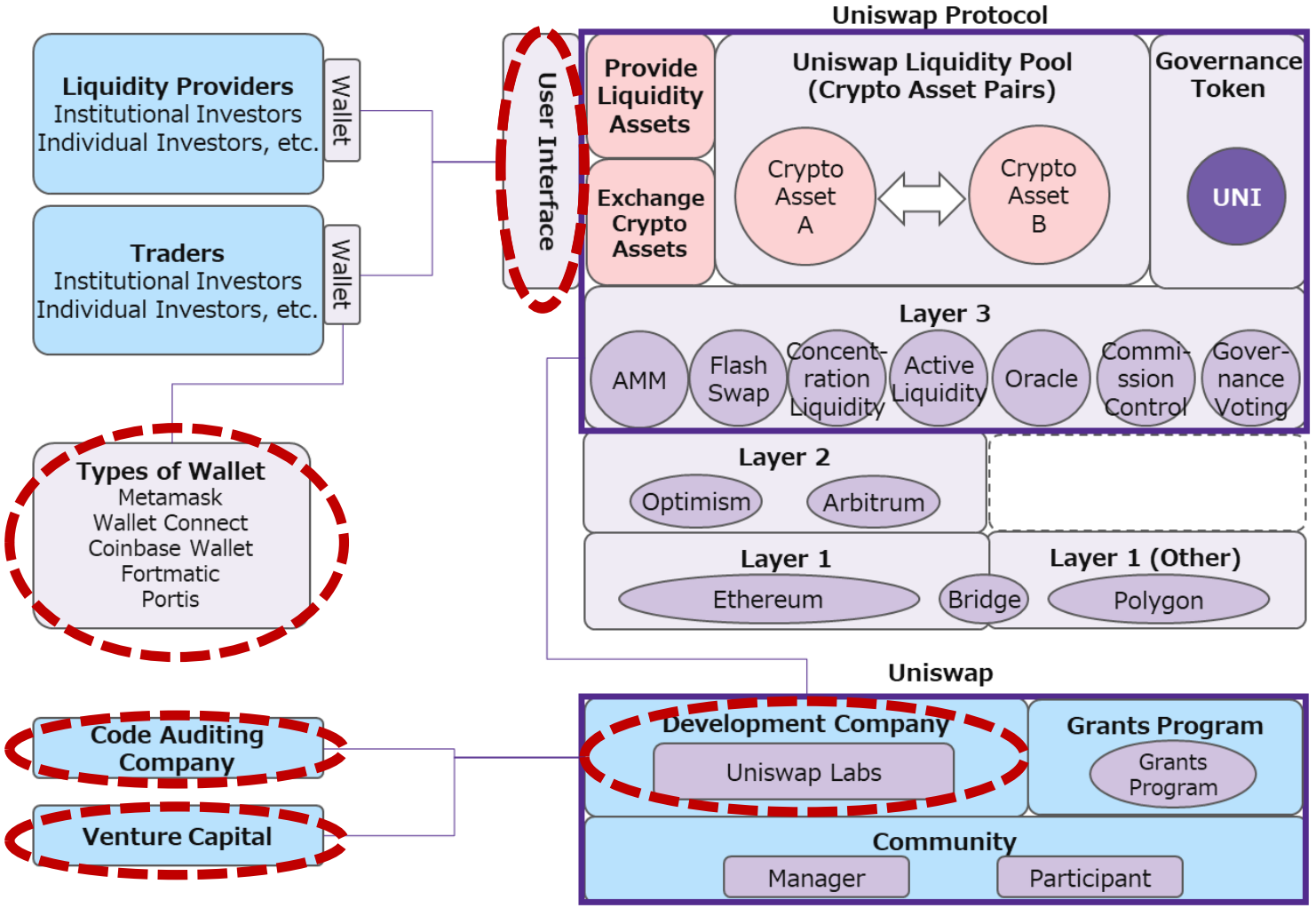



Figure 2-2-4 How the Uniswap Reentrancy Vulnerability Works

# 2-2 Analysis of decentralized exchange Uniswap

## 2-2-5 Uniswap's Main Trust Points

- ✓ Uniswap Labs (US-based development team) provides user interface (website) for token exchange
- ✓ Other trust points: wallet providers, code auditing firms, VCs (large holders of governance tokens)




Considered to be trust point

Figure 2-2-5-1 Main trust points in Uniswap

# 2-2 Analysis of the decentralized exchange Uniswap

## 2-2-5 Uniswap's Main Trust Points

✓ Large governance token holders, including venture capitalists who received approximately 18% of UNI as initial investors, can be considered to have a strong influence on decision making.

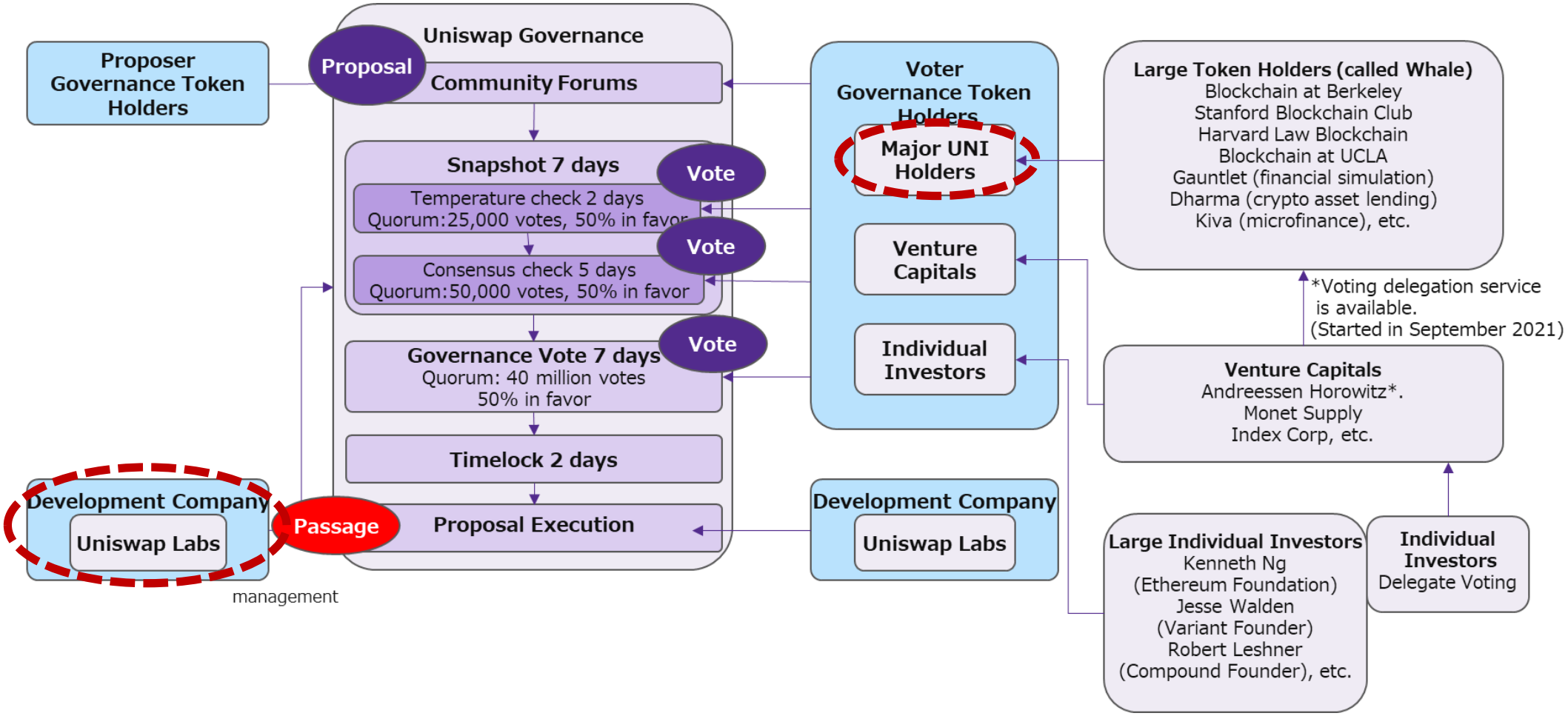



Figure 2-2-5-2 Main Trust Points in Uniswap (Governance Voting)

# 2-3 Analysis of Stablecoin Maker (DAI)

## 2-3-1 Project Overview

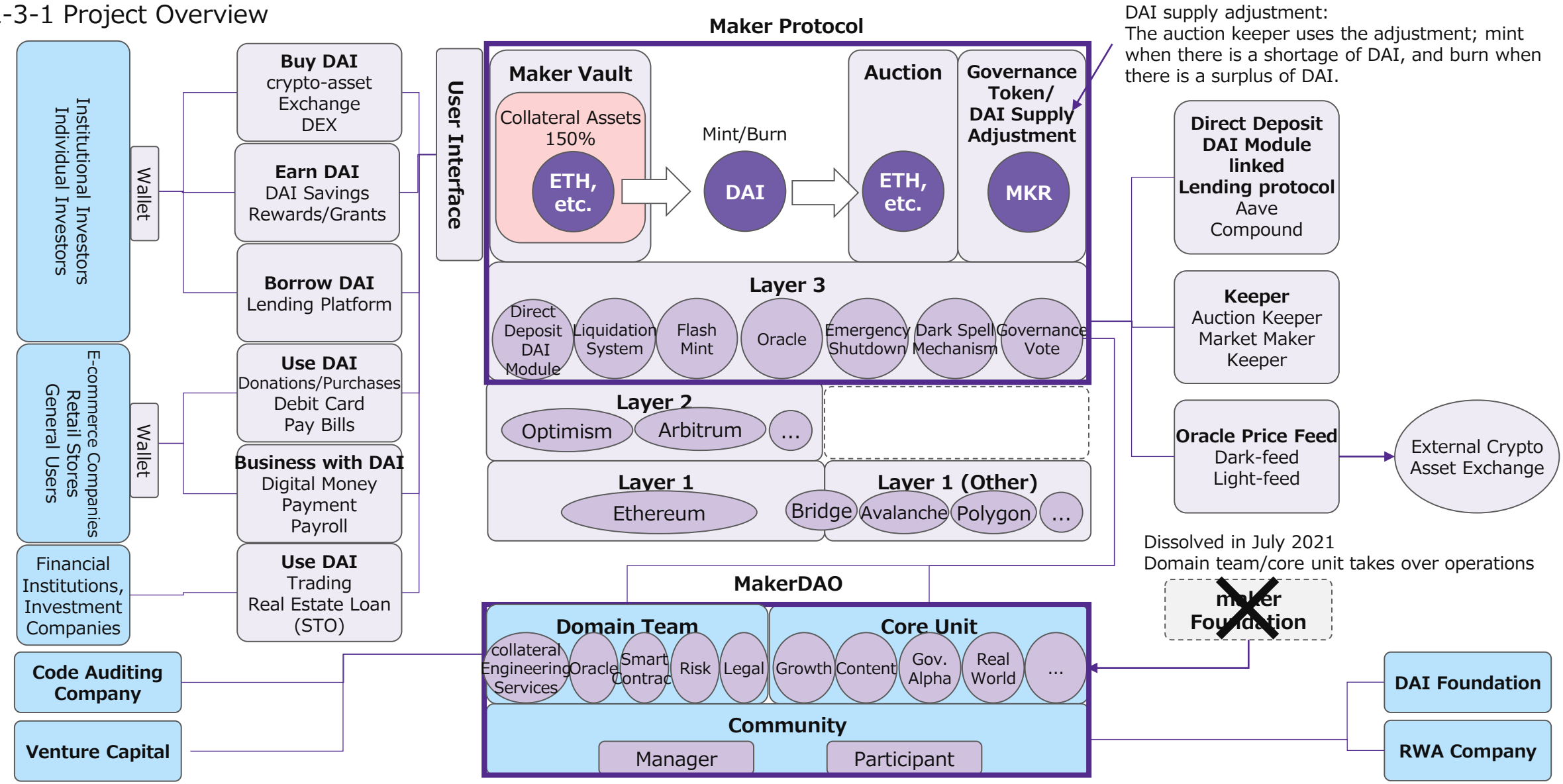
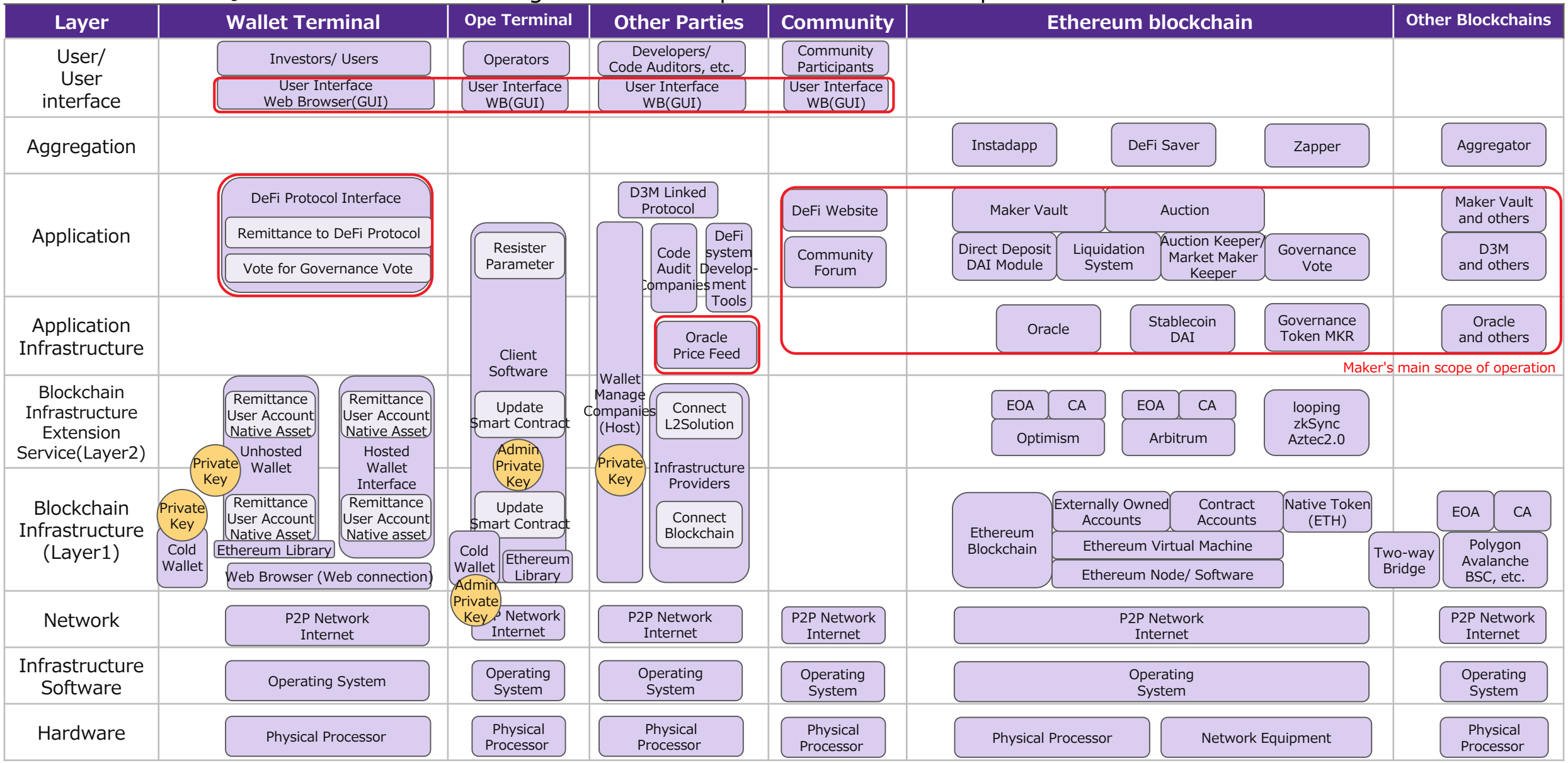



Figure 2-3-1-1 Main components of Maker

# 2-3 Analysis of Stablecoin Maker (DAI)

## 2-3-1 Overall Project Overview

Figure 2-3-1-2 Map of Maker's main components



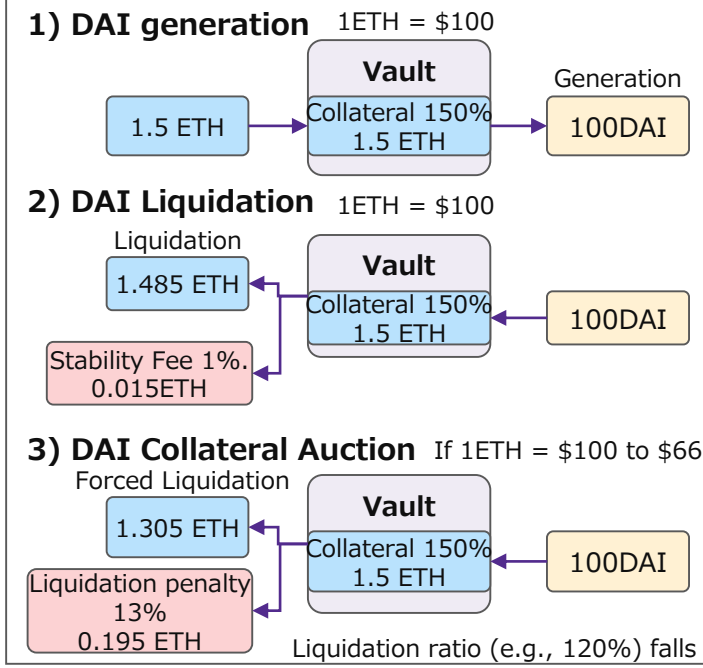
# 2-3 Analysis of Stablecoin Maker (DAI)

## 2-3-2 Main Technological Characteristics

### (1) Maker Vault

**Functional Overview**

- ✓ Stablecoin DAI is generated by depositing collateral assets (crypto-assets such as ETH or stablecoins such as USDC) into the Maker Vault contract
- ✓ A Stability Fee is charged when DAI is returned. If the fee exceeds the threshold, the DAI and MKR are exchanged at the Surplus Auction, and the MKR used for bidding is burned.
- ✓ Interfaces built by Oasis and the community (Instadapp, Zerion, MyEtherWallet, etc.) makes it easy to access to the Maker Vault.
- ✓ If the value of collateral falls below the liquidation ratio due to a decline in the value of collateral or other reasons, the collateral is automatically (compulsorily) liquidated through a Collateral Auction.




1) DAI generation
Put 150% collateral assets in Vault to generate DAI.

2) DAI liquidation
Buy collateral in Vault and return assets after stabilization fees deducted.

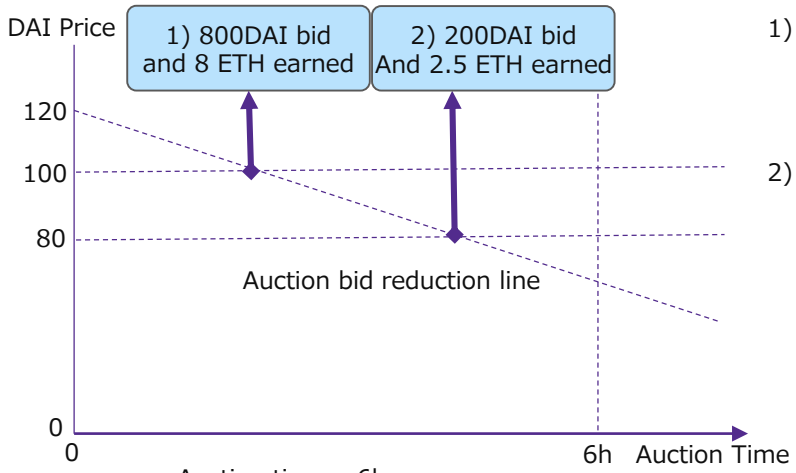
3) DAI collateral auction
If the collateral falls below the liquidation ratio due to the collateral is forced to be liquidated after the liquidation penalty deducted.

### (2) Liquidation System 2.0

**Functional Overview**

- ✓ When the collateral ratio falls below a predetermined level and the Vault is forced into liquidation, the collateral assets deposited in the collateral-deficient Vault are auctioned to liquidate the liabilities (DAI). Auction participants acquire collateral assets by bidding for DAI.
- ✓ New liquidation mechanism for Dutch auction method launched.
- ✓ Allows partial bids and allows one or more bidders to split the auction amount by dividing the asking price to purchase the collateral.
- ✓ Support for Flash Loan, which allows participants to participate in auctions by borrowing and repaying at the same time, even if they do not have the original funds.

**Liquidation System 2.0** Liquidation auction for 1,000 DAI




1) After the auction begins at 1 ETH = 100 DAI, Bid 800 DAI and 8 ETH earned.

2) Then, at the time of 1 ETH = 80 DAI, bidding 200 DAI and 2.5 ETH earned.

Auction time : 6h
Auction start buffer : 120%.
1 ETH = 100 DAI
*1 hour later than actual market price due to use of oracle price

# 2-3 Analysis of Stablecoin Maker (DAI)

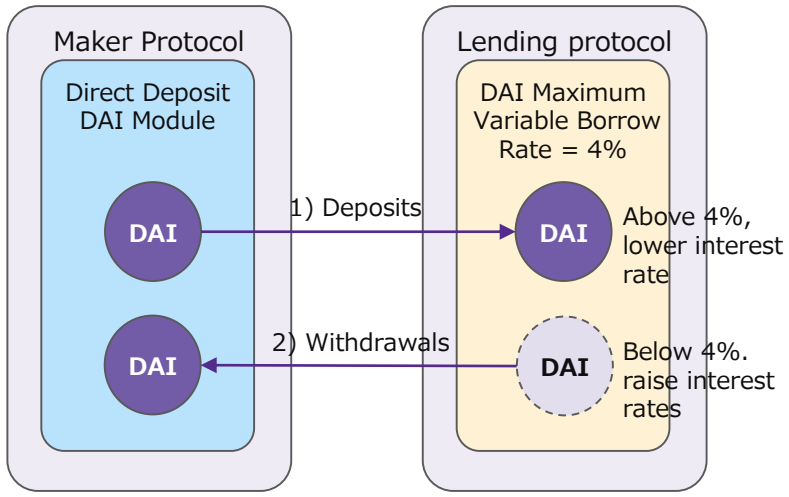
## 2-3-2 Main Technological Characteristics

### (3) Direct Deposit DAI Module (D3M)

**Functional Overview**

- ✓ A mechanism that works in conjunction with third-party lending protocols to efficiently transfer DAI to the liquidity pool of such protocols, thereby adjusting the variable interest rate of DAI to be below the target interest rate determined by Maker governance (governance vote).
- ✓ Automatically deposit/withdraw DAI to ensure target interest rates are met.
- ✓ Already applied to Aave and Compound; application to Maple under consideration (under vote) (as of March 2022).

**Direct Deposit DAI Module**




Maximum borrow variable rate is applied for each selected asset.

1) In case of high demand for DAI
If the DAI maximum variable borrow rate exceeds the target, lower the interest rate.

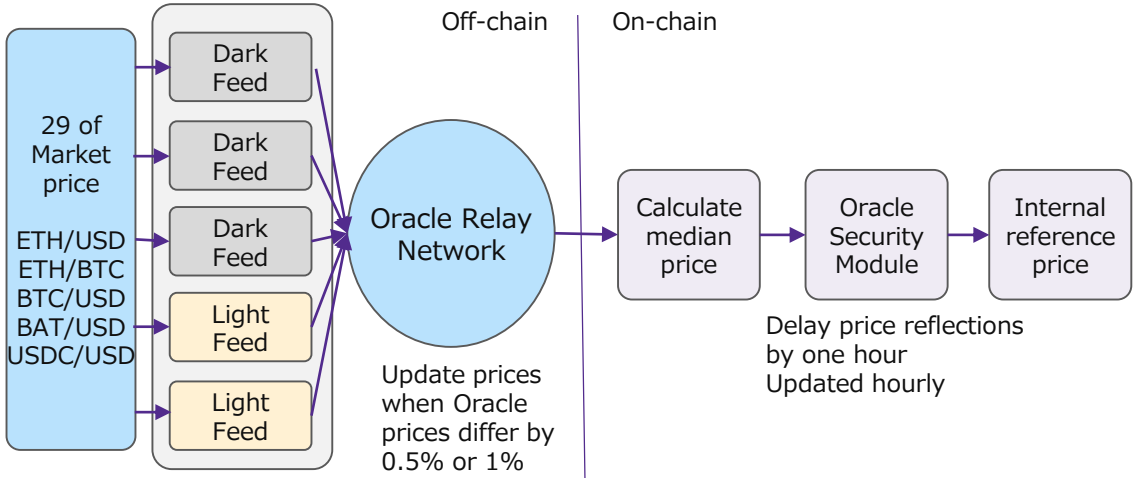
2) In case of low demand for DAI
If the DAI maximum variable borrow rate falls below the target, raise the interest rate.

### (4) Oracle management

**Functional Overview**

- ✓ The Maker protocol calculates the median price of the required market price (e.g. ETH/USD) from a set of prices received from the Oracle price and determines the reference price required for DAI issuance, collateral clearing, etc. Determination of reference prices required for DAI issuance, collateral liquidation, etc.
- ✓ The Oracle Security Module (OSM) intentionally delays price reflection by one hour to respond to sudden market fluctuations and oracle.

**How the Oracle price calculation works**




<Oracle Price Feed>
Dark feeds: BOTs run by anonymous individuals (15 feeds as of April 2022)
Light Feed: BOTs executed by published organizations (9 feeds as of April 2022)
dYdX, KyberNetwork, Infura, Etherscan, etc.
Calculate median price of 20 feeds (quorum 13 feeds)

# 2-3 Analysis of Stablecoin Maker (DAI)

## 2-3-2 Main Technological Characteristics

| Item | Summary | Supplementary information |
|---|---|---|
| (5) Maker Protocol Auctions | 1) Surplus Auction<br>If DAI exceeds the Maker buffer limit, the excess DAI is used to purchase MKR tokens as surplus to reduce the amount of MKR tokens<br>2) Debt auctions<br>When DAI is insufficient for outstanding obligations, MKR tokens are issued and sold to bidders to secure DAI<br>3) Collateral auction<br>Forced liquidation of collateral by charging a liquidation penalty in the event of collateral shortages due to falling token prices, etc. | - |
| (6) Keeper | ✓ Keepers are external agents (mainly BOTs) that run automatically for arbitrage according to an algorithm<br>✓ Market Maker Keeper<br>➢ DAI will be sold when DAI is above the target price (1USD) and DAI will be purchased when DAI is below the target price. 24 designated exchanges (Binance, Coinbase, etc.) can build keepers<br>✓ Auction Keeper<br>➢ Participate and bid in surplus, debt, and collateral auctions | ✓ Market Maker Keeper automatically executes trades by referencing the market price on the designated exchange. |
| (7) Flashmint | ✓ DAI can be created under the condition of borrowing and returning (including fees) in one transaction.<br>✓ Arbitrage opportunities available with no collateral required | ✓ There is a debt limit (DAI/ETH: 15 billion ETH, etc.) |
| (8) DAI Savings Rate (DSR) | ✓ Any DAI holder can earn interest on their savings.<br>✓ Access via Oasis Save Portal or Maker Protocol Gateways<br>✓ The parameters that determine the amount of money a DAI holder gets are determined by on-chain governance<br>✓ If DAI exceeds 1 USD, MKR holders lower their DSR; if DAI is less than 1 USD, MKR holders raise their DAI. | - |

# 2-3 Analysis of Stablecoin Maker (DAI)

## 2-3-2 Main Technological Characteristics

| Item | Summary | Supplementary information |
|---|---|---|
| (9) GSM (Governance Security Module) | ✓ The GSM allows for a certain amount of time to wait for code amendments and other actions after a proposal is passed by a governance vote.<br>✓ Review changes made to the system and, if those changes are deemed malicious, respond with a proposal cancellation (likely to be implemented by the core team) or an Emergency Shutdown (voted on by MKR holders) during the GSM delay time | ✓ GSM delay time is 48 hours (as of January 2022) |
| (10) Dark Spell Mechanism | ✓ Mechanisms for modifying smart contracts to fix critical vulnerabilities<br>✓ Apply protocol fixes without downtime<br>✓ Work Process<br>1) Darkspell (modified code) developed by MakerDAO's Smart Contract Domain team. (Code is kept secret until the correction takes effect to prevent reverse engineering to read the contents during the on-chain voting and GSM delay period before the correction code is applied.)<br>2) Communicate dark spells to certain members in the community and trusted third parties.<br>3) Trusted third party quickly coordinates discussions and recognizes votes.<br>4) Trusted third party directs the governance facilitator to schedule a voting.<br>5) Wait for GSM delay period after voting is scheduled and passed.<br>6) Apply the code modification after the GSM delay period has elapsed.<br>7) Trusted third party and smart contract domain team to create a darkspell post-mortem analysis and publish it to the entire community. | ✓ Interested parties<br>➢ Smart Contract Domain Team<br>➢ Governance Facilitator<br>➢ Trusted Third Party (selected by on-chain voting. Currently not registered)<br>➢ Certain members of the Maker community (not to be disclosed)<br>✓ A different process than regular governance and executive voting<br>➢ Voting time is set to 24 hours (fixed)<br>➢ No quorum or threshold for passage of the vote is defined. |

# 2-3 Analysis of Stablecoin Maker (DAI)

## 2-3-2 Main Technological Characteristics

| Item | Summary | Supplementary information |
|---|---|---|
| (11) Emergency Shutdown | ✓ Ability to shut down the Maker protocol to protect it from malicious attacks or to facilitate Maker protocol upgrades.<br>✓ MKR holder deposits MKR in the Emergency Shutdown Module (ESM), which is immediately executed when the threshold is exceeded.<br>✓ Execution is done in 3 phases, followed by redeployment depending on the cause of the outbreak<br>1) Maker protocol shutdown<br>Oracle Price Feed Frozen, Vault Owners Withdraw Assets<br>2) Auction processing after emergency stop<br>After the shutdown starts, forced clearing by collateral auction starts, and the protocol stops after all auctions are completed.<br>3) DAI holder claims the remaining collateral<br>DAI holders claim collateral directly at a fixed rate<br>Vault holders have priority over DAI holders<br>4) Redeploy protocols according to the nature of the attack<br>➢Governance Attacks<br>Disable the attacker and redeploy with everything else intact<br>➢Oracle Attack<br>Fix the oracle module and redeploy with everything else intact<br>➢Black Swan Event<br>Redeploy with new improvements<br>➢Unreasonable emergency shutdown<br>Disable the attacker and redeploy with everything else intact | ✓ Threshold for initiating emergency shutdown is 75,000 MKR (as of January 2022)<br>✓ Black Swan Event: A Major Surprise Attack<br>✓ Difficult to prepare countermeasure, such as Oracle attacks and other highly coordinated external price manipulation, and there is no direct workaround |

# 2-3 Analysis of Stablecoin Maker (DAI)

## 2-3-3 Governance operations

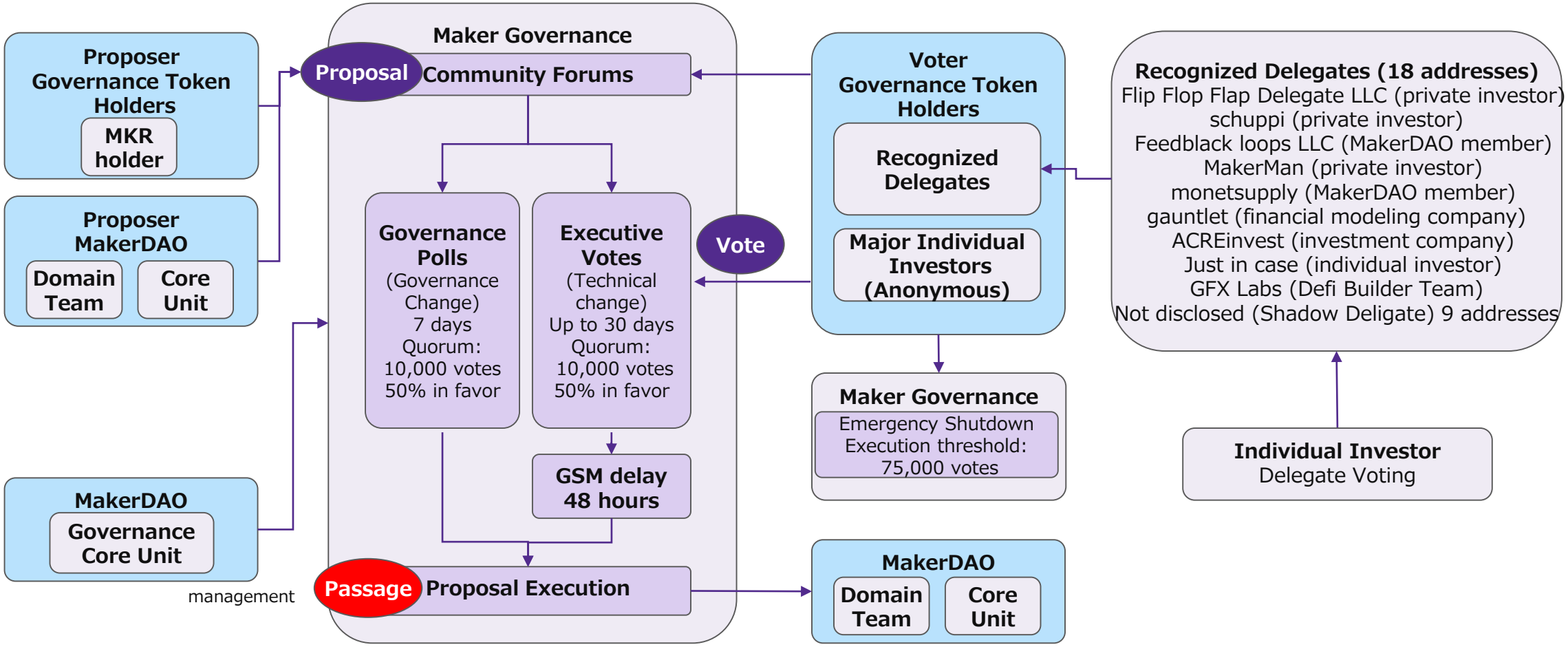
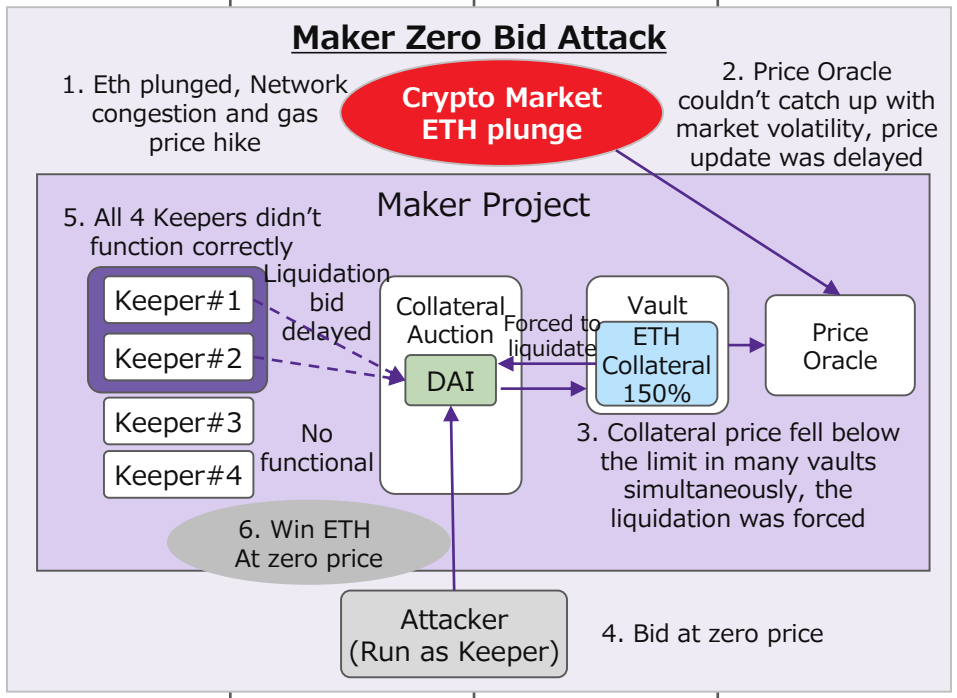



Figure 2-3-3 Governance Voting Process with MKR

# 2-3 Analysis of Stablecoin Maker (DAI)

## 2-3-4 Incident Cases

| Date of Occurrence | Amount of Damage | Related DeFi | Related Elements | Case Summary | Cause of Occurrence |
|---|---|---|---|---|---|
| March 12, 2020 | Approximately $8.32 million | Maker | Ethereum<br>Oracle<br>DAO<br>Stablecoin | The company lost approximately $8.32 million worth of ETH due to zero bidding after it was attacked for a weakness that prevented proper bidding when Maker's collateral forced liquidation occurred due to network congestion and gas fee spikes caused by the ETH price collapse.<br><Case flow><br>1. Black Thursday (stock market crash due to COVID-19 and the U.S. travel ban etc.) caused crypto-assets such as ETH to plunge (ETH: $194 to $111, a 43% drop); transactions on Ethereum spiked, causing network congestion and a spike in gas prices.<br>2. Due to the above, Maker's Price Oracle was unable to update prices and delayed; it could not keep up with the market price of ETH, resulting in a delay in the reflection of the reference price.<br>3. Subsequently, the price oracle was updated at once, resulting in a drop of approximately 20% in the price of ETH within Maker. A large number of Vaults experienced ETH collateral shortages, and a forced liquidation (collateral auction) of approximately 1,200 Vaults was executed.<br>4. In the collateral auction, the attacker set up a "zero bid" (exchanged DAI at zero value for ETH).<br>5. Due to forced liquidation, four keepers submitted DAI purchase bids for liquidation, but all four did not function properly and failed to submit bids.<br>✓ Keeper#1, #2 Due to gas price spike, bid transaction was not processed within the time limit (10 minutes).<br>✓ Keeper#3 Maker Foundation operated the system, but it did not work due to technical problems caused by network congestion.<br>✓ Keeper#4 DAI to be cleared was exhausted and processing stopped for several hours. | ✓ Gas price spike in Ethereum due to the ETH price collapse, which exploited the fact that any Keeper was not working properly to set up a zero bid.<br>✓ Post-incident investigations suggested that the Ethereum network congestion may have been deliberate due to a large number of meaningless transactions, and that the attackers may have created a gas price spike that prevented Keeper from working properly, thus creating a zero-bid attack. |



# 2-3 Analysis of Stablecoin Maker (DAI)

## 2-3-4 Incident Cases

| Date of Occurrence | Amount of Damage | Related DeFi | Related Elements | Case Summary | Cause of Occurrence |
|---|---|---|---|---|---|
| - | - | - | - | 6. The attacker made zero bids (bids to purchase ETH at zero DAI) and all four keepers did not work, so the attacker won the bids and stole a total of $8.32 million worth of ETH. (Of the 4,447 auction bids made by Keeper and attackers, 1,462 were zero bids.)<br>7. Conducted a Maker Protocol debt auction on March 19 to eliminate the $5.4 million collateral shortfall created by the zero bid by issuing additional MKRs (as of March 29, 20,980 MKRs were generated and 5.3 million DAI were provided) | - |

# 2-3 Analysis of Stablecoin Maker (DAI)

2-3-5 Maker's main trust points

- ✓ The Maker Foundation, once the center of community management, was dissolved last year, and MakerDAO is now primarily responsible for its operations.
- ✓ Certain trust points will continue to exist: Keepers (external agents working for arbitrage), affiliated legal entities (e.g., DAI Foundation), Domain Teams (teams within the community that exist to manage the Maker protocol, etc.), etc.

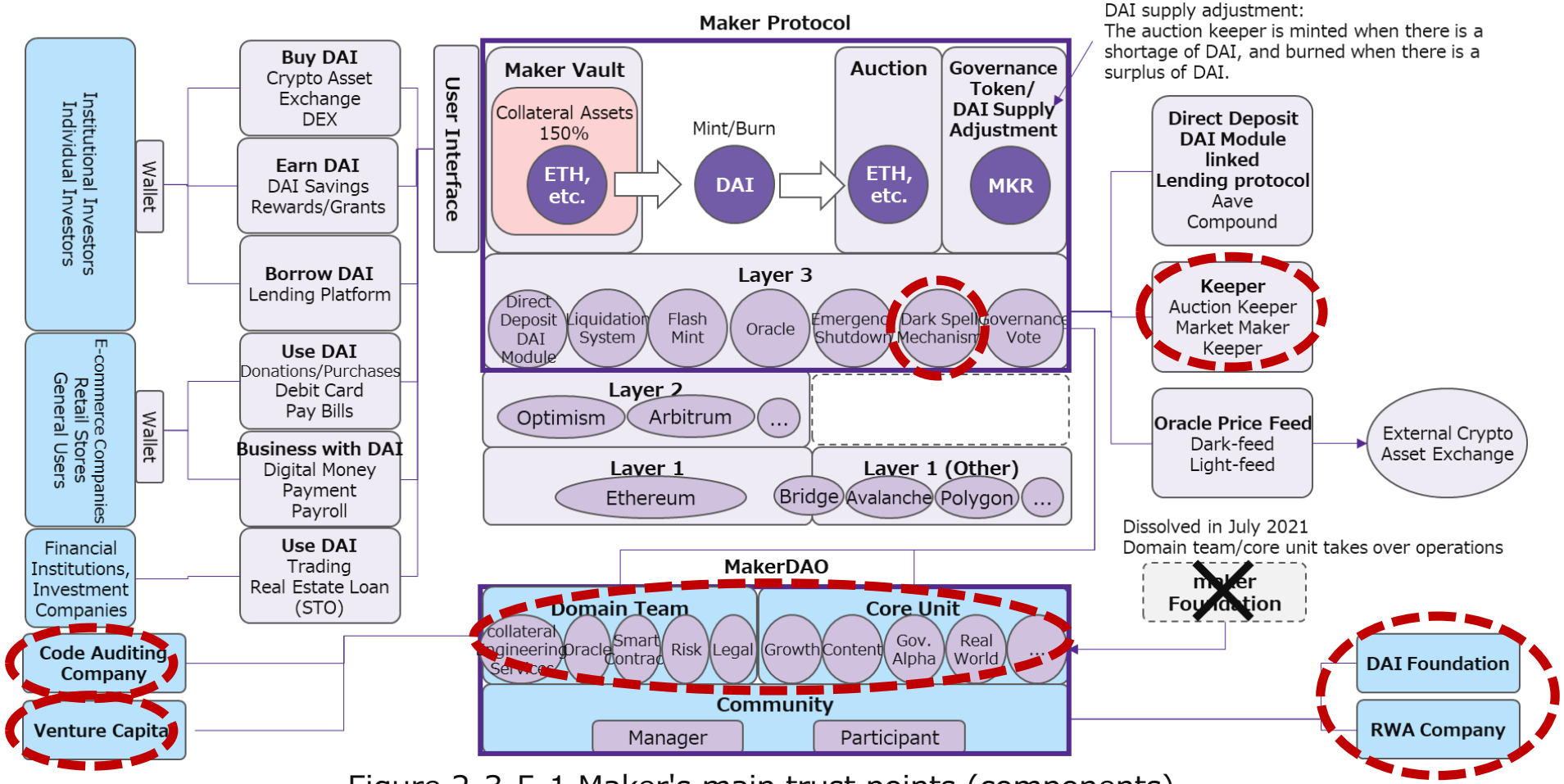



Figure 2-3-5-1 Maker's main trust points (components)

# 2-3 Analysis of Stablecoin Maker (DAI)

2-3-5 Maker's main trust points

- ✓ Large governance token holders, composed of a small number of voting proxies, have a strong influence on decision making
- ✓ MakerDAO Domain Teams and Core Units are involved to a certain extent in each stage of governance proposal, voting, and proposal implementation

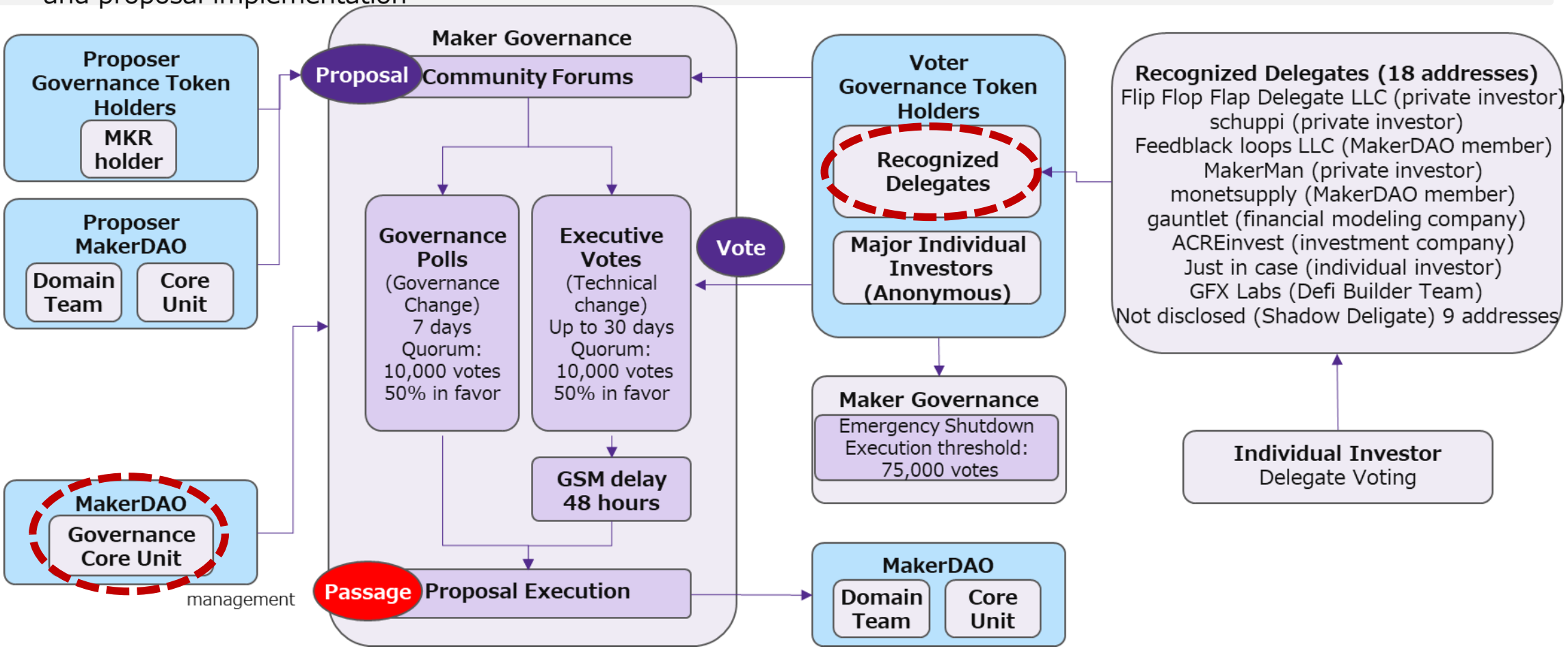



Figure 2-3-5-2 Maker's Main Trust Points (Governance Voting)

# 2-4 Analysis of Lending Aave

## 2-4-1 Overall Project Overview

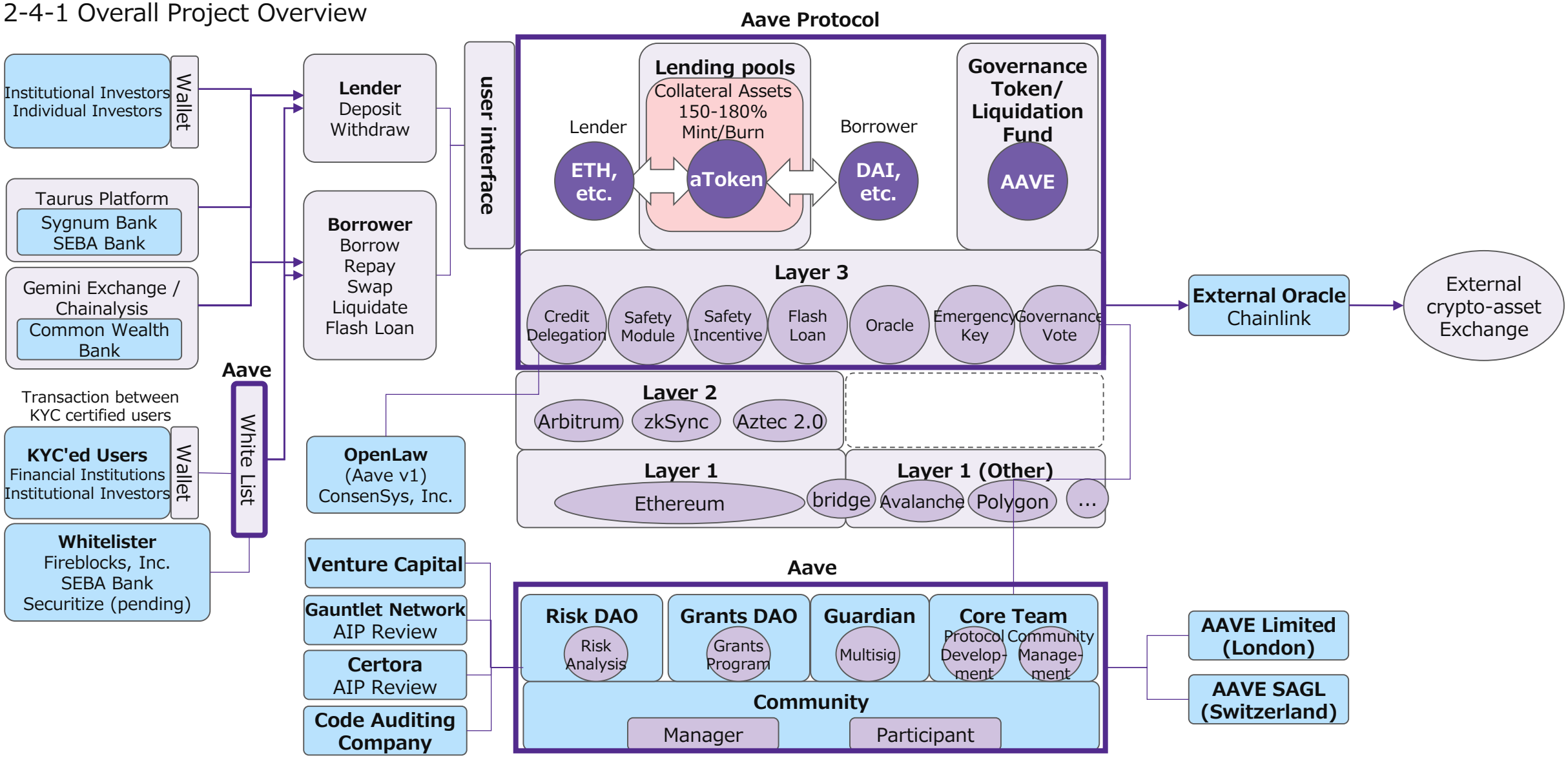
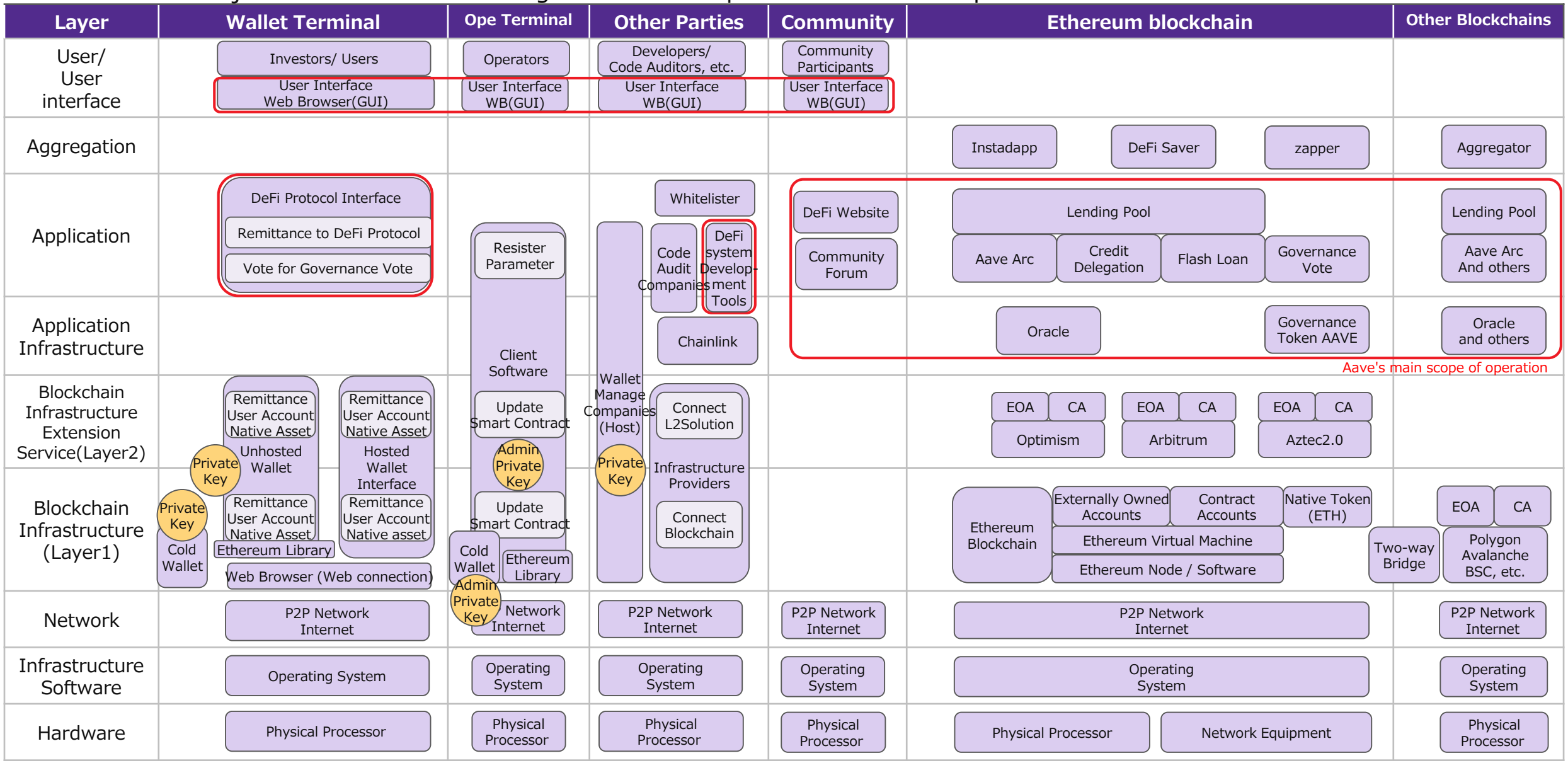



Figure 2-4-1-1 Main components of Aave

# 2-4 Analysis of Lending Aave

## 2-4-1 Overall Project Overview

Figure 2-4-1-2 Map of Aave's main components

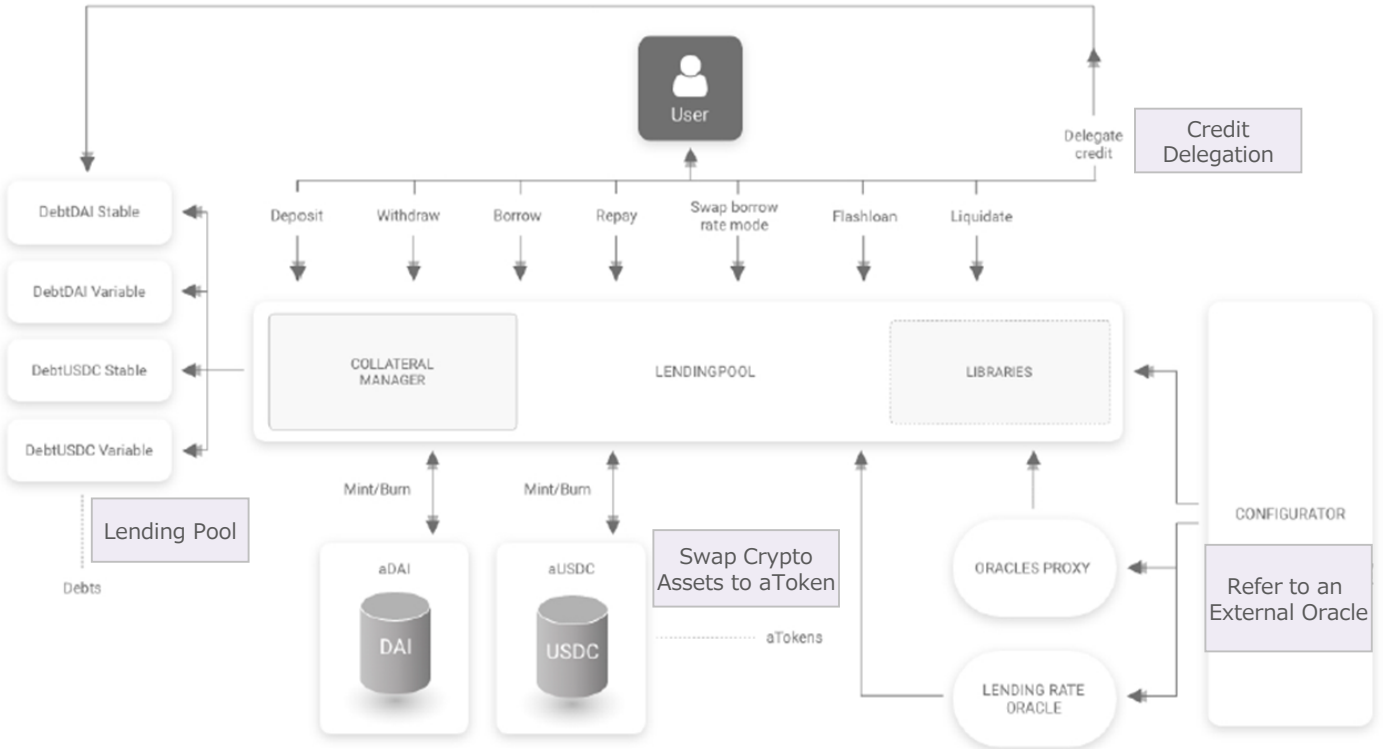


# 2-4 Analysis of Lending Aave

## 2-4-2 Main Technological Characteristics　(1) Overall view of the protocol

**Functional Overview**

- ✓ Users (individuals, institutions, etc.) can earn interest by depositing crypto-assets (including some stablecoins) into the Aave protocol's lending pool (smart contracts), and can borrow from the pool on the condition that they deposit the prescribed collateral assets. (As of January 2022, more than 30 crypto-assets and stablecoins including ETH, LINK, USDT, and AAVE are supported).
- ✓ When crypto-assets are deposited into the Lending Pool, the pool receives aToken (e.g., aETH) with the initial letter "a" of the crypto-asset on a 1:1 basis, and the proceeds earned by the pool is distributed to the aToken holders. The aToken is burned when the crypto-asset is withdrawn.
- ✓ crypto-asset prices refer to an external oracle (Chainlink) .
- ✓ Lending and borrowing rates are calculated systematically by referencing the oracle.
- ✓ Liquidation occurs if collateral asset prices decline at the time of borrowing.
- ✓ The user who deposited the crypto-assets can assign a line of credit secured by the crypto-assets to another party, and the assignee can borrow without collateral (credit delegation). In return for the credit risk, the transferor (Delegator) receives additional revenue.



# 2-4 Analysis of Lending Aave

## 2-4-2 Main Technological Characteristics

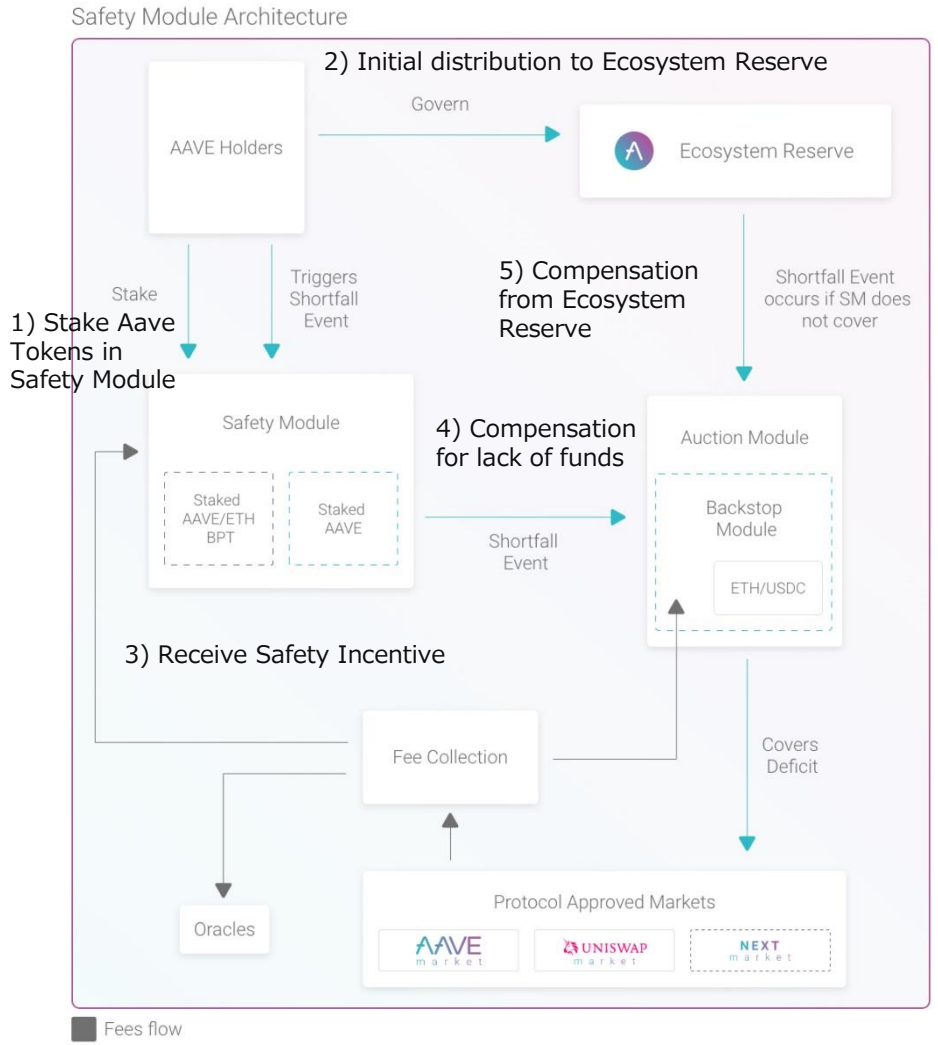
### (2) Safety Module/ Safety Incentive

**Functional Overview**

- ✓ Safety Module (SM): A mechanism to compensate for a large amount of liquidation from AAVE tokens staked voluntarily by users for the purpose of resolving the protocol's insolvency.
- ✓ Safety incentive (SI): A system whereby a fee is earned in exchange for staking out SMs.

**Details of Safety Module/ Safety Incentive**

| # | Description |
|---|---|
| 1) | The AAVE token holder stakes (locks) the AAVE token in the SM. |
| 2) | A portion of AAVE's fee income is paid to the stake as compensation. |
| 3) | In the event of a shortage of funds due to the occurrence of a major liquidation or other event, AAVE tokens deposited with SM will be sold through an auction (Auction Module) (to be compensated from up to 30% of the staked AAVE tokens). |
| 4) | The funds acquired through the auction will be used to eliminate the funding shortfall. |
| 5) | If funds are still insufficient after the auction, they will be covered from the Ecosystem Reserve. These compensations will be made by selling AAVE tokens through the Auction Module protocol. |



# 2-4 Analysis of Lending Aave

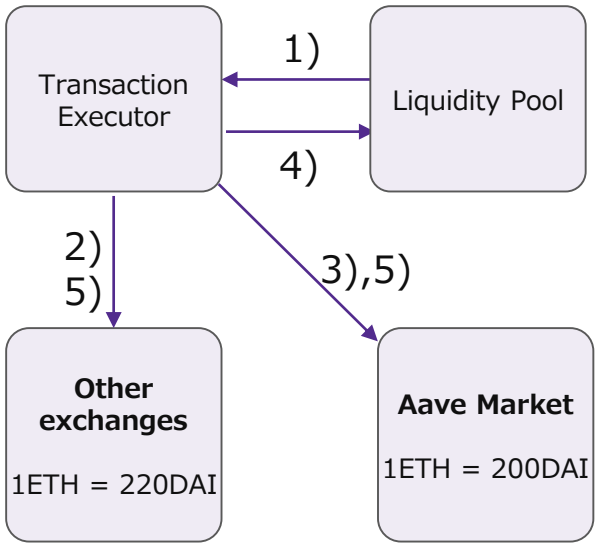
## 2-4-2 Main Technological Characteristics

### (3) Flash Loan

**Functional Overview**

- ✓ A system that enables borrowing, etc., without the need to deposit collateral in advance by completing all borrowing and repayment within one transaction.
- ✓ Arbitrage and collateral exchange are expected to be the main applications.
- ✓ The fee is 0.09% of the borrowed token-denominated debt. In addition, there is a gas fee for deployments and smart contract executions.
- ✓ The design is designed to prevent flash loan attacks by providing a more plentiful supply than demand for crypto-assets via liquidity pools.

**Flash loan example**




<Specific example of a Flash Loan (assuming arbitrage opportunities arise between the AAVE market and other exchanges>
Execute the following 1) to 5) in one transaction.

| # | Description. |
|---|---|
| 1) | Borrow 1 ETH from the liquidity pool on an unsecured basis.<br>At this time, 1 ETH shall be exchangeable for 200 DAI in the Aave Market. |
| 2) | Book an exchange transaction at 220 DAI for the 1 ETH borrowed in (i) at another exchange where there is a difference in exchange rates. |
| 3) | Make a reservation to exchange 200 DAI for 1 ETH at Aave Market. |
| 4) | Return 1 ETH and 0.0009 ETH with 0.09% commission. |
| 5) | The exchange transaction reservation is executed. As a result, a profit equivalent to 19.82 DAI* is earned (gas fees are actually deducted from this amount). 20DAI- 0.0009ETH (0.18DAI) |

# 2-4 Analysis of Lending Aave

## 2-4-2 Main Technological Characteristics

### (4) Credit Delegation

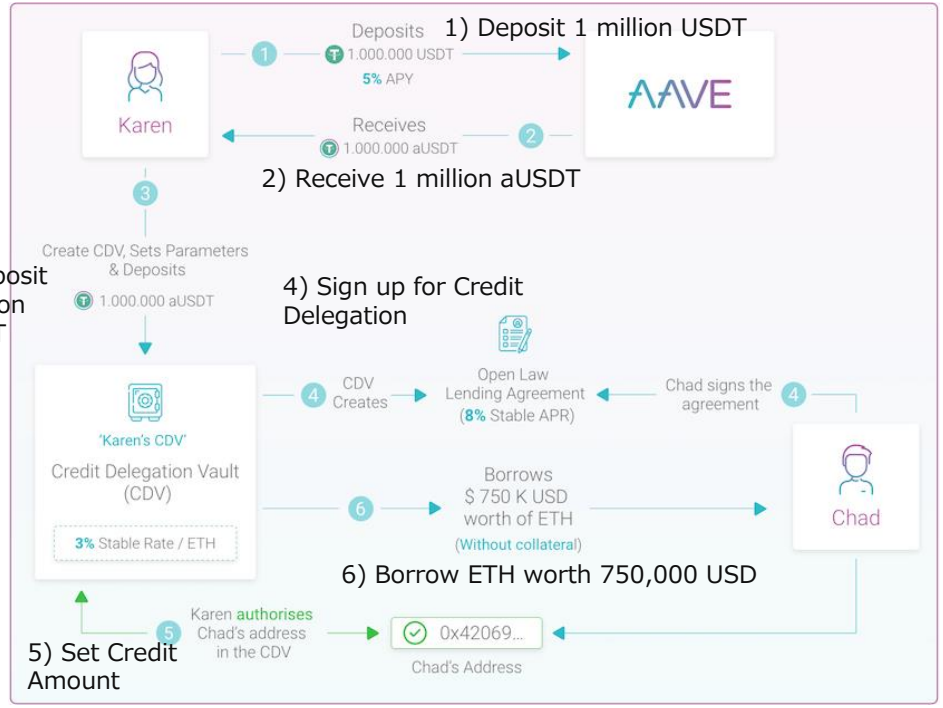
**Functional Overview**

- ✓ A credit delegation is a mechanism whereby a person who deposits crypto-assets with Aave can enjoy additional yield by ceding a line of credit secured by those crypto-assets to another party.
- ✓ The lender and borrower agree on the interest rate and term, and enter into a contract. Currently, one transferee can be designated for each collateralized asset, but in the future, the ability to transfer to multiple transferees will be considered.

<Specific examples of Credit Delegation>

- ➢ In the example in Figure 2-4-2-4, Karen pledges collateral on Chad's behalf, allowing Chad to borrow crypto-assets.
- ➢ In V1, the contract between Karen and Chad was made enforceable using OpenLaw, an electronic contracting service that includes smart contracts, based on an off-chain agreement between the two parties. In V2, the electronic contract function is incorporated into Aave.

**Example of credit delegation**




| # | Description |
|---|---|
| 1)<br>2) | Karen deposits 1,000,000 USDT into Aave's lending pool and obtains 1,000,000 aUSDT. |
| 3) | Karen obtains ETH at a fixed rate of 3% by depositing 1 million aUSDT in the Credit Delegation Vault (CDV). |
| 4) | Chad and Karen, who wish to borrow on an unsecured basis, agree on the amount of credit, interest rate (8% annual interest rate in the figure), and other borrowing terms and conditions, and sign a contract (in AaveV1, the credit delegation contract is signed by OpenLaw). |
| 5) | After the contract is signed, Karen establishes the amount of Chad's credit according to the contract. |
| 6) | Chad borrows to the extent of the relevant credit amount (in the figure, ETH equivalent to 750,000 USD is borrowed). The credit mandate allows Karen to earn a higher yield and Chad to raise funds without collateral. |

# 2-4 Analysis of Lending Aave

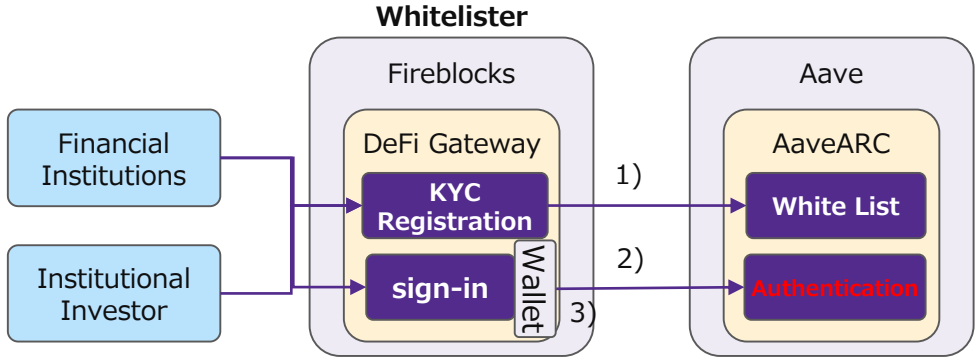
## 2-4-2 Main Technological Characteristics (5) AaveArc / Whitelister

**Functional Overview**

<AaveARC>
- ✓ A Permissioned Institutional DeFi Protocol designed to enable institutional investors and others to participate in the DeFi ecosystem in a compliant manner.
- ✓ KYC and financial due diligence can be performed by institutional investors, utilizing the key features of the AAVE protocol only with other institutional investors who have received similar approval to operate. The four crypto-assets covered at this time are ETH, WBTC, USDC, and AAVE.
- ✓ Deployed on Arbitrum and Optimism, Ethereum's L2 solution, in January 2022

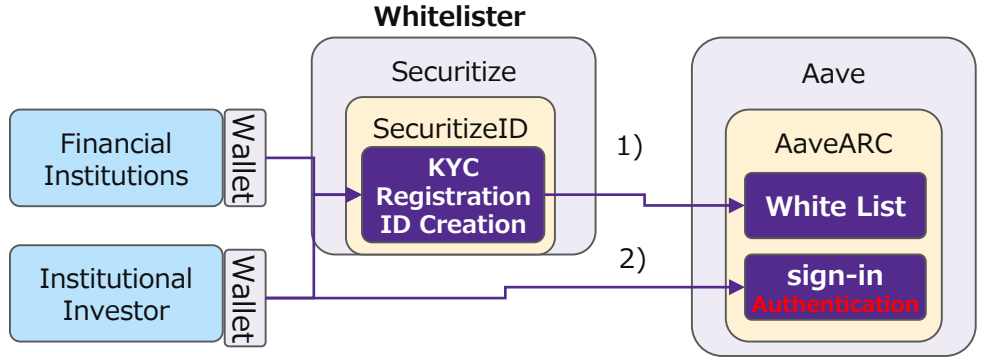
<Whitelister>
- ✓ Perform due diligence on institutional investors accessing the AAVE protocol via AaveArc, approve and "white list" all participating institutions to ensure compliance with KYC and AML regulations.
- ✓ Fireblocks is the first company that was qualified; Securitize (US) and SEBA Bank (Switzerland) are in the process of implementing governance proposals (as of February 2022).

### Fireblocks DeFi Gateway




<Flow of authentication>
1) Execute KYC with Fireblocks framework and whitelist financial institutions and institutional investors.
2) Whitelisted users access AaveArc via Fireblocks' DeFi gateway.
3) Use Fireblocks' secure Multi Party Computing (MPC) wallet.
30 registered financial institutions and institutional investors:
Bluefire Capital, Celsius, CoinShares, Seba Bank, GSR, Ribbit Capital, and QCP Capital, Wintermute, etc.

### SecuritizeID




<Flow of authentication>
1) When a financial institution or institutional investor creates a SecuritizeID in its own wallet, the wallet is linked to the AaveARC whitelist.
2) Once you sign in to AaveArc from the wallet and obtain authorization, the wallet address is authorized to perform transactions such as lending, borrowing, and clearing on AaveArc.

# 2-4 Analysis of Lending Aave

## 2-4-3 Governance operations

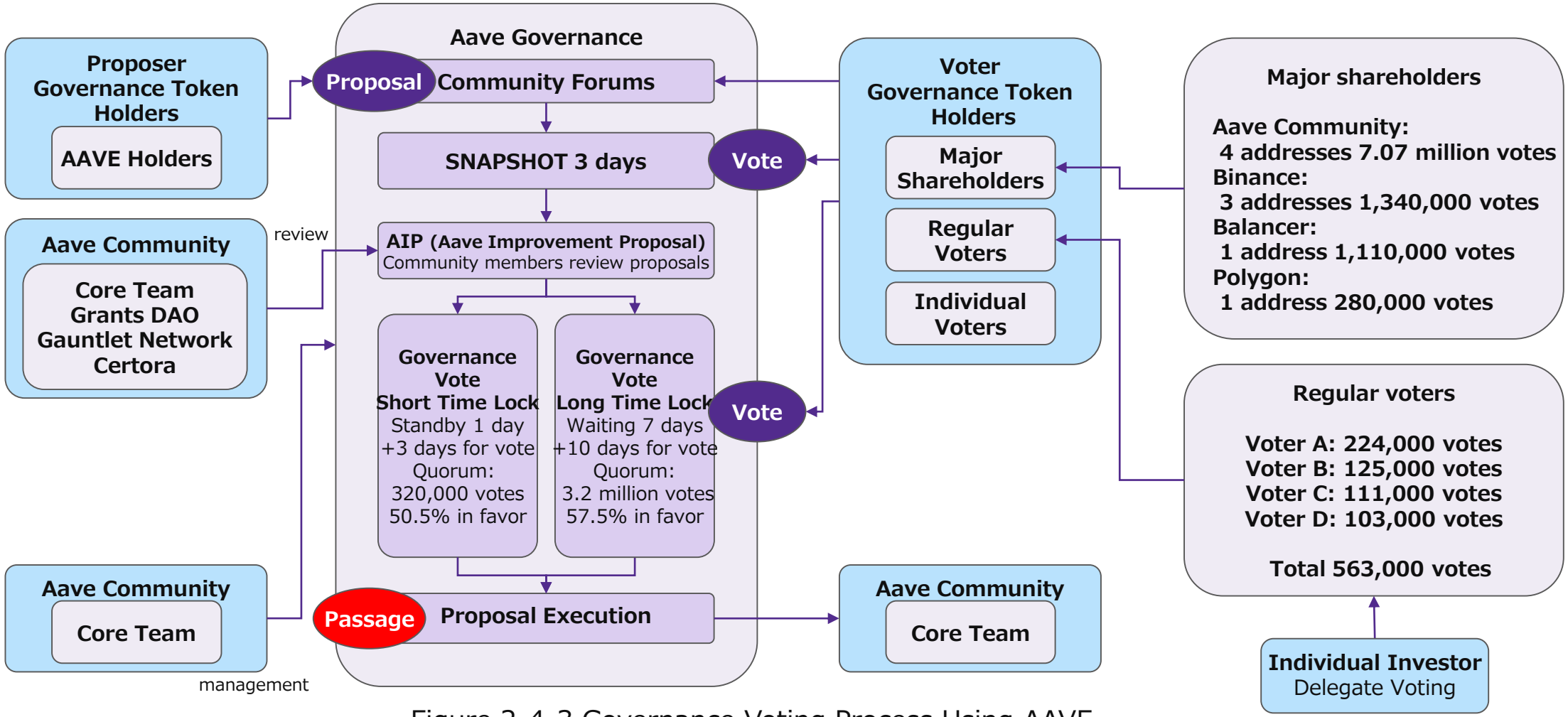



Figure 2-4-3 Governance Voting Process Using AAVE

# 2-4 Analysis of Lending Aave

2-4-4 AAVE's main trust points

- Whitelister (KYC provider) involved to provide institutional lending services
- Guardian: 10 people selected from the community to manage the multisig and have the authority to suspend protocols, etc.

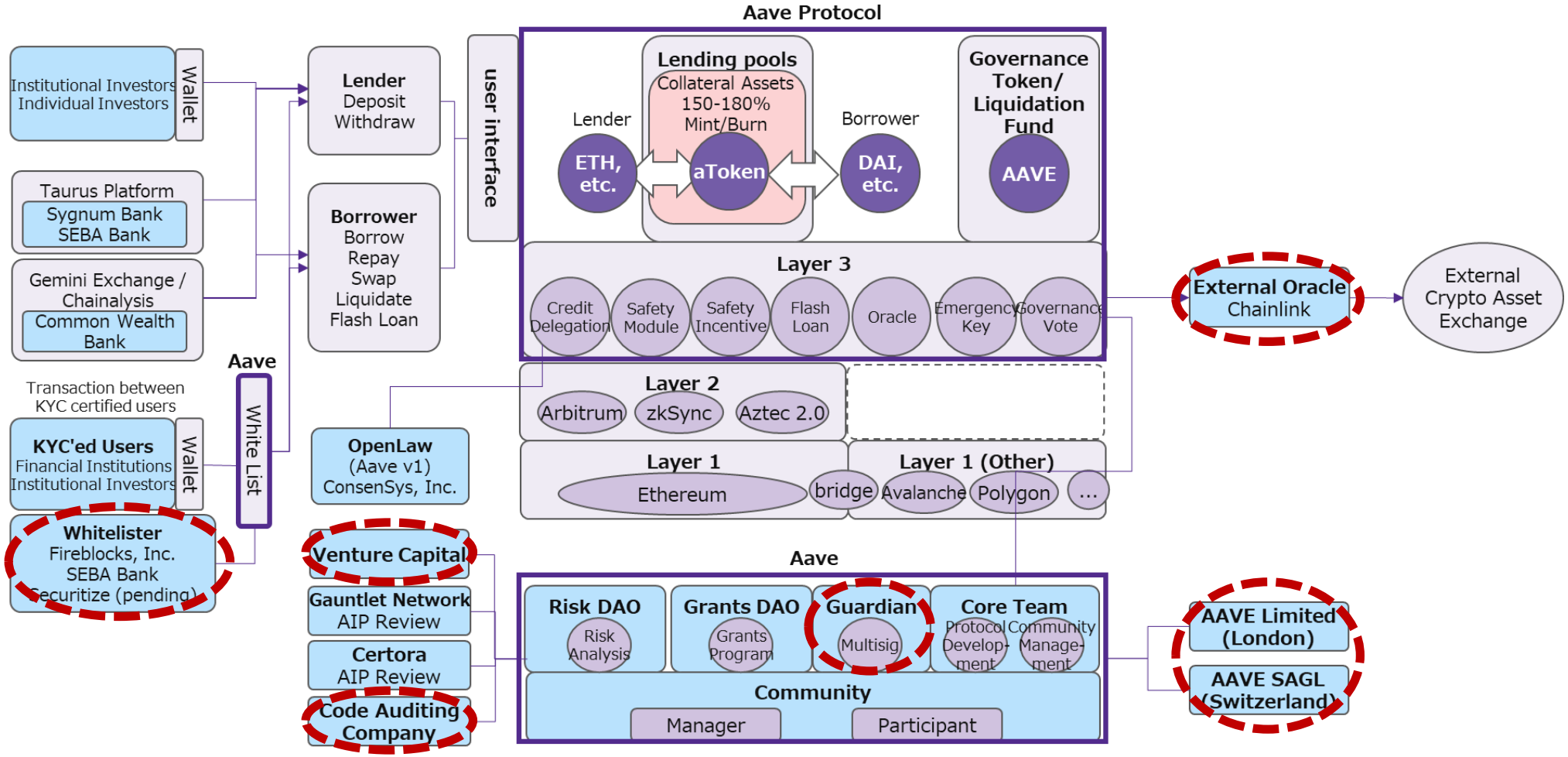



Figure 2-4-4-1 Aave's main trust points (components)

# 2-4 Analysis of Lending Aave

2-4-4 AAVE's main trust points

- ✓ Some governance token holders, such as large token holding voters and constant voters, are considered to have significant influence.
- ✓ DAO's core team and subcontractors who review the AIP to ensure quality are also considered to have some influence.

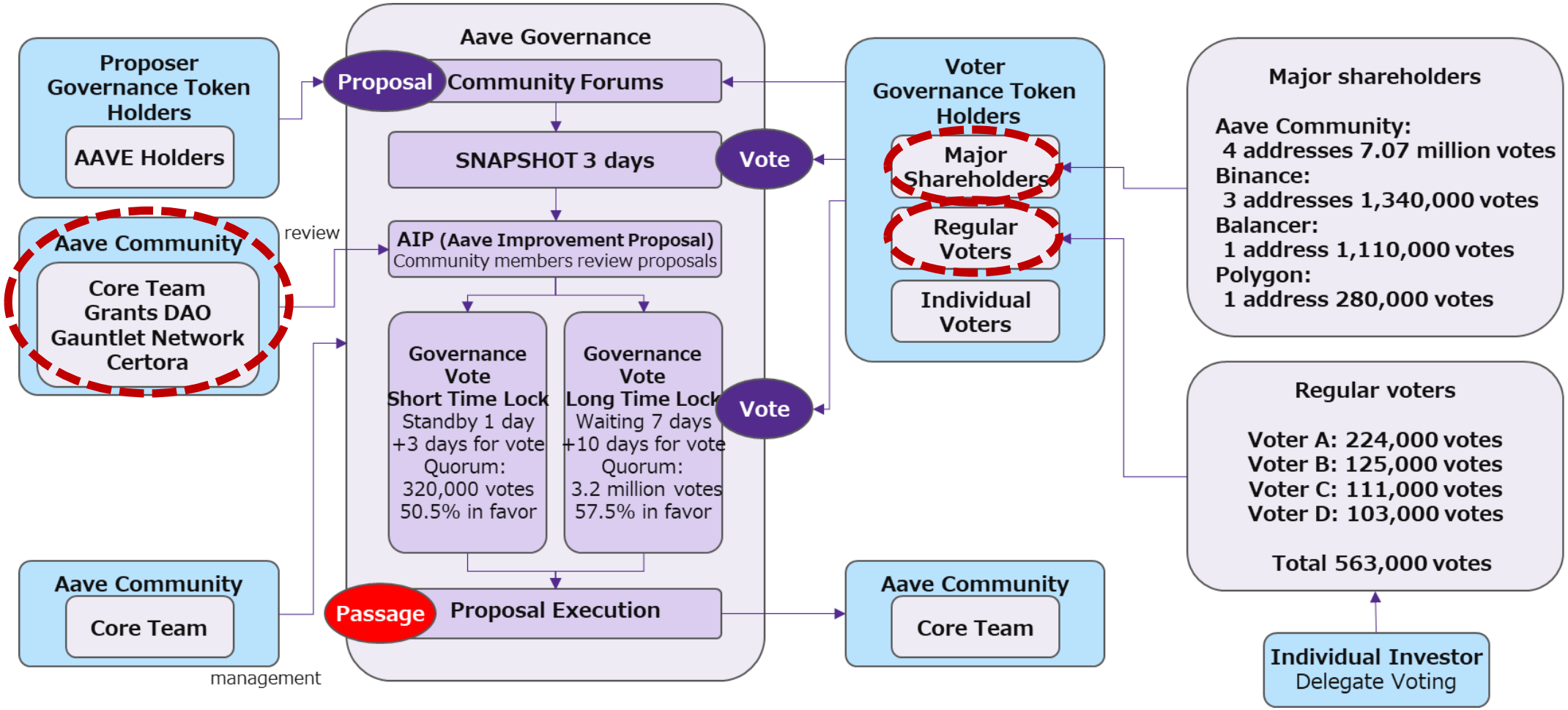
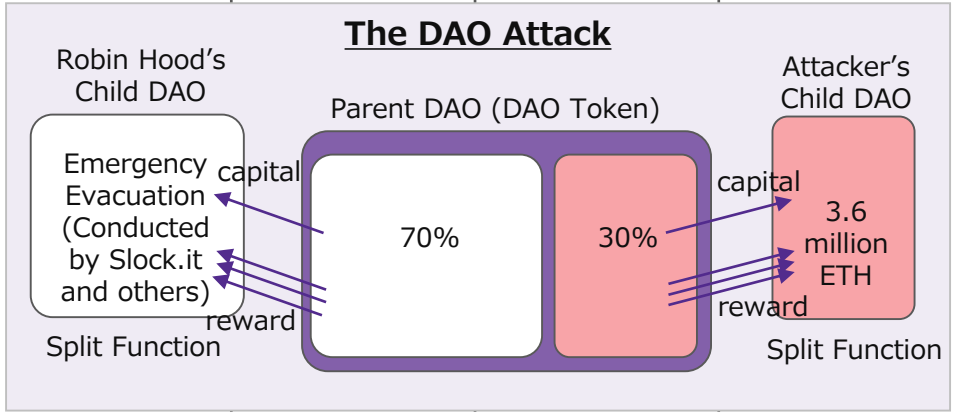



Figure 2-4-4-2 Aave's Main Trust Points (Governance Voting)

# 2-5 Major Incident Case Analysis of Other DeFi Projects

## 2-5-1 The DAO Attack

| Date of Occurrence | Amount of Damage | Related DeFi | Related Elements | Case Summary | Cause of Occurrence |
|---|---|---|---|---|---|
| June 17, 2016 | No loss due to hard fork<br><br>Temporary theft amounted to approximately $70 million (3.6 million ETH) | The DAO | DAO Token<br>Ethereum<br>ETH | The attacker took advantage of a vulnerability in The DAO's reward transfer function to transfer a large amount of rewards to their own child DAO (their own exclusive address for disbursing funds), which was tied to the parent DAO, and obtained 3.6 million ETH. However, since the child DAO's funds could not be transferred for 27 days, The DAO avoided damage by performing a hard fork of Ethereum (transaction deactivation) before that time.<br><br><Case flow><br>1. The DAO's Split function was used to create its own child DAO independent of the parent DAO.<br>2. Exploiting a vulnerability in the Split function, the attacker embedded a smart contract that automatically repeated the remittance of rewards before the parent DAO's balance was updated for the transfer of funds from the parent DAO to the child DAO, and repeatedly transferred more funds than the attacker held to the child DAO for a total of 3.6 million ETH.<br>3. As an emergency measure, the defenders set up the "RobinHoodGroup" and evacuated 70% of the total funds using the same technique as the attackers. (They quickly evacuated the funds by devising a way to get more rewards than the attackers)<br>4. The attacker was unable to transfer 3.6 million ETH of funds from the child DAO because of the restriction that funds in the child DAO using the Split function could not be transferred for 27 days.<br>5. The following three proposals were considered as possible solutions to the incident, and 3) Hard fork was executed.<br>1) Do not fork and surrender the funds to the attacker<br>2) Soft fork and freeze the attacker's account<br>3) Perform a hard fork and make it look as if the transaction itself never happened.<br>6. Opposition to the hard fork split within Ethereum, creating Ethereum Classic, which maintained the original transaction record. | 1) Phenomenal Factors<br>i. Reentrancy Vulnerability: The DAO's smart contract did not take into account the possibility of reentrancy and updated the internal token balance after funds and rewards were transferred.<br>ii. A mechanism to update running smart contracts was lacking<br>2) Motivational Factors<br>Slock.it failed to recognize ii) above and failed to deploy the modified code before it was attacked. |



# 2-5 Major Incident Case Analysis of Other DeFi Projects

## 2-5-1 The DAO Attack

### ■ How the incident occurred (1/3)

| Date | Events | Contents | Supplement Information |
|---|---|---|---|
| November, 2015 | DAO Proposal | ✓ The DAO, an investment fund organization launched by German company Slock.it UG, has announced that it issues DAO tokens in exchange for the virtual currency ETH, calling it "crowdfunding" | ✓ At the Ethereum Developer Conference in London, Christoph Jentzsch, CEO of Slock.it, described the DAO proposal as a "commercial DAO |
| April 29, 2016 | Deploying The DAO Code | ✓ Slock.it deployed DAO code to the Ethereum blockchain | - |
| April 30 ~ ~ May 28, 2016 | Provision and sale of DAO tokens | ✓ DAO tokens are now offered and sold.<br>✓ During the offering period, DAO sold approximately 1.15 billion DAO tokens in exchange for a total of approximately 12 million ETH (valued at approximately $150 million at the time) | ✓ Token prices varied from approximately 1 to 1.5 ETH per 100 DAO tokens, depending on when the tokens were purchased during the offering period<br>✓<br>✓ Note: Since DAO tokens are securities, the U.S. SEC indicated in a July 2017 report that it was originally required to register the offering and sale of DAO tokens. |
| May 26, 2016 | The DAO Code Vulnerability Surfaces and Security Proposals | ✓ GitHub user discovers flaw in smart contract code<br>✓ This user notified Ethereum developer and Bitcoin Foundation founder Peter Vessenes<br>✓ In response to these concerns, Slock.it published the "DAO Security Proposal" calling for the development of specific updates to The DAO's code and the appointment of security experts | ✓ Slock.it initially proposed a broader security proposal that included the formation of a "DAO Security" group, the establishment of a "bug bounty program," and regular external audits of DAO's code, but the cost of this proposal (125,000 ETH: paid from The DAO's funds) was immediately criticized as too high, and Slock.it) was immediately criticized as too high, and Slock.it decided to revise its proposal and submit it |
| June 3, 2016 | Proposal to Suspend DAO Proposal | ✓ Christoph Jentzsch, CEO of Slock.it, on behalf of Slock.it, recommends that all investment proposals be suspended until changes are implemented to fix vulnerabilities in DAO's code | - |

# 2-5 Major Incident Case Analysis of Other DeFi Projects

## 2-5-1 The DAO Attack

### ■ How the Incident Occurred (2/3)

| Date | Events | Contents | Supplement Information |
|---|---|---|---|
| June 6, 2016 | DAO Vulnerability Disclosure | ✓ Vulnerability in The DAO Smart Contract Announced by Slock.it<br>✓ There was a code update on GitHub on the same day. | ✓ Slock.it Says Workaround for The DAO Vulnerability Created, No Longer DAO Funds at Risk of Vulnerability<br>✓ However, workaround code was developed but not deployed |
| June 17, 2016 | DAO incident occurred | ✓ Attackers stole approximately 3.6 million ETH (30% of the ETH raised by the DAO offering) | ✓ The stolen ETH was held at an address controlled by the attacker, but the attacker could not move the ETH from that address for 27 days due to the DAO code |
| - | Prevention of DAO fund outflows | - Since there was no quick solution to update the smart contract, The DAO stakeholders formed the "RobinHoodGroup". They collected $60,000 in DAO tokens from the community and investors through donations and recovered 70% of the funds using the same tactics as the attackers | - Key members of the RobinHoodGroup<br>➢ Griff Green, Community Manager, Slock.it, Inc.<br>➢ Ethereum developer Alex Van de Sander<br>➢ Christoph Jentzch, CEO of Slock.it, etc. |
| June 28 ~ July 15, 2016 | Consideration of solutions | ✓ The following three proposals were discussed as possible solutions to the stolen 3.6 million ETH<br>1) do nothing<br>Attackers gain 3.6 million ETH<br>2) soft fork<br>The attacker's child DAO is frozen and cannot be transferred. However, 3.6 million ETH will not be returned to the investor and will be a loss to the investor<br>3) hard fork<br>Transfer all investor funds, including the stolen 3.6 million ETH, from The DAO to a recovery address to avoid investor losses | ✓ The hard fork was an emergency plan proposed by the Ethereum Foundation and was highly controversial in the community, as it went against the blockchain philosophy that transactions should be irreversible.<br>✓ Opinions in favor of hard forking<br>➢ Humans should make the final decision through social consensus.<br>➢ It is ethically wrong for the attacker to profit and requires community intervention.<br>➢ Leaving ETH in the hands of an attacker could reduce its value in the future.<br>✓ Opinions of opponents of hard forking<br>➢ The unwinding of transactions is contrary to the blockchain philosophy of "Code is Law", "Trustworthiness", and "Immutability".<br>➢ It undermines the original purpose of the Ethereum blockchain and makes the rules of the code base subject to human interests. |

# 2-5 Major Incident Case Analysis of Other DeFi Projects

2-5-1 The DAO Attack

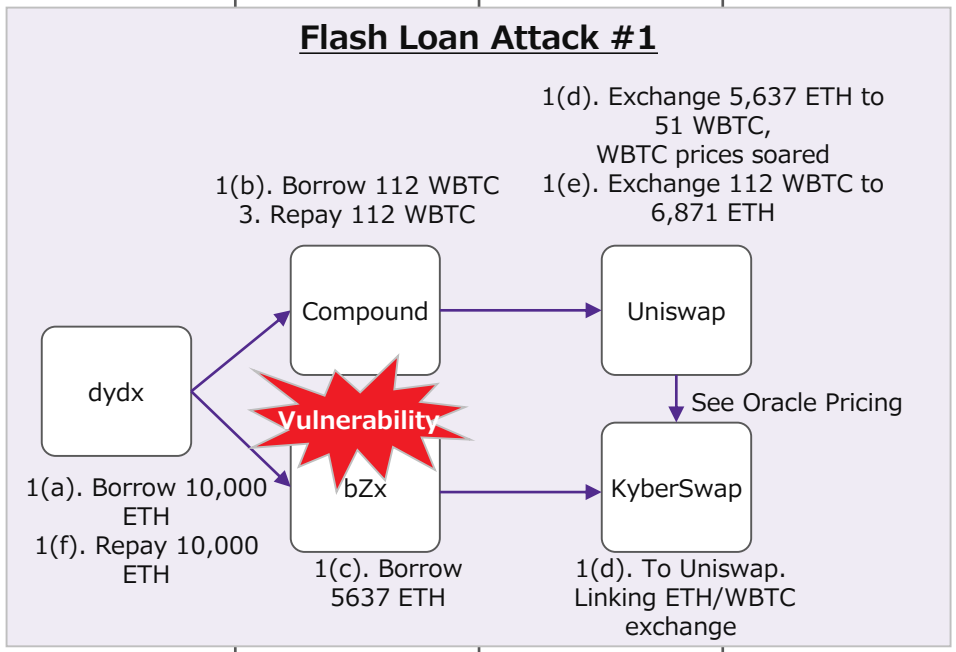
## ■ How the Incident Occurred (3/3)

| Date | Events | Contents | Supplement Information |
|---|---|---|---|
| June 24, 2016 | Soft Fork Consideration - Abandoned | ✓ Ethereum Foundation and the community initially tried to resolve the issue through a soft fork, but decided not to implement the soft fork after a flaw was found in the soft fork code that allowed for a DoS attack | - |
| July 15, 2016 | Hard Fork Agreed | ✓ A vote on the hard fork proposal was held and passed in the form of sending a small amount of ETH to the voting platform | |
| July 20, 2016 | Implement Hard Fork | ✓ A new forked Ethereum blockchain became active after the majority of the Ethereum blockchain's nodes adopted the necessary software update | |
| July 29, 2016 | Birth of Ethereum Classic | ✓ Hours after the hard fork, opponents of the hard fork resumed mining the original blockchain and Ethereum Classic was born | - |

# 2-5 Major Incident Case Analysis of Other DeFi Projects

## 2-5-2 Flash Loan Attack #1

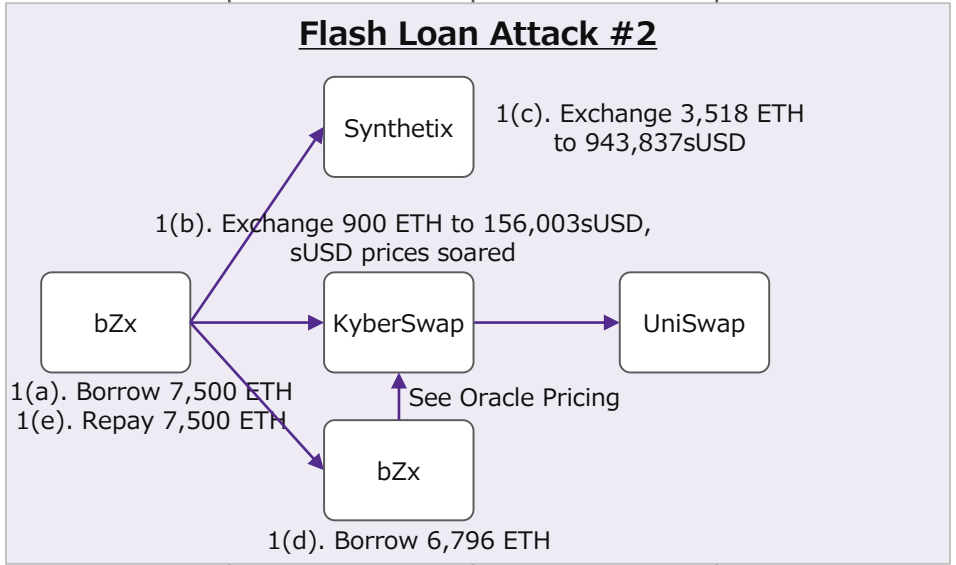
| Date of Occurrence | Amount of Damage | Related DeFi | Related Elements | Case Summary | Cause of Occurrence |
|---|---|---|---|---|---|
| February 15, 2020 | Approximately $350,000 (1,271ETH) | dYdX<br>Compound<br>bZx<br>KyberSwap<br>Uniswap | Flash Loan<br>Oracle | By attacking a vulnerability in bZx's margin trading smart contract, the attacker intentionally inflated the price of WBTC through the mass exchange of ETH and stole 1,271 ETH through arbitrage.<br><br><Case flow><br>1. The following a) to f) were continuously executed in one transaction by Flash Loan.<br>a) The attacker borrowed 10,000 ETH from dYdX via Flash Loan. (Major DeFi's that offer the Flash Loan feature: Aave, dYdX, Equalizer, etc.)<br>b) The same attacker borrowed 112 WBTC from Compound with 5,500 ETH as collateral.<br>c) The same attacker borrowed 5,637 ETH from bZx on margin trading with 1,300 ETH as collateral. (leveraged at approx. 4.3x more than usual)<br>d) 5,637 ETH borrowed on bZx was exchanged for 51 WBTC on KyberSwap<br>KyberSwap exchanged ETH for WBTC on Uniswap, one of several decentralized exchanges it partners with The large amount of ETH being exchanged caused Uniswap's WBTC price to rise to about three times its normal level (Uniswap's exchange rate).<br>(Uniswap's exchange rate: 38 ETH/WBTC at normal time -> soared to 109 ETH/WBTC, about 3 times the normal rate)<br>e) Aiming to take advantage of the surge in WBTC prices on Uniswap, the attacker exchanged 112 WBTC that was borrowed from Compound on Uniswap for ETH, earning 6,871 ETH.<br>f) With dYdX, the 10,000 ETH borrowed from Flash Loan is repaid, resulting in a profit of 71 ETH as the difference.<br>(Profit 71 ETH = 6,871 ETH exchanged + 4,200 ETH unused - 10,000 ETH repaid)<br>2. WBTC price then returned to normal, at 38 ETH/WBTC.<br>3. The attacker repaid 112 WBTC borrowed at Compound and liquidated for 4,300 ETH. As a result, The difference from the collateral was the profit of 1,200 ETH worth of WBTC was obtained. | ✓ Due to an attack that exploited a vulnerability in bZx's margin trading smart contract.<br><br>✓ A large amount of ETH was exchanged into WBTC using the bZx margin trading function, and due to a vulnerability that prevented positions from being liquidated due to insufficient ETH collateral even though the WBTC price was rising (ETH price was falling), the WBTC price was intentionally inflated and the difference was stolen through arbitrage. |



# 2-5 Major Incident Case Analysis of Other DeFi Projects

## 2-5-3 Flash Loan Attack #2

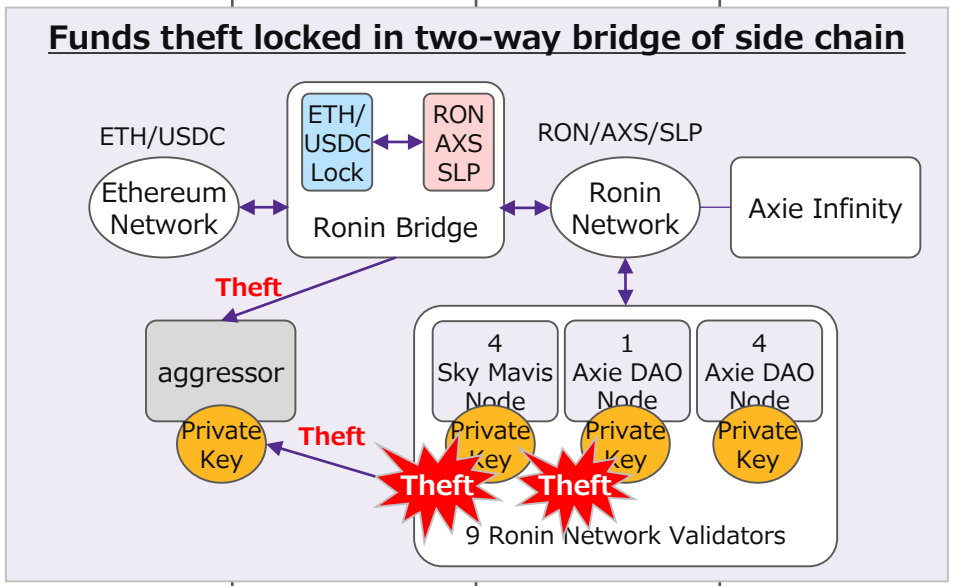
| Date of Occurrence | Amount of Damage | Related DeFi | Related Elements | Case Summary | Cause of Occurrence |
|---|---|---|---|---|---|
| February 18, 2020 | 633,000 U.S. dollars (2,378 ETH) | bZx<br>KyberSwap<br>Synthetix | Flash Loan<br>Oracle<br>ETH | By attacking the Oracle vulnerability in bZx, the attacker intentionally inflated the sUSD price by mass exchange of ETH and stole 2,378 ETH through arbitrage.<br><br><Case flow><br>1. The following a) to e) were continuously executed in one transaction by Flash Loan.<br>a) The attacker borrowed 7,500 ETH from bZx with a Flash Loan.<br>b) Exchanged 540 ETH for 92,419sUSD on KyberSwap. Then 360 ETH was exchanged for 63,584sUSD. (Exchanged 900ETH for 156,003sUSD in total)<br>KyberSwap exchanged ETH for sUSD on Uniswap, one of several decentralized exchanges it partners with. This caused KyberSwap's sUSD price to rise approximately threefold.<br>KyberSwap's exchange rate: 0.00372 ETH/sUSD under normal conditions -> soared about 3 times to 0.00899 ETH/sUSD.<br>c) At Synthetix , 6,000 ETH was exchanged for sUSD. 3,518 ETH was exchanged for 943,837 sUSD due to sUSD shortage and 2,482 ETH was refunded. (Exchange rate: 0.00372 ETH/sUSD under normal circumstances)<br>d) Borrowed 6,796 ETH from bZx with 1.1 million sUSD as collateral. At normal sUSD prices, the borrowing limit would be about 4,000 ETH, but bZx was able to borrow 6,796 ETH due to the soaring sUSD because of the Oracle reference to KyberSwap. (The attacker left the borrowed state without repayment)<br>e) The 7,500 ETH borrowed from bZx was repaid and a profit of 2,378 ETH was earned.<br>(Profit 2,378 ETH = 6,796 ETH borrowed + 3,082 ETH unused - 7,500 ETH repaid) | bZx's reliance on KyberSwap for Oracle price references caused the kyberSwap to intentionally inflate the sUSD price, and when the difference between the normal price and the swap price increased, arbitrage was used to steal the difference. |



# 2-5 Major Incident Case Analysis of Other DeFi Projects

## 2-5-4 Stealing of funds locked in a two-way bridge in a side chain (Ronin Network)

| Date of Occurrence | Amount of Damage | Related DeFi | Related Elements | Case Summary | Cause of Occurrence |
|---|---|---|---|---|---|
| March 23, 2022 | Approximately $620.1 million | Axie Infinity | Ronin Network<br>Ronin Bridge<br>PoA | ✓ On March 23, the private keys of some validators of the Ronin Network running Axie Infinity were stolen, and the funds for the two-way bridge connecting the Ethereum network and the Ronin Network (Ronin Bridge ) were stolen.<br>✓ March 29, the incident was discovered when a user was unable to withdraw funds from Ronin Bridge. Sky Mavis, the operator company in Vietnam of Ronin Bridge, shut down Roni Bridge and investigated the cause.<br>✓ April 6, Sky Mavis raises $150 million from several VC firms to cover losses.<br>✓ April 14, The U.S. Federal Bureau of Investigation (FBI) announces that the North Korean hacker group "Lazarus Group" and "APT38" are responsible for the attack.<br>✓ As of April 20, Ronin Bridge is out of service.<br><br><Case flow><br>1. March 23, Private keys on 5 of the 9 nodes of the Ronin Network Validator were stolen, and ETH and USDC locked in the Ronin Bridge were stolen. ETH and USDC locked in Ronin Bridge were stolen. (The system required the approval of 5 of the 9 nodes.)<br>2. March 29, User is unable to withdraw ETH from Ronin Bridge and incident was discovered. Validator threshold was immediately revised from 5 to 8. Confirmed that most of the stolen funds were held in the attacker's wallet. Investigation of the attacker and monitoring of the wallet is underway in cooperation with government agencies.<br>3. March 31, Replaced 4 nodes managed by Sky Mavis that were stolen and 1 node at Axie DAO (Sky Mavis is planning to migrate to a DAO and it is a candidate DAO to migrate to). New validators are being considered for addition.<br><Stolen Funds and crypto-assets><br>Total $620.1 million<br>➢ ETH 173,600 ETH ($594.6 million)<br>➢ USDC $25.5 million | The cause was that the private keys of 5 of 9 nodes of the Ronin Network Validator were stolen.<br>✓ Sky Mavis 4 nodes<br>An attack on the Sky Mavis system resulted in the theft of the private keys of all four nodes of validators stored on the centralized server. (Means of attack undisclosed).<br>✓ Axie DAO 1 node<br>In November 2021, as a countermeasure to the skyrocketing fees associated with Ronin Network's rapid transaction growth, one Axie DAO node was added to provide free transactions to users, and the Sky Mavis node was allowed to sign by proxy.<br>✓ That action was completed in December 2021, but Sky Mavis did not remove the proxy signature authorization list. As a result, it was automatically stolen in conjunction with the theft of the 4 Sky Mavis nodes. |



# 2-5 Major Incident Case Analysis of Other DeFi Projects

## 2-5-5 Major Incident Cases after 2020

| Date of Occurrence | cause | Related DeFi | Amount of Damage | Case Summary |
|---|---|---|---|---|
| April 19,2020 | Software vulnerabilities (Reentrancy) | Lendf.Me (Lending) | US$25 million [of which $21 million was collected]. | ✓ ERC777 token reentrancy attack that exploited a vulnerability in Ethereum.<br>✓ The attackers had trouble cashing in the stolen crypto-assets (ETH, etc.) and most of them were returned. |
| August 25, 2020 | Software vulnerabilities (Defects in staking pool processing) | YFValue (current Value DeFi) (Yield Farming) | Up to US$170 million [Full recovery] | ✓ A vulnerability in the YFValue (YFV) staking pool caused the YFValue timer to reset, locking some funds in the pool and preventing them from being withdrawn<br>✓ A total of $170 million in the staking pool was at risk of being locked and not being able to be withdrawn, and extorted from the attackers.<br>✓ The management team then bailed out the funds locked in the staking pool. |
| September 14, 2020 | Software vulnerabilities (Unauthorized token issuance) | bZx (derivative) | US$8 million [Full recovery] | ✓ Approximately $8 million was stolen when a vulnerability was exploited that allowed bZx's iToken (a token that can accumulate interest) to be illegally amplified.<br>✓ Later, they found the attacker and recovered the full amount. |
| October 26, 2020 | Fraudulent manipulation of Oracle prices (Depletion of collateral assets) | Harvest Finance (Yield Farming) | US$34 million [of which $2.5 million was collected]. | ✓ The attacker transferred 20 WETH to Harvest Finance's contract and manipulated the price of Curve to deplete funds in crypto-assets (fUSDT, fUSDC). The attackers then converted the funds into renBTC, stealing a total of approximately $34 million. The attackers attacked end-to-end over a seven-minute period, giving no response time<br>✓ The attackers used the Ethereum mixing platform "Tornado.cash" to conceal the funds transfer.<br>✓ Attackers returned $2.5 million to the developer at USDT and USDC. |
| November 30, 2020 | Software vulnerabilities (Reimbursement processing defects) | Saffron Finance (Lending) | US$50 million [Full recovery] | ✓ Smart contract redemption error (vulnerability that prevents funds from being withdrawn after writing certain inputs) was attacked and deposits of 50 million DAI were locked for 8 weeks. |

# 2-5 Major Incident Case Analysis of Other DeFi Projects

## 2-5-5 Major Incident Cases after 2020

| Date of Occurrence | cause | Related DeFi | Amount of Damage | Case Summary |
|---|---|---|---|---|
| May 18, 2021 | Fraudulent manipulation of oracle prices (Depletion of collateral assets) | Venus (Lending) | US$77 million | ✓ The price of the Venus token (XVS) doubled due to price manipulation by large traders. Hundreds of millions of dollars worth of BTC and ETH were borrowed using the inflated XVS as collateral for the loans.<br>✓ When the price of XVS fell and the cryptocurrency borrowed against XVS had to be repaid, the system could not handle the repayment on time due to the low liquidity of XVS, resulting in a loss of $7.7 million in Venus protocols.<br>✓ Since there is a 10% fee for providing liquidity, the attacker earned $55 million, the liquidity provider earned $20 million, and the reseller earned $2 million in this case. |
| August 10, 2021 | Software vulnerabilities (Blockchain-to-blockchain transaction glitches) | Poly Network (cross-chain bridge) | US$610 million [Full refund] | ✓ Poly Network suffered a hacking attack that exploited a vulnerability in blockchain-to-blockchain transactions, stealing over $610 million in crypto-assets and transferring them to multiple accounts including Binance Smart Chain, Ethereum, and Polygon.<br>✓ A statement was issued that the attack was carried out to make the vulnerability known, and the full amount was returned a few days later. |
| October 27, 2021 | Software vulnerabilities (Flash loan attacks) | Cream Finance (Lending) | US$130 million | ✓ Flash loan attacks stole a total of approximately $130 million in Cream LP tokens and ERC-20 tokens.<br>✓ This was Cream Finance's third flash loan hit, following two in February and one in August. |
| October 30, 2021 | Inadequate management of private keys | BoyX High Speed (BXH) (DEX) | US$139 million | ✓ Private Key Compromise Leads to $139 Million Outflow<br>✓ The attacker may have hacked into the private keyholder's computer or was one of BXH's technical staff |
| November 5, 2021 | Inadequate management of private keys | bZx (derivative) | US$55 million [Full refund] | ✓ Developers' private keys used to control project deployment between Polygon and BSC were compromised and $55 million stolen<br>✓ bZx DAO voted to approve plan for full compensation for damages |

# 2-5 Major Incident Case Analysis of Other DeFi Projects

## 2-5-5 Major Incident Cases after 2020

| Date of Occurrence | cause | Related DeFi | Amount of Damage | Case Summary |
|---|---|---|---|---|
| November 30, 2021 | Software vulnerabilities (Inadequate token pricing) | Monox (DEX) | US$31 million | ✓ A smart contract vulnerability (where the same token price was used as the reference price for the sale and purchase of tokens) was exploited to manipulate and inflate the price of Mono tokens, which were then exchanged and withdrawn for other tokens. |
| December 2, 2021 | Software vulnerabilities (Unauthorized insertion of phishing UI) | Badger DAO (Yield Farming) | US$120 million | ✓ The attacker created a malicious API key and inserted a phishing UI (User Interface) by attacking a flaw in Cloudflare on an external network.<br>✓ The user's address was stolen by the criminal and the funds were stolen by the user clicking on the UI. |
| February 2, 2022 | Software vulnerabilities (Defects in the signature verification process) | Wormhole (two-way bridge) | US$320 million | ✓ A vulnerability in the smart contract (a flaw in the contract that verifies signatures) was exploited, and funds locked in the bridge were stolen.<br>✓ Wormhole's parent company, JumpCrypto, covered the damage with its own funds to support the Solana ecosystem. |

# 2-5 Major Incident Case Analysis of Other DeFi Projects

## 2-5-5 Major Incident Cases after 2020

| Date of Occurrence | cause | Related DeFi | Amount of Damage | Case Summary |
|---|---|---|---|---|
| April 17, 2022 | Software vulnerabilities (Inadequate emergency commit conditions) | Beanstalk (stablecoin) | US$182 | ✓ Governance voting smart contract vulnerability exploited and funds stolen by Flash Loan<br>✓ Incident Flow<br>1) The day before the incident, two proposals were made: a malicious governance proposal (specifying a malicious smart contract address) and 2) a normal proposal (dummy Ukrainian donation proposal).<br>Intentionally the attacker made it look ilke that the proposal 1) is a proposal with an incorrect address and let it get mixed in other proposals as if it is a normal one.<br>2) On the day of the incident, Flash Loan performed the following on Aave<br>➢ Borrowed a total of $1 billion from Aave in ETH, USDC, and USDT<br>➢ Borrowed funds to purchase 2/3 of Beanstalk's governor tokens<br>➢ Vote for malicious proposals with purchased governance tokens<br>➢ Successfully executed a malicious smart contract by activating Beanstalk's Emergency Commit and stole Beanstalk's funds<br>✓ Cause of the incident<br>1) No one in the community noticed the malicious proposal.<br>➢ Verification of proposals depended on the cooperation of community members, and no one was able to find a malicious proposal<br>2) There was no mechanism to cancel malicious proposals in the Emergency Commit.<br>➢ There needed to be a mechanism to cancel proposals and a cancellation period.<br>3) Inadequate conditions for activation of Emergency Commit in Beanstalk<br>➢ (Activation condition) 1 day after proposal & 2/3 or more affirmative votes to be executed<br>➢ If the proposal is passed and a certain period of time (e.g., two days) is waited, it would not be attacked by Flash Loan.<br>4) Aave's Flash Loan was abused.<br>➢ Aave's Flash Loan was exploited to attack other DeFi projects because of its unsecured, unlimited borrowing |

# 2-5 Major Incident Case Analysis of Other DeFi Projects

## 2-5-5 Major Incident Cases after 2020

| Date of Occurrence | cause | Related DeFi | Amount of Damage | Case Summary |
|---|---|---|---|---|
| May 10, 2022 | Significant drop in market price due to massive selling of stablecoins | Terra Blockchain TerraUSD (UST) Anchor Protocol | Decline in market prices UST 83%. LUNA 99% | ✓ The market price failed to maintain 1USD due to massive selling of Stablecoin UST and fell significantly . There have been two previous occasions when the price was temporarily unable to maintain 1USD, but this time the price was unable to return.<br>✓ Case Flow<br>1) May 5, The overall price of crypto-assets, including Bitcoin and ETH, fell. (Bitcoin fell up to 32% on 5/12)<br>2) May 7, A large withdrawal ($1.4 billion) from Anchor Protocol reduces deposit volume and the price of stablecoin UST begins to drop. (The large withdrawer is unknown. Asset management companies BlackRock and Citadel denied the involvement)<br>3) May 8, UST was sold for $258 million, further lowering the price.<br>4) May 9-10, UST fell 2% and could no longer hold 1USD; LFG (Luna Foundation Guard) released the entire amount of about $4 billion in Bitcoin they were holding to maintain the price, but they were unable to get back to 1USD due to lack of funds against selling. The price did not return to 1USD due to lack of funds for the sell-off. (UST market cap was $18.64 billion as of may 8)<br>- USTs were sold in large quantities due to the uncertainly in the market, causing the price to collapse, and the algorithm minted a large number of native token LUNAs, causing the price of LUNAs to fall.<br>- Total LUNA supply: approx. 730 million tokens as of 5/5 → increased to 6.5 trillion tokens as of 5/13 (approx. 8,900x)<br>5) May 13, Terra blockchain operations were temporarily suspended.<br>- Market price UST: $1.0 to $0.17 (down 83%); LUNA: $80 to $0.02 (down 99%)<br>*Anchor Protocol: a savings protocol for the Terra blockchain that offers up to 19.5% yield when depositing UST tokens.<br>✓ LUNA: Native token of the Terra blockchain, used to maintain the price of USTs. (burns when UST exceeds 1USD, and mints when UST falls below 1USD to maintain UST = 1USD) |

# 2-6 Analysis of Trust Points

| Classification | Elements | Contents of Trust Point |
|---|---|---|
| Trust Point | Ethereum Library | ✓ Various services outside the blockchain, such as wallets that access the Ethereum blockchain, use a common library provided by the Ethereum Foundation and others, and users assume that this library functions correctly. |
| | Ethereum Node Software | ✓ Nodes running on the Ethereum blockchain are encouraged to use common software provided by the Ethereum Foundation and others, and node operators assume that this software functions correctly (node operators assume that the developers and suppliers of the respective software provide code that is free from vulnerabilities). (Node operators assume that the developers and suppliers of the respective software are providing code that is free from vulnerabilities and other problems). |
| | Infrastructure Provider Provision Services | ✓ In order to use the Ethereum blockchain, transactions are executed from an Ethereum node, but building this node yourself is burdensome, and you may use the services of an inexpensive infrastructure provider. This service user assumes that the infrastructure provider's service works correctly. |
| | Code embedded in the web browser | ✓ The code that runs in web browsers when using DeFi and wallets is provided by DeFi, infrastructure providers, etc., and it is assumed that the code embedded by DeFi, infrastructure providers, etc., works correctly. |
| | Generic codes used by DeFi | ✓ When developing DeFi protocols, peripheral functions, etc., generic open source code may be imported from outside the supply chain, etc., to achieve specific functions, etc., assuming that the code provided by the supplier works correctly in such cases. |
| | Internet | ✓ The network connections of the decentralized financial system, such as the connection between investors' and users' wallets and infrastructure providers, and the P2P network between Ethereum nodes operated by miners, are via the Internet, and are provided by several different Internet service providers, data center operators, and other Internet interconnected services. Investors, users, and miners assume that the Internet connection services behave correctly. |
| | External Oracle Services | ✓ Some DeFi projects do not calculate Oracle prices within their own projects for the purpose of Oracle attack protection, etc., but use external Oracle price provider services such as Chainlink to obtain market prices and commission rates for their tokens. This DeFi project assumes that the external oracle price providing services behave correctly. |

# 2-6 Analysis of Trust Points

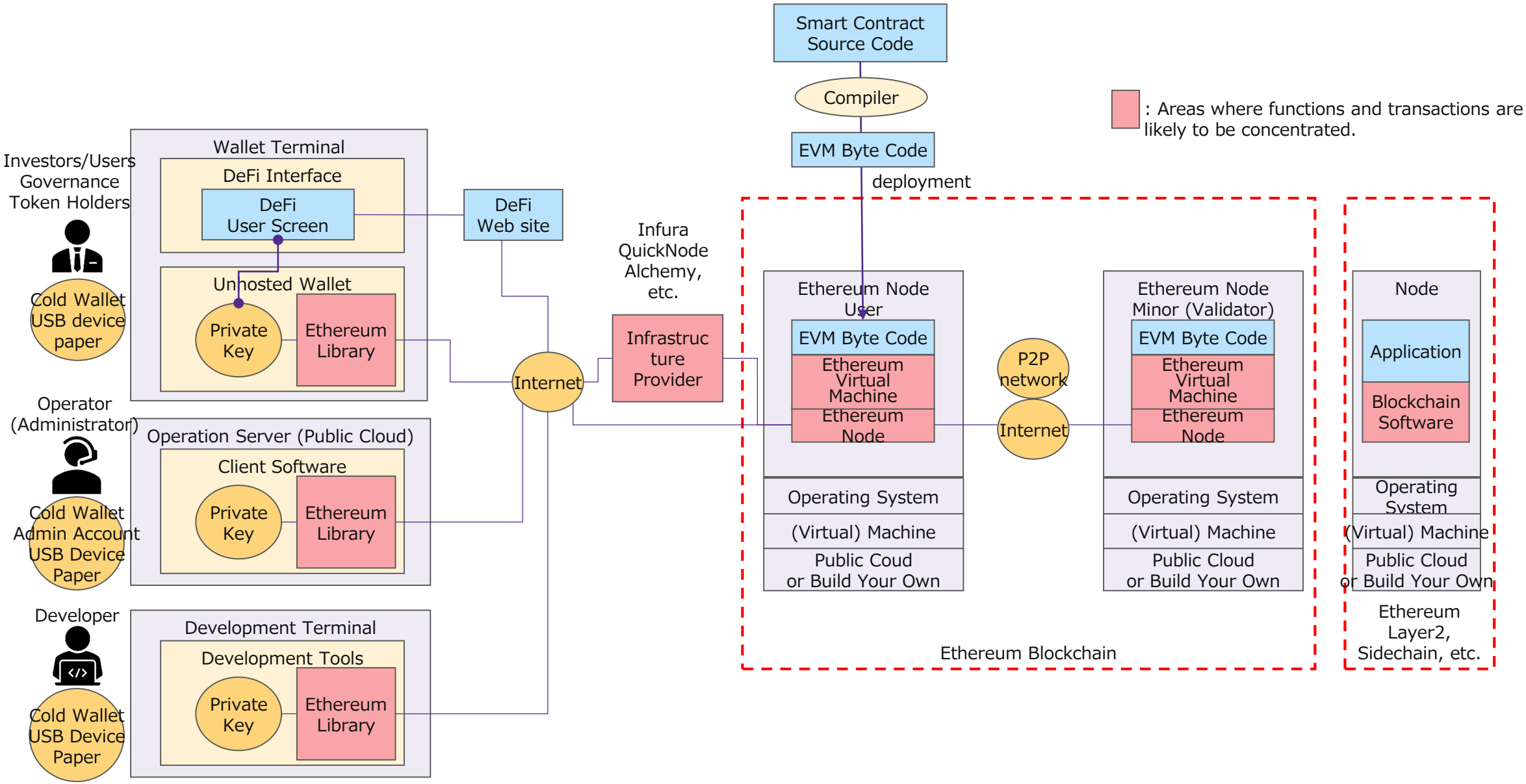



Figure 2-6-1 Analysis of trust points in the chains of trust (wallet terminals, operational servers, and Ethereum nodes)

# 2-6 Analysis of Trust Points

| Classification | Elements | Contents of Trust Point |
|---|---|---|
| Trust Point | Execution of DeFi protocol processing (BOT processing to perform clearing, etc.) | ✓ The services provided by the DeFi protocol use multiple external BOTs (applications that automatically execute certain tasks and processes) to execute processes such as token price maintenance and clearing, but the details of these BOTs are not disclosed, and users assume that the BOTs act correctly. |
| | DeFi protocol development (e.g., modification of smart contracts) | ✓ When modifying a smart contract, such as by proposing a governance vote, most governance vote participants do not understand the content of the smart contract's code and assume that it acts correctly according to the proposal. |
| | Delegation of governance vote | ✓ Governance voting actually operates on a minority vote, and many individual voters may delegate their vote to a large token holder. These individual voters assume that the major token holders to whom they have delegated their vote act as they expect. |
| | Deploy smart contracts and parameter modifications passed by governance vote | ✓ After a proposal to modify a smart contract or parameter, such as adding a feature or changing the interest rate, is passed by a governance vote, it is not deployed automatically, but must be deployed by the administrator or authority. The proposer assumes that this administrator or authority ~~will~~ correctly and promptly deploys what has been passed. |
| | Emergency Smart Contract Modification | ✓ In the event that an urgent smart contract modification is required, such as the discovery of a vulnerability, the vulnerability may not be disclosed to the outside world but only to the parties involved, in accordance with Ethereum's Development Guide and other relevant guidelines. Users assume that the core team of the DeFi project and other administrators and developers ~~will~~ correctly modify the smart contract and respond without causing any damage. |
| | Cancellation of emergency system shutdowns and malicious proposals by the Authority | ✓ Some DeFi projects have a rule that emergency system shutdowns and malicious proposal cancellations are passed by a multisig vote of the authority appointed by the governance vote. Users assume that system shutdowns and proposal cancellations by the authority are carried out for legitimate reasons. |
| | Funds lock for two-way bridges connecting to side chains | ✓ The two-way bridge connecting the main chain and side chains was designed to lock funds to be transferred between chains, and large amounts of funds were concentrated and stored in the two-way bridge. The funds transferred between chains are secured by the funds locked in the two-way bridge, and if the locked funds are leaked due to an attack, etc., the funds cannot be transferred between chains anymore. (Example: Ronin Network Incident) |

# 2-6 Analysis of Trust Points

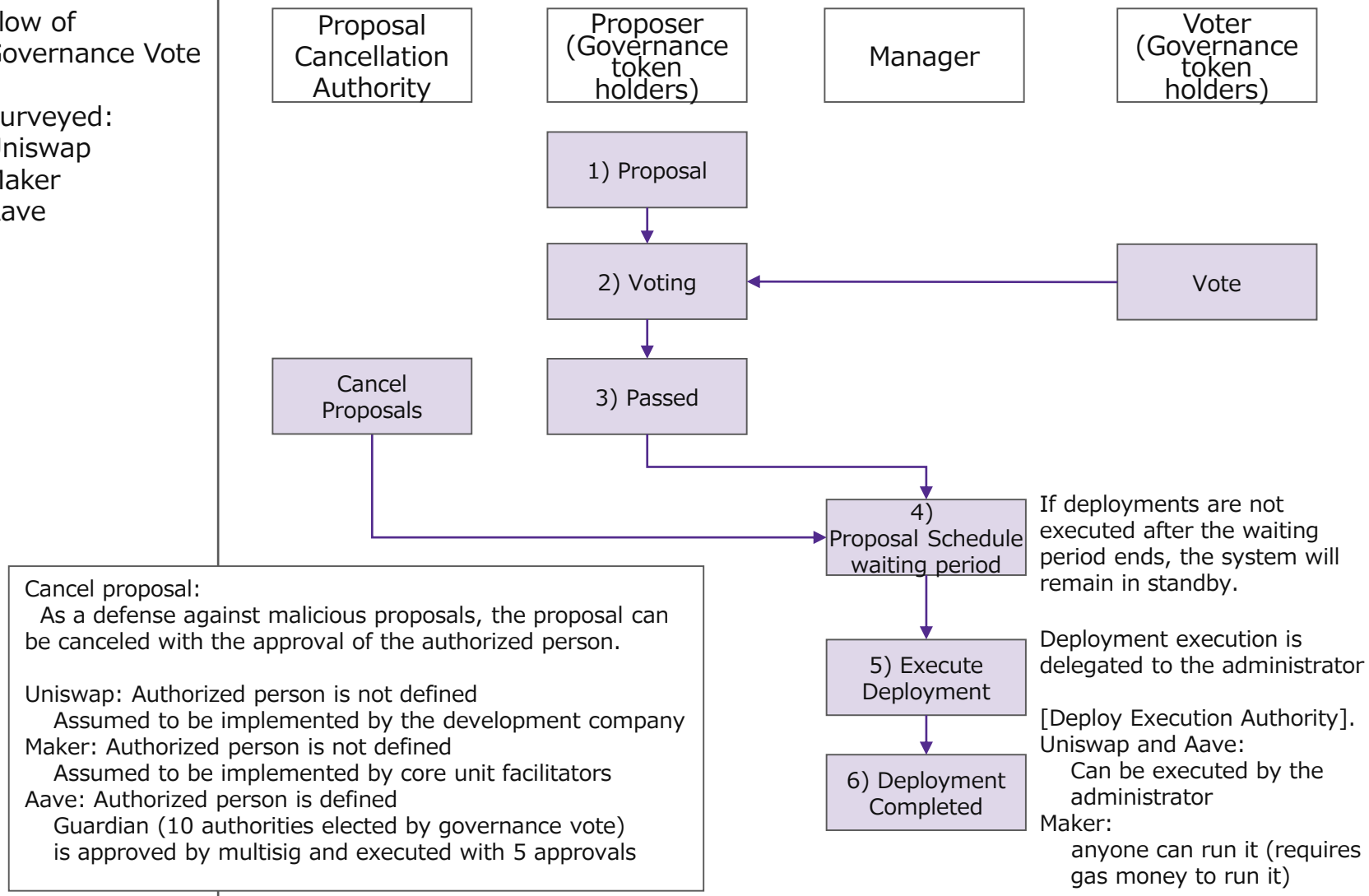
| Item | Overview of Smart Contract Processing | Description |
|---|---|---|
| Flow of Governance Vote<br><br>Surveyed:<br>Uniswap<br>Maker<br>Aave |  | 1) Proposer writes proposal on-chain<br><br>2) Governance token holders vote during the voting period.<br><br>3) The proposal will be approved if the voting fixed number and the votes in favor are met.<br><br>4) The administrator schedules the proposal and waits for the waiting period. Authorized person can cancel the proposal by the end of the waiting period.<br><br>5) After the waiting period, administrator executes deployment.<br><br>6) Deployment is complete and the proposal is reflected in the smart contract. |



Figure 2-6-2 Analysis of Trust Points in the chains of trust (Governance Voting and Deployment)

# 2-6 Analysis of Trust Points

| classification | elements | Contents of Trust Point |
|---|---|---|
| Weakest Link | Sidechain validator private key management | ✓ Among the multiple layers of components that make up the sidechain, such as the blockchain infrastructure and DeFi, there was a weakness in the private key management of the validator, and this weakness was exploited to steal funds locked in the two-way bridge. (Example: Ronin Network Incident) |
| | Verification against malicious proposals | ✓ When a malicious proposal is made, verification depends on the cooperation of community members, so the role of conducting verification is not clear and no one could discover the malicious proposal. In a decentralized organization, it is unclear whether verification is ensured for malicious proposals because the community is free to participate and roles are not clearly defined (Example: Beanstalk Incident). |

# Chapter 3: Analysis of Risks and Risk Mitigation Measures in a Decentralized Financial System

# 3. Analysis of risks and risk mitigation measures in a decentralized financial system

## 3-1 Risks in System Operation

| Main Items | Sub Items | Risk Events | Possible Risk Factors | Risk Mitigation Measures (Proposal) | Notes |
|---|---|---|---|---|---|
| Infrastructure provider | Concentration of use of services provided by infrastructure providers | ✓ Smart contract-driven processing by users is concentrated in a few highly convenient infrastructure providers | ✓ The infrastructure is provided by a highly convenient infrastructure provider because it is difficult for users to build their own Ethereum nodes and other blockchain connectivity due to technical and cost issues. | ✓ Infrastructure providers should inform users of the risks associated with concentrated use of their services (e.g., by providing a mechanism to check risks when using services).<br>✓ Recommend using multiple infrastructure providers depending on the severity of the DeFi service shutdown | ✓ It is necessary to make users with low literacy aware of the risks involved. |
| | Dependence on infrastructure provider services | ✓ Service interruptions due to software vulnerabilities in infrastructure providers, etc., prevent the execution of smart contract-driven software that uses them (Example: Infura incident). | ✓ Users rely on infrastructure providers to keep their services up and running. | | |
| | Suspension of services of infrastructure providers | ✓ Users trust that the infrastructure provider's service will be trouble-free, and no countermeasures are taken in anticipation of problems. | ✓ Users are not considering how to address possible service shutdown of infrastructure providers (e.g., use of multiple providers). | ✓ Infrastructure providers to implement measures to strengthen resilience to failures, such as chaos engineering, to prevent accidental service shutdown<br>✓ Infrastructure providers obtain quality certification (SOC2) to reduce the risk of service shutdown | ✓ Possible measures to be taken include<br>i ) Chaos Engineering:<br>A method of injecting failures into the production environment and keeping recovery functions running at all times, as implemented by Netflix and AWS.<br>ii ) SOC2: (System and Organization Controls 2)<br>Use the internal control and assurance reporting framework at the outsourcing provider (trustee company) |

# 3. Analysis of risks and risk mitigation measures in a decentralized financial system

## 3-1 Risks in System Operation

| Main Items | Sub Items | Risk Events | Possible Risk Factors | Risk Mitigation Measures (Proposal) | Notes |
|---|---|---|---|---|---|
| DeFi Protocol | Unlimited borrowing of funds through Flash Loan | ✓ Huge transactions in the Flash Loan will deplete the liquidity pool and cause the token price to collapse. | ✓ Users can borrow crypto-assets with no collateral and limit. (However, there is a disadvantage that borrowing a large amount of money may result in higher fees, and advanced knowledge is required to earn a profit) | ✓ DeFi protocol developers should be aware of the risks of this matter and consider setting transaction limits, etc.<br>i ) Set collateral amount when using Flash Loan (n% of borrowed funds)<br>ii ) Maximum amount of Flash Loan usage | ✓ Changing unsecured borrowing to secured borrowing will prevent abuse by requiring large amounts of collateral for large amounts of borrowing. |
| | DeFi service shutdown in case of emergency | ✓ In the event of an outflow of funds or issuance of tokens due to an external attack, DeFi service cannot be stopped in an emergency and the damage cannot be stopped. | ✓ No consideration of emergency shutdown of DeFi protocol as a measure of emergency<br>✓ Smart contracts cannot be stopped by blockchain specifications, so the DeFi protocol must be used. | ✓ Instruct the DeFi project to create a feature that allows for emergency shutdown of the DeFi protocol in the event of an emergency. | ✓ We believe that it is extremely difficult to develop a complete smart contract that is unaffected by an attack.<br>✓ Therefore, it is important to have an emergency shutdown function as a measure of minimizing damage in the event of an emergency. |

# 3. Analysis of risks and risk mitigation measures in a decentralized financial system

## 3-1 Risks in System Operation

| Main Items | Sub Items | Risk Events | Possible Risk Factors | Risk Mitigation Measures (Proposal) | Notes |
|---|---|---|---|---|---|
| DeFi Protocol | Measures for unforeseen circumstances | ✓ Failure to respond quickly in the event of unforeseen events (e.g., market price collapse, external attacks, etc.), affecting services<br>✓ Possibility of lack of clarity on contingency plans | ✓ Not having contingency policies and procedures in place<br>✓ Failure to implement contingency mechanisms and functions | ✓ DeFi projects develop contingency plans for unforeseen events and identify necessary system measures.<br>✓ Implement responses the measures such as external Oracle suspension, DeFi protocol emergency shutdown, etc., in accordance with that policy.<br>✓ DeFi project plans and conducts regular drills of the contingency plan to ensure a smooth implementation in the event of an outbreak. | ✓ Contingency plans and periodic training exercises could be a way for blockchain management organizations to issue guidance for DeFi projects.<br>✓ Maker has established five major contingencies and has developed contingency plans for them.<br>✓ Periodic training could include methods such as hardening.<br>*Hardening:<br>To split a team into two teams of operators and attackers to actually attack and defend to gain hands-on experience. |

# 3. Analysis of risks and risk mitigation measures in a decentralized financial system

## 3-1 Risks in System Operation

| Main Items | Sub Items | Risk Events | Possible Risk Factors | Risk Mitigation Measures (Proposal) | Notes |
|---|---|---|---|---|---|
| Oracle | Oracle Attack | ✓ External attacks target vulnerabilities in Oracle pricing<br>✓ (e.g., arbitrage by intentionally generating a difference between the market price and the internal oracle price) | ✓ Oracle pricing methods vary from DeFi project to project, and no safe implementation method has been established<br>✓ Of the DeFi projects, oracle prices may be linked to market prices for specific projects | ✓ The blockchain management organization should review and disseminate the standardization and recommended method of Oracle pricing across the DeFi project. | ✓ Ensure a certain level of safety by informing users of safe Oracle usage. |
| | Delay in reflecting external oracle prices | ✓ Delays in external oracle price references due to network congestion, etc., result in a difference between the external market and internal oracle prices. | ✓ If an Oracle price is intentionally delayed, the Oracle price cannot keep up with sudden changes in market prices, resulting in a large difference. | | |

# 3. Analysis of risks and risk mitigation measures in a decentralized financial system

## 3-2 Risks in System Development

| Main Items | Sub Items | Risk Events | Possible Risk Factors | Risk Mitigation Measures (Proposal) | Notes |
|---|---|---|---|---|---|
| Smart Contract | ✓ Smart contract not upgradeable | ✓ If vulnerabilities are discovered in non-upgradeable smart contracts, there is a concern that they cannot be fixed, increasing the damage caused by attacks.<br>✓ The problem is that the expected correction cannot be made when there is a problem related to upgradability. | ✓ It is extremely difficult for developers and code auditing companies to eliminate all smart contract vulnerabilities, and non-upgradability is risky. | ✓ We believe that making smart contracts upgradable will reduce risk. | ✓ Smart contract upgrades are generally provided by infrastructure providers (e.g., Open Zeppelin Upgrades Plugins), so it is important to consider which service to deploy. |
| | ✓ Code Vulnerability | ✓ Incidents using publicly known code vulnerabilities are recurring, and vulnerabilities are not preventable.<br>i ) Reentrancy vulnerabilities (The DAO, Uniswap, etc.)<br>ii ) Flash Loan attacks (bZx, Harvest Finance, etc.) | ✓ Developers and code auditing companies have technical difficulty detecting all vulnerabilities from the complex functionality of smart contracts. | ✓ In developing the DeFi protocol, use the latest technology to ensure the quality of software development and eliminate vulnerabilities as much as possible.<br>i ) Formal verification<br>ii ) Automated testing by machine learning, etc.<br>✓ The blockchain governing body should be responsible for sharing case studies and recommending technologies to be developed. | ✓ Need to consider ways to reach out to blockchain management organizations |

# 3. Analysis of risks and risk mitigation measures in a decentralized financial system

## 3-2 Risks in System Development

| Main Items | Sub Items | Risk Events | Possible Risk Factors | Risk Mitigation Measures (Proposal) | Notes |
|---|---|---|---|---|---|
| Smart Contract | Test Verification Constraints | ✓ Partial test verification is not possible in the test net, but even in the main net, there are restrictions on testing, and complete test verification is not possible. | ✓ Developers are concerned about deploying to the main net without having transaction confirmation for incentives in the test net (same functionality as the main net, but no transaction fees, different transaction congestion, etc.) | ✓ Provide a means for Testnet to confirm transactions related to incentives.<br>✓ Depending on the contents, test methods in the main net will be considered. | ✓ Although it is preferable to enhance the functionality of the test net as a countermeasure, we believe that there are issues that make feasibility difficult, such as cost, etc. Therefore, it is necessary to further study the feasibility. |
| | Code audit concerns | ✓ Complex processes may make it more difficult for code audits to find vulnerable (e.g., in case it has across multiple smart contracts). | ✓ As attacks against smart contracts become more sophisticated, code auditors' specialized skills and audit tool validation techniques are not keeping up with new or complex attack patterns. | ✓ Code auditing companies improve the detection accuracy of smart contract vulnerability detection techniques and tools.<br>✓ Code auditing firms should collaborate on a system for technical improvement (e.g., by holding periodic competitions and ranking them). | ✓ Examples of analysis techniques for code auditing tools<br>i ) Static verification<br>Verify smart contract code<br>ii ) Dynamic verification<br>Verification while executing smart contracts<br>iii ) Formal verification<br>✓ Using formal and mathematical methods, prove that the code is correct in the light of the formal specification description and properties |

# 3. Analysis of risks and risk mitigation measures in a decentralized financial system

## 3-2 Risks in System Development

| Main Items | Sub Items | Risk Events | Possible Risk Factors | Risk Mitigation Measures (Proposal) | Notes |
|---|---|---|---|---|---|
| Blockchain | Attack on funds locked in two-way bridge | ✓ Heavy losses due to attacks on validator private key targeting funds locked in two-way bridges between Ethereum and sidechains (Example: March 2022 Ronin Network).<br>✓ Billions of dollars of funds are locked up at Polygon and Avalanche, and there are concerns that if an attack were to occur and funds were stolen, the damage could be catastrophic. | ✓ The specification is to lock funds in a two-way bridge for the exchange of funds between Ethereum and the sidechain, and these funds are targeted | ✓ Implementation of measures to prevent attacks targeting funds (e.g., upgrading private key management technology, disseminating secure private key management methods, etc.)<br>✓ Revise specifications for locking funds in two-way bridges (to avoid concentrating large amounts of funds in one place). | ✓ Examples of private key storage technologies<br>i ) Secret decentralization<br>ii ) Social Wallet<br>iii ) Social Wallet<br>✓ Review of specifications for two-way bridges requires feasibility study |

# 3. Analysis of risks and risk mitigation measures in a decentralized financial system

## 3-2 Risks in System Development

| Main Items | Sub Items | Risk Events | Possible Risk Factors | Risk Mitigation Measures (Proposal) | Notes |
|---|---|---|---|---|---|
| Blockchain | Connections between blockchains | ✓ External attacks targeting vulnerabilities in processing across the blockchain.<br>✓ Cross-chain smart contract invocation vulnerability case study (Poly Network)<br>✓ Example of signature verification vulnerability in the Token Bridge Protocol (Wormhole) | ✓ Transactions across the blockchain are complex and difficult to verify through testing (test cases are not exhaustive, lack of anomaly tests, boundary condition tests, etc.). | ✓ In developing the DeFi protocol, use the latest technology to ensure the quality of software development and eliminate vulnerabilities as much as possible.<br>i ) Formal verification<br>ii ) Automated testing by machine learning, etc.<br>✓ The blockchain governing body should be responsible for sharing case studies and recommending technologies to be developed. | ✓ Need to consider ways to reach out to blockchain management organizations |
| | Main chain impact from quality issues with other blockchains and layer 2 solutions | ✓ The use of side and tiered chains and layer 2 solutions is increasing as a scaling measure for Ethereum.<br>✓ Connecting to other blockchains or layer 2 solutions with quality concerns increases the risk of the main chain being affected by vulnerability attacks, etc. (e.g. Polygon has multiple reported vulnerabilities) | ✓ There are a number of blockchain and layer 2 solutions, some of which have vulnerabilities and other concerns.<br>✓ No mechanism to compare and disclose information on vulnerabilities of platforms | ✓ The quality assurance should be discussed among the DeFi project stakeholders when considering the linkage with Layer 2 solutions and other blockchains. | ✓ Infrastructure providers are reportedly working to ensure quality by directly checking the effects of protocols with other DeFi project developers who work together. |

# 3. Analysis of risks and risk mitigation measures in a decentralized financial system

## 3-2 Risks in System Development

| Main Items | Sub Items | Risk Events | Possible Risk Factors | Risk Mitigation Measures (Proposal) | Notes |
|---|---|---|---|---|---|
| DeFi Protocol | Defects in some functions of DeFi protocol (Lack of consideration of when gas prices soar) | ✓ The sudden spike in gas prices prevents the DeFi project's clearing process, etc. from operating properly and interrupts business processing (Keeper transactions cannot keep up with the spike in gas prices). | ✓ Developers are not taking into account that some DeFi protocols try to keep up with gas prices for their own transactions in the event of a sudden gas price spike | ✓ Apply Ethereum and 2nd Layer scaling technology to create a mechanism that does not cause sudden gas price spikes | ✓ The following scaling measures are planned and implemented<br>✓ Use of Ethereum 2.0 (sharding, planned)<br>✓ Use of layer 2 Solutions<br>✓ Use of Side Chains |
| | Defects in some functions of DeFi protocol (Lack of zero bidding prevention) | ✓ Zero-bid processing drains funds while the original process is stuck due to soaring gas prices. | ✓ Developers are not incorporating processes to prevent transactions that are not supposed to occur, such as zero bidding in some DeFi protocols. | ✓ Set a minimum amount in the DeFi protocol to prevent zero bidding.<br>✓ The problem that the bidding function didn’t work as it can be solved by taking measures for when gas prices rise. | ✓ Maker set the minimum bid at 3% of the original price. |

# 3. Analysis of risks and risk mitigation measures in a decentralized financial system

## 3-2 Risks in System Development

| Main Items | Sub Items | Risk Events | Possible Risk Factors | Risk Mitigation Measures (Proposal) | Notes |
|---|---|---|---|---|---|
| DeFi Protocol | Interlocking between DeFi protocols | ✓ Interlocking between DeFi protocols can be exploited to break assumptions made by external factors (e.g., Oracle pricing)<br>✓ Huge sums of money borrowed through Flash Loan (unsecured and unlimited) are put into liquidity pools of other DeFi protocols, causing a sudden change in the price of Oracles<br>✓ If the market price of a specific external DeFi protocol is referenced in the Oracle, manipulating the price of that specific protocol will cause the Oracle price to fluctuate. | ✓ DeFi protocol does not set a cap on the amount of transactions (e.g., the amount deposited in the liquidity pool)<br>✓ The DeFi protocol is not designed to be linked from various DeFi projects. | ✓ Considering that DeFi protocols are linked from various external DeFi protocols, it is considered necessary to test and validate for self-protection<br>✓ Test validation methods should be included in the code vulnerability measures. | ✓ Need to consider ways to reach out to blockchain management organizations |

# 3. Analysis of risks and risk mitigation measures in a decentralized financial system

## 3-3 Risks in Governance

| Main Items | Sub Items | Risk Events | Possible Risk Factors | Risk Mitigation Measures (Proposal) | Notes |
|---|---|---|---|---|---|
| Governance Voting | Not enough for a quorum to vote | ✓ Quorum for governance voting is low and decisions are made by a minority opinion (very low quorum of 1-4% for major DeFi projects) | ✓ Low turnout for the governance voting, which may have resulted in a smaller quorum for the proposal to pass. | ✓ Increase to the originally desired quorum as turnout for governance voting increases. | ✓ Instruct the governing body to establish rules to maintain an appropriate turnout and quorum so that governance voting is not biased in favor of a few opinions.<br>✓ Guidance to the governing body should be provided by the blockchain governing body |
| | Low voter turnout | ✓ Low turnout for governance voting, with decisions being made by a small percentage of voters (extremely low turnout for major DeFi projects, about 2-9%) | ✓ Governance tokens are valuable and speculative in the crypto-asset market, so speculative token holders are less willing to vote | ✓ Improve incentives for governor token holders to vote, such as voting mandate mechanisms and token grants for voting | ✓ Instruct the governing body to establish rules to maintain an appropriate turnout and quorum so that governance voting is not biased in favor of a few opinions.<br>✓ Guidance to the governing body should be provided by the blockchain governing body |

# 3. Analysis of risks and risk mitigation measures in a decentralized financial system

## 3-3 Risks in Governance

| Main Items | Sub Items | Risk Events | Possible Risk Factors | Risk Mitigation Measures (Proposal) | Notes |
|---|---|---|---|---|---|
| Governance Voting | Verification of malicious proposals | ✓ In the event of a malicious proposal, since verification is dependent on the cooperation of community members, there is a concern that no one will be able to detect a malicious proposal because the role of conducting verification is not clear. | ✓ In decentralized organizations, communities are free to participate and roles are not specified.<br>✓ It is unclear whether verification will be ensured for malicious proposals | ✓ The role of the governing body should include an explicit proposal verifier (preferably paid). Or consider proposal verification through formal verification, etc.<br>✓ Set appropriate working periods (proposal time locks) to validate malicious proposals. | ✓ Guidance to establish rules for the governing body regarding the role of the verifier of the proposal and disclosure of its contents.<br>✓ Guidance to the governing body should be provided by the blockchain governing body |
| | Dependency on smart contract modifications | ✓ When a governance voting proposal modifies a smart contract, most governance voting participants do not understand the content of the smart contract code and assume that it will act correctly according to the proposal | ✓ Only a small percentage of governance voting participants are technically capable of interpreting smart contracts<br>✓ Insufficient disclosure of information on the contents of the proposal, and there is a concern that the legitimacy of the proposal cannot be guaranteed. | ✓ The role of the governing body should include disclosing the contents of the smart contract to the voters for the verifier or the proposal (to check for any discrepancies with the proposal). | ✓ Same as above |

# 3. Analysis of risks and risk mitigation measures in a decentralized financial system

## 3-4 Risks in engagement with financial markets

| Main Items | Sub Items | Risk Events | Possible Risk Factors | Risk Mitigation Measures (Proposal) | Notes |
|---|---|---|---|---|---|
| Relationship with Financial Institutions | Risk of loss to financial institutions | ✓ Potential for financial institutions that connect with DeFi applications to trade crypto-assets to incur losses during market price declines or incidents | ✓ Risk of loss associated with the use of DeFi protocols, which may have latent vulnerabilities, and with holding volatile crypto-assets | ✓ Perform verification on the reliability of the DeFi protocol.<br>✓ Set asset allocations and maximum amounts considering the volatility of crypto-assets | ✓ crypto-assets are highly volatile, and the risk of theft of funds due to attacks, etc. must be taken into account |
| Corporate Relations | Risk of corporate loss | ✓ The possibility that companies that have invested in crypto-assets, including governance tokens, may suffer losses as a result of price declines. | | | |
| Smart Contract | Market stability | ✓ The price decline of a specific crypto-asset will automatically cascade to other crypto-assets through smart contracts, destabilizing the market as a whole. | ✓ Smart contracts automatically execute transactions according to code, but do not incorporate mechanisms to stabilize financial markets (e.g., functions to prevent propagation of effects). | ✓ Consider market stabilization functions, such as ripple effect of price volatility chain prevention, to prevent unforeseen events from affecting the financial markets. | ✓ Possible market stabilizing functions for crypto-assets include<br>✓ Ability to reflect Oracle prices moderately in sudden price changes<br>✓ The function to suppress the reflection of Oracle prices when price fluctuations exceed the base amount, etc. |